

교육기관

개인정보 보호 법령 모음집



KERIS

한국교육학술정보원
KOREA EDUCATION AND RESEARCH INFORMATION SERVICE

개인정보보호부



교육기관을 위한
개인정보 보호 법령
모음집

모음집 활용 안내

본 모음집은 교육기관에서 개인정보 보호법과
관련 법령의 내용을 한 눈에 볼 수 있도록
모은 자료로 안전한 개인정보 보호에 활용하시기 바랍니다.



CONTENTS

I	개인정보 보호 법령 요약본	
	1. 자체 제작 요약본	7
II	개인정보 보호법 및 시행령	
	1. 개인정보 보호법	77
	2. 개인정보 보호법 시행령	133
III	개인정보 보호법 관련 고시	
	1. 개인정보의 안전성 확보조치	197
	2. 표준 개인정보 보호지침	205
	3. 개인정보 보호책임자 경력 인정에 관한 고시	233
	4. 개인정보 보호법 위반에 대한 과징금 부과 기준	235
	5. 가명정보의 결합 및 반출 등에 관한 고시	242
	6. 개인정보 국외 이전 운영 등에 관한 규정	255
	7. 개인정보 처리 방법에 관한 고시	265
	8. 개인정보 처리방침 평가에 관한 고시	277
	9. 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시	282
	10. 개인정보 보호수준 평가에 관한 고시	343
	11. 개인정보 영향평가에 관한 고시	346
	12. 개인정보 전송 방법 및 개인정보관리 전문기관..고시안	375
	13. 보건의료 분야 정보전송자 및 전송 요구 정보.. 고시안	395
IV	교육분야 등 관련 서식 등 참고자료	
	1. 교육부 개인정보 보호지침	399
	2. 교육분야 개인정보 유출사고 대응 매뉴얼	406
	3. (학년초) 개인정보 처리 유의사항	447
	4. 개인정보보호 현장 실태점검 체크리스트	455
	5. 표준 내부관리계획	479

Chapter

I

교육기관을 위한 개인정보 보호 법령 요약본



본 문서는 2024.12.02. 기준 개인정보 보호법과 시행령 및 관련 고시와 가이드라인을 내용 별로 정리한 문서입니다. 오타 제보 받습니다. (ywkim100@gmail.com)

개인 업무·학습 및 교육용으로 사용이 가능하고 상업 목적으로 사용을 제한합니다.

법	시행령	안전성확보 조치 기준	기타 고시	표준지침	결합/이전고시	가이드
---	-----	----------------	-------	------	---------	-----

제1장 총칙		
2	용어의 정의	
	개인정보	살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보 가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보 나. 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보(결합과 입수가능성은 시간/비용/기술을 합리적 고려) 다. 가/나목의 내용을 가명처리를 통해 원래의 상태로 복원하기 위한 추가정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보
	가명처리	개인정보 일부를 삭제, 일부/전부 대체 등의 방법으로 추가 정보 없이는 특정 개인 식별이 불가하게 처리하는 것
	처리	개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공,공개, 파기, 그 밖에 이와 유사한 행위
	정보주체	처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람
	개인정보파일	개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물
	개인 정보 처리자	업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등
	공공기관	다음 각목의 기관을 말함 가. 국회, 법원… 행정사무를 처리하는 기관, 중앙행정기관 및 그 소속 기관, 지방자치단체 나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관 1. 국가인권위원회 1의2. 고위공직자범죄수사처 2. 공공기관의 운영에 관한 법률 제4조에 따른 공공기관 3. 지방공사와 지방공단 4. 특별법에 따라 설립된 특수법인 5. 초·중등교육법, 고등교육법, 그 밖의 다른 법률에 따라 설치된 각급 학교
	고정형 영상정보 처리기기	일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치 가. 일정한 공간에 설치된 카메라를 통하여 지속적 또는 주기적으로 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정장소에 전송하는 장치 나. 가목에 따라 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치
	네트워크 카메라	일정한 공간에 지속적으로 설치된 기기로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통해 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치
	고정형영상정보처리기기 운영자	법 제25조제1항 각 호에 따라 고정형 영상정보처리기기를 설치·운영하는 자

이동형 영상정보 처리기기		사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치하여 사람 또는 사물의 영상등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치
	착용	안경 또는 시계 등 사람의 신체 또는 의복에 착용하여 촬영하거나 촬영 영상을 수집·저장 또는 전송하는 장치
	휴대	휴대전화기 또는 디지털카메라 등 사람이 손쉽게 휴대하면서 촬영/촬영 영상을 수/저/전송하는 장치
	부착·거치	차량이나 무인항공기 등 이동 가능한 물체에 고정적으로 부착 또는 거치하여 촬영/영상을 수/저/전송하는 장치
이동형영상정보처리기기 운영자		법 제25조의2제1항 각 호에 따라 업무를 목적으로 이동형 영상정보처리기기를 운영하는 자
개인정보 처리시스템	데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성된 시스템	
이용자	정보통신망법 제2조제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자	
접속기록	개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신 가능한 상태 계정, 접속일시(년월일,시분초), 접속지 정보(접속한자의 단말기 정보 또는 IP주소 등) 처리한 정보주체 정보(이름, ID 등), 수행업무(수집, 생성, 연계, 검색, 출력, 정정, 복구, 공개, 이용, 제공, 파기 등)	
정보통신망	전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계	
P2P(Peer to Peer)	정보통신망을 통해 서버의 도움없이 개인과 개인이 직접 연결되어 파일을 공유하는 것	
공유설정	컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것	
모바일 기기	무선망을 이용할 수 있는 스마트폰, 태블릿 컴퓨터 등 개인정보 처리에 이용되는 휴대용 기기	
비밀번호	정보주체 및 개인정보취급자 등이 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열(타인에게 공개X 정보)	
생체정보	지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보	
생체인식정보	생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보	
인증정보	개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속을 요청하는 자의 신원을 검증하는데 사용되는 정보	
내부망	인터넷망 차단, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간	
위험도 분석	개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위	
보조저장매체	이동형 하드디스크(HDD), 유에스비(USB)메모리 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체	
친목단체	학교, 지역, 기업, 인터넷 커뮤니티 등을 단위로 구성되는 것으로서 자원봉사, 취미, 정치, 종교 등 공통의 관심사나 목표를 가진 사람간의 친목도모를 위한 각종 동창회, 동호회, 향우회, 반상회 및 동아리 등의 모임	
개인정보 보호책임자	개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항 또는 제3항에 해당하는 자	

	개인정보 취급자	개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등
	개인영상정보	법 제2조제1호에 따른 개인정보 중 고정형 또는 이동형 영상정보처리기에 의해 촬영·처리되는 영상 형태의 개인정보
	공개된 장소	공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 또는 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소 (학교 운동장, 교실 복도는 공개된 장소이며, 교실, 기술사 복도 등은 비공개된 장소)
3	개인정보보호원칙	<p>개인정보 처리 목적을 명확하게 하여야 하고 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집</p> <p>개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용 불가</p> <p>개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장</p> <p>개인정보의 처리 방법/종류에 따라 정보주체의 권리가 침해받을 가능성, 위험 정도를 고려하여 안전하게 관리</p> <p>개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장</p> <p>정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리</p> <p>개인정보의 익명처리를 우선적으로 고려하고 목적달성이 어려울 경우 가명에 의하여 처리</p> <p>이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수/실천함으로써 정보주체의 신뢰를 얻기 위하여 노력</p>
4	정보주체의 권리	<p>개인정보의 처리에 관한 정보를 제공받을 권리</p> <p>개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리</p> <p>개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다) 및 전송을 요구할 권리</p> <p>개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리</p> <p>개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리</p> <p>완전히 자동화된 개인정보 처리에 따른 결정을 거부하거나 그에 대한 설명 등을 요구할 권리</p>
5	국가 등의 책무	<p>국가/자치단체는 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등 피해를 방지로 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구해야함</p> <p>국가/자치단체는 정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책을 마련해야함</p> <p>국가/자치단체는 만 14세 미만 아동이 개인정보 처리가 미치는 영향 및 권리 등을 명확하게 알 수 있도록 개인정보 보호에 필요한 시책을 마련해야함</p> <p>국가/자치단체는 개인정보의 처리의 불합리한 사회적 관행을 개선하기 위하여 개인정보처리자의 자율적인 개인정보 보호활동을 존중하고 촉진·지원해야함</p> <p>국가/자치단체는 개인정보의 처리에 관한 법령 또는 조례를 적용할 때에는 정보주체의 권리가 보장될 수 있도록 개인정보 보호 원칙에 맞게 적용해야함</p>
6	다른 법률과의 관계	개인정보의 처리 및 보호에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따름

제2장 개인정보 보호정책의 수립 등

7	개인정보 보호위원회	<p>개인정보보호 사무를 독립적 수행을 위해 국무총리 소속으로 개인정보 보호위원회 구성</p> <p>정부조직법 제2조에 따른 중앙행정기관으로 본다.</p> <p>법 제7조의8 제3호, 제4호와 제7조의9 제1항의 제1호는 정부조직법 제18조를 적용하지 않음</p>
---	------------	---

7-2	보호위원회의 구성 등	
	상임위원 2명(위원장 1명, 부위원장1명)을 포함한 9명의 위원으로 구성	
	대통령은 아래의 제청 및 추천으로 보호위원회 위원을 임명 또는 위촉	
	위원 위촉 인원 (총 9명)	위원장과 부위원장은 국무총리의 제청으로 2명, 위원장의 제청으로 2명 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로 2명, 그 외의 교섭단체 추천으로 3명
	위원의 경력 조건	1. 개인정보보호 업무 담당 3급 이상 공무원 경력 2. 판사·검사·변호사의 직에 10년 이상 경력 3. 공공기관 또는 단체(처리자로 구성된 단체 포함)에 3년 이상 임원으로 재직하였거나 이들 기관 또는 단체로부터 추천받은 사람으로 개인정보보호 업무를 3년 이상 담당 4. 개인정보 관련 분야에 전문지식이 있고 고등교육법 제2조제1호에 따른 학교에서 부교수 이상 5년 경력
7-3	위원장	
	보호위원회를 대표하고, 회의를 주재하며, 소관 사무를 총괄	
	부위원장은 위원장 부재시 직무를 대행하고 위원장/부위원장 부재시 위원회가 미리 정하는 위원이 위원장의 직무를 대행	
	위원장은 국회에 출석하여 소관 사무에 관해 의견을 진술 할 수 있고, 국회에서 요구하면 출석하여 보고하거나 답변해야함	
	위원장은 국무회의에 출석하여 발언할 수 있으며 그 소관 사무에 관해 국무총리에게 의안 제출 건의 가능	
7-4	위원의 임기	
	위원의 임기는 3년, 한 차례만 연임 가능 위원 궐위된 때에는 지체없이 새로운 위원을 임명 또는 위촉해야하며 임기는 새로 개시	
7-5	위원의 신분보장	
	위원은 다음 사항을 제외하고는 그 의사에 반하여 면직 또는 해촉되지 아니함	
	1. 장기간 심신장애로 직무 수행 불가능 2. 제7조의7(결격사유)에 해당하는 경우 3. 이 법 또는 그 밖의 다른 법률에 따른 직무상의 의무를 위반한 경우	
	위원은 법률과 양심에 따라 독립적으로 직무를 수행	
7-6	겸직금지 등	
	위원은 재직 중 다음 직을 겸하거나 직무와 관련된 영리업무*에 종사 금지. 정치활동 관여 금지	
	1. 국회의원 또는 지방의회의원 2. 국가공무원 또는 지방공무원 3. 그 밖에 대통령령으로 정하는 직 (현재 없음)	
	보호위원회 위원은 영리 목적으로 다음 업무에 종사 금지	
	1. 법 제7조의9제1항에 따라 보호위원회가 심의·의결하는 사항과 관련된 업무 2. 법 제40조제1항에 따라 개인정보 분쟁조정위원회가 개인정보에 관한 분쟁 조정하는 사항과 관련된 업무	
7-7	결격사유	
	결격사유	1. 대한민국 국민이 아닌 사람 2. 국가공무원법 제33조 각 호의 해당하는 사람 3. 정당법 제22조에 따른 당원
	당연 퇴직 사항	국가공무원법 제33조제2호 파산선고를 받은 사람으로서 면책신청을 하지 않거나 면책불허가 또는 면책취소 확정
		국가공무원법 제33조제5호, 형법 제129조부터 제132조까지, 성폭력법 제2조, 아동청소년 보호법 제2조제2호 등

7-8	보호위원회의 소관 사무
	1. 개인정보 보호와 관련된 법령의 개선 2. 개인정보 보호와 관련된 정책·제도·계획 수립, 집행 3. 정보주체의 권리침해에 대한 조사 및 이에 따른 처분 4. 개인정보 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁의 조정 5. 개인정보 보호를 위한 국제기구 및 외국의 개인정보 보호기구와의 교류·협력 6. 개인정보 보호에 관한 법령·정책·제도·실태 등의 조사·연구, 교육 및 홍보 7. 개인정보 보호에 관한 기술개발의 지원·보급, 기술의 표준화 및 전문인력의 양성 8. 이 법 및 다른 법령에 따라 보호위원회 사무로 규정된 사항
7-9	보호위원회의 심의·의결 사항 등
	개인정보 침해요인 평가, 기본계획(제9조) 및 기본계획에 따른 시행계획, 개인정보 보호와 관련된 정책, 제도 및 법령의 개선
	개인정보의 처리에 관한 공공기관 간의 의견조정, 개인정보 보호에 관한 법령의 해석·운용
	개인정보의 목적외 이용·제공(제18조제2항제5호), 국외이전 중지 명령(제28조의9) , 영향평가 결과(제33조제4항) 제64조의2에 따른 과징금 부과
	개인정보 보호에 영향을 미치는 내용이 포함된 법령이나 조례에 대한 의견제시 및 개선권고(제61조) 제63조의2(사전 실태점검)에 따른 시정권고에 관한 사항
	개인정보 침해 근거가 있고 피해 발생 우려시 위반한 자에게 행위 중지, 정지 및 그 밖에 필요한 조치에 대한 시정조치 실시(제64조)
	범죄협조에 대한 고발, 개인정보 보호 관련 위반행위에 대한 책임자 징계 권고 등(제65조)에 따른 고발 및 징계권고
	개선권고, 시정조치 명령, 고발 및 징계권고, 과태료 부과에 대한 결과 공표(제66조) 및 공표 명령
	제75조에 따른 과태료 부과
	소관 법령 및 보호위원회 규칙의 제정·개정 및 폐지에 관한 사항
	개인정보 보호와 관련하여 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항
	그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의·의결하는 사항
	심의·의결하기 위해 관련 관계 공무원, 관련 전문가/단체 및 사업자로부터 의견 청취, 관계 기관 등에 대한 자료 제출이나 사실조회 요구
	요구받은 관계 기관 등을 특별한 사정이 없으면 이에 따라야 함
	개인정보 보호 관련 정책/제도/법령의 개선 사항을 심의·의결한 경우 개선 권고 가능, 개선 권고시 그 권고의 내용 이행 여부를 점검 가능
	위원회는 권고시 그 내용과 사유 등을 함께 통보해야 함
	권고내용의 이행여부 점검하기 위해 관계 기관에 권고사항의 이행결과에 대한 자료 제출을 요청 가능
	보호위원회는 제7조의9 제1항에 따른 심의·의결 사항에 대해 사전에 전문적인 검토를 위한 분야별 전문위원회를 둘 수 있음
	전문위원회 분야 : 개인정보의 국외 이전 분야, 그 밖에 보호위원회가 필요하다고 인정하는 분야
	각 전문위원회는 위원장 1명을 포함한 20명 이내의 위원으로 성별을 고려하여 구성
	전문위원회 위원장은 보호위원회 위원장이 전문위원회 위원 중에서 지명
	전문위원회 위원은 다음 사람 중에서 보호위원회 위원장이 임명하거나 위촉
	보호위원회 위원
	개인정보 보호 관련 업무를 담당하는 중앙행정기관의 관계 공무원
	개인정보 보호에 관한 전문 지식과 경험이 풍부한 사람
	개인정보 보호와 관련된 단체 또는 사업자단체에 속하거나 그 단체의 추천을 받은 사람

전문위원회의 구성 및 운영 등에 필요한 사항은 보호위원회의 의결을 거쳐 보호위원회 위원장이 정함	
정책의 일관성 있는 추진과 관련 사항에 대한 관계 중앙행정기관 간 협의를 위한 개인정보 보호 정책협의회 둘 수 있음	
협의 사항	법 제9조에 따른 개인정보 보호 기본계획 및 법 제10조에 따른 시행계획 등 개인정보 보호와 관련된 주요 정책
	개인정보 보호와 관련된 주요 법령의 제·개정
	개인정보 보호와 관련된 주요 정책의 협력 및 의견조정
	개인정보 침해사고 예방 및 대응
	개인정보 보호 기술개발 및 전문인력의 양성
	그 밖에 개인정보 보호와 관련하여 관계 중앙행정기관 간 협의가 필요한 사항
정책협의회는 관계 중앙행정기관의 고위공무원단에 속하는 공무원 또는 그에 상응하는 공무원으로서 개인정보 보호 관련 업무 담당자 중 소속기관의 장이 지명하는 사람으로 구성하되 정책협의회 의장은 보호위원회의 부위원장이 함	
정책협의회는 업무 수행을 위해 필요시 실무협의회 또는 분야별 협의회 구성 가능	
실무협의회 및 분야별 협의회 의장은 보호위원회 소속 공무원 중에서 의장이 임명	
실무협의회 및 분야별 협의회는 업무 수행을 위해 필요시 관계기관·단체 및 전문가 등에게 출석, 자료 또는 의견 제출 등 필요한 협조 요청 가능	
정책협의회의 운영 등에 필요한 사항은 정책협의회 의결을 거쳐 의장이 정함	
가명정보의 결합체계와 관련하여 가명정보 결합체계 협의회를 보호위원회에 둔다	
개인정보의 가명처리 및 가명정보 결합체계 연구 및 개선에 관한 사항	
가명정보의 결합과 관련한 개인정보 보호·활용에 필요한 사항	
결합전문기관의 지정·재지정 및 지정 취소에 관한 사항	
결합전문기관의 관리·감독에 관한 사항	
그 밖에 가명정보 제도 운영 등에 관하여 협의가 필요한 사항	
가명정보 결합체계 협의회는 개보위, 관계 중앙행정기관의 장(이하 중행장)의 가명정보 결합 등에 관한 업무를 담당하는 부서의 장으로 구성	
개인정보 보호 정책의 효율적 추진과 자율적 강화를 위해 시·도 개인정보보호 관계기관협의회를 둘 수 있음	
협의회 내용	시·도 개인정보 보호 정책
	관계 기관·단체 등의 의견 수렴 및 전달, 개인정보 보호 우수사례 공유
	그 밖에 개인정보 보호와 관련하여 시·도협의회 협의가 필요한 사항
	기타 시·도협의회 구성 및 운영 등에 필요한 사항은 시·도의 조례로 정함
보호위원회, 전문위원회 또는 정책협의회 출석 위원, 법 제7조의9 제2항에 따라 출석자, 전문위원회 및 정책협의회 출석자는 경비 지급 가능	
7-10	회의
회의는 위원장이 필요하다고 인정하는 경우, 재적위원 4분의 1 이상의 요구가 있는 경우 위원장이 소집	
위원장 또는 2명 이상의 위원은 보호위원회에 의안을 제의할 수 있음	
회의는 재적위원 과반수의 출석으로 개의하고 출석위원 과반수의 찬성으로 의결	
7-11	위원의 제척·기피·회피
위원의 제척·기피·회피 가능한 경우	위원 또는 배우자/전 배우자가 사안의 당사자이거나 사건 관련 권리자 또는 의무자 관계에 있는 경우
	사안의 당사자와 친족이거나 친족이었던 경우
	사안에 관해 증언, 감정, 법률자문을 한 경우
	사안에 관해 당사자의 대리인으로서 관여하거나 관여하였던 경우
	위원이나 위원이 속한 공공기관·법인 또는 단체 등이 조언 등 지원을 하고 있는 자와 이해관계가 있는 경우

위원에게 공정을 기대하기 어려운 사정이 있는 경우 당사자는 기피신청 가능, 위원회는 의결로 기피신청 결정			
위원이 상기 사유가 있는 경우 해당 사안에 대해 회피 가능			
7-12	소위원회 효율적 업무수행을 위해 개인정보 침해 정도가 경미하거나 유사·반복되는 사항 등을 심의·의결할 소위원회 운영 가능 3명의 위원으로 구성 소위원회가 심의·의결한 것은 보호위원회가 심의·의결한 것으로 본다 소위원회 회의는 전원의 출석과 출석위원 전원의 찬성으로 의결		
7-13	사무처 사무를 처리하기 위해 보호위원회는 사무처를 두며, 이 법 규정 이외 보호위원회 조지기에 관한 사항은 대통령령으로 정함		
7-14	운영 등 이 법과 다른 법령에 규정된 것 외에 보호위원회의 운영 등에 필요한 사항은 보호위원회의 규칙으로 정함		
8-2	개인정보 침해요인 평가 중앙행정기관의 장은 개인정보 처리가 수반하는 소관 법령 제정 또는 개정시 보호위원회에 개인정보 침해요인 평가를 요청해야 함 보호위원회는 요청을 받으면 분석·검토하여 그 법령의 소관기관의 장에게 개선 필요 사항을 권고할 수 있음 개인정보 침해요인 평가의 절차와 방법은 대통령령으로 정함		
	중앙행정기관의 장은 개인정보 침해요인 평가 요청시 관련 요청서를 보호위원회에 제출해야함 <table border="1"> <tr> <td>요청서 포함내용</td><td> 1. 법령을 통해 도입되거나 변경되는 개인정보 처리를 수반하는 정책·제도의 목적과 주요 내용 2. 개인정보 처리 정책·제도의 도입·변경에 따른 개인정보 침해요인 자체 분석* 3. 개인정보 처리 정책·제도의 도입·변경에 따른 개인정보 보호 대책 </td></tr> </table> 보호위원회는 [필요성, 권리보장 적정성, 안전성 등]을 고려하여 그 결과를 중행장에게 통보해야함 중행장은 개선 권고를 받은 경우 권고내용을 이행하도록 노력해야 하며 이행이 곤란한 경우 사유를 통보해야 함 위원회는 침해요인 평가를 위해 필요한 자료 등을 해당 중행장에게 요청 가능 위원회는 침해요인 평가 세부기준 및 방법 등 침해요인 평가에 필요한 지침을 수립하여 중행장에게 통보 가능 위원회는 침해요인 평가 실시를 위해 필요시 관계 전문가에게 자문 등을 할 수 있음	요청서 포함내용	1. 법령을 통해 도입되거나 변경되는 개인정보 처리를 수반하는 정책·제도의 목적과 주요 내용 2. 개인정보 처리 정책·제도의 도입·변경에 따른 개인정보 침해요인 자체 분석* 3. 개인정보 처리 정책·제도의 도입·변경에 따른 개인정보 보호 대책
요청서 포함내용	1. 법령을 통해 도입되거나 변경되는 개인정보 처리를 수반하는 정책·제도의 목적과 주요 내용 2. 개인정보 처리 정책·제도의 도입·변경에 따른 개인정보 침해요인 자체 분석* 3. 개인정보 처리 정책·제도의 도입·변경에 따른 개인정보 보호 대책		
9	기본계획 보호위원회는 3년마다 개인정보 보호 기본계획을 관계 중앙행정기관의 장과 협의하여 수립 <table border="1"> <tr> <td>기본계획 내용</td><td> 기본목표/추진방향, 제도·법령 개선, 침해방지 대책, 자율규제의 활성화, 교육·홍보의 활성화, 전문인력 양성 등 </td></tr> </table> 국회, 법원, 헌법재판소, 중앙선거관리위원회는 해당 기관의 개인정보 보호를 위한 기본계획을 수립·시행 가능 보호위원회는 3년마다 시작되는 해의 전년도 6월 30일까지 수립해야 함	기본계획 내용	기본목표/추진방향, 제도·법령 개선, 침해방지 대책, 자율규제의 활성화, 교육·홍보의 활성화, 전문인력 양성 등
기본계획 내용	기본목표/추진방향, 제도·법령 개선, 침해방지 대책, 자율규제의 활성화, 교육·홍보의 활성화, 전문인력 양성 등		
10	시행계획 중행장은 기본계획에 따라 매년 9월 30일까지 다음 해 시행계획을 작성, 보호위원회에 제출하고 보호위원회는 제출된 시행계획을 12월 31일까지 심의/의결해야 함 보호위원회는 매년 6월 30일까지 다음 해 시행계획의 작성 방법 등에 관한 지침을 마련하여 중행장에게 통보 중행장은 통보된 지침에 따라 기본계획 중 다음 해에 시행할 소관 분야의 시행계획을 작성하여 매년 9월 30일까지 보호위원회 제출		

11	자료제출 요구 등	
	위원회는 개인정보처리자의 법규준수 현황과 개인정보 관리 실태 등에 관한 자료 제출, 의견 진술 등을 요구 가능	
	기본계획을 효율적으로 수립·추진 하기 위해 필요한 최소한의 범위로 한정하여 요구해야 함	
	위원회는 개인정보관리 수준 및 실태파악 등을 위한 조사 실시 가능	
	중행장은 시행계획 수립 및 추진을 위해 소관 분야의 개인정보처리자에게 자료제출 등을 요구 가능	
	기본계획을 효율적으로 수립·추진 하기 위해 필요한 최소한의 범위로 한정하여 요구해야 함	
	위원회 또는 중행장으로부터 자료제출 등을 요구받은 자는 특별한 사정이 없으면 이에 따라야 함	
	위원회(또는 중행장)이 개인정보처리자에게 자료의 제출 또는 의견 진술 등을 요구할 수 있는 사항 개인정보/개인정보파일의 관리와 고정형 또는 이동형 영상정보처리기의 설치·운영에 관한 사항 개인정보 보호책임자의 지정 여부에 관한 사항 개인정보의 안전성 확보를 위한 기술적·관리적·물리적 조치에 관한 사항 정보주체의 개인정보 열람, 정정, 삭제, 처리정지의 요구 및 조치현황에 관한 사항 그 밖에 법 및 대통령령의 준수에 관한 사항 등 기본계획의 수립·추진을 위해 필요한 사항	
11-2	개인정보 보호수준 평가	
	보호위원회는 공공기관 중 중앙행정기관 및 그 소속기관, 지방자치단체, 대통령령으로 정하는 기관을 대상으로 매년 개인정보 보호 수준 평가해야 함	
	대상 기관	중앙행정기관 및 그 소속기관
		지방자치단체
		공공기관의 운영에 관한 법률 제4조에 따른 공공기관
		지방공기업법에 따른 지방공사와 지방공단
		특수법인, 대학 중 개인정보 처리 업무의 특성 등을 고려, 보호위원회가 고시하는 기준에 해당하는 기관을 정할 수 있음
		특별법에 의하여 설립된 특수법인과 고등교육법 제2조에 따른 대학 중에서 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 기관 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 기관 3년간 개인정보 유출 등 개인정보 침해사고 2회 이상 발생, 과징금 또는 과태료 처분 1회 이상 기관 기타 개인정보 처리 및 관리에 있어 개인정보 침해 우려가 크다고 판단되는 기관
		지정된 평가 대상은 최초 평가 준비기간을 고려하여 차년도부터 평가 실시, 3년간 평가
	수준 평가에 필요한 경우 해당 공공기관의 장에게 관련 자료 제출 요구 가능	
	수준 평가의 결과를 인터넷 홈페이지 등을 통해 공개 가능	
	결과에 따라 우수기관 및 직원에 대해 포상 가능, 보호를 위해 필요한 경우 공공기관의 장에게 개선 권고, 이행조치 및 결과를 보호위원회에 통보해야 함	
	세부 기준·방법·절차 및 자료 제출의 범위 등 필요한 사항은 대통령령으로 정함	
	평가 기준	1. 개인정보 보호 정책·업무 수행실적 및 개선 정도 2. 개인정보 관리체계의 적정성 3. 정보주체 권리보장을 위한 조치사항 및 이행 정도 4. 개인정보 침해방지 조치사항 및 안전성 확보 조치 이행 정도 5. 그 밖에 개인정보의 처리 및 안전한 관리를 위해 필요한 조치 사항의 준수 여부
		평가 시행전 평가대상, 평가기준·방법 및 평가지표 등을 포함한 평가계획을 마련하여 평가대상 기관의 장에게 통보해야 함

효율적 평가 실시를 위해 개인정보 보호 전문지식과 경험이 풍부한 전문가로 평가단을 구성·운영 가능	
평가관련 제출 자료 (최소한의 범위 한정)	<ol style="list-style-type: none"> 1. 평가대상기관이 개인정보 보호수준을 자체적으로 점검한 경우 그 결과 및 증명자료 2. 제1호의 증명자료의 검증에 필요한 자료 3. 그 밖에 개인정보의 안전한 관리 여부 등 개인정보 보호수준을 평가하기 위해 필요한 자료
평가대상기관의 장이 제출한 자료를 기준으로 평가를 진행하거나 평가대상기관을 방문하여 평가 가능	
보호위원회는 중행장 또는 지자체장에게 소속 기관 등 소관 분야 평가대상기관의 평가준비 or 평가결과에 따른 조치를 위해 필요사항 지원 요청 가능	
지원 요청을 받은 장은 특별한 사유가 없는 한 요청에 따른 지원을 하기 위해 노력해야 함	
보호위원회는 평가의 전문성·공정성 확보를 위해 평가단을 구성·운영 가능	
평가단은 단장 1명을 포함하여 보호위원회가 위촉하는 개인정보 관련 경력과 전문지식이 풍부한 전문가로 구성	
<ol style="list-style-type: none"> 1. 고등교육법 제2조에 따른 학교에서 조교수 이상 재직자로 개인정보보호 관련 경력 3년 이상 2. 개인정보 보호 또는 정보보안 분야에서 3년 이상 업무 경력을 갖춘 사람 3. 기타 개인정보 관련 분야에 경력과 전문지식이 풍부하다고 보호위원회가 인정하는 사람 	
평가단원의 임기는 위촉된 날부터 1년으로 하되 연임할 수 있으며, 단장 및 단원은 보호위원회 위원장이 위촉	
단원이 대상 기관과 직접적인 이해관계 또는 공정성이 어려운 현저한 사유가 있는 경우 평가에 관여 못함. 스스로 회피 가능	
평가단 업무	1. 평가 대상 제출자료에 대한 검증, 평가 및 적정성 여부 판단
	2. 평가 대상 현장검증 및 자문
	3. 평가 결과 평정
	4. 그 밖에 개인정보 보호수준 평가의 효율적 수행 및 개선을 위한 지원
보호위원회는 평가 결과에 따라 선정한 우수기관 또는 소속 직원에 대해 표창 수여, 포상금 지급 등의 우대조치 가능	
보호위원회는 평가 결과 하위 등급기관에 대해 현장 컨설팅 및 실태점검 실시 가능	
보호위원회는 중행장/지자체장에게 소속 기관·단체 등 소관 분야 공공기관에 대해 컨설팅, 교육, 기술지원 및 주기적 점검 등의 필요 사항 지원 요청 가능	
보호위원회는 평가 결과가 업무평가 등에 반영될 수 있도록 소관 기관의 장에게 평가 결과를 제공 가능	
12	개인정보 보호지침 보호위원회는 개인정보의 처리에 관한 기준 등에 관한 표준 개인정보 보호지침을 정하여 그 준수를 권장 가능
13	자율규제의 촉진 및 지원 보호위원회는 처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위한 필요한 시책을 마련해야 함 개인정보 보호 관련 교육·홍보, 기관·단체의 육성 및 지원, 개인정보보호 인증마크의 도입·시행 지원 처리자의 자율적인 규약의 제정·시행 지원 및 기타 자율적 개인정보보호활동을 지원하기 위해 필요한 사항
13-2	개인정보 보호의 날 매년 9월 30일을 개인정보 보호의 날로 지정, 국가/자치단체는 개인정보 보호의 날이 포함된 주간에 개인정보 보호 문화 확산을 위해 각종 행사를 실시 가능
14	국제협력 정부는 국제적 환경에서의 보호 수준 향상을 위해 또한 국외 이전으로 침해되지 않도록 필요한 관련 시책 마련

제3장 개인정보의 처리

제1절 개인정보의 수집, 이용, 제공 등

15	수집·이용 가능한 범위 (수집할 수 있으며, 수집 목적 범위에서 이용할 수 있다): <i>수집 및 이용하지 마라, 하지만 해당의 경우 그렇게 해도 처벌하지 않겠다</i>	
	정보주체의 동의를 받은 경우	
	법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우	
	공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우	
	정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위해 필요한 경우	
	명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우	
	사유가 해소된 경우 처리를 즉시 중단하고, 정보주체에게 사전 동의없이 수집·이용 사실과 그 사유 및 이용내역을 알려야 함	
	개인정보처리자의 정당한 이익 달성을 위해 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우 (정당한 이익과 관련성 및 합리적 범위 미초과)	
	공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우	
	수집시 고지사항(4가지)	
	수집·이용 목적, 항목, 보유 및 이용 기간, 거부권 및 거부에 따른 불이익 내용	
	당초 수집 목적과 합리적 관련 범위내 아래 조건을 고려하여 정보주체의 동의없이 개인정보 이용 가능 (정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려함)	
	동의없는 이용을 위한 고려사항	<ol style="list-style-type: none"> 1. 당초 수집 목적과 관련성이 있는지 여부 2. 개인정보를 수집한 정황과 처리 관행에 비추어 볼 때 추가적으로 이용 또는 제공이 예측 가능성 여부 3. 정보주체의 이익을 부당하게 침해하는지 여부 4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부
	개인정보의 추가적인 이용 또는 제공이 지속적으로 발생하는 경우 상기 판단기준을 처리방침에 공개하고, 보호책임자는 기준 준수 여부를 점검해야 함	
	명함, 인터넷 홈페이지 등에서 개인정보를 수집하는 경우 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용 가능	
	대리인을 통해 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인의 개인정보를 수집·이용 가능	
	근로자와 사용자가 근로계약 체결 시 "근로기준법"에 따른 임금 지급, 교육, 증명서 발급, 근로자 복지제공을 위해 동의없이 수집·이용 가능	
16	수집 제한	
	목적에 필요한 최소한의 개인정보를 수집. 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담	
	최소한의 정보 외의 개인정보 수집에는 동의 거부 가능함을 구체적으로 고지하고 수집	
	최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 서비스의 제공 거부 불가	
17	제3자 제공 (목적내 범위에서 제공하는 경우에 한함) 제3자 : 처리자를 제외한 모든 자를 의미하며, 대리인과 수탁자는 제외	
	가능한 경우	정보주체의 별도 동의를 받은 경우(국외의 제3자 제공시에도 별도 동의 필요)
		법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
		공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

	명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
	개인정보처리자의 정당한 이익 달성을 위해 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우
	공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우
	"제공"이란 저장매체나 출력물 등을 물리적 이전, 네트워크를 통한 전송, 제3자의 접근권한 부여, 처리자와 제3자의 개인정보 공유 등 개인정보의 이전 또는 공동 이용 상태를 초래하는 모든 행위
	"제3자"란 정보주체와 정보주체에 관한 개인정보를 수집·보유하고 있는 개인정보처리자를 제외한 모든 자를 의미
제3자 동의시 고지사항: (5가지)	제공받는 자 : 성명(법인 또는 단체는 그 명칭), 연락처 제공받는 자의 이용 목적, 제공하는 개인정보 항목, 제공받는 자의 보유 및 이용 기간, 거부권 및 불이익 사항
당초 수집 목적과 합리적 관련 범위내 아래 조건을 고려하여 정보주체의 동의없이 개인정보 제공 가능 (정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려함)	
동의없는 제공을 위한 고려사항	1. 당초 수집 목적과 관련성이 있는지 여부 2. 개인정보를 수집한 정황과 처리 관행에 비추어 볼 때 추가적으로 이용 또는 제공이 예측 가능성 여부 3. 정보주체의 이익을 부당하게 침해하는지 여부 4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부
	개인정보의 추가적인 이용 또는 제공이 지속적으로 발생하는 경우 상기 판단기준을 처리방침에 공개하고, 보호책임자는 기준 준수 여부를 점검해야 함
18	목적의 이용·제공 제한 처리자는 수집한 목적 범위를 초과하여 이용 금지 (제15조제1항의 범위) "제3자 제공이 가능한 경우" 라도 범위를 초과하여 제공 금지(제17조제1항 및 제28조의8제1항 [국외이전]의 범위) 다음 어느 하나에 해당하는 경우, 정보주체/제3자의 이익을 부당하게 침해 우려를 제외하고 목적 외의 용도로 이용·제3자 제공 가능 정보주체의 별도 동의를 받은 경우 (홈페이지 등에 공개 제외 가능) 다른 법률에 특별한 규정이 있는 경우 명백히 정보주체/제3자의 급박한 생명, 신체, 재산의 이익을 위해 필요하다고 인정되는 경우 사유 해소시 처리를 즉시 중단하고 정보주체에게 사전 동의없이 제공한 사실과 그 사유 및 이용내역을 알려야 함 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우 (공공기관은 5가지 경우도 추가 가능), 이 경우 민감/고유식별정보 해당 제외 가능 (영제18조/제19조단서) 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우 (홈페이지 등에 공개 제외 가능) 법원의 재판업무 수행을 위하여 필요한 경우 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

목적외 이용·제3자 동의시 고지사항

제공받는자(성명[법인등 명칭] 및 연락처), 제공받는자의 이용 목적(제공시에는 제공받는 자의 이용 목적), 제공하는 개인정보 항목, 개인정보의 보유 및 이용 기간(제공시에는 제공받는자의 보유 및 이용 기간), 거부권 및 불이익 사항

목적외 이용·제3자 제공시 보호위원회 고시에 따라 공고 (공공기관만 해당)

목적외 이용·제3자 제공한 날부터 30일 이내에 10일 이상 계속 관보나 인터넷 홈페이지 등에 게재해야 함

- | | |
|--------|---------------------------|
| (공개내용) | 1. 목적외이용등을 한 날짜 |
| | 2. 목적외이용등의 법적 근거 |
| | 3. 목적외이용등의 목적 |
| | 4. 목적외이용등을 한 개인정보의 항목(구성) |

목적외 제3자 제공하는 자는 제공받는 자에게

이용 목적, 이용방법, 기타 필요한 사항에 대해 제한하거나

개인정보의 안전성 확보를 위해 필요한 조치를 마련하도록 서면으로 요청

안전성 확보 조치 결과를 받지 못한 경우 최소한 1회 이상 결과 제출을 요청하는 행위 필요

목적외 제3자 제공시 개인정보의 안전성 확보조치

제공하는 자가 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대해 제한하거나 안전성 확보를 위해 필요한 구체적인 조치 마련을 문서로 요청

요청을 받은 자는 개인정보의 안전성 확보를 위해 필요한 조치를 하고 문서로 회신

제공하는 자는 제공받는 자와 개인정보의 안전성 확보조치 책임관계를 명확히 해야함

목적외 이용·제3자 제공시 대장 기록 관리 (공공기관의 경우)

1. 이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭
2. 이용기관 또는 제공받는 기관의 명칭
3. 이용 목적 또는 제공받는 목적
4. 이용 또는 제공의 법적 근거
5. 이용하거나 제공하는 개인정보의 항목
6. 이용 또는 제공의 날짜, 주기 또는 기간
7. 이용하거나 제공하는 형태
8. 제3자 제공시 제한하거나 필요한 조치를 마련할 것을 요청한 경우 그 내용

19 개인정보를 제공받은 자의 이용·제공 제한

정보주체의 별도 동의, 다른 법률에 특별한 규정이 있는 경우만 이용·제공 가능

20 정보주체 이외로부터 수집한 개인정보의 수집 출처 등 **통지**

정보주체 이외로부터 수집한 개인정보는 정보주체의 요구 시 해당 사항을 정보주체에게 통지해야 함

- | | |
|----------|---------------------------------------|
| 통지
사항 | 개인정보의 수집 출처, 개인정보의 처리 목적 |
| | 개인정보 처리의 정지를 요구하거나 동의를 철회할 권리가 있다는 사실 |

연락처 등 정보주체에게 알릴 수 있는 정보가 없을 경우는 통지 제외 가능

(정보주체 요구 및 처리자 요건에 따른 정보주체)

통지 예외 사항 : 정보주체의 권리보다 명백히 우선하는 경우로

통지로 인하여 타인의 생명·신체를 해할 우려시, 타인의 재산과 그 밖의 이익을 부당침해 우려시

통지를 요구하는 대상이 되는 개인정보가 보호위 등록 대상 제외되는 개인정보파일에 포함되어 있는 경우

정보주체의 요구시 3일 이내에 3개 항목을 정보주체에게 알려야 함. 거부시에는 3일 이내에 거부 근거와 사유를 정보주체에게 알려야 함	
거부대상 사항	1. 고지를 요구하는 대상이 되는 개인정보가 법령에서 등록 예외대상인 개인정보파일에 포함되어 있는 경우 2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산, 이익을 부당하게 침해할 우려가 있는 경우
정보주체가 요구를 하지 않아도 통지해야하는 개인정보처리자 요건	
대상 개인정보처리자	5만명 이상 민감정보·고유식별정보 처리하는 자 100만명 이상 개인정보를 처리하는 자
통지 예외 사항	법 제20조의2(개인정보 이용·제공 내역의 통지)에 따라 통지한 경우에 제외
통지 방법 및 시기	서면, 전자우편, 전화, 문자전송 등 정보주체가 쉽게 알 수 있는 방법으로 제공받은 날부터 3개월 이내에 알려야 함 재화 및 서비스 제공 과정에서 쉽게 알 수 있도록 알림창을 통해 알리는 방법으로 제공받은 날부터 3개월 이내에 알려야 함
통지 시기 제한	정보주체 직접 동의 받은 범위에서 연 2회 이상 주기적 처리 시 제공받은 날부터 3개월 이내 또는 동의받은 날부터 연 1회 이상
통지 내역 보관	통지대상 개인정보를 파기할 때까지 고지한 내역(알린 사실, 알린 시기, 알린 방법)을 보관·관리해야함

20-2 개인정보 이용·제공 내역의 통지

개인정보 보호법에 따라 수집한 개인정보의 이용·제공 내역이나 해당 내역을 확인할 수 있는 방법을 주기적으로 연 1회 이상 통지해야 함 (연락처 등 미수집 시 제외)	
※ 개보법이 아닌 다른 법률에 따라 수집한 개인정보에 대해서는 이용·제공 내역을 통지하지 않아도 됨	
대상 개인정보 처리자	저장·관리하고 있는 개인정보가 전년도말 기준 직전 3개월간 일일 평균 5만명 이상 민감정보·고유식별정보 처리하는 자 100만명 이상 개인정보를 처리하는 자
통지 예외 정보주체	1. 통지에 대한 거부의를 표시한 정보주체 2. 업무수행을 위해 소속된 임직원의 개인정보를 처리한 경우 해당 정보주체 3. 업무수행을 위해 다른 공공기관, 단체 등의 임직원 또는 개인의 연락처 등의 개인정보를 처리한 경우 해당 정보주체 4. 법률에 규정이 있거나 법령상 의무를 준수하기 위해 이용·제공한 개인정보의 정보주체 5. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위해 이용·제공한 개인정보의 정보주체
통지 항목	1. 개인정보의 수집·이용 목적, 수집한 개인정보 항목 2. 개인정보를 제공받는 자, 그 제공 목적, 제공한 개인정보의 항목 단, 통신비밀보호법 제13조, 제13조의2, 제13조의4 및 전기통신사업법 제83조제3항에 따라 제공한 정보(통신사실 확인서)는 제외
통지 방법	서면, 전자우편, 전화, 문자전송 등 정보주체가 쉽게 알 수 있는 방법 재화 및 서비스 제공 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법 (정보시스템 접속 방법 통지하는 경우로 한정)
통합 통지 가능한 내용	법 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 통지)에 따른 개인정보의 수집 출처 등 통지 법 제20조의2(개인정보 이용·제공 내역의 통지)에 따른 개인정보 이용·제공 내역의 통지 영 제42조의6 제13항에 따른 개인정보 전송 내역 통지 (시행일 2025.3.13.)

21	개인정보의 파기
보유기간의 경과, 개인정보의 처리 목적 달성, 가명정보의 처리기간 경과 등 그 개인정보가 불필요 시 지체 없이(5일 이내) 그 개인정보를 파기	
파기할 때에는 복구 또는 재생되지 아니하도록 조치해야 함	
개인정보를 파기하지 않고 보존하여야 하는 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리	
종류별 파기 방법	전자적 파일 형태인 경우
	복원이 불가능한 방법으로 영구 삭제
	기술적 특성으로 인해 상기 영구 삭제가 곤란한 경우 익명정보(법 제58조의2)로 처리, 복원이 불가능하도록 조치
	그 외 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 파쇄 또는 소각
파기 유형	완전파괴(소각, 파쇄 등)
	전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용한 삭제
	데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
부분 파기 방법	전자적 파일 형태 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
	기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제
	기술적 특성으로 상기 방법으로 파기가 곤란한 경우 법 제58조의2에 해당하는 정보로 처리, 복원이 불가능하도록 조치
개인정보 처리자는 파기에 관한 사항을 기록·관리해야 함, 개인정보 보호책임자는 파기 시행 후 파기 결과를 확인해야 함	
보존해야 하는 개인정보의 경우 물리적 또는 기술적 방법으로 분리하여 저장·관리 해야함	
분리 저장·관리 할 경우 개인정보처리방침 등을 통해 법령에 근거한다는 점을 정보주체가 알도록 고지 필요	
공공기관의 경우 공공기관의 개인정보파일 파기하는 경우 (표준지침 제55조 및 제56조 적용)	
개인정보파일의 보유기간 경과, 처리 목적 달성 등 불필요한 경우 지체없이 파기. 다른 법령에 따라 보존 시 파기 예외	
보유기간, 처리 목적 등을 반영한 개인정보 파기계획을 수립·시행 (내부 관리계획에 포함하여 시행 가능)	
취급자는 파기 사유가 발생한 개인정보파일을 선정하고 파기 요청서에 명칭, 파기 방법 등을 기재하여 책임자 승인을 받아 파기	
책임자는 개인정보 파기 시행 후 파기 결과를 확인하고 개인정보파일 파기 관리대장을 작성	
취급자는 개인정보파일을 파기한 경우 개인정보파일의 등록사실에 대한 삭제를 책임자에게 요청 (개인정보 파기는 해당 X)	
파일 등록의 삭제를 요청받은 책임자는 그 사실을 확인하고 지체없이 등록 사실 삭제 후 그 사실을 보호위원회에 통보	
22	동의를 받는 방법
각각의 동의사항 구분하여 명확하게 인지하도록 알리고 각각 동의 받아야 함, 동의 여부를 선택할 수 있다는 사실을 명확하게 알도록 구분하여 명시적 표시	
구분동의 사항	제15조제1항제1호(개인정보 수집·이용 정보주체 동의)에 따라 동의 받는 경우
	제17조제1항제1호(제3자 제공 정보주체 동의)에 따라 동의 받는 경우
	제18조제1항제1호(목적 외 이용·제공 정보주체 동의)에 따라 동의 받는 경우, (제공받는 자의 정보 추가로 고지 필요)
	제19조제1호(제공받은 자가 별도로 정보주체 동의)에 따라 동의 받는 경우, (제공받는 자의 정보 추가로 고지 필요)

제23조제1항제1호(민감정보 정보주체 동의)에 따라 동의 받는 경우	
제24조제1항제1호(고유식별정보 정보주체 동의)에 따라 동의 받는 경우	
재화나 서비스를 홍보하거나 판매를 권유하기 위해 동의를 받는 경우	
정보주체를 보호하기 위해 동의사항을 구분하여 동의를 받아야 할 필요가 있는 경우로 대통령령으로 정하는 경우 (현재 없음)	
제22조의2제1항(아동의 개인정보 보호)에 따른 만 14세 미만 아동의 개인정보 처리를 위해 법정대리인의 동의 받는 경우	
제28조의9제1항제1호(개인정보의 국외 이전)에 따른 국외 이전 목적으로 동의 받는 경우	
정보주체의 동의를 적법하기 위한 모두 조건	1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것 2. 동의 내용이 구체적이고 명확할 것 3. 평이하고 이해하기 쉬운 문구를 사용할 것 4. 정보주체에게 동의 여부에 대한 의사를 명확하게 표시할 수 있는 방법을 제공할 것
동의를 받는 방법	1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급 or 우편 또는 팩스 등의 방법 전달하고 정보주체 서명/날인 동의서 받기
	2. 전화를 통해 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 함
	3. 전화를 통해 동의 내용을 정보주체에게 알리고 인터넷주소 등을 통해 확인하도록 한 후 다시 통화로 동의 의사표시를 확인
	4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시
	5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받기
	6. 그 밖에 상기 규정에 따른 방법에 준하는 방법으로 내용을 알리고 동의의 의사표시를 확인
서면 동의를 받을 때는 중요내용 에 대해서는 명확히 표시하여 알아보기 쉽게 해야함 (보호위원회 고시로 정하는 방법에 따라 표시)	
중요내용의 표시방법	종이 인쇄물, 컴퓨터 표시화면 등 서면 동의를 요구하는 매체의 특성과 정보주체의 이용환경을 고려하여
	글씨의 크기 , 색깔, 굵기 또는 밑줄 등을 통해 그 내용을 명확히 표시
	동의사항이 많은 경우 중요한 내용이 쉽게 확인될 수 있게 그 밖의 내용과 별도로 구분하여 표시
중요내용	목적 재화나 서비스의 홍보 또는 판매 권유 등을 위한 연락할 수 있다는 사실
	항목 민감정보 항목, 고유식별정보 항목(주민등록번호 제외)
	기간 개인정보의 보유 및 이용기간(제공 시에는 제공받는 자의 보유 및 이용기간)
	제공 시 3자 제공시 제공받는 자와 제공받는 자의 목적
정보주체 동의없이 처리 가능 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여 처리방침에 공개하거나 서면등의 방법 *으로 알려야 함	
동의없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담	
* 서면등의 방법이란 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법을 말한다.	
동의없이 수집·수집할 수 있는 법적 근거 등을 정보주체에게 알리기 위해 노력해야 함 (동의없는 수집이라는 고지를 권고함)	
선택사항 미동의 또는 목적외 이용·제공 미동의 또는 재화 또는 서비스 홍보/판매 권유 미동의를 이유로 재화 또는 서비스 제공 거부 금지	

전화로 동의 수집시 통화내용을 녹취할 때 녹취사실을 정보주체에게 고지해야 함	
친목단체 운영을 위해 개인정보 수집시 정보주체의 동의없이 수집·이용 가능	
	<ol style="list-style-type: none"> 1. 친목단체 가입을 위한 성명 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항 2. 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부 현황에 관한 사항 3. 친목단체의 활동에 대한 구성원의 참석 여부 및 활동내용에 관한 사항 4. 기타 친목단체의 구성원 상호간 친교와 화합을 위해 다른 구성원에게 알리기 원하는 생일, 취향 등에 관한 사항
정보주체의 동의를 받기 위해 동의서를 작성하는 경우 [알기쉬운 개인정보 처리 동의 안내서]를 준수	
중행장은 적법한 동의 방법과 관련하여 소관 분야의 처리자별 업무, 업종의 특성 및 정보주체의 수 등을 고려하여 보호지침으로 정하여 권장 가능	

22-2 아동의 개인정보 보호

만 14세 미만 아동의 개인정보를 처리하기 위해 이 법에 따른 동의 시 법정대리인의 동의를 받아야 하며, 법정대리인의 동의 여부를 확인해야 함

정보주체의 동의를 적법 모두 조건	<ol style="list-style-type: none"> 1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것 2. 동의 내용이 구체적이고 명확할 것 3. 평이하고 이해하기 쉬운 문구를 사용할 것 4. 정보주체에게 동의 여부에 대한 의사를 명확하게 표시할 수 있는 방법을 제공할 것
법정대리인의 동의 여부를 확인하는 방법	<ol style="list-style-type: none"> 1. 동의내용 기재 사이트에 대리인이 동의여부를 표시하도록 하고 처리자가 그 동의 표시 확인용 문자메시지 알림 2. 동의내용 기재 사이트에 대리인이 동의여부를 표시하도록 하고 신용카드/직불카드 등 정보 제공 받는 방법 3. 동의내용 기재 사이트에 대리인이 동의여부를 표시하도록 하고 휴대전화 본인인증 등을 통해 본인여부 확인 4. 동의 서면을 직접 발급/우편/팩스로 전달하고 대리인이 동의내용에 서명날인 후 제출하는 방법 5. 동의내용을 전자우편을 발송해 대리인으로부터 동의 의사표시가 적인 전자우편을 전송받는 방법 6. 전화로 동의내용을 대리인에게 알리고 동의를 얻거나 인터넷주소 등 동의내용 확인 방법을 안내하고 재차 전화로 동의 7. 상기 방법에 준하는 방법으로 대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

수집 매체의 특성상 동의내용을 전부 표시가 어려운 경우 확인 할 수 있는 방법(IP, 사업장 전화번호 등)을 안내할 수 있음

법정대리인 동의받기 위해 최소한의 정보(성명, 연락처)는 아동으로부터 직접 수집 가능

법정대리인 동의 관련 주의사항	법정대리인의 성명, 연락처를 수집할 때는 해당 아동에게 자신의 신분과 연락처, 법정대리인 정보 수집 이유를 알려야 함
	수집한 법정대리인의 개인정보는 법정대리인 동의를 얻기 위한 목적으로만 이용해야 함
	법정대리인의 동의 거부 또는 동의 미확인시 수집일로부터 5일 이내 파기

동의 시 고지 등을 할 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용해야 함

제2절 개인정보의 처리 제한

23	민감정보의 처리 제한	
	민감정보는 원칙적 처리 금지. 별도 동의 또는 법령 에서 허용한 경우 민감정보를 처리자는 제29조에 따른 안전성 확보에 필요한 조치를 해야함	
	재화 또는 서비스 제공 과정에 공개되는 정보에 민감정보가 포함되어 위험성이 있다고 판단 시 제공 전에 민감정보 공개 가능성 및 비공개를 선택하는 방법을 정보주체가 알아보기 쉽게 알려야함 (이루다 사건 영향?)	
	처리가능한 경우	관련 고지사항 고지 후(수집이용시-4가지 고지사항, 제3자 제공시-5가지 고지사항) 정보주체의 별도 동의 를 받은 경우
		법령에서 민감정보의 처리를 요구하거나 허용하는 경우
		공공기관은 법(제18조제2항제5호~제9호)에 해당하는 경우 아래 2~5는 민감정보로 보지 않음
	민감정보 종류	1. 사생활 침해 우려가 있는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보
		2. 유전자검사 등의 결과로 얻어진 유전정보
		3. '형의 실효 등에 관한 법률' 제2조제5호에 따른 범죄경력자료 해당 정보
		4. 신체/생리/행동적 특징에 관한 정보로 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보
		5. 인종이나 민족에 관한 정보
24	고유식별정보의 처리 제한	
	고유식별정보는 원칙적 처리 금지. 법령 에서 허용한 경우 처리자는 암호화 등 영 제21조에 따른 안전성 확보(영 제30조 준용)에 필요한 조치를 해야함	
	고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호	
	처리가능한 경우	관련 고지사항 고지후(수집/이용-4가지 고지사항, 제3자 제공시-5가지 고지사항) 정보주체의 별도 동의 를 받은 경우
		법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우
		공공기관은 법(제18조제2항제5호~제9호)에 해당하는 경우 고유식별정보 처리 가능
	위원회는 조사 대상에 해당하는 고유식별정보를 처리하는 자에 대해 안전성 확보에 필요한 조치를 하였는 지 여부를 3년마다 1회 이상 조사해야 함	
	조사 대행 기관	한국인터넷진흥원, 기술적·재정적 능력과 설비 보유를 인정하여 보호위원회가 고시하는 법인, 단체 또는 기관
	조사 대상	1. 1만명 이상의 정보주체 고유식별정보를 처리하는 공공기관 (이전에는 공공기관 전체 해당)
		2. 보호위원회가 법 위반 이력 및 내용·정도, 고유식별정보 처리의 위험성 등을 고려해 조사가 필요하다고 인정한 공공기관
		3. 공공기관 외의 자로서 5만명 이상의 정보주체 고유식별정보를 처리하는 자
	조사 방법	대상 개인정보처리자에게 온라인 또는 서면을 통해 필요한 자료를 제출하게 하는 방법
	보호수준 평가, 보호 인증 등에 따라 안전성 확보에 필요한 조치에 대해 정기적 확인이 된 경우 정기적인 조사에 갈음 가능	
	조사 실시 인정 경우	1. 법 11조의2에 따라 개인정보 보호수준 평가를 받은 경우 2. 법 제32조의2에 따라 개인정보 보호 인증을 받은 경우 3. 신용정보법 제45조의5에 따른 개인신용정보 활용·관리실태에 대한 상시평가 등 다른 법률에 따라 고유식별정보의 안전성 확보조치 이행여부에 대한 정기적인 점검하는 경우로서 중행장의 요청에 따라 해당 점검이 조사에 준하는 것으로 보호위원회가 인정하는 경우

보호위원회(KISA 포함)는 다음 사무를 수행하기 위해 불가피한 경우 민감정보/고유식별정보 처리 가능
개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항 심의·의결
개인정보 보호에 관한 법령의 해석·운용에 관한 사항 심의·의결
법 제18조제2항제5호에 따른 개인정보의 이용·제공에 관한 사항 심의·의결
주민등록번호 대체방법 제공을 위한 시스템 구축 등 제반조치 마련 및 지원에 관한 사무
가명정보 처리 관련 과징금 부과, 주민등록번호 관련 과징금 부과, ISP등에 대한 과징금 부과 특례에 관한 사무
개인정보침해 신고센터의 업무에 관한 사무
법 제63조의 제1항, 제2항, 제7항에 따른 자료의 제출, 검사 및 점검에 관한 사무

24-2	주민등록번호의 처리 제한 (주민등록번호는 원칙적 처리 금지, 정보주체 동의로도 수집할 수 없음)	
	처리 가능한 경우	법률, 대통령령, 국회규칙, 대법원규칙, 헌법재판소규칙, 선관위규칙, 감사원규칙에서 구체적으로 요구하거나 허용한 경우 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위해 명백히 필요한 경우 주민등록번호 처리가 불가피한 경우로 보호위가 고시로 정하는 경우 (현재 없음)
	암호화를 통해 안전하게 보관하고, 정보주체가 인터넷 홈페이지를 통해 회원가입하는 단계에서는 주민등록번호 없이 가입하는 방법을 제공해야 함 초기 패스워드, 회원아이디 및 패스워드 찾기 등에서도 주민등록번호 사용 금지 세부 암호화 관련 내용은 개인정보의 안전성 확보조치 기준 고시의 "제7조 개인정보의 암호화" 적용 필요	

25	고정형 영상정보처리기의 설치·운영 제한	
	공개된 장소에 설치 원칙적 금지. 처리가능한 경우가 있으나 불특정 다수가 이용하는 목욕실·화장실 등 사생활 침해 우려 장소 내부에는 설치 금지 교도소, 정신보건 시설 등 법령에 근거한 교정시설, 정신의료기관, 정신요양시설 및 정신재활시설에는 상기 단서에도 불구하고 가능	
	처리 가능한 경우	1. 법령에서 구체적으로 허용하는 경우 2. 범죄의 예방 및 수사를 위해 필요한 경우 3. 시설의 안전 및 관리, 화재 예방을 위해 정당한 권한을 가진 자가 설치·운영하는 경우 4. 교통단속을 위해 정당한 권한을 가진 자가 설치·운영하는 경우 5. 교통정보의 수집·분석 및 제공을 위해 정당한 권한을 가진 자가 설치·운영하는 경우 6. 촬영된 영상정보를 저장하지 아니하는 경우로서 대통령령으로 정하는 경우 6-1. 출입자 수 등 통계값 산출을 위해 필요한 경우 6-2. 성별, 연령대 등 통계적 특성값을 도출하기 위해 필요한 경우 6-3. 상기와 준하는 경우로서 보호위원회의 심의·의결을 거친 경우
	고정형 영상정보처리기를 설치·운영하려는 공공기관의 장 및 교정시설 등에 설치·운영하려는 자는 설치·운영 또는 목적 변경 에 따른 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴해야 함	
	일반 의견 수렴 절차	행정절차법에 따른 행정예고의 실시 또는 의견 청취 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회, 설문조사 또는 여론조사
	특수한 경우 [제25조 제2항]	교도소, 정신보건 시설 등에 근거한 교정시설, 정신의료기관, 정신요양시설 및 정신재활시설에 설치할 경우 의견 수렴 대상은 1. 관계전문가 2. 해당 시설에 종사자, 해당 시설에 구금되어 있거나 보호받고 있는 자 또는 그 사람의 보호자 등 이해관계인

고정형영상정보처리기기운영자는 업무 총괄할 관리책임자를 지정해야하며, 개인정보 보호책임자가 관리책임자의 업무를 수행할 수 있음

관리 책임자 업무	1. 개인영상정보 보호 계획의 수립 및 시행
	2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
	3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
	4. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
	5. 개인영상정보 보호 교육 계획 수립 및 시행
	6. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
	7. 그 밖에 개인영상정보의 보호를 위해 필요한 업무
공공기관의 장이 기관내/기관간에 관리 및 정보 연계 등을 위해 통합하여 설치·운영(통합관리)하는 경우 해당 내용을 알기쉽게 안내판에 기재해야 함	
개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공 금지 (아래는 예외사항으로 가능한 경우)	
공공 기관만 해당	1. 정보주체 동의 시
	2. 다른 법률에 특별한 규정이 있는 경우
	3. 명백히 급박한 생명, 신체, 재산의 이익을 위해 필요가 인정되는 경우
	4. 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 필요한 경우로 법 제28조의2/3에 따라 가명처리한 경우
	5. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우
	6. 개인영상정보를 목적 외의 용도로 이용·제3자에게 미제공 시 다른 법률상 소관업무 수행 불가하여 보호위원회 의결된 경우
	7. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
	8. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
	9. 법원의 재판업무 수행을 위하여 필요한 경우
	10. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우
고정형 또는 이동형영상정보처리기기운영자는 운영·관리 방침에 명시한 보관기관이 경과하거나 처리 목적 달성, 가명정보의 처리 기간 경과 등 개인영상정보가 불필요하게 되었을 때에는 지체없이 파기해야 함. 다른 법령에 특별한 규정이 있는 경우에는 파기 안함	
고정형영상정보처리기기운영자는 보유 목적의 달성을 위한 최소한의 기간 산정이 곤란한 경우 보관기간을 수집 후 30일 이내로 함	
파기 방법	개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
	전자지적 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제
영상정보 기록·관리 포함 내용	1. 개인영상정보 파일의 명칭
	2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭
	3. 이용 또는 제공의 목적
	4. 법령상 이용 또는 제공 근거가 있는 경우 그 근거
	5. 이용 또는 제공의 기간이 정해져 있는 경우에는 그 기간
	6. 이용 또는 제공의 형태
	7. 이용 또는 제공한 개인영상정보의 업무처리 담당자
영상정보 파기 관리대장	1. 파기하는 개인영상정보 파일의 명칭
	2. 개인영상정보 파기 일시 (사전에 파기 시기 등을 정한 자동삭제의 경우에는 파기 주기 및 자동 삭제 여부에 관한 확인 시기)
	3. 개인영상정보 파기 담당자

설치·운영하는 자는 정보주체가 쉽게 인식하도록 안내판의 설치 등 필요한 조치를 수행해야 함	
안내판 내용	1. 설치 목적 및 장소
	2. 촬영 범위 및 시간
	3. 관리책임자의 연락처
	4. 공공기관이 위탁한 경우에는 안내판 등에 위탁받은 자(수탁자)의 명칭 및 연락처 (일반은 표준지침 존재/위임은 없음)
	그 밖에 대통령령으로 정하는 사항(현재 없음)
설치 방법	안내판 크기, 설치 위치 등은 자율로 정하되 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 판독 용이하게 설치
설치 예외	군사시설, 국가중요시설, 보안업무규정 제32조에 따른 국가보안시설
건물 안에 여러 개의 영상정보처리기기를 설치·운영하는 경우 출입구 잘보이는 곳에 해당 시설 또는 장소 전체가 설치지역임을 표시 가능	
설치 목적과 다른 목적으로 임의 조작 및 다른 곳을 촬영 금지. 녹음기능 사용 금지	
안내판 설치를 갈음하여 인터넷 홈페이지에 안내판 내용의 사항을 게재 가능한 경우	
1. 공공기관이 원거리 촬영, 과속/신호위반 단속 또는 교통흐름조사 등의 목적으로 개인정보 침해의 우려가 적은 경우	
2. 산불감시용 영상정보처리기기를 설치하는 경우 등 장소적 특성으로 인해 안내판 설치가 불가능하거나 설치하더라도 정보주체가 인식이 어려운 경우	
인터넷 홈페이지에도 안내판 고지내용을 게재할 수 없는 경우 공개 방법	
운영자의 사업장·영업소·사무소·점포 등의 보기 쉬운 장소에 게시	
관보(공공기관만 해당)나 운영자의 사업장 등이 있는 시도 이상의 지역을 주된 보급지역 신문 게시	
개인정보가 유출등이 되지 않도록 제29조에 따라 안전성 확보 조치 해야 함	
고정형 영상정보처리기기 운영·관리 방침을 마련해야 함. (개인정보 처리방침에 포함시킨 경우에는 별도 마련 불필요)	
수립 및 변경시 정보주체가 쉽게 확인할 수 있도록 공개해야 함	
방침 포함 내용	1. 고정형 영상정보처리기기의 설치 근거 및 설치 목적
	2. 고정형 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
	3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
	4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
	5. 고정형영상정보처리기기운영자의 영상정보 확인 방법 및 장소
	6. 정보주체의 영상정보 열람 등 요구에 대한 조치
	7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
	8. 그 밖에 고정형 영상정보처리기기의 설치·운영 및 관리에 필요한 사항
방침의 공개 방법	1. 운영·관리 방침을 인터넷 홈페이지에 지속적으로 게재
	2. 인터넷 홈페이지에 게재가 어려운 경우
	사업장등의 보기 쉬운 장소에 게시
	관보 또는 시도 이상의 지역을 주된 보급지역으로 하는 신문에 게시
	같은 제목으로 연2회 이상 발행하여 정보주체에 배포하는 간행물 또는 청구서 등에 지속적으로 실기
재화나 서비스 제공의 경우는 서로 작성한 계약서 등에 실어 정보주체에게 발급하는 방법	

영상정보처리기기의 설치·운영에 관한 사무를 문서로 위탁할 수 있음. 공공기관이 위탁시 추가적인 절차 및 요건 준수 필요	
공공기관이 위탁시 문서에 포함해야 하는 내용	1. 위탁하는 사무의 목적 및 범위
	2. 재위탁 제한에 관한 사항
	3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
	4. 영상정보의 관리 현황 점검에 관한 사항
	5. 위탁받는 자가 준수해야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항
	제3자에게 위탁시 그 내용을 안내판 및 영상정보처리기기 운영·관리 방침에 수탁자의 명칭 등을 공개
	제3자에게 위탁한 경우 안전하게 처리하고 있는 지를 관리·감독해야 함

25-2 이동형 영상정보처리기기의 운영 제한

업무를 목적으로 공개된 장소에서 처리가능한 경우를 제외하고 이동형 영상정보처리기기로 사람 또는 관련 사물의 영상 촬영 금지.	
처리 가능한 경우	법 제15조제1항 각 호의 어느 하나에 해당하는 경우
	촬영 사실을 명확히 표시, 정보주체가 촬영사실을 알게 했음에도 불구하고 촬영 거부 의사 없는 경우 : 합리적 범위 초과 금지
	상기 내용에 준하는 경우로서 대통령령으로 정하는 경우(현재 없음)
촬영 사실 표시	촬영하는 경우에도 불빛, 소리, 안내판, 서면, 안내 방송 또는 그 밖에 준하는 수단을 통해 정보주체가 쉽게 알 수 있도록 표시
	드론에 의한 항공촬영 등 촬영 방법의 특성상 정보주체에게 표시하기 어려운 경우 <div> <div></div> <div>보호위원회가 이동형 영상정보처리기기의 촬영 사실 표시를 지원하기 위한 홈페이지를 통해 공지 (촬영 사실 및 목적, 촬영 일시 및 장소 등)</div> </div>
누구든지 목욕실, 화장실, 발한실, 탈의실 등 사생활 침해 우려 장소의 내부를 볼 수 있는 곳에서 사람 또는 관련 사물의 영상촬영 금지	
영상촬영 금지에도 불구하고 인명의 구조·구급 등을 위하여 필요한 경우로서 대통령령으로 정하는 경우에는 가능	
범죄, 재난, 화재 또는 이에 준하는 상황에서 인명의 구조·구급 등을 위해 영상 촬영이 필요한 경우	
안전성 확보조치, 운영·관리 방침, 위탁 업무와 관련하여 고정형 영상정보처리기기에서 요구하는 규정을 준용	
이동형 영상정보처리기기 운영·관리 방침을 마련하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개해야 함	
방침은 별도로 정하거나 개인정보 처리방침에 포함하여 정할 수 있음. (홈페이지 등에 공개)	
방침 내용	이동형 영상정보처리기기의 운영 근거 및 운영 목적
	이동형 영상정보처리기기의 설치 대수
	관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
	영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
	이동형영상정보처리기기운영자의 영상정보 확인 방법 및 장소
	정보주체의 영상정보 열람등 요구에 대한 조치
	영상정보 보호를 위한 기술적·관리적 및 물리적 조치
	그 밖에 이동형 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

26 업무 위탁에 따른 개인정보의 처리 제한

"위탁자" : 업무를 위탁하는 개인정보처리자, "수탁자" : 개인정보 처리업무를 위탁받아 처리하는 자 **및 다시 위탁받은 제3자를 포함**

제3자에게 개인정보 처리 업무를 위탁하는 경우 문서에 의해 위탁해야 함	
위탁시 포함 내용	위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
	개인정보의 기술적·관리적 보호조치에 관한 사항
	위탁 업무의 목적 및 범위
	재위탁 제한에 관한 사항 (재위탁시 위탁자 승인 필요 내용 포함 권고)
	개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
	위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
	수탁자가 준수해야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항
수탁자 선정시 인력과 물적 시설, 재정 부담 능력, 기술 보유의 정도, 책임능력 등 개인정보 처리 및 보호 역량을 종합적으로 고려해야 함	
수탁자는 위탁받은 개인정보의 처리업무를 제3자에게 재위탁하려는 경우에는 위탁자의 동의를 받아야 함	
위탁자는 정보주체가 언제든지 쉽게 확인할 수 있도록 위탁자 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재 해야 함	
위탁 내용 공개 방법	인터넷 홈페이지에 지속적으로 게재
	인터넷 홈페이지에 게재가 어려운 경우
	사업장등의 보기 쉬운 장소에 게시
	관보 또는 시도 이상의 지역을 주된 보급지역으로 하는 신문에 게시
	같은 제목으로 연2회 이상 발행하여 정보주체에 배포하는 간행물 또는 청구서 등에 지속적으로 실기
재화나 서비스 제공의 경우는 서로 작성한 계약서 등에 실어 정보주체에게 발급하는 방법	
위탁자는 홍보 및 마케팅 업무를 위탁하는 경우 서면등의 방법 으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 함. 위탁 업무의 내용이나 수탁자가 변경된 경우에도 알려야 함	
과실없이 어려운 경우 인터넷 홈페이지에 30일 이상 게재 , 홈페이지가 없는 경우 사업장 등 보기 쉬운 장소에 30일 이상 게시	
위탁자 의무	1. 수탁자 교육 실시
	2. 수탁자의 개인정보 처리 현황 점검
	3. 문서로 위탁시 포함내용에 대해 개인정보를 안전하게 처리하는 지 감독
수탁자는 위탁받은 업무 범위를 초과하여 이용·제3자 제공 금지	
수탁자가 위탁받은 업무와 관련하여 위반해서 발생한 손해배상책임에 대해서는 수탁자를 개인정보처리자의 소속직원으로 간주	
수탁자는 제15조~제25조의2, 제27조~제31조, 제33조~제38조까지 및 제59조, 제63조 및 제63조의2 준용한다. (수탁자 법적 의무사항 확대)	
27	영업양도 등에 따른 개인정보의 이전 제한 양도·합병 등으로 개인정보를 이전하는 경우 해당 사항을 서면등의 방법으로 정보주체에게 공지 공지 내용 1. 개인정보를 이전하려는 사실 2. 개인정보를 이전받는 자(영업양수자등)의 성명(법인 명칭), 주소, 전화번호 및 그 밖의 연락처 3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차 이전 내용 알림이 어려운 경우 인터넷 홈페이지에 30일 이상 게재해야 함 게재가 정당한 사유로 어려운 경우 영업양도자등의 사업자등의 보기 쉬운 장소에 30일 이상 게시하는 방법 영업양도자등의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 신문 등에 실는 방법

<p>각급학교 폐교/통폐합에 따른 이전은 교육부장관/교육감이 지정한 개인정보처리자가 이전 실시</p> <p>홈페이지 게재는 이전하려는 자 또는 받는 자가 게재</p> <p>학교 통폐합 관련 행정예고 등에 이전 관련 사항을 포함하여 공고한 경우 게재 사항 같음</p>	
28	<p>개인정보취급자에 대한 감독</p> <p>임직원, 파견, 시간제근로자 등 개인정보처리자 지휘로 개인정보를 처리하는 자(개인정보취급자)의 범위를 최소한으로 제한하고 적절한 관리·감독</p> <p>개인정보취급자에게 정기적으로 필요한 교육을 실시</p> <p>교육기관의 개인정보 보호담당자는 신규 발령 1년 이내에 15시간 이상의 개인정보보호 교육 이수</p> <p>취급자를 최소한으로 두어야 하며, 처리범위도 최소한으로 제한해야 함</p> <p>시스템 접근권한을 업무의 성격에 따라 최소한의 범위로 업무담당자에게 차등 부여하고 접근권한 관리하기 위한 조치를 취해야 함</p> <p>취급자에게 보안서약서 징구 등 적절한 관리 감독하고, 인사이동으로 업무 변경시 접근권한을 즉시 변경 또는 말소해야 함</p>

<p>제3절 가명정보의 처리에 관한 특례 (법 제28조의2 및 제28조의3에 따라 가명정보를 처리하는 자에 대한 특례임)</p>	
28-2	<p>가명정보의 처리 등</p> <p>개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위해 정보주체 동의없이 가명정보 처리 가능 (가명처리 전 정보주체 거부시 가명처리 불가능)</p> <p>가명정보를 제3자에게 제공하는 경우 개인 재식별에 사용될 수 있는 정보는 포함 금지</p>
28-3	<p>가명정보의 결합 제한</p> <p>서로 다른 처리자 간의 가명정보 결합은 전문기관이 수행 (전문기관은 보호위원회 또는 관계 중앙행정기관의 장이 지정)</p> <p>결합을 수행한 기관 외부로 결합된 정보를 반출시 처리자는 가명정보 또는 익명정보(법 제58조의2)로 처리한 뒤 전문기관의 장의 승인 필요</p> <p>결합의 절차와 방법, 전문기관의 지정과 지정 취소 기준·절차, 관리·감독, 반출 및 승인 기준·절차 등은 대통령령으로 정함</p> <div style="display: flex;"> <div style="writing-mode: vertical-rl; text-orientation: upright; padding-right: 10px;"> 결합 전문기관 지정 기준 </div> <div> <ol style="list-style-type: none"> 고시에 따라 조직 구성하고 관련 자격이나 경력을 갖춘 사람을 3명 이상 상시 고용 고시에 따라 가명정보의 안전한 결합을 위한 공간, 시설 및 장비 구축하고 관련 정책 및 절차 등을 마련 고시에 따라 재정 능력을 갖추 것 (자본금 50억원 이상 or 기본재산/자본총계 50억원 이상) 최근 3년 이내에 법 제66조에 따른 공표 내용에 포함된 적이 없을 것 (과태료 부과 내용 및 결과 공표) 최근 3년 이내에 법 제66조에 따라 공표되거나 공표명령을 받은 사실이 없을 것(과태료 부과 내용 및 결과 공표) <i>2025.1.1. 변경</i> 최근 1년 이내에 영 제29조의2 제5항에 따른 지정취소 및 제4항 단서에 따라 재지정되지 않은 사실이 없을 것 <i>2025.1.1. 추가</i> </div> </div> <p>결합전문기관 지정받으려는 경우 지정신청서 및 첨부서류(정관 or 규약, 지정신청서, 기준 충족여부 증빙서류)를 첨부하여 보호위 또는 중행장에게 제출</p> <div style="display: flex;"> <div style="writing-mode: vertical-rl; text-orientation: upright; padding-right: 10px;"> 신용정보법 제26조의4에 따라 데이터전문기관으로 지정받은 기관은 "기준 증빙 서류" 중 일부를 생략할 수 있음 </div> <div> <p>지정신청자는 필요시 결합전문기관 사업계획서 또는 그에 준하는 서류를 제출하여 지정 기준에 적합한지 여부 확인 가능</p> </div> </div>

지정신청서를 받은 보호위원회등은 제출한 법인등이 지정 기준에 적합한 경우에는 결합전문기관으로 지정 가능	
보호위원회등은 결합전문기관을 지정하기 위해 지정심사위원회를 구성하여 심사해야 함 (5명의 위원으로 구성)	
신청받은 날의 다음날부터 2개월 이내에 지정 여부를 결정, 불가피한 경우 1개월 범위에서 그 기간을 연장 가능	
기간산정 예외	지정신청자의 서류보완 등에 소요된 기간 법/시행령에 따른 의무 위반 관련하여 지정신청자를 상대로 형사소송 절차가 진행되고 있거나 보호위원회등에 의한 조사·검사 등 절차가 진행되어 지정심사에 중대한 영향이 인정되는 경우 그 절차가 끝날 때 까지의 기간
지정기준을 충족하는 경우 결합전문기관 지정서를 발급	
결합전문기관은 지정 기준에 해당하는 사실의 변경시 보호위원회등에 사실을 알리고, 보호위원회등은 변경내용 확인 필요	
지정의 유효기간은 지정을 받은 날부터 3년, 보호위원회등은 결합전문기관의 연장 신청 시 지정 기준에 적합한 경우 재지정 가능	
정당한 사유없이 결합·반출 실적이 없거나 현저히 업무수행 실적이 저조한 경우에는 재지정 이후 결합 활성화를 위한 운영계획, 사업수행 의지 등을 검토하여 재지정하지 않을 수 있음 <i>(시행일 2025.1.1)</i>	
결합전문기관은 재지정 받으려는 경우 만료일 6개월~3개월 전까지 증명 서류를 갖추어 재지정을 신청	
재지정 신청을 받은 경우 신청을 받은 날부터 3개월 이내에 그 결과를 통지해야 함	
위원회 또는 중행장은 위원회가 고시하는 기준을 갖춘 법인, 단체, 기관을 결합전문기관으로 지정 가능	
결합전문기관 지정의 유효기간은 지정 받은 날부터 3년, 유효기간의 연장 신청시 재지정 가능	
결합전문기관은 재지정 받으려는 경우 만료일 6개월 전부터 3개월 전까지 지정 기준 부합 증명 서류로 신청	
보호위원회등은 지정기간 만료일 6개월 전에 만료사실을 알려줄 수 있음	
재지정 신청을 받은 보호위원회 등은 지정기간 만료일 전까지 그 결과를 재지정 신청 결합전문기관에 통지해야함	
위원회 또는 중행장은 결합전문기관의 지정을 취소 가능	
위원회 또는 중행장은 결합전문기관의 지정을 취소하는 경우 청문해야 함	
위원회 또는 중행장은 전문기관을 지정·재지정·지정 취소했을 때에는 이를 관보에 공고하거나 위원회 또는 중행장 홈페이지에 고시해야 함	
지정 취소 필수	거짓이나 부정한 방법으로 결합전문기관으로 지정받은 경우 결합전문기관 스스로 지정 취소를 요청하거나 폐업한 경우
지정 취소 가능	결합전문기관 지정 기준을 충족하지 못하게 된 경우 결합 및 분석 등과 관련된 정보의 유출 등 침해사고가 발생한 경우 그 밖에 법 또는 시행령에 따른 의무를 위반한 경우
보호위원회등은 지정 취소 가능 항목에 해당하는 경우 결합전문기관에 시정·보완을 요구할 수 있음	
지정을 취소한 경우 해당 결합전문기관이 수행 중인 업무를 중단하도록 하고 신청자와 협의하여 다른 기관으로 이관	
관련 중앙행정기관의 장이 전문기관을 지정·재지정·지정 취소한 경우 보호위원회에 상기 홈페이지 고시 내용을 통보해야 함	
지정 등에 따른 홈페이지 고시내용	결합전문기관의 명칭 및 주소 담당부서 및 연락처 지정 유효기간(지정 또는 재지정의 경우) 취소 일시 및 취소 사유(지정 취소의 경우)
결합전문기관에 결합을 신청하려는 개인정보처리자는 결합신청서와 서류를 해당 결합전문기관에 제출해야 함	

결합 신청자 제출 서류	사업자등록증, 법인등기부 등본 등 결합신청자 관련 서류
	결합 대상 가명정보에 관한 서류
	결합 목적을 증명할 수 있는 서류
	그 밖에 가명정보의 결합 및 반출에 필요하다고 보호위원회가 정하여 고시하는 서류
결합전문기관은 특정 개인을 알아볼 수 없도록 위원회 고시하는 절차와 방법에 따라 가명정보를 결합	
절차 및 방법	KISA 및 위원회 지정기관은 결합전문기관이 특정 개인을 알아볼 수 없도록 하는데 필요한 지원 업무를 수행 가능
가명정보의 결합 신청 절차	
결합신청자는 결합신청서와 다음 관련 서류를 결합전문기관에 제출	
가. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류	
나. 결합 대상 가명정보에 관한 서류 (전체 항목명, 가명처리 대상 항목명, 가명처리 내역 등) (사전 협의시 가명처리 내역에 관한 서류는 가명정보 전송 시에 제출 가능)	
다. 결합 목적을 증명할 수 있는 서류	
라. 반출 정보의 안전조치계획 및 이를 증명할 수 있는 서류	
결합전문기관은 신청서 및 첨부서류를 확인하고 필요시 보완을 요구하거나 가명처리 수준에 대해 권고 가능	
결합전문기관은 결합 일정 및 절차 등 결합에 필요한 사항을 결합신청자와 협의	
결합기관관리기관은 결합키 생성에 필요한 사항을 결합신청자와 협의	
결합신청자는 결합기관관리기관과 협의 결과에 따라 결합키와 결합에 필요한 일련번호를 결합기관관리기관에게 전송	
결합기관관리기관은 결합신청자들의 결합키와 일련번호를 이용하여 지체없이 결합키연계정보를 생성	
결합물 확인 및 추출	결합기관관리기관은 결합신청자 요청이 있는 경우 결합키연계정보 생성과정에서 결합물 확인하여 결합신청자에게 통보
	결합신청자는 기관관리기관에 결합대상정보 추출에 필요한 일련번호를 요청 가능 (관련 필요한 자료를 제출)
	결합기관관리기관은 일련번호 요청을 받은 경우 특성, 결합물 등을 고려하여 추출 가능 여부를 통보 추출이 가능하다고 판단한 경우 결합대상정보의 추출에 필요한 일련번호 전송 (추출 원칙이 있음)
결합신청자는 결합대상정보 확정시 가명처리하여 가명처리내역, 결합에 필요한 일련번호와 함께 결합전문기관에 전송	
결합전문기관은 결합대상정보의 가명처리 수준을 확인한 후 필요한 경우 추가처리를 요청 가능	
결합기관관리기관은 결합전문기관이 가명정보 결합을 위해 결합키연계정보의 전송 요구시 지체없이 전송	
결합전문기관은 결합기관관리기관에서 받은 결합키연계정보로 가명정보를 결합	
결합완료 등 결합키연계정보가 불필요하게 된 때에는 이를 지체없이 파기	
모의 결합 절차	결합신청자는 결합 유용성 확인을 위해 결합 수행 전 결합전문기관과 협의하여 일부 가명정보의 결합 요청 가능
	결합신청자는 결합키 또는 모의결합키(결합키등)를 결합전문기관에 전송
	결합전문기관은 모의결합 대상정보의 특성, 결합물 등을 고려하여 모의결합 가능 여부를 신청자에게 통지
	모의결합이 가능한 경우 모의결합 대상 정보의 결합키를 선정하여 결합신청자에게 전송 (추출고려)
결합신청자는 대상정보를 가명처리하여 가명처리 내역, 결합에 필요한 결합키등과 함께 결합전문기관에 전송	
결합전문기관은 모의결합 대상정보의 가명처리 수준을 확인한 후 필요시 추가처리를 요청 가능	

결합신청자는 결합전문기관으로부터 모의결합된 정보를 제공받아 안전한 공간에서 분석 가능			
결합신청자는 분석한 정보 등 결과물을 결합전문기관 외부로 반출 불가능			
결합전문기관은 모의결합된 정보를 제공시 결합기등은 삭제하고 결합신청자에게 제공해야 함			
결합신청자가 분석을 마친 경우 결합전문기관은 모의결합에 사용된 모든 정보를 파기해야 함			
결합전문기관은 결합신청자의 요청시 안전한 공간에서 결합된 정보를 분석하도록 할 수 있음			
결합신청자는 결합된 정보를 반출하려면 반출신청서와 첨부서류를 결합전문기관에 제출			
결합신청자는 결합정보 반출을 위해 필요시 안전한 공간에서 사전에 가명정보 또는 익명정보로 처리			
반출서류	반출대상정보에 관한 서류(추가적인 서류 제출이 필요한 경우)		
	반출목적 증명할 수 있는 서류(추가적인 서류 제출이 필요한 경우)		
	반출정보의 안전조치 계획 및 이를 증빙할 수 있는 서류		
결합전문기관은 5일 이내 반출심사위원회 구성 등 일정을 통지하고 구체적인 사항을 협의			
위원 구성	개인정보 보호에 관해 경험과 학식이 풍부한 3~7인의 위원으로 구성		
	결합신청자의 임직원 등 이해관계자는 반출심사위원회 위원으로 참여 불가능		
반출승인 고려사항	결합 목적과 반출 정보가 관련성이 있을 것		
	특정 개인을 알아볼 가능성이 없을 것		
	반출 정보에 대한 안전조치 계획이 있을 것		
	결합신청자는 반출심사시 필요한 사항을 제출하고 이를 설명해야 함		
	결합신청자의 임직원 등 이해관계자는 반출심사위원회 위원으로 참여 불가		
결합전문기관의 가명정보 결합 (자체결합)			
결합전문기관은 자신이 보유한 가명정보와 다른 처리자가 보유한 가명정보를 제3자에게 제공하는 경우 직접 결합 가능			
자 체 결 합 시 준 수 사 항	이해관계가 없는 외부전문가 3인이 특정 업무를 수행	외부 전문가 자격요건	개인정보 보호 관련 업무 경력 or 관련 단체 추천받은 자
			개인정보처리자로 구성된 단체에서 활동 경력 or 관련 단체 추천받은 자
			그 밖에 개인정보 보호와 관련한 경력과 전문성이 있는 자
		수행 업무	결합신청서 및 첨부 서류의 확인과 보완 요구
			결합대상 정보의 가명처리 수준 확인과 추가 처리 요청
	반출심사위원회를 결합전문기관과 이해관계가 없는 외부전문가로만 구성		
	결합신청자 업무를 수행하는 담당자는 결합전문기관 업무에 참여 금지		
	결합전문기관 보유 가명정보와 결합한 가명정보를 물리적 분리 보관 및 각 정보에 대한 접근권한 통제·관리		
	반출심사위원회는 유사 다른 결합전문기관의 임직원/추천 외부전문가로 구성		
	상기 회피목적으로 타 기관과 교차하여 위원회 구성 의뢰/수행 금지		
	제3자 제공시 면제	결합정보 이용할 경우 직전 분기까지 가명정보 제3자 제공 누적 실적 범위에서 자체결합 수행	
		자체결합 관련 내용을 인터넷 사이트에 공개	
		공개 내용	결합된 정보의 이용자 및 관리책임자
	결합된 정보의 활용 목적, 항목, 활용 기간		

결합전문기관은 자체결합에 대한 상기 내용을 기록 보관하고, 매 분기 마지막 달의 다음 달 말일까지 보호위원회에 제출

1. 결합신청서 및 첨부서류

- 가. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류
 나. 결합 대상 가명정보에 관한 서류 (전체 항목명, 가명처리 대상 항목명, 가명처리 내역 등)
 다. 결합 목적을 증명할 수 있는 서류
 라. 반출 정보의 안전조치계획 및 이를 증명할 수 있는 서류

2. 반출심사결과 및 심사위원 명단

3. 결합정보 및 심사 대상 정보에 대한 파기 대장

4. 외부전문가 3인 명단 및 자격 관련 서류

5. 외부전문가 3인이 이해관계가 없음을 증명하는 확인 서류

6. 외부전문가가 수행한 서류의 확인과 보완 요구 및 가명처리 수준에 대한 권고 내용

7. 결합전문기관 보유 가명정보와 결합한 가명정보에 대한 물리적 분리 및 보관 확인 서류

8. 결합업무 관련 담당자가 결합신청자 업무와 관련 없음을 확인 가능한 서류

9. 가명정보 제3자 제공 누적 실적 및 자체결합 실적 수치 관련 확인 서류

10. 반출심사위원회 위원별 이해관계가 없음을 증명하는 확인 서류

11. 결합전문기관 보유 가명정보와 결합한 가명정보에 대한 물리적 분리 보관 및 각 정보에 대한 접근권한 통제·관리 확인 서류

12. 자체결합 관련 내용에 대한 인터넷 사이트 공개 내역 관련 서류

결합전문기관은 가명정보 결합 및 반출 실적 보고서 작성 시 자체결합 실적은 별도로 분리해서 작성

결합전문기관의 지원

지원내용	결합 전 가명처리
	반출을 위한 결합된 정보의 가명·익명처리 또는 결합된 가명정보 분석
	반출한 정보 분석
	가명정보를 반출하려는 결합신청자에 대한 개인정보 보호 교육

결합전 가명처리, 결합된 정보 가명·익명처리 또는 분석, 반출한 정보 분석을 수행한 담당자는 결합신청 접수 및 가명처리 수준 확인 업무에 참여 제한 (직무 분리)

결합전문기관은 가명정보의 결합·반출 등으로 해당 가명정보의 결합·반출과정에서 제공받거나 생성한 정보가 불필요시 지체없이 파기

결합전문기관은 매년 1월 31일까지 전년도에 생성된 다음 사항을 보호위원회에 제출

1. 결합신청서 및 첨부서류

- 가. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류
 나. 결합 대상 가명정보에 관한 서류 (전체 항목명, 가명처리 대상 항목명, 가명처리 내역 등)
 다. 결합 목적을 증명할 수 있는 서류
 라. 반출 정보의 안전조치계획 및 이를 증명할 수 있는 서류

3. 반출심사에 대한 결과 및 심사위원 명단

4. 결합정보 및 심사 대상 정보에 대한 파기 대장

결합기관관리기관은 가명정보의 결합이 완료되는 등 결합키와 결합키연계정보가 불필요하게 된 때에는 지체없이 파기

결합전문기관은 결합신청자가 정당한 사유없이 결합 완료일로부터 14일 이상 반출 전 처리 등 반출의 의사가 없다고 판단되면 결합절차 종료 가능

결합신청자는 결합전문기관 외부로 반출 시 안전한 공간에서 결합된 정보를 가명정보 또는 익명정보로 처리한 뒤 결합전문기관의 승인 필요	
결합전문기관은 기준을 충족하는 경우 반출을 승인해야 함 (반출 승인을 위한 반출심사위원회를 구성해야 함)	
반출 승인 조건	1. 결합목적과 반출정보가 관련성이 있을 것 2. 특정 개인을 알아볼 가능성이 없을 것 3. 반출 정보에 대한 안전조치 계획이 있을 것
결합전문기관은 결합, 반출 등에 필요한 비용을 결합신청자에게 청구 가능	
[위원회 또는 중행장]은 지정한 결합전문기관의 업무수행 능력 및 기술·시설 유지 여부 등을 관리·감독을 해야 함	
[결합전문기관]은 관리·감독을 위한 서류를 보호위원회가 고시하는 바에 따라 보호위원회 또는 관계 중행장에게 제출해야 함 (1월 31일까지)	
제출 서류	1. 가명정보의 결합·반출 실적 보고서 2. 결합전문기관의 지정 기준을 유지하고 있음을 증명할 수 있는 서류 3. 가명정보의 안전성 확보에 필요한 조치 여부를 증명할 수 있는 서류로서 보호위원회가 정한 서류
[위원회]는 결합전문기관에 대한 관리·감독을 해야 함 가명정보의 결합 및 반출 승인 과정에서의 법 위반 여부 결합 신청자에 대한 가명정보 처리실태 그 밖에 가명정보의 안전한 처리를 위해 필요한 사항으로 보호위원회가 정하여 고시한 사항	
28-4	가명정보에 대한 안전조치의무 등 개인정보처리자는 가명정보 처리시 추가 정보를 별도 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치가 필요 처리자는 가명정보 및 추가 정보에 대한 안전성 확보 조치를 해야 함 1. 영 제30조에 따른 개인정보 안전성 확보조치 2. 가명정보와 추가 정보의 별도 분리 보관. 다만, 추가정보가 불필요한 경우 추가정보를 파기 3. 가명정보 또는 추가 정보에 대한 접근권한 분리 소상공인으로 접근권한 분리가 어려운 정당한 사유가 있는 경우 업무 수행에 필요한 최소한의 접근 권한만 부여하고 접근권한의 보유 현황을 기록으로 보관하는 등 관리·통제 처리자는 처리목적 등을 고려하여 가명정보의 처리 기간을 별도로 정할 수 있음 처리자는 가명정보를 처리하는 경우 가명정보 처리 목적, 제3자 제공시 제공받는 자 등 가명정보의 처리내용 관리를 위한 관련 기록 작성·보관 1. 가명정보 처리의 목적 2. 가명처리한 개인정보의 항목 3. 가명정보의 이용내역 4. 제3자 제공 시 제공받는 자 5. 가명정보의 처리기간(처리기간을 별도로 정한 경우에 한함) 교육기관은 가명정보 처리 이용 및 보유기간 6. 그 밖에 가명정보의 처리 내용을 관리하기 위하여 보호위원회가 필요하다고 인정하여 고시하는 사항 7. 가명정보 처리 작업 기간 8. 위탁 사항 (해당시) 9. 제한사항(가명정보 처리 유형에 따라 제한사항을 규정한 경우 해당 내용 명시)
교육분야 추가적인 필요 항목	

		10. 처리구분-가명정보 생성/결합/제공/공개/수신 등
		11. 가명처리를 수행한 자(위탁한 경우 위탁자)
		12. 가명정보 처리 책임자
		13. 기타 사항 (추가정보 삭제/분리보관 등에 관한 정보)
		상기 가명정보 관리대장은 가명정보를 파기한 날부터 3년 이상 보관해야 함
28-5	가명정보 처리시 금지의무 등	법 제28조의2 또는 제28조의3에 따라 가명정보를 처리하는 자는 특정 개인 재식별 목적으로 가명정보 처리 금지 처리자는 가명정보를 처리 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우 즉시 처리 중지, 지체없이 회수·파기
28-7	적용 범위: 가명정보는 다음 사항 적용을 제외	가명정보는 제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지), 제20조의2(개인정보 이용·제공 내역의 통지), 제27조(영업양도.. 이전 제한), 제34조제1항(개인정보 유출시 정보주체에게 통지), 제35조~제37조(개인정보의 열람/전송요구/정정·삭제/처리정지)
28-8	개인정보의 국외 이전	개인정보를 국외로 제공(조회 경우 포함)·처리위탁·보관(이전) 금지
국외 이전이 가능한 경우		1. 정보주체에게 별도 동의를 받은 경우
		동의시 고지 사항
		1. 이전되는 개인정보 항목
		2. 개인정보가 이전되는 국가, 시기 및 방법
		3. 개인정보를 이전받는 자의 성명(법인인 경우 명칭과 연락처)
		4. 개인정보를 이전받는 자의 개인정보 이용 목적 및 보유·이용 기간
		5. 개인정보의 이전을 거부하는 방법, 절차 및 거부의 효과
		2. 법률, 대한민국을 당사자로 하는 조약 또는 그 밖의 국제협정에 개인정보 국외 이전 관련 특별한 규정이 있는 경우
		3. 계약의 체결 및 이행을 위해 개인정보의 처리위탁·보관이 필요한 경우로 처리방침 공개 또는 정보주체에게 알린 경우
		동의시 고지사항의 내용을 개인정보 처리방침에 공개 동의시 고지사항의 내용을 서면등의 방법으로 정보주체에게 알림
		4. 이전받는 자가 개인정보 보호 인증 등 보호위원회가 정하여 고시하는 인증을 받은 경우로 다음 조치를 모두 한 경우
		가. 개인정보 보호에 필요한 안전조치 및 정보주체 권리보장에 필요한 조치
		나. 인증받은 사항을 개인정보가 이전되는 국가에서 이행하기 위해 필요한 조치
		인증 고지 절차
		1. 영 제34조의6에 따른 개인정보 보호 인증 전문기관의 평가
		2. 영 제5조제1항제1호에 따른 국외이전전문위원회의 평가
		3. 정책협의회의 협의
		유효기간
		5년의 범위에서 유효기간을 정하여 고시
		향후 반영 예정
		5. 이전되는 국가 또는 국제기구의 보호체계, 정보주체 권리보장 범위, 피해구제 절차 등이 이 법에 따른 보호 수준과 실질적으로 동등한 수준으로 갖추었다고 보호위원회가 인정하는 경우
		인정시 고려사항
		1. 이전대상국등의 법령, 규정 또는 규칙 등 보호체계가 보호원칙에 부합하고 정보주체 권리를 충분히 보장 여부
		2. 이전대상국등에 보호체계를 보장하고 집행할 책임이 있는 독립적 감독기관 존재 여부
		3. 이전대상국등의 공공기관이 법률에 따라 처리하는지 여부 및 피해구제 절차 등 실질적으로 정보주체 보호 여부

		4. 이전대상국등에 정보주체가 쉽게 접근할 수 있는 피해구제 절차가 존재하는 지 여부 및 피해구제 절차가 정보주체를 효과적으로 보호하고 있는지 여부
		5. 이전대상국등의 감독기관이 보호위원회와 정보주체의 권리보호에 관하여 원활한 상호 협력이 가능한지 여부
		6. 그 밖에 보호위원회가 정하여 고시하는 사항
		향후 반영 예정
동시 고지사항 중 어느 하나에 사항을 변경하는 경우 정보주체에게 알리고 동의 필요		
상기 국외 이전이 가능한 경우에 제17조~제19조까지의 규정 및 제5장(정보주체의 권리 보장)의 규정을 준수하고 보호조치를 수행해야 함		
준수 규정	국외 이전 관련 다른 규정 : 제28조의8~제28조의11	
	제17조(개인정보의 제공), 제18조(개인정보의 목적 외 이용·제공 제한), 제19조(개인정보를 제공받은 자의 이용·제공 제한)	
	제5장 정보주체의 권리보장	
보호조치	개인정보 보호를 위한 안전성 확보 조치	
	개인정보 침해에 대한 고충처리 및 분쟁 해결에 관한 조직	
	그 밖에 정보주체의 개인정보 보호를 위해 필요한 조치	
국외이전시 보호조치 관련 내용을 이전받는 자와 미리 협의하고 이를 계약내용 등에 반영해야 함		
이 법을 위반하는 사항을 내용으로 개인정보의 국외 이전에 관한 계약 체결 금지		
개인정보의 국외 이전 중지 명령		
보호위원회는 국외 이전이 계속되거나 추가적인 국외 이전 예상되는 경우 국외 이전 중지 명령 가능		
국외 이전 중지 명령 가능한 경우	1. 제28조의8 제1항(국외이전 금지/예외적 허용), 제4항(규정 및 보호조치 준수), 제5항(법 위반 내용의 계약 체결) 위반한 경우	
	2. 이전받는 자나 이전되는 국가 또는 국제기구가 법에 따른 개인정보 보호 수준에 비해 개인정보를 적정하게 보호하지 아니하여 정보주체에게 피해가 발생하거나 발생할 우려가 현저한 경우	
국외 이전 중지 명령시 고려사항	1. 국외로 이전되었거나 추가적인 국외 이전이 예상되는 개인정보의 유형 및 규모	
	2. 제28조의8 제1항/제4항/제5항 위반의 중대성 정도	
	3. 정보주체에게 발생하였거나 발생할 우려가 있는 피해가 중대하거나 회복하기 어려운 피해인지 여부	
	4. 국외 이전의 중지를 명하는 것이 중지를 명하지 않았을 경우보다 명백히 정보주체에게 이익이 되는 지 여부	
	5. 법 제64조제1항에 따른 지정조치를 기다려서는 정보주체의 피해를 구제하거나 방지하기가 현저히 곤란한지 여부	
	6. 이전받는 자나 이전 국가/국제기구가 피해구제를 위한 실효적인 절차 등 보호하기 위한 수단과 집행 방안 보유 여부	
	7. 이전받는 자나 이전 국가/국제기구에서 중대한 침해사고가 발생하는 등 보호하기 어렵다 인정할 사유가 존재하는지 여부	
국외 이전 중지 명하려는 경우 국외이전전문위원회의 평가를 거쳐야 함		
이의제기 하려는 자는 이의신청서에 이의 내용, 사유 및 증명 서류를 첨부하여 보호위원회에 제출		
국외 이전 중지 명령을 받은 처리자는 명령을 받은 날부터 7일 이내에 보호위원회에 이의를 제기할 수 있음		
이의제기하려는 자는 이의신청서에 이의신청 사유를 증명할 수 있는 서류를 첨부하여 보호위원회에 제출해야 함		
보호위원회는 서류를 받은 날로부터 30일 이내에 그 처리결과를 처리자에게 문서로 알려야 함		

<p>보호위원회는 국외이전 중지 명령의 해제를 할 수 있음</p> <ol style="list-style-type: none"> 1. 보호위원회가 이전 중지 명령에 해당하지 않는다고 인정하는 경우 2. 보호위원회가 개인정보처리자의 이의제기가 정당하다고 인정하는 경우 3. 그 밖에 보호위원회가 필요하다고 인정하는 경우 <p>국외 이전 중지를 명령받은 처리자가 중지 명령의 해제를 요청하려는 경우 해제신청서와 관련 증빙서류를 첨부하여 제출</p> <p>보호위원회는 제1항에 따라 중지 명령을 해제할 때에는 해당 개인정보처리자에게 문서로 알려야 함</p>	
28-10	<p>상호주의</p> <p>개인정보의 국외 이전을 제한하는 국가의 개인정보처리자에 대해 해당 국가의 수준에 상응하는 제한을 할 수 있음. 조약/국제협정의 이행에 필요시 제외</p>
28-11	<p>준용규정</p> <p>개인정보의 국외 이전받은 자가 제3국으로 이전하는 경우 법 제28조의8 및 제28조의9를 준용</p> <p>국외 이전 관련 세부적인 내용은 향후 반영 예정</p>

제4장 개인정보의 안전한 관리

29 안전조치의무

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 해야함

개인정보의 안전한 처리를 위한 내부관리계획의 수립·시행 및 점검

가. 취급자에 대한 관리·감독 및 교육에 관한 사항

나. 책임자 지정 등 조직의 구성·운영에 관한 사항

다. 접근권한, 접근통제, 암호화, 접속기록 관리, 보안프로그램 관리, 물리적 보안조치 등의 이행에 필요한 사항

개인정보에 대한 접근 권한 제한 조치

가. DB시스템 등 개인정보처리시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행

나. 정당한 권한을 가진 자에 의한 접근여부 확인을 위한 인증수단 적용 기준의 설정 및 운영

다. 그 밖에 개인정보에 대한 접근권한을 제한하기 위해 필요한 조치

개인정보에 대한 접근 통제 조치

가. 개인정보처리시스템에 대한 침입 탐지·차단하기 위해 필요한 조치

나. 취급자의 PC 등에 대한 인터넷망의 차단

(특정 기준 해당하는 개인정보처리자만 해당 : 100만명 이상)

다. 그 밖에 개인정보에 대한 접근을 통제하기 위해 필요한 조치

개인정보를 안전하게 저장·전송하는데 필요한 조치

가. 비밀번호 일방향 암호화 저장 등 인증정보의 암호화 저장 또는 상응 조치

나. 주민등록번호 등 고시에 정하는 정보의 암호화 저장 또는 상응 조치

다. 정보통신망을 통한 개인정보 또는 인증정보를 송·수신하는 경우 해당 정보의 암호화 또는 상응 조치

라. 그 밖에 암호화 또는 이에 상응하는 기술을 이용한 보안조치

개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치

가. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독

나. 개인정보처리시스템에 대한 접속기록의 안전한 보관

다. 그 밖에 접속기록 보관 및 위·변조 방지를 위해 필요한 조치

개인정보에 대한 보안프로그램의 설치 및 갱신

개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

그 밖에 개인정보의 안전성 확보 조치를 위해 필요한 사항

안전성 확보조치 세부기준 (개인정보의 안전성 확보조치 기준, 2023.9.22시행, 개인정보보호위원회고시 제2023-6호)

내부관리계획에 다음 사항을 수립·시행해야 함 (1만명 미만 정보주체 처리 소상공인·개인·단체는 생략 가능)

1. 개인정보 보호 조직의 구성 및 운영에 관한 사항
2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
3. 개인정보보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
5. 접근 권한의 관리에 관한 사항
6. 접근 통제에 관한 사항
7. 개인정보의 암호화 조치에 관한 사항
8. 접속기록 보관 및 점검에 관한 사항
9. 악성프로그램 등 방지에 관한 사항

10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항
11. 물리적 안전조치에 관한 사항
12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
13. 위험 분석 및 관리에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항
16. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항(포함 권고)
- 10만명 이상의 정보주체 처리 대기업·공공기관 등 또는 100만명 이상의 정보주체 처리 중소기업·단체는 의무
17. 출력·복사시 안전조치 (포함 권고)
18. 개인정보의 파기 (포함 권고)
17. 그 밖에 개인정보 보호를 위하여 필요한 사항

중요한 변경이 있는 경우 즉시 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리

개인정보보호책임자는 내부관리계획의 이행실태를 연 1회 이상 점검·관리해야 함
(접근권한 관리, 접속기록, 암호화 조치, 추가적 이용·제공 등)

처리자는 책임자 및 취급자 대상으로 사업규모, 개인정보 보유수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시 (연 1회 이상)

교육목적 및 대상, 교육 내용, 교육 일정 및 방법을 정하여 실시 필요

(접근권한의 관리)

접근권한을 취급자에게만 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여해야 함

취급자 또는 취급자의 업무 변경시 지체없이 시스템 접근 권한 변경 또는 말소해야 함

접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고 최소 3년간 보관해야 함

시스템 접근 계정을 발급하는 경우 **정당한 사유가 없는 한 취급자별로 발급해야**하고, 다른 취급자와 공유 금지

취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리

정당한 권한의 취급자 또는 정보주체만이 접근할 수 있도록 일정 횟수 이상 인증 실패한 경우 접근 제한 등 필요 조치해야 함

(접근통제)

정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 안전조치 수행

1. 접속권한을 IP주소 등으로 제한하여 미인가자 접근 제한

2. 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

취급자가 외부에서 개인정보처리시스템 접속시 안전한 인증수단(인증서, 보안토큰, 일회용 비밀번호 등)을 적용해야함

일반 개인정보처리자의 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 인증수단 적용 가능

개인정보가 권한없는 자에게 공개·유출 방지를 위한 개인정보처리시스템, 취급자PC, 모바일 기기 등에 접근 통제 등 조치

취급자가 일정시간 이상 업무처리 중지시 자동으로 시스템 접속이 차단되도록 보호조치 실시

업무용 모바일 기기의 분실·도난 등으로 개인정보 유출 방지를 위한 모바일 기기에 비밀번호 설정 등 보호조치 실시

업무용PC 또는 모바일 기기를 이용시 운영체제나 보안프로그램 등에서 제공하는 접근통제 기능 이용 가능

100만명 이상 ISP등 개인정보를 다운로드 또는 파기할 수 있거나 시스템 접근 권한을 설정할 수 있는 취급자PC 등에 대해 인터넷망 차단 조치

클라우드컴퓨팅서비스를 이용하는 경우 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치

(개인정보의 암호화)

비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통한 송·수신시 안전한 암호 알고리즘으로 암호화

비밀번호는 일방향 암호화 저장

이용자의 개인정보에 대해 다음 항목은 안전한 암호 알고리즘으로 암호화 저장

고유식별정보, 신용카드번호, 계좌번호, 생체인식정보

이용자가 아닌 정보주체의 개인정보는 다음 항목과 같이 저장하는 경우 암호화

1. 인터넷망 구간, DMZ에 고유식별정보를 저장하는 경우
2. 내부망에 고유식별정보를 저장하는 경우

개인정보 영향평가 결과 및 암호화 미적용시 위험도 분석에 따른 결과에 따라

주민등록번호 외의 고유식별정보에 대해서는 암호화 안할 수 있음 (암호화 권장)

정보통신망을 통하여 개인정보를 인터넷망 구간으로 송·수신시 안전한 암호 알고리즘으로 암호화

이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 취급자의 PC, 모바일 기기 및 보조저장매체 등에 저장시 안전한 암호 알고리즘으로 암호화 저장

암호화된 개인정보를 안전하게 보관하기 위해 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립·시행

10만명 이상의 정보주체 처리 대기업·공공기관 등 또는 100만명 이상의 정보주체 처리 중소기업·단체만 해당

구분		개인정보 처리 유형(처리자별)				
		송수신		저장		
		인터넷구 간 송수신	정보통신망 송수신 (내부망 포함)	이용자 개인정보 (취급자의 컴퓨터, 모바일기기, 보조저 장매체 저장 포함)	이용자 이외 정보주체의 개인정보	
인터넷구간 및 DMZ 저장	내부망 저장			취급자의 컴퓨터, 모바일기기, 보조저장매체에 저장		
모든 개인정보		★		★		
인증 정보	비밀번호	○		○ (일방향)		
	생체인식정보 등	○ (생체인식정보외의 인증정보 포함)				
주민등록번호		○	○	○	○	★ (상용 암호화 SW 또는 안전한 암호화 알고리즘)
여권번호		○	○	○	○	
운전면허번호		○	○	○	(내부망 저장시 영향평가 결과, 위험도 분석 결과를 고려해 정할 수 있음)	
외국인등록번호		○	○	○		
생체인식정보		○	○	○	○	
계좌번호		○		○		
신용카드번호		○		○		

일정규모(10만명 대·중견·공 / 100만명 중소·단체) 이상의 개인정보처리자는 암호키 관리 절차 수립 및 시행 필요

(접속기록의 보관 및 점검)

개인정보처리시스템에 접속한 접속기록은 1년 이상 보관·관리

다음 개인정보처리자는 2년 이상 접속기록을 보관·관리

5만명 이상의 정보주체의 개인정보를 처리하는 개인정보처리시스템

고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템

기간통신사업자에 해당하는 경우

접속기록 등을 월 1회 이상 점검 및 개인정보를 다운로드한 경우 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인

접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하기 위한 조치

(악성프로그램 등 방지)

악성프로그램 등을 방지·치료할 수 있는 백신SW 등의 보안프로그램을 설치·운영

자동 업데이트 기능 사용하거나, **정당한 사유가 없는 한** 일 1회 이상 업데이트를 실시하여 최신 상태 유지

발견된 악성프로그램 등은 삭제 등 대응조치

악성프로그램 경보 발령시 또는 사용 SW에 대한 보안 업데이트 공지가 있는 경우 **정당한 사유가 없는 한** 즉시 업데이트

(물리적 안전조치)

개인정보를 보관하고 있는 물리적 장소(전산실, 자료보관실)를 별도 운영하는 경우 출입통제 절차를 수립·운영

개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관

개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련

업무용PC 또는 모바일 기기만을 이용해 개인정보를 처리시 보안대책 미적용 가능

(재해·재난 대비 안전조치)

100만명 대기업등,
10만명 기업/단체만
해당

화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 조치

1. 위기대응 매뉴얼 등 대응절차 마련 및 정기적 점검

2. 개인정보처리시스템 백업 및 복구를 위한 계획 마련

(출력·복사시 보호조치)

개인정보처리시스템에서 개인정보 출력시(인쇄, 화면표시, 파일생성 등) 용도 특정 및 용도에 따라 출력 항목을 최소화

개인정보가 포함된 종이 인쇄물, 외부 저장매체 등 개인정보의 출력·복사물을 안전 관리를 위해 필요한 안전조치 수행

(개인정보의 파기)

개인정보 파기시 조치 사항

1. 완전파괴(소각·파쇄 등)

2. 전용 소자장비(자기장 이용 삭제 장비)를 이용하여 삭제

3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

개인정보 일부 파기시 상기 방법의 파기가 어려운 경우 조치 사항

1. 전자적 파일 형태인 경우 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독

2. 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 해당 부분을 마스킹, 구멍 뚫기 삭제

기술적 특성(블록체인)으로 파기가 현저히 곤란한 경우 법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하게 조치

개인정보처리자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 않도록 안전성 확보조치

1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 (1만명 미만의 정보주체 개인정보 처리 소상공인·개인·단체는 생략 가능)
2. 개인영상정보에 대한 접근통제 및 접근권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용(네트워크 카메라는 안전한 전송을 위한 암호화, 저장시 비밀번호 설정 등)
4. 처리기록 보관 및 위·변조 방지를 위한 조치 (생성 일시, 열람관련 목적, 열람자, 열람일시 등 기록·관리 조치 등)
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

공공기관의 장이 고정형 영상정보처리기를 설치·운영하는 경우 보호지침의 준수 여부에 대한 자체점검을 실시하여 다음 해 3월 31일까지 결과 등록

자체점검시
고려사항

1. 고정형 영상정보처리기의 운영·관리 방침에 열거된 사항
2. 관리책임자의 업무 수행 현황
3. 고정형 영상정보처리기의 설치 및 운영 현황
4. 개인영상정보 수집 및 이용·제공·파기 현황
5. 위탁 및 수탁자에 대한 관리·감독 현황
6. 정보주체의 권리행사에 대한 조치 현황
7. 기술적·관리적·물리적 조치 현황
8. 고정형 영상정보처리기 설치·운영의 필요성 지속 여부 등

공공기관의 장은 자체점검을 완료한 후에 그 결과를 홈페이지 등에 공개

공공기관 외의 고정형 운영자는 고정형 영상정보처리기 설치·운영으로 정보주체의 침해가 우려되는 경우 자체점검 등 침해방지 적극 노력해야 함

공공시스템 운영기관 등의 개인정보 안전성 확보조치 등

공공시스템 대상 개인정보처리시스템

1. 2개 이상의 공통 또는 유사한 업무 지원을 위해 단일 시스템 구축, 다른 기관 접속·이용할 수 있는 아래의 시스템 중 하나
 - 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
 - 나. 개인정보처리시스템에 대한 취급자의 수가 200명 이상인 시스템
 - 다. 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보를 처리하는 시스템
2. 2개 이상의 공통 또는 유사한 업무 지원을 위해 표준시스템 개발, 다른 기관이 운영할 수 있도록 배포한 표준배포시스템으로 대국민 서비스를 위한 행정업무 또는 민원업무 처리용으로 사용하는 경우
3. 기관의 고유한 업무 수행을 지원하기 위해 기관별로 운영하는 아래의 개별 시스템 중 하나
 - 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
 - 나. 개인정보처리시스템에 대한 취급자의 수가 200명 이상인 시스템
 - 다. 주민등록정보시스템과 연계하여 운영되는 시스템
 - 라. 총 사업비가 100억원 이상인 시스템

공공시스템 대상 제외 개인정보처리시스템

1. 체계적인 개인정보 검색이 어려운 경우
2. 내부적 업무처리만을 위해 사용되는 경우
3. 그 밖에 개인정보가 유출될 가능성이 상대적으로 낮은 경우 보호위원회가 인정 시

공공시스템운영기관은 공공시스템에 대해 추가적인 안전성 확보조치해야함

1. 공공시스템별 내부관리계획에 안전성 확보조치 내용에 다음이 포함
 - 가. 공공시스템운영기관 관리책임자의 지정에 관한 사항
 - 나. 관리책임자의 역할 및 책임에 관한 사항
 - 다. 취급자의 역할 및 책임에 관한 사항
 - 라. 취급자에 대한 관리·감독 및 교육에 관한 사항
 - 마. 접근 권한의 관리에 관한 사항
 - 바. 접근 통제에 관한 사항
 - 사. 접속기록 보관 및 점검에 관한 사항

아. 공공시스템운영기관의 접근 권한의 관리에 관한 사항(고시 제16조)	
1). 공공시스템 접근권한 부여·변경·말소시 인사정보와 연계	
2). 인사정보에 미등록된 자는 계정 발급 금지	
3). 계정 발급시 개인정보보호 교육 실시 및 보안서약서 징구 긴급상황 등 불가피한 경우 그 사유를 접근권한 관리대장에 기록 및 보관	
4). 정당한 권한의 취급자에게만 접근권한이 부여·관리되는지 여부 확인 접근관리 대장 등을 이용하여 부여·변경·말소 내역을 반기별 1회 이상 점검	
5). 이용기관은 소관 취급자 계정발급 등 접근권한의 부여·관리를 직접하는 경우 상기 조치 수행 인사정보 등록자만 계정 발급, 계정 발급시 교육, 관리대장 반기별 1회 이상 점검	
자. 공공시스템운영기관의 접속기록의 보관 및 점검에 관한 사항(고시 제17조)	
1). 접속기록 등을 자동화된 방식으로 분석하여 불법적인 개인정보 유출 및 오·남용 시도 탐지하고 그 사유를 소명하도록 하는 등 필요한 조치해야 함	
2). 이용기관이 소관 취급자의 접속기록을 직접 점검할 수 있는 기능을 제공해야 함	
2. 공공시스템이용기관이 취급자에게 접근권한 부여·변경·말소 등을 할 수 있는 접근권한의 안전한 관리를 위해 필요한 조치	
3. 개인정보에 대한 불법 접근 및 침해사고 방지를 위한 공공시스템 접속기록의 저장·분석·점검·관리 등의 조치	
공공시스템 운영기관 및 이용기관은 불법적인 접근 사실이 확인되는 경우 지체없이 정보주체에게 관련 사항(해당 사실, 피해 예방 등)을 통지	
통지 예외 사항	1. 개인정보 유출에 따라 정보주체에게 개인정보의 분실·도난·유출에 대해 통지한 경우
	2. 다른 법령에 따라 정보주체에게 개인정보에 접근한 사실과 피해 예방 등을 위해 필요한 사항을 통지한 경우
공공시스템운영기관 및 개발·배포공공기관은 공공시스템 규모, 특성, 이용기관의 수를 고려하여 전담부서 지정하여 운영하거나 전담인력 배치해야 함	
공공시스템운영기관은 공공시스템별 총괄 관리 부서의 장을 관리책임자로 지정. 총괄관리 부서가 없는 경우 관련 부서의 장 중에서 관리책임자를 지정	
공공시스템운영기관은 안전성 확보조치 이행상황 점검 및 개선 사항 협의를 위해 공공시스템운영협의회를 공공시스템별로 설치·운영해야 함. 2개 이상의 공공시스템을 운영하는 경우에는 통합하여 설치·운영 가능	
협의회 구성 대상 기관	1. 공공시스템운영기관
	2. 공공시스템 운영을 위탁하는 경우 해당 수탁자
	3. 공공시스템운영기관이 필요하다고 인정하는 공공시스템이용기관

30 개인정보 처리방침의 수립 및 공개

개인정보처리자는 개인정보 처리방침을 수립·공개

공공기관의 개인정보 처리방침은 보호위원회에 등록된 개인정보파일에 한정
(등록대상이 아닌 개인정보파일에 대한 내용은 처리방침에 기재 및 공개 불필요)

포 합 내 용	0. 제목 및 서문
	1. 개인정보의 처리 목적
	2. 개인정보의 처리 및 보유 기간
	3. 개인정보의 제3자 제공에 관한 사항(해당시)
	4. 개인정보의 파기절차 및 파기방법 (다른 법령에 따라 보존하는 경우 보존근거와 보존하는 개인정보 항목을 포함)
	5. 제23조제3항에 따라 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당시) - 재화/서비스 제공과정에서 공개되는 문제

6. 개인정보처리의 위탁에 관한 사항(해당시) - 수탁자 담당자 연락처, 수탁자의 관리현황 점검 결과 등
7. 가명정보의 처리 등에 관한 사항(해당시) - 제28조의2 및 제28조의3에 따른 가명정보만 해당
가. 가명정보 처리 목적
나. 가명정보 처리 및 보유 기간(선택)
다. 가명정보 제3자 제공에 관한 사항(해당시)
라. 가명정보 처리의 위탁에 관한 사항(해당시)
마. 처리하는 가명정보의 항목
바. 가명정보의 안전성 확보 조치에 관한 사항
8. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
9. 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항 담당자, 부서의 명칭과 전화번호 등 연락처
10. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당시)
11. 처리하는 개인정보의 항목
12. 개인정보의 안전성 확보 조치에 관한 사항
13. 개인정보의 추가적인 이용·제공이 지속적 발생 시 판단 기준 등(해당시)
14. 국외에서 국내 정보주체의 개인정보를 직접 수집하여 처리하는 경우 개인정보를 처리하는 국가명(해당시)
15. 개인정보를 국외 이전 시 국외 이전의 근거와 법 제28조의8제2항 각 호의 사항(해당시)
가. 이전되는 개인정보 항목
나. 개인정보가 이전되는 국가, 시기 및 방법
다. 개인정보를 이전받는 자의 성명(법인인 경우 명칭과 연락처)
라. 개인정보를 이전받는 자의 개인정보 이용 목적 및 보유·이용 기간
마. 개인정보의 이전을 거부하는 방법, 절차 및 거부의 효과
16. 개인정보 처리방침의 변경에 관한 사항
17. 국내대리인을 지정하는 경우 국내대리인의 성명, 주소, 전화번호 및 전자우편 주소(해당시)
18. 개인정보의 열람, 정정·삭제, 처리정지 요구권 등 정보주체의 권리·의무 및 그 행사방법에 관한 사항
19. 개인정보의 열람청구를 접수·처리하는 부서
20. 정보주체의 권익침해에 대한 구제방법
21. 개인정보 영향평가 수행 결과 (권장)
22. 개인정보 관리수준진단 결과 (권장)
23. 고정형 및 이동형 영상정보처리기기 운영·관리에 관한 사항 (권장)
24. 14세 미만 아동의 개인정보 처리에 관한 사항 (권장) (해당시)
25. 개인정보 자동 수집 장치를 통해 제3자가 형태정보를 수집 허용 시 수집·이용 및 거부에 관한 사항 (권장) (해당시)
26. 그 밖에 개인정보처리자가 처리 기준 및 보호조치 등에 관해 자율적으로 개인정보 처리방침에 포함하여 정한 사항 (권장)
개인정보 처리방침의 수립·변경시에는 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 게재해야 함

		"개인정보 처리방침", 크기/색상(굵은 글씨체 or 홈페이지 내 다른 글씨와 다른 색깔), 첫페이지에 배치 등 처리방침 변경시 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개해야하며, 변경 전·후 비교 공개해야 함	
방침의 공개방법		운영·관리 방침을 인터넷 홈페이지에 지속적으로 게재	
		인터넷 홈페이지에 게재가 어려운 경우	
	하나 이상의 방법으로 게시	사업장등의 보기 쉬운 장소에 게시	
		관보 또는 시도 이상의 지역을 주된 보급지역으로 하는 신문에 게시	
		같은 제목으로 연2회 이상 발행, 정보주체에 배포하는 간행물 또는 청구서 등에 지속적으로 실기	
		재화나 서비스 제공의 경우는 서로 작성한 계약서 등에 실어 정보주체에게 발급하는 방법	
개인정보 처리방침의 내용과 정보주체와의 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것으로 적용			
30-2	개인정보 처리방침의 평가 및 개선권고		
보호위원회는 개인정보 처리방침에 대해 평가하고 개선 필요시 처리자에게 개인정보 처리 개선을 권고			
평가 사항	개인정보 처리방침에 포함할 사항을 적절하게 정하는지 여부		
	개인정보 처리방침을 알기 쉽게 작성했는지 여부		
	개인정보 처리방침을 정보주체가 쉽게 확인할 수 있는 방법으로 공개 여부		
평가대상의 선정시 고려사항	1. 개인정보처리자의 유형 및 매출액* 규모 (*매출액 미산정시 법인세법 제4조제3항제1호에 따른 수익사업에서 생기는 소득)		
	2. 민감정보 및 고유식별정보 등 처리하는 개인정보의 유형 및 규모		
	3. 개인정보 처리의 법적 근거 및 방식		
	4. 법 위반행위 발생 여부		
	5. 아동·청소년 등 정보주체의 특성		
평가대상 선정시 평가 개시 10전까지 해당 개인정보처리자에게 평가내용·일정 및 절차 등이 포함된 평가계획을 통보			
평가에 필요한 경우 해당 개인정보처리자에게 의견을 제출하도록 요청 가능			
평가 후 그 결과를 지체없이 개인정보처리자에게 통보			
31	개인정보 보호책임자의 지정		
개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자 지정			
지정/변경하는 경우 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 공개해야 함			
책임자 공개시 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개 (책임자와 함께 공개 가능)			
「소상공인기본법」 제2조제1항에 따른 소상공인에 해당하는 개인정보처리자는 미지정 가능, 이 경우 사업주 또는 대표자가 책임자가 됨			
책임자 업무	1. 개인정보 보호 계획의 수립 및 시행		
	2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선		
	3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제		
	4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축		
	5. 개인정보 보호 교육 계획의 수립 및 시행		
	6. 개인정보파일의 보호 및 관리·감독		
	7. 개인정보 처리방침의 수립·변경 및 시행		
	8. 개인정보 처리와 관련된 인적·물적 자원 및 정보의 관리(이전 "개인정보 보호 관련 자료의 관리")		
	9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기		

보호책임자는 필요시 개인정보의 처리 현황, 처리 체계 등에 대해 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있음

보호책임자는 개인정보 보호와 관련하여 법령의 위반사실을 알게 된 경우 즉시 개선조치 실시, 필요시 소속 기관 또는 단체의 장에게 개선조치를 보고

처리자는 보호책임자가 관련 업무를 수행함에 있어서 정당한 이유없이 불이익을 주거나 받게 해서는 안되며 업무를 독립적으로 수행할 수 있도록 보장

공공기관 개인정보 보호책임자 요건

책임자 지정 요건 등

1. 국회, 법원, 헌법재판소, 중선관위의 행정사무를 처리하는 기관 및 중앙행정기관 : 고위공무원단에 속하는 공무원 또는 상당...

2. 1 외 정무직공무원이 장인 국가기관 : 3급 이상 또는 그에 상당하는 공무원)

3. 1 및 2 외 고위공무원, 3급 공무원 또는 상당하는 공무원 이상의 공무원이 장인 국가기관 : 4급 또는 상당...

4. 1~3 이외의 국가기관 : 개인정보처리 업무 담당 부서장

5. 시·도/시·도교육청 : 3급 이상 또는 상당하는 공무원

6. 시·군 및 자치구 : 4급 이상 또는 상당하는 공무원

7. 각급학교-(학교의 행정사무를 총괄하는 사람) - 유/초중고 : 원장/교장

개인정보 보호책임자 자격 요건 강화 요구 대상 대학의 경우 교직원을 말함

8. 1~7 외의 공공기관 : 개인정보처리 업무 담당 부서장. 단, 2명 이상인 경우 기관장이 지명하는 부서의 장

공공기관 외 개인정보처리자의 개인정보 보호책임자 요건

사업주 또는 대표자, 임원(임원이 없는 경우 개인정보 처리 관련 업무를 담당하는 부서의 장)

개인정보 보호책임자 자격요건 강화 요구 대상 개인정보처리자 (공공기관, 지방공사·지방공단, 특수법인, 각급 학교 중에서)

개인정보보호/정보보호/정보기술 경력을 총 4년 이상 필수로 보유하고
그 중 개인정보보호 경력을 2년 이상 보유

동일 기간에 두 가지 이상 업무가 중복되는 경우 하나의 경력만 인정

학위를 취득한 경우 경력을 인정할 수 있으나 여러 학위 등에 대해 처리자가 정하는 하나의 학위만 인정

그 밖의 보호위원회가 고시하는 자격 취득, 교육을 이수한 경우 고시하는 바에 따라 경력으로 인정

별표 1

학위별 경력 인정 기간

구분	경력 인정 요건	인정기간
개인정보 보호경력	개인정보보호 관련 박사학위 취득자	2년
	개인정보보호 관련 석사학위 취득자	1년
	개인정보보호 관련 학사학위 취득자	6개월
정보보호 경력	정보보호 관련 박사학위 취득자	2년
	정보보호 관련 석사학위 취득자	1년
	정보보호 관련 학사학위 취득자	6개월
정보기술 경력	정보기술 관련 박사학위 취득자	2년
	정보기술 관련 석사학위 취득자	1년
	정보기술 관련 학사학위 취득자	6개월

별표 1의 자격요건을 갖추어야 하는 개인정보처리자 요건

1. 연간 매출액등이 1,500억원 이상인 자로

가. 5만명 이상 정보주체의 민감정보 또는 고유식별정보 처리

나. 100만명 이상 정보주체의 개인정보 처리

2. 직전 연도 12/31 기준 학생 수(대학원 재학생 포함)가 2만명 이상인 대학

3. 의료법(제3조의4)에 따른 상급종합병원

4. 공공시스템운영기관

보호위원회는 보호책임자에 대한 교육과정을 개설·운영하는 등 지원 가능

보호위원회는 보호책임자 역량 강화를 위해 경력 개발 및 직무 수행과 관련된 교육과정을 운영 가능
보호위원회가 주관 or 위탁한 기관이 운영하는 교육과정을 이수한 경우 다음 경력 인정 요건을 갖춘 것으로 봄

구분	경력 인정 요건	인정기간
개인정보 보호경력	ISMS-P 인증심사원	1년
	개인정보 영향평가 전문인력	
	변호사법 제4조에 따른 변호사 자격 취득자	
정보보호, 정보기술 경력	정보관리기술사, 컴퓨터시스템응용기술사	1년
	정보보안기사, 정보처리기사	6개월

※ 각각의 자격을 보유한 경우 구분된 경력 내 하나의 자격만 인정하며 구분된 경력별로 중복 인정 가능

인정 교육과정 내 포함 사항

1. 개인정보 관련 법률·정책·제도 및 최신 이슈
2. 개인정보 보호책임자의 역할 및 업무 수행에 필요한 사항
3. 개인정보 처리단계별 관리 방안
4. 개인정보 보호 기술
5. 개인정보 유출사고 대응
6. 개인정보 보호 우수사례
7. 그 밖에 개인정보처리자의 개인정보 보호를 위해 필요한 사항 등

보호위원회/보호위원회의 위탁받은 교육기관은 대면 또는 비대면으로 교육을 운영하고, 교육의 효과를 확인할 수 있는 평가 또는 결과보고서 제출 등 적절한 검증체계를 교육과정에 갖추어야 함

교육을 이수한 경우 최대 3개월 범위 내에서 개인정보 보호경력으로 인정 가능

※ 교육과정, 경력 인정 등에 대해서는 고시 발령인 4년 전 교육부터 적용

개인정보처리자는 개인정보 보호책임자의 독립성 보장을 위해 다음 사항 준수

(**"종합적 이해와 전문가적 역량 갖추기"**는 삭제됨)

(소상공인과 같이 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우는 제외)

독립적 업무 수행보장 등의 세부내용	1. 개인정보 처리와 관련된 정보에 대한 접근 보장
	2. 개인정보 보호 계획의 수립·시행 및 그 결과에 대해 정기적으로 대표자 및 이사회에 직접 보고할 수 있는 체계의 구축
	3. 업무 수행에 적합한 조직체계의 마련 및 인적·물적 자원의 제공
	4. 부당한 자서에 대한 불어행을 이유로 한 불어약의 금지 (해당 항목 삭제됨)

개인정보처리자는 공동의 사업 수행을 위해 개인정보 보호책임자 협의회를 구성·운영 가능

공동의 사업	1. 개인정보처리자의 개인정보 보호 강화를 위한 정책의 조사, 연구 및 수립 지원
	2. 개인정보 침해사고 분석 및 대책 연구
	3. 개인정보 보호책임자 지정·운영, 업무 수행 현황 등 실태 파악 및 제도 개선을 위한 연구
	4. 개인정보 보호책임자 교육 등 개인정보 보호책임자의 개인정보 보호 역량 및 전문성 향상
	5. 개인정보 보호책임자의 업무와 관련된 국내외 주요 동향의 조사, 분석 및 공유
	6. 그 밖에 개인정보처리시스템등의 안전한 관리를 위하여 필요한 사업

보호위원회는 개인정보 보호책임자 협의회에 필요한 지원 가능

보호위원회는 예산의 범위에서 개인정보 보호책임자 협의회 운영과 사업에 필요한 행정적·재정적 지원을 할 수 있다.

31-2	국내대리인의 지정	
	국내에 주소 또는 영업소가 없는 개인정보처리자 중 일정 요건에 해당하는 개인정보처리자는 국내대리인을 문서로 지정	
	국내대리인의 대리사항	개인정보 보호책임자의 업무
		개인정보 유출 등의 통지 및 신고
		물품·서류 등 자료의 제출
	국내대리인 지정대상요건	전년도 전체 매출액이 1조원 이상인 자(전년도 평균환율을 적용하여 원화로 환산한 금액 적용)
		전년도말 기준 직전 3개월간 저장·관리되는 개인정보의 수가 일일평균 100만명 이상
		법 63조제1항에 따라 관계 물품·서류 등 자료의 제출을 요구받은 자로서 지정 필요가 있다고 보호위원회가 심의·의결한 자
	국내대리인은 국내에 주소 또는 영업소가 있어야 함	
	개인정보처리자는 국내대리인을 지정하는 경우 개인정보 처리방침에 추가적으로 내용을 포함	
	국내대리인의 성명(법인의 경우 그 명칭 및 대표자의 성명)	
	국내대리인의 주소(법인의 경우 영업소의 소재지), 전화번호 및 전자우편 주소	
	국내대리인이 대리 사항에 대해 이 법을 위반한 경우 개인정보처리자가 그 행위를 한 것으로 간주	
32	개인정보파일의 등록 및 공개 (공공기관만 해당)	
	공공기관의 장은 개인정보파일을 보호위원회에 등록해야 함 (영향평가를 한 경우 같이 등록)	
	등록주체	교육청, 각급학교 등은 교육부를 통해 보호위원회에 등록해야함
	개인정보파일 운용 취급자는 개인정보보호책임자에게 개인정보파일 등록을 신청해야 함 (신청서식 활용)	
	개인정보 파일 내용	개인정보파일의 명칭
		개인정보파일의 운영 근거 및 목적
		개인정보파일에 기록되는 개인정보의 항목
		개인정보의 처리방법
		개인정보의 보유기간
		개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
		개인정보파일을 운용하는 공공기관의 명칭
		개인정보파일로 보유하고 있는 개인정보의 정보주체 수
		해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서
		개인정보의 열람 요구를 접수·처리하는 부서
		개인정보파일의 개인정보 중 열람을 제한 or 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유
		개인정보 영향평가를 받은 개인정보파일의 경우에는 그 영향평가 결과
		국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속기관 포함)에서 관리하는 개인정보파일
	국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일	
	국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일	
	범죄의 수사, 공소의 제기 및 유지 등에 관한 사항을 기록한 개인정보파일	
	조세관련 법치행위 조사, 관세관련 법치행위 조사 관한 사항 기록 개인정보파일	
	일회적으로 운영되는 파일 등 지속적으로 관리할 필요성이 낮다고 인정되는 개인정보파일로...	
	등록 제외 요건	1. 회의 참석 수당 지급, 자료·물품의 송부, 금전의 정산 등 단순 업무 수행을 위해 운영되는 개인정보파일
		2. 공중위생 등 공공의 안전과 안녕을 위해 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
		3. 그 밖에 일회적 업무 처리만을 위해 수집된 개인정보파일로서 저장되거나 기록되지 않는 개인정보파일
	다른 법령에 따라 비밀로 분류된 개인정보파일	
	CCTV등 영상정보처리기를 통하여 처리되는 개인영상정보파일	
	금융실명거래 및 비밀보장에 관한 법률에 따른 금융기관이 금융업무 취급을 위해 보유하는 개인정보파일	

보호위원회는 필요시 개인정보파일 등록여부와 그 내용을 검토하여 공공기관의 장에게 개선을 권고 가능	
개인정보파일을 운용하는 경우 시작한 날부터 60일내에 등록사항의 등록을 신청하고, 사항이 변경된 경우에도 변경등록을 신청해야 함	
등록절차	초·중·고/교육청 산하기관 → 교육청, 교육청/대학/교육부 산하기관 → 교육부를 거쳐 등록 및 변경등록
교육기관 등은 교육부가 제공하는 '개인정보파일 표준목록'에 따라 등록하고 표준목록에 명시된 기간동안 보유	
개인정보파일대장은 개인정보파일 1개당 1개의 대장을 작성·관리해야 함	
개인정보파일 보존기간이 명시되지 않은 경우 기관장의 결재를 통하고, 공공기록물관리에 관한 법률의 기록관리기준표 이하로 산정해야 함	
기타 세부적인 내용은 표준 개인정보 보호지침 제51조~제61조 참조	

32-2 개인정보 보호 인증

보호위원회는 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관해 인증 가능 유효기간 : 3년 , 사후관리 : 연 1회 이상	
보호위원회는 다음 1호의 경우 인증을 취소하고 2~4호의 경우 인증을 취소할 수 있음	
<ol style="list-style-type: none"> 1. 거짓이나 그 밖의 부정한 방법으로 개인정보 보호 인증을 받은 경우 2. 사후관리를 거부 또는 방해한 경우 3. 인증기준에 미달하게 된 경우 4. 개인정보 보호 관련 법령을 위반하고 그 위반사유가 중대한 경우 	
개인정보 보호 인증 전문기관 : 한국인터넷진흥원, 보호위원회가 지정·고시하는 법인, 단체 또는 기관으로 심사원 5명 이상에 적합 인정 필요	
세부 내용은 영 제34조의2~제34조의8 및 고시(정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시) 참조	

33 개인정보 영향평가(공공기관만 해당)

개인정보파일 운용 또는 변경하기 전에 평가기관을 통해 영향평가를 하고 그 결과를 내부승인절차를 거쳐 2개월 이내에 보호위원회에 제출해야 함	
보호위원회는 제출받은 영향평가 결과에 대해 의견을 제시할 수 있음	
영향평가서에 개선사항으로 지적된 부분에 대한 이행현황을 1년 이내에 보호위원회에 제출해야 함	
영향평가 대상 기준	5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보 포함
	50만명 이상의 정보주체에 관한 개인정보 (7판 내부 또는 외부에 있는 다른 개인정보파일과 연계시 연계결과)
	100만명 이상의 정보주체에 관한 개인정보
	기 영향평가를 받은 개인정보파일의 운용체계를 변경(검색체계 등)하려는 경우 변경된 부분에 한정
영향평가 고려사항	처리하는 개인정보의 수
	개인정보의 제3자 제공 여부
	정보주체의 권리를 해할 가능성 및 그 위험 정도
민감정보 또는 고유식별정보의 처리 여부, 개인정보 보유기간	
영향평가를 한 개인정보파일을 등록할 때에는 영향평가 결과를 함께 첨부해야 함	
보호위원회는 요건을 갖춘 자를 영향평가를 수행하는 기관으로 지정 및 지정취소 가능	
영향평가기관 지정 요건	1. 최근 5년간 다음 하나의 업무 수행의 대가로 받은 금액의 합계액이 2억원 이상인 법인
	영향평가 업무 또는 이와 유사한 업무
	정보시스템 구축 업무 중 정보보호컨설팅 업무
	정보시스템 감리 업무 중 정보보호컨설팅 업무
	정보보호산업에 해당하는 업무중 정보보호 컨설팅 업무 또는 주요정보통신기반시설 관련 정보보호업무

영향평가기관 취소 사유	2. 개인정보 영향평가와 관련된 분야에서의 업무 경력 등 전문인력 10명 이상 상시 고용하는 법인
	3. 신원확인 및 출입통제를 위한 설비를 갖춘 사무실과 기록 및 자료의 안전한 관리를 위한 설비를 구비한 법인
	거짓이나 그 밖의 부정한 방법으로 평가기관의 지정을 받은 경우
	지정된 평가기관 스스로 지정취소를 원하는 경우나 폐업한 경우
	지정요건을 충족하지 못하게 된 경우 신고의무를 이행하지 아니한 경우 그 밖에 법 또는 이 영에 따른 의무를 위반한 경우
보호위원회는 지정을 취소하는 경우 행정절차법에 따른 청문을 실시해야 함	
공공기관 외의 처리자는 개인정보파일 운용으로 인해 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가 하기 위해 노력해야 함	
영향평가의 평가기준 등	
영향평가 내용	해당 개인정보파일에 포함되는 개인정보의 종류·성질, 정보주체의 수 및 그에 따른 개인정보 침해의 가능성
	고유식별정보, 영상개인정보, 법제29조 등의 안전성 확보 조치의 수준 및 이에 따른 개인정보 침해 가능성
	개인정보 침해의 위험요인별 조치 여부
	그 밖에 법 및 규칙에 따라 필요한 조치 또는 의무 위반 요소에 관한 사항
	영향평가 수행 및 관련 절차
영향평가 결과	평가기관은 평가기준에 따라 개인정보 침해의 위험요인을 분석·평가
	평가 결과를 영향평가서로 작성
	1. 영향평가의 대상 및 범위
	2. 평가 분야 및 항목
	3. 평가기준에 따른 개인정보 침해의 위험요인에 대한 분석·평가
영향평가 내용	4. 분석·평가 결과에 따라 조치한 내용 및 개선 계획
	5. 영향평가의 결과
	6. 상기 사항에 대해 요약한 내용
	작성된 영향평가서를 해당 공공기관의 장에게 발송
	공공기관의 장은 개인정보파일을 운용 또는 변경하기 전에 그 영향평가서를 보호위원회에 제출
보호위원회 또는 공공기관의 장은 영향평가서 요약 내용을 공개할 수 있음	
평가기관은 지정된 후 요건, 기관 명칭 등 변경이 발생한 날부터 14일 이내에 신고해야하며, 양도·양수 발생 시에는 60일 이내에 신고해야 함	
영향평가서 내용	개인정보파일 운용과 관련된 사업의 개요 및 개인정보파일 운용의 목적
	영향평가 대상 개인정보파일의 개요
	평가기준에 따른 개인정보 침해의 위험요인에 대한 분석·평가 및 개선 필요 사항
	영향평가 수행 인력 및 비용
영향평가 관련 세부 내용은 영 제35조~38조 및 고시(개인정보 영향평가에 관한 고시) 참조	
34	개인정보 유출 등의 통지
개인정보 유출등이 되었음을 알게 되었을 때에는 서면등의 방법으로 72시간 이내에 해당 정보주체에게 그 사실을 알려야 함	
단, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우 유출 통지 포함 내용에 대해 홈페이지에 30일 이상 게시하는 것으로 통지를 갈음	
(홈페이지를 미운영시 사업장등의 보기 쉬운 장소에 30일 이상 게시하는 것으로 통지 갈음)	

72시간 이내에 정보주체에게 통지하지 않을 수 있는 예외 사유 (단, 해당 사유가 해소된 후 지체없이 통지해야 함)	
1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위해 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우 2. 천재지변이나 그 밖에 부득이한 사유로 72시간 이내에 통지하기 곤란한 경우	
유출 통지 포함 내용	1. 유출된 개인정보의 항목
	2. 유출된 시점과 그 경위
	3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
	4. 개인정보처리자의 대응조치 및 피해 구제절차
	5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
유출등 사고 발생 시점으로부터 72시간 이내에 유출등 통지를 못한 경우 실제 사고를 알게된 시점을 입증해야 함	
유출 관련 항목 및 시점과 경위에 대한 구체적인 내용 확인 불가시 그때까지 확인된 내용 및 그 외 내용(3호~5호)에 대해 서면등의 방법으로 우선 통지	
정보주체에게 유출이 발생한 사실, 통지항목 중 확인된 사항을 먼저 알리고 추후 확인되면 즉시 추가 내용을 포함하여 통지	
유출등이 된 경우 그 피해를 최소화 하기 위한 대책을 마련하고 필요한 조치를 해야 함	
개인정보 유출등에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화하도록 노력해야 함	
개인정보 유출등 사고 발생시 신속한 대응을 통해 피해발생을 최소화하기 위해 "개인정보 유출등 대응 매뉴얼"을 마련해야 함	
대상기관	공공기관, 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자
포함내용	유출등 통지·조치 절차, 영업점·인터넷회선 확충 등 고객 민원 대응조치
	현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등
개인정보의 유형, 경로 및 규모등에 따라 유출 통지 내용을 지체없이 보호위원회 또는 한국인터넷진흥원으로 신고해야 함 (기술 지원을 받을 수 있음)	
1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우	
2. 민감정보 또는 고유식별정보가 유출등이 된 경우	
3. 개인정보처리시스템 또는 취급자의 개인정보 처리 정보기기가 해킹되어 유출등	
구체적인 내용을 확인하지 못한 경우 유출등이 된 사실, 확인된 내용 및 3호~5호 사항을 서면등의 방법으로 우선 신고. 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고	
개인정보처리자는 개인정보 포털(www.privacy.go.kr)을 통하여 유출등 신고 가능. (교육기관은 privacy.moe.go.kr 병행 필요)	
신고 제외 요건	유출등의 경로가 확인되어 해당 개인정보를 회수·삭제 등의 조치를 통해 정보주체 권익 침해 가능성이 현저히 낮아진 경우
유출 유형	개인정보가 포함된 서면, 아동식저장장치, 휴대용컴퓨터등을 분실하거나 도난당한 경우
	개인정보가 저장된 데이터베이스등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
	처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일등 저장매체가 권한이 없는 자에게 잘못 전달된 경우
	커터 권한이 없는 자에게 개인정보가 전달된 경우
유출 정의	개인정보의 분실·도난·유출(유출등)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말한다

34-2	노출된 개인정보의 삭제·차단
	<p>고유식별정보, 계좌정보, 신용카드정보 등 개인정보가 정보통신망을 통하여 공중에 노출되지 않도록 해야 함</p> <p>공중에 노출된 개인정보에 대해 보호위원회 또는 한국인터넷진흥원의 요청이 있는 경우 노출된 개인정보에 대한 삭제·차단 등 필요한 조치 수행</p>

제5장 정보주체의 권리 보장

35	개인정보의 열람
	정보주체는 자신의 개인정보 열람을 해당 개인정보처리자에게 처리자가 마련한 방법과 절차에 따라 요구 가능
열람 요구 사항	1. 개인정보의 항목 및 내용
	2. 개인정보의 수집·이용의 목적
	3. 개인정보 보유 및 이용 기간
	4. 개인정보의 제3자 제공 현황
	5. 개인정보 처리에 동의한 사실 및 내용
	정보주체는 공공기관에 열람을 요구할 때에는 직접 열람을 요구하거나 보호위원회에 열람요구서를 제출하여 열람을 요구 가능
	보호위원회를 통한 열람시 열람요구서를 보호위원회에 제출하고 보호위원회는 지체없이 열람요구서를 해당 공공기관에 이송
	개인영상정보의 경우 공공기관 대상으로는 별도로 개인영상정보 열람·존재확인 청구서로 요구해야 함
	개인정보처리자는 열람요구를 받을 때에는 10일 이내 에 정보주체가 해당 개인정보를 열람할 수 있게 해야함.
	열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며 그 사유 소멸시 10일 이내 열람 제공
열람 제한 또는 거절 사유	1. 법률에 따라 열람이 금지되거나 제한되는 경우
	2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
	3. 공공기관이 다음 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우
	가. 조세의 부과·징수 또는 환급에 관한 업무
	나. 각급 학교, 평생교육시설, 그 밖의 법률에 따라 설치된 고등교육기관 성적 평가 또는 입학자 선발에 관한 업무
	다. 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무
	라. 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
	마. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무
	국가안보 사안에 해당시 제공한 제3자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정 가능
	개인정보처리자는 열람 요구방법과 절차가 수집 방법 및 절차에 비해 어렵지 않도록 다음 항목을 준수
<div>1. 서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법으로 제공</div> <div>2. 정당한 사유가 있는 경우외에는 개인정보를 수집한 창구 또는 방법과 동일하게 열람을 요구 가능하게 제공</div> <div>3. 인터넷 홈페이지를 운영하는 경우 홈페이지에 열람 요구 방법과 절차를 공개 (개인정보 처리방침)</div>	

개인정보처리자가 전체 또는 일부 열람 허용시 열람할 개인정보, 열람이 가능한 날짜, 시간, 장소 등을 열람통지서로 정보주체에게 알려야 함	
일부 열람 허용시 그 사유와 이의제기 방법을 포함하여 정보주체에게 알려야함. 즉시 열람할 경우 열람통지서 발급 생략 가능	
개인정보처리자는 정보주체가 열람 요구한 사항 중 일부가 제한되는 경우 그 일부만 열람하도록 제한 가능	
개인정보처리자가 정보주체의 열람을 연기하거나 거절하려는 경우 열람 요구일로부터 10일 이내에 통보 해야 함	
열람, 정정·삭제, 처리정지 또는 동의철회 등의 요구를 받았을 때에는 열람등요구를 한 사람이 본인이거나 정당한 대리인인지 확인해야 함	
공공기관인 개인정보처리자는 행정정보 공동이용을 통해 본인이나 대리인 확인이 가능한 경우 이를 통해 확인해야 함	
행정정보 공동이용을 할 수 없거나 정보주체가 확인에 동의하지 아니하는 경우에는 안함	
정보주체는 개인영상정보에 대해 열람등을 요구할 수 있고 지체없이 필요한 조치를 취해야 함	
개인영상정보 열람등 요구시 본인 또는 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인해야 함	
개인영상정보 열람등 요구시에는 정보주체 자신이 촬영된 개인영상정보에 한함	
개인영상정보 열람등 요구 거절시에는 10일 이내에 서면 등으로 거부 사유를 정보주체에게 통지	
개인영상정보 열람등 요구에 대해 열람 허용 또는 열람 요구 거절시에는 관련 사항을 기록하고 관리해야 함	
기록 내용	1. 개인영상정보 열람등을 요구한 정보주체의 성명 및 연락처
	2. 정보주체가 열람등을 요구한 개인영상정보 파일의 명칭 및 내용
	3. 개인영상정보 열람등의 목적
	4. 개인영상정보 열람등을 거부한 경우 그 거부의 구체적 사유
	5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유
	6. 개인영상정보 열람등의 업무처리 담당자
개인영상정보 이용, 제3자 제공, 파기 및 열람등 요구에 관한 기록 및 관리는 개인영상정보 관리대장을 활용 가능	
개인영상정보 관련 열람등 조치를 취하는 경우 만일 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해 우려 시 해당되는 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 보호조치 필요	

35-2 개인정보의 전송 요구 (시행일 2025.3.13)

정보주체는 처리 능력 등 기준에 해당하는 개인정보처리자에 대해 다음 요건을 모두 충족하는 개인정보를 자신에게 전송할 것을 요구 가능

전송요구 가능 개인정보 요건	1. 정보주체가 전송을 요구하는 개인정보가 정보주체 본인에 관한 개인정보
	가. 개인정보 직접 동의, 민감정보 직접 동의, 고유식별정보 직접 동의에 따라 처리되는 개인정보
모두 충족 필요	나. 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체 요청에 따른 조치 이행에 처리되는 개인정보
	다. 정보주체의 이익이나 공익적 목적을 위해 관계 중행장의 요청에 따라 보호위원회 심의·의결된 개인정보 (법령 규정/법령상 의무 및 공공기관 소관 업무 수행 개인정보, 법령상 허용 민감정보나 고유식별정보)
2. 전송을 요구하는 개인정보가 개인정보처리자가 수집한 개인정보를 기초로 분석·가공하여 별도로 생성한 정보가 아닐 것	
3. 전송을 요구하는 개인정보가 컴퓨터 등 정보처리장치로 처리되는 개인정보	

처리 능력 등 기준에 해당하는 개인정보처리자 (본인대상 정보전송자) 어느 하나에 해당	1. 영리를 목적으로 하는 법인 중 다음 각 목의 요건을 모두 충족하는 자 가. 「중소기업기본법」 제2조에 따른 중소기업이 아닐 것 나. 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 정보주체 수가 일일평균 10만명 이상
	2. 기관·법인 또는 단체 중 전년도 말 3개월 간 저장·관리되고 있는 정보주체 수가 일일평균 100만명 이상인 자
	3. 법 제35조의2제2항에 따른 개인정보처리자
	1. 「의료법」 제3조의4에 따른 상급종합병원 및 보건복지부장관과 협의하여 보호위원회가 고시 기준 해당자
	2. 「전기통신사업법」 기간통신역무를 제공하는 자 중 보호위원회와 과기정통부가 공동으로 정한 고시 기준 해당자
	3. 「전자상거래법」에 따른 통신판매업자/통신판매중개업자 중 하나의 요건에 해당하면서 보호위원회가 고시 기준 해당자
	가. 직전 사업연도의 매출액 또는 직전 3개 사업연도의 평균 매출액이 1,500억원 이상 나. 전년 말 기준 직전 3개월 간 저장·관리 정보주체 수가 일일평균 100만명 이상
	4. 「전기통신사업법」의 부가통신역무를 제공하는 자 중 보호위원회와 과기정통부가 공동으로 정한 고시 기준자
	가. 직전 사업연도의 매출액 또는 직전 3개 사업연도의 평균 매출액이 1,500억원 이상일 것 나. 전년 말 기준 직전 3개월 간 저장·관리 정보주체 수가 일일평균 100만명 이상
	4. 그 밖에 법 제35조의2제1항에 따른 개인정보 전송을 할 능력이 있다고 보호위원회가 정하여 고시하는 자
정보주체는 매출액 등 기준에 해당하는 개인정보처리자에게 전송요구 대상인 개인정보를 기술적으로 허용되는 합리적인 범위에서 다음 각 호의 자에게 전송할 것을 요구할 수 있음	
1. 개인정보관리 전문기관	
2. 대통령령으로 정하는 시설 및 기술 기준을 충족하는 자(일반수신자)	
개인정보를 전송받아 확인하는 자로 전송 요구 관련 제반 시스템, 불법적인 접근 및 침해사고 방지를 위한 보호설비 및 기술, 전송 내역 기록·보관을 위한 시스템 등 보호위원회가 고시하는 시설 및 기술을 갖춘 자	
일반수신자는 법 제35조의3 제1항에 따른 전문기관 지정을 받지 않고 해당 업무를 수행 금지	
매출액 등 기준에 해당하는 개인정보 처리자 요건	1. 「의료법」 제3조의4에 따른 상급종합병원 및 보건복지부장관과 협의하여 보호위원회가 고시 기준 해당자
	2. 「전기통신사업법」 기간통신역무를 제공하는 자 중 보호위원회와 과기정통부가 공동으로 정한 고시 기준 해당자
	3. 「전자상거래법」에 따른 통신판매업자/통신판매중개업자 중 하나의 요건에 해당하면서 보호위원회가 고시 기준 해당자
	가. 직전 사업연도의 매출액 또는 직전 3개 사업연도의 평균 매출액이 1,500억원 이상일 것 나. 전년도 말 기준 직전 3개월 간 저장·관리되고 있는 정보주체 수가 일일평균 100만명 이상일 것
	4. 「전기통신사업법」의 부가통신역무를 제공하는 자 중 보호위원회와 과기정통부가 공동으로 정한 고시 기준 해당자
제3자대상 정보전송자	가. 직전 사업연도의 매출액 또는 직전 3개 사업연도의 평균 매출액이 1,500억원 이상일 것 나. 전년도 말 기준 직전 3개월 간 저장·관리되고 있는 정보주체 수가 일일평균 100만명 이상일 것
	나. 전년도 말 기준 직전 3개월 간 저장·관리되고 있는 정보주체 수가 일일평균 100만명 이상일 것
시설 및 기술 기준을 충족하는 자 요건 : 현재 행정예고안 등 관련 사항 없음	

상기 개인정보 전송을 요구받은 개인정보처리자는 일부 법률의 규정에도 불구하고 정보주체에 관한 개인정보를 전송해야 함	
전송필요 법률의 규정	국세기본법 제81조의13 및 지방세기본법 제86조 및 그 밖의 유사 대통령령으로 정하는 법률의 규정
정보주체는 전송 요구를 철회할 수 있음	
정보주체의 본인 여부가 확인되지 아니하는 경우 등에는 전송 요구를 거절하거나 전송을 중단 가능	
전송 대상 정보에서 제외 가능한 정보	1. 정보의 전송으로 인하여 제3자의 권리나 정당한 이익을 침해하거나 침해할 우려가 있는 정보 다른 법령에 따라 정보주체 본인이 제공받거나 열람할 수 있는 정보는 제외
	2. 복호화되지 아니하도록 일방향 암호화하여 저장된 정보
	3. 전송시 본인 대상 정보전송자의 정상적인 업무 수행에 현저한 지장을 주는 경우 등 본인 대상 정보전송자의 시간/비용/기술 등을 고려, 합리적인 범위를 벗어나 전송 요구에 응하기에 어렵다고 판단된 정보
	4. 본인 대상 정보전송자가 시스템 내부관리 목적으로 보유한 개인정보 등 명백히 정보주체 권리 관련성 없다고 판단된 정보
	5. 그 밖에 제1호부터 제4호까지와 유사한 사항으로서 보호위원회가 정하여 고시하는 정보
정보주체는 법 제35조의2제2항에 따라 제3자 대상 정보전송자에 대하여 다음 각 호의 정보를 법 제35조의2제2항 각 호의 자에게 전송할 것을 요구 가능	
정보주체가 제3자 대상 정보전송자에 개인정보관리 전송 가능한 정보	1. 제3자 대상 정보전송자가 보유한 어느 하나에 해당하는 보건의료정보로서 복지부와 협의하여 보호위원회가 고시하는 정보 가. 진단내역, 처방내역, 검체·영상·병리검사결과 등 「의료법」22조/23조에 따라 환자진료 등 관련 생성된 정보 나. 처방약품명과 일수, 조제 내용 및 복약지도 내용 등 「약사법」 제30조에 따라 조제 등과 관련하여 생성된 정보 다. 「의료기기법」의 의료기기(「의료기기산업법」에 따른 혁신의료기기를 포함한다)를 통해 생성·수집된 정보 라. 그 밖에 가목부터 다목과 유사한 정보로서 복지부장관이 인정하는 보건의료 분야 기관·단체가 보유한 정보
	2. 제3자 대상 정보전송자가 보유한 기간통신서비스 가입정보 및 이용정보, 청구정보, 납부정보 등 「전기통신사업법」 제2조제11호에 따른 기간통신역무에 관한 정보로서 보호위원회와 과기정통부가 공동으로 정하여 고시하는 정보
	3. 제3자 대상 정보전송자가 보유한 주문정보, 구매정보, 이용정보, 지불정보 등 제42조의2제2항제3호에 해당하는 자가 상품 또는 서비스를 거래하거나 거래를 중개하기 위해 처리하는 정보로서 보호위원회가 정하여 고시하는 정보
	4. 그 밖에 제3자 대상 정보전송자가 보유한 부가통신역무에 관한 정보로서 보호위와 과기정통부가 공동으로 고시하는 정보
	시행령 42조의4 제2항까지 검토한 내용
정보주체는 전송 요구로 인하여 타인의 권리나 정당한 이익을 침해해서 안됨 (침해할 경우에 대한 거절 및 중단 내용 포함 확인 필요)	

35-3 개인정보관리 전문기관

개인정보관리 전문기관은 보호위원회 또는 관계 중행장으로부터 지정을 받아야 함	
개인정보관리 전문기관 수행업무	1. 개인정보의 전송 요구권 행사 지원
	2. 정보주체의 권리행사를 지원하기 위한 개인정보 전송시스템의 구축 및 표준화
	3. 정보주체의 권리행사를 지원하기 위한 개인정보의 관리·분석
	4. 그 밖에 정보주체의 권리 행사를 효과적으로 지원하기 위해 정한 업무
제3자 대상 정보전송자가 보유한 보건의료정보등에 대한 권리행사 지원을 위한 개인정보의 관리·분석 업무	

개인정보관리 전문기관 지정요건	1. 개인정보를 전송·관리·분석할 수 있는 기술수준 및 전문성					
	2. 개인정보를 안전하게 관리할 수 있는 안전성 확보조치 수준					
	3. 개인정보관리 전문기관의 안정적인 운영에 필요한 재정능력					
현재 행정예고안 등 관련 사항 없음						
개인정보관리 전문기관 지정취소요건	1. 거짓이나 부정한 방법으로 지정을 받은 경우					
	2. 개인정보관리 전문기관 지정요건을 갖추지 못하게 된 경우					
보호위원회 및 관계 중행장은 지정을 취소하는 경우에는 행정절차법에 따른 청문을 실시해야 함						
보호위원회 및 관계 중행장은 개인정보관리 전문기관에 대해 업무 수행에 필요한 지원 가능						
개인정보관리 전문기관은 정보주체의 요구에 따라 업무를 수행하는 경우 정보주체로부터 그 업무 수행에 필요한 비용 수취 가능						
세부 대통령령...	현재 행정예고안 등 관련 사항 없음					
35-4	<p>개인정보 전송 관리 및 지원</p> <p>보호위원회는 제35조의2 제1항 및 제2항에 따른 개인정보처리자 및 개인정보관리 전문기관 현황, 활용내역 및 관리실태 등을 체계적으로 관리·감독</p> <p>보호위원회는 개인정보가 안전하고 효율적으로 전송될 수 있도록 개인정보 전송 지원 플랫폼을 구축·운영 가능</p> <table> <tr> <td rowspan="4">개인정보 전송 지원 플랫폼 포함내용</td><td>1. 개인정보관리 전문기관 현황 및 전송 가능한 개인정보 항목 목록</td></tr> <tr> <td>2. 정보주체의 개인정보 전송 요구·철회 내역</td></tr> <tr> <td>3. 개인정보의 전송 이력 관리 등 지원 기능</td></tr> <tr> <td>4. 그 밖에 개인정보 전송을 위하여 필요한 사항</td></tr> </table> <p>보호위원회는 플랫폼의 효율적 운영을 위해 개인정보관리 전문기관에서 구축·운영하는 전송시스템을 상호 연계하거나 통합 가능</p> <p>이 경우 보호위원회는 관계 중행장 및 해당 개인정보관리 전문기관과 사전에 협의해야 함</p> <p>현재 행정예고안 등 관련 사항 없음</p>	개인정보 전송 지원 플랫폼 포함내용	1. 개인정보관리 전문기관 현황 및 전송 가능한 개인정보 항목 목록	2. 정보주체의 개인정보 전송 요구·철회 내역	3. 개인정보의 전송 이력 관리 등 지원 기능	4. 그 밖에 개인정보 전송을 위하여 필요한 사항
개인정보 전송 지원 플랫폼 포함내용	1. 개인정보관리 전문기관 현황 및 전송 가능한 개인정보 항목 목록					
	2. 정보주체의 개인정보 전송 요구·철회 내역					
	3. 개인정보의 전송 이력 관리 등 지원 기능					
	4. 그 밖에 개인정보 전송을 위하여 필요한 사항					
36	<p>개인정보의 정정·삭제</p> <p>자신의 개인정보를 열람한 정보주체는 처리자에게 정정 또는 삭제를 요구할 수 있으며, 다른 법령에서 개인정보가 수집대상으로 명시된 삭제 요구 불가</p> <p>개인정보처리자가 마련한 방법과 절차에 따라 요구해야 함</p> <p>정정 또는 삭제 요구시 다른 법령 절차 규정을 제외하고는 10일 이내에 개인정보를 조사하여 요구에 따른 필요 조치를 한 후 그 결과를 정보주체에게 통지</p> <p>조치를 한 사실 또는 조치 요구에 따르지 아니한 경우 그 사실 및 이유와 이의제기방법을 정정·삭제 결과 통지서로 통지</p> <p>삭제를 요구 받았을 경우 복구 또는 재생되지 않도록 조치. 다른 법령에서 수집대상으로 명시되어 삭제 불가시 그 내용을 정보주체에게 통지</p> <p>삭제 못하는 경우 그 사실, 이유, 이의제기 방법을 관련 통지서로 해당 정보주체에게 10일 이내에 알려야 함</p> <p>처리자는 정정 또는 삭제 요구시 요구사항 확인에 필요한 증거자료를 정보주체에게 제출하게 할 수 있음 (권고... 본인확인 등)</p> <p>다른 개인정보처리자로부터 개인정보를 제공받아 개인정보파일을 처리하는 경우 정보주체의 요구시 그 요구에 따라 해당 개인정보를 정정·삭제하거나 요구사항을 해당 개인정보를 제공한 기관의 장에게 지체없이 알리고 그 처리 결과에 따라 필요한 조치를 해야함</p>					

37	<div> <div>개인정보의 처리정지 등</div> <div> <p>정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지 요구 또는 동의 철회 가능</p> <p>공공기관은 등록대상 개인정보파일 내의 정보주체 개인정보로 한정</p> <p>개인정보처리자는 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 10일 이내에 개인정보 처리의 전부를 정지하거나 일부를 정지후 결과 통지</p> <p>동의 철회 시 지체없이 수집된 개인정보를 복구·재생 불가능하게 파기 등 필요한 조치. 처리정지 요구 거절 사유에 해당하는 경우 관련 조치 미이행 가능</p> <p>처리정지 요구 거절 또는 동의 철회에 따른 조치 미이행 시 정보주체에게 10일 이내에 그 사유를 알려야함</p> <table border="1"> <tr> <td rowspan="4">요구 거절 사유</td><td>법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우</td></tr> <tr> <td>다른 사람의 생명·신체를 해하거나 타인의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우</td></tr> <tr> <td>공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우</td></tr> <tr> <td>약정한 서비스 제공 불가 등 계약의 이행이 곤란한 경우로 계약 해지 의사를 명확하게 밝히지 아니한 경우</td></tr> </table> <p>처리정지된 개인정보는 지체없이 해당 개인정보의 파기 등 필요한 조치를 해야함</p> <p>처리정지 조치시 초지한 사실을 10일 이내, 처리정지 요구 거절시 그 사실 및 이유와 이의제기방법을 10일 이내에 각각 관련 통지서로 알려야함</p> </div> </div>	요구 거절 사유	법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우	다른 사람의 생명·신체를 해하거나 타인의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우	공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우	약정한 서비스 제공 불가 등 계약의 이행이 곤란한 경우로 계약 해지 의사를 명확하게 밝히지 아니한 경우			
요구 거절 사유	법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우								
	다른 사람의 생명·신체를 해하거나 타인의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우								
	공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우								
	약정한 서비스 제공 불가 등 계약의 이행이 곤란한 경우로 계약 해지 의사를 명확하게 밝히지 아니한 경우								
37-2	<div> <div>자동화된 결정에 대한 정보주체의 권리 등</div> <div> <p>정보주체는 완전히 자동화된 시스템으로 개인정보를 처리하여 이루어지는 결정(자동화된 결정)이 자신의 권리 또는 의무에 중대한 영향을 미치는 경우</p> <p>해당 개인정보처리자에 대해 해당 결정을 거부할 수 있는 권리를 가짐 (직접 동의받은 경우, 법률 규정 또는 법률상 의무 준수, 체결한 계약 이행 또는 체결 과정에서 조치 이행 관련은 거부 불가)</p> <p>정보주체는 자동화된 결정에 대해 거부하는 경우 개인정보처리자가 마련하여 공개한 방법과 절차를 따라야 함</p> <p>개인정보처리자는 거부/설명/검토 요구에 대한 방법과 절차를 마련하는 경우 준수해야 할 사항에 관해 제41조제2항을 준용 (수집 방법과 절차보다 쉽게) 준용하는 경우 "열람 요구"는 "거부·설명등요구"로 본다</p> <p>개인정보처리자는 정보주체가 거부하는 경우 정당한 사유가 없으면 다음의 조치를 하고 그 결과를 정보주체에게 알려야 함</p> <table border="1"> <tr> <td>조치 내용 및 통지 내용</td><td>1. 해당 자동화된 결정을 적용하지 않는 조치 2. 인적 개입에 의한 재처리</td></tr> </table> <p>정보주체는 개인정보처리자가 자동화된 결정을 한 경우에는 그 결정에 대해 설명 등을 요구 가능</p> <table border="1"> <tr> <td rowspan="3">설명 또는 검토 요구 대상</td><td>자동화된 결정에 대해 설명 또는 검토를 요구 가능. 이 경우 개인정보처리자가 마련하여 공개한 방법과 절차를 따라야 함</td></tr> <tr> <td>1. 해당 자동화된 결정의 기준 및 처리 과정 등에 대한 설명 2. 정보주체가 개인정보 추가 등의 의견을 제출하여 처리자가 해당 의견을 자동화된 결정에 반영할 수 있는 지에 대한 검토</td></tr> <tr> <td>개인정보처리자는 정보주체가 자동화된 결정에 대해 "해당 자동화된 결정의 기준 및 처리 과정 등에 대한 설명"을 요구하는 경우 정당한 사유가 없으면 다음 내용을 포함하여 간결하고 의미있는 설명을 정보주체에게 제공해야 함</td></tr> </table> <table border="1"> <tr> <td>제공 설명 내용</td><td>1. 해당 자동화된 결정의 결과 2. 해당 자동화된 결정에 사용된 주요 개인정보의 유형 3. 상기 개인정보의 유형이 자동화된 결정에 미친 영향 등 자동화된 결정의 주요 기준 4. 해당 자동화된 결정에 사용된 주요 개인정보의 처리 과정 등 자동화된 결정이 이루어지는 절차</td></tr> </table> <p>정보주체가 설명을 요구시 개인정보처리자는 정보주체의 권리 또는 의무에 중대한 영향을 미치지 않는 경우 설명없이 아래의 사항 통지 가능</p> </div> </div>	조치 내용 및 통지 내용	1. 해당 자동화된 결정을 적용하지 않는 조치 2. 인적 개입에 의한 재처리	설명 또는 검토 요구 대상	자동화된 결정에 대해 설명 또는 검토를 요구 가능. 이 경우 개인정보처리자가 마련하여 공개한 방법과 절차를 따라야 함	1. 해당 자동화된 결정의 기준 및 처리 과정 등에 대한 설명 2. 정보주체가 개인정보 추가 등의 의견을 제출하여 처리자가 해당 의견을 자동화된 결정에 반영할 수 있는 지에 대한 검토	개인정보처리자는 정보주체가 자동화된 결정에 대해 "해당 자동화된 결정의 기준 및 처리 과정 등에 대한 설명"을 요구하는 경우 정당한 사유가 없으면 다음 내용을 포함하여 간결하고 의미있는 설명을 정보주체에게 제공해야 함	제공 설명 내용	1. 해당 자동화된 결정의 결과 2. 해당 자동화된 결정에 사용된 주요 개인정보의 유형 3. 상기 개인정보의 유형이 자동화된 결정에 미친 영향 등 자동화된 결정의 주요 기준 4. 해당 자동화된 결정에 사용된 주요 개인정보의 처리 과정 등 자동화된 결정이 이루어지는 절차
조치 내용 및 통지 내용	1. 해당 자동화된 결정을 적용하지 않는 조치 2. 인적 개입에 의한 재처리								
설명 또는 검토 요구 대상	자동화된 결정에 대해 설명 또는 검토를 요구 가능. 이 경우 개인정보처리자가 마련하여 공개한 방법과 절차를 따라야 함								
	1. 해당 자동화된 결정의 기준 및 처리 과정 등에 대한 설명 2. 정보주체가 개인정보 추가 등의 의견을 제출하여 처리자가 해당 의견을 자동화된 결정에 반영할 수 있는 지에 대한 검토								
	개인정보처리자는 정보주체가 자동화된 결정에 대해 "해당 자동화된 결정의 기준 및 처리 과정 등에 대한 설명"을 요구하는 경우 정당한 사유가 없으면 다음 내용을 포함하여 간결하고 의미있는 설명을 정보주체에게 제공해야 함								
제공 설명 내용	1. 해당 자동화된 결정의 결과 2. 해당 자동화된 결정에 사용된 주요 개인정보의 유형 3. 상기 개인정보의 유형이 자동화된 결정에 미친 영향 등 자동화된 결정의 주요 기준 4. 해당 자동화된 결정에 사용된 주요 개인정보의 처리 과정 등 자동화된 결정이 이루어지는 절차								

	<p>1. 자동화된 결정에 사용되는 주요 개인정보의 유형과 자동화된 결정의 관계</p> <p>2. 자동화된 결정 과정에서의 고려사항 및 주요 개인정보가 처리되는 절차</p>
	<p>개인정보처리자는 (자동결정 거부시 조치 및 통지/설명 요구시 설명 제공/조치 의견 검토 및 반영결과 통지)에 따라 정보주체의 거부·설명등요구에 따른 조치를 하는 경우 요구받은 날부터 30일 이내에 서면등의 방법으로 알려야 함</p> <p>단, 30일 이내에 어려운 정당한 사유시 정보주체에게 그 사유를 알리고 2회 한정 각각 30일의 범위에서 그 기간을 연장 가능</p>
	<p>개인정보처리자는 자동화된 결정의 기준과 절차, 개인정보가 처리되는 방식 등을 정보주체가 쉽게 확인할 수 있도록 5가지 사항을 공개해야 함</p>
	<p>인터넷 홈페이지 등을 통해 공개하며, 홈페이지를 운영하지 않거나 지속적 알릴 필요가 없는 경우 사전에 서면등의 방법 이용</p>
자동화된 결정의 기준과 절차 공개내용	<p>1. 자동화된 결정이 이루어진다는 사실, 그 목적, 대상 정보주체의 범위</p> <p>2. 자동화된 결정에 사용되는 주요 개인정보의 유형과 자동화된 결정의 관계</p> <p>3. 자동화된 결정 과정에서의 고려사항 및 주요 개인정보가 처리되는 절차</p> <p>4. 자동화된 결정 과정에서 민감정보 또는 14세 미만 아동의 개인정보를 처리시 그 목적 및 처리하는 구체적 항목</p> <p>5. 자동화된 결정에 대해 정보주체가 거부·설명등요구를 할 수 있다는 사실과 그 방법 및 절차</p>
	<p>공개시 정보주체가 쉽게 알고 이해할 수 있도록 표준화·체계화된 용어를 사용하고, 동영상·그림·도표 등 방법 활용 가능</p>
	<p>자동화된 결정을 거부하거나 설명 등을 요구한 경우에는 정당한 사유가 없는 한 적용을 중단하거나 인적 개입에 의한 재처리·설명 등 필요한 조치</p>
	<p>개인정보처리자는 정보주체가 거부하거나 설명 등을 요구한 경우 정당한 사유가 없으면 정보주체가 제출한 의견 반영 여부를 검토하고 반영 여부/결과 통지</p>
	<p>개인정보처리자는 다른 사람의 생명·신체·재산과 그 밖의 이익을 부당하게 침해할 우려 등 정당한 사유가 있어 법 제38조제5항에 따라 거부·설명등요구를 거절하는 경우에는 그 사유를 정보주체에게 지체없이 서면등의 방법으로 알려야 함</p>
	<p>정보주체의 거부·설명등요구에 따른 조치에 관한 세부 사항은 고시에서...</p>
38	<p>권리행사의 방법 및 절차</p> <p>정보주체는 열람/정정·삭제/처리정지, 동의철회 등 요구를 절차에 따라 법정대리인 또는 위임받은 자에게 위임장을 제출하여 하게 할 수 있음</p> <p>간편한 방법을 제공해야하며, 수집시 요구되지 않았던 증빙서류 요구나 추가적인 절차를 요구할 수 없음</p> <p>만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람등 요구 가능</p> <p>개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본 우송을 청구하는 경우)를 청구 가능</p> <p>개인정보 전송 요구 시 전송을 위해 추가로 필요한 설비 등을 함께 고려하여 수수료를 산정 가능</p> <p>열람등요구를 하게된 사유가 개인정보처리자에게 있는 경우 청구 불가</p> <p>수수료 또는 우송료는 국가기관(수입인지), 지방자치단체(수입증지), 기타는 개인정보처리자가 정하는 방법</p> <p>세부 내용 등은 시행령 제47조 참조</p> <p>개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차 마련 및 정보주체가 알 수 있도록 공개</p> <p>개인정보처리자는 열람등요구에 대한 거절 등에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내</p> <p>정보주체 자신의 개인영상정보에 대한 파기를 요구하는 때에는 보존을 요구하였던 개인영상정보에 대해서만 파기를 요구할 수 있음 : 해당 파기조치를 취한 경우에는 그 내용을 기록·관리해야 함</p>

39	<div data-bbox="169 127 336 165" data-label="Section-Header"> 손해배상책임 </div> <div data-bbox="220 174 1501 300" data-label="Text"> <p>정보주체는 개인정보처리자에게 손해배상 청구 가능. 개인정보처리자는 고의 또는 과실이 없음을 입증할 책임 있음 고의 또는 중대한 과실로 개인정보 분실·도난·유출·위조·변조 또는 훼손된 경우 손해액의 5배 이내의 손해배상액을 정함. 다만, 고의 또는 중대한 과실이 없음을 증명한 경우 제외</p> </div> <div data-bbox="220 300 1501 678" data-label="Table"> <table> <tr> <td data-bbox="220 300 336 678">배상액 산정 고려사항</td><td data-bbox="336 300 1501 678"> <ol style="list-style-type: none"> 고의 또는 손해 발생의 우려를 인식한 정도 위반행위로 인하여 입은 피해 규모 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익 위반행위에 따른 벌금 및 과징금 위반행위의 기간·횟수 등 개인정보처리자의 재산상태 개인정보처리자가 유출 등 후 개인정보를 회수하기 위하여 노력한 정도 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도 </td></tr> </table> </div>	배상액 산정 고려사항	<ol style="list-style-type: none"> 고의 또는 손해 발생의 우려를 인식한 정도 위반행위로 인하여 입은 피해 규모 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익 위반행위에 따른 벌금 및 과징금 위반행위의 기간·횟수 등 개인정보처리자의 재산상태 개인정보처리자가 유출 등 후 개인정보를 회수하기 위하여 노력한 정도 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도
배상액 산정 고려사항	<ol style="list-style-type: none"> 고의 또는 손해 발생의 우려를 인식한 정도 위반행위로 인하여 입은 피해 규모 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익 위반행위에 따른 벌금 및 과징금 위반행위의 기간·횟수 등 개인정보처리자의 재산상태 개인정보처리자가 유출 등 후 개인정보를 회수하기 위하여 노력한 정도 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도 		
39-2	<div data-bbox="169 678 416 716" data-label="Section-Header"> 법정손해배상의 청구 </div> <div data-bbox="220 725 1501 808" data-label="Text"> <p>개인정보처리자의 고의 또는 과실로 개인정보 분실·도난·유출·위조·변조 또는 훼손된 경우 300만원 이하의 손해액을 배상 청구 가능</p> </div> <div data-bbox="220 808 1501 860" data-label="Text"> <p>개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없음</p> </div> <div data-bbox="220 860 1501 943" data-label="Text"> <p>법원은 청구가 있는 경우 변론 전체의 취지와 증거조사의 결과를 고려하여 300만원 이하의 범위에서 손해액을 인정 가능</p> </div> <div data-bbox="220 943 1501 994" data-label="Text"> <p>법정손해배상 청구한 정보주체는 사실심의 변론이 종결 전까지 그 청구를 손해배상책임 청구로 변경 가능</p> </div>		
39-3	<div data-bbox="169 994 320 1032" data-label="Section-Header"> 자료의 제출 </div> <div data-bbox="220 1041 1501 1124" data-label="Text"> <p>법원은 위반 행위로 인한 손해배상청구소송에서 당사자 신청에 따라 상대방 당사자에게 해당 손해의 증명 또는 손해액의 산정 필요 자료의 제출 명령 가능</p> </div> <div data-bbox="220 1124 1501 1176" data-label="Text"> <p>제출명령을 받은 자가 그 자료의 제출을 거부할 정당한 이유가 있는 경우 거부 가능</p> </div> <div data-bbox="220 1176 1501 1258" data-label="Text"> <p>제출명령 받은 자가 그 자료의 제출을 거부할 정당한 이유가 있다고 주장하는 경우에는 그 주장의 당부를 판단하기 위한 자료의 제시 명령 가능</p> </div> <div data-bbox="220 1258 1501 1310" data-label="Text"> <p>법원은 해당 자료를 다른 사람이 보게 하여서는 안됨</p> </div> <div data-bbox="220 1310 1501 1393" data-label="Text"> <p>제출할 자료가 영업비밀에 해당하나 손해의 증명 또는 손해액의 산정에 반드시 필요한 경우에는 정당한 사유로 보지 않음.</p> </div> <div data-bbox="220 1393 1501 1444" data-label="Text"> <p>법원은 제출명령의 목적 내에서 열람할 수 있는 범위 또는 열람할 수 있는 사람을 지정</p> </div> <div data-bbox="220 1444 1501 1527" data-label="Text"> <p>법원은 정당한 이유없이 제출명령을 따르지 아니한 경우 자료의 기재에 대한 신청인의 주장을 진실한 것으로 인정 가능</p> </div> <div data-bbox="220 1527 1501 1671" data-label="Text"> <p>법원은 자료 미제출에 따라 신청인의 주장을 인정하려는 경우 신청인이 자료의 기재에 관해 구체적 주장하기에 현저히 곤란한 사정이 있고 자료로 증명할 사실을 다른 증거로 증명 및 기대하기도 어려운 경우에는 신청인이 자료의 기재로 증명하려는 사실에 관한 주장을 진실한 것으로 인정 가능</p> </div>		
39-4	<div data-bbox="169 1671 320 1709" data-label="Section-Header"> 비밀유지명령 </div> <div data-bbox="220 1718 1501 1843" data-label="Text"> <p>법원은 위반 행위로 인한 손해배상청구소송에서 당사자의 신청에 따른 결정으로 다음 각 호의 자에게 그 당사자가 보유한 영업비밀을 해당 소송의 계속적인 수행 외 목적으로 사용하거나 그 영업비밀에 관련된 이항에 따른 명령을 받은 자 외의 자에게 공개 금지 명령 가능</p> </div> <div data-bbox="220 1843 1501 1926" data-label="Text"> <p>신청 시점까지 다음 각 호의 자가 준비서면의 열람이나 증거조사 외의 방법으로 영업비밀을 이미 취득하고 있는 경우 예외</p> </div> <div data-bbox="220 1926 1501 2051" data-label="List-Group"> <ol style="list-style-type: none"> 다른 당사자(법인의 경우 그 대표자) 당사자를 위하여 해당 소송을 대리하는 자 그 밖에 해당 소송으로 영업비밀을 알게 된 자 </div>		

비밀유지명령을 신청하는 자는 필요한 사유를 모두 소명해야 함				
1. 이미 제출하였거나 제출하여야 할 준비서면, 이미 조사하였거나 조사하여야 할 증거 또는 제39조의3제1항에 따라 제출하였거나 제출하여야 할 자료에 영업비밀이 포함되어 있다는 것				
2. 제1호의 영업비밀이 해당 소송 수행 외의 목적으로 사용되거나 공개되면 당사자의 영업에 지장을 줄 우려가 있어 이를 방지하기 위하여 영업비밀의 사용 또는 공개를 제한할 필요가 있다는 것				
비밀유지명령의 신청은 서면으로 하여야 함				
서면에 포함 내용	1. 비밀유지명령을 받을 자			
	2. 비밀유지명령의 대상이 될 영업비밀을 특정하기에 충분한 사실			
	3. 비밀유지명령을 신청하는 자가 소명해야 하는 사항 2가지의 사유에 해당하는 사실			
법원은 비밀유지명령이 결정된 경우에는 그 결정서를 비밀유지명령을 받을 자에게 송달해야 함				
비밀유지명령은 송달할 결정서가 비밀유지명령을 받을 자에게 송달된 때부터 효력이 발생				
비밀유지명령의 신청을 기각하거나 각하한 재판에 대해서는 즉시항고 가능				
39-5	비밀유지명령의 취소			
	생략			
39-6	소송기록 열람 등의 청구 통지 등			
	생략			
39-7	손해배상의 보장			
개인정보처리자로서 기준에 해당하는 자는 손해배상 및 법정손해배상에 따른 손해배상책임의 이행을 위해 보험 또는 공제에 가입하거나 준비금 적립 필요				
가입대상 개인정보처리자 모두 충족조건	전년도 매출액이 10억원 이상 (매출액을 산정하지 않는 경우 법인세법 제4조제3항제1호에 따른 수익사업에서 생기는 소득)			
	전년도말 기준 직전 3개월간 정보주체(소속 임직원 제외) 수 일일평균 1만명 이상 (합병 등으로 이전받은 경우 받은 시점 기준)			
적용 예외 기관	가. 대통령령으로 정하는 공공기관, 비영리법인 및 단체			
	1. 공운법 제4조에 따른 공공기관, 지방공사와 지방공단, 특별법에 따라 설립된 특수법인, 초중고/대학 (제32조제4항 각호에 해당하는 공공기관은 제외-책임자 자격요건 강화대상)			
	2. 공익법인의 설립·운영에 관한 법률 제2조에 따른 공익법인			
	3. 비영리민간단체 지원법 제4조에 따라 등록된 단체			
	나. 소상공인으로서(소상공인기본법 제2조제1항) 대통령령으로 정하는 자에게 개인정보 처리를 위탁한 자			
	1. 소상공인으로부터 개인정보가 유출등이 되지 않도록 개인정보의 저장·관리 업무를 위탁받은 자			
2. 상기 위탁 업무에 대해 법 제39조 및 제39조의2에 따른 손해배상 이행 보장보험 또는 공제 가입 or 준비금 적립자				
다. 다른 법률에 따라 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립한 개인정보처리자				
가입대상 개인정보처리자가 보험 또는 공제에 가입하거나 준비금을 적립할 경우 최저가입금액 기준은 다음과 같음				
최저가입금액	가입대상 개인정보처리자의 가입금액 산정요소		최저가입금액 (최소적립금액)	평균보험금*
	정보주체수	매출액등		
	100만명이상	800억원 초과	10억원	
		50억원 초과 800억원 이하	5억원	
		10억원원 이상 50억원 이하	2억원	
	10만명이상 100만명 미만	800억원 초과	5억원	
		50억원 초과 800억원 이하	2억원	
		10억원원 이상 50억원 이하	1억원	
	1만명이상 10만명 미만	800억원 초과	2억원	
		50억원 초과 800억원 이하	1억원	
10억원원 이상 50억원 이하		5천만원		
보험 또는 공제 가입과 준비금 적립을 병행하는 경우 합산한 금액이 상기 최저가입금액의 기준 이상이어야 함				

제7장 개인정보 분쟁조정위원회

40 설치 및 구성

위원장 1명을 포함한 30명 이내의 위원으로 구성, 당연직과 위촉위원으로 구성, 임기 2년으로 1차에 한해 연임 가능

보호위원회 위원장이 위촉하며, 대통령령으로 정하는 국가기관 소속 공무원은 당연직위원이 됨

당연직위원	보호위원회의 고위공무원단의 일반직공무원으로서 개인정보 보호에 관한 업무를 담당하는 자 중 보호위 위원장이 지명한 자
위촉위원 요건	개인정보 보호업무를 관장하는 중앙행정기관 고위공무원단 공무원으로 재직하였던 사람 또는 이에 상당하는 공공부문/단체의 직에 재직 또는 재직하였던 사람으로서 개인정보 보호업무를 경험한 사람
	대학이나 공인된 연구기관에서 부교수 이상 또는 이에 상당하는 직에 재직하고 있거나 재직하였던 사람
	판사·검사 또는 변호사로 재직하고 있거나 재직하였던 사람
	개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람
	개인정보처리자로 구성된 사업자단체의 임원으로 재직하고 있거나 재직하였던 사람

분쟁조정 업무 효율성을 위한 조정사건의 분야별 5명 이내의 조정부 구성 가능.

1명은 변호사 자격이 있는 위원으로 구성

분쟁조정위원회 위원장은 조정부의 회의를 소집하고, 소집하려면 회의 날짜·시간·장소 및 안건을 정하여 회의 개최 7일 전까지 조정부의 각 위원에게 알려야 함 긴급한 사정이 있는 경우 예외 가능

조정부의 장은 조정부 위원 중에서 호선

조정부의 구성 및 운영 등에 필요한 세부 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회의 위원장이 정함

분쟁조정위원회에서 위임받은 경우 조정부 의결은 위원회 의결로 간주

재직위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결

분쟁조정위원회 위원장은 분쟁조정위원회의 회의를 소집하려면 회의 날짜·시간·장소 및 안건을 정하여 회의 개최 7일 전까지 각 위원에게 알려야 함

분쟁조정위원회 및 조정부의 회의는 공개하지 않음. 필요하다고 인정시 의결로 당사자 또는 이해관계인에게 방청 허용 가능

분쟁 조정 관련 사항의 전문적인 검토를 위해 분야별 전문위원회(분쟁조정전문위원회-분조전위) 둘 수 있음
분조전위는 위원장 1명을 포함한 10명 이내 위원으로 구성

위원은 분쟁조정위원회 위원장이 임명하거나 위촉하고, 위원장은 위원 중에서 분쟁조정위원회 위원장이 지명

분조전위 위원대상 조건	1. 분쟁조정위원회 위원
	2. 개인정보 보호 관련 업무를 담당하는 중앙행정기관의 관계 공무원
	3. 대학에서 개인정보 보호 분야의 조교수 이상으로 재직하고 있거나 재직하였던 사람
	4. 공인된 연구기관에서 개인정보 보호 관련 분야의 5년 이상 연구경력이 있는 사람
	5. 변호사 자격을 취득한 후 개인정보 보호 관련 분야에 1년 이상 경력이 있는 사람
	6. 그 밖에 개인정보 보호 및 분쟁의 조정과 관련하여 전문지식과 경험이 풍부한 사람

구성 및 운영 등에 필요한 세부 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회 위원장이 정함

보호위원회는 분쟁조정 접수, 사실 확인 등 분쟁조정에 필요한 사무를 처리 가능

해당 사무처리는 보호위원회의 사무기구가 수행

사무기구는 분쟁조정 접수·진행 및 당사자 통지 등 필요 사무를 전자적 처리를 위해 분쟁조정업무시스템을 구축·운영 가능

	<p>분쟁조정위원회, 조정부, 분조전위 회의에 출석한 위원 등에게 예산의 범위에서 수당과 여비 지급 가능</p> <p>공무원인 위원이 그 소관 업무와 직접적으로 관련되어 출석하는 경우 제외</p> <p>기타 분쟁의 조정절차 및 조정업무의 처리 등 운영 및 집단분쟁조정을 위해 필요한 사항은 분쟁조정위원회 의결을 거쳐 분쟁조정위원회 위원장이 정함</p>		
41	<p>위원의 신분보장</p> <p>자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고 본인 의사에 반해 면직되거나 해촉되지 않음</p>		
42	<p>위원의 제척·기피·회피</p> <p>다음 항목에 해당하는 위원은 분쟁조정사건의 심의·의결에서 제척</p> <ol style="list-style-type: none"> 1. 위원/배우자/배우자였던 자가 그 사건의 당사자가 되거나 그 사건에 관해 공동 권리자 또는 의무자 관계 2. 위원이 그 사건의 당사자와 친족이거나 친족이었던 경우 3. 위원이 그 사건에 관해 증언, 감정, 법률자문을 한 경우 4. 위원이 그 사건에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우 <p>당사자는 위원에게 공정한 심의·의결을 기대하기 어려운 사정이 있으면 위원장에게 기피신청 가능. 위원장은 의결없이 기피신청 결정</p> <p>위원이 제척사유 또는 당사자의 기피신청 대상에 해당하는 경우 스스로 그 사건의 심의·의결에서 회피 가능</p>		
43	<p>조정의 신청 등</p> <p>개인정보와 관련한 분쟁의 조정을 원하는 자는 분쟁조정위원회에 분쟁조정을 신청 가능</p> <p>분쟁조정위원회는 당사자 일방으로부터 분쟁조정 신청을 받을 때에는 그 신청내용을 상대방에 알려야함</p> <p>개인정보처리자가 분쟁조정의 통지를 받은 경우에는 특별한 사유가 없으면 분쟁조정에 응해야 함</p> <p>사유에 따라 분쟁조정 불응하려는 경우 분쟁조정 통지를 받은 날부터 10일 이내에 그 사유를 명시하여 불응의사 알려야 함</p>		
44	<p>처리기간</p> <p>분쟁조정 신청을 받은 날부터 60일 이내에 이를 심사하여 조정안 작성해야 함, 부득이한 사정이 있을 경우 의결로 처리기간 연장 가능</p> <p>처리기간을 연장한 경우에는 기간연장의 사유와 그 밖의 기간연장에 관한 사항을 신청인에게 알려야함</p>		
45	<p>자료의 요청 및 사실조사 등</p> <p>분쟁조정위원회는 분쟁조정 신청을 받았을 때에는 조정을 위해 필요한 자료를 분쟁당사자에게 요청할 수 있고 정당한 사유가 없으면 응해야 함</p> <p>분쟁 조정을 위해 사실 확인이 필요한 경우 분조위 위원 또는 분쟁조정 사무기구의 소속 공무원으로 하여금 자료를 조사·열람하게 할 수 있음</p> <p>이 경우 분쟁당사자는 해당 조사·열람을 거부할 정당한 사유가 있을 때 그 사유를 소명하고 조사·열람 거부 가능</p> <p>분조위는 조사·열람시 7일 전까지 조사·열람 대상자에게 문서로 알려야 함. 조사·열람 목적을 침해할 우려가 있는 경우 미리 알리지 않을 수 있음</p> <table border="1"> <tr> <td>사건 알림 문서에 포함할 내용</td><td> <ol style="list-style-type: none"> 1. 조사·열람의 목적 2. 조사·열람의 기간과 장소 3. 조사·열람을 하는 사람의 직위와 성명 4. 조사·열람의 범위와 내용 5. 정당한 사유가 있는 경우 조사·열람을 거부할 수 있다는 사실 6. 정당한 사유없이 조사·열람을 거부·방해 또는 기피할 경우 불이익의 내용 7. 그 밖에 분쟁조정을 위한 조사·열람에 필요한 사항 </td></tr> </table>	사건 알림 문서에 포함할 내용	<ol style="list-style-type: none"> 1. 조사·열람의 목적 2. 조사·열람의 기간과 장소 3. 조사·열람을 하는 사람의 직위와 성명 4. 조사·열람의 범위와 내용 5. 정당한 사유가 있는 경우 조사·열람을 거부할 수 있다는 사실 6. 정당한 사유없이 조사·열람을 거부·방해 또는 기피할 경우 불이익의 내용 7. 그 밖에 분쟁조정을 위한 조사·열람에 필요한 사항
사건 알림 문서에 포함할 내용	<ol style="list-style-type: none"> 1. 조사·열람의 목적 2. 조사·열람의 기간과 장소 3. 조사·열람을 하는 사람의 직위와 성명 4. 조사·열람의 범위와 내용 5. 정당한 사유가 있는 경우 조사·열람을 거부할 수 있다는 사실 6. 정당한 사유없이 조사·열람을 거부·방해 또는 기피할 경우 불이익의 내용 7. 그 밖에 분쟁조정을 위한 조사·열람에 필요한 사항 		

분조위는 조사·열람시 분쟁당사자 또는 분쟁당사자가 지명하는 자가 입회하거나 의견을 진술하도록 요청할 수 있음					
조사·열람을 하는 위원 또는 공무원은 그 권한을 표시하는 증표를 지니고 관계인에게 내보여야 함					
분조위는 분쟁 조정을 위해 필요하다고 인정하면 관계 기관 등에 자료 또는 의견의 제출 등 필요한 협조를 요청 가능					
분쟁조정위원회는 필요시 분쟁당사자나 참고인을 위원회에 출석하도록 하여 그 의견을 들을 수 있음					
분조위는 의견을 들으려면 회의 일시 및 장소를 정하여 회의 개최 15일 전까지 분쟁당사자 또는 참고인에게 출석 통지					
분쟁조정위원회는 법 제45조(자료의 요청 등) 및 제47조(분쟁의 조정)에 따른 사무 수행을 위해 민감정보와 고유식별정보 처리 가능					
45-2	진술의 원용 제한 조정절차에서의 의견과 진술은 소송(해당 조정에 대한 존재심은 제외)에서 원용하지 못함				
46	조정 전 합의 권고 분쟁조정위원회는 분쟁조정 신청을 받았을 때에는 당사자에게 그 내용을 제시하고 조정 전 합의를 권고 가능				
47	분쟁의 조정 분쟁조정위원회는 다음 어느 하나의 사항을 포함하여 조정안을 작성할 수 있고, 작성되면 지체없이 각 당사자에게 제시해야 함 <table border="1" data-bbox="209 891 1520 1055"> <tr> <td rowspan="3">조정안 포함 사항</td><td>조사 대상 침해행위의 중지</td></tr> <tr> <td>원상회복, 손해배상, 그 밖에 필요한 구제조치</td></tr> <tr> <td>같거나 비슷한 침해의 재발을 방지하기 위하여 필요한 조치</td></tr> </table> <p>조정안 제시받은 당사자가 제시받은 날부터 15일 이내에 수락 여부를 알리지 않으면 조정 수락으로 간주 15일 이내에 수락 여부를 알리지 않으면 조정에 수락한 것으로 본다는 사실을 조정안 제시할 때 같이 알려야 함</p> <p>조정안을 거부하려는 당사자는 조정안을 제시받은 날부터 15일 이내에 인편, 등기우편 또는 전자우편의 방법으로 그 의사를 분쟁조정위원회에 알려야 함</p> <p>공무원인 위원이 그 소관 업무와 직접적으로 관련되어 출석하는 경우 제외 해당 사무처리는 보호위원회의 사무기구가 수행 사무기구는 분쟁조정 접수·진행 및 당사자 통지 등 필요 사무를 전자적 처리를 위해 분쟁조정업무시스템을 구축·운영 가능</p> <p>조정내용 수락시 분조위는 조정서 작성, 분조위 위원장과 각 당사자가 기명날인 or 서명 후 조정서 정본을 지체없이 각 당사자 또는 그 대리인에게 송달 15일 이내 의견 제시 없어서 수락한 것으로 간주한 경우 각 당사자의 기명날인 및 서명은 생략 가능하고 조정의 내용은 재판상 화해와 동일한 효력 가짐</p>	조정안 포함 사항	조사 대상 침해행위의 중지	원상회복, 손해배상, 그 밖에 필요한 구제조치	같거나 비슷한 침해의 재발을 방지하기 위하여 필요한 조치
조정안 포함 사항	조사 대상 침해행위의 중지				
	원상회복, 손해배상, 그 밖에 필요한 구제조치				
	같거나 비슷한 침해의 재발을 방지하기 위하여 필요한 조치				
48	조정 거부 및 중지 분조위는 조정하는 것이 적합하지 아니하다고 인정하거나 부정한 목적으로 조정이 신청되었다고 인정시 그 조정을 거부할 수 있음 조정 거부시 조정거부의 사유 등을 신청인에게 알려야 함 신청된 조정사건에 대한 처리절차를 진행하던 중 한 쪽 당사자가 소를 제기하면 그 조정의 처리를 중지하고 이를 당사자에게 알려야 함				
49	집단분쟁조정 피해 또는 권리침해가 다수의 정보주체에게 같거나 비슷한 유형으로 발생시 아래의 경우 위원회에 집단분쟁조정을 의뢰 또는 신청 가능				

<div>집단분쟁조정 대상 요건</div> <div>요건 모두 만족 필요</div>	<div>1. 피해 또는 권리침해를 입은 정보주체의 수가 다음 각 목의 정보주체를 제외하고 50명 이상일 것</div> <div>가. 개인정보처리자와 분쟁해결이나 피해보상에 관한 합의가 이루어진 정보주체</div> <div>나. 같은 사안으로 다른 법령에 따라 설치된 분쟁조정기구에서 분쟁조정 절차가 진행 중인 정보주체</div> <div>다. 해당 개인정보 침해로 인한 피해에 대하여 법원에 소(訴)를 제기한 정보주체</div> <div>2. 사건의 중요한 쟁점이 사실상 또는 법률상 공통될 것</div>
<div>분조위는 의결로써 집단분쟁조정 절차의 개시를 할 수 있고 14일 이상의 기간동안 그 절차의 개시를 공고해야 함</div> <div>분조위는 집단분쟁조정의 당사자가 아닌 정보주체 또는 개인정보처리자로부터 분쟁조정 당사자에 추가로 포함될 수 있도록 하는 신청을 받을 수 있음</div>	
<div>추가로 집단분쟁조정의 당사자로 참가하려면 공고기간에 문서로 참가 신청을 해야함</div> <div>분조위는 참가 신청을 받은 경우 신청기간(공고기간)이 끝난 후 10일 이내에 참가 인정 여부를 문서로 알려야 함</div>	
<div>분조위는 의결로써 집단분쟁조정의 당사자 중 공동의 이익을 대표하기 적합한 1인 또는 수인을 대표당사자로 선임 가능</div>	
<div>집단분쟁조정의 당사자인 정보주체들 중 일부 정보주체가 소를 제기한 경우 그 절차는 계속되면 일부 정보주체들만 그 절차에서 제외</div>	
<div>분조위는 처리자가 조정의 내용을 수락한 경우 조정 당사자가 아닌 자로 피해를 입은 정보주체의 보상계획서를 작성하여 분조위에 제출하도록 권고 가능</div>	
<div>집단분쟁조정의 기간은 14일 이상의 개시 공고가 종료된 날의 다음 날부터 60일 이내, 부득이한 사정이 있는 경우 의결로 처리기간 연장 가능</div>	
<div>집단분쟁조정 절차 개시 공고기간내에 당사자 참가 신청을 추가로 받으면 10일 이내에 참가 인정 여부를 문서로 알려야함</div>	
<div>집단분쟁조정 절차의 개시 공고는 분조위의 인터넷 홈페이지 또는 전국을 보급지역으로 하는 일반 일간신문에 게재하는 방법으로 함</div>	
<div>50</div>	<div>조정절차 등</div> <div>분조위의 운영 및 분쟁조정 절차에 관하여 이 법에서 규정하지 아니한 사항은 민사조정법을 준용</div>
<div>50-2</div>	<div>개선의견의 통보</div> <div>분조위는 소관 업무 수행 관련 개인정보 보호 및 정보주체의 권리 보호를 위한 개선의견을 보호위원회 및 관계 중행장에게 통보 가능</div>

제8장 개인정보 단체소송

51 단체소송의 대상 등

집단분쟁조정을 거부하거나 집단분쟁조정 결과 수락하지 아니한 경우에 법원에 권리침해 행위의 금지·중지를 구하는 소송 제기 가능

단체
소송
가능
단체

1. 「소비자기본법」 제29조에 따라 공정거래위원회에 등록한 소비자단체로서 다음 요건을 모두 갖춘 단체

가. 정관에 따라 상시적으로 정보주체의 권익증진을 주된 목적으로 하는 단체일 것

나. 단체의 정회원수가 1천명 이상일 것

다. 「소비자기본법」 제29조에 따른 등록 후 3년이 경과하였을 것

2. 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 다음 요건을 모두 갖춘 단체

가. 법률상 또는 사실상 동일한 침해를 입은 100명 이상의 정보주체로부터 단체소송의 제기를 요청받을 것

나. 정관에 개인정보 보호를 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동실적이 있을 것

다. 단체의 상시 구성원수가 5천명 이상일 것

라. 중앙행정기관에 등록되어 있을 것

52~57 전속관할, 소송대리인의 선임, 소송허가신청, 소송허가요건 등, 확정판결의 효력, 「민사소송법」의 적용 등 생략

제9장 보칙

58 적용의 일부 제외

다음 개인정보는 제3장에서 제8장까지를 적용하지 않음

1. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보
2. 언론, 종교단체, 정당이 각각 취재·보도, 선교, 입후보자 추천 등 고유 목적을 달성하기 위해 수집·이용하는 개인정보

제외 항목 제3장부터 제7장 모두 제외

주의 의무 필요 최소한의 기간에 최소한의 개인정보만 처리해야하며, 안전한 관리를 위한 필요 조치, 고충처리 등 마련

공개된 장소에 고정형 영상정보처리기를 설치·운영하여 처리되는 개인정보(법령 허용, 범죄 예방 등, 시설안전, 교통관련 영상개인정보) 적용 예외

제외 항목 15조(수집·이용)
22조(동의를 받는방법)
22조의2(아동의 개인정보 보호)
27조(영업양도 등에 따른 개인정보의 이전 제한) 제1항 및 제2항
34조(개인정보 유출 통지 등)
37조(개인정보의 처리정지 등)

동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위한 개인정보

제외 항목 15조(수집·이용)
30조(개인정보 처리방침의 수립 및 공개)
31조(개인정보 보호책임자의 지정)

58-2 적용제외 : 익명정보

시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보(익명정보)는 개보법 적용 제외

59 금지행위

개인정보를 처리하거나 처리하였던 자에 대한 금지행위

거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위

업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위

정당한 권한 없이 또는 허용된 권한을 초과해 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위

60 비밀유지 등

보호위원회의 업무, 영향평가 업무, 분쟁조정위원회의 분쟁조정 업무에 종사하거나 했던 사람은 타인에게 누설 또는 목적외 용도 이용 금지. 다만, 다른 법률에 특별한 규정이 있는 경우에는 가능

제7조의8 및 제7조의9에 따른 보호위원회의 업무

제28조의3에 따른 전문기관의 지정 업무 및 전문기관의 업무

제32조의2에 따른 개인정보 보호 인증 업무

제33조에 따른 영향평가 업무

제35조의3에 따른 개인정보관리 전문기관의 지정 업무 및 개인정보관리 전문기관의 업무

제40조에 따른 분쟁조정위원회의 분쟁조정 업무

61	의견제시 및 개선권고	
		위원회는 개인정보 보호에 영향을 미치는 내용이 포함된 법령/조례에 대해 필요 인정시 심의·의결을 거쳐 관계 기관에 의견 제시 가능
		위원회는 처리자에게 개인정보 처리 실태의 개선을 권고 가능. 권고받은 처리자는 이행을 위해 성실하게 노력하며 조치 결과를 알려야함
		중앙행정기관의 장은 필요시 소관 법률에 따라 처리자에게 개인정보 처리 실태의 개선을 권고 가능. 권고받은 처리자는 조치결과를 알려야함
62	침해 사실의 신고 등	
		개인정보에 관한 권리 또는 이익을 침해받은 사람은 보호위원회에 그 침해 사실을 신고 가능
		한국인터넷진흥원은 개인정보침해 신고센터를 설치·운영해야 함
	신고센터 업무	1. 개인정보 처리와 관련한 신고의 접수·상담 관련해서 딸린 업무 2. 사실의 조사·확인 및 관계자의 의견 청취 및 관련해서 딸린 업무
63	자료제출 요구 및 검사	
		보호위원회는 개인정보처리자에게 아래의 상황발생시 관계 물품·서류 등 자료를 제출하게 할 수 있음
	요구 및 검사 대상	1. 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우
		2. 법 위반에 대한 신고를 받거나 민원이 접수된 경우
		3. 개인정보 유출 등 정보주체의 개인정보에 관한 권리 또는 이익을 침해하는 사건·사고 등이 발생했거나 가능성이 있는 경우
		보호위원회는 처리자가 자료를 제출하지 않거나 법 위반 사실이 인정되면 처리자 및 법 위반 관련 관계인의 사업장에 출입하여 서류 등 검사 가능
		이 경우 검사를 하는 공무원은 그 권한을 나타내는 증표를 지니고 관계인에게 내보여야 함
		보호위원회는 자료의 제출 요구 및 검사 등을 위해 KISA의 장에게 기술적인 사항을 자문하는 등 필요 지원 요청 가능
		보호위원회는 위반행위로 인해 중대한 개인정보 침해사고가 발생한 경우 신속하고 효과적인 대응을 위해 관계 기관의 장에게 협조요청 가능
	협조요청 가능 기관	1. 중앙행정기관 2. 지방자치단체 3. 그 밖에 법령 또는 자치법규에 따라 행정권한을 가지고 있거나 위임 또는 위탁받은 공공기관
		협조요청을 받은 관계 기관의 장은 특별한 사정이 없으면 이에 따라야 함
		자료제출 요구, 검사 절차 및 방법 등에 관한 세부 사항은 "개인정보 보호위원회의 조사 및 처분에 관한 규정" 고시 참조
		보호위원회는 요구에 따라 제출받거나 수집한 서류·자료 등을 이 법에 따른 경우를 제외하고는 제3자 제공 or 일반 공개 금지
		보호위원회는 정보통신망을 통해 자료의 제출 등을 받은 경우나 수집 자료 등을 전자화한 경우 유출되지 않게 보완조치해야 함(제도적/기술적)
63-2	사전 실태점검	
		보호위원회는 제63조제1항이 아닌 경우로 침해사고 발생의 위험성이 높고 취약점을 사전에 점검할 필요시 해당 처리자에 대한 보호실태 점검 가능
		보호위원회는 실태점검을 실시하여 이 법을 위반하는 사항을 발견한 경우 처리자에 시정방안을 정하여 따를 것을 권고 가능

시정권고를 받은 처리자는 통보받은 날부터 10일 이내에 해당 권고를 수락하는지 여부를 보호위원회에 통지하고 그 이행 결과를 보호위원회에 알려야 함
시정권고를 받은 자가 해당 권고를 수락한 때에는 법 제64조 제1항에 따른 시정조치 명령을 받은 것으로 본다
보호위원회는 시정권고를 받은 자가 해당 권고를 수락하지 아니하거나 이행하지 아니한 경우 제63조 제2항에 따른 검사 가능
보호위원회는 관계 중행장과 합동으로 개인정보 보호실태를 점검 가능

64 시정조치 등

보호위원회는 이 법을 위반한 자에 대해 다음 조치를 명할 수 있음

시정조치 내용	개인정보 침해행위의 중지
	개인정보 처리의 일시적인 정지
	그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치
예외 기관	중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 시정조치 대상에서 제외
	중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속기관 및 소관 공공기관이 위반시 시정조치 내용을 명할 수 있음
	보호위원회는 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회가 위반시 지정조치 권고 가능하고 특별한 사유 없는 한 존중

64-2 과징금의 부과

전체 매출액의 3% 이하 과징금 부과. 매출액이 없거나 매출액 산정이 곤란한 경우(공공기관 등) 20억원 이하 범위에서 과징금을 부과

수집·이용 위반(제15조제1항), 제3자 제공 위반(제17조제1항), 목적외 이용·제공 위반(제18조제1항·제2항)

제공받은 자의 이용·제공 위반(제19조)

아동의 개인정보 보호 위반(제22조의2제1항)으로 법정대리인의 동의를 받지 않고 만 14세 미만 아동의 개인정보를 처리

정보주체의 동의를 받지 아니하고 민감정보를 처리한 경우

고유식별정보/주민등록번호 처리 제한 위반(제24조제1항, 제24조의2제1항)하여
고유식별정보·주민등록번호를 처리한 경우

업무위탁 제한(제26조제4항)에 따른 관리·감독 또는 교육을 소홀히 하여 수탁자가 이 법의 규정을 위반한 경우

가명정보 처리 금지의무(제28조의5제1항)를 위반하여 재식별 목적으로 가명정보를 처리한 경우

국외 이전 제한(제28조의8제1항)을 위반하여 개인정보를 국외로 이전한 경우

국외 이전 중지 명령(제28조의9제1항)을 위반하여 국외 이전 중지 명령을 따르지 아니한 경우

개인정보가 유출등이 된 경우. 다만, 방지를 위해 개인정보처리자가 안전성 확보 조치(제29조)에 필요한 조치 다 한 경우 예외

과징금 부과시 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액을 기준으로 과징금을 산정

과징금 부과시 처리자가 정당한 사유없이 매출액 산정의 제출을 거부하거나 거짓의 자료를 제출한 경우에는 해당 처리자의 전체 매출액 기준으로 산정

해당 처리자 및 비슷한 규모 처리자의 개인정보 보유규모, 재무제표 등 회계자료, 상품·용역의 가격 등 자료에 근거 추정 가능

과징금 부과시 위반행위에 상응하는 비례성과 침해예방에 대한 효과성이 확보될 수 있도록 고려

과징금 부과시 고려사항	1. 위반행위의 내용 및 정도
	2. 위반행위의 기간 및 횟수
	3. 위반행위로 인하여 취득한 이익의 규모
	4. 암호화 등 안전성 확보 조치 이행 노력
	5. 개인정보가 유출등이 된 경우 위반행위와의 관련성 및 유출등의 규모
	6. 위반행위로 인한 피해의 회복 및 피해 확산 방지 조치의 이행 여부
	7. 개인정보처리자의 업무 형태 및 규모
	8. 개인정보처리자가 처리하는 개인정보의 유형과 정보주체에게 미치는 영향
	9. 위반행위로 인한 정보주체의 피해 규모
	10. 개인정보 보호 인증, 자율적인 보호 활동 등 개인정보 보호를 위한 노력
	11. 보호위원회와의 협조 등 위반행위를 시정하기 위한 조치 여부
과징금 부과시 예외 사항	1. 지급불능·지급정지 또는 자본잠식 등의 사유로 객관적으로 과징금을 낼 능력이 없다고 인정되는 경우
	2. 본인의 행위가 위법하지 아니한 것으로 잘못 인식할 만한 정당한 사유가 있는 경우
	3. 위반행위의 내용·정도가 경미하거나 산정된 과징금이 소액인 경우
	4. 그 밖에 정보주체에게 피해가 발생하지 아니하였거나 경미한 경우
	개인정보처리자가 위반행위를 시정하고 보호위원회 고시 기준에 해당 하는 경우
	1. 위반행위의 내용·정도가 경미하거나 사소한 부주의나 오류로 인한 위반행위인 경우
	2. 정보주체 피해 미발생 또는 경미한 경우로 위반행위를 시정하고 유출 등의 통지·신고 미위반
구체적인 과징금 산정기준과 산정 절차	
세부 내용은 시행령 제60조의2 참조, 개인정보 보호법 위반에 대한 과징금 부과기준 고시 참조	
과징금을 내야 할 자가 납부기한까지 이를 내지 아니하면 납부기한의 다음날부터 미납 과징금 6%에 해당하는 가산금을 징수(60개월 이내만 적용)	
납부기한까지 내지 아니하면 기간을 정하여 독촉하고, 독촉으로 지정한 기간 내에 과징금과 가산금을 내지 아니하면 국세강제징수의 예에 따라 징수	
과징금을 환급시 낸 날부터 환급날까지 기간에 대해 국세기본법 시행령 제43조의2제2항 본문에 따른 이자율을 적용 하여 환급가산금을 지급	
과징금 부과처분이 취소되어 판결에 따라 새로운 과징금 부과시 기 납부 과징금에서 새로운 과징금을 공제한 나머지 금액에 대해서만 환급가산금을 지급	
세부 내용은 시행령 제60조의3, 제60조의4 및 제60조의5 참조, 개인정보 보호법 위반에 대한 과징금 부과기준 고시 참조	
65	고발 및 징계권고
위원회는 처리자에게 법규의 위반에 따른 범죄혐의 인정되는 이유가 있을 때에는 관할 수사기관에 그 내용을 고발 가능	
위원회는 법규 위반행위가 있다고 인정되는 이유가 있을 때에는 책임자(대표자 및 책임 임원 포함)를 징계할 것을 처리자에게 권고 가능	
관계 중앙행정기관장은 소관 법률에 따라 처리자에 대해 고발하거나 소속기관·단체 등의 장에게 징계권고 가능.	
권고를 받은 사람은 이를 존중해야하며 그 결과를 권고한 보호위원회/관계 중앙행정기관장에게 통보	
개선권고 및 징계권고는 권고사항, 권고사유 및 조치 결과 회신기간 등을 문서로 해야 함	

권고받은 자는 권고 내용에 따라 필요한 조치를 하고, 그 결과를 보호위원회 또는 관계 중행장에게 문서로 통보해야 함

권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보해야 함

66 결과의 공표

보호위원회는 개선권고, 시정조치 명령, 고발 또는 징계권고 및 과태료 부과 내용 및 결과를 공표 가능

보호위원회는 인터넷홈페이지 등에 위반행위 등에 대한 내용을 게재하여 공표 가능

공표 내용	위반행위의 내용
	위반행위를 한 자
	개선권고, 시정조치 명령, 과징금의 부과, 고발, 징계권고, 과태료 부과 내용 및 결과

보호위원회는 개선권고 등을 한 경우에는 처분 등을 받은 자에게 해당 처분 등을 받았다는 사실을 공표할 것을 명할 수 있음

공표의 내용·횟수, 매체와 지면의 크기 등을 정하여 명해야 하며, 처분등을 받은 자와 공표 문안 등에 관해 협의 가능

공표 내용 : 위반행위의 내용, 위반행위를 한 자, 처분등을 받았다는 사실

공표시
고려사항 보호위원회는 위반행위의 내용 및 정도, 위반 기간 및 횟수, 위반행위로 인하여 발생한 피해의 범위 및 결과 등을 고려

보호위원회는 공표 또는 공표명령에 대한 심의·의결 전에 처분등을 받은 자에게 소명자료를 제출하거나 의견 진술 기회를 주어야 함

67 연차보고: 보호위원회는 필요한 자료를 제출받아 매년 개인정보 보호시책 수립 및 시행 관한 보고서를 작성하여 국회에 제출

보호위원회는 관계기관에게 필요 자료를 제출받아 매년 개인정보 보호시책의 수립 및 시행에 관한 보고서를 작성하여 국회에 제출

보고서 포함 내용	1. 정보주체의 권리침해 및 그 구제현황
	2. 개인정보 처리에 관한 실태조사 및 개인정보 보호수준 평가 등의 결과
	3. 개인정보 보호시책의 추진현황 및 실적
	4. 개인정보 관련 해외의 입법 및 정책 동향
	5. 주민등록번호 처리와 관련된 법률·대통령령·국회규칙·대법원규칙 등 및 감사원규칙의 제정·개정 현황
	6. 그 밖에 개인정보 보호시책에 관하여 공개 또는 보고해야 할 사항

68 권한의 위임·위탁

이 법에 따른 위원회/중행장의 권한은 그 일부를 대통령령으로 특별시장, 광역시장, 도지사, 특별자치도지사 또는 전문기관에 위임/위탁 가능

권한을 위임 또는 위탁받은 기관은 위임 또는 위탁받은 업무의 처리 결과를 위원회 또는 관계 중행장에게 통보해야 함

보호위원회는 전문기관에 권한의 일부를 위임하거나 위탁하는 경우 해당 전문기관의 업무 수행을 위해 필요한 경비를 출연 가능

대체가입수단
제공 지원 한국지역정보개발원, 한국인터넷진흥원, 기타 관련 능력과 설비를 보유한 것으로 인정하여 고시한 법인·기관·단체

한국인터넷진흥원 또는 위원회가	1. 개인정보 보호를 위한 국제기구와 외국의 개인정보 보호기구와의 교류·협력
	2. 개인정보 보호에 관한 법령·정책·제도·실태 등의 조사·연구
	3. 개인정보 보호에 관한 기술개발의 지원·보급
	4. 개인정보 보호에 관한 교육·홍보

	정하여 고시한 법인·기관·단 체의 위탁 업무내용	5. 개인정보 보호와 관련된 기관·단체의 육성 및 지원 6. 관계 전문가의 육성 및 영향평가 기준의 개발 7. 개인정보 열람 요구의 접수 및 처리 8. 자료제출 요구 및 검사 중 다음 사항과 관련된 자료 제출 요구 및 검사 개인정보 유출 등의 신고에 대한 기술지원 침해 사실의 신고에 따라 개인정보침해 신고센터에 접수된 신고의 접수·처리 등 상담 보호위원회가 업무를 위탁한 경우 위탁받은 기관과 위탁업무의 내용을 관보나 보호위원회의 인터넷 홈페이지에 공고해야 함
69	벌칙 적용 시의 공무원 의제 위원회 위원 중 공무원이 아닌 위원 및 공무원이 아닌 직원은 "형법"이나 그 밖의 법률에 따른 벌칙 적용시 공무원으로 봄 위원회/중행장의 권한을 위탁한 업무에 종사하는 관계 기관의 임직원은 "형법" 제129조부터 제132조까지의 규정을 적용시 공무원으로 봄 (수뢰/사전수뢰-뇌물 수수/요구, 제3자 뇌물 제공/요구, 수뢰후 부정처사/사후수뢰, 알선수뢰 등의 범죄)	
70	벌칙 (대부분 벌칙 대상에 제26조제8항에 따라 준용되는 경우를 포함 고려 필요) 10년 이하 징역 또는 1억원 이하 벌금 공공기관의 개인정보 처리업무 방해 목적으로 개인정보를 변경하거나 말소하여 업무 수행의 중단·마비 등 지장을 초래한 자 거짓이나 부정한 수단/방법으로 다른 사람이 처리하는 개인정보 취득 후 영리/부정한 목적으로 제3자에게 제공한 자와 이를 교사·알선한 자	
71	5년 이하 징역 또는 5천만원 이하 벌금 (제17조제1항제2호) 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자 (제18조제1항/제2항, 제19조, 제26조제5항, 제27조제3항 또는 제28조의2) 개인정보처리자/제공받은자/수탁자/영업양수자등의 목적외 이용·제공 위반 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 (제22조의2제1항) 위반하여 법정대리인의 동의를 받지 않고 만 14세 미만 아동의 개인정보를 처리한 자 (제23조제1항) 위반하여 민감정보를 처리한 자 (제24조제1항) 위반하여 고유식별정보를 처리한 자 (제28조의3제1항) 전문기관으로 지정받지 아니하고 가명정보를 결합한 자 (제28조의3제2항) 전문기관 승인을 받지않고 외부로 결합된 정보를 반출하거나 제3자에게 제공한자 및 그 사정을 알면서도...제공받은 자 (제28조의5제1항) 재식별 금지를 위반하여 특정 개인을 알아보기 위한 목적으로 가명정보를 처리한 자 (제59조제2호) 개인정보를 처리하였거나 처리하였던 자가 업무상 알게 된 개인정보를 누설하거나 권한없이 다른 사람이 이용하게 제공한 자 및 그 사정을 알면서도 영리/부정 목적으로 개인정보를 제공받은 자 (제59조의제3호) 개인정보 처리하였거나 처리하였던 자가 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자	

72	3년 이하징역 또는 3천만원 이하벌금
	(제25조제5항) 고정형 영상정보처리기기의 설치 목적과 다른 목적으로 고정형을 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자
	(제59조제1호) 개인정보를 처리하였거나 처리하였던 자가 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리/부정한 목적으로 개인정보를 제공받은 자
	(제60조) 보호위원회 업무, 개인정보 보호 인증 업무, 영향평가 업무, 분쟁조정 업무에 종사하거나 종사하였던 자가 직무상 알게된 비밀을 누설하거나 직무상 목적 외에 이용한 자
73	2년 이하징역 또는 2천만원 이하벌금
	(제36조제2항) 개인정보 정정·삭제 등 요구에 필요 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자
	(제37조제2항) 정보주체의 처리정지 요구에도 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자
	(제39조의4) 국내외에서 정당한 이유없이 비밀유지명령을 위반한 자
	비밀유지명령을 신청한 자의 고소가 없으면 공소를 제기 못함
	(제63조제1항) 자료제출 요구에 대해 법 위반사항을 은폐 또는 축소할 목적으로 자료제출을 거부하거나 거짓의 자료를 제출한 자
	(제64조제2항) 출입·검사 시 자료의 은닉·폐기, 접근 거부 또는 위조·변조 등을 통해 조사를 거부·방해 또는 기피한 자
74	양벌규정
	10년 이하 징역 또는 1억원 이하 벌금에 해당하는 위반행위시 법인 또는 개인을 7천만원 이하의 벌금 에 처함
	위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 제외
	2~5년이하 징역 또는 2~5천만원 이하 벌금에 해당하는 위반행위시 법인 또는 개인을 해당 조문의 벌금형을 부과 함
	위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 제외
74-2	몰수·추징 등
	2~10년 이하 징역 또는 2~1억원 이하 벌금에 해당하는 죄를 지은 자가 해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수 가능하며 몰수할 수 없을 때에는 그 가액을 추징 가능 (이 경우 몰수 또는 추징은 다른 벌칙에 부가하여 과할 수 있음)
75	과태료
	5천만원 이하 과태료
	(제25조제2항) 고정형 영상정보처리기기의 설치·운영 제한을 위반하여 사생활 침해 우려 장소의 내부에 설치·운영한 자
	(제25조의2제2항) 이동형 영상정보처리기기로 사생활 침해 우려 장소의 내부의 사람 또는 그 사람 관련 사물의 영상을 촬영한 자

3천만원 이하 과태료

(제16조제3항)(제22조제5항) 최소한의 정보 이외 정보 수집 미동의 또는 선택사항 미동의를 이유로 재화나 서비스 제공을 거부한 자
(제20조제1항·제2항) 정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지를 위반하여 통지내용을 알리지 아니한 자
(제20조의2제1항) 개인정보의 이용·제공 내역이나 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 통지하지 아니한 자
(제21조제1항) 개인정보 파기를 위반하여 개인정보를 파기등 필요한 조치를 하지 아니한 자(가명정보 처리기간 경과 포함)
(제23조제2항)(제24조제3항)(제25조제6항)(제28조의4제1항)(제29조) 위반하여 민감정보, 고유식별정보, 영상개인정보, 가명정보 등에 대해안전성 확보에 필요한 조치를 하지 아니한 자
(제23조제3항) 재화/서비스 제공 과정에서 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 알리지 아니한 자
(제24조의2제1항) (법령주의/이익명백한 경우를 제외하고 처리 금지) 위반하여 주민번호를 처리한 자
(제24조의2제2항) 주민등록번호 암호화 조치를 위반하여 암호화 조치를 하지 아니한 자
(제24조의2제3항) 주민번호 처리 가능여부와 상관없이 홈페이지 회원가입 단계에서 주민번호 이외의 사용 방법을 제공하지 않은 자
(제25조제1항) 공개된 장소 설치할 수 있는 경우 이외에 고정형 영상정보처리기를 설치·운영한 자
(제25조의2제1항) 업무 목적으로 공개된 장소에 촬영할 수 있는 경우 이외에 이동형 영상정보처리기로 사람 또는 그 사람 관련 사물의 영상을 촬영한 자
(제26조제3항) 재화/서비스 홍보하거나 판매를 권유하는 업무를 위탁하는 경우 그 업무 내용과 수탁자를 정보주체에게 알리지 아니한 자
(제28조의5제2항) 개인을 알아볼 수 있는 정보가 생성되었음에도 이용을 중지하지 아니하거나 이를 회수·파기하지 아니한 자
(제28조의8제4항) 개인정보 국외 이전하는 경우 관련 보호조치를 하지 아니한 자(안전성 확보조치, 고충처리/분쟁해결 조치, 기타 필요조치 등)
(제32조의2제6항) 개인정보 보호 인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한 자
(제33조제1항) 공공기관의 장이 개인정보 영향평가를 하지 아니하거나 그 결과를 보호위원회에 제출하지 아니한 자
(제34조제1항) 정보주체에게 개인정보 유출 통지 내용을 알리지 아니한 자
(제34조제3항) 개인정보 유출등으로 신고대상에 해당하나 보호위원회 또는 한국인터넷진흥원으로 신고하지 아니한 자
(제35조제3항) 개인정보 열람요구를 받았음에도 불구하고 정당한 사유없이 열람을 제한하거나 거절한 자
(제35조의3제1항) 개인정보관리 전문기관 지정을 받지않고 업무를 수행한 자
(제35조의3제3항) 개인정보관리 전문기관 금지 행위를 한 자(전송요구 강요 또는 부당하게 유도, 정보주체 권리 제한 우려 행위 등)
(제36조제2항) 개인정보 정정·삭제요구를 받았음에도 불구하고 정당한 사유없이 정정·삭제 등 필요한 조치를 아니한 자
(제37조제3항 또는 제5항) 동의 철회에 따른 파기 또는 처리가 정지된 개인정보에 대해 파기 등 필요한 조치를 위반한 자

(제37조의2제3항) 자동화된 결정 거부하거나 이에 대한 설명을 요구한 경우 정당한 사유없이 정보주체의 요구에 따르지 아니한 자
(제63조제1항) 보호위원회가 요구한 관계 물품·서류 등 자료를 제출하지 아니하거나 거짓으로 제출한 자
(제63조제2항) 자료 제출을 거부하거나 법을 위반한 처리자의 사무소나 사업장의 출입·검사를 거부·방해 또는 기피한 자
(제64조제1항) 보호위원회의 시정조치에 따른 시정명령에 따르지 아니한 자

2천만원 이하 과태료

(제26조제6항) 위탁자의 동의를 받지 아니하고 제3자에게 다시 위탁한 자
(제31조의2제1항) 국내대리인을 지정하지 아니한 자

1천만원 이하 과태료

(제11조의2제2항) 개인정보 보호수준 평가와 관련하여 정당한 사유없이 자료를 제출하지 아니하거나 거짓으로 제출한 자
(제21조제3항) 목적 달성한 개인정보를 보존해야할 경우 개인정보를 분리하여 저장·관리하지 아니한 자
(제22조제1~3항) 구분동의 위반, 중요한 내용 표기 등 방법 위반, 동의없이 처리하는 개인정보에 대한 항목 및 법적 근거에 대한 미고지 등을 위반한 자
(제26조제1항) 개인정보 처리업무 위탁시 포함되어야할 내용이 문서에 의하지 아니한 자
(제26조제2항) 개인정보 처리업무 위탁 내용과 수탁자를 정보주체에게 정하는 방법에 따라 공개하지 아니한 자
(제27조제1항, 제2항) 영업의 양도·합병 등으로 개인정보 이전시 정보주체에게 고지사항을 알리지 않은 자
(제28조의4제3항) 가명정보 처리시 목적, 제3자 제공시 받는 자 등 관련 내용 기록을 작성하여 보관하지 아니한 자
(제30조제1항 또는제2항) 개인정보 처리방침을 정하지 아니하거나 이를 공개하지 아니한 자
(제31조제1항) 개인정보 보호책임자를 지정하지 아니한 자 (부적합한 자 지정 포함)
(제35조제3항·제4항) (제36조제2항·제4항 또는 제37조제3항) 열람, 정정·삭제, 처리정지 관련해서 알려야 할 사항을 알리지 아니한 자
(제45조제1항) 분조위에서 분쟁당사자에게 자료를 요청한 경우 자료를 정당한 사유없이 제출하지 아니하거나 거짓으로 제출한 자
(제45조제2항) 분조위에서 분쟁당사자에게 출입·조사·열람을 요청한 경우 정당한 사유없이 거부·방해 또는 기피한 자

Chapter

II

개인정보 보호법 및 시행령



제1장 총칙

제1조(목적) 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.<개정 2014. 3. 24.>

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.<개정 2014. 3. 24., 2020. 2. 4., 2023. 3. 14.>

1. “개인정보”란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
 - 가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
 - 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
 - 다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 “가명정보”라 한다)
- 1의2. “가명처리”란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.
2. “처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
5. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
6. “공공기관”이란 다음 각 목의 기관을 말한다.
 - 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
 - 나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관

7. “고정형 영상정보처리기기”란 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.
- 7의2. “이동형 영상정보처리기기”란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(據置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.
8. “과학적 연구”란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다.

제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

- ② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
- ③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
- ④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
- ⑤ 개인정보처리자는 제30조에 따른 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.<개정 2023. 3. 14.>
- ⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
- ⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적 달성을 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.<개정 2020. 2. 4.>
- ⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.<개정 2023. 3. 14.>

1. 개인정보의 처리에 관한 정보를 제공받을 권리
2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
3. 개인정보의 처리 여부를 확인하고 개인정보에 대한 열람(사본의 발급을 포함한다. 이하 같다) 및 전송을 요구할 권리
4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

6. 완전히 자동화된 개인정보 처리에 따른 결정을 거부하거나 그에 대한 설명 등을 요구할 권리

- 제5조(국가 등의 책무)** ① 국가와 지방자치단체는 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 피해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구하여야 한다.
- ② 국가와 지방자치단체는 제4조에 따른 정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책을 마련하여야 한다.
- ③ 국가와 지방자치단체는 만 14세 미만 아동이 개인정보 처리가 미치는 영향과 정보주체의 권리 등을 명확하게 알 수 있도록 만 14세 미만 아동의 개인정보 보호에 필요한 시책을 마련하여야 한다.<신설 2023. 3. 14.>
- ④ 국가와 지방자치단체는 개인정보의 처리에 관한 불합리한 사회적 관행을 개선하기 위하여 개인정보처리자의 자율적인 개인정보 보호활동을 존중하고 촉진·지원하여야 한다.<개정 2023. 3. 14.>
- ⑤ 국가와 지방자치단체는 개인정보의 처리에 관한 법령 또는 조례를 적용할 때에는 정보주체의 권리가 보장될 수 있도록 개인정보 보호 원칙에 맞게 적용하여야 한다.<개정 2023. 3. 14.>

- 제6조(다른 법률과의 관계)** ① 개인정보의 처리 및 보호에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.<개정 2023. 3. 14.>
- ② 개인정보의 처리 및 보호에 관한 다른 법률을 제정하거나 개정하는 경우에는 이 법의 목적과 원칙에 맞도록 하여야 한다.<신설 2023. 3. 14.>

제2장 개인정보 보호정책의 수립 등

- 제7조(개인정보 보호위원회)** ① 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 개인정보 보호위원회(이하 “보호위원회”라 한다)를 둔다.<개정 2020. 2. 4.>
- ② 보호위원회는 「정부조직법」 제2조에 따른 중앙행정기관으로 본다. 다만, 다음 각 호의 사항에 대하여는 「정부조직법」 제18조를 적용하지 아니한다.<개정 2020. 2. 4.>
1. 제7조의8제3호 및 제4호의 사무
 2. 제7조의9제1항의 심의·의결 사항 중 제1호에 해당하는 사항
- ③ 삭제<2020. 2. 4.>
- ④ 삭제<2020. 2. 4.>
- ⑤ 삭제<2020. 2. 4.>
- ⑥ 삭제<2020. 2. 4.>
- ⑦ 삭제<2020. 2. 4.>
- ⑧ 삭제<2020. 2. 4.>
- ⑨ 삭제<2020. 2. 4.>

제7조의2(보호위원회의 구성 등) ① 보호위원회는 상임위원 2명(위원장 1명, 부위원장 1명)을 포함한 9명의 위원으로 구성한다.

② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.

1. 개인정보 보호 업무를 담당하는 3급 이상 공무원(고위공무원단에 속하는 공무원을 포함한다)의 직에 있거나 있었던 사람
2. 판사·검사·변호사의 직에 10년 이상 있거나 있었던 사람
3. 공공기관 또는 단체(개인정보처리자로 구성된 단체를 포함한다)에 3년 이상 임원으로 재직하였거나 이들 기관 또는 단체로부터 추천받은 사람으로서 개인정보 보호 업무를 3년 이상 담당하였던 사람
4. 개인정보 관련 분야에 전문지식이 있고 「고등교육법」 제2조제1호에 따른 학교에서 부교수 이상으로 5년 이상 재직하고 있거나 재직하였던 사람

③ 위원장과 부위원장은 정무직 공무원으로 임명한다.

④ 위원장, 부위원장, 제7조의13에 따른 사무처의 장은 「정부조직법」 제10조에도 불구하고 정부위원이 된다.

[본조신설 2020. 2. 4.]

제7조의3(위원장) ① 위원장은 보호위원회를 대표하고, 보호위원회의 회의를 주재하며, 소관 사무를 총괄한다.

② 위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 부위원장이 그 직무를 대행하고, 위원장·부위원장이 모두 부득이한 사유로 직무를 수행할 수 없을 때에는 위원회가 미리 정하는 위원이 위원장의 직무를 대행한다.

③ 위원장은 국회에 출석하여 보호위원회의 소관 사무에 관하여 의견을 진술할 수 있으며, 국회에서 요구하면 출석하여 보고하거나 답변하여야 한다.

④ 위원장은 국무회의에 출석하여 발언할 수 있으며, 그 소관 사무에 관하여 국무총리에게 의안 제출을 건의할 수 있다.

[본조신설 2020. 2. 4.]

제7조의4(위원의 임기) ① 위원의 임기는 3년으로 하되, 한 차례만 연임할 수 있다.

② 위원이 궐위된 때에는 지체 없이 새로운 위원을 임명 또는 위촉하여야 한다. 이 경우 후임으로 임명 또는 위촉된 위원의 임기는 새로이 개시된다.

[본조신설 2020. 2. 4.]

제7조의5(위원의 신분보장) ① 위원은 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 그 의사에 반하여 면직 또는 해촉되지 아니한다.

1. 장기간 심신장애로 인하여 직무를 수행할 수 없게 된 경우

2. 제7조의7의 결격사유에 해당하는 경우
 3. 이 법 또는 그 밖의 다른 법률에 따른 직무상의 의무를 위반한 경우
- ② 위원은 법률과 양심에 따라 독립적으로 직무를 수행한다.

[본조신설 2020. 2. 4.]

제7조의6(겸직금지 등) ① 위원은 재직 중 다음 각 호의 직(職)을 겸하거나 직무와 관련된 영리업무에 종사하여서는 아니 된다.

1. 국회의원 또는 지방의회의원
 2. 국가공무원 또는 지방공무원
 3. 그 밖에 대통령령으로 정하는 직
- ② 제1항에 따른 영리업무에 관한 사항은 대통령령으로 정한다.
- ③ 위원은 정치활동에 관여할 수 없다.

[본조신설 2020. 2. 4.]

제7조의7(결격사유) ① 다음 각 호의 어느 하나에 해당하는 사람은 위원이 될 수 없다.

1. 대한민국 국민이 아닌 사람
 2. 「국가공무원법」 제33조 각 호의 어느 하나에 해당하는 사람
 3. 「정당법」 제22조에 따른 당원
- ② 위원이 제1항 각 호의 어느 하나에 해당하게 된 때에는 그 직에서 당연 퇴직한다. 다만, 「국가공무원법」 제33조제2호는 파산선고를 받은 사람으로서 「채무자 회생 및 파산에 관한 법률」에 따라 신청기한 내에 면책신청을 하지 아니하였거나 면책불허가 결정 또는 면책 취소가 확정된 경우만 해당하고, 같은 법 제33조제5호는 「형법」 제129조부터 제132조까지, 「성폭력범죄의 처벌 등에 관한 특례법」 제2조, 「아동·청소년의 성보호에 관한 법률」 제2조제2호 및 직무와 관련하여 「형법」 제355조 또는 제356조에 규정된 죄를 범한 사람으로서 금고 이상의 형의 선고유예를 받은 경우만 해당한다.

[본조신설 2020. 2. 4.]

제7조의8(보호위원회의 소관 사무) 보호위원회는 다음 각 호의 소관 사무를 수행한다.<개정 2023. 3. 14.>

1. 개인정보의 보호와 관련된 법령의 개선에 관한 사항
2. 개인정보 보호와 관련된 정책·제도·계획 수립·집행에 관한 사항
3. 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항
4. 개인정보의 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁의 조정
5. 개인정보 보호를 위한 국제기구 및 외국의 개인정보 보호기구와의 교류·협력
6. 개인정보 보호에 관한 법령·정책·제도·실태 등의 조사·연구, 교육 및 홍보에 관한 사항
7. 개인정보 보호에 관한 기술개발의 지원·보급, 기술의 표준화 및 전문인력의 양성에 관한 사항

8. 이 법 및 다른 법령에 따라 보호위원회의 사무로 규정된 사항
[본조신설 2020. 2. 4.]

제7조의9(보호위원회의 심의·의결 사항 등) ① 보호위원회는 다음 각 호의 사항을 심의·의결한다.<개정 2023. 3. 14.>

1. 제8조의2에 따른 개인정보 침해요인 평가에 관한 사항
 2. 제9조에 따른 기본계획 및 제10조에 따른 시행계획에 관한 사항
 3. 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항
 4. 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항
 5. 개인정보 보호에 관한 법령의 해석·운용에 관한 사항
 6. 제18조제2항제5호에 따른 개인정보의 이용·제공에 관한 사항
 - 6의2. 제28조의9에 따른 개인정보의 국외 이전 중지 명령에 관한 사항
 7. 제33조제4항에 따른 영향평가 결과에 관한 사항
 8. 제64조의2에 따른 과징금 부과에 관한 사항
 9. 제61조에 따른 의견제시 및 개선권고에 관한 사항
 - 9의2. 제63조의2제2항에 따른 시정권고에 관한 사항
 10. 제64조에 따른 시정조치 등에 관한 사항
 11. 제65조에 따른 고발 및 징계권고에 관한 사항
 12. 제66조에 따른 처리 결과의 공표 및 공표명령에 관한 사항
 13. 제75조에 따른 과태료 부과에 관한 사항
 14. 소관 법령 및 보호위원회 규칙의 제정·개정 및 폐지에 관한 사항
 15. 개인정보 보호와 관련하여 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항
 16. 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의·의결하는 사항
- ② 보호위원회는 제1항 각 호의 사항을 심의·의결하기 위하여 필요한 경우 다음 각 호의 조치를 할 수 있다.

1. 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람이나 시민사회단체 및 관련 사업자로부터의 의견 청취
 2. 관계 기관 등에 대한 자료제출이나 사실조회 요구
- ③ 제2항제2호에 따른 요구를 받은 관계 기관 등은 특별한 사정이 없으면 이에 따라야 한다.
- ④ 보호위원회는 제1항제3호의 사항을 심의·의결한 경우에는 관계 기관에 그 개선을 권고할 수 있다.
- ⑤ 보호위원회는 제4항에 따른 권고 내용의 이행 여부를 점검할 수 있다.

[본조신설 2020. 2. 4.]

제7조의10(회의) ① 보호위원회의 회의는 위원장이 필요하다고 인정하거나 재적위원 4분의 1 이상의 요구가 있는 경우에 위원장이 소집한다.

- ② 위원장 또는 2명 이상의 위원은 보호위원회에 의안을 제의할 수 있다.

- ③ 보호위원회의 회의는 재적위원 과반수의 출석으로 개의하고, 출석위원 과반수의 찬성으로 의결한다.

[본조신설 2020. 2. 4.]

제7조의11(위원의 제척·기피·회피) ① 위원은 다음 각 호의 어느 하나에 해당하는 경우에는 심의·의결에서 제척된다.

1. 위원 또는 그 배우자나 배우자였던 자가 해당 사안의 당사자가 되거나 그 사건에 관하여 공동의 권리자 또는 의무자의 관계에 있는 경우
2. 위원이 해당 사안의 당사자와 친족이거나 친족이었던 경우
3. 위원이 해당 사안에 관하여 증언, 감정, 법률자문을 한 경우
4. 위원이 해당 사안에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우
5. 위원이나 위원이 속한 공공기관·법인 또는 단체 등이 조언 등 지원을 하고 있는 자와 이해관계가 있는 경우

- ② 위원에게 심의·의결의 공정성을 기대하기 어려운 사정이 있는 경우 당사자는 기피 신청을 할 수 있고, 보호위원회는 의결로 이를 결정한다.

- ③ 위원이 제1항 또는 제2항의 사유가 있는 경우에는 해당 사안에 대하여 회피할 수 있다.

[본조신설 2020. 2. 4.]

제7조의12(소위원회) ① 보호위원회는 효율적인 업무 수행을 위하여 개인정보 침해 정도가 경미하거나 유사·반복되는 사항 등을 심의·의결할 소위원회를 둘 수 있다.

- ② 소위원회는 3명의 위원으로 구성한다.

- ③ 소위원회가 제1항에 따라 심의·의결한 것은 보호위원회가 심의·의결한 것으로 본다.

- ④ 소위원회의 회의는 구성위원 전원의 출석과 출석위원 전원의 찬성으로 의결한다.

[본조신설 2020. 2. 4.]

제7조의13(사무처) 보호위원회의 사무를 처리하기 위하여 보호위원회에 사무처를 두며, 이 법에 규정된 것 외에 보호위원회의 조직에 관한 사항은 대통령령으로 정한다.

[본조신설 2020. 2. 4.]

제7조의14(운영 등) 이 법과 다른 법령에 규정된 것 외에 보호위원회의 운영 등에 필요한 사항은 보호위원회의 규칙으로 정한다.

[본조신설 2020. 2. 4.]

제8조 삭제<2020. 2. 4.>

제8조의2(개인정보 침해요인 평가) ① 중앙행정기관의 장은 소관 법령의 제정 또는 개정을 통하여 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우에는 보호위원회에 개인정보 침해요인 평가를 요청하여야 한다.

- ② 보호위원회가 제1항에 따른 요청을 받은 때에는 해당 법령의 개인정보 침해요인을 분석·검토하여 그 법령의 소관기관의 장에게 그 개선을 위하여 필요한 사항을 권고할 수 있다.

- ③ 제1항에 따른 개인정보 침해요인 평가의 절차와 방법에 관하여 필요한 사항은 대통령령으로 정한다.

[본조신설 2015. 7. 24.]

제9조(기본계획) ① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보 보호 기본계획(이하 “기본계획”이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다.<개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24.>

- ② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 개인정보 보호의 기본목표와 추진방향
2. 개인정보 보호와 관련된 제도 및 법령의 개선
3. 개인정보 침해 방지를 위한 대책
4. 개인정보 보호 자율규제의 활성화
5. 개인정보 보호 교육·홍보의 활성화
6. 개인정보 보호를 위한 전문인력의 양성
7. 그 밖에 개인정보 보호를 위하여 필요한 사항

- ③ 국회, 법원, 헌법재판소, 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호를 위한 기본계획을 수립·시행할 수 있다.

제10조(시행계획) ① 중앙행정기관의 장은 기본계획에 따라 매년 개인정보 보호를 위한 시행계획을 작성하여 보호위원회에 제출하고, 보호위원회의 심의·의결을 거쳐 시행하여야 한다.

- ② 시행계획의 수립·시행에 필요한 사항은 대통령령으로 정한다.

제11조(자료제출 요구 등) ① 보호위원회는 기본계획을 효율적으로 수립하기 위하여 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등에 개인정보처리자의 법규 준수 현황과 개인정보 관리 실태 등에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24.>

- ② 보호위원회는 개인정보 보호 정책 추진, 성과평가 등을 위하여 필요한 경우 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등을 대상으로 개인정보관리 수준 및 실태파악 등을 위한 조사를 실시할 수 있다.<신설 2015. 7. 24., 2017. 7. 26., 2020. 2. 4.>

- ③ 중앙행정기관의 장은 시행계획을 효율적으로 수립·추진하기 위하여 소관 분야의 개인정보처리자에게 제1항에 따른 자료제출 등을 요구할 수 있다.<개정 2015. 7. 24.>

- ④ 제1항부터 제3항까지에 따른 자료제출 등을 요구받은 자는 특별한 사정이 없으면 이에 따라야 한다.<개정 2015. 7. 24.>

- ⑤ 제1항부터 제3항까지에 따른 자료제출 등의 범위와 방법 등 필요한 사항은 대통령령으로 정한다.<개정 2015. 7. 24.>

- 제11조의2(개인정보 보호수준 평가)** ① 보호위원회는 공공기관 중 중앙행정기관 및 그 소속기관, 지방자치단체, 그 밖에 대통령령으로 정하는 기관을 대상으로 매년 개인정보 보호 정책·업무의 수행 및 이 법에 따른 의무의 준수 여부 등을 평가(이하 “개인정보 보호수준 평가”라 한다)하여야 한다.
- ② 보호위원회는 개인정보 보호수준 평가에 필요한 경우 해당 공공기관의 장에게 관련 자료를 제출하게 할 수 있다.
- ③ 보호위원회는 개인정보 보호수준 평가의 결과를 인터넷 홈페이지 등을 통하여 공개할 수 있다.
- ④ 보호위원회는 개인정보 보호수준 평가의 결과에 따라 우수기관 및 그 소속 직원에 대하여 포상할 수 있고, 개인정보 보호를 위하여 필요하다고 인정하면 해당 공공기관의 장에게 개선을 권고할 수 있다. 이 경우 권고를 받은 공공기관의 장은 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 보호위원회에 알려야 한다.
- ⑤ 그 밖에 개인정보 보호수준 평가의 기준·방법·절차 및 제2항에 따른 자료 제출의 범위 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2023. 3. 14.]

- 제12조(개인정보 보호지침)** ① 보호위원회는 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 표준 개인정보 보호지침(이하 “표준지침”이라 한다)을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>
- ② 중앙행정기관의 장은 표준지침에 따라 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.
- ③ 국회, 법원, 헌법재판소 및 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호지침을 정하여 시행할 수 있다.

- 제13조(자율규제의 촉진 및 지원)** 보호위원회는 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위하여 다음 각 호의 필요한 시책을 마련하여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>
1. 개인정보 보호에 관한 교육·홍보
 2. 개인정보 보호와 관련된 기관·단체의 육성 및 지원
 3. 개인정보 보호 인증마크의 도입·시행 지원
 4. 개인정보처리자의 자율적인 규약의 제정·시행 지원
 5. 그 밖에 개인정보처리자의 자율적 개인정보 보호활동을 지원하기 위하여 필요한 사항

- 제13조의2(개인정보 보호의 날)** ① 개인정보의 보호 및 처리의 중요성을 국민에게 알리기 위하여 매년 9월 30일을 개인정보 보호의 날로 지정한다.
- ② 국가와 지방자치단체는 개인정보 보호의 날이 포함된 주간에 개인정보 보호 문화 확산을 위한 각종 행사를 실시할 수 있다. [본조신설 2023. 3. 14.]

제14조(국제협력) ① 정부는 국제적 환경에서의 개인정보 보호 수준을 향상시키기 위하여 필요한 시책을 마련하여야 한다.

② 정부는 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하여야 한다.

제3장 개인정보의 처리

제1절 개인정보의 수집, 이용, 제공 등

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

<개정 2023. 3. 14.>

1. 정보주체의 동의를 받은 경우
 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
 3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
 4. 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우
 5. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
 6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.
 7. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우
- ② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
1. 개인정보의 수집·이용 목적
 2. 수집하려는 개인정보의 항목
 3. 개인정보의 보유 및 이용 기간
 4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
- ③ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다.<신설 2020. 2. 4.>

제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를

수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

- ② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.<신설 2013. 8. 6.>
- ③ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.<개정 2013. 8. 6.>

제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.<개정 2020. 2. 4., 2023. 3. 14.>

- 1. 정보주체의 동의를 받은 경우
- 2. 제15조제1항제2호, 제3호 및 제5호부터 제7호까지에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우
- ② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
 - 1. 개인정보를 제공받는 자
 - 2. 개인정보를 제공받는 자의 개인정보 이용 목적
 - 3. 제공하는 개인정보의 항목
 - 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
 - 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
- ③ 삭제<2023. 3. 14.>
- ④ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다.<신설 2020. 2. 4.>

제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제28조의8제1항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.<개정 2020. 2. 4., 2023. 3. 14.>

- ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지에 따른 경우는 공공기관의 경우로 한정한다.<개정 2020. 2. 4., 2023. 3. 14.>

1. 정보주체로부터 별도의 동의를 받은 경우
 2. 다른 법률에 특별한 규정이 있는 경우
 3. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
 4. 삭제<2020. 2. 4.>
 5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
 6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
 7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
 8. 법원의 재판업무 수행을 위하여 필요한 경우
 9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우
 10. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우
- ③ 개인정보처리자는 제2항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
1. 개인정보를 제공받는 자
 2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)
 3. 이용 또는 제공하는 개인정보의 항목
 4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
- ④ 공공기관은 제2항제2호부터 제6호까지, 제8호부터 제10호까지에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 보호위원회가 고시로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4., 2023. 3. 14.>
- ⑤ 개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

[제목개정 2013. 8. 6.]

제19조(개인정보를 제공받은 자의 이용·제공 제한) 개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를

제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 된다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우

제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 통지) ①

개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.

<개정 2023. 3. 14.>

1. 개인정보의 수집 출처
 2. 개인정보의 처리 목적
 3. 제37조에 따른 개인정보 처리의 정지를 요구하거나 동의를 철회할 권리가 있다는 사실
- ② 제1항에도 불구하고 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제17조제1항제1호에 따라 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 개인정보처리자가 수집한 정보에 연락처 등 정보주체에게 알릴 수 있는 개인정보가 포함되지 아니한 경우에는 그러하지 아니하다.<신설 2016. 3. 29.>
- ③ 제2항 본문에 따라 알리는 경우 정보주체에게 알리는 시기·방법 및 절차 등 필요한 사항은 대통령령으로 정한다.<신설 2016. 3. 29.>
- ④ 제1항과 제2항 본문은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다.<개정 2016. 3. 29., 2023. 3. 14.>
1. 통지를 요구하는 대상이 되는 개인정보가 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
 2. 통지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

[제목개정 2023. 3. 14.]

제20조의2(개인정보 이용·제공 내역의 통지) ① 대통령령으로 정하는 기준에 해당하는

개인정보처리자는 이 법에 따라 수집한 개인정보의 이용·제공 내역이나 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 주기적으로 정보주체에게 통지하여야 한다. 다만, 연락처 등 정보주체에게 통지할 수 있는 개인정보를 수집·보유하지 아니한 경우에는 통지하지 아니할 수 있다.

- ② 제1항에 따른 통지의 대상이 되는 정보주체의 범위, 통지 대상 정보, 통지 주기 및 방법 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2023. 3. 14.]

제21조(개인정보의 파기) ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과 등 그 개인정보가 불필요하게 되었을 때에는 지체

없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.<개정 2023. 3. 14.>

- ② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.
- ③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.
- ④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제22조의2제1항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다. 이 경우 다음 각 호의 경우에는 동의 사항을 구분하여 각각 동의를 받아야 한다.<개정 2017. 4. 18., 2023. 3. 14.>

- 1. 제15조제1항제1호에 따라 동의를 받는 경우
- 2. 제17조제1항제1호에 따라 동의를 받는 경우
- 3. 제18조제2항제1호에 따라 동의를 받는 경우
- 4. 제19조제1호에 따라 동의를 받는 경우
- 5. 제23조제1항제1호에 따라 동의를 받는 경우
- 6. 제24조제1항제1호에 따라 동의를 받는 경우
- 7. 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 경우
- 8. 그 밖에 정보주체를 보호하기 위하여 동의 사항을 구분하여 동의를 받아야 할 필요가 있는 경우로서 대통령령으로 정하는 경우

② 개인정보처리자는 제1항의 동의를 서면(「전자문서 및 전자거래 기본법」 제2조제1호에 따른 전자문서를 포함한다)으로 받을 때에는 개인정보의 수집·이용 목적, 수집·이용하려는 개인정보의 항목 등 대통령령으로 정하는 중요한 내용을 보호위원회가 고시로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다.<신설 2017. 4. 18., 2017. 7. 26., 2020. 2. 4.>

③ 개인정보처리자는 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 제30조제2항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 정보주체에게 알려야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.<개정 2016. 3. 29., 2017. 4. 18., 2023. 3. 14.>

④ 삭제<2023. 3. 14.>

⑤ 개인정보처리자는 정보주체가 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제1항제3호 및 제7호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.<개정 2017. 4. 18., 2023. 3. 14.>

⑥ 삭제<2023. 3. 14.>

⑦ 제1항부터 제5항까지에서 규정한 사항 외에 정보주체의 동의를 받는 세부적인 방법에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다.<개정 2017. 4. 18., 2023. 3. 14.>

제22조의2(아동의 개인정보 보호) ① 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 하며, 법정대리인이 동의하였는지를 확인하여야 한다.

② 제1항에도 불구하고 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보로서 대통령령으로 정하는 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.

③ 개인정보처리자는 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 할 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용하여야 한다.

④ 제1항부터 제3항까지에서 규정한 사항 외에 동의 및 동의 확인 방법 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2023. 3. 14.]

제2절 개인정보의 처리 제한

제23조(민감정보의 처리 제한) ① 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.<개정 2016. 3. 29.>

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.<신설 2016. 3. 29.>

③ 개인정보처리자는 재화 또는 서비스를 제공하는 과정에서 공개되는 정보에 정보주체의 민감정보가 포함됨으로써 사생활 침해의 위험성이 있다고 판단하는 때에는 재화 또는 서비스의 제공 전에 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 정보주체가 알아보기 쉽게 알려야 한다.<신설 2023. 3. 14.>

제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 “고유식별정보”라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른

개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우

2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

② 삭제<2013. 8. 6.>

③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.<개정 2015. 7. 24.>

④ 보호위원회는 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제3항에 따라 안전성 확보에 필요한 조치를 하였는지에 관하여 대통령령으로 정하는 바에 따라 정기적으로 조사하여야 한다.<신설 2016. 3. 29., 2017. 7. 26., 2020. 2. 4.>

⑤ 보호위원회는 대통령령으로 정하는 전문기관으로 하여금 제4항에 따른 조사를 수행하게 할 수 있다.<신설 2016. 3. 29., 2017. 7. 26., 2020. 2. 4.>

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.<개정 2014. 11. 19., 2016. 3. 29., 2017. 7. 26., 2020. 2. 4.>

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.<신설 2014. 3. 24., 2015. 7. 24.>

③ 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.<개정 2014. 3. 24.>

④ 보호위원회는 개인정보처리자가 제3항에 따른 방법을 제공할 수 있도록 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련·지원할 수 있다.<개정 2014. 3. 24., 2017. 7. 26., 2020. 2. 4.>

[본조신설 2013. 8. 6.]

제25조(고정형 영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치·운영하여서는 아니 된다.<개정 2023. 3. 14.>

1. 법령에서 구체적으로 허용하고 있는 경우
 2. 범죄의 예방 및 수사를 위하여 필요한 경우
 3. 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
 4. 교통단속을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
 5. 교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
 6. 촬영된 영상정보를 저장하지 아니하는 경우로서 대통령령으로 정하는 경우
- ② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 고정형 영상정보처리기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.<개정 2023. 3. 14.>
- ③ 제1항 각 호에 따라 고정형 영상정보처리기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 고정형 영상정보처리기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.<개정 2023. 3. 14.>
- ④ 제1항 각 호에 따라 고정형 영상정보처리기를 설치·운영하는 자(이하 “고정형영상정보처리기기운영자”라 한다)는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다. 다만, 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, 「통합방위법」 제2조제13호에 따른 국가중요시설, 그 밖에 대통령령으로 정하는 시설의 경우에는 그러하지 아니하다.<개정 2016. 3. 29., 2023. 3. 14.>
1. 설치 목적 및 장소
 2. 촬영 범위 및 시간
 3. 관리책임자의 연락처
 4. 그 밖에 대통령령으로 정하는 사항
- ⑤ 고정형영상정보처리기기운영자는 고정형 영상정보처리기기의 설치 목적과 다른 목적으로 고정형 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추서는 아니 되며, 녹음기능은 사용할 수 없다.<개정 2023. 3. 14.>
- ⑥ 고정형영상정보처리기기운영자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다.<개정 2015. 7. 24., 2023. 3. 14.>
- ⑦ 고정형영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 고정형 영상정보처리기기 운영·관리 방침을 마련하여야 한다. 다만, 제30조에 따른 개인정보 처리방침을 정할 때 고정형 영상정보처리기기 운영·관리에 관한 사항을 포함시킨 경우에는 고정형 영상정보처리기기 운영·관리 방침을 마련하지 아니할 수 있다.<개정 2023. 3. 14.>

- ⑧ 고정형영상정보처리기기운영자는 고정형 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 고정형 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.

<개정 2023. 3. 14.>

[제목개정 2023. 3. 14.]

제25조의2(이동형 영상정보처리기기의 운영 제한) ① 업무를 목적으로 이동형

영상정보처리기기를 운영하려는 자는 다음 각 호의 경우를 제외하고는 공개된 장소에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상(개인정보에 해당하는 경우로 한정한다. 이하 같다)을 촬영하여서는 아니 된다.

1. 제15조제1항 각 호의 어느 하나에 해당하는 경우
 2. 촬영 사실을 명확히 표시하여 정보주체가 촬영 사실을 알 수 있도록 하였음에도 불구하고 촬영 거부 의사를 밝히지 아니한 경우. 이 경우 정보주체의 권리를 부당하게 침해할 우려가 없고 합리적인 범위를 초과하지 아니하는 경우로 한정한다.
 3. 그 밖에 제1호 및 제2호에 준하는 경우로서 대통령령으로 정하는 경우
- ② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실, 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있는 곳에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하여서는 아니 된다. 다만, 인명의 구조·구급 등을 위하여 필요한 경우로서 대통령령으로 정하는 경우에는 그러하지 아니하다.
- ③ 제1항 각 호에 해당하여 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우에는 불빛, 소리, 안내판 등 대통령령으로 정하는 바에 따라 촬영 사실을 표시하고 알려야 한다.
- ④ 제1항부터 제3항까지에서 규정한 사항 외에 이동형 영상정보처리기기의 운영에 관하여는 제25조제6항부터 제8항까지의 규정을 준용한다.

[본조신설 2023. 3. 14.]

제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게

개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다.<개정 2023. 3. 14.>

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
 2. 개인정보의 기술적·관리적 보호조치에 관한 사항
 3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항
- ② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(개인정보 처리 업무를 위탁받아 처리하는 자로부터 위탁받은 업무를 다시 위탁받은 제3자를 포함하며, 이하 “수탁자”라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.<개정 2023. 3. 14.>

- ③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.
- ④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

<개정 2015. 7. 24.>

- ⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.
- ⑥ 수탁자는 위탁받은 개인정보의 처리 업무를 제3자에게 다시 위탁하려는 경우에는 위탁자의 동의를 받아야 한다.<신설 2023. 3. 14.>
- ⑦ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.

<개정 2023. 3. 14.>

- ⑧ 수탁자에 관하여는 제15조부터 제18조까지, 제21조, 제22조, 제22조의2, 제23조, 제24조, 제24조의2, 제25조, 제25조의2, 제27조, 제28조, 제28조의2부터 제28조의5까지, 제28조의7부터 제28조의11까지, 제29조, 제30조, 제30조의2, 제31조, 제33조, 제34조, 제34조의2, 제35조, 제35조의2, 제36조, 제37조, 제37조의2, 제38조, 제59조, 제63조, 제63조의2 및 제64조의2를 준용한다. 이 경우 “개인정보처리자”는 “수탁자”로 본다.<개정 2023. 3. 14.>

제27조(영업양도 등에 따른 개인정보의 이전 제한) ① 개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음 각 호의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다.

1. 개인정보를 이전하려는 사실
 2. 개인정보를 이전받는 자(이하 “영업양수자등”이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처
 3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차
- ② 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 대통령령으로 정하는 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.
- ③ 영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다. 이 경우 영업양수자등은 개인정보처리자로 본다.

제28조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자(이하 “개인정보취급자”라

한다)의 범위를 최소한으로 제한하고, 개인정보취급자에 대하여 적절한 관리·감독을 하여야 한다.<개정 2023. 3. 14.>

- ② 개인정보처리자는 개인정보의 적절한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

제3절 가명정보의 처리에 관한 특례

제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

- ② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.

[본조신설 2020. 2. 4.]

제28조의3(가명정보의 결합 제한) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

- ② 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명정보 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다.
③ 제1항에 따른 결합 절차와 방법, 전문기관의 지정과 지정 취소 기준·절차, 관리·감독, 제2항에 따른 반출 및 승인 기준·절차 등 필요한 사항은 대통령령으로 정한다.

[본조신설 2020. 2. 4.]

제28조의4(가명정보에 대한 안전조치의무 등) ① 개인정보처리자는 제28조의2 또는 제28조의3에 따라 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.<개정 2023. 3. 14.>

- ② 개인정보처리자는 제28조의2 또는 제28조의3에 따라 가명정보를 처리하는 경우 처리목적 등을 고려하여 가명정보의 처리 기간을 별도로 정할 수 있다.<신설 2023. 3. 14.>
③ 개인정보처리자는 제28조의2 또는 제28조의3에 따라 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자, 가명정보의 처리 기간(제2항에 따라 처리 기간을 별도로 정한 경우에 한한다) 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 하며, 가명정보를 파기한 경우에는 파기한 날부터 3년 이상 보관하여야 한다.<개정 2023. 3. 14.>

[본조신설 2020. 2. 4.]

제28조의5(가명정보 처리 시 금지의무 등) ① 제28조의2 또는 제28조의3에 따라 가명정보를 처리하는 자는 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다.<개정 2023. 3. 14.>

- ② 개인정보처리자는 제28조의2 또는 제28조의3에 따라 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.<개정 2023. 3. 14.>

[본조신설 2020. 2. 4.]

제28조의6 삭제<2023. 3. 14.>

제28조의7(적용범위) 제28조의2 또는 제28조의3에 따라 처리된 가명정보는 제20조, 제20조의2, 제27조, 제34조제1항, 제35조, 제35조의2, 제36조 및 제37조를 적용하지 아니한다.<개정 2023. 3. 14.>

[본조신설 2020. 2. 4.]

제4절 개인정보의 국외 이전

제28조의8(개인정보의 국외 이전) ① 개인정보처리자는 개인정보를 국외로 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 절에서 “이전”이라 한다)하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 국외로 이전할 수 있다.

1. 정보주체로부터 국외 이전에 관한 별도의 동의를 받은 경우
2. 법률, 대한민국을 당사자로 하는 조약 또는 그 밖의 국제협정에 개인정보의 국외 이전에 관한 특별한 규정이 있는 경우
3. 정보주체와의 계약의 체결 및 이행을 위하여 개인정보의 처리위탁·보관이 필요한 경우로서 다음 각 목의 어느 하나에 해당하는 경우
 - 가. 제2항 각 호의 사항을 제30조에 따른 개인정보 처리방침에 공개한 경우
 - 나. 전자우편 등 대통령령으로 정하는 방법에 따라 제2항 각 호의 사항을 정보주체에게 알린 경우
4. 개인정보를 이전받는 자가 제32조의2에 따른 개인정보 보호 인증 등 보호위원회가 정하여 고시하는 인증을 받은 경우로서 다음 각 목의 조치를 모두 한 경우
 - 가. 개인정보 보호에 필요한 안전조치 및 정보주체 권리보장에 필요한 조치
 - 나. 인증받은 사항을 개인정보가 이전되는 국가에서 이행하기 위하여 필요한 조치
5. 개인정보가 이전되는 국가 또는 국제기구의 개인정보 보호체계, 정보주체 권리보장 범위, 피해구제 절차 등이 이 법에 따른 개인정보 보호 수준과 실질적으로 동등한 수준을 갖추었다고 보호위원회가 인정하는 경우

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 미리 다음 각 호의 사항을 정보주체에게 알려야 한다.

1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 시기 및 방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭과 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간
5. 개인정보의 이전을 거부하는 방법, 절차 및 거부의 효과

- ③ 개인정보처리자는 제2항 각 호의 어느 하나에 해당하는 사항을 변경하는 경우에는 정보주체에게 알리고 동의를 받아야 한다.
- ④ 개인정보처리자는 제1항 각 호 외의 부분 단서에 따라 개인정보를 국외로 이전하는 경우 국외 이전과 관련한 이 법의 다른 규정, 제17조부터 제19조까지의 규정 및 제5장의 규정을 준수하여야 하고, 대통령령으로 정하는 보호조치를 하여야 한다.
- ⑤ 개인정보처리자는 이 법을 위반하는 사항을 내용으로 하는 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.
- ⑥ 제1항부터 제5항까지에서 규정한 사항 외에 개인정보 국외 이전의 기준 및 절차 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2023. 3. 14.]

제28조의9(개인정보의 국외 이전 중지 명령) ① 보호위원회는 개인정보의 국외 이전이 계속되고 있거나 추가적인 국외 이전이 예상되는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보처리자에게 개인정보의 국외 이전을 중지할 것을 명할 수 있다.

- 1. 제28조의8제1항, 제4항 또는 제5항을 위반한 경우
- 2. 개인정보를 이전받는 자나 개인정보가 이전되는 국가 또는 국제기구가 이 법에 따른 개인정보 보호 수준에 비하여 개인정보를 적정하게 보호하지 아니하여 정보주체에게 피해가 발생하거나 발생할 우려가 현저한 경우
- ② 개인정보처리자는 제1항에 따른 국외 이전 중지 명령을 받은 경우에는 명령을 받은 날부터 7일 이내에 보호위원회에 이의를 제기할 수 있다.
- ③ 제1항에 따른 개인정보 국외 이전 중지 명령의 기준, 제2항에 따른 불복 절차 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2023. 3. 14.]

제28조의10(상호주의) 제28조의8에도 불구하고 개인정보의 국외 이전을 제한하는 국가의 개인정보처리자에 대해서는 해당 국가의 수준에 상응하는 제한을 할 수 있다. 다만, 조약 또는 그 밖의 국제협정의 이행에 필요한 경우에는 그러하지 아니하다.

[본조신설 2023. 3. 14.]

제28조의11(준용규정) 제28조의8제1항 각 호 외의 부분 단서에 따라 개인정보를 이전받은 자가 해당 개인정보를 제3국으로 이전하는 경우에 관하여는 제28조의8 및 제28조의9를 준용한다. 이 경우 “개인정보처리자”는 “개인정보를 이전받은 자”로, “개인정보를 이전받는 자”는 “제3국에서 개인정보를 이전받는 자”로 본다.

[본조신설 2023. 3. 14.]

제4장 개인정보의 안전한 관리

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에

따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.<개정 2015. 7. 24.>

제30조(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 “개인정보 처리방침”이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다.<개정 2016. 3. 29., 2020. 2. 4., 2023. 3. 14.>

1. 개인정보의 처리 목적
 2. 개인정보의 처리 및 보유 기간
 3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
 - 3의2. 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
 - 3의3. 제23조제3항에 따른 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정한다)
 4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
 - 4의2. 제28조의2 및 제28조의3에 따른 가명정보의 처리 등에 관한 사항(해당되는 경우에만 정한다)
 5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
 6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
 7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
 8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항
- ② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.
- ③ 개인정보 처리방침의 내용과 개인정보처리자와 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용한다.
- ④ 보호위원회는 개인정보 처리방침의 작성지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

제30조의2(개인정보 처리방침의 평가 및 개선권고) ① 보호위원회는 개인정보 처리방침에 관하여 다음 각 호의 사항을 평가하고, 평가 결과 개선이 필요하다고 인정하는 경우에는 개인정보처리자에게 제61조제2항에 따라 개선을 권고할 수 있다.

1. 이 법에 따라 개인정보 처리방침에 포함하여야 할 사항을 적정하게 정하고 있는지 여부
2. 개인정보 처리방침을 알기 쉽게 작성하였는지 여부
3. 개인정보 처리방침을 정보주체가 쉽게 확인할 수 있는 방법으로 공개하고 있는지 여부

② 개인정보 처리방침의 평가 대상, 기준 및 절차 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2023. 3. 14.]

제31조(개인정보 보호책임자의 지정 등) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다. 다만, 종업원 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 개인정보처리자의 경우에는 지정하지 아니할 수 있다.<개정 2023. 3. 14.>

② 제1항 단서에 따라 개인정보 보호책임자를 지정하지 아니하는 경우에는 개인정보처리자의 사업주 또는 대표자가 개인정보 보호책임자가 된다.<신설 2023. 3. 14.>

③ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.<개정 2023. 3. 14.>

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

④ 개인정보 보호책임자는 제3항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.<개정 2023. 3. 14.>

⑤ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.<개정 2023. 3. 14.>

⑥ 개인정보처리자는 개인정보 보호책임자가 제3항 각 호의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 되며, 개인정보 보호책임자가 업무를 독립적으로 수행할 수 있도록 보장하여야 한다.<개정 2023. 3. 14.>

⑦ 개인정보처리자는 개인정보의 안전한 처리 및 보호, 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위하여 제1항에 따른 개인정보 보호책임자를 구성원으로 하는 개인정보 보호책임자 협의회를 구성·운영할 수 있다.<신설 2023. 3. 14.>

⑧ 보호위원회는 제7항에 따른 개인정보 보호책임자 협의회에 필요한 지원을 할 수 있다.<신설 2023. 3. 14.>

⑨ 제1항에 따른 개인정보 보호책임자의 자격요건, 제3항에 따른 업무 및 제6항에 따른 독립성 보장 등에 필요한 사항은 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정한다.<개정 2023. 3. 14.>

[제목개정 2023. 3. 14.]

제31조의2(국내대리인의 지정) ① 국내에 주소 또는 영업소가 없는 개인정보처리자로서 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 자는 다음 각 호의 사항을 대리하는 자(이하 “국내대리인”이라 한다)를 지정하여야 한다. 이 경우

국내대리인의 지정은 문서로 하여야 한다.<개정 2023. 3. 14.>

1. 제31조제3항에 따른 개인정보 보호책임자의 업무
2. 제34조제1항 및 제3항에 따른 개인정보 유출 등의 통지 및 신고
3. 제63조제1항에 따른 물품·서류 등 자료의 제출

② 국내대리인은 국내에 주소 또는 영업소가 있어야 한다.<개정 2023. 3. 14.>

③ 개인정보처리자는 제1항에 따라 국내대리인을 지정하는 경우에는 다음 각 호의 사항을 개인정보 처리방침에 포함하여야 한다.<개정 2023. 3. 14.>

1. 국내대리인의 성명(법인의 경우에는 그 명칭 및 대표자의 성명을 말한다)
2. 국내대리인의 주소(법인의 경우에는 영업소의 소재지를 말한다), 전화번호 및 전자우편 주소

④ 국내대리인이 제1항 각 호와 관련하여 이 법을 위반한 경우에는 개인정보처리자가 그 행위를 한 것으로 본다.<개정 2023. 3. 14.>

[본조신설 2020. 2. 4.]

[제39조의11에서 이동 <2023. 3. 14.>]

제32조(개인정보파일의 등록 및 공개) ① 공공기관의 장이 개인정보파일을 운용하는 경우에는 다음 각 호의 사항을 보호위원회에 등록하여야 한다. 등록된 사항이 변경된 경우에도 또한 같다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

1. 개인정보파일의 명칭
2. 개인정보파일의 운영 근거 및 목적
3. 개인정보파일에 기록되는 개인정보의 항목
4. 개인정보의 처리방법
5. 개인정보의 보유기간
6. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
7. 그 밖에 대통령령으로 정하는 사항

② 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 제1항을 적용하지 아니한다.<개정 2023. 3. 14.>

1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일
3. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
4. 일회적으로 운영되는 파일 등 지속적으로 관리할 필요성이 낮다고 인정되어 대통령령으로 정하는 개인정보파일
5. 다른 법령에 따라 비밀로 분류된 개인정보파일

③ 보호위원회는 필요하면 제1항에 따른 개인정보파일의 등록여부와 그 내용을 검토하여 해당 공공기관의 장에게 개선을 권고할 수 있다.<개정 2013. 3. 23.,

2014. 11. 19., 2017. 7. 26., 2020. 2. 4., 2023. 3. 14.>

- ④ 보호위원회는 정보주체의 권리 보장 등을 위하여 필요한 경우 제1항에 따른 개인정보파일의 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4., 2023. 3. 14.>
- ⑤ 제1항에 따른 등록과 제4항에 따른 공개의 방법, 범위 및 절차에 관하여 필요한 사항은 대통령령으로 정한다.
- ⑥ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 개인정보파일 등록 및 공개에 관하여는 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정한다.

제32조의2(개인정보 보호 인증) ① 보호위원회는 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관하여 인증할 수 있다.<개정 2017. 7. 26., 2020. 2. 4.>

- ② 제1항에 따른 인증의 유효기간은 3년으로 한다.
- ③ 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령으로 정하는 바에 따라 제1항에 따른 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 취소하여야 한다.<개정 2017. 7. 26., 2020. 2. 4.>
 - 1. 거짓이나 그 밖의 부정한 방법으로 개인정보 보호 인증을 받은 경우
 - 2. 제4항에 따른 사후관리를 거부 또는 방해한 경우
 - 3. 제8항에 따른 인증기준에 미달하게 된 경우
 - 4. 개인정보 보호 관련 법령을 위반하고 그 위반사유가 중대한 경우
- ④ 보호위원회는 개인정보 보호 인증의 실효성 유지를 위하여 연 1회 이상 사후관리를 실시하여야 한다.<개정 2017. 7. 26., 2020. 2. 4.>
- ⑤ 보호위원회는 대통령령으로 정하는 전문기관으로 하여금 제1항에 따른 인증, 제3항에 따른 인증 취소, 제4항에 따른 사후관리 및 제7항에 따른 인증 심사원 관리 업무를 수행하게 할 수 있다.<개정 2017. 7. 26., 2020. 2. 4.>
- ⑥ 제1항에 따른 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.
- ⑦ 제1항에 따른 인증을 위하여 필요한 심사를 수행할 심사원의 자격 및 자격 취소 요건 등에 관하여는 전문성과 경력 및 그 밖에 필요한 사항을 고려하여 대통령령으로 정한다.
- ⑧ 그 밖에 개인정보 관리체계, 정보주체 권리보장, 안전성 확보조치가 이 법에 부합하는지 여부 등 제1항에 따른 인증의 기준·방법·절차 등 필요한 사항은 대통령령으로 정한다.

[본조신설 2015. 7. 24.]

제33조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그

위험요인의 분석과 개선 사항 도출을 위한 평가(이하 “영향평가”라 한다)를 하고 그 결과를 보호위원회에 제출하여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4., 2023. 3. 14.>

- ② 보호위원회는 대통령령으로 정하는 인력·설비 및 그 밖에 필요한 요건을 갖춘 자를 영향평가를 수행하는 기관(이하 “평가기관”이라 한다)으로 지정할 수 있으며, 공공기관의 장은 영향평가를 평가기관에 의뢰하여야 한다.<신설 2023. 3. 14.>
- ③ 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.<개정 2023. 3. 14.>
 - 1. 처리하는 개인정보의 수
 - 2. 개인정보의 제3자 제공 여부
 - 3. 정보주체의 권리를 해할 가능성 및 그 위험 정도
 - 4. 그 밖에 대통령령으로 정한 사항
- ④ 보호위원회는 제1항에 따라 제출받은 영향평가 결과에 대하여 의견을 제시할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4., 2023. 3. 14.>
- ⑤ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.<개정 2023. 3. 14.>
- ⑥ 보호위원회는 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4., 2023. 3. 14.>
- ⑦ 보호위원회는 제2항에 따라 지정된 평가기관이 다음 각 호의 어느 하나에 해당하는 경우에는 평가기관의 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 경우에는 평가기관의 지정을 취소하여야 한다.<신설 2023. 3. 14.>
 - 1. 거짓이나 그 밖의 부정한 방법으로 지정을 받은 경우
 - 2. 지정된 평가기관 스스로 지정취소를 원하거나 폐업한 경우
 - 3. 제2항에 따른 지정요건을 충족하지 못하게 된 경우
 - 4. 고의 또는 중대한 과실로 영향평가업무를 부실하게 수행하여 그 업무를 적정하게 수행할 수 없다고 인정되는 경우
 - 5. 그 밖에 대통령령으로 정하는 사유에 해당하는 경우
- ⑧ 보호위원회는 제7항에 따라 지정을 취소하는 경우에는 「행정절차법」에 따른 청문을 실시하여야 한다.<신설 2023. 3. 14.>
- ⑨ 제1항에 따른 영향평가의 기준·방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.<개정 2023. 3. 14.>
- ⑩ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.<개정 2023. 3. 14.>
- ⑪ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.<개정 2023. 3. 14.>

제34조(개인정보 유출 등의 통지·신고) ① 개인정보처리자는 개인정보가 분실·도난·유출(이하 이 조에서 “유출등”이라 한다)되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.<개정 2023. 3. 14.>

1. 유출등이 된 개인정보의 항목
 2. 유출등이 된 시점과 그 경위
 3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
 4. 개인정보처리자의 대응조치 및 피해 구제절차
 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- ② 개인정보처리자는 개인정보가 유출등이 된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.<개정 2023. 3. 14.>
- ③ 개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각 호의 사항을 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4., 2023. 3. 14.>
- ④ 제1항에 따른 유출등의 통지 및 제3항에 따른 유출등의 신고의 시기, 방법, 절차 등에 필요한 사항은 대통령령으로 정한다.<개정 2023. 3. 14.>

[제목개정 2023. 3. 14.]

제34조의2(노출된 개인정보의 삭제·차단) ① 개인정보처리자는 고유식별정보, 계좌정보, 신용카드정보 등 개인정보가 정보통신망을 통하여 공중(公衆)에 노출되지 아니하도록 하여야 한다.<개정 2023. 3. 14.>

- ② 개인정보처리자는 공중에 노출된 개인정보에 대하여 보호위원회 또는 대통령령으로 지정한 전문기관의 요청이 있는 경우에는 해당 정보를 삭제하거나 차단하는 등 필요한 조치를 하여야 한다.<개정 2023. 3. 14.>

[본조신설 2020. 2. 4.]

[제39조의10에서 이동, 종전 제34조의2는 삭제 <2023. 3. 14.>]

제5장 정보주체의 권리 보장

제35조(개인정보의 열람) ① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

- ② 제1항에도 불구하고 정보주체가 자신의 개인정보에 대한 열람을 공공기관에 요구하고자 할 때에는 공공기관에 직접 열람을 요구하거나 대통령령으로 정하는

바에 따라 보호위원회를 통하여 열람을 요구할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

- ③ 개인정보처리자는 제1항 및 제2항에 따른 열람을 요구받았을 때에는 대통령령으로 정하는 기간 내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 이 경우 해당 기간 내에 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 지체 없이 열람하게 하여야 한다.
- ④ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.
1. 법률에 따라 열람이 금지되거나 제한되는 경우
 2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
 3. 공공기관이 다음 각 목의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우
- 가. 조세의 부과·징수 또는 환급에 관한 업무
- 나. 「초·중등교육법」 및 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무
- 다. 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무
- 라. 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
- 마. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무
- ⑤ 제1항부터 제4항까지의 규정에 따른 열람 요구, 열람 제한, 통지 등의 방법 및 절차에 관하여 필요한 사항은 대통령령으로 정한다.

제35조의2(개인정보의 전송 요구)

- ① 정보주체는 개인정보 처리 능력 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자에 대하여 다음 각 호의 요건을 모두 충족하는 개인정보를 자신에게로 전송할 것을 요구할 수 있다.
1. 정보주체가 전송을 요구하는 개인정보가 정보주체 본인에 관한 개인정보로서 다음 각 목의 어느 하나에 해당하는 정보일 것
- 가. 제15조제1항제1호, 제23조제1항제1호 또는 제24조제1항제1호에 따른 동의를 받아 처리되는 개인정보
- 나. 제15조제1항제4호에 따라 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 처리되는 개인정보
- 다. 제15조제1항제2호·제3호, 제23조제1항제2호 또는 제24조제1항제2호에 따라 처리되는 개인정보 중 정보주체의 이익이나 공익적 목적을 위하여 관계 중앙행정기관의 장의 요청에 따라 보호위원회가 심의·의결하여 전송 요구의 대상으로 지정한 개인정보

2. 전송을 요구하는 개인정보가 개인정보처리자가 수집한 개인정보를 기초로 분석·가공하여 별도로 생성한 정보가 아닐 것
3. 전송을 요구하는 개인정보가 컴퓨터 등 정보처리장치로 처리되는 개인정보일 것
- ② 정보주체는 매출액, 개인정보의 보유 규모, 개인정보 처리 능력, 산업별 특성 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자에 대하여 제1항에 따른 전송 요구 대상인 개인정보를 기술적으로 허용되는 합리적인 범위에서 다음 각 호의 자에게 전송할 것을 요구할 수 있다.
 1. 제35조의3제1항에 따른 개인정보관리 전문기관
 2. 제29조에 따른 안전조치의무를 이행하고 대통령령으로 정하는 시설 및 기술 기준을 충족하는 자
- ③ 개인정보처리자는 제1항 및 제2항에 따른 전송 요구를 받은 경우에는 시간, 비용, 기술적으로 허용되는 합리적인 범위에서 해당 정보를 컴퓨터 등 정보처리장치로 처리 가능한 형태로 전송하여야 한다.
- ④ 제1항 및 제2항에 따른 전송 요구를 받은 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 법률의 관련 규정에도 불구하고 정보주체에 관한 개인정보를 전송하여야 한다.
 1. 「국세기본법」 제81조의13
 2. 「지방세기본법」 제86조
 3. 그 밖에 제1호 및 제2호와 유사한 규정으로서 대통령령으로 정하는 법률의 규정
- ⑤ 정보주체는 제1항 및 제2항에 따른 전송 요구를 철회할 수 있다.
- ⑥ 개인정보처리자는 정보주체의 본인 여부가 확인되지 아니하는 경우 등 대통령령으로 정하는 경우에는 제1항 및 제2항에 따른 전송 요구를 거절하거나 전송을 중단할 수 있다.
- ⑦ 정보주체는 제1항 및 제2항에 따른 전송 요구로 인하여 타인의 권리나 정당한 이익을 침해하여서는 아니 된다.
- ⑧ 제1항부터 제7항까지에서 규정한 사항 외에 전송 요구의 대상이 되는 정보의 범위, 전송 요구의 방법, 전송의 기한 및 방법, 전송 요구 철회의 방법, 전송 요구의 거절 및 전송 중단의 방법 등 필요한 사항은 대통령령으로 정한다.

[본조신설 2023. 3. 14.]

[시행일 미지정] 제35조의2

제35조의3(개인정보관리 전문기관) ① 다음 각 호의 업무를 수행하려는 자는

보호위원회 또는 관계 중앙행정기관의 장으로부터 개인정보관리 전문기관의 지정을 받아야 한다.

1. 제35조의2에 따른 개인정보의 전송 요구권 행사 지원
2. 정보주체의 권리행사를 지원하기 위한 개인정보 전송시스템의 구축 및 표준화
3. 정보주체의 권리행사를 지원하기 위한 개인정보의 관리·분석
4. 그 밖에 정보주체의 권리행사를 효과적으로 지원하기 위하여 대통령령으로 정하는 업무

- ② 제1항에 따른 개인정보관리 전문기관의 지정요건은 다음 각 호와 같다.
1. 개인정보를 전송·관리·분석할 수 있는 기술수준 및 전문성을 갖추었을 것
 2. 개인정보를 안전하게 관리할 수 있는 안전성 확보조치 수준을 갖추었을 것
 3. 개인정보관리 전문기관의 안정적인 운영에 필요한 재정능력을 갖추었을 것
- ③ 개인정보관리 전문기관은 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.
1. 정보주체에게 개인정보의 전송 요구를 강요하거나 부당하게 유도하는 행위
 2. 그 밖에 개인정보를 침해하거나 정보주체의 권리를 제한할 우려가 있는 행위로서 대통령령으로 정하는 행위
- ④ 보호위원회 및 관계 중앙행정기관의 장은 개인정보관리 전문기관이 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보관리 전문기관의 지정을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 지정을 취소하여야 한다.
1. 거짓이나 부정한 방법으로 지정을 받은 경우
 2. 제2항에 따른 지정요건을 갖추지 못하게 된 경우
- ⑤ 보호위원회 및 관계 중앙행정기관의 장은 제4항에 따라 지정을 취소하는 경우에는 「행정절차법」에 따른 청문을 실시하여야 한다.
- ⑥ 보호위원회 및 관계 중앙행정기관의 장은 개인정보관리 전문기관에 대하여 업무 수행에 필요한 지원을 할 수 있다.
- ⑦ 개인정보관리 전문기관은 정보주체의 요구에 따라 제1항 각 호의 업무를 수행하는 경우 정보주체로부터 그 업무 수행에 필요한 비용을 받을 수 있다.
- ⑧ 제1항에 따른 개인정보관리 전문기관의 지정 절차, 제2항에 따른 지정요건의 세부기준, 제4항에 따른 지정취소의 절차 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2023. 3. 14.]

제35조의4(개인정보 전송 관리 및 지원) ① 보호위원회는 제35조의2제1항 및 제2항에 따른 개인정보처리자 및 제35조의3제1항에 따른 개인정보관리 전문기관 현황, 활용내역 및 관리실태 등을 체계적으로 관리·감독하여야 한다.

- ② 보호위원회는 개인정보가 안전하고 효율적으로 전송될 수 있도록 다음 각 호의 사항을 포함한 개인정보 전송 지원 플랫폼을 구축·운영할 수 있다.
1. 개인정보관리 전문기관 현황 및 전송 가능한 개인정보 항목 목록
 2. 정보주체의 개인정보 전송 요구·철회 내역
 3. 개인정보의 전송 이력 관리 등 지원 기능
 4. 그 밖에 개인정보 전송을 위하여 필요한 사항
- ③ 보호위원회는 제2항에 따른 개인정보 전송지원 플랫폼의 효율적 운영을 위하여 개인정보관리 전문기관에서 구축·운영하고 있는 전송 시스템을 상호 연계하거나 통합할 수 있다. 이 경우 관계 중앙행정기관의 장 및 해당 개인정보관리 전문기관과 사전에 협의하여야 한다.
- ④ 제1항부터 제3항까지의 규정에 따른 관리·감독과 개인정보 전송지원 플랫폼의 구축 및 운영에 필요한 사항은 대통령령으로 정한다.

제36조(개인정보의 정정·삭제) ① 제35조에 따라 자신의 개인정보를 열람한

정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다.
다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.

- ② 개인정보처리자는 제1항에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.
- ③ 개인정보처리자가 제2항에 따라 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.
- ④ 개인정보처리자는 정보주체의 요구가 제1항 단서에 해당될 때에는 지체 없이 그 내용을 정보주체에게 알려야 한다.
- ⑤ 개인정보처리자는 제2항에 따른 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.
- ⑥ 제1항·제2항 및 제4항에 따른 정정 또는 삭제 요구, 통지 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

제37조(개인정보의 처리정지 등) ① 정보주체는 개인정보처리자에 대하여 자신의

개인정보 처리의 정지를 요구하거나 개인정보 처리에 대한 동의를 철회할 수 있다.
이 경우 공공기관에 대해서는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구하거나 개인정보 처리에 대한 동의를 철회할 수 있다.<개정 2023. 3. 14.>

- ② 개인정보처리자는 제1항에 따른 처리정지 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.<개정 2023. 3. 14.>
 - 1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
 - 2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
 - 3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
 - 4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우
- ③ 개인정보처리자는 정보주체가 제1항에 따라 동의를 철회한 때에는 지체 없이 수집된 개인정보를 복구·재생할 수 없도록 파기하는 등 필요한 조치를 하여야

한다. 다만, 제2항 각 호의 어느 하나에 해당하는 경우에는 동의 철회에 따른 조치를 하지 아니할 수 있다.<신설 2023. 3. 14.>

- ④ 개인정보처리자는 제2항 단서에 따라 처리정지 요구를 거절하거나 제3항 단서에 따라 동의 철회에 따른 조치를 하지 아니하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다.<개정 2023. 3. 14.>
- ⑤ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.<개정 2023. 3. 14.>
- ⑥ 제1항부터 제5항까지의 규정에 따른 처리정지의 요구, 동의 철회, 처리정지의 거절, 통지 등의 방법 및 절차에 필요한 사항은 대통령령으로 정한다.<개정 2023. 3. 14.>

제37조의2(자동화된 결정에 대한 정보주체의 권리 등) ① 정보주체는 완전히 자동화된 시스템(인공지능 기술을 적용한 시스템을 포함한다)으로 개인정보를 처리하여 이루어지는 결정(「행정기본법」 제20조에 따른 행정청의 자동적 처분은 제외하며, 이하 이 조에서 “자동화된 결정”이라 한다)이 자신의 권리 또는 의무에 중대한 영향을 미치는 경우에는 해당 개인정보처리자에 대하여 해당 결정을 거부할 수 있는 권리를 가진다. 다만, 자동화된 결정이 제15조제1항제1호·제2호 및 제4호에 따라 이루어지는 경우에는 그러하지 아니하다.

- ② 정보주체는 개인정보처리자가 자동화된 결정을 한 경우에는 그 결정에 대하여 설명 등을 요구할 수 있다.
- ③ 개인정보처리자는 제1항 또는 제2항에 따라 정보주체가 자동화된 결정을 거부하거나 이에 대한 설명 등을 요구한 경우에는 정당한 사유가 없는 한 자동화된 결정을 적용하지 아니하거나 인적 개입에 의한 재처리·설명 등 필요한 조치를 하여야 한다.
- ④ 개인정보처리자는 자동화된 결정의 기준과 절차, 개인정보가 처리되는 방식 등을 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.
- ⑤ 제1항부터 제4항까지에서 규정한 사항 외에 자동화된 결정의 거부·설명 등을 요구하는 절차 및 방법, 거부·설명 등의 요구에 따른 필요한 조치, 자동화된 결정의 기준·절차 및 개인정보가 처리되는 방식의 공개 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2023. 3. 14.]

제38조(권리행사의 방법 및 절차) ① 정보주체는 제35조에 따른 열람, 제35조의2에 따른 전송, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지 및 동의 철회, 제37조의2에 따른 거부·설명 등의 요구(이하 “열람등요구”라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.<개정 2020. 2. 4., 2023. 3. 14.>

- ② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람등요구를 할 수 있다.

- ③ 개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다. 다만, 제35조의2제2항에 따른 전송 요구의 경우에는 전송을 위해 추가로 필요한 설비 등을 함께 고려하여 수수료를 산정할 수 있다.<개정 2023. 3. 14.>
- ④ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다. 이 경우 열람등요구의 방법과 절차는 해당 개인정보의 수집 방법과 절차보다 어렵지 아니하도록 하여야 한다.<개정 2023. 3. 14.>
- ⑤ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

제39조(손해배상책임) ① 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 삭제<2015. 7. 24.>

③ 개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 5배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 개인정보처리자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다.<신설 2015. 7. 24., 2023. 3. 14.>

④ 법원은 제3항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다.<신설 2015. 7. 24.>

1. 고의 또는 손해 발생의 우려를 인식한 정도
2. 위반행위로 인하여 입은 피해 규모
3. 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익
4. 위반행위에 따른 벌금 및 과징금
5. 위반행위의 기간·횟수 등
6. 개인정보처리자의 재산상태
7. 개인정보처리자가 정보주체의 개인정보 분실·도난·유출 후 해당 개인정보를 회수하기 위하여 노력한 정도
8. 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도

제39조의2(법정손해배상의 청구) ① 제39조제1항에도 불구하고 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를

고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.

- ③ 제39조에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.

[본조신설 2015. 7. 24.]

제6장 삭제

제39조의3(자료의 제출) ① 법원은 이 법을 위반한 행위로 인한 손해배상청구소송에서 당사자의 신청에 따라 상대방 당사자에게 해당 손해의 증명 또는 손해액의 산정에 필요한 자료의 제출을 명할 수 있다. 다만, 제출명령을 받은 자가 그 자료의 제출을 거부할 정당한 이유가 있으면 그러하지 아니하다.

- ② 법원은 제1항에 따른 제출명령을 받은 자가 그 자료의 제출을 거부할 정당한 이유가 있다고 주장하는 경우에는 그 주장의 당부(當否)를 판단하기 위하여 자료의 제시를 명할 수 있다. 이 경우 법원은 그 자료를 다른 사람이 보게 하여서는 아니 된다.

- ③ 제1항에 따라 제출되어야 할 자료가 「부정경쟁방지 및 영업비밀보호에 관한 법률」 제2조제2호에 따른 영업비밀(이하 “영업비밀”이라 한다)에 해당하나 손해의 증명 또는 손해액의 산정에 반드시 필요한 경우에는 제1항 단서에 따른 정당한 이유로 보지 아니한다. 이 경우 법원은 제출명령의 목적 내에서 열람할 수 있는 범위 또는 열람할 수 있는 사람을 지정하여야 한다.

- ④ 법원은 제1항에 따른 제출명령을 받은 자가 정당한 이유 없이 그 명령에 따르지 아니한 경우에는 자료의 기재에 대한 신청인의 주장을 진실한 것으로 인정할 수 있다.

- ⑤ 법원은 제4항에 해당하는 경우 신청인이 자료의 기재에 관하여 구체적으로 주장하기에 현저히 곤란한 사정이 있고 자료로 증명할 사실을 다른 증거로 증명하는 것을 기대하기도 어려운 경우에는 신청인이 자료의 기재로 증명하려는 사실에 관한 주장을 진실한 것으로 인정할 수 있다.

[전문개정 2023. 3. 14.]

제39조의4(비밀유지명령) ① 법원은 이 법을 위반한 행위로 인한 손해배상청구소송에서 당사자의 신청에 따른 결정으로 다음 각 호의 자에게 그 당사자가 보유한 영업비밀을 해당 소송의 계속적인 수행 외의 목적으로 사용하거나 그 영업비밀에 관계된 이 항에 따른 명령을 받은 자 외의 자에게 공개하지 아니할 것을 명할 수 있다. 다만, 그 신청 시점까지 다음 각 호의 자가 준비서면의 열람이나 증거조사 외의 방법으로 그 영업비밀을 이미 취득하고 있는 경우에는 그러하지 아니하다.

1. 다른 당사자(법인인 경우에는 그 대표자를 말한다)
2. 당사자를 위하여 해당 소송을 대리하는 자
3. 그 밖에 해당 소송으로 영업비밀을 알게 된 자

- ② 제1항에 따른 명령(이하 “비밀유지명령”이라 한다)을 신청하는 자는 다음 각 호의 사유를 모두 소명하여야 한다.

1. 이미 제출하였거나 제출하여야 할 준비서면, 이미 조사하였거나 조사하여야 할 증거 또는 제39조의3제1항에 따라 제출하였거나 제출하여야 할 자료에 영업비밀이 포함되어 있다는 것
 2. 제1호의 영업비밀이 해당 소송 수행 외의 목적으로 사용되거나 공개되면 당사자의 영업에 지장을 줄 우려가 있어 이를 방지하기 위하여 영업비밀의 사용 또는 공개를 제한할 필요가 있다는 것
- ③ 비밀유지명령의 신청은 다음 각 호의 사항을 적은 서면으로 하여야 한다.
1. 비밀유지명령을 받을 자
 2. 비밀유지명령의 대상이 될 영업비밀을 특정하기에 충분한 사실
 3. 제2항 각 호의 사유에 해당하는 사실
- ④ 법원은 비밀유지명령이 결정된 경우에는 그 결정서를 비밀유지명령을 받을 자에게 송달하여야 한다.
- ⑤ 비밀유지명령은 제4항의 결정서가 비밀유지명령을 받을 자에게 송달된 때부터 효력이 발생한다.
- ⑥ 비밀유지명령의 신청을 기각하거나 각하한 재판에 대해서는 즉시항고를 할 수 있다.

[전문개정 2023. 3. 14.]

- 제39조의5(비밀유지명령의 취소)** ① 비밀유지명령을 신청한 자 또는 비밀유지명령을 받은 자는 제39조의4제2항 각 호의 사유에 부합하지 아니하는 사실이나 사정이 있는 경우 소송기록을 보관하고 있는 법원(소송기록을 보관하고 있는 법원이 없는 경우에는 비밀유지명령을 내린 법원을 말한다)에 비밀유지명령의 취소를 신청할 수 있다.
- ② 법원은 비밀유지명령의 취소신청에 대한 재판이 있는 경우에는 그 결정서를 그 신청을 한 자 및 상대방에게 송달하여야 한다.
- ③ 비밀유지명령의 취소신청에 대한 재판에 대해서는 즉시항고를 할 수 있다.
- ④ 비밀유지명령을 취소하는 재판은 확정되어야 효력이 발생한다.
- ⑤ 비밀유지명령을 취소하는 재판을 한 법원은 비밀유지명령의 취소신청을 한 자 또는 상대방 외에 해당 영업비밀에 관한 비밀유지명령을 받은 자가 있는 경우에는 그 자에게 즉시 비밀유지명령의 취소 재판을 한 사실을 알려야 한다.

[전문개정 2023. 3. 14.]

- 제39조의6(소송기록 열람 등의 청구 통지 등)** ① 비밀유지명령이 내려진 소송(모든 비밀유지명령이 취소된 소송은 제외한다)에 관한 소송기록에 대하여 「민사소송법」 제163조제1항에 따라 열람 등의 신청인을 당사자로 제한하는 결정이 있었던 경우로서 당사자가 같은 항에서 규정하는 비밀 기재부분의 열람 등의 청구를 하였으나 그 청구 절차를 해당 소송에서 비밀유지명령을 받지 아니한 자가 밟은 경우에는 법원서기관, 법원사무관, 법원주사 또는 법원주사보(이하 이 조에서 “법원사무관등”이라 한다)는 같은 항의 신청을 한 당사자(그 열람 등의 청구를 한 자는 제외한다. 이하 제3항에서 같다)에게 그 청구 직후에 그 열람 등의 청구가 있었다는 사실을 알려야 한다.

- ② 법원사무관등은 제1항의 청구가 있었던 날부터 2주일이 지날 때까지(그 청구 절차를 밟은 자에 대한 비밀유지명령 신청이 그 기간 내에 이루어진 경우에는 그 신청에 대한 재판이 확정되는 시점까지를 말한다) 그 청구 절차를 밟은 자에게 제1항의 비밀 기재부분의 열람 등을 하게 하여서는 아니 된다.
- ③ 제2항은 제1항의 열람 등의 청구를 한 자에게 제1항의 비밀 기재부분의 열람 등을 하게 하는 것에 대하여 「민사소송법」 제163조제1항의 신청을 한 당사자 모두가 동의하는 경우에는 적용되지 아니한다.

[전문개정 2023. 3. 14.]

제39조의7(손해배상의 보장) ① 개인정보처리자로서 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 제39조 및 제39조의2에 따른 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.<개정 2023. 3. 14.>

- ② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 조치를 하지 아니할 수 있다.<개정 2023. 3. 14.>
1. 대통령령으로 정하는 공공기관, 비영리법인 및 단체
 2. 「소상공인기본법」 제2조제1항에 따른 소상공인으로서 대통령령으로 정하는 자에게 개인정보 처리를 위탁한 자
 3. 다른 법률에 따라 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립한 개인정보처리자
- ③ 제1항 및 제2항에 따른 개인정보처리자의 손해배상책임 이행 기준 등에 필요한 사항은 대통령령으로 정한다.<신설 2023. 3. 14.>

[본조신설 2020. 2. 4.]

[제39조의9에서 이동, 종전 제39조의7은 삭제 <2023. 3. 14.>]

제7장 개인정보 분쟁조정위원회

제40조(설치 및 구성) ① 개인정보에 관한 분쟁의 조정(調停)을 위하여 개인정보 분쟁조정위원회(이하 “분쟁조정위원회”라 한다)를 둔다.

- ② 분쟁조정위원회는 위원장 1명을 포함한 30명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다.<개정 2015. 7. 24., 2023. 3. 14.>
- ③ 위촉위원은 다음 각 호의 어느 하나에 해당하는 사람 중에서 보호위원회 위원장이 위촉하고, 대통령령으로 정하는 국가기관 소속 공무원은 당연직위원이 된다.<개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24.>
1. 개인정보 보호업무를 관장하는 중앙행정기관의 고위공무원단에 속하는 공무원으로 재직하였던 사람 또는 이에 상당하는 공공부문 및 관련 단체의 직에 재직하고 있거나 재직하였던 사람으로서 개인정보 보호업무를 경험한 사람
 2. 대학이나 공인된 연구기관에서 부교수 이상 또는 이에 상당하는 직에 재직하고

있거나 재직하였던 사람

3. 판사·검사 또는 변호사로 재직하고 있거나 재직하였던 사람

4. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람

5. 개인정보처리자로 구성된 사업자단체의 임원으로 재직하고 있거나 재직하였던 사람

④ 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이

위촉한다.<개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24.>

⑤ 위원장과 위촉위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다.<개정 2015. 7. 24.>

⑥ 분쟁조정위원회는 분쟁조정 업무를 효율적으로 수행하기 위하여 필요하면 대통령령으로 정하는 바에 따라 조정사건의 분야별로 5명 이내의 위원으로 구성되는 조정부를 둘 수 있다. 이 경우 조정부가 분쟁조정위원회에서 위임받아 의결한 사항은 분쟁조정위원회에서 의결한 것으로 본다.

⑦ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

⑧ 보호위원회는 분쟁조정 접수, 사실 확인 등 분쟁조정에 필요한 사무를 처리할 수 있다.<개정 2015. 7. 24.>

⑨ 이 법에서 정한 사항 외에 분쟁조정위원회 운영에 필요한 사항은 대통령령으로 정한다.

제41조(위원의 신분보장) 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다.

제42조(위원의 제척·기피·회피) ① 분쟁조정위원회의 위원은 다음 각 호의 어느 하나에 해당하는 경우에는 제43조제1항에 따라 분쟁조정위원회에 신청된 분쟁조정사건(이하 이 조에서 “사건”이라 한다)의 심의·의결에서 제척(除斥)된다.

1. 위원 또는 그 배우자나 배우자였던 자가 그 사건의 당사자가 되거나 그 사건에 관하여 공동의 권리자 또는 의무자의 관계에 있는 경우

2. 위원이 그 사건의 당사자와 친족이거나 친족이었던 경우

3. 위원이 그 사건에 관하여 증언, 감정, 법률자문을 한 경우

4. 위원이 그 사건에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우

② 당사자는 위원에게 공정한 심의·의결을 기대하기 어려운 사정이 있으면 위원장에게 기피신청을 할 수 있다. 이 경우 위원장은 기피신청에 대하여 분쟁조정위원회의 의결을 거치지 아니하고 결정한다.

③ 위원이 제1항 또는 제2항의 사유에 해당하는 경우에는 스스로 그 사건의 심의·의결에서 회피할 수 있다.

제43조(조정 신청 등) ① 개인정보와 관련한 분쟁의 조정을 원하는 자는 분쟁조정위원회에 분쟁조정을 신청할 수 있다.

② 분쟁조정위원회는 당사자 일방으로부터 분쟁조정 신청을 받았을 때에는 그 신청내용을 상대방에게 알려야 한다.

- ③ 개인정보처리자가 제2항에 따른 분쟁조정 의 통지를 받은 경우에는 특별한 사유가 없으면 분쟁조정에 응하여야 한다.<개정 2023. 3. 14.>

제44조(처리기간) ① 분쟁조정위원회는 제43조제1항에 따른 분쟁조정 신청을 받은 날부터 60일 이내에 이를 심사하여 조정안을 작성하여야 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.

- ② 분쟁조정위원회는 제1항 단서에 따라 처리기간을 연장한 경우에는 기간연장의 사유와 그 밖의 기간연장에 관한 사항을 신청인에게 알려야 한다.

제45조(자료의 요청 및 사실조사 등) ① 분쟁조정위원회는 제43조제1항에 따라 분쟁조정 신청을 받았을 때에는 해당 분쟁의 조정을 위하여 필요한 자료를 분쟁당사자에게 요청할 수 있다. 이 경우 분쟁당사자는 정당한 사유가 없으면 요청에 따라야 한다.

- ② 분쟁조정위원회는 분쟁의 조정을 위하여 사실 확인이 필요한 경우에는 분쟁조정위원회의 위원 또는 대통령령으로 정하는 사무기구의 소속 공무원으로 하여금 사건과 관련된 장소에 출입하여 관련 자료를 조사하거나 열람하게 할 수 있다. 이 경우 분쟁당사자는 해당 조사·열람을 거부할 정당한 사유가 있을 때에는 그 사유를 소명하고 조사·열람에 따르지 아니할 수 있다.<신설 2023. 3. 14.>

- ③ 제2항에 따른 조사·열람을 하는 위원 또는 공무원은 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 한다.<신설 2023. 3. 14.>

- ④ 분쟁조정위원회는 분쟁의 조정을 위하여 필요하다고 인정하면 관계 기관 등에 자료 또는 의견의 제출 등 필요한 협조를 요청할 수 있다.<신설 2023. 3. 14.>

- ⑤ 분쟁조정위원회는 필요하다고 인정하면 분쟁당사자나 참고인을 위원회에 출석하도록 하여 그 의견을 들을 수 있다.<개정 2023. 3. 14.>

[제목개정 2023. 3. 14.]

제45조의2(진술의 원용 제한) 조정절차에서의 의견과 진술은 소송(해당 조정에 대한 준재심은 제외한다)에서 원용(援用)하지 못한다.

[본조신설 2023. 3. 14.]

제46조(조정 전 합의 권고) 분쟁조정위원회는 제43조제1항에 따라 분쟁조정 신청을 받았을 때에는 당사자에게 그 내용을 제시하고 조정 전 합의를 권고할 수 있다.

제47조(분쟁의 조정) ① 분쟁조정위원회는 다음 각 호의 어느 하나의 사항을 포함하여 조정안을 작성할 수 있다.

1. 조사 대상 침해행위의 중지
2. 원상회복, 손해배상, 그 밖에 필요한 구제조치
3. 같거나 비슷한 침해의 재발을 방지하기 위하여 필요한 조치

- ② 분쟁조정위원회는 제1항에 따라 조정안을 작성하면 지체 없이 각 당사자에게 제시하여야 한다.

- ③ 제2항에 따라 조정안을 제시받은 당사자가 제시받은 날부터 15일 이내에 수락

여부를 알리지 아니하면 조정을 수락한 것으로 본다.<개정 2023. 3. 14.>

- ④ 당사자가 조정내용을 수락한 경우(제3항에 따라 수락한 것으로 보는 경우를 포함한다) 분쟁조정위원회는 조정서를 작성하고, 분쟁조정위원회의 위원장과 각 당사자가 기명날인 또는 서명을 한 후 조정서 정본을 지체 없이 각 당사자 또는 그 대리인에게 송달하여야 한다. 다만, 제3항에 따라 수락한 것으로 보는 경우에는 각 당사자의 기명날인 및 서명을 생략할 수 있다.<개정 2023. 3. 14.>
- ⑤ 제4항에 따른 조정의 내용은 재판상 화해와 동일한 효력을 갖는다.

제48조(조정거부 및 중지) ① 분쟁조정위원회는 분쟁의 성질상 분쟁조정위원회에서 조정하는 것이 적합하지 아니하다고 인정하거나 부정한 목적으로 조정이 신청되었다고 인정하는 경우에는 그 조정을 거부할 수 있다. 이 경우 조정거부의 사유 등을 신청인에게 알려야 한다.

② 분쟁조정위원회는 신청된 조정사건에 대한 처리절차를 진행하던 중에 한 쪽 당사자가 소를 제기하면 그 조정의 처리를 중지하고 이를 당사자에게 알려야 한다.

제49조(집단분쟁조정) ① 국가 및 지방자치단체, 개인정보 보호단체 및 기관, 정보주체, 개인정보처리자는 정보주체의 피해 또는 권리침해가 다수의 정보주체에게 같거나 비슷한 유형으로 발생하는 경우로서 대통령령으로 정하는 사건에 대하여는 분쟁조정위원회에 일괄적인 분쟁조정(이하 “집단분쟁조정”이라 한다)을 의뢰 또는 신청할 수 있다.

② 제1항에 따라 집단분쟁조정을 의뢰받거나 신청받은 분쟁조정위원회는 그 의결로써 제3항부터 제7항까지의 규정에 따른 집단분쟁조정의 절차를 개시할 수 있다. 이 경우 분쟁조정위원회는 대통령령으로 정하는 기간 동안 그 절차의 개시를 공고하여야 한다.

③ 분쟁조정위원회는 집단분쟁조정의 당사자가 아닌 정보주체 또는 개인정보처리자로부터 그 분쟁조정의 당사자에 추가로 포함될 수 있도록 하는 신청을 받을 수 있다.

④ 분쟁조정위원회는 그 의결로써 제1항 및 제3항에 따른 집단분쟁조정의 당사자 중에서 공동의 이익을 대표하기에 가장 적합한 1인 또는 수인을 대표당사자로 선임할 수 있다.

⑤ 분쟁조정위원회는 개인정보처리자가 분쟁조정위원회의 집단분쟁조정의 내용을 수락한 경우에는 집단분쟁조정의 당사자가 아닌 자로서 피해를 입은 정보주체에 대한 보상계획서를 작성하여 분쟁조정위원회에 제출하도록 권고할 수 있다.

⑥ 제48조제2항에도 불구하고 분쟁조정위원회는 집단분쟁조정의 당사자인 다수의 정보주체 중 일부의 정보주체가 법원에 소를 제기한 경우에는 그 절차를 중지하지 아니하고, 소를 제기한 일부의 정보주체를 그 절차에서 제외한다.

⑦ 집단분쟁조정의 기간은 제2항에 따른 공고가 종료된 날의 다음 날부터 60일 이내로 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.

⑧ 집단분쟁조정의 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제50조(조정절차 등) ① 제43조부터 제49조까지의 규정에서 정한 것 외에 분쟁의 조정방법, 조정절차 및 조정업무의 처리 등에 필요한 사항은 대통령령으로 정한다.

② 분쟁조정위원회의 운영 및 분쟁조정 절차에 관하여 이 법에서 규정하지 아니한

사항에 대하여는 「민사조정법」을 준용한다.

제50조의2(개선의견의 통보) 분쟁조정위원회는 소관 업무 수행과 관련하여 개인정보 보호 및 정보주체의 권리 보호를 위한 개선의견을 보호위원회 및 관계 중앙행정기관의 장에게 통보할 수 있다.

[본조신설 2023. 3. 14.]

제8장 개인정보 단체소송

제51조(단체소송의 대상 등) 다음 각 호의 어느 하나에 해당하는 단체는

개인정보처리자가 제49조에 따른 집단분쟁조정을 거부하거나 집단분쟁조정 결과 수락하지 아니한 경우에는 법원에 권리침해 행위의 금지·중지를 구하는 소송(이하 “단체소송”이라 한다)을 제기할 수 있다.

1. 「소비자기본법」 제29조에 따라 공정거래위원회에 등록한 소비자단체로서 다음 각 목의 요건을 모두 갖춘 단체
 - 가. 정관에 따라 상시적으로 정보주체의 권익증진을 주된 목적으로 하는 단체일 것
 - 나. 단체의 정회원수가 1천명 이상일 것
 - 다. 「소비자기본법」 제29조에 따른 등록 후 3년이 경과하였을 것
2. 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 다음 각 목의 요건을 모두 갖춘 단체
 - 가. 법률상 또는 사실상 동일한 침해를 입은 100명 이상의 정보주체로부터 단체소송의 제기를 요청받을 것
 - 나. 정관에 개인정보 보호를 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동실적이 있을 것
 - 다. 단체의 상시 구성원수가 5천명 이상일 것
 - 라. 중앙행정기관에 등록되어 있을 것

제52조(전속관할) ① 단체소송의 소는 피고의 주된 사무소 또는 영업소가 있는 곳, 주된 사무소나 영업소가 없는 경우에는 주된 업무담당자의 주소가 있는 곳의 지방법원 본원 합의부의 관할에 전속한다.

- ② 제1항을 외국사업자에 적용하는 경우 대한민국에 있는 이들의 주된 사무소·영업소 또는 업무담당자의 주소에 따라 정한다.

제53조(소송대리인의 선임) 단체소송의 원고는 변호사를 소송대리인으로 선임하여야 한다.

제54조(소송허가신청) ① 단체소송을 제기하는 단체는 소장과 함께 다음 각 호의 사항을 기재한 소송허가신청서를 법원에 제출하여야 한다.

1. 원고 및 그 소송대리인
2. 피고

3. 정보주체의 침해된 권리의 내용
- ② 제1항에 따른 소송허가신청서에는 다음 각 호의 자료를 첨부하여야 한다.
 1. 소제기단체가 제51조 각 호의 어느 하나에 해당하는 요건을 갖추고 있음을 소명하는 자료
 2. 개인정보처리자가 조정을 거부하였거나 조정결과를 수락하지 아니하였음을 증명하는 서류

제55조(소송허가요건 등) ① 법원은 다음 각 호의 요건을 모두 갖춘 경우에 한하여 결정으로 단체소송을 허가한다.

1. 개인정보처리자가 분쟁조정위원회의 조정을 거부하거나 조정결과를 수락하지 아니하였을 것
 2. 제54조에 따른 소송허가신청서의 기재사항에 흠결이 없을 것
- ② 단체소송을 허가하거나 불허가하는 결정에 대하여는 즉시항고할 수 있다.

제56조(확정판결의 효력) 원고의 청구를 기각하는 판결이 확정된 경우 이와 동일한 사안에 관하여는 제51조에 따른 다른 단체는 단체소송을 제기할 수 없다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 판결이 확정된 후 그 사안과 관련하여 국가·지방자치단체 또는 국가·지방자치단체가 설립한 기관에 의하여 새로운 증거가 나타난 경우
2. 기각판결이 원고의 고의로 인한 것임이 밝혀진 경우

제57조(「민사소송법」의 적용 등) ① 단체소송에 관하여 이 법에 특별한 규정이 없는 경우에는 「민사소송법」을 적용한다.

- ② 제55조에 따른 단체소송의 허가결정이 있는 경우에는 「민사집행법」 제4편에 따른 보전처분을 할 수 있다.
- ③ 단체소송의 절차에 관하여 필요한 사항은 대법원규칙으로 정한다.

제9장 보칙

제58조(적용의 일부 제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제3장부터 제8장까지를 적용하지 아니한다.<개정 2023. 3. 14.>

1. 삭제<2023. 3. 14.>
 2. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보
 3. 삭제<2023. 3. 14.>
 4. 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보
- ② 제25조제1항 각 호에 따라 공개된 장소에 고정형 영상정보처리기를 설치·운영하여 처리되는 개인정보에 대해서는 제15조, 제22조, 제22조의2, 제27조제1항·제2항, 제34조 및 제37조를 적용하지 아니한다.<개정 2023. 3. 14.>

- ③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30조 및 제31조를 적용하지 아니한다.
- ④ 개인정보처리자는 제1항 각 호에 따라 개인정보를 처리하는 경우에도 그 목적을 위하여 필요한 범위에서 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치, 개인정보의 처리에 관한 고충처리, 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하여야 한다.

제58조의2(적용제외) 이 법은 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보에는 적용하지 아니한다.

[본조신설 2020. 2. 4.]

제59조(금지행위) 개인정보를 처리하거나 처리하였던 자는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.<개정 2023. 3. 14.>

1. 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위
2. 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위
3. 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 이용, 훼손, 멸실, 변경, 위조 또는 유출하는 행위

제60조(비밀유지 등) 다음 각 호의 업무에 종사하거나 종사하였던 자는 직무상 알게 된 비밀을 다른 사람에게 누설하거나 직무상 목적 외의 용도로 이용하여서는 아니 된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.<개정 2020. 2. 4., 2023. 3. 14.>

1. 제7조의8 및 제7조의9에 따른 보호위원회의 업무
2. 제28조의3에 따른 전문기관의 지정 업무 및 전문기관의 업무
3. 제32조의2에 따른 개인정보 보호 인증 업무
4. 제33조에 따른 영향평가 업무
5. 제35조의3에 따른 개인정보관리 전문기관의 지정 업무 및 개인정보관리 전문기관의 업무
6. 제40조에 따른 분쟁조정위원회의 분쟁조정 업무

[시행일: 2024. 3. 15.] 제60조제5호

제61조(의견제시 및 개선권고) ① 보호위원회는 개인정보 보호에 영향을 미치는 내용이 포함된 법령이나 조례에 대하여 필요하다고 인정하면 심의·의결을 거쳐 관계 기관에 의견을 제시할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

- ② 보호위원회는 개인정보 보호를 위하여 필요하다고 인정하면 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은

개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 보호위원회에 알려야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

- ③ 관계 중앙행정기관의 장은 개인정보 보호를 위하여 필요하다고 인정하면 소관 법률에 따라 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 관계 중앙행정기관의 장에게 알려야 한다.
- ④ 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관에 대하여 개인정보 보호에 관한 의견을 제시하거나 지도·점검을 할 수 있다.

제62조(침해 사실의 신고 등) ① 개인정보처리자가 개인정보를 처리할 때 개인정보에 관한 권리 또는 이익을 침해받은 사람은 보호위원회에 그 침해 사실을 신고할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

- ② 보호위원회는 제1항에 따른 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위하여 대통령령으로 정하는 바에 따라 전문기관을 지정할 수 있다. 이 경우 전문기관은 개인정보침해 신고센터(이하 “신고센터”라 한다)를 설치·운영하여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>
- ③ 신고센터는 다음 각 호의 업무를 수행한다.
 - 1. 개인정보 처리와 관련한 신고의 접수·상담
 - 2. 사실의 조사·확인 및 관계자의 의견 청취
 - 3. 제1호 및 제2호에 따른 업무에 딸린 업무
- ④ 보호위원회는 제3항제2호의 사실 조사·확인 등의 업무를 효율적으로 하기 위하여 필요하면 「국가공무원법」 제32조의4에 따라 소속 공무원을 제2항에 따른 전문기관에 파견할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

제63조(자료제출 요구 및 검사) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보처리자에게 관계 물품·서류 등 자료를 제출하게 할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

- 1. 이 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우
 - 2. 이 법 위반에 대한 신고를 받거나 민원이 접수된 경우
 - 3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우
- ② 보호위원회는 개인정보처리자가 제1항에 따른 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원으로 하여금 개인정보처리자 및 해당 법 위반사실과 관련한 관계인의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하게 할 수 있다. 이 경우 검사를 하는 공무원은 그 권한을 나타내는 증표를 지니고 이를 관계인에게 내보여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24., 2017. 7. 26., 2020. 2. 4.>

- ③ 보호위원회는 이 법 등 개인정보 보호와 관련된 법규의 위반행위로 인하여 중대한 개인정보 침해사고가 발생한 경우 신속하고 효과적인 대응을 위하여 다음 각 호의 어느 하나에 해당하는 관계 기관의 장에게 협조를 요청할 수 있다.<개정 2023. 3. 14.>
1. 중앙행정기관
 2. 지방자치단체
 3. 그 밖에 법령 또는 자치법규에 따라 행정권한을 가지고 있거나 위임 또는 위탁받은 공공기관
- ④ 제3항에 따라 협조를 요청받은 관계 기관의 장은 특별한 사정이 없으면 이에 따라야 한다.<개정 2023. 3. 14.>
- ⑤ 제1항 및 제2항에 따른 자료제출 요구, 검사 절차 및 방법 등에 관하여 필요한 사항은 보호위원회가 정하여 고시할 수 있다.<개정 2023. 3. 14.>
- ⑥ 보호위원회는 제1항 및 제2항에 따라 제출받거나 수집한 서류·자료 등을 이 법에 따른 경우를 제외하고는 제3자에게 제공하거나 일반에 공개해서는 아니 된다.<신설 2020. 2. 4., 2023. 3. 14.>
- ⑦ 보호위원회는 정보통신망을 통하여 자료의 제출 등을 받은 경우나 수집한 자료 등을 전자화한 경우에는 개인정보·영업비밀 등이 유출되지 아니하도록 제도적·기술적 보완조치를 하여야 한다.<신설 2020. 2. 4., 2023. 3. 14.>

- 제63조의2(사전 실태점검)** ① 보호위원회는 제63조제1항 각 호에 해당하지 아니하는 경우로서 개인정보 침해사고 발생의 위험성이 높고 개인정보 보호의 취약점을 사전에 점검할 필요성이 인정되는 개인정보처리자에 대하여 개인정보 보호실태를 점검할 수 있다.
- ② 보호위원회는 제1항에 따른 실태점검을 실시하여 이 법을 위반하는 사항을 발견한 경우 해당 개인정보처리자에 대하여 시정방안을 정하여 이에 따를 것을 권고할 수 있다.
- ③ 제2항에 따른 시정권고를 받은 개인정보처리자는 이를 통보받은 날부터 10일 이내에 해당 권고를 수락하는지 여부에 관하여 보호위원회에 통지하여야 하며, 그 이행 결과를 보호위원회가 고시로 정하는 바에 따라 보호위원회에 알려야 한다.
- ④ 제2항에 따른 시정권고를 받은 자가 해당 권고를 수락한 때에는 제64조제1항에 따른 시정조치 명령(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회의 경우에는 제64조제3항에 따른 권고를 말한다)을 받은 것으로 본다.
- ⑤ 보호위원회는 제2항에 따른 시정권고를 받은 자가 해당 권고를 수락하지 아니하거나 이행하지 아니한 경우 제63조제2항에 따른 검사를 할 수 있다.
- ⑥ 보호위원회는 관계 중앙행정기관의 장과 합동으로 제1항에 따른 개인정보 보호실태를 점검할 수 있다.

[본조신설 2023. 3. 14.]

- 제64조(시정조치 등)** ① 보호위원회는 이 법을 위반한 자(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 제외한다)에 대하여 다음 각 호에 해당하는 조치를 명할 수 있다.<개정 2013. 3. 23, 2014. 11. 19, 2017. 7. 26, 2020. 2. 4, 2023. 3. 14.>

1. 개인정보 침해행위의 중지
 2. 개인정보 처리의 일시적인 정지
 3. 그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치
- ② 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관이 이 법을 위반하였을 때에는 제1항 각 호에 해당하는 조치를 명할 수 있다.
<개정 2023. 3. 14.>
- ③ 보호위원회는 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회가 이 법을 위반하였을 때에는 해당 기관의 장에게 제1항 각 호에 해당하는 조치를 하도록 권고할 수 있다. 이 경우 권고를 받은 기관은 특별한 사유가 없으면 이를 존중하여야 한다.<개정 2023. 3. 14.>

제64조의2(과징금의 부과) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보처리자에게 전체 매출액의 100분의 3을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 20억원을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다.

1. 제15조제1항, 제17조제1항, 제18조제1항·제2항(제26조제8항에 따라 준용되는 경우를 포함한다) 또는 제19조를 위반하여 개인정보를 처리한 경우
 2. 제22조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 처리한 경우
 3. 제23조제1항제1호(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 정보주체의 동의를 받지 아니하고 민감정보를 처리한 경우
 4. 제24조제1항·제24조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고유식별정보 또는 주민등록번호를 처리한 경우
 5. 제26조제4항에 따른 관리·감독 또는 교육을 소홀히 하여 수탁자가 이 법의 규정을 위반한 경우
 6. 제28조의5제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 특정 개인을 알아보기 위한 목적으로 정보를 처리한 경우
 7. 제28조의8제1항(제26조제8항 및 제28조의11에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 국외로 이전한 경우
 8. 제28조의9제1항(제26조제8항 및 제28조의11에 따라 준용되는 경우를 포함한다)을 위반하여 국외 이전 중지 명령을 따르지 아니한 경우
 9. 개인정보처리자가 처리하는 개인정보가 분실·도난·유출·위조·변조·훼손된 경우. 다만, 개인정보가 분실·도난·유출·위조·변조·훼손되지 아니하도록 개인정보처리자가 제29조(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.
- ② 보호위원회는 제1항에 따른 과징금을 부과하려는 경우 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액을 기준으로 과징금을 산정한다.

- ③ 보호위원회는 제1항에 따른 과징금을 부과하려는 경우 개인정보처리자가 정당한 사유 없이 매출액 산정자료의 제출을 거부하거나 거짓의 자료를 제출한 경우에는 해당 개인정보처리자의 전체 매출액을 기준으로 산정하되 해당 개인정보처리자 및 비슷한 규모의 개인정보처리자의 개인정보 보유 규모, 재무제표 등 회계자료, 상품·용역의 가격 등 영업현황 자료에 근거하여 매출액을 추정할 수 있다.
- ④ 보호위원회는 제1항에 따른 과징금을 부과하는 경우에는 위반행위에 상응하는 비례성과 침해 예방에 대한 효과성이 확보될 수 있도록 다음 각 호의 사항을 고려하여야 한다.
1. 위반행위의 내용 및 정도
 2. 위반행위의 기간 및 횟수
 3. 위반행위로 인하여 취득한 이익의 규모
 4. 암호화 등 안전성 확보 조치 이행 노력
 5. 개인정보가 분실·도난·유출·위조·변조·훼손된 경우 위반행위와의 관련성 및 분실·도난·유출·위조·변조·훼손의 규모
 6. 위반행위로 인한 피해의 회복 및 피해 확산 방지 조치의 이행 여부
 7. 개인정보처리자의 업무 형태 및 규모
 8. 개인정보처리자가 처리하는 개인정보의 유형과 정보주체에게 미치는 영향
 9. 위반행위로 인한 정보주체의 피해 규모
 10. 개인정보 보호 인증, 자율적인 보호 활동 등 개인정보 보호를 위한 노력
 11. 보호위원회와의 협조 등 위반행위를 시정하기 위한 조치 여부
- ⑤ 보호위원회는 다음 각 호의 어느 하나에 해당하는 사유가 있는 경우에는 과징금을 부과하지 아니할 수 있다.
1. 지급불능·지급정지 또는 자본잠식 등의 사유로 객관적으로 과징금을 낼 능력이 없다고 인정되는 경우
 2. 본인의 행위가 위법하지 아니한 것으로 잘못 인식할 만한 정당한 사유가 있는 경우
 3. 위반행위의 내용·정도가 경미하거나 산정된 과징금이 소액인 경우
 4. 그 밖에 정보주체에게 피해가 발생하지 아니하였거나 경미한 경우로서 대통령령으로 정하는 사유가 있는 경우
- ⑥ 제1항에 따른 과징금은 제2항부터 제5항까지를 고려하여 산정하되, 구체적인 산정기준과 산정절차는 대통령령으로 정한다.
- ⑦ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니하면 납부기한의 다음 날부터 내지 아니한 과징금의 연 100분의 6에 해당하는 가산금을 징수한다. 이 경우 가산금을 징수하는 기간은 60개월을 초과하지 못한다.
- ⑧ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니한 경우에는 기간을 정하여 독촉하고, 독촉으로 지정한 기간 내에 과징금과 제7항에 따른 가산금을 내지 아니하면 국세강제징수의 예에 따라 징수한다.
- ⑨ 보호위원회는 법원의 판결 등의 사유로 제1항에 따라 부과된 과징금을 환급하는 경우에는

과징금을 낸 날부터 환급하는 날까지의 기간에 대하여 금융회사 등의 예금이자율 등을 고려하여 대통령령으로 정하는 이자율을 적용하여 계산한 환급가산금을 지급하여야 한다.

- ⑩ 보호위원회는 제9항에도 불구하고 법원의 판결에 따라 과징금 부과처분이 취소되어 그 판결이유에 따라 새로운 과징금을 부과하는 경우에는 당초 납부한 과징금에서 새로 부과하기로 결정한 과징금을 공제한 나머지 금액에 대해서만 환급가산금을 계산하여 지급한다.

[본조신설 2023. 3. 14.]

제65조(고발 및 징계권고) ① 보호위원회는 개인정보처리자에게 이 법 등 개인정보 보호와 관련된 법규의 위반에 따른 범죄혐의가 있다고 인정될 만한 상당한 이유가 있을 때에는 관할 수사기관에 그 내용을 고발할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

- ② 보호위원회는 이 법 등 개인정보 보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때에는 책임이 있는 자(대표자 및 책임있는 임원을 포함한다)를 징계할 것을 해당 개인정보처리자에게 권고할 수 있다. 이 경우 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 보호위원회에 통보하여야 한다.<개정 2013. 3. 23., 2013. 8. 6., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

- ③ 관계 중앙행정기관의 장은 소관 법률에 따라 개인정보처리자에 대하여 제1항에 따른 고발을 하거나 소속 기관·단체 등의 장에게 제2항에 따른 징계권고를 할 수 있다. 이 경우 제2항에 따른 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 관계 중앙행정기관의 장에게 통보하여야 한다.

제66조(결과의 공표) ① 보호위원회는 제61조에 따른 개선권고, 제64조에 따른 시정조치 명령, 제64조의2에 따른 과징금의 부과, 제65조에 따른 고발 또는 징계권고 및 제75조에 따른 과태료 부과 내용 및 결과에 대하여 공표할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4., 2023. 3. 14.>

- ② 보호위원회는 제61조에 따른 개선권고, 제64조에 따른 시정조치 명령, 제64조의2에 따른 과징금의 부과, 제65조에 따른 고발 또는 징계권고 및 제75조에 따른 과태료 부과처분 등을 한 경우에는 처분 등을 받은 자에게 해당 처분 등을 받았다는 사실을 공표할 것을 명할 수 있다.<개정 2023. 3. 14.>

- ③ 제1항 및 제2항에 따른 개선권고 사실 등의 공표 및 공표명령의 방법, 기준 및 절차 등은 대통령령으로 정한다.<개정 2023. 3. 14.>

제67조(연차보고) ① 보호위원회는 관계 기관 등으로부터 필요한 자료를 제출받아 매년 개인정보 보호시책의 수립 및 시행에 관한 보고서를 작성하여 정기국회 개회 전까지 국회에 제출(정보통신망에 의한 제출을 포함한다)하여야 한다.

- ② 제1항에 따른 보고서에는 다음 각 호의 내용이 포함되어야 한다.<개정 2016. 3. 29., 2023. 3. 14.>

1. 정보주체의 권리침해 및 그 구제현황

2. 개인정보 처리에 관한 실태조사 및 개인정보 보호수준 평가 등의 결과
3. 개인정보 보호시책의 추진현황 및 실적
4. 개인정보 관련 해외의 입법 및 정책 동향
5. 주민등록번호 처리와 관련된 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙의 제정·개정 현황
6. 그 밖에 개인정보 보호시책에 관하여 공개 또는 보고하여야 할 사항

제68조(권한의 위임·위탁) ① 이 법에 따른 보호위원회 또는 관계 중앙행정기관의 장의 권한은 그 일부를 대통령령으로 정하는 바에 따라 특별시장, 광역시장, 도지사, 특별자치도지사 또는 대통령령으로 정하는 전문기관에 위임하거나 위탁할 수 있다.

<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

② 제1항에 따라 보호위원회 또는 관계 중앙행정기관의 장의 권한을 위임 또는 위탁받은 기관은 위임 또는 위탁받은 업무의 처리 결과를 보호위원회 또는 관계 중앙행정기관의 장에게 통보하여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

③ 보호위원회는 제1항에 따른 전문기관에 권한의 일부를 위임하거나 위탁하는 경우 해당 전문기관의 업무 수행을 위하여 필요한 경비를 출연할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

제69조(벌칙 적용 시의 공무원 의제) ① 보호위원회의 위원 중 공무원이 아닌 위원 및 공무원이 아닌 직원은 「형법」이나 그 밖의 법률에 따른 벌칙을 적용할 때에는 공무원으로 본다.<신설 2020. 2. 4.>

② 보호위원회 또는 관계 중앙행정기관의 장의 권한을 위탁한 업무에 종사하는 관계 기관의 임직원은 「형법」 제129조부터 제132조까지의 규정을 적용할 때에는 공무원으로 본다.<신설 2020. 2. 4.>

제10장 벌칙

제70조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.<개정 2015. 7. 24.>

1. 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단·마비 등 심각한 지장을 초래한 자
2. 거짓이나 그 밖의 부정한 수단이나 방법으로 다른 사람이 처리하고 있는 개인정보를 취득한 후 이를 영리 또는 부정한 목적으로 제3자에게 제공한 자와 이를 교사·알선한 자

제71조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.<개정 2016. 3. 29., 2020. 2. 4., 2023. 3. 14.>

1. 제17조제1항제2호에 해당하지 아니함에도 같은 항 제1호(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알면서도 개인정보를 제공받은 자
2. 제18조제1항·제2항, 제27조제3항 또는 제28조의2(제26조제8항에 따라 준용되는 경우를 포함한다), 제19조 또는 제26조제5항을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
3. 제22조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 처리한 자
4. 제23조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 민감정보를 처리한 자
5. 제24조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고유식별정보를 처리한 자
6. 제28조의3제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 보호위원회 또는 관계 중앙행정기관의 장으로부터 전문기관으로 지정받지 아니하고 가명정보를 결합한 자
7. 제28조의3제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 전문기관의 장의 승인을 받지 아니하고 결합을 수행한 기관 외부로 결합된 정보를 반출하거나 이를 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 결합된 정보를 제공받은 자
8. 제28조의5제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 특정 개인을 알아보기 위한 목적으로 가명정보를 처리한 자
9. 제59조제2호를 위반하여 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
10. 제59조제3호를 위반하여 다른 사람의 개인정보를 이용, 훼손, 멸실, 변경, 위조 또는 유출한 자

제72조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.<개정 2023. 3. 14.>

1. 제25조제5항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보처리기기의 설치 목적과 다른 목적으로 고정형 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자
2. 제59조제1호를 위반하여 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
3. 제60조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자

제73조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

1. 제36조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자
2. 제37조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 처리를 정지하지 아니하고 개인정보를 계속 이용하거나 제3자에게 제공한 자
3. 국내외에서 정당한 이유 없이 제39조의4에 따른 비밀유지명령을 위반한 자
4. 제63조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 자료제출 요구에 대하여 법 위반사항을 은폐 또는 축소할 목적으로 자료제출을 거부하거나 거짓의 자료를 제출한 자
5. 제63조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 출입·검사 시 자료의 은닉·폐기, 접근 거부 또는 위조·변조 등을 통하여 조사를 거부·방해 또는 기피한 자

② 제1항제3호의 죄는 비밀유지명령을 신청한 자의 고소가 없으면 공소를 제기할 수 없다.

[전문개정 2023. 3. 14.]

제74조(양벌규정) ① 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제70조에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인을 7천만원 이하의 벌금에 처한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

② 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

제74조의2(몰수·추징 등) 제70조부터 제73조까지의 어느 하나에 해당하는 죄를 지은 자가 해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 이를 몰수할 수 없을 때에는 그 가액을 추징할 수 있다. 이 경우 몰수 또는 추징은 다른 벌칙에 부가하여 과할 수 있다.

[본조신설 2015. 7. 24.]

제75조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다.

1. 제25조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보처리기기를 설치·운영한 자
 2. 제25조의2제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영한 자
- ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.
1. 제16조제3항·제22조제5항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 재화 또는 서비스의 제공을 거부한 자
 2. 제20조제1항·제2항을 위반하여 정보주체에게 같은 조 제1항 각 호의 사실을 알리지 아니한 자
 3. 제20조의2제1항을 위반하여 개인정보의 이용·제공 내역이나 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 통지하지 아니한 자
 4. 제21조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 아니한 자
 5. 제23조제2항·제24조제3항·제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·제29조(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자
 6. 제23조제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 알리지 아니한 자
 7. 제24조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 주민등록번호를 처리한 자
 8. 제24조의2제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 암호화 조치를 하지 아니한 자
 9. 제24조의2제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체가 주민등록번호를 사용하지 아니할 수 있는 방법을 제공하지 아니한 자
 10. 제25조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보처리기기를 설치·운영한 자
 11. 제25조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 사람 또는 그 사람과 관련된 사물의 영상을 촬영한 자
 12. 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자
 13. 제28조의5제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인을 알아볼 수 있는 정보가 생성되었음에도 이용을 중지하지 아니하거나 이를 회수·파기하지 아니한 자
 14. 제28조의8제4항(제26조제8항 및 제28조의11에 따라 준용되는 경우를 포함한다)을 위반하여 보호조치를 하지 아니한 자
 15. 제32조의2제6항을 위반하여 인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한 자
 16. 제33조제1항을 위반하여 영향평가를 하지 아니하거나 그 결과를 보호위원회에

제출하지 아니한 자

17. 제34조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
 18. 제34조제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하지 아니한 자
 19. 제35조제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 열람을 제한하거나 거절한 자
 20. 제35조의3제1항에 따른 지정을 받지 아니하고 같은 항 제2호의 업무를 수행한 자
 21. 제35조의3제3항을 위반한 자
 22. 제36조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정정·삭제 등 필요한 조치를 하지 아니한 자
 23. 제37조제3항 또는 제5항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 파기 등 필요한 조치를 하지 아니한 자
 24. 제37조의2제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정당한 사유 없이 정보주체의 요구에 따르지 아니한 자
 25. 제63조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 관계 물품·서류 등 자료를 제출하지 아니하거나 거짓으로 제출한 자
 26. 제63조제2항(제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 출입·검사를 거부·방해 또는 기피한 자
 27. 제64조제1항에 따른 시정조치 명령에 따르지 아니한 자
- ③ 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다.
1. 제26조제6항을 위반하여 위탁자의 동의를 받지 아니하고 제3자에게 다시 위탁한 자
 2. 제31조의2제1항을 위반하여 국내대리인을 지정하지 아니한 자
- ④ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.
1. 제11조의2제2항을 위반하여 정당한 사유 없이 자료를 제출하지 아니하거나 거짓으로 제출한 자
 2. 제21조제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 분리하여 저장·관리하지 아니한 자
 3. 제22조제1항부터 제3항까지(제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 동의를 받은 자
 4. 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서로 하지 아니한 자
 5. 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자
 6. 제27조제1항·제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 아니한 자
 7. 제28조의4제3항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 관련 기록을 작성하여 보관하지 아니한 자

8. 제30조제1항 또는 제2항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리방침을 정하지 아니하거나 이를 공개하지 아니한 자
 9. 제31조제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 보호책임자를 지정하지 아니한 자
 10. 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제4항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자
 11. 제45조제1항에 따른 자료를 정당한 사유 없이 제출하지 아니하거나 거짓으로 제출한 자
 12. 제45조제2항에 따른 출입·조사·열람을 정당한 사유 없이 거부·방해 또는 기피한 자
- ⑤ 제1항부터 제4항까지에 따른 과태료는 대통령령으로 정하는 바에 따라 보호위원회가 부과·징수한다. 이 경우 보호위원회는 위반행위의 정도·동기·결과, 개인정보처리자의 규모 등을 고려하여 과태료를 감경하거나 면제할 수 있다.

[전문개정 2023. 3. 14.]

[시행일: 2024. 3. 15.] 제75조제2항제16호, 제75조제2항제20호, 제75조제2항제21호, 제75조제2항제24호, 제75조제4항제1호, 제75조제4항제9호

제76조(과태료에 관한 규정 적용의 특례) 제75조의 과태료에 관한 규정을 적용할 때 제64조의2에 따라 과징금을 부과한 행위에 대하여는 과태료를 부과할 수 없다. <개정 2023. 3. 14.>

[본조신설 2013. 8. 6.]

부칙 <법률 제19234호, 2023. 3. 14.>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. 다만, 다음 각 호의 개정규정은 각 호의 구분에 따른 날부터 시행한다.

1. 제11조의2, 제31조, 제35조의3, 제37조의2, 제39조의7, 제60조제5호, 제75조제2항제16호·제20호·제21호·제24호 및 같은 조 제4항제1호·제9호의 개정규정: 공포 후 1년이 경과한 날
2. 제35조의2의 개정규정: 공포 후 1년이 경과한 날부터 공포 후 2년이 넘지 아니하는 범위에서 대통령령으로 정하는 날

제2조(개인정보 유출 등의 통지·신고에 관한 적용례) 제34조의 개정규정은 이 법 시행 이후 개인정보가 분실·도난·유출되었음을 알게 된 경우부터 적용한다.

제3조(손해배상청구소송에서 자료의 제출 및 비밀유지 명령 등에 관한 적용례) 제39조의3부터 제39조의6까지의 개정규정은 이 법 시행 이후 손해배상청구의 소를 제기하는 경우부터 적용한다.

제4조(분쟁조정제에 관한 적용례) 제43조제3항, 제45조제2항부터 제4항까지, 제45조의2

및 제47조제3항·제4항의 개정규정은 이 법 시행 이후 분쟁조정 또는 집단분쟁조정이 신청되거나 의뢰되는 경우부터 적용한다.

제5조(적용의 일부 제외에 관한 적용례) 제58조의 개정규정은 이 법 시행 이후 개인정보를 처리하는 경우부터 적용한다.

제6조(결과의 공표에 관한 적용례) 제66조제2항의 개정규정은 이 법 시행 이후 제61조에 따른 개선권고, 제64조에 따른 시정조치 명령, 제64조의2에 따른 과징금의 부과, 제65조에 따른 고발 또는 징계권고 및 제75조에 따른 과태료 부과 처분의 대상이 되는 행위를 한 경우부터 적용한다.

제7조(연차보고에 관한 적용례) 제67조의 개정규정은 이 법 시행 이후 그 다음 연도에 작성하는 보고서부터 적용한다.

제8조(과징금 부과에 관한 경과조치 등) ① 이 법 시행 전에 종료된 위반행위에 대한 과징금의 부과는 제64조의2의 개정규정에도 불구하고 종전의 제28조의6, 제34조의2 및 제39조의15에 따른다.

② 이 법 시행 당시 종료되지 아니한 위반행위에 대한 과징금의 부과는 제64조의2의 개정규정에 따른다.

제9조(개인정보파일의 등록에 관한 경과조치) 이 법 시행 당시 종전의

제58조제1항제1호에 따른 개인정보가 포함된 개인정보파일을 운용하고 있는 공공기관의 장은 이 법 시행일부터 60일 이내에 해당 개인정보파일을 제32조의 개정규정에 따라 보호위원회에 등록을 하여야 한다.

제10조(개인정보 영향평가에 관한 경과조치) 이 법 시행 당시 종전의

제58조제1항제1호에 따른 개인정보가 포함된 개인정보파일(제33조제1항에 따른 영향평가의 대상이 되는 개인정보파일에 한정한다)을 운용하고 있는 공공기관의 장은 이 법 시행일부터 2년 이내에 영향평가를 실시하고 그 결과를 보호위원회에 제출하여야 한다.

제11조(다른 법률의 개정) ① 공직선거법 일부를 다음과 같이 개정한다. 제176조제3항 중 “「개인정보 보호법」 제2조제7호에 따른 영상정보처리기기”를 “「개인정보 보호법」 제2조제7호에 따른 고정형 영상정보처리기기”로 한다.

② 국민체육진흥법 일부를 다음과 같이 개정한다. 제18조의15의 제목 중 “영상정보처리기기”를 “고정형 영상정보처리기기”로 하고, 같은 조 제1항부터 제3항까지 중 “영상정보처리기기”를 각각 “고정형 영상정보처리기기”로 한다.

③ 법률 제18853호 동물보호법 전부개정법률 일부를 다음과 같이 개정한다. 제87조의 제목 중 “영상정보처리기기”를 “고정형 영상정보처리기기”로 하고, 같은 조 제1항·제2항, 같은 조 제3항 각 호 외의 부분, 같은 항 제1호, 같은 조 제4항 각 호 외의 부분 및 같은 조 제5항 중 “영상정보처리기기”를 각각 “고정형 영상정보처리기기”로 한다. 제97조제3항제9호 중 “영상정보처리기기”를 “고정형 영상정보처리기기”로 한다.

④ 보행안전 및 편의증진에 관한 법률 일부를 다음과 같이 개정한다. 제6조제1항제3호 중 “「개인정보 보호법」 제2조제7호에 따른 영상정보처리기기(이하 “영상정보처리기기”라

한다)”를 “「개인정보 보호법」 제2조제7호에 따른 고정형 영상정보처리기기(이하 “고정형 영상정보처리기기”라 한다)”로 한다. 제10조제2항제3호 중 “영상정보처리기기”를 “고정형 영상정보처리기기”로 한다. 제24조의 제목 중 “영상정보처리기기”를 “고정형 영상정보처리기기”로 하고, 같은 조 제1항 본문·단서, 같은 조 제2항부터 제4항까지 중 “영상정보처리기기”를 각각 “고정형 영상정보처리기기”로 한다. 제29조제1항 중 “영상정보처리기기”를 “고정형 영상정보처리기기”로 한다.

- ⑤ 신용정보의 이용 및 보호에 관한 법률 일부를 다음과 같이 개정한다.
제15조제2항제1호 중 “「개인정보 보호법」 제15조제1항제2호부터 제6호까지”를 “「개인정보 보호법」 제15조제1항제2호부터 제7호까지”로 한다.
제20조제4항제1호가목 중 “「개인정보 보호법」 제31조제2항제1호부터 제5호까지의 업무”를 “「개인정보 보호법」 제31조제3항제1호부터 제5호까지에 따른 업무”로 하고, 같은 조 제5항 중 “「개인정보 보호법」 제31조제3항 및 제5항의 규정”을 “「개인정보 보호법」 제31조제4항 및 제6항”으로 한다.
- ⑥ 아동복지법 일부를 다음과 같이 개정한다. 제32조의 제목 중 “영상정보처리기기”를 “고정형 영상정보처리기기”로 하고, 같은 조 제3항 및 제4항 중 “영상정보처리기기”를 각각 “고정형 영상정보처리기기”로 한다.
- ⑦ 응급의료에 관한 법률 일부를 다음과 같이 개정한다. 제47조제2항제3호 중 “「개인정보 보호법」 제2조제7호에 따른 영상정보처리기기”를 “「개인정보 보호법」 제2조제7호에 따른 고정형 영상정보처리기기”로 하고, 같은 조 제4항 중 “영상정보처리기기”를 “고정형 영상정보처리기기”로 한다.
- ⑧ 재난 및 안전관리 기본법 일부를 다음과 같이 개정한다. 제74조의3제1항제2호가목 중 “영상정보처리기기”를 “고정형 영상정보처리기기”로 한다.
- ⑨ 전자장치 부착 등에 관한 법률 일부를 다음과 같이 개정한다. 제16조의3제2항 중 “영상정보처리기기”를 “고정형 영상정보처리기기”로 한다.
- ⑩ 학교체육 진흥법 일부를 다음과 같이 개정한다. 제7조제3항 및 제4항 중 “영상정보처리기기”를 각각 “고정형 영상정보처리기기”로 한다.
- ⑪ 학교폭력예방 및 대책에 관한 법률 일부를 다음과 같이 개정한다. 제20조의7제1항 중 “「개인정보 보호법」 제2조제7호에 따른 영상정보처리기기”를 “「개인정보 보호법」 제2조제7호에 따른 고정형 영상정보처리기기”로 한다.

제1장 총칙

제1조(목적) 이 영은 「개인정보 보호법」에서 위임된 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(공공기관의 범위) 「개인정보 보호법」(이하 “법”이라 한다) 제2조제6호나목에서 “대통령령으로 정하는 기관”이란 다음 각 호의 기관을 말한다.<개정 2020. 7. 14.>

1. 「국가인권위원회법」 제3조에 따른 국가인권위원회
- 1의2. 「고위공직자범죄수사처 설치 및 운영에 관한 법률」 제3조제1항에 따른 고위공직자범죄수사처
2. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
3. 「지방공기업법」에 따른 지방공사와 지방공단
4. 특별법에 따라 설립된 특수법인
5. 「초·중등교육법」, 「고등교육법」, 그 밖의 다른 법률에 따라 설치된 각급 학교

제3조(영상정보처리기기의 범위) ① 법 제2조제7호에서 “대통령령으로 정하는 장치”란 다음 각 호의 장치를 말한다.<개정 2023. 9. 12.>

1. 폐쇄회로 텔레비전: 다음 각 목의 어느 하나에 해당하는 장치
 - 가. 일정한 공간에 설치된 카메라를 통하여 지속적 또는 주기적으로 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송하는 장치
 - 나. 가목에 따라 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치
2. 네트워크 카메라: 일정한 공간에 설치된 기기를 통하여 지속적 또는 주기적으로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치

② 법 제2조제7호의2에서 “대통령령으로 정하는 장치”란 다음 각 호의 장치를 말한다.<신설 2023. 9. 12.>

1. 착용형 장치: 안경 또는 시계 등 사람의 신체 또는 의복에 착용하여 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치
2. 휴대형 장치: 이동통신단말장치 또는 디지털 카메라 등 사람이 휴대하면서 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치
3. 부착·거치형 장치: 차량이나 드론 등 이동 가능한 물체에 부착 또는 거치(據置)하여 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치

제2장 개인정보 보호위원회

제4조 삭제<2020. 8. 4.>

제4조의2(영리업무의 금지) 법 제7조제1항에 따른 개인정보 보호위원회(이하 “보호위원회”라 한다)의 위원은 법 제7조의6제1항에 따라 영리를 목적으로 다음 각 호의 어느 하나에 해당하는 업무에 종사해서는 안 된다.

1. 법 제7조의9제1항에 따라 보호위원회가 심의·의결하는 사항과 관련된 업무
2. 법 제40조제1항에 따른 개인정보 분쟁조정위원회(이하 “분쟁조정위원회”라 한다)가 조정하는 사항과 관련된 업무

[본조신설 2020. 8. 4.]

제5조(전문위원회) ① 보호위원회는 법 제7조의9제1항에 따른 심의·의결 사항에 대하여 사전에 전문적으로 검토하기 위하여 보호위원회에 다음 각 호의 분야별 전문위원회(이하 “전문위원회”라 한다)를 둔다.<개정 2020. 8. 4., 2023. 9. 12.>

1. 개인정보의 국외 이전 분야
 2. 그 밖에 보호위원회가 필요하다고 인정하는 분야
- ② 제1항에 따라 전문위원회를 두는 경우 각 전문위원회는 위원장 1명을 포함한 20명 이내의 위원으로 성별을 고려하여 구성하되, 전문위원회 위원은 다음 각 호의 사람 중에서 보호위원회 위원장이 임명하거나 위촉하고, 전문위원회 위원장은 보호위원회 위원장이 전문위원회 위원 중에서 지명한다.<개정 2016. 7. 22., 2020. 8. 4., 2023. 9. 12.>
1. 보호위원회 위원
 2. 개인정보 보호 관련 업무를 담당하는 중앙행정기관의 관계 공무원
 3. 개인정보 보호에 관한 전문지식과 경험이 풍부한 사람
 4. 개인정보 보호와 관련된 단체 또는 사업자단체에 속하거나 그 단체의 추천을 받은 사람
- ③ 제1항 및 제2항에서 규정한 사항 외에 전문위원회의 구성 및 운영 등에 필요한 사항은 보호위원회의 의결을 거쳐 보호위원회 위원장이 정한다.<신설 2023. 9. 12.>

제5조의2(개인정보 보호 정책협의회) ① 개인정보 보호 정책의 일관성 있는 추진과 개인정보 보호 관련 사안에 대한 관계 중앙행정기관 간 협의를 위하여 보호위원회에 개인정보 보호 정책협의회(이하 “정책협의회”라 한다)를 둘 수 있다.

- ② 정책협의회는 다음 각 호의 사항을 협의한다.
1. 법 제9조에 따른 개인정보 보호 기본계획 및 법 제10조에 따른 시행계획 등 개인정보 보호와 관련된 주요 정책
 2. 개인정보 보호와 관련된 주요 법령의 제·개정
 3. 개인정보 보호와 관련된 주요 정책의 협력 및 의견조정
 4. 개인정보 침해사고 예방 및 대응
 5. 개인정보 보호 기술개발 및 전문인력의 양성

6. 그 밖에 개인정보 보호와 관련하여 관계 중앙행정기관 간 협의가 필요한 사항
- ③ 정책협의회는 관계 중앙행정기관의 고위공무원단에 속하는 공무원 또는 그에 상당하는 공무원으로서 개인정보 보호와 관련된 업무를 담당하는 사람 중 소속 기관의 장이 지명하는 사람으로 구성하되, 정책협의회의 의장(이하 이 조에서 “의장”이라 한다)은 보호위원회의 부위원장으로 한다.
- ④ 정책협의회는 업무를 수행하기 위하여 필요한 경우에는 실무협의회 또는 분야별 협의회를 둘 수 있다.
- ⑤ 실무협의회 및 분야별 협의회의 의장은 보호위원회 소속 공무원 중에서 의장이 임명한다.
- ⑥ 정책협의회, 실무협의회 및 분야별 협의회는 업무를 수행하기 위하여 필요한 경우에는 관계 기관·단체 및 전문가 등에게 출석, 자료 또는 의견의 제출 등 필요한 협조를 요청할 수 있다.
- ⑦ 제1항부터 제6항까지에서 규정한 사항 외에 정책협의회의 운영 등에 필요한 사항은 정책협의회의 의결을 거쳐 의장이 정한다.

[본조신설 2020. 8. 4.]

제5조의3(시·도 개인정보 보호 관계 기관 협의회) ① 개인정보 보호 정책의 효율적인 추진과 자율적인 개인정보 보호 강화를 위하여 특별시, 광역시, 특별자치시, 도, 특별자치도(이하 “시·도”라 한다)에 시·도 개인정보 보호 관계 기관 협의회(이하 “시·도협의회”라 한다)를 둘 수 있다.

② 시·도협의회는 다음 각 호의 사항을 협의한다.

1. 시·도 개인정보 보호 정책
2. 관계 기관·단체 등의 의견 수렴 및 전달
3. 개인정보 보호 우수사례 공유
4. 그 밖에 개인정보 보호와 관련하여 시·도협의회의 협의가 필요한 사항

③ 제1항 및 제2항에서 규정한 사항 외에 시·도협의회의 구성 및 운영 등에 필요한 사항은 시·도의 조례로 정한다.

[본조신설 2020. 8. 4.]

제6조(의사의 공개) 보호위원회의 의사(議事)는 공개한다. 다만, 보호위원회 위원장이 필요하다고 인정하는 경우에는 공개하지 아니할 수 있다.

제7조(공무원 등의 파견) 보호위원회는 그 업무 수행을 위하여 필요하다고 인정하는 경우에는 공공기관에 그 소속 공무원 또는 임직원의 파견을 요청할 수 있다.

제8조 삭제 <2020. 8. 4.>

제9조(출석수당 등) 보호위원회, 전문위원회 또는 정책협의회에 출석한 위원, 법 제7조의9제2항에 따라 보호위원회에 출석한 사람, 전문위원회에 출석한 사람 또는 정책협의회에 출석한 사람에게는 예산의 범위에서 수당·여비, 그 밖에 필요한

경비를 지급할 수 있다. 다만, 공무원이 그 소관 업무와 직접 관련되어 출석하는 경우에는 그렇지 않다.<개정 2020. 8. 4.>

제9조의2(정책·제도·법령 개선 권고의 절차 등) ① 보호위원회는 법 제7조의9제4항에 따라 관계 기관에 정책·제도 및 법령의 개선을 권고하는 경우에는 그 내용과 사유 등을 함께 통보해야 한다.<개정 2020. 8. 4.>

② 보호위원회는 법 제7조의9제5항에 따른 권고내용의 이행여부를 점검하기 위하여 관계 기관에 권고사항의 이행결과에 대한 자료 제출을 요청할 수 있다.<개정 2020. 8. 4.>

[본조신설 2016. 7. 22.]

제9조의3(개인정보 침해요인 평가 절차 등) ① 중앙행정기관의 장은 법 제8조의2제1항에 따라 개인정보 침해요인 평가(이하 “침해요인 평가”라 한다)를 요청하는 경우 다음 각 호의 사항을 포함하는 개인정보 침해요인 평가 요청서(전자문서를 포함한다)를 보호위원회에 제출하여야 한다.

1. 법령(법령안을 포함한다)을 통하여 도입되거나 변경되는 개인정보 처리를 수반하는 정책·제도의 목적과 주요 내용
 2. 개인정보 처리를 수반하는 정책·제도의 도입·변경에 따른 제2항 각 호의 사항에 대한 개인정보 침해요인 자체 분석
 3. 개인정보 처리를 수반하는 정책·제도의 도입·변경에 따른 개인정보 보호 대책
- ② 보호위원회는 제1항에 따른 요청서를 받은 경우에는 다음 각 호의 사항을 고려하여 침해요인 평가를 하고, 그 결과를 해당 중앙행정기관의 장에게 통보하여야 한다.
1. 개인정보 처리의 필요성
 2. 개인정보 주체의 권리보장의 적정성
 3. 개인정보 관리의 안전성
 4. 그 밖에 침해요인 평가에 필요한 사항
- ③ 중앙행정기관의 장은 법 제8조의2제2항에 따른 권고를 받은 경우에는 그 내용을 해당 법령안에 반영하는 등 권고내용을 이행하도록 노력하여야 한다. 다만, 보호위원회의 권고대로 이행하기 곤란한 경우에는 그 사유를 보호위원회에 통보하여야 한다.
- ④ 보호위원회는 침해요인 평가를 하는 경우에는 침해요인 평가에 필요한 자료 등을 해당 중앙행정기관의 장에게 요청할 수 있다.
- ⑤ 보호위원회는 침해요인 평가의 세부기준 및 방법 등 침해요인 평가에 필요한 지침을 수립하여 중앙행정기관의 장에게 통보할 수 있다.
- ⑥ 보호위원회는 침해요인 평가를 실시하기 위하여 필요하면 관계 전문가에게 자문을 등을 할 수 있다.

[본조신설 2016. 7. 22.]

제10조 삭제<2020. 8. 4.>

제3장 기본계획 및 시행계획의 수립절차

- 제11조(기본계획의 수립절차 등)** ① 보호위원회는 3년마다 법 제9조에 따른 개인정보 보호 기본계획(이하 “기본계획”이라 한다)을 그 3년이 시작되는 해의 전년도 6월 30일까지 수립해야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2016. 7. 22., 2020. 8. 4.>
- ② 보호위원회는 제1항에 따라 기본계획을 작성하는 경우에는 관계 중앙행정기관의 장으로부터 개인정보 보호 관련 중장기 계획과 시책 등을 반영한 부문별 계획을 제출받아 기본계획에 반영할 수 있다. 이 경우 보호위원회는 기본계획의 목표, 추진방향 및 부문별 계획의 작성 지침 등에 관하여 관계 중앙행정기관의 장과 협의하여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2016. 7. 22.>
- ③ 보호위원회는 기본계획이 확정되면 지체 없이 관계 중앙행정기관의 장에게 통보하여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2016. 7. 22.>

- 제12조(시행계획의 수립절차 등)** ① 보호위원회는 매년 6월 30일까지 다음 해 시행계획의 작성방법 등에 관한 지침을 마련하여 관계 중앙행정기관의 장에게 통보해야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2016. 7. 22., 2020. 8. 4.>
- ② 관계 중앙행정기관의 장은 제1항의 지침에 따라 기본계획 중 다음 해에 시행할 소관 분야의 시행계획을 작성하여 매년 9월 30일까지 보호위원회에 제출해야 한다.<개정 2020. 8. 4.>
- ③ 보호위원회는 제2항에 따라 제출된 시행계획을 그 해 12월 31일까지 심의·의결해야 한다.<개정 2020. 8. 4.>

- 제13조(자료제출 요구 등의 범위와 방법)** ① 보호위원회는 법 제11조제1항에 따라 개인정보처리자에게 다음 각 호의 사항에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2016. 7. 22., 2023. 9. 12.>
1. 해당 개인정보처리자가 처리하는 개인정보 및 개인정보파일의 관리와 고정형 영상정보처리기기 또는 이동형 영상정보처리기기의 설치·운영에 관한 사항
 2. 법 제31조에 따른 개인정보 보호책임자의 지정 여부에 관한 사항
 3. 개인정보의 안전성 확보를 위한 기술적·관리적·물리적 조치에 관한 사항
 4. 정보주체의 열람, 개인정보의 정정·삭제·처리정지의 요구 및 조치 현황에 관한 사항
 5. 그 밖에 법 및 이 영의 준수에 관한 사항 등 기본계획의 수립·추진을 위하여 필요한 사항
- ② 보호위원회는 제1항에 따라 자료의 제출이나 의견의 진술 등을 요구할 때에는 기본계획을 효율적으로 수립·추진하기 위하여 필요한 최소한의 범위로 한정하여 요구하여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2016. 7. 22.>
- ③ 법 제11조제3항에 따라 중앙행정기관의 장이 소관 분야의 개인정보처리자에게 자료의 제출 등을 요구하는 경우에는 제1항과 제2항을 준용한다. 이 경우 “보호위원회”는 “중앙행정기관의 장”으로, “법 제11조제1항”은 “법

제11조제3항”으로 본다.<개정 2013. 3. 23., 2014. 11. 19., 2016. 7. 22.>

제13조의2(개인정보 보호수준 평가의 대상·기준·방법·절차 등) ① 법

제11조의2제1항에서 “대통령령으로 정하는 기관”이란 다음 각 호의 기관을 말한다.

1. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
2. 「지방공기업법」에 따른 지방공사와 지방공단
3. 그 밖에 제2조제4호 및 제5호에 따른 공공기관 중 공공기관의 개인정보 처리 업무의 특성 등을 고려하여 보호위원회가 고시하는 기준에 해당하는 기관

② 법 제11조의2제1항에 따른 개인정보 보호수준 평가(이하 “개인정보 보호수준 평가”라 한다)의 기준은 다음 각 호와 같다.

1. 개인정보 보호 정책·업무 수행실적 및 개선 정도
2. 개인정보 관리체계의 적정성
3. 정보주체의 권리보장을 위한 조치사항 및 이행 정도
4. 개인정보 침해방지 조치사항 및 안전성 확보 조치 이행 정도
5. 그 밖에 개인정보의 처리 및 안전한 관리를 위해 필요한 조치 사항의 준수 여부

③ 보호위원회는 개인정보 보호수준 평가를 시행하기 전에 평가대상, 평가기준·방법 및 평가지표 등을 포함한 평가계획을 마련하여 개인정보 보호수준 평가 대상 기관(이하 “평가대상기관”이라 한다)의 장에게 통보해야 한다.

④ 보호위원회는 개인정보 보호수준 평가를 효율적으로 실시하기 위해 개인정보 보호에 관한 전문적인 지식과 경험이 풍부한 전문가를 포함하여 평가단을 구성·운영할 수 있다.

⑤ 보호위원회는 법 제11조의2제2항에 따라 다음 각 호의 자료를 제출하게 할 수 있다.

1. 평가대상기관이 개인정보 보호수준을 자체적으로 점검한 경우 그 결과 및 증명자료
2. 제1호의 증명자료의 검증에 필요한 자료
3. 그 밖에 개인정보의 안전한 관리 여부 등 개인정보 보호수준을 평가하기 위해 필요한 자료

⑥ 보호위원회는 제5항에 따라 평가대상기관의 장이 제출한 자료를 기준으로 평가를 진행하거나 평가대상기관을 방문하여 평가할 수 있다.

⑦ 보호위원회는 중앙행정기관의 장 또는 지방자치단체의 장에게 소속 기관 등 소관 분야 평가대상기관의 평가준비 또는 평가결과에 따른 개인정보 보호 조치를 위해 필요한 사항을 지원하도록 요청할 수 있다. 이 경우 요청을 받은 중앙행정기관의 장 또는 지방자치단체의 장은 요청에 따른 지원을 하기 위해 노력해야 한다.

⑧ 제1항부터 제7항까지의 규정에 따른 개인정보 보호수준 평가에 관한 세부 사항은 보호위원회가 정하여 고시한다.

[본조신설 2024. 3. 12.]

제14조(자율규제의 촉진 및 지원) 보호위원회는 법 제13조제2호에 따라

개인정보처리자의 자율적인 개인정보 보호활동을 촉진하기 위하여 예산의 범위에서

개인정보 보호와 관련된 기관 또는 단체에 필요한 지원을 할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

제4장 개인정보의 처리

제14조의2(개인정보의 추가적인 이용·제공의 기준 등) ① 개인정보처리자는 법

제15조제3항 또는 제17조제4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 “개인정보의 추가적인 이용 또는 제공”이라 한다)하려는 경우에는 다음 각 호의 사항을 고려해야 한다.

1. 당초 수집 목적과 관련성이 있는지 여부
2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부
3. 정보주체의 이익을 부당하게 침해하는지 여부
4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

② 개인정보처리자는 개인정보의 추가적인 이용 또는 제공이 지속적으로 발생하는 경우에는 제1항 각 호의 고려사항에 대한 판단 기준을 법 제30조제1항에 따른 개인정보 처리방침에 공개하고, 법 제31조제1항에 따른 개인정보 보호책임자가 해당 기준에 따라 개인정보의 추가적인 이용 또는 제공을 하고 있는지 여부를 점검해야 한다.<개정 2023. 9. 12.>

[본조신설 2020. 8. 4.]

제15조(개인정보의 목적 외 이용 또는 제3자 제공의 관리) 공공기관은 법

제18조제2항에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 다음 각 호의 사항을 보호위원회가 정하여 고시하는 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리해야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

1. 이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭
2. 이용기관 또는 제공받는 기관의 명칭
3. 이용 목적 또는 제공받는 목적
4. 이용 또는 제공의 법적 근거
5. 이용하거나 제공하는 개인정보의 항목
6. 이용 또는 제공의 날짜, 주기 또는 기간
7. 이용하거나 제공하는 형태
8. 법 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용

제15조의2(개인정보 수집 출처 등 통지 대상·방법·절차) ① 법 제20조제2항

본문에서 “대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다. 이 경우 다음 각 호에 규정된

정보주체의 수는 전년도 말 기준 직전 3개월 간 일일평균을 기준으로 산정한다.<개정 2023. 9. 12.>

1. 5만명 이상의 정보주체에 관하여 법 제23조에 따른 민감정보(이하 “민감정보”라 한다) 또는 법 제24조제1항에 따른 고유식별정보(이하 “고유식별정보”라 한다)를 처리하는 자
 2. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자
- ② 제1항 각 호의 어느 하나에 해당하는 개인정보처리자는 법 제20조제1항 각 호의 사항을 다음 각 호의 어느 하나에 해당하는 방법으로 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알려야 한다. 다만, 법 제17조제2항제1호부터 제4호까지의 사항에 대하여 같은 조 제1항제1호에 따라 정보주체의 동의를 받은 범위에서 연 2회 이상 주기적으로 개인정보를 제공받아 처리하는 경우에는 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알리거나 그 동의를 받은 날부터 기산하여 연 1회 이상 정보주체에게 알려야 한다.<개정 2023. 9. 12.>
1. 서면·전자우편·전화·문자전송 등 정보주체가 통지 내용을 쉽게 확인할 수 있는 방법
 2. 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법
- ③ 개인정보처리자는 법 제20조제2항에 따라 개인정보의 수집 출처 등에 관한 사항을 알리는 것과 법 제20조의2제1항에 따른 이용·제공 내역의 통지를 함께 할 수 있다.<신설 2023. 9. 12.>
- ④ 제1항 각 호의 어느 하나에 해당하는 개인정보처리자는 제2항에 따라 알린 경우 다음 각 호의 사항을 법 제21조 또는 제37조제5항에 따라 해당 개인정보를 파기할 때까지 보관·관리하여야 한다.<개정 2023. 9. 12.>
1. 정보주체에게 알린 사실
 2. 알린 시기
 3. 알린 방법

[본조신설 2016. 9. 29.]

[제목개정 2023. 9. 12.]

제15조의3(개인정보 이용·제공 내역의 통지) ① 법 제20조의2제1항 본문에서

“대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다. 이 경우 다음 각 호에 규정된 정보주체의 수는 전년도 말 기준 직전 3개월 간 일일평균을 기준으로 산정한다.

1. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자
 2. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자
- ② 법 제20조의2제1항에 따른 통지의 대상이 되는 정보주체는 다음 각 호의 정보주체를 제외한 정보주체로 한다.
1. 통지에 대한 거부의를 표시한 정보주체
 2. 개인정보처리자가 업무수행을 위해 그에 소속된 임직원의 개인정보를 처리한

- 경우 해당 정보주체
3. 개인정보처리자가 업무수행을 위해 다른 공공기관, 법인, 단체의 임직원 또는 개인의 연락처 등의 개인정보를 처리한 경우 해당 정보주체
 4. 법률에 특별한 규정이 있거나 법령 상 의무를 준수하기 위하여 이용·제공한 개인정보의 정보주체
 5. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 이용·제공한 개인정보의 정보주체
- ③ 법 제20조의2제1항에 따라 정보주체에게 통지해야 하는 정보는 다음 각 호와 같다.
1. 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목
 2. 개인정보를 제공받은 제3자와 그 제공 목적 및 제공한 개인정보의 항목. 다만, 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 제외한다.
- ④ 법 제20조의2제1항에 따른 통지는 다음 각 호의 어느 하나에 해당하는 방법으로 연 1회 이상 해야 한다.
1. 서면·전자우편·전화·문자전송 등 정보주체가 통지 내용을 쉽게 확인할 수 있는 방법
 2. 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법(법 제20조의2제1항에 따른 개인정보의 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 통지하는 경우로 한정한다)

[본조신설 2023. 9. 12.]

제16조(개인정보의 파기방법) ① 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 해야 한다.<개정 2014. 8. 6., 2022. 7. 19.>

1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제. 다만, 기술적 특성으로 영구 삭제가 현저히 곤란한 경우에는 법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치해야 한다.
 2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각
- ② 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 보호위원회가 정하여 고시한다.<신설 2014. 8. 6., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

제17조(동의를 받는 방법) ① 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 다음 각 호의 조건을 모두 충족해야 한다.

<신설 2023. 9. 12.>

1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것
 2. 동의를 받으려는 내용이 구체적이고 명확할 것
 3. 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것
 4. 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것
- ② 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 다음 각 호의 어느

하나에 해당하는 방법으로 정보주체의 동의를 받아야 한다.<개정 2023. 9. 12.>

1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법
2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법
4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법
6. 그 밖에 제1호부터 제5호까지의 규정에 따른 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

③ 법 제22조제2항에서 “대통령령으로 정하는 중요한 내용”이란 다음 각 호의 사항을 말한다.<신설 2017. 10. 17., 2023. 9. 12.>

1. 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
2. 처리하려는 개인정보의 항목 중 다음 각 목의 사항

가. 민감정보

나. 제19조제2호부터 제4호까지의 규정에 따른 여권번호, 운전면허의 면허번호 및 외국인등록번호

3. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
4. 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

④ 개인정보처리자는 정보주체로부터 법 제22조제1항 각 호에 따른 동의를 받으려는 때에는 정보주체가 동의 여부를 선택할 수 있다는 사실을 명확하게 알 수 있도록 표시해야 한다.<개정 2023. 9. 12.>

⑤ 법 제22조제3항 전단에서 “대통령령으로 정하는 방법”이란 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(이하 “서면등의 방법”이라 한다)을 말한다.<개정 2023. 9. 12.>

⑥ 중앙행정기관의 장은 제2항에 따른 동의방법 중 소관 분야의 개인정보처리자별 업무, 업종의 특성 및 정보주체의 수 등을 고려하여 적절한 동의방법에 관한 기준을 법 제12조제2항에 따른 개인정보 보호지침(이하 “개인정보 보호지침”이라 한다)으로 정하여 그 기준에 따라 동의를 받도록 개인정보처리자에게 권장할 수 있다.<개정 2015. 12. 30., 2017. 10. 17., 2023. 9. 12.>

제17조의2(아동의 개인정보 보호) ① 개인정보처리자는 법 제22조의2제1항에 따라 법정대리인이 동의했는지를 확인하는 경우에는 다음 각 호의 어느 하나에 해당하는 방법으로 해야 한다.

1. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고
개인정보처리자가 그 동의 표시를 확인했음을 법정대리인의 휴대전화
문자메시지로 알리는 방법
 2. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고
법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법
 3. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고
법정대리인의 휴대전화 본인인증 등을 통하여 본인 여부를 확인하는 방법
 4. 동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나 우편 또는 팩스를
통하여 전달하고, 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록
하는 방법
 5. 동의 내용이 적힌 전자우편을 발송하고 법정대리인으로부터 동의의 의사표시가
적힌 전자우편을 전송받는 방법
 6. 전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 받거나 인터넷주소 등
동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를
받는 방법
 7. 그 밖에 제1호부터 제6호까지의 규정에 준하는 방법으로서 법정대리인에게 동의
내용을 알리고 동의의 의사표시를 확인하는 방법
- ② 법 제22조의2제2항에서 “대통령령으로 정하는 정보”란 법정대리인의 성명 및
연락처에 관한 정보를 말한다.
- ③ 개인정보처리자는 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운
경우에는 인터넷주소 또는 사업장 전화번호 등 동의 내용을 확인할 수 있는 방법을
법정대리인에게 안내할 수 있다.

[본조신설 2023. 9. 12.]

제18조(민감정보의 범위) 법 제23조제1항 각 호 외의 부분 본문에서 “대통령령으로
정하는 정보”란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만,
공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느
하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.<개정 2016. 9. 29.,
2020. 8. 4.>

1. 유전자검사 등의 결과로 얻어진 유전정보
2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보
3. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼
목적으로 일정한 기술적 수단을 통해 생성한 정보
4. 인종이나 민족에 관한 정보

제19조(고유식별정보의 범위) 법 제24조제1항 각 호 외의 부분에서 “대통령령으로
정하는 정보”란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만,
공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느

하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.<개정 2016. 9. 29., 2017. 6. 27., 2020. 8. 4.>

1. 「주민등록법」 제7조의2제1항에 따른 주민등록번호
2. 「여권법」 제7조제1항제1호에 따른 여권번호
3. 「도로교통법」 제80조에 따른 운전면허의 면허번호
4. 「출입국관리법」 제31조제5항에 따른 외국인등록번호

제20조 삭제<2014. 8. 6.>

제21조(고유식별정보의 안전성 확보 조치) ① 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조를 준용한다. 이 경우 “법 제29조”는 “법 제24조제3항”으로, “개인정보”는 “고유식별정보”로 본다.<개정 2020. 8. 4., 2023. 9. 12.>

② 법 제24조제4항에서 “대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다.<개정 2024. 3. 12.>

1. 1만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 공공기관
2. 보호위원회가 법 위반 이력 및 내용·정도, 고유식별정보 처리의 위험성 등을 고려하여 법 제24조제4항에 따른 조사가 필요하다고 인정하는 공공기관
3. 공공기관 외의 자로서 5만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 자

③ 보호위원회는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에 대하여 법 제24조제4항에 따라 안전성 확보에 필요한 조치를 하였는지를 3년마다 1회 이상 조사해야 한다.<개정 2017. 7. 26., 2020. 8. 4., 2024. 3. 12.>

④ 다음 각 호의 어느 하나에 해당하는 경우로서 고유식별정보의 안전성 확보 조치에 대한 점검이 이루어진 경우에는 제3항에 따른 조사를 실시한 것으로 본다.<신설 2024. 3. 12.>

1. 법 제11조의2에 따라 개인정보 보호수준 평가를 받은 경우
2. 법 제32조의2에 따라 개인정보 보호 인증을 받은 경우
3. 「신용정보의 이용 및 보호에 관한 법률」 제45조의5에 따른 개인신용정보 활용·관리 실태에 대한 상시평가 등 다른 법률에 따라 고유식별정보의 안전성 확보 조치 이행 여부에 대한 정기적인 점검이 이루어지는 경우로서 관계 중앙행정기관의 장의 요청에 따라 해당 점검이 제3항에 따른 조사에 준하는 것으로 보호위원회가 인정하는 경우

⑤ 제3항에 따른 조사는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에게 온라인 또는 서면을 통하여 필요한 자료를 제출하게 하는 방법으로 한다.<개정 2024. 3. 12.>

⑥ 법 제24조제5항에서 “대통령령으로 정하는 전문기관”이란 다음 각 호의 기관을 말한다.<개정 2017. 7. 26., 2020. 8. 4., 2024. 3. 12.>

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른

한국인터넷진흥원(이하 “한국인터넷진흥원”이라 한다)

2. 법 제24조제4항에 따른 조사를 수행할 수 있는 기술적·재정적 능력과 설비를 보유한 것으로 인정되어 보호위원회가 정하여 고시하는 법인, 단체 또는 기관

[전문개정 2016. 9. 29.]

제21조의2(주민등록번호 암호화 적용 대상 등) ① 법 제24조의2제2항에 따라 암호화 조치를 하여야 하는 암호화 적용 대상은 주민등록번호를 전자적인 방법으로 보관하는 개인정보처리자로 한다.

② 제1항의 개인정보처리자에 대한 암호화 적용 시기는 다음 각 호와 같다.

1. 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자:
2017년 1월 1일
2. 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자:
2018년 1월 1일

③ 보호위원회는 기술적·경제적 타당성 등을 고려하여 제1항에 따른 암호화 조치의 세부적인 사항을 정하여 고시할 수 있다.<개정 2017. 7. 26., 2020. 8. 4.>

[본조신설 2015. 12. 30.]

제22조(고정형 영상정보처리기기 설치·운영 제한의 예외) ① 법

제25조제1항제6호에서 “대통령령으로 정하는 경우”란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.<신설 2023. 9. 12.>

1. 출입자 수, 성별, 연령대 등 통계값 또는 통계적 특성값 산출을 위해 촬영된 영상정보를 일시적으로 처리하는 경우
2. 그 밖에 제1호에 준하는 경우로서 보호위원회의 심의·의결을 거친 경우

② 법 제25조제2항 단서에서 “대통령령으로 정하는 시설”이란 다음 각 호의 시설을 말한다.<개정 2017. 5. 29., 2020. 8. 4., 2023. 9. 12.>

1. 「형의 집행 및 수용자의 처우에 관한 법률」 제2조제1호에 따른 교정시설
2. 「정신건강증진 및 정신질환자 복지서비스 지원에 관한 법률」 제3조제5호부터 제7호까지의 규정에 따른 정신의료기관(수용시설을 갖추고 있는 것만 해당한다), 정신요양시설 및 정신재활시설

③ 중앙행정기관의 장은 소관 분야의 개인정보처리자가 법 제25조제2항 단서에 따라 제2항 각 호의 시설에 고정형 영상정보처리기기를 설치·운영하는 경우 정보주체의 사생활 침해를 최소화하기 위하여 필요한 세부 사항을 개인정보 보호지침으로 정하여 그 준수를 권장할 수 있다.<개정 2023. 9. 12.>

[제목개정 2023. 9. 12.]

제23조(고정형 영상정보처리기기 설치 시 의견 수렴) ① 법 제25조제1항 각 호에 따라 고정형 영상정보처리기기를 설치·운영하려는 공공기관의 장은 다음 각 호의 어느 하나에 해당하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.<개정 2023. 9. 12.>

1. 「행정절차법」에 따른 행정예고의 실시 또는 의견청취
 2. 해당 고정형 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회·설문조사 또는 여론조사
- ② 법 제25조제2항 단서에 따른 시설에 고정형 영상정보처리기기를 설치·운영하려는 자는 다음 각 호의 사람으로부터 의견을 수렴하여야 한다.<개정 2023. 9. 12.>
1. 관계 전문가
 2. 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

[제목개정 2023. 9. 12.]

제24조(안내판의 설치 등) ① 법 제25조제1항 각 호에 따라 고정형 영상정보처리기기를 설치·운영하는 자(이하 “고정형영상정보처리기기운영자”라 한다)는 고정형 영상정보처리기기가 설치·운영되고 있음을 정보주체가 쉽게 알아볼 수 있도록 같은 조 제4항 각 호의 사항이 포함된 안내판을 설치하여야 한다. 다만, 건물 안에 여러 개의 고정형 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 고정형 영상정보처리기기 설치지역임을 표시하는 안내판을 설치할 수 있다.<개정 2016. 9. 29., 2023. 9. 12.>

1.~3. 삭제<2016. 9. 29.>

- ② 제1항에도 불구하고 고정형 영상정보처리기기운영자가 설치·운영하는 고정형 영상정보처리기기가 다음 각 호의 어느 하나에 해당하는 경우에는 안내판 설치를 갈음하여 고정형영상정보처리기기운영자의 인터넷 홈페이지에 법 제25조제4항 각 호의 사항을 게재할 수 있다.<개정 2016. 9. 29., 2023. 9. 12.>
1. 공공기관이 원거리 촬영, 과속·신호위반 단속 또는 교통흐름조사 등의 목적으로 고정형 영상정보처리기기를 설치하는 경우로서 개인정보 침해의 우려가 적은 경우
 2. 산불감시용 고정형 영상정보처리기기를 설치하는 경우 등 장소적 특성으로 인하여 안내판을 설치하는 것이 불가능하거나 안내판을 설치하더라도 정보주체가 쉽게 알아볼 수 없는 경우
- ③ 제2항에 따라 인터넷 홈페이지에 법 제25조제4항 각 호의 사항을 게재할 수 없으면 고정형영상정보처리기기운영자는 다음 각 호의 어느 하나 이상의 방법으로 법 제25조제4항 각 호의 사항을 공개하여야 한다.<개정 2016. 9. 29., 2020. 8. 4., 2023. 9. 12.>
1. 고정형영상정보처리기기운영자의 사업장·영업소·사무소·점포 등(이하 “사업장등”이라 한다)의 보기 쉬운 장소에 게시하는 방법
 2. 관보(고정형영상정보처리기기운영자가 공공기관인 경우만 해당한다)나 고정형영상정보처리기기운영자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 또는 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 실는 방법
- ④ 법 제25조제4항 각 호 외의 부분 단서에서 “대통령령으로 정하는 시설”이란

「보안업무규정」 제32조에 따른 국가보안시설을 말한다.<개정 2016. 9. 29.>

제25조(고정형 영상정보처리기기 운영·관리 방침) ① 고정형영상정보처리기기운영자는 법 제25조제7항에 따라 다음 각 호의 사항이 포함된 고정형 영상정보처리기기 운영·관리 방침을 마련해야 한다.<개정 2023. 9. 12.>

1. 고정형 영상정보처리기기의 설치 근거 및 설치 목적
 2. 고정형 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
 3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
 4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
 5. 고정형영상정보처리기기운영자의 영상정보 확인 방법 및 장소
 6. 정보주체의 영상정보 열람 등 요구에 대한 조치
 7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
 8. 그 밖에 고정형 영상정보처리기기의 설치·운영 및 관리에 필요한 사항
- ② 제1항에 따라 마련한 고정형 영상정보처리기기 운영·관리 방침의 공개에 관하여는 제31조제2항 및 제3항을 준용한다. 이 경우 “개인정보처리자”는 “고정형영상정보처리기기운영자”로, “법 제30조제2항”은 “법 제25조제7항”으로, “개인정보 처리방침”은 “고정형 영상정보처리기기 운영·관리 방침”으로 본다.<개정 2023. 9. 12.>

[제목개정 2023. 9. 12.]

제26조(공공기관의 고정형 영상정보처리기기 설치·운영 사무의 위탁) ① 법

제25조제8항 단서에 따라 공공기관이 고정형 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다.<개정 2023. 9. 12.>

1. 위탁하는 사무의 목적 및 범위
 2. 재위탁 제한에 관한 사항
 3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
 4. 영상정보의 관리 현황 점검에 관한 사항
 5. 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항
- ② 제1항에 따라 사무를 위탁한 경우에는 제24조제1항부터 제3항까지의 규정에 따른 안내판 등에 위탁받는 자의 명칭 및 연락처를 포함시켜야 한다.

[제목개정 2023. 9. 12.]

제27조(이동형 영상정보처리기기 운영 제한의 예외) 법 제25조의2제2항 단서에서 “대통령령으로 정하는 경우”란 범죄, 화재, 재난 또는 이에 준하는 상황에서 인명의 구조·구급 등을 위하여 사람 또는 그 사람과 관련된 사물의 영상(개인정보에 해당하는 경우로 한정한다. 이하 같다)의 촬영이 필요한 경우를 말한다.

[본조신설 2023. 9. 12.]

[종전 제27조는 제27조의3으로 이동 <2023. 9. 12.>]

제27조의2(이동형 영상정보처리기기 촬영 사실 표시 등) 법 제25조의2제1항 각 호에
해당하여 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을
촬영하는 경우에는 불빛, 소리, 안내판, 안내서면, 안내방송 또는 그 밖에 이에
준하는 수단이나 방법으로 정보주체가 촬영 사실을 쉽게 알 수 있도록 표시하고
알려야 한다. 다만, 드론을 이용한 항공촬영 등 촬영 방법의 특성으로 인해
정보주체에게 촬영 사실을 알리기 어려운 경우에는 보호위원회가 구축하는 인터넷
사이트에 공지하는 방법으로 알릴 수 있다.

[본조신설 2023. 9. 12.]

제27조의3(영상정보처리기기 설치·운영 지침) 보호위원회는 법 및 이 영에서 규정한
사항 외에 고정형 영상정보처리기기의 설치·운영 및 이동형 영상정보처리기기의
운영에 관한 기준, 설치·운영 사무의 위탁 등에 관하여 법 제12조제1항에 따른 표준
개인정보 보호지침을 정하여 고정형영상정보처리기기운영자와 이동형
영상정보처리기기를 운영하는 자에게 그 준수를 권장할 수 있다.<개정 2013. 3. 23.,
2014. 11. 19., 2017. 7. 26., 2020. 8. 4., 2023. 9. 12.>

[제27조에서 이동 <2023. 9. 12.>]

제28조(개인정보의 처리 업무 위탁 시 조치) ① 법 제26조제1항제3호에서

“대통령령으로 정한 사항”이란 다음 각 호의 사항을 말한다.

1. 위탁업무의 목적 및 범위
 2. 재위탁 제한에 관한 사항
 3. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
 4. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
 5. 법 제26조제2항에 따른 수탁자(이하 “수탁자”라 한다)가 준수하여야 할 의무를
위반한 경우의 손해배상 등 책임에 관한 사항
- ② 법 제26조제2항에서 “대통령령으로 정하는 방법”이란 개인정보 처리 업무를
위탁하는 개인정보처리자(이하 “위탁자”라 한다)가 위탁자의 인터넷 홈페이지에
위탁하는 업무의 내용과 수탁자를 지속적으로 게재하는 방법을 말한다.
- ③ 제2항에 따라 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나
이상의 방법으로 위탁하는 업무의 내용과 수탁자를 공개하여야 한다.<개정 2023. 9.
12.>
1. 위탁자의 사업장등의 보기 쉬운 장소에 게시하는 방법
 2. 관보(위탁자가 공공기관인 경우만 해당한다)나 위탁자의 사업장등이 있는 시·도
이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」
제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문
또는 인터넷신문에 실는 방법
 3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·
홍보지 또는 청구서 등에 지속적으로 실는 방법

4. 재화나 서비스를 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

④ 법 제26조제3항 전단에서 “대통령령으로 정하는 방법”이란 서면등의 방법을 말한다.<개정 2023. 9. 12.>

⑤ 위탁자가 과실 없이 제4항에 따른 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 위탁자의 경우에는 사업장등의 보기 쉬운 장소에 30일 이상 게시하여야 한다.

⑥ 위탁자는 수탁자가 개인정보 처리 업무를 수행하는 경우에 법 또는 이 영에 따라 개인정보처리자가 준수하여야 할 사항과 법 제26조제1항 각 호의 사항을 준수하는지를 같은 조 제4항에 따라 감독하여야 한다.

제29조(영업양도 등에 따른 개인정보 이전의 통지) ① 법 제27조제1항 각 호 외의 부분과 같은 조 제2항 본문에서 “대통령령으로 정하는 방법”이란 서면등의 방법을 말한다.

② 법 제27조제1항에 따라 개인정보를 이전하려는 자(이하 이 항에서 “영업양도자등”이라 한다)가 과실 없이 제1항에 따른 방법으로 법 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지에 게재할 수 없는 정당한 사유가 있는 경우에는 다음 각 호의 어느 하나의 방법으로 법 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 있다.<개정 2020. 8. 4.>

1. 영업양도자등의 사업장등의 보기 쉬운 장소에 30일 이상 게시하는 방법
2. 영업양도자등의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 또는 같은 조 제2호에 따른 일반일간신문·일반주간신문 또는 인터넷신문에 실는 방법

제4장의2 가명정보의 처리에 관한 특례

제29조의2(결합전문기관의 지정 및 지정 취소) ① 법 제28조의3제1항에 따른 전문기관(이하 “결합전문기관”이라 한다)의 지정 기준은 다음 각 호와 같다.

1. 보호위원회가 정하여 고시하는 바에 따라 가명정보의 결합·반출 업무를 담당하는 조직을 구성하고, 개인정보 보호와 관련된 자격이나 경력을 갖춘 사람을 3명 이상 상시 고용할 것
2. 보호위원회가 정하여 고시하는 바에 따라 가명정보를 안전하게 결합하기 위하여 필요한 공간, 시설 및 장비를 구축하고 가명정보의 결합·반출 관련 정책 및 절차 등을 마련할 것
3. 보호위원회가 정하여 고시하는 기준에 따른 재정 능력을 갖출 것
4. 최근 3년 이내에 법 제66조에 따른 공표 내용에 포함된 적이 없을 것

- ② 법인, 단체 또는 기관이 법 제28조의3제1항에 따라 결합전문기관으로 지정을 받으려는 경우에는 보호위원회가 정하여 고시하는 결합전문기관 지정신청서에 다음 각 호의 서류(전자문서를 포함한다. 이하 같다)를 첨부하여 보호위원회 또는 관계 중앙행정기관의 장에게 제출해야 한다.
 1. 정관 또는 규약
 2. 제1항에 따른 지정 기준을 갖추었음을 증명할 수 있는 서류로서 보호위원회가 정하여 고시하는 서류
- ③ 보호위원회 또는 관계 중앙행정기관의 장은 제2항에 따라 지정신청서를 제출한 법인, 단체 또는 기관이 제1항에 따른 지정 기준에 적합한 경우에는 결합전문기관으로 지정할 수 있다.
- ④ 결합전문기관 지정의 유효기간은 지정을 받은 날부터 3년으로 하며, 보호위원회 또는 관계 중앙행정기관의 장은 결합전문기관이 유효기간의 연장을 신청하면 제1항에 따른 지정 기준에 적합한 경우에는 결합전문기관으로 재지정할 수 있다.
- ⑤ 보호위원회 또는 관계 중앙행정기관의 장은 결합전문기관이 다음 각 호의 어느 하나에 해당하는 경우에는 결합전문기관의 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 경우에는 지정을 취소해야 한다.
 1. 거짓이나 부정한 방법으로 결합전문기관으로 지정을 받은 경우
 2. 결합전문기관 스스로 지정 취소를 요청하거나 폐업한 경우
 3. 제1항에 따른 결합전문기관의 지정 기준을 충족하지 못하게 된 경우
 4. 결합 및 반출 등과 관련된 정보의 유출 등 개인정보 침해사고가 발생한 경우
 5. 그 밖에 법 또는 이 영에 따른 의무를 위반한 경우
- ⑥ 보호위원회 또는 관계 중앙행정기관의 장은 제5항에 따라 결합전문기관의 지정을 취소하려는 경우에는 청문을 해야 한다.
- ⑦ 보호위원회 또는 관계 중앙행정기관의 장은 결합전문기관을 지정, 재지정 또는 지정 취소한 경우에는 이를 관보에 공고하거나 보호위원회 또는 해당 관계 중앙행정기관의 홈페이지에 게시해야 한다. 이 경우 관계 중앙행정기관의 장이 결합전문기관을 지정, 재지정, 또는 지정 취소한 경우에는 보호위원회에 통보해야 한다.
- ⑧ 제1항부터 제7항까지에서 규정한 사항 외에 결합전문기관의 지정, 재지정 및 지정 취소 등에 필요한 사항은 보호위원회가 정하여 고시한다.

[본조신설 2020. 8. 4.]

제29조의3(개인정보처리자 간 가명정보의 결합 및 반출 등) ① 결합전문기관에 가명정보의 결합을 신청하려는 개인정보처리자(이하 “결합신청자”라 한다)는 보호위원회가 정하여 고시하는 결합신청서에 다음 각 호의 서류를 첨부하여 결합전문기관에 제출해야 한다.

1. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류
2. 결합 대상 가명정보에 관한 서류
3. 결합 목적을 증명할 수 있는 서류

4. 그 밖에 가명정보의 결합 및 반출에 필요하다고 보호위원회가 정하여 고시하는 서류
- ② 결합전문기관은 법 제28조의3제1항에 따라 가명정보를 결합하는 경우에는 특정 개인을 알아볼 수 없도록 해야 한다. 이 경우 보호위원회는 필요하면 한국인터넷진흥원 또는 보호위원회가 지정하여 고시하는 기관으로 하여금 특정 개인을 알아볼 수 없도록 하는 데에 필요한 업무를 지원하도록 할 수 있다.
- ③ 결합신청자는 법 제28조의3제2항에 따라 결합전문기관이 결합한 정보를 결합전문기관 외부로 반출하려는 경우에는 결합전문기관에 설치된 안전성 확보에 필요한 기술적·관리적·물리적 조치가 된 공간에서 제2항에 따라 결합된 정보를 가명정보 또는 법 제58조의2에 해당하는 정보로 처리한 뒤 결합전문기관의 승인을 받아야 한다.
- ④ 결합전문기관은 다음 각 호의 기준을 충족하는 경우에는 법 제28조의3제2항에 따른 반출을 승인해야 한다. 이 경우 결합전문기관은 결합된 정보의 반출을 승인하기 위하여 반출심사위원회를 구성해야 한다.
1. 결합 목적과 반출 정보가 관련성이 있을 것
 2. 특정 개인을 알아볼 가능성이 없을 것
 3. 반출 정보에 대한 안전조치 계획이 있을 것
- ⑤ 결합전문기관은 결합 및 반출 등에 필요한 비용을 결합신청자에게 청구할 수 있다.
- ⑥ 제1항부터 제5항까지에서 규정한 사항 외에 가명정보의 결합 절차와 방법, 반출 및 승인 등에 필요한 사항은 보호위원회가 정하여 고시한다.

[본조신설 2020. 8. 4.]

제29조의4(결합전문기관의 관리·감독 등) ① 보호위원회 또는 관계 중앙행정기관의 장은 결합전문기관을 지정한 경우에는 해당 결합전문기관의 업무 수행능력 및 기술·시설 유지 여부 등을 관리·감독해야 한다.

- ② 결합전문기관은 제1항에 따른 관리·감독을 위하여 다음 각 호의 서류를 매년 보호위원회 또는 관계 중앙행정기관의 장에게 제출해야 한다.
1. 가명정보의 결합·반출 실적보고서
 2. 결합전문기관의 지정 기준을 유지하고 있음을 증명할 수 있는 서류
 3. 가명정보의 안전성 확보에 필요한 조치를 하고 있음을 증명할 수 있는 서류로서 보호위원회가 정하여 고시하는 서류
- ③ 보호위원회는 다음 각 호의 사항을 관리·감독해야 한다.
1. 결합전문기관의 가명정보의 결합 및 반출 승인 과정에서의 법 위반 여부
 2. 결합신청자의 가명정보 처리 실태
 3. 그 밖에 가명정보의 안전한 처리를 위하여 필요한 사항으로서 보호위원회가 정하여 고시하는 사항

[본조신설 2020. 8. 4.]

제29조의5(가명정보에 대한 안전성 확보 조치) ① 개인정보처리자는 법 제28조의4제1항에

따라 가명정보 및 가명정보를 원래의 상태로 복원하기 위한 추가 정보(이하 이 조에서 “추가정보”라 한다)에 대하여 다음 각 호의 안전성 확보 조치를 해야 한다.<개정 2021. 2. 2., 2023. 9. 12.>

1. 제30조에 따른 안전성 확보 조치
2. 가명정보와 추가정보의 분리 보관. 다만, 추가정보가 불필요한 경우에는 추가정보를 파기해야 한다.
3. 가명정보와 추가정보에 대한 접근 권한의 분리. 다만, 「소상공인기본법」 제2조에 따른 소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등 접근 권한의 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 접근 권한만 부여하고 접근 권한의 보유 현황을 기록으로 보관하는 등 접근 권한을 관리·통제해야 한다.

② 법 제28조의4제3항에서 “대통령령으로 정하는 사항”이란 다음 각 호의 사항을 말한다.<개정 2023. 9. 12.>

1. 가명정보 처리의 목적
2. 가명처리한 개인정보의 항목
3. 가명정보의 이용내역
4. 제3자 제공 시 제공받는 자
5. 가명정보의 처리 기간(법 제28조의4제2항에 따라 가명정보의 처리 기간을 별도로 정한 경우로 한정한다)
6. 그 밖에 가명정보의 처리 내용을 관리하기 위하여 보호위원회가 필요하다고 인정하여 고시하는 사항

[본조신설 2020. 8. 4.]

제29조의6 삭제<2023. 9. 12.>

제4장의3 개인정보의 국외 이전

제29조의7(개인정보의 국외 처리위탁·보관 시 정보주체에게 알리는 방법) 법

제28조의8제1항제3호나목에서 “전자우편 등 대통령령으로 정하는 방법”이란 서면등의 방법을 말한다.

[본조신설 2023. 9. 12.]

제29조의8(개인정보의 국외 이전 인증) ① 보호위원회는 법 제28조의8제1항제4호 각 목 외의 부분에 따른 인증을 고시하려는 경우에는 다음 각 호의 순서에 따른 절차를 모두 거쳐야 한다.

1. 제34조의6에 따른 개인정보 보호 인증 전문기관의 평가
2. 제5조제1항제1호에 따른 개인정보의 국외 이전 분야 전문위원회(이하

“국외이전전문위원회”라 한다)의 평가

3. 정책협의회의 협의

② 보호위원회는 법 제28조의8제1항제4호 각 목 외의 부분에 따른 인증을 고시할 때에는 5년의 범위에서 유효 기간을 정하여 고시할 수 있다.

③ 제1항 및 제2항에서 규정한 사항 외에 인증의 고시 절차 등에 관하여 필요한 사항은 보호위원회가 정하여 고시한다.

[본조신설 2023. 9. 12.]

제29조의9(국가 등에 대한 개인정보 보호 수준 인정) ① 보호위원회는 법

제28조의8제1항제5호에 따라 개인정보가 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 장에서 “이전”이라 한다)되는 국가 또는 국제기구(이하 “이전대상국등”이라 한다)의 개인정보 보호체계, 정보주체 권리보장 범위, 피해구제 절차 등이 법에 따른 개인정보 보호 수준과 실질적으로 동등한 수준을 갖추었다고 인정하려는 경우에는 다음 각 호의 사항을 종합적으로 고려해야 한다.

1. 이전대상국등의 법령, 규정 또는 규칙 등 개인정보 보호체계가 법 제3조에서 정하는 개인정보 보호 원칙에 부합하고, 법 제4조에서 정하는 정보주체의 권리를 충분히 보장하고 있는지 여부
 2. 이전대상국등에 개인정보 보호체계를 보장하고 집행할 책임이 있는 독립적 감독기관이 존재하는지 여부
 3. 이전대상국등의 공공기관(이와 유사한 사무를 수행하는 기관을 포함한다)이 법률에 따라 개인정보를 처리하는지 여부 및 이에 대한 피해구제 절차 등 정보주체에 대한 보호수단이 존재하고 실질적으로 보장되는지 여부
 4. 이전대상국등에 정보주체가 쉽게 접근할 수 있는 피해구제 절차가 존재하는지 여부 및 피해구제 절차가 정보주체를 효과적으로 보호하고 있는지 여부
 5. 이전대상국등의 감독기관이 보호위원회와 정보주체의 권리 보호에 관하여 원활한 상호 협력이 가능한지 여부
 6. 그 밖에 이전대상국등의 개인정보 보호체계, 정보주체의 권리보장 범위, 피해구제 절차 등의 개인정보 보호 수준을 인정하기 위해 필요한 사항으로서 보호위원회가 정하여 고시하는 사항
- ② 보호위원회는 제1항에 따른 인정을 하려는 경우에는 다음 각 호의 절차를 거쳐야 한다.
1. 국외이전전문위원회의 평가
 2. 정책협의회의 협의
- ③ 보호위원회는 제1항에 따른 인정을 할 때에는 정보주체의 권리 보호 등을 위하여 필요한 경우 이전대상국등으로 이전되는 개인정보의 범위, 이전받는 개인정보처리자의 범위, 인정 기간, 국외 이전의 조건 등을 이전대상국등별로 달리 정할 수 있다.
- ④ 보호위원회는 제1항에 따른 인정을 한 경우에는 인정 기간 동안 이전대상국등의

개인정보 보호수준이 법에 따른 수준과 실질적으로 동등한 수준을 유지하고 있는지 점검해야 한다.

- ⑤ 보호위원회는 제1항에 따른 인정을 받은 이전대상국등의 개인정보 보호체계, 정보주체의 권리보장 범위, 피해구제 절차 등의 수준이 변경된 경우에는 해당 이전대상국등의 의견을 듣고 해당 이전대상국등에 대한 인정을 취소하거나 그 내용을 변경할 수 있다.
- ⑥ 보호위원회가 제1항에 따른 인정을 하거나 제5항에 따라 인정을 취소하거나 그 내용을 변경하는 경우에는 그 사실을 관보에 고시하고 보호위원회 인터넷 홈페이지에 게재해야 한다.
- ⑦ 제1항부터 제6항까지에서 규정한 사항 외에 이전대상국등에 대한 인정에 필요한 사항은 보호위원회가 정하여 고시한다.

[본조신설 2023. 9. 12.]

제29조의10(개인정보의 국외 이전 시 보호조치 등) ① 개인정보처리자는 법

제28조의8제1항 각 호 외의 부분 단서에 따라 개인정보를 국외로 이전하는 경우에는 같은 조 제4항에 따라 다음 각 호의 보호조치를 해야 한다.

- 1. 제30조제1항에 따른 개인정보 보호를 위한 안전성 확보 조치
 - 2. 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 조치
 - 3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 조치
- ② 개인정보처리자는 법 제28조의8제1항 각 호 외의 부분 단서에 따라 개인정보를 국외로 이전하는 경우에는 제1항 각 호의 사항에 관하여 이전받는 자와 미리 협의하고 이를 계약내용 등에 반영해야 한다.

[본조신설 2023. 9. 12.]

제29조의11(국외 이전 중지 명령의 기준 등) ① 보호위원회는 법 제28조의9제1항에

따라 개인정보의 국외 이전을 중지할 것을 명하려는 경우에는 다음 각 호의 사항을 종합적으로 고려해야 한다.

- 1. 국외로 이전되었거나 추가적인 국외 이전이 예상되는 개인정보의 유형 및 규모
- 2. 법 제28조의8제1항, 제4항 또는 제5항 위반의 중대성
- 3. 정보주체에게 발생하거나 발생할 우려가 있는 피해가 중대하거나 회복하기 어려운 피해인지 여부
- 4. 국외 이전의 중지를 명하는 것이 중지를 명하지 않는 것보다 명백히 정보주체에게 이익이 되는지 여부
- 5. 법 제64조제1항 각 호에 해당하는 조치를 통해 개인정보의 보호 및 침해 방지가 가능한지 여부
- 6. 개인정보를 이전받는 자나 개인정보가 이전되는 이전대상국등이 정보주체의 피해구제를 위한 실효적인 수단을 갖추고 있는지 여부
- 7. 개인정보를 이전받는 자나 개인정보가 이전되는 이전대상국등에서 중대한

개인정보 침해가 발생하는 등 개인정보를 적정하게 보호하기 어렵다고 인정할 만한 사유가 존재하는지 여부

- ② 보호위원회는 법 제28조의9제1항에 따라 개인정보의 국외 이전을 중지할 것을 명하려는 경우에는 국외이전전문위원회의 평가를 거쳐야 한다.
- ③ 보호위원회는 법 제28조의9제1항에 따라 개인정보의 국외 이전을 중지할 것을 명할 때에는 개인정보처리자에게 중지명령의 내용, 사유, 이의 제기 절차·방법 및 그 밖에 필요한 사항을 문서로 알려야 한다.
- ④ 제1항부터 제3항까지에서 규정한 사항 외에 개인정보의 국외 이전 중지 명령의 기준 등에 관하여 필요한 사항은 보호위원회가 정하여 고시한다.

[본조신설 2023. 9. 12.]

- 제29조의12(국외 이전 중지 명령에 대한 이의 제기)** ① 법 제28조의9제2항에 따라 이의를 제기하려는 자는 같은 조 제1항에 따른 국외 이전 중지 명령을 받은 날부터 7일 이내에 보호위원회가 정하는 이의신청서에 이의신청 사유를 증명할 수 있는 서류를 첨부하여 보호위원회에 제출해야 한다.
- ② 보호위원회는 제1항에 따라 이의신청서를 제출받은 날부터 30일 이내에 그 처리결과를 해당 개인정보처리자에게 문서로 알려야 한다.
 - ③ 제1항 및 제2항에서 규정한 사항 외에 이의 제기의 절차 등에 관하여 필요한 사항은 보호위원회가 정하여 고시한다.

[본조신설 2023. 9. 12.]

제5장 개인정보의 안전한 관리

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.<개정 2023. 9. 12.>

- 1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부 관리계획의 수립·시행 및 점검
 - 가. 법 제28조제1항에 따른 개인정보취급자(이하 “개인정보취급자”라 한다)에 대한 관리·감독 및 교육에 관한 사항
 - 나. 법 제31조에 따른 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항
 - 다. 제2호부터 제8호까지의 규정에 따른 조치를 이행하기 위하여 필요한 세부 사항
- 2. 개인정보에 대한 접근 권한을 제한하기 위한 다음 각 목의 조치
 - 가. 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템(이하 “개인정보처리시스템”이라 한다)에 대한 접근 권한의 부여·변경·말소 등에 관한 기준의 수립·시행
 - 나. 정당한 권한을 가진 자에 의한 접근인지를 확인하기 위해 필요한 인증수단

적용 기준의 설정 및 운영

다. 그 밖에 개인정보에 대한 접근 권한을 제한하기 위하여 필요한 조치

3. 개인정보에 대한 접근을 통제하기 위한 다음 각 목의 조치

가. 개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치

나. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등으로서

보호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷망의 차단. 다만, 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 이용자 수가 일일평균 100만명 이상인 개인정보처리자만 해당한다.

다. 그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치

4. 개인정보를 안전하게 저장·전송하는데 필요한 다음 각 목의 조치

가. 비밀번호의 일방향 암호화 저장 등 인증정보의 암호화 저장 또는 이에 상응하는 조치

나. 주민등록번호 등 보호위원회가 정하여 고시하는 정보의 암호화 저장 또는 이에 상응하는 조치

다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 통하여 정보주체의 개인정보 또는 인증정보를 송신·수신하는 경우 해당 정보의 암호화 또는 이에 상응하는 조치

라. 그 밖에 암호화 또는 이에 상응하는 기술을 이용한 보안조치

5. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 다음 각 목의 조치

가. 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독

나. 개인정보처리시스템에 대한 접속기록의 안전한 보관

다. 그 밖에 접속기록 보관 및 위조·변조 방지를 위하여 필요한 조치

6. 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대해 컴퓨터바이러스, 스파이웨어, 랜섬웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하는 등의 기능이 포함된 프로그램의 설치·운영과 주기적 갱신·점검 조치

7. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

8. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치

② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

제30조의2(공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등) ① 개인정보의 처리 규모, 접근 권한을 부여받은 개인정보취급자의 수 등 보호위원회가 고시하는 기준에 해당하는 개인정보처리시스템(이하 “공공시스템”이라 한다)을 운영하는 공공기관(이하 “공공시스템운영기관”이라 한다)은 법 제29조에 따라 이 영 제30조의 안전성 확보 조치 외에 다음 각 호의 조치를 추가로 해야 한다.<개정 2024. 3. 12.>

1. 제30조제1항제1호에 따른 내부 관리계획에 공공시스템별로 작성한 안전성 확보 조치를 포함할 것
 2. 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 이 조에서 “공공시스템이용기관”이라 한다)이 정당한 권한을 가진 개인정보취급자에게 접근 권한을 부여·변경·말소 등을 할 수 있도록 하는 등 접근 권한의 안전한 관리를 위해 필요한 조치
 3. 개인정보에 대한 불법적인 접근 및 침해사고 방지를 위한 공공시스템 접속기록의 저장·분석·점검·관리 등의 조치
- ② 공공시스템운영기관 및 공공시스템이용기관은 정당한 권한 없이 또는 허용된 권한을 초과하여 개인정보에 접근한 사실이 확인되는 경우에는 지체 없이 정보주체에게 해당 사실과 피해 예방 등을 위해 필요한 사항을 통지해야 한다. 이 경우 다음 각 호의 어느 하나에 해당하는 경우에는 통지를 한 것으로 본다.
1. 법 제34조제1항에 따라 정보주체에게 개인정보의 분실·도난·유출에 대하여 통지한 경우
 2. 다른 법령에 따라 정보주체에게 개인정보에 접근한 사실과 피해 예방 등을 위해 필요한 사항을 통지한 경우
- ③ 공공시스템운영기관(공공시스템을 개발하여 배포하는 공공기관이 따로 있는 경우에는 그 공공기관을 포함한다. 이하 이 조에서 같다)은 해당 공공시스템의 규모와 특성, 해당 공공시스템이용기관의 수 등을 고려하여 개인정보의 안전한 관리에 관련된 업무를 전담하는 부서를 지정하여 운영하거나 전담인력을 배치해야 한다.
- ④ 공공시스템운영기관은 공공시스템별로 해당 공공시스템을 총괄하여 관리하는 부서의 장을 관리책임자로 지정해야 한다. 다만, 해당 공공시스템을 총괄하여 관리하는 부서가 없을 때에는 업무 관련성 및 수행능력 등을 고려하여 해당 공공시스템운영기관의 관련 부서의 장 중에서 관리책임자를 지정해야 한다.
- ⑤ 공공시스템운영기관은 공공시스템의 안전성 확보 조치 이행상황 점검 및 개선에 관한 사항을 협의하기 위하여 다음 각 호의 기관으로 구성되는 공공시스템운영협의회를 공공시스템별로 설치·운영해야 한다. 다만, 하나의 공공기관이 2개 이상의 공공시스템을 운영하는 경우에는 공공시스템운영협의회를 통합하여 설치·운영할 수 있다.
1. 공공시스템운영기관
 2. 공공시스템의 운영을 위탁하는 경우 해당 수탁자

3. 공공시스템운영기관이 필요하다고 인정하는 공공시스템이용기관
- ⑥ 보호위원회는 공공시스템운영기관이 개인정보의 안전성 확보 조치를 이행하는데 필요한 지원을 할 수 있다.
- ⑦ 제1항부터 제6항까지에서 규정한 사항 외에 공공시스템운영기관 등의 개인정보의 안전성 확보 조치에 필요한 사항은 보호위원회가 정하여 고시한다.

[본조신설 2023. 9. 12.]

제31조(개인정보 처리방침의 내용 및 공개방법 등) ① 법 제30조제1항제8호에서 “대통령령으로 정한 사항”이란 다음 각 호의 사항을 말한다.<개정 2016. 9. 29., 2020. 8. 4., 2023. 9. 12., 2024. 3. 12.>

1. 처리하는 개인정보의 항목
 2. 법 제28조의8제1항 각 호에 따라 개인정보를 국외로 이전하는 경우 국외 이전의 근거와 같은 조 제2항 각 호의 사항
 3. 제30조에 따른 개인정보의 안전성 확보 조치에 관한 사항
 4. 국외에서 국내 정보주체의 개인정보를 직접 수집하여 처리하는 경우 개인정보를 처리하는 국가명
- ② 개인정보처리자는 법 제30조제2항에 따라 수립하거나 변경한 개인정보 처리방침을 개인정보처리자의 인터넷 홈페이지에 지속적으로 게재하여야 한다.
- ③ 제2항에 따라 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 수립하거나 변경한 개인정보 처리방침을 공개하여야 한다.<개정 2023. 9. 12.>
1. 개인정보처리자의 사업장등의 보기 쉬운 장소에 게시하는 방법
 2. 관보(개인정보처리자가 공공기관인 경우만 해당한다)나 개인정보처리자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 실는 방법
 3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 실는 방법
 4. 재화나 서비스를 제공하기 위하여 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

제31조의2(개인정보 처리방침의 평가 대상 및 절차) ① 보호위원회는 법

제30조의2제1항에 따라 개인정보 처리방침을 평가하는 경우 다음 각 호의 사항을 종합적으로 고려하여 평가 대상을 선정한다.<개정 2024. 3. 12.>

1. 개인정보처리자의 유형 및 매출액(매출액을 산정하지 않는 경우에는 「법인세법」 제4조제3항제1호에 따른 수익사업에서 생기는 소득을 말하며, 이하 제32조 및 제48조의7에서 “매출액등”이라 한다) 규모
2. 민감정보 및 고유식별정보 등 처리하는 개인정보의 유형 및 규모

3. 개인정보 처리의 법적 근거 및 방식
4. 법 위반행위 발생 여부
5. 아동·청소년 등 정보주체의 특성

- ② 보호위원회는 제1항에 따라 평가 대상 개인정보 처리방침을 선정한 경우에는 평가 개시 10일 전까지 해당 개인정보처리자에게 평가 내용·일정 및 절차 등이 포함된 평가계획을 통보해야 한다.
- ③ 보호위원회는 법 제30조의2에 따른 개인정보 처리방침의 평가에 필요한 경우에는 해당 개인정보처리자에게 의견을 제출하도록 요청할 수 있다.
- ④ 보호위원회는 법 제30조의2에 따라 개인정보 처리방침을 평가한 후 그 결과를 지체 없이 해당 개인정보처리자에게 통보해야 한다.
- ⑤ 제1항부터 제4항까지에서 규정한 사항 외에 개인정보 처리방침 평가를 위한 세부적인 대상 선정 기준과 절차는 보호위원회가 정하여 고시한다.

[본조신설 2023. 9. 12.]

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① 법 제31조제1항 단서에서 “종업원 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 「소상공인기본법」 제2조제1항에 따른 소상공인에 해당하는 개인정보처리자를 말한다.

<신설 2024. 3. 12.>

- ② 법 제31조제3항제7호에서 “대통령령으로 정한 업무”란 다음 각 호와 같다.<개정 2024. 3. 12.>

1. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
2. 개인정보 처리와 관련된 인적·물적 자원 및 정보의 관리
3. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

- ③ 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다.<개정 2016. 7. 22., 2024. 3. 12.>

1. 공공기관: 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등
 - 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관: 고위공무원단에 속하는 공무원(이하 “고위공무원”이라 한다) 또는 그에 상당하는 공무원
 - 나. 가목 외에 정무직공무원을 장(長)으로 하는 국가기관: 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상당하는 공무원
 - 다. 가목 및 나목 외에 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관: 4급 이상 공무원 또는 그에 상당하는 공무원
 - 라. 가목부터 다목까지의 규정에 따른 국가기관 외의 국가기관(소속 기관을 포함한다): 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장
 - 마. 시·도 및 시·도 교육청: 3급 이상 공무원 또는 그에 상당하는 공무원
 - 바. 시·군 및 자치구: 4급 이상 공무원 또는 그에 상당하는 공무원
 - 사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람. 다만,

제4항제2호에 해당하는 경우에는 교직원을 말한다.

아. 가목부터 사목까지의 규정에 따른 기관 외의 공공기관: 개인정보 처리 관련 업무를 담당하는 부서의 장. 다만, 개인정보 처리 관련 업무를 담당하는 부서의 장이 2명 이상인 경우에는 해당 공공기관의 장이 지명하는 부서의 장이 된다.

2. 공공기관 외의 개인정보처리자: 다음 각 목의 어느 하나에 해당하는 사람

가. 사업주 또는 대표자

나. 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)

④ 다음 각 호의 어느 하나에 해당하는 개인정보처리자(공공기관의 경우에는 제2조제2호부터 제5호까지에 해당하는 경우로 한정한다)는 제3항 각 호의 구분에 따른 사람 중 별표 1에서 정하는 요건을 갖춘 사람을 개인정보 보호책임자로 지정해야 한다.<개정 2024. 3. 12.>

1. 연간 매출액등이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자 (제2조제5호에 따른 각급 학교 및 「의료법」 제3조에 따른 의료기관은 제외한다)

가. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자

나. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자

2. 직전 연도 12월 31일 기준으로 재학생 수(대학원 재학생 수를 포함한다)가 2만명 이상인 「고등교육법」 제2조에 따른 학교

3. 「의료법」 제3조의4에 따른 상급종합병원

4. 공공시스템운영기관

⑤ 보호위원회는 개인정보 보호책임자가 법 제31조제3항의 업무를 원활히 수행할 수 있도록 개인정보 보호책임자에 대한 교육과정을 개설·운영하는 등 지원을 할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4., 2024. 3. 12.>

⑥ 개인정보처리자(법 제31조제2항에 따라 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우는 제외한다)는 법 제31조제6항에 따른 개인정보 보호책임자의 독립성 보장을 위해 다음 각 호의 사항을 준수해야 한다.<신설 2024. 3. 12.>

1. 개인정보 처리와 관련된 정보에 대한 개인정보 보호책임자의 접근 보장

2. 개인정보 보호책임자가 개인정보 보호 계획의 수립·시행 및 그 결과에 관하여 정기적으로 대표자 또는 이사회에 직접 보고할 수 있는 체계의 구축

3. 개인정보 보호책임자의 업무 수행에 적합한 조직체계의 마련 및 인적·물적 자원의 제공

제32조의2(개인정보 보호책임자 협의회의 사업 범위 등) ① 법 제31조제7항에서

“대통령령으로 정하는 공동의 사업”이란 다음 각 호의 사업을 말한다.

1. 개인정보처리자의 개인정보 보호 강화를 위한 정책의 조사, 연구 및 수립 지원

2. 개인정보 침해사고 분석 및 대책 연구

3. 개인정보 보호책임자 지정·운영, 업무 수행 현황 등 실태 파악 및 제도 개선을 위한 연구

4. 개인정보 보호책임자 교육 등 개인정보 보호책임자의 개인정보 보호 역량 및 전문성 향상

5. 개인정보 보호책임자의 업무와 관련된 국내외 주요 동향의 조사, 분석 및 공유
 6. 그 밖에 개인정보처리시스템 등의 안전한 관리를 위해 필요한 사업
- ② 보호위원회는 법 제31조제8항에 따라 예산의 범위에서 개인정보 보호책임자 협의회의 운영과 사업에 필요한 행정적·기술적 지원을 할 수 있다.

[본조신설 2024. 3. 12.]

[중전 제32조의2는 제32조의3으로 이동 <2024. 3. 12.>]

- 제32조의3(국내대리인 지정 대상자의 범위)** ① 법 제31조의2제1항 각 호 외의 부분 전단에서 “대통령령으로 정하는 자”란 다음 각 호의 어느 하나에 해당하는 자를 말한다.
1. 전년도(법인인 경우에는 전 사업연도를 말한다) 전체 매출액이 1조원 이상인 자
 2. 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 국내 정보주체의 수가 일일평균 100만명 이상인 자
 3. 법 제63조제1항에 따라 관계 물품·서류 등 자료의 제출을 요구받은 자로서 국내대리인을 지정할 필요가 있다고 보호위원회가 심의·의결한 자
- ② 제1항제1호에 따른 전체 매출액은 전년도 평균환율을 적용하여 원화로 환산한 금액을 기준으로 한다.

[본조신설 2023. 9. 12.]

[제32조의2에서 이동 <2024. 3. 12.>]

- 제33조(개인정보파일의 등록사항 등)** ① 법 제32조제1항제7호에서 “대통령령으로 정하는 사항”이란 다음 각 호의 사항을 말한다.<개정 2023. 9. 12.>
1. 개인정보파일을 운용하는 공공기관의 명칭
 2. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
 3. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서
 4. 제41조에 따른 개인정보의 열람 요구를 접수·처리하는 부서
 5. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유
- ② 법 제32조제2항제4호에서 “대통령령으로 정하는 개인정보파일”이란 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.<신설 2023. 9. 12.>
1. 회의 참석 수당 지급, 자료·물품의 송부, 금전의 정산 등 단순 업무 수행을 위해 운영되는 개인정보파일로서 지속적 관리 필요성이 낮은 개인정보파일
 2. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
 3. 그 밖에 일회적 업무 처리만을 위해 수집된 개인정보파일로서 저장되거나 기록되지 않는 개인정보파일

[제목개정 2023. 9. 12.]

- 제34조(개인정보파일의 등록 및 공개 등)** ① 개인정보파일(법 제32조제2항 및 이 영 제33조제2항에 따른 개인정보파일은 제외한다. 이하 이 조에서 같다)을 운용하는

공공기관의 장은 그 운용을 시작한 날부터 60일 이내에 보호위원회가 정하여 고시하는 바에 따라 보호위원회에 법 제32조제1항 및 이 영 제33조제1항에 따른 등록사항(이하 “등록사항”이라 한다)의 등록을 신청하여야 한다. 등록 후 등록된 사항이 변경된 경우에도 또한 같다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4., 2023. 9. 12.>

② 보호위원회는 법 제32조제4항에 따라 개인정보파일의 등록 현황을 공개하는 경우 이를 보호위원회가 구축하는 인터넷 사이트에 게재해야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4., 2023. 9. 12.>

③ 보호위원회는 제1항에 따른 개인정보파일의 등록사항을 등록하거나 변경하는 업무를 전자적으로 처리할 수 있도록 시스템을 구축·운영할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

제34조의2(개인정보 보호 인증의 기준·방법·절차 등) ① 보호위원회는 제30조제1항 각 호의 사항을 고려하여 개인정보 보호의 관리적·기술적·물리적 보호대책의 수립 등을 포함한 법 제32조의2제1항에 따른 인증의 기준을 정하여 고시한다.<개정 2017. 7. 26., 2020. 8. 4., 2023. 9. 12.>

② 법 제32조의2제1항 따라 개인정보 보호의 인증을 받으려는 자(이하 이 조 및 제34조의3에서 “신청인”이라 한다)는 다음 각 호의 사항이 포함된 개인정보 보호 인증신청서(전자문서로 된 신청서를 포함한다)를 제34조의6에 따른 개인정보 보호 인증 전문기관(이하 “인증기관”이라 한다)에 제출하여야 한다.<개정 2024. 3. 12.>

1. 인증 대상 개인정보 처리시스템의 목록
2. 개인정보 관리체계를 수립·운영하는 방법과 절차
3. 개인정보 관리체계 및 보호대책 구현과 관련되는 문서 목록

③ 인증기관은 제2항에 따른 인증신청서를 받은 경우에는 신청인과 인증의 범위 및 일정 등에 관하여 협의하여야 한다.

④ 법 제32조의2제1항에 따른 개인정보 보호 인증심사는 제34조의8에 따른 개인정보 보호 인증심사원이 서면심사 또는 현장심사의 방법으로 실시한다.

⑤ 인증기관은 제4항에 따른 인증심사의 결과를 심의하기 위하여 정보보호에 관한 학식과 경험이 풍부한 사람을 위원으로 하는 인증위원회를 설치·운영하여야 한다.

⑥ 제1항부터 제5항까지에서 규정한 사항 외에 인증신청, 인증심사, 인증위원회의 설치·운영 및 인증서의 발급 등 개인정보 보호 인증에 필요한 세부사항은 보호위원회가 정하여 고시한다.<개정 2017. 7. 26., 2020. 8. 4.>

[본조신설 2016. 7. 22.]

제34조의3(개인정보 보호 인증의 수수료) ① 신청인은 인증기관에 개인정보 보호 인증 심사에 소요되는 수수료를 납부하여야 한다.

② 보호위원회는 개인정보 보호 인증 심사에 투입되는 인증 심사원의 수 및 인증심사에 필요한 일수 등을 고려하여 제1항에 따른 수수료 산정을 위한 구체적인

기준을 정하여 고시한다.<개정 2017. 7. 26., 2020. 8. 4.>

[본조신설 2016. 7. 22.]

제34조의4(인증취소) ① 인증기관은 법 제32조의2제3항에 따라 개인정보 보호 인증을 취소하려는 경우에는 제34조의2제5항에 따른 인증위원회의 심의·의결을 거쳐야 한다.

② 보호위원회 또는 인증기관은 법 제32조의2제3항에 따라 인증을 취소한 경우에는 그 사실을 당사자에게 통보하고, 관보 또는 인증기관의 홈페이지에 공고하거나 게시해야 한다.<개정 2017. 7. 26., 2020. 8. 4.>

[본조신설 2016. 7. 22.]

제34조의5(인증의 사후관리) ① 법 제32조의2제4항에 따른 사후관리 심사는 서면심사 또는 현장심사의 방법으로 실시한다.

② 인증기관은 제1항에 따른 사후관리를 실시한 결과 법 제32조의2제3항 각 호의 사유를 발견한 경우에는 제34조의2제5항에 따른 인증위원회의 심의를 거쳐 그 결과를 보호위원회에 제출해야 한다.<개정 2017. 7. 26., 2020. 8. 4.>

[본조신설 2016. 7. 22.]

제34조의6(개인정보 보호 인증 전문기관) ① 법 제32조의2제5항에서 “대통령령으로 정하는 전문기관”이란 다음 각 호의 기관을 말한다.<개정 2016. 9. 29., 2017. 7. 26., 2020. 8. 4.>

1. 한국인터넷진흥원

2. 다음 각 목의 요건을 모두 충족하는 법인, 단체 또는 기관 중에서 보호위원회가 지정·고시하는 법인, 단체 또는 기관

가. 제34조의8에 따른 개인정보 보호 인증심사원 5명 이상을 보유할 것

나. 보호위원회가 실시하는 업무수행 요건·능력 심사에서 적합하다고 인정받을 것

② 제1항제2호에 해당하는 법인, 단체 또는 기관의 지정과 그 지정의 취소에 필요한 세부기준 등은 보호위원회가 정하여 고시한다.<개정 2017. 7. 26., 2020. 8. 4.>

[본조신설 2016. 7. 22.]

제34조의7(인증의 표시 및 홍보) 법 제32조의2제6항에 따라 인증을 받은 자가 인증 받은 내용을 표시하거나 홍보하려는 경우에는 보호위원회가 정하여 고시하는 개인정보 보호 인증표시를 사용할 수 있다. 이 경우 인증의 범위와 유효기간을 함께 표시해야 한다.<개정 2017. 7. 26., 2020. 8. 4.>

[본조신설 2016. 7. 22.]

제34조의8(개인정보 보호 인증심사원의 자격 및 자격 취소 요건) ① 인증기관은 법 제32조의2제7항에 따라 개인정보 보호에 관한 전문지식을 갖춘 사람으로서 인증심사에 필요한 전문 교육과정을 이수하고 시험에 합격한 사람에게 개인정보 보호 인증심사원(이하 “인증심사원”이라 한다)의 자격을 부여한다.

② 인증기관은 법 제32조의2제7항에 따라 인증심사원이 다음 각 호의 어느 하나에

해당하는 경우 그 자격을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 자격을 취소하여야 한다.

1. 거짓이나 부정한 방법으로 인증심사원 자격을 취득한 경우
2. 개인정보 보호 인증 심사와 관련하여 금전, 금품, 이익 등을 부당하게 수수한 경우
3. 개인정보 보호 인증 심사 과정에서 취득한 정보를 누설하거나 정당한 사유 없이 업무상 목적 외의 용도로 사용한 경우

③ 제1항 및 제2항에 따른 전문 교육과정의 이수, 인증심사원 자격의 부여 및 취소 등에 관한 세부 사항은 보호위원회가 정하여 고시한다.<개정 2017. 7. 26., 2020. 8. 4.>

[본조신설 2016. 7. 22.]

제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 “대통령령으로 정하는 기준에 해당하는 개인정보파일”이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.<개정 2016. 9. 29.>

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 “영향평가”라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

제36조(평가기관의 지정 및 지정취소) ① 보호위원회는 법 제33조제2항에 따라 다음 각 호의 요건을 모두 갖춘 법인을 개인정보 영향평가기관(이하 “평가기관”이라 한다)으로 지정할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2015. 12. 22., 2017. 7. 26., 2020. 8. 4., 2023. 9. 12.>

1. 최근 5년간 다음 각 목의 어느 하나에 해당하는 업무 수행의 대가로 받은 금액의 합계액이 2억원 이상인 법인
 - 가. 영향평가 업무 또는 이와 유사한 업무
 - 나. 「전자정부법」 제2조제13호에 따른 정보시스템(정보보호시스템을 포함한다)의 구축 업무 중 정보보호컨설팅 업무(전자적 침해행위에 대비하기 위한 정보시스템의 분석·평가와 이에 기초한 정보 보호 대책의 제시 업무를 말한다. 이하 같다)
 - 다. 「전자정부법」 제2조제14호에 따른 정보시스템 감리 업무 중 정보보호컨설팅 업무
 - 라. 「정보보호산업의 진흥에 관한 법률」 제2조제1항제2호에 따른 정보보호산업에 해당하는 업무 중 정보보호컨설팅 업무
 - 마. 「정보보호산업의 진흥에 관한 법률」 제23조제1항제1호 및 제2호에 따른 업무

2. 개인정보 영향평가와 관련된 분야에서의 업무 경력 등 보호위원회가 정하여 고시하는 자격을 갖춘 전문인력을 10명 이상 상시 고용하고 있는 법인
3. 다음 각 목의 사무실 및 설비를 갖춘 법인
 - 가. 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실
 - 나. 기록 및 자료의 안전한 관리를 위한 설비
- ② 평가기관으로 지정받으려는 자는 보호위원회가 정하여 고시하는 평가기관 지정신청서에 다음 각 호의 서류를 첨부하여 보호위원회에 제출해야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2017. 10. 17., 2020. 8. 4.>
 1. 정관
 2. 대표자의 성명
 3. 제1항제2호에 따른 전문인력의 자격을 증명할 수 있는 서류
 4. 그 밖에 보호위원회가 정하여 고시하는 서류
- ③ 제2항에 따라 평가기관 지정신청서를 제출받은 보호위원회는 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 다음 각 호의 서류를 확인해야 한다. 다만, 신청인이 제2호의 확인에 동의하지 않는 경우에는 신청인에게 그 서류를 첨부하게 해야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>
 1. 법인 등기사항증명서
 2. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(외국인인 경우만 해당한다)
- ④ 보호위원회는 제1항에 따라 평가기관을 지정한 경우에는 지체 없이 평가기관 지정서를 발급하고, 다음 각 호의 사항을 관보에 고시해야 한다. 고시된 사항이 변경된 경우에도 또한 같다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>
 1. 평가기관의 명칭·주소 및 전화번호와 대표자의 성명
 2. 지정 시 조건을 붙이는 경우 그 조건의 내용
- ⑤ 법 제33조제7항제5호에서 “대통령령으로 정하는 사유에 해당하는 경우”란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.<개정 2023. 9. 12.>
 1. 제6항에 따른 신고의무를 이행하지 않은 경우
 2. 평가기관으로 지정된 날부터 2년 이상 계속하여 정당한 사유 없이 영향평가 실적이 없는 경우
 3. 제38조제2항 각 호 외의 부분에 따른 영향평가서 등 영향평가 업무 수행 과정에서 알게 된 정보를 누설한 경우
 4. 그 밖에 법 또는 이 영에 따른 의무를 위반한 경우
- ⑥ 제1항에 따라 지정된 평가기관은 지정된 후 다음 각 호의 어느 하나에 해당하는 사유가 발생한 경우에는 보호위원회가 정하여 고시하는 바에 따라 그 사유가 발생한 날부터 14일 이내에 보호위원회에 신고해야 한다. 다만, 제3호에 해당하는 경우에는 그 사유가 발생한 날부터 60일 이내에 신고해야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2017. 10. 17., 2020. 8. 4.>
 1. 제1항 각 호의 어느 하나에 해당하는 사항이 변경된 경우

2. 제4항제1호에 해당하는 사항이 변경된 경우
3. 평가기관을 양도·양수하거나 합병하는 등의 사유가 발생한 경우

⑦ 삭제<2023. 9. 12.>

[제37조에서 이동, 종전 제36조는 제37조로 이동 <2023. 9. 12.>]

제37조(영향평가 시 고려사항) 법 제33조제3항제4호에서 “대통령령으로 정한 사항”이란 다음 각 호의 사항을 말한다.<개정 2023. 9. 12.>

1. 민감정보 또는 고유식별정보의 처리 여부
2. 개인정보 보유기간

[제36조에서 이동, 종전 제37조는 제36조로 이동 <2023. 9. 12.>]

제38조(영향평가의 평가기준 등) ① 법 제33조제9항에 따른 영향평가의 기준(이하 “평가기준”이라 한다)은 다음 각 호와 같다.<개정 2016. 7. 22., 2023. 9. 12.>

1. 해당 개인정보파일에 포함되는 개인정보의 종류·성질, 정보주체의 수 및 그에 따른 개인정보 침해의 가능성
2. 법 제23조제2항, 제24조제3항, 제24조의2제2항, 제25조제6항(제25조의2제4항에 따라 준용되는 경우를 포함한다) 및 제29조에 따른 안전성 확보 조치의 수준 및 이에 따른 개인정보 침해의 가능성
3. 개인정보 침해의 위험요인별 조치 여부
4. 그 밖에 법 및 이 영에 따라 필요한 조치 또는 의무 위반 요소에 관한 사항

② 법 제33조제2항에 따라 영향평가를 의뢰받은 평가기관은 평가기준에 따라 개인정보파일의 운용으로 인한 개인정보 침해의 위험요인을 분석·평가한 후 다음 각 호의 사항이 포함된 평가 결과를 영향평가서로 작성하여 해당 공공기관의 장에게 보내야 하며, 공공기관의 장은 제35조 각 호에 해당하는 개인정보파일을 운용 또는 변경하기 전에 그 영향평가서를 보호위원회에 제출해야 한다.<개정 2023. 9. 12.>

1. 영향평가의 대상 및 범위
2. 평가 분야 및 항목
3. 평가기준에 따른 개인정보 침해의 위험요인에 대한 분석·평가
4. 제3호의 분석·평가 결과에 따라 조치한 내용 및 개선계획
5. 영향평가의 결과
6. 제1호부터 제5호까지의 사항에 대하여 요약한 내용

③ 보호위원회 또는 공공기관의 장은 제2항제6호에 따른 영향평가서 요약 내용을 공개할 수 있다.<신설 2023. 9. 12.>

④ 보호위원회는 법 및 이 영에서 정한 사항 외에 평가기관의 지정 및 영향평가의 절차 등에 관한 세부 기준을 정하여 고시할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4., 2023. 9. 12.>

제39조(개인정보 유출 등의 통지) ① 개인정보처리자는 개인정보가

분실·도난·유출(이하 이 조 및 제40조에서 “유출등”이라 한다)되었음을 알게

되었을 때에는 서면등의 방법으로 72시간 이내에 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 지체 없이 정보주체에게 알릴 수 있다.

1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우
 2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우
- ② 제1항에도 불구하고 개인정보처리자는 같은 항에 따른 통지를 하려는 경우로서 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 통지해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지해야 한다. <개정 2024. 3. 12.>
- ③ 제1항 및 제2항에도 불구하고 개인정보처리자는 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 법 제34조제1항 각 호 외의 부분 단서에 따라 같은 항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항 및 제2항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 30일 이상 게시하는 것으로 제1항 및 제2항의 통지를 갈음할 수 있다.

[전문개정 2023. 9. 12.]

[제40조에서 이동, 종전 제39조는 제40조로 이동 <2023. 9. 12.>]

제40조(개인정보 유출 등의 신고) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 법 제34조제1항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 같은 조 제3항 전단에 따른 전문기관에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.

1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
 2. 민감정보 또는 고유식별정보가 유출등이 된 경우
 3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우
- ② 제1항에도 불구하고 개인정보처리자는 제1항에 따른 신고를 하려는 경우로서 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 신고해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다.

- ③ 법 제34조제3항 전단 및 후단에서 “대통령령으로 정하는 전문기관”이란 각각 한국인터넷진흥원을 말한다.

[전문개정 2023. 9. 12.]

[제39조에서 이동, 종전 제40조는 제39조로 이동 <2023. 9. 12.>]

제40조의2(노출된 개인정보의 삭제·차단 요청 기관) 법 제34조의2제2항에서 “대통령령으로 지정한 전문기관”이란 한국인터넷진흥원을 말한다.

[전문개정 2023. 9. 12.]

제6장 정보주체의 권리 보장

제41조(개인정보의 열람절차 등) ① 정보주체는 법 제35조제1항에 따라 자신의 개인정보에 대한 열람을 요구하려면 다음 각 호의 사항 중 열람하려는 사항을 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2017. 10. 17.>

1. 개인정보의 항목 및 내용
2. 개인정보의 수집·이용의 목적
3. 개인정보 보유 및 이용 기간
4. 개인정보의 제3자 제공 현황
5. 개인정보 처리에 동의한 사실 및 내용

② 개인정보처리자는 제1항에 따른 열람 요구 방법과 절차를 마련하는 경우 해당 개인정보의 수집 방법과 절차에 비하여 어렵지 아니하도록 다음 각 호의 사항을 준수하여야 한다.<신설 2017. 10. 17.>

1. 서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법으로 제공할 것
2. 개인정보를 수집한 창구의 지속적 운영이 곤란한 경우 등 정당한 사유가 있는 경우를 제외하고는 최소한 개인정보를 수집한 창구 또는 방법과 동일하게 개인정보의 열람을 요구할 수 있도록 할 것
3. 인터넷 홈페이지를 운영하는 개인정보처리자는 홈페이지에 열람 요구 방법과 절차를 공개할 것

③ 정보주체가 법 제35조제2항에 따라 보호위원회를 통하여 자신의 개인정보에 대한 열람을 요구하려는 경우에는 보호위원회가 정하여 고시하는 바에 따라 제1항 각 호의 사항 중 열람하려는 사항을 표시한 개인정보 열람요구서를 보호위원회에 제출해야 한다. 이 경우 보호위원회는 지체 없이 그 개인정보 열람요구서를 해당 공공기관에 이송해야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2017. 10. 17., 2020. 8. 4.>

④ 법 제35조제3항 전단에서 “대통령령으로 정하는 기간”이란 10일을 말한다.<개정 2017. 10. 17.>

- ⑤ 개인정보처리자는 제1항 및 제3항에 따른 개인정보 열람 요구를 받은 날부터 10일 이내에 정보주체에게 해당 개인정보를 열람할 수 있도록 하는 경우와 제42조제1항에 따라 열람 요구 사항 중 일부를 열람하게 하는 경우에는 열람할 개인정보와 열람이 가능한 날짜·시간 및 장소 등(제42조제1항에 따라 열람 요구 사항 중 일부만을 열람하게 하는 경우에는 그 사유와 이의제기방법을 포함한다)을 보호위원회가 정하여 고시하는 열람통지서로 해당 정보주체에게 알려야 한다. 다만, 즉시 열람하게 하는 경우에는 열람통지서 발급을 생략할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2017. 10. 17., 2020. 8. 4.>

제42조(개인정보 열람의 제한·연기 및 거절) ① 개인정보처리자는 제41조제1항에 따른 열람 요구 사항 중 일부가 법 제35조제4항 각 호의 어느 하나에 해당하는 경우에는 그 일부에 대하여 열람을 제한할 수 있으며, 열람이 제한되는 사항을 제외한 부분은 열람할 수 있도록 하여야 한다.

- ② 개인정보처리자가 법 제35조제3항 후단에 따라 정보주체의 열람을 연기하거나 같은 조 제4항에 따라 열람을 거절하려는 경우에는 열람 요구를 받은 날부터 10일 이내에 연기 또는 거절의 사유 및 이의제기방법을 보호위원회가 정하여 고시하는 열람의 연기·거절 통지서로 해당 정보주체에게 알려야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

제43조(개인정보의 정정·삭제 등) ① 정보주체는 법 제36조제1항에 따라 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구하려면 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다. 이 경우 개인정보처리자가 개인정보의 정정 또는 삭제 요구 방법과 절차를 마련할 때에는 제41조제2항을 준용하되, “열람”은 “정정 또는 삭제”로 본다.<개정 2017. 10. 17.>

- ② 다른 개인정보처리자로부터 개인정보를 제공받아 개인정보파일을 처리하는 개인정보처리자는 법 제36조제1항에 따른 개인정보의 정정 또는 삭제 요구를 받으면 그 요구에 따라 해당 개인정보를 정정·삭제하거나 그 개인정보 정정·삭제에 관한 요구 사항을 해당 개인정보를 제공한 기관의 장에게 지체 없이 알리고 그 처리 결과에 따라 필요한 조치를 하여야 한다.<개정 2017. 10. 17.>
- ③ 개인정보처리자는 제1항과 제2항에 따른 개인정보 정정·삭제 요구를 받은 날부터 10일 이내에 법 제36조제2항에 따라 해당 개인정보의 정정·삭제 등의 조치를 한 경우에는 그 조치를 한 사실을, 법 제36조제1항 단서에 해당하여 삭제 요구에 따르지 아니한 경우에는 그 사실 및 이유와 이의제기방법을 보호위원회가 정하여 고시하는 개인정보 정정·삭제 결과 통지서로 해당 정보주체에게 알려야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2017. 10. 17., 2020. 8. 4.>

제44조(개인정보의 처리정지 등) ① 정보주체는 법 제37조제1항에 따라 개인정보처리자에게 자신의 개인정보 처리의 정지를 요구하려면 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다. 이 경우 개인정보처리자가 개인정보의

처리 정지 요구 방법과 절차를 마련할 때에는 제41조제2항을 준용하되, “열람”은 “처리 정지”로 본다.<개정 2017. 10. 17.>

- ② 개인정보처리자는 제1항에 따른 개인정보 처리정지 요구를 받은 날부터 10일 이내에 법 제37조제2항 본문에 따라 해당 개인정보의 처리정지 조치를 한 경우에는 그 조치를 한 사실을, 같은 항 단서에 해당하여 처리정지 요구에 따르지 않은 경우에는 그 사실 및 이유와 이의제기방법을 보호위원회가 정하여 고시하는 개인정보 처리정지 요구에 대한 결과 통지서로 해당 정보주체에게 알려야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2017. 10. 17., 2020. 8. 4.>

제44조의2(자동화된 결정에 대한 거부 및 설명 등 요구의 방법 및 절차) ①

정보주체는 법 제37조의2제1항에 따른 자동화된 결정(이하 “자동화된 결정”이라 한다)에 대해 같은 항 본문에 따라 거부하는 경우에는 개인정보처리자가 마련하여 제44조의4제1항제5호에 따라 공개하는 방법과 절차에 따라야 한다.

- ② 정보주체는 법 제37조의2제2항에 따라 자동화된 결정에 대해 개인정보처리자에게 다음 각 호의 설명 또는 검토를 요구할 수 있다. 이 경우 정보주체의 설명 또는 검토 요구는 개인정보처리자가 마련하여 제44조의4제1항제5호에 따라 공개하는 방법과 절차에 따라야 한다.

1. 해당 자동화된 결정의 기준 및 처리 과정 등에 대한 설명
2. 정보주체가 개인정보 추가 등의 의견을 제출하여 개인정보처리자가 해당 의견을 자동화된 결정에 반영할 수 있는지에 대한 검토

- ③ 제1항 및 제2항에 따른 정보주체의 자동화된 결정에 대한 거부, 설명 및 검토 요구(이하 “거부·설명등요구”라 한다)의 방법과 절차를 개인정보처리자가 마련하는 경우 준수해야 할 사항에 관하여는 제41조제2항을 준용한다. 이 경우 “열람 요구”는 “거부·설명등요구”로 본다.

[본조신설 2024. 3. 12.]

제44조의3(거부·설명등요구에 따른 조치) ① 개인정보처리자는 정보주체가

제44조의2제1항에 따라 자동화된 결정에 대해 거부하는 경우에는 정당한 사유가 없으면 다음 각 호의 어느 하나에 해당하는 조치를 하고 그 결과를 정보주체에게 알려야 한다.

1. 해당 자동화된 결정을 적용하지 않는 조치
2. 인적 개입에 의한 재처리

- ② 개인정보처리자는 정보주체가 제44조의2제2항에 따라 자동화된 결정에 대해 같은 항 제1호에 따른 설명을 요구하는 경우 정당한 사유가 없으면 다음 각 호의 사항을 포함한 간결하고 의미있는 설명을 정보주체에게 제공해야 한다. 다만, 개인정보처리자는 해당 자동화된 결정이 정보주체의 권리 또는 의무에 중대한 영향을 미치지 않는 경우에는 정보주체에게 제44조의4제1항제2호 및 제3호의 사항을 알릴 수 있다.

1. 해당 자동화된 결정의 결과
 2. 해당 자동화된 결정에 사용된 주요 개인정보의 유형
 3. 제2호에 따른 개인정보의 유형이 자동화된 결정에 미친 영향 등 자동화된 결정의 주요 기준
 4. 해당 자동화된 결정에 사용된 주요 개인정보의 처리 과정 등 자동화된 결정이 이루어지는 절차
- ③ 개인정보처리자는 정보주체가 제44조의2제2항에 따라 같은 항 제2호에 따른 검토를 요구하는 경우에는 정당한 사유가 없으면 정보주체가 제출한 의견의 반영 여부를 검토하고 정보주체에게 반영 여부 및 반영 결과를 알려야 한다.
- ④ 개인정보처리자는 다른 사람의 생명·신체·재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 등 정당한 사유가 있어 법 제38조제5항에 따라 거부·설명등요구를 거절하는 경우에는 그 사유를 정보주체에게 지체 없이 서면등의 방법으로 알려야 한다.
- ⑤ 개인정보처리자는 제1항부터 제3항까지의 규정에 따라 정보주체의 거부·설명등요구에 따른 조치를 하는 경우에는 정보주체의 거부·설명등요구를 받은 날부터 30일 이내에 서면등의 방법으로 해야 한다. 다만, 30일 이내에 처리하기 어려운 정당한 사유가 있는 경우에는 정보주체에게 그 사유를 알리고 2회에 한정하여 각각 30일의 범위에서 그 기간을 연장할 수 있다.
- ⑥ 제1항부터 제5항까지의 규정에 따른 정보주체의 거부·설명등요구에 따른 조치에 관한 세부 사항은 보호위원회가 정하여 고시한다.

[본조신설 2024. 3. 12.]

제44조의4(자동화된 결정의 기준과 절차 등의 공개) ① 개인정보처리자는 법

제37조의2제4항에 따라 다음 각 호의 사항을 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지 등을 통해 공개해야 한다. 다만, 인터넷 홈페이지 등을 운영하지 않거나 지속적으로 알려야 할 필요가 없는 경우에는 미리 서면등의 방법으로 정보주체에게 알릴 수 있다.

1. 자동화된 결정이 이루어진다는 사실과 그 목적 및 대상이 되는 정보주체의 범위
 2. 자동화된 결정에 사용되는 주요 개인정보의 유형과 자동화된 결정의 관계
 3. 자동화된 결정 과정에서의 고려사항 및 주요 개인정보가 처리되는 절차
 4. 자동화된 결정 과정에서 민감정보 또는 14세 미만 아동의 개인정보를 처리하는 경우 그 목적 및 처리하는 개인정보의 구체적인 항목
 5. 자동화된 결정에 대하여 정보주체가 거부·설명등요구를 할 수 있다는 사실과 그 방법 및 절차
- ② 개인정보처리자는 제1항 각 호의 사항을 공개할 때에는 정보주체가 해당 내용을 쉽게 알 수 있도록 표준화·체계화된 용어를 사용해야 하며, 정보주체가 쉽게 이해할 수 있도록 동영상·그림·도표 등 시각적인 방법 등을 활용할 수 있다.

[본조신설 2024. 3. 12.]

제45조(대리인의 범위 등) ① 법 제38조에 따라 정보주체를 대리할 수 있는 자는 다음 각 호와 같다.

1. 정보주체의 법정대리인
2. 정보주체로부터 위임을 받은 자

② 제1항에 따른 대리인이 법 제38조에 따라 정보주체를 대리할 때에는 개인정보처리자에게 보호위원회가 정하여 고시하는 정보주체의 위임장을 제출하여야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

제46조(정보주체 또는 대리인의 확인) ① 개인정보처리자는 제41조제1항에 따른 열람, 제43조제1항에 따른 정정·삭제, 법 제37조제1항에 따른 처리정지 또는 동의 철회 등의 요구(이하 이 조, 제47조 및 제48조에서 “열람등요구”라 한다)를 받았을 때에는 열람등요구를 한 사람이 본인이거나 정당한 대리인인지를 확인하여야 한다.<개정 2020. 8. 4., 2023. 9. 12.>

② 공공기관인 개인정보처리자가 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 제1항에 따른 확인을 할 수 있는 경우에는 행정정보의 공동이용을 통하여 확인하여야 한다. 다만, 해당 공공기관이 행정정보의 공동이용을 할 수 없거나 정보주체가 확인에 동의하지 아니하는 경우에는 그러하지 아니하다.

제47조(수수료 등의 금액 등) ① 법 제38조제3항에 따른 수수료와 우송료의 금액은 열람등요구에 필요한 실비의 범위에서 해당 개인정보처리자가 정하는 바에 따른다. 다만, 개인정보처리자가 지방자치단체인 경우에는 그 지방자치단체의 조례로 정하는 바에 따른다.

② 개인정보처리자는 열람등요구를 하게 된 사유가 그 개인정보처리자에게 있는 경우에는 수수료와 우송료를 청구해서는 아니 된다.

③ 법 제38조제3항에 따른 수수료 또는 우송료는 다음 각 호의 구분에 따른 방법으로 낸다. 다만, 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속 기관(이하 이 조에서 “국가기관”이라 한다) 또는 지방자치단체인 개인정보처리자는 「전자금융거래법」 제2조제11호에 따른 전자지급수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 내게 할 수 있다.<개정 2023. 9. 12.>

1. 국가기관인 개인정보처리자에게 내는 경우: 수입인지
2. 지방자치단체인 개인정보처리자에게 내는 경우: 수입증지
3. 국가기관 및 지방자치단체 외의 개인정보처리자에게 내는 경우: 해당 개인정보처리자가 정하는 방법

제48조(열람 요구 지원시스템의 구축 등) ① 개인정보처리자는 열람등요구 및 그에 대한 통지를 갈음하여 해당 업무를 전자적으로 처리할 수 있도록 시스템을 구축·운영하거나 그 밖의 절차를 정하여 해당 업무를 처리할 수 있다.

- ② 보호위원회는 개인정보처리자 중 공공기관이 보유하고 있는 개인정보에 관한 열람등요구 및 그에 대한 통지에 관한 공공기관의 업무 수행을 효율적으로 지원하기 위하여 시스템을 구축·운영할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

제6장의2 삭제

제48조의2 ~ 제48조의6 삭제<2023. 9. 12.>

제48조의7(손해배상책임의 이행을 위한 보험 등 가입 대상자의 범위 및 기준 등) ①

법 제39조의7제1항에서 “대통령령으로 정하는 기준에 해당하는 자”란 다음 각 호의 요건을 모두 갖춘 자(이하 “가입대상개인정보처리자”라 한다)를 말한다.<개정 2024. 3. 12.>

1. 전년도(법인의 경우에는 직전 사업연도를 말한다)의 매출액등이 10억원 이상일 것
2. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는

정보주체(제15조의3제2항제2호에 해당하는 정보주체는 제외한다. 이하 이 조에서 같다)의 수가 일일평균 1만명 이상일 것. 다만, 해당 연도에 영업의 전부 또는 일부의 양수, 분할·합병 등으로 개인정보를 이전받은 경우에는 이전받은 시점을 기준으로 정보주체의 수가 1만명 이상일 것

- ② 법 제39조의7제2항제1호에서 “대통령령으로 정하는 공공기관, 비영리법인 및 단체”란 다음 각 호의 기관을 말한다.<신설 2024. 3. 12.>

1. 공공기관. 다만, 제2조제2호부터 제5호까지에 해당하는 공공기관으로서 제32조제4항 각 호에 해당하는 공공기관은 제외한다.
2. 「공익법인의 설립·운영에 관한 법률」 제2조에 따른 공익법인
3. 「비영리민간단체 지원법」 제4조에 따라 등록한 단체

- ③ 법 제39조의7제2항제2호에서 “대통령령으로 정하는 자”란 다음 각 호의 요건을 모두 갖춘 자를 말한다.<개정 2024. 3. 12.>

1. 「소상공인기본법」 제2조제1항에 따른 소상공인으로부터 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인정보의 저장·관리 업무를 위탁받은 자
2. 제1호에 따라 위탁받은 업무에 대하여 법 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 한 자

- ④ 가입대상개인정보처리자가 보험 또는 공제에 가입하거나 준비금을 적립할 경우 최저가입금액(준비금을 적립하는 경우 최소적립금액을 말한다. 이하 이 조에서 같다)의 기준은 별표 1의4와 같다. 다만, 가입대상개인정보처리자가 보험 또는 공제 가입과 준비금 적립을 병행하는 경우에는 보험 또는 공제 가입금액과 준비금 적립금액을 합산한 금액이 별표 1의4에서 정한 최저가입금액의 기준 이상이어야 한다.<개정 2023. 9. 12., 2024. 3. 12.>

[본조신설 2020. 8. 4.]

제48조의8 ~ 제48조의13 삭제 <2023. 9. 12.>

제7장 개인정보 분쟁조정

제48조의14(당연직위원) 분쟁조정위원회의 당연직위원은 보호위원회의 고위공무원단에 속하는 일반직공무원으로서 개인정보 보호에 관한 업무를 담당하는 사람 중 보호위원회 위원장이 지명하는 사람으로 한다.<개정 2017. 7. 26., 2020. 8. 4.>

[본조신설 2016. 7. 22.]

[제48조의2에서 이동 <2020. 8. 4.>]

제49조(조정부의 구성 및 운영) ① 법 제40조제6항에 따른 조정부(이하 “조정부”라 한다)는 분쟁조정위원회 위원장이 지명하는 5명 이내의 위원으로 구성하되, 그 중 1명은 변호사 자격이 있는 위원으로 한다.<개정 2016. 7. 22.>

② 분쟁조정위원회 위원장은 조정부의 회의를 소집한다.

③ 분쟁조정위원회의 위원장은 조정부의 회의를 소집하려면 회의 날짜·시간·장소 및 안건을 정하여 회의 개최 7일 전까지 조정부의 각 위원에게 알려야 한다. 다만, 긴급한 사정이 있는 경우에는 그러하지 아니하다.

④ 조정부의 장은 조정부 위원 중에서 호선(互選)한다.

⑤ 제1항부터 제4항까지의 규정에서 정한 사항 외에 조정부의 구성 및 운영 등에 필요한 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회의 위원장이 정한다.

제49조의2(분쟁조정 전문위원회) ① 분쟁조정위원회는 개인정보에 관한 분쟁의 조정과 관련된 사항의 전문적인 검토를 위하여 분쟁조정위원회에 분야별 전문위원회(이하 “분쟁조정전문위원회”라 한다)를 둘 수 있다.

② 분쟁조정전문위원회는 위원장 1명을 포함한 10명 이내의 위원으로 구성한다.

③ 분쟁조정전문위원회 위원은 다음 각 호의 사람 중에서 분쟁조정위원회 위원장이 임명하거나 위촉하고, 분쟁조정전문위원회 위원장은 분쟁조정전문위원회 위원 중에서 분쟁조정위원회 위원장이 지명한다.

1. 분쟁조정위원회 위원

2. 개인정보 보호 관련 업무를 담당하는 중앙행정기관의 관계 공무원

3. 대학에서 개인정보 보호 분야의 조교수 이상으로 재직하고 있거나 재직하였던 사람

4. 공인된 연구기관에서 개인정보 보호 관련 분야의 5년 이상 연구경력이 있는 사람

5. 변호사 자격을 취득한 후 개인정보 보호 관련 분야에 1년 이상 경력이 있는 사람

6. 그 밖에 개인정보 보호 및 분쟁의 조정과 관련하여 전문지식과 경험이 풍부한 사람

④ 제1항부터 제3항까지에서 규정한 사항 외에 분쟁조정전문위원회의 구성 및 운영 등에 필요한 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회 위원장이 정한다.

[본조신설 2023. 9. 12.]

제50조(사무기구) ① 법 제40조제8항에 따른 분쟁조정 접수 및 사실 확인 등 분쟁조정에 필요한 사무처리는 보호위원회의 사무기구가 수행한다.<개정 2020. 8. 4.>
 ② 사무기구는 분쟁조정 접수·진행 및 당사자 통지 등 분쟁조정에 필요한 사무를 전자적으로 처리하기 위하여 분쟁조정업무시스템을 구축하여 운영할 수 있다.<신설 2020. 8. 4.>
 [전문개정 2016. 7. 22.]

제51조(분쟁조정위원회 등의 운영) ① 분쟁조정위원회 위원장은 분쟁조정위원회의 회의를 소집하며, 그 의장이 된다.
 ② 분쟁조정위원회 위원장이 분쟁조정위원회의 회의를 소집하려면 회의 날짜·시간·장소 및 안건을 정하여 회의 개최 7일 전까지 각 위원에게 알려야 한다. 다만, 긴급한 사정이 있는 경우에는 그러하지 아니하다.
 ③ 분쟁조정위원회 및 조정부의 회의는 공개하지 아니한다. 다만, 필요하다고 인정되는 경우에는 분쟁조정위원회의 의결로 당사자 또는 이해관계인에게 방청을 하게 할 수 있다.

제51조의2(조정 불응 의사의 통지) 개인정보처리자는 법 제43조제3항에 따른 특별한 사유가 있어 분쟁조정에 응하지 않으려는 경우에는 법 제43조제2항에 따른 분쟁조정의 통지를 받은 날부터 10일 이내에 그 사유를 명시하여 분쟁조정 불응 의사를 분쟁조정위원회에 알려야 한다.

[본조신설 2023. 9. 12.]

제51조의3(분쟁조정위원회의 사무기구 및 조사·열람 등) ① 법 제45조제2항 전단에서 “대통령령으로 정하는 사무기구”란 제50조제1항에 따라 분쟁조정에 필요한 사무처리를 담당하는 보호위원회의 사무기구를 말한다.

② 분쟁조정위원회는 법 제45조제2항에 따라 조사·열람을 하려는 경우에는 그 7일 전까지 조사·열람 대상자에게 다음 각 호의 사항을 문서로 알려야 한다. 다만, 조사·열람 목적을 침해할 우려가 있는 경우에는 미리 알리지 않을 수 있다.

1. 조사·열람의 목적
2. 조사·열람의 기간과 장소
3. 조사·열람을 하는 사람의 직위와 성명
4. 조사·열람의 범위와 내용
5. 정당한 사유가 있는 경우 조사·열람을 거부할 수 있다는 사실
6. 정당한 사유 없이 조사·열람을 거부·방해 또는 기피할 경우 불이익의 내용
7. 그 밖에 분쟁조정을 위한 조사·열람에 필요한 사항

③ 분쟁조정위원회는 법 제45조제2항에 따라 조사·열람을 할 때에는 분쟁당사자 또는 분쟁당사자가 지명하는 자가 입회하거나 의견을 진술하도록 요청할 수 있다.

④ 분쟁조정위원회는 법 제45조제5항에 따라 의견을 들으려면 회의 일시 및 장소를 정하여 회의 개최 15일 전까지 분쟁당사자 또는 참고인에게 출석을 통지해야 한다.

[본조신설 2023. 9. 12.]

제51조의4(조정안에 대한 거부 의사 통지 등) ① 분쟁조정위원회는 법 제47조제2항에 따라 당사자에게 조정안을 제시할 때에는 같은 조 제3항에 따라 조정안을 제시받은 날부터 15일 이내에 수락 여부를 알리지 않으면 조정을 수락한 것으로 본다는 사실을 알려야 한다.

② 법 제47조제2항에 따라 조정안을 제시받은 당사자는 조정안을 거부하려는 경우에는 조정안을 제시받은 날부터 15일 이내에 인편, 등기우편 또는 전자우편의 방법으로 그 의사를 분쟁조정위원회에 알려야 한다.

[본조신설 2023. 9. 12.]

제52조(집단분쟁조정 신청 대상) 법 제49조제1항에서 “대통령령으로 정하는 사건”이란 다음 각 호의 요건을 모두 갖춘 사건을 말한다.

1. 피해 또는 권리침해를 입은 정보주체의 수가 다음 각 목의 정보주체를 제외하고 50명 이상일 것
 - 가. 개인정보처리자와 분쟁해결이나 피해보상에 관한 합의가 이루어진 정보주체
 - 나. 같은 사안으로 다른 법령에 따라 설치된 분쟁조정기구에서 분쟁조정 절차가 진행 중인 정보주체
 - 다. 해당 개인정보 침해로 인한 피해에 대하여 법원에 소(訴)를 제기한 정보주체
2. 사건의 중요한 쟁점이 사실상 또는 법률상 공통될 것

제53조(집단분쟁조정 절차의 개시) ① 법 제49조제2항 후단에서 “대통령령으로 정하는 기간”이란 14일 이상의 기간을 말한다.

② 법 제49조제2항 후단에 따른 집단분쟁조정 절차의 개시 공고는 분쟁조정위원회의 인터넷 홈페이지 또는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 일반일간신문에 게재하는 방법으로 한다.<개정 2015. 12. 30.>

제54조(집단분쟁조정 절차에 대한 참가 신청) ① 법 제49조에 따른 집단분쟁조정(이하 “집단분쟁조정”이라 한다)의 당사자가 아닌 정보주체 또는 개인정보처리자가 법 제49조제3항에 따라 추가로 집단분쟁조정의 당사자로 참가하려면 법 제49조제2항 후단의 공고기간에 문서로 참가 신청을 하여야 한다.

② 분쟁조정위원회는 제1항에 따라 집단분쟁조정 당사자 참가 신청을 받으면 제1항의 신청기간이 끝난 후 10일 이내에 참가 인정 여부를 문서로 알려야 한다.

제55조(집단분쟁조정 절차의 진행) ① 집단분쟁조정 절차가 개시된 후

제52조제1호가목부터 다목까지의 어느 하나에 해당하게 된 정보주체는 당사자에서 제외된다.

② 분쟁조정위원회는 제52조 각 호의 요건을 모두 갖춘 사건에 대하여 집단분쟁조정 절차가 개시되고 나면 그 후 집단분쟁조정 당사자 중 일부가 같은 조 제1호가목부터 다목까지의 어느 하나에 해당하게 되어 같은 조 제1호의 요건을 갖추지 못하게 되더라도 집단분쟁조정 절차를 중지하지 아니한다.

제56조(수당과 여비) 분쟁조정위원회, 조정부 및 분쟁조정전문위원회의 회의에 출석한 위원 등에게는 예산의 범위에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 그 소관 업무와 직접적으로 관련되어 출석하는 경우에는 그러하지 아니하다.<개정 2023. 9. 12.>

제57조(분쟁조정 세칙) 법 및 이 영에서 규정한 사항 외에 분쟁의 조정절차 및 조정업무의 처리 등 분쟁조정위원회의 운영 및 집단분쟁조정을 위하여 필요한 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회의 위원장이 정한다.<개정 2023. 9. 12.>

제8장 보칙 및 벌칙

제58조(개선권고 및 징계권고) ① 법 제61조제2항·제3항에 따른 개선권고 및 법 제65조제2항·제3항에 따른 징계권고는 권고 사항, 권고 사유 및 조치 결과 회신기간 등을 분명하게 밝힌 문서로 하여야 한다.
② 제1항에 따른 권고를 받은 자는 권고 내용에 따라 필요한 조치를 하고, 그 결과를 보호위원회 또는 관계 중앙행정기관의 장에게 문서로 통보해야 한다. 다만, 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보해야 한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

제59조(침해 사실의 신고 등) 보호위원회는 법 제62조제2항에 따라 개인정보에 관한 권리 또는 이익 침해 사실 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위한 전문기관으로 한국인터넷진흥원을 지정한다.<개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

제60조(자료제출 요구 및 검사) ① 법 제63조제1항제3호에서 “대통령령으로 정하는 경우”란 개인정보 유출 등 정보주체의 개인정보에 관한 권리 또는 이익을 침해하는 사건·사고 등이 발생하였거나 발생할 가능성이 상당히 있는 경우를 말한다.
② 보호위원회는 법 제63조제1항 및 제2항에 따른 자료의 제출 요구 및 검사 등을 위하여 한국인터넷진흥원의 장에게 기술적인 사항을 자문하는 등 필요한 지원을 요청할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2015. 12. 30., 2017. 7. 26., 2020. 8. 4.>
③ ~ ⑦ 삭제<2023. 9. 12.>

제60조의2(과징금의 산정기준 등) ① 법 제64조의2제1항 각 호 외의 부분 본문에 따른 전체 매출액은 위반행위가 있었던 사업연도(이하 이 조에서 “해당사업연도”라 한다) 직전 3개 사업연도의 해당 개인정보처리자의 연평균 매출액으로 한다. 다만, 해당사업연도의 첫날 현재 사업을 개시한 지 3년이 되지 않은 경우에는 그 사업개시일부터 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액으로 하며, 해당사업연도에 사업을 개시한 경우에는 사업개시일부터

위반행위일까지의 매출액을 연매출액으로 환산한 금액으로 한다.

- ② 법 제64조의2제1항 각 호 외의 부분 단서에서 “대통령령으로 정하는 경우”란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.
1. 다음 각 목의 어느 하나에 해당하는 사유로 영업실적이 없는 경우
 - 가. 영업을 개시하지 않은 경우
 - 나. 영업을 중단한 경우
 - 다. 수익사업을 영위하지 않는 등 가목 및 나목에 준하는 경우
 2. 재해 등으로 인하여 매출액 산정자료가 소멸되거나 훼손되는 등 객관적인 매출액의 산정이 곤란한 경우
- ③ 법 제64조의2제2항에 따른 위반행위와 관련이 없는 매출액은 제1항에 따른 전체 매출액 중 다음 각 호의 어느 하나에 해당하는 금액으로 한다.
1. 개인정보의 처리와 관련이 없는 재화 또는 서비스의 매출액
 2. 제4항에 따라 제출받은 자료 등에 근거하여 보호위원회가 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 재화 또는 서비스의 매출액이 아닌 것으로 인정하는 매출액
- ④ 보호위원회는 제1항부터 제3항까지의 규정에 따른 매출액 산정 등을 위하여 재무제표 등의 자료가 필요한 경우 20일 이내의 기간을 정하여 해당 개인정보처리자에게 관련 자료의 제출을 요청할 수 있다.
- ⑤ 법 제64조의2제5항제4호에서 “대통령령으로 정하는 사유가 있는 경우”란 해당 개인정보처리자가 위반행위를 시정하고 보호위원회가 정하여 고시하는 기준에 해당되는 경우를 말한다.
- ⑥ 법 제64조의2제6항에 따른 과징금의 산정기준과 산정절차는 별표 1의5와 같다.

[본조신설 2023. 9. 12.]

제60조의3(과징금의 부과 및 납부) ① 보호위원회는 법 제64조의2에 따라 과징금을 부과하려는 경우에는 해당 위반행위를 조사·확인한 후 위반사실·부과금액·이의 제기 방법 및 이의 제기 기간 등을 서면으로 명시하여 과징금 부과대상자에게 통지해야 한다.

- ② 제1항에 따라 통지를 받은 자는 통지를 받은 날부터 30일 이내에 보호위원회가 지정하는 금융기관에 과징금을 납부해야 한다.
- ③ 제2항에 따라 과징금의 납부를 받은 금융기관은 과징금을 납부한 자에게 영수증을 발급해야 한다.
- ④ 금융기관이 제2항에 따라 과징금을 수납한 때에는 지체 없이 그 사실을 보호위원회에 통보해야 한다.

[본조신설 2023. 9. 12.]

제60조의4(과징금의 납부기한 연기 및 분할 납부) ① 보호위원회는 법 제64조의2제1항에 따른 과징금의 납부기한을 「행정기본법」 제29조 및 같은 법 시행령 제7조에 따라

연기하는 경우에는 원래 납부기한의 다음 날부터 2년을 초과할 수 없다.

② 보호위원회는 법 제64조의2제1항에 따른 과징금을 「행정기본법」 제29조 및 같은 법 시행령 제7조에 따라 분할 납부하게 하는 경우에는 각 분할된 납부기한 간의 간격은 6개월을 초과할 수 없으며, 분할 횟수는 6회를 초과할 수 없다.

③ 제1항 및 제2항에서 규정한 사항 외에 과징금 납부기한 연기 및 분할 납부 신청 등에 필요한 사항은 보호위원회가 정하여 고시한다.

[본조신설 2023. 9. 12.]

제60조의5(환급가산금의 이자율) 법 제64조의2제9항에서 “대통령령으로 정하는 이자율”이란 「국세기본법 시행령」 제43조의3제2항 본문에 따른 이자율을 말한다.

[본조신설 2023. 9. 12.]

제61조(결과의 공표) ① 보호위원회는 법 제66조제1항에 따라 다음 각 호의 사항을 보호위원회 인터넷 홈페이지 등에 게재하여 공표할 수 있다.

1. 위반행위의 내용

2. 위반행위를 한 자

3. 개선권고, 시정조치 명령, 과징금의 부과, 고발, 징계권고, 과태료 부과 내용 및 결과

② 보호위원회는 법 제66조제2항에 따라 개선권고, 시정조치 명령, 과징금의 부과, 고발, 징계권고 및 과태료 부과처분 등(이하 이 조에서 “처분등”이라 한다)을 받은 자에게 다음 각 호의 사항을 공표할 것을 명할 수 있다. 이 경우 공표의 내용·횟수, 매체와 지면의 크기 등을 정하여 명해야 하며, 처분등을 받은 자와 공표 문안 등에 관하여 협의할 수 있다.

1. 위반행위의 내용

2. 위반행위를 한 자

3. 처분등을 받았다는 사실

③ 보호위원회는 제1항에 따라 공표하려는 경우 또는 제2항에 따라 공표할 것을 명하려는 경우에는 위반행위의 내용 및 정도, 위반 기간 및 횟수, 위반행위로 인하여 발생한 피해의 범위 및 결과 등을 고려해야 한다.

④ 보호위원회는 공표 또는 공표명령에 대한 심의·의결 전에 처분등을 받은 자에게 소명자료를 제출하거나 의견을 진술할 수 있는 기회를 주어야 한다.

[전문개정 2023. 9. 12.]

제62조(업무의 위탁) ① 삭제<2015. 12. 30.>

② 보호위원회는 법 제68조제1항에 따라 법 제24조의2제4항에 따른 대체가입수단 제공의 지원에 관한 업무를 다음 각 호의 기관에 위탁할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2015. 12. 30., 2017. 7. 26., 2020. 8. 4., 2022. 7. 19.>

1. 「전자정부법」 제72조제1항에 따른 한국지역정보개발원

2. 한국인터넷진흥원

3. 대체가입수단의 개발·제공·관리 업무를 안전하게 수행할 수 있는 기술적·재정적

능력과 설비를 보유한 것으로 인정되어 보호위원회가 정하여 고시하는 법인·기관·단체

③ 보호위원회는 법 제68조제1항에 따라 다음 각 호의 사항에 관한 업무를 제4항에 따른 기관에 위탁할 수 있다.<개정 2013. 3. 23., 2014. 11. 19., 2015. 12. 30., 2017. 7. 26., 2020. 8. 4., 2022. 7. 19., 2023. 9. 12.>

1. 법 제7조의8제5호에 따른 개인정보 보호를 위한 국제기구와 외국의 개인정보 보호기구와의 교류·협력

2. 법 제7조의8제6호에 따른 개인정보 보호에 관한 법령·정책·제도·실태 등의 조사·연구

3. 법 제7조의8제7호에 따른 개인정보 보호에 관한 기술개발의 지원·보급

4. 법 제13조제1호에 따른 개인정보 보호에 관한 교육·홍보

5. 법 제13조제2호에 따른 개인정보 보호와 관련된 기관·단체의 육성 및 지원

6. 법 제33조제6항에 따른 관계 전문가의 육성 및 영향평가 기준의 개발

7. 법 제35조제2항에 따른 열람 요구의 접수 및 처리

8. 법 제63조에 따른 자료제출 요구 및 검사 중 다음 각 목의 사항과 관련된 자료제출 요구 및 검사

가. 법 제34조제3항 전단에 따른 신고에 대한 기술지원

나. 법 제62조에 따라 개인정보침해 신고센터에 접수된 신고의 접수·처리 및 상담

9. 제36조제2항에 따른 평가기관 지정신청서의 접수 및 같은 조 제6항에 따른 신고 사항의 접수

④ 보호위원회가 제3항 각 호의 사항에 관한 업무를 위탁할 수 있는 기관은 다음 각 호와 같다.<신설 2022. 7. 19.>

1. 한국인터넷진흥원

2. 개인정보 보호 분야에 전문성을 갖춘 것으로 인정되어 보호위원회가 정하여 고시하는 법인·기관 또는 단체

⑤ 보호위원회가 제2항부터 제4항까지의 규정에 따라 업무를 위탁하는 경우에는 위탁받는 기관과 위탁업무의 내용을 관보나 보호위원회의 인터넷 홈페이지에 공고해야 한다.<개정 2022. 7. 19.>

[제목개정 2022. 7. 19.]

제62조의2(민감정보 및 고유식별정보의 처리) ① 보호위원회(제62조제3항에 따라 보호위원회의 권한을 위탁받은 자를 포함한다)는 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 민감정보와 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.<개정 2020. 8. 4., 2023. 9. 12.>

1. 법 제7조의9제1항제4호부터 제6호까지의 규정에 따른 사항의 심의·의결에 관한 사무

2. 법 제24조의2제4항에 따른 주민등록번호 대체 방법 제공을 위한 시스템 구축 등 제반조치 마련 및 지원에 관한 사무

3. 삭제<2023. 9. 12.>

4. 법 제62조제3항에 따른 개인정보침해 신고센터의 업무에 관한 사무
5. 법 제63조제1항 및 제2항에 따른 자료의 제출 및 검사에 관한 사무
6. 법 제63조의2에 따른 사전 실태점검에 관한 사무
7. 법 제64조의2에 따른 과징금의 부과 및 징수에 관한 사무

② 분쟁조정위원회는 법 제45조, 제47조 및 제49조에 따른 개인정보 분쟁 조정에 관한 사무를 수행하기 위하여 불가피한 경우 민감정보와 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.<개정 2020. 8. 4., 2023. 9. 12.>

[본조신설 2014. 8. 6.]

[제목개정 2020. 8. 4.]

제62조의3(규제의 재검토) ① 보호위원회는 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 3년마다(매 3년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 해야 한다.<신설 2020. 8. 4., 2022. 3. 8., 2023. 9. 12., 2024. 3. 12.>

1. 제36조에 따른 평가기관의 지정대상, 지정취소 요건 및 변경신고 사유: 2022년 1월 1일
2. 제15조의3에 따른 개인정보 이용·제공내역을 통지해야 하는 자의 범위, 통지해야 하는 정보의 종류 및 통지 주기와 방법: 2023년 9월 15일
3. 제48조의7에 따른 손해배상책임의 이행을 위한 보험 등 가입 대상자의 범위 및 기준: 2020년 8월 5일
4. 제29조의3에 따른 개인정보처리자 간 가명정보의 결합: 2024년 1월 1일

② 보호위원회는 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 2년마다(매 2년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 해야 한다.<개정 2024. 3. 12.>

1. 제31조에 따른 개인정보 처리방침의 내용 및 공개방법 등: 2015년 1월 1일
2. 제32조제4항·제6항 및 별표 1에 따른 개인정보 보호책임자의 자격 요건 및 개인정보 보호책임자의 독립성 보장을 위한 개인정보처리자의 준수 사항: 2025년 1월 1일
3. 제44조의2부터 제44조의4까지의 규정에 따른 자동화된 결정의 거부·설명등요구의 절차 및 방법, 자동화된 결정의 거부·설명등요구에 따른 조치, 자동화된 결정의 기준과 절차 등의 공개: 2025년 1월 1일

③ 삭제<2022. 3. 8.>

[전문개정 2014. 12. 9.]

제63조(과태료의 부과기준) 법 제75조에 따른 과태료의 부과기준은 별표 2와 같다.<개정 2020. 8. 4., 2023. 9. 12.>

부칙 <대통령령 제34309호, 2024. 3. 12.>

제1조(시행일) 이 영은 2024년 3월 15일부터 시행한다. 다만, 대통령령 제33723호 개인정보 보호법 시행령 일부개정령 제30조의2제1항의 개정규정 및 제32조제4항제4호의 개정규정은 2024년 9월 15일부터 시행한다.

제2조(개인정보 보호책임자에 관한 경과조치) ① 이 영 시행 당시 종전의 제32조제2항에 따라 개인정보 보호책임자를 지정한 개인정보처리자로서 제32조제4항의 개정규정에 따른 개인정보처리자(공공시스템운영기관은 제외한다)에 해당하는 경우에는 이 영 시행일부터 2년 동안 제32조제3항·제4항 및 별표 1에 따른 개인정보 보호책임자를 지정한 것으로 본다.

② 부칙 제1조 단서에 따른 시행일 당시 종전의 제32조제2항에 따라 개인정보 보호책임자를 지정한 개인정보처리자로서 제32조제4항제4호의 개정규정에 따른 공공시스템운영기관에 해당하는 경우(같은 항 제1호부터 제3호까지의 개정규정에 따른 개인정보처리자에 해당하지 않는 경우로 한정한다)에는 부칙 제1조 단서에 따른 시행일부터 2년 동안 제32조제3항·제4항 및 별표 1에 따른 개인정보 보호책임자를 지정한 것으로 본다.

개인정보 보호책임자의 자격(제32조제4항 관련)

1. 제32조제4항에 따라 개인정보 보호책임자로 지정되는 사람은 개인정보보호 경력, 정보보호 경력, 정보기술 경력을 합하여 총 4년 이상 보유하고, 그 중 개인정보보호 경력을 최소 2년 이상 보유해야 한다.
2. 제1호에서 “개인정보보호 경력”이란 공공기관, 기업체, 교육기관 및 연구기관 등에서 개인정보보호 관련 정책 및 제도·개인정보 영향평가·개인정보 보호 인증심사 등 개인정보보호 업무를 수행한 경력, 개인정보보호 관련 컨설팅 또는 법률자문 경력을 말한다.
3. 제1호에서 “정보보호 경력”이란 공공기관, 기업체, 교육기관 및 연구기관 등에서 정보보호를 위한 공통기반기술, 시스템·네트워크 보호, 응용서비스 보호, 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 등 정보보호 업무를 수행한 경력, 정보보호 관련 컨설팅 또는 법률자문 경력을 말한다.
4. 제1호에서 “정보기술 경력”이란 공공기관, 기업체, 교육기관 및 연구기관 등에서 정보통신서비스, 정보통신기기, 소프트웨어 및 컴퓨터 관련 서비스 분야의 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 등 정보기술 업무를 수행한 경력, 정보기술 관련 컨설팅 또는 법률자문 경력을 말한다.

비고:

- 가. 동일 기간에 두 가지 이상 업무가 중복되는 경우에는 하나의 경력만 인정한다.
- 나. 개인정보보호, 정보보호, 정보기술 관련 학위를 취득한 경우에는 아래의 표에 따라 경력으로 인정한다. 다만, 여러 학위를 취득한 경우에는 개인정보 보호책임자를 지정하려는 개인정보처리자가 정하는 하나의 학위만 경력으로 인정한다.

학 위	경력 인정기간
개인정보보호 관련 박사	개인정보보호 경력 2년
개인정보보호 관련 석사	개인정보보호 경력 1년

개인정보보호 관련 학사	개인정보보호 경력 6개월
정보보호 관련 박사	정보보호 경력 2년
정보보호 관련 석사	정보보호 경력 1년
정보보호 관련 학사	정보보호 경력 6개월
정보기술 관련 박사	정보기술 경력 2년
정보기술 관련 석사	정보기술 경력 1년
정보기술 관련 학사	정보기술 경력 6개월

다. 그 밖에 보호위원회가 정하여 고시하는 자격을 취득하거나 교육을 이수한 경우 등의 해당 취득자격이나 이수교육 등에 대해서는 보호위원회가 정하여 고시하는 바에 따라 개인정보보호 경력, 정보보호 경력 또는 정보기술 경력으로 인정한다.

■ 개인정보 보호법 시행령 [별표 1의4] <개정 2024. 3. 12.>

손해배상책임의 이행을 위한 최저가입금액(최소적립금액)의 기준(제48조의7제4항 관련)

가입대상개인정보처리자의 가입금액 산정요소		최저가입금액 (최소적립금액)
정보주체 수	매출액등	
100만명 이상	800억원 초과	10억원
	50억원 초과 800억원 이하	5억원
	10억원 이상 50억원 이하	2억원
10만명 이상 100만명 미만	800억원 초과	5억원
	50억원 초과 800억원 이하	2억원
	10억원 이상 50억원 이하	1억원
1만명 이상 10만명 미만	800억원 초과	2억원
	50억원 초과 800억원 이하	1억원
	10억원 이상 50억원 이하	5천만원

비고: 이 표에서 “매출액등”이란 제31조의2제1항제1호에 따른 매출액등을 말한다.

■ 개인정보 보호법 시행령 [별표 1의5] <개정 2023. 9. 12.>

과징금의 산정기준과 산정절차(제60조의2제6항 관련)

1. 과징금의 산정단계

과징금은 법 제64조의2제4항 각 호에 따른 고려 사항과 이에 영향을 미치는 행위를 종합적으로 고려하여 제2호가목에 따라 산정된 기준금액에 같은 호 나목에 따른 1차 조정, 같은 호 다목에 따른 2차 조정, 같은 호 라목에 따른 부과과징금 결정을 순차적으로 거쳐 산정한다. 다만, 가중하는 경우에도 법 제64조의2제1항 각 호 외의 부분에 따른 과징금 금액의 상한을 넘을 수 없다.

2. 과징금의 산정단계에 따른 산정방식과 고려 사유

가. 기준금액의 산정

- 1) 기준금액은 제60조의2제1항에 따른 전체 매출액에서 같은 조 제3항에 따른 위반행위와 관련이 없는 매출액을 제외한 매출액에 위반행위의 중대성에 따라 다음과 같이 구분된 과징금의 산정비율(이하 “부과기준율”이라 한다)을 곱하여 산출한 금액으로 한다.

위반행위의 중대성	부과기준율
매우 중대한 위반행위	2.1% 이상 2.7% 이하
중대한 위반행위	1.5% 이상 2.1% 미만
보통 위반행위	0.9% 이상 1.5% 미만
약한 위반행위	0.03% 이상 0.9% 미만

- 2) 제60조의2제2항 각 호의 어느 하나에 해당하는 경우에는 1)에도 불구하고 위반행위의 중대성에 따라 기준금액을 다음과 같이 한다.

위반행위의 중대성	기준금액
매우 중대한 위반행위	7억원 이상 18억원 이하
중대한 위반행위	2억원 이상 7억원 미만
보통 위반행위	5천만원 이상 2억원 미만
약한 위반행위	5백만원 이상 5천만원 미만

- 3) 위반행위의 중대성은 다음의 사항을 종합적으로 고려하여 판단한다.

가) 위반행위의 내용 및 정도

나) 암호화 등 안전성 확보 조치 이행 노력

다) 개인정보가 분실·도난·유출·위조·변조·훼손된 경우 위반행위와의
관련성 및 분실·도난·유출·위조·변조·훼손의 규모

라) 개인정보처리자가 처리하는 개인정보의 유형과 정보주체에게 미치는
영향

마) 위반행위로 인한 정보주체의 피해 규모

나. 1차 조정

위반행위의 기간 및 횟수, 위반행위로 인하여 취득한 이익의 규모,
개인정보처리자의 업무 형태 및 규모를 고려하여 가목에 따른 기준금액의
100분의 90의 범위에서 보호위원회가 정하여 고시하는 기준에 따라
가중하거나 감경할 수 있다.

다. 2차 조정

다음의 사항(법 제64조의2제4항 각 호의 사항 중 가목에 따른 기준금액
산정 및 나목에 따른 1차 조정 단계에서 고려된 사항은 제외한다)을
종합적으로 고려하여 1차 조정을 거친 금액의 100분의 50의 범위에서
보호위원회가 정하여 고시하는 기준에 따라 가중하거나 감경할 수 있다.

- 1) 보호위원회와의 협조 등 위반행위를 시정하기 위한 조치 여부
- 2) 위반행위로 인한 피해의 회복 및 피해 확산 방지 조치의 이행 여부
- 3) 개인정보 보호 인증, 자율적인 보호 활동 등 개인정보 보호를 위한 노력
- 4) 위반행위의 주도 여부
- 5) 위반행위 사실의 자진신고 여부

라. 부과과징금의 결정

- 1) 다음의 사항을 고려하여 다목에 따라 산정된 과징금이 과중하다고
인정되는 경우에는 해당 금액의 100분의 90 범위에서 감경할 수 있다.

가) 위반행위자의 현실적인 부담능력

나) 경제위기 등으로 위반행위자가 속한 시장·산업 여건이 현저하게
변동되거나 지속적으로 악화된 상태인지 여부

- 2) 법 제64조의2제5항 각 호의 어느 하나에 해당하는 경우에는 과징금을
부과하지 않을 수 있다.

3. 세부 기준

매출액의 산정에 관한 세부 기준, 위반행위의 중대성 판단 기준, 1차 조정 및
2차 조정을 위한 세부 기준, 부과과징금의 결정을 위한 세부 기준과 그 밖에
과징금의 부과에 필요한 사항은 보호위원회가 정하여 고시한다.

■ 개인정보 보호법 시행령 [별표 2] <개정 2023. 9. 12.> [시행일: 2024. 3. 15.] 제2호가목, 제2호고목, 제2호보목, 제2호소목, 제2호초목

과태료의 부과기준(제63조 관련)

1. 일반기준

가. 위반행위의 횟수에 따른 과태료의 가중된 부과기준은 최근 3년간 같은 위반행위로 과태료 부과처분을 받은 경우에 적용한다. 이 경우 기간의 계산은 위반행위에 대하여 과태료 부과처분을 받은 날과 그 처분 후 다시 같은 위반행위를 하여 적발된 날을 기준으로 한다.

나. 가목에 따라 가중된 부과처분을 하는 경우 가중처분의 적용 차수는 그 위반행위 전 부과처분 차수(가목에 따른 기간 내에 과태료 부과처분이 둘 이상 있었던 경우에는 높은 차수를 말한다)의 다음 차수로 한다.

다. 부과권자는 다음의 어느 하나에 해당하는 경우에는 제2호의 개별기준에 따른 과태료 금액을 줄이거나 면제할 수 있다. 다만, 과태료를 체납하고 있는 위반행위자에 대해서는 그렇지 않다.

- 1) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우
- 2) 위반의 내용·정도가 경미하다고 인정되는 경우
- 3) 위반행위자가 「중소기업기본법」 제2조에 따른 중소기업자인 경우 등 위반행위자의 업무 형태 및 규모에 비해 과중하다고 인정되는 경우
- 4) 위반행위자가 법 위반상태를 시정하거나 해소하기 위하여 노력한 것이 인정되는 경우
- 5) 위반행위자가 위반행위로 인한 피해의 회복 및 피해 확산 방지 조치를 이행한 경우
- 6) 위반행위자가 법 제32조의2에 따른 개인정보 보호 인증을 받거나 자율적인 보호 활동을 하는 등 개인정보 보호를 위하여 노력한 것이 인정되는 경우
- 7) 위반행위자가 위반행위 사실을 자진신고한 경우
- 8) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료 금액을 줄이거나 면제할 필요가 있다고 인정되는 경우

라. 부과권자는 다음의 어느 하나에 해당하는 경우에는 제2호의 개별기준에 따른 과태료의 2분의 1 범위에서 그 금액을 늘려 부과할 수 있다. 다만, 늘려 부과하는 경우에도 법 제75조제1항부터 제4항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.

- 1) 위반의 내용·정도가 중대하여 정보주체 등에게 미치는 피해가 크다고 인정되는 경우
- 2) 그 밖에 위반행위의 정도·기간, 위반행위의 동기와 그 결과 등을 고려하여 과태료 금액을 늘릴 필요가 있다고 인정되는 경우

2. 개별기준

(단위: 만원)

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
가. 법 제11조의2제2항을 위반하여 정당한 사유 없이 자료를 제출하지 않거나 거짓으로 제출한 경우 1) 자료를 제출하지 않은 경우 2) 자료를 거짓으로 제출한 경우	법 제75조 제4항제1호	100 200	200 400	400 800
나. 법 제16조제3항·제22조제5항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 재화 또는 서비스의 제공을 거부한 경우	법 제75조 제2항제1호	600	1,200	2,400
다. 법 제20조제1항·제2항을 위반하여 정보주체에게 같은 조 제1항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제2호	600	1,200	2,400
라. 법 제20조의2제1항을 위반하여 개인정보의 이용·제공 내역이나 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 통지하지 않은 경우	법 제75조 제2항제3호	600	1,200	2,400
마. 법 제21조제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제4호	600	1,200	2,400

바. 법 제21조제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 분리하여 저장·관리하지 않은 경우	법 제75조 제4항제2호	200	400	800
사. 법 제22조제1항부터 제3항까지(법 제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 동의를 받은 경우	법 제75조 제4항제3호	200	400	800
아. 법 제23조제2항·제24조제3항·제25조제6항(법 제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·제29조(법 제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제5호	600	1,200	2,400
자. 법 제23조제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 알리지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
차. 법 제24조의2제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 주민등록번호를 처리한 경우	법 제75조 제2항제7호	600	1,200	2,400
카. 법 제24조의2제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 암호화 조치를 하지 않은 경우	법 제75조 제2항제8호	600	1,200	2,400
타. 법 제24조의2제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체가 주민등록번호를 사용하지 않을 수 있는 방법을 제공하지 않은 경우	법 제75조 제2항제9호	600	1,200	2,400
파. 법 제25조제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보처리기를 설치·운영한 경우	법 제75조 제2항제10호	600	1,200	2,400

하. 법 제25조제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보처리기기를 설치·운영한 경우	법 제75조 제1항제1호	1,000	2,000	4,000
거. 법 제25조의2제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 사람 또는 그 사람과 관련된 사물의 영상을 촬영한 경우	법 제75조 제2항제11호	600	1,200	2,400
너. 법 제25조의2제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 이동형 영상정보처리기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영한 경우	법 제75조 제1항제2호	1,000	2,000	4,000
더. 법 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서로 하지 않은 경우	법 제75조 제4항제4호	200	400	800
러. 법 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 않은 경우	법 제75조 제4항제5호	200	400	800
머. 법 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조 제2항제12호	600	1,200	2,400
버. 법 제26조제6항을 위반하여 위탁자의 동의를 받지 않고 제3자에게 다시 위탁한 경우	법 제75조 제3항제1호	400	800	1,600
서. 법 제27조제1항·제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 않은 경우	법 제75조 제4항제6호	200	400	800
어. 법 제28조의4제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 관련 기록을 작성하여 보관하지 않은 경우	법 제75조 제4항제7호	200	400	800

저. 법 제28조의5제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인을 알아볼 수 있는 정보가 생성되었음에도 이용을 중지하지 않거나 이를 회수·파기하지 않은 경우	법 제75조 제2항제13호	600	1,200	2,400
처. 법 제28조의8제4항(법 제26조제8항 및 제28조의11에 따라 준용되는 경우를 포함한다)을 위반하여 보호조치를 하지 않은 경우	법 제75조 제2항제14호	600	1,200	2,400
커. 법 제30조제1항 또는 제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리방침을 정하지 않거나 이를 공개하지 않은 경우	법 제75조 제4항제8호	200	400	800
터. 법 제31조제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 보호책임자를 지정하지 않은 경우	법 제75조 제4항제9호	200	400	800
퍼. 법 제31조의2제1항을 위반하여 국내대리인을 지정하지 않은 경우	법 제75조 제3항제2호	2,000		
허. 법 제32조의2제6항을 위반하여 인증을 받지 않았음에도 거짓으로 인증의 내용을 표시하거나 홍보한 경우	법 제75조 제2항제15호	600	1,200	2,400
고. 법 제33조제1항을 위반하여 영향평가를 하지 않거나 그 결과를 보호위원회에 제출하지 않은 경우	법 제75조 제2항제16호	600	1,200	2,400
노. 법 제34조제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제17호	600	1,200	2,400
도. 법 제34조제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 보호위원회 또는 전문기관에 신고하지 않은 경우	법 제75조 제2항제18호	600	1,200	2,400
로. 법 제35조제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 열람을 제한하거나 거절한 경우	법 제75조 제2항제19호	600	1,200	2,400

모. 법 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제4항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조 제4항제10 호	200	400	800
보. 법 제35조의3제1항에 따른 지정을 받지 않고 같은 항 제2호의 업무를 수행한 경우	법 제75조 제2항제20 호	600	1,200	2,400
소. 법 제35조의3제3항을 위반한 경우	법 제75조 제2항제21호	600	1,200	2,400
오. 법 제36조제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정정·삭제 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제22 호	600	1,200	2,400
조. 법 제37조제3항 또는 제5항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제23 호	600	1,200	2,400
초. 법 제37조의2제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정당한 사유 없이 정보주체의 요구에 따르지 않은 경우	법 제75조 제2항제24 호	600	1,200	2,400
코. 법 제45조제1항에 따른 자료를 정당한 사유 없이 제출하지 않거나 거짓으로 제출한 경우 1) 자료를 제출하지 않은 경우 2) 자료를 거짓으로 제출한 경우	법 제75조 제4항제11 호	100 200	200 400	400 800
토. 법 제45조제2항에 따른 출입·조사·열람을 정당한 사유 없이 거부·방해 또는 기피한 경우	법 제75조 제4항제12 호	200	400	800
포. 법 제63조제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 관계 물품·서류 등 자료를 제출하지 않거나 거짓으로 제출한 경우	법 제75조 제2항제25 호			

1) 자료를 제출하지 않은 경우		300	600	1,200
2) 자료를 거짓으로 제출한 경우		600	1,200	2,400
호. 법 제63조제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 출입·검사를 거부·방해 또는 기피한 경우	법 제75조 제2항제26호	600	1,200	2,400
구. 법 제64조제1항에 따른 시정조치 명령에 따르지 않은 경우	법 제75조 제2항제27호	600	1,200	2,400

Chapter



개인정보 보호법 관련 고시



[시행 2023. 9. 22.] [개인정보보호위원회고시 제2023-6호, 2023. 9. 22., 일부개정]

제1장 총칙

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제29조와 같은 법 시행령(이하 "령"이라 한다) 제16조제2항, 제30조 및 제30조의2에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성된 시스템을 말한다.
2. "이용자"란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
3. "접속기록"이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
4. "정보통신망"이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
5. "P2P(Peer to Peer)"란 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.
6. "공유설정"이란 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
7. "모바일 기기"란 무선망을 이용할 수 있는 스마트폰, 태블릿 컴퓨터 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
8. "비밀번호"란 정보주체 및 개인정보취급자 등이 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
9. "생체정보"란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기

위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

10. "생체인식정보"란 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
11. "인증정보"란 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속을 요청하는 자의 신원을 검증하는데 사용되는 정보를 말한다.
12. "내부망"이란 인터넷망 차단, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
13. "위험도 분석"이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
14. "보조저장매체"란 이동형 하드디스크(HDD), 유에스비(USB)메모리 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 연결·분리할 수 있는 저장매체를 말한다.

제2장 개인정보의 안전성 확보조치

제3조(안전조치의 적용 원칙) 개인정보처리자는 처리하는 개인정보의 보유 수, 유형 및 정보주체에게 미치는 영향 등을 고려하여 스스로의 환경에 맞는 개인정보의 안전성 확보에 필요한 조치를 적용하여야 한다.

제4조(내부 관리계획의 수립·시행 및 점검) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.

1. 개인정보 보호 조직의 구성 및 운영에 관한 사항
2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
3. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
5. 접근 권한의 관리에 관한 사항
6. 접근 통제에 관한 사항
7. 개인정보의 암호화 조치에 관한 사항
8. 접속기록 보관 및 점검에 관한 사항
9. 악성프로그램 등 방지에 관한 사항
10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항
11. 물리적 안전조치에 관한 사항
12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
13. 위험 분석 및 관리에 관한 사항

14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
 15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항
 16. 그 밖에 개인정보 보호를 위하여 필요한 사항
- ② 개인정보처리자는 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시하여야 한다.
1. 교육목적 및 대상
 2. 교육 내용
 3. 교육 일정 및 방법
- ③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.
- ④ 개인정보 보호책임자는 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상 점검·관리 하여야 한다.

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.

- ② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.
- ③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
- ④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.
- ⑤ 개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.
- ⑥ 개인정보처리자는 정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 한다.

제6조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한
 2. 개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응
- ② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를

처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.

- ③ 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.
- ④ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.
- ⑤ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.
- ⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자는 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단 조치를 하여야 한다. 다만, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치를 하여야 한다.

제7조(개인정보의 암호화) ① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

- ② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

- 1. 주민등록번호
- 2. 여권번호
- 3. 운전면허번호
- 4. 외국인등록번호
- 5. 신용카드번호
- 6. 계좌번호
- 7. 생체인식정보

- ③ 개인정보처리자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.

- 1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우
- 2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)

가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과

나. 암호화 미적용시 위험도 분석에 따른 결과

- ④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.
- ⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.
- ⑥ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자의

개인정보처리시스템에 대한 접속기록을 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다.

- 1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
 - 2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우
 - 3. 개인정보처리자로서 「전기통신사업법」제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우
- ② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.
- ③ 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.

제9조(악성프로그램 등 방지) ① 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

- 1. 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지
 - 2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치
- ② 개인정보처리자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.

- 제10조(물리적 안전조치)** ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.
- ② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
- ③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

- 제11조(재해·재난 대비 안전조치)** 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 다음 각 호의 조치를 하여야 한다.
1. 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검
 2. 개인정보처리시스템 백업 및 복구를 위한 계획을 마련

- 제12조(출력·복사시 안전조치)** ① 개인정보처리자는 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.
- ② 개인정보처리자는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.

- 제13조(개인정보의 파기)** ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.
1. 완전파괴(소각·파쇄 등)
 2. 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제
 3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
- ② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.
1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
 2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제
- ③ 기술적 특성으로 제1항 및 제2항의 방법으로 파기하는 것이 현저히 곤란한 경우에는 법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치를 하여야 한다.

제3장 공공시스템 운영기관 등의 개인정보 안전성 확보조치

제14조(공공시스템운영기관의 안전조치 기준 적용) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리시스템 중에서 개인정보보호위원회(이하 "보호위원회"라 한다)가 지정하는 개인정보처리시스템(이하 "공공시스템"이라 한다)을 운영하는 공공기관(이하 "공공시스템 운영기관"이라 한다)은 제2장의 개인정보의 안전성 확보 조치 외에 이 장의 조치를 하여야 한다.

1. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 단일 시스템을 구축하여 다른 기관이 접속하여 이용할 수 있도록 한 단일접속 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우
 - 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
 - 나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
 - 다. 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보를 처리하는 시스템
 2. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 표준이 되는 시스템을 개발하여 다른 기관이 운영할 수 있도록 배포한 표준배포 시스템으로서 대국민 서비스를 위한 행정업무 또는 민원업무 처리용으로 사용하는 경우
 3. 기관의 고유한 업무 수행을 지원하기 위하여 기관별로 운영하는 개별 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우
 - 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
 - 나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
 - 다. 「주민등록법」에 따른 주민등록정보시스템과 연계하여 운영되는 시스템
 - 라. 총 사업비가 100억원 이상인 시스템
- ② 제1항에도 불구하고 보호위원회는 다음 각 호의 어느 하나에 해당하는 개인정보처리시스템에 대하여는 공공시스템으로 지정하지 않을 수 있다.
1. 체계적인 개인정보 검색이 어려운 경우
 2. 내부적 업무처리만을 위하여 사용되는 경우
 3. 그 밖에 개인정보가 유출될 가능성이 상대적으로 낮은 경우로서 보호위원회가 인정하는 경우

제15조(공공시스템운영기관의 내부 관리계획의 수립·시행) 공공시스템운영기관은 공공시스템 별로 다음 각 호의 사항을 포함하여 내부 관리계획을 수립하여야 한다.

1. 영 제30조의2제4항에 따른 관리책임자(이하 "관리책임자"라 한다)의 지정에 관한 사항
2. 관리책임자의 역할 및 책임에 관한 사항
3. 제4조제1항제3호에 관한 사항 중 개인정보취급자의 역할 및 책임에 관한 사항
4. 제4조제1항제4호부터 제6호까지 및 제8호에 관한 사항
5. 제16조 및 제17조에 관한 사항

제16조(공공시스템운영기관의 접근 권한의 관리) ① 공공시스템운영기관은 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소하려는 때에는 인사정보와 연계하여야 한다.

- ② 공공시스템운영기관은 인사정보에 등록되지 않은 자에게 제5조제4항에 따른 계정을 발급해서는 안된다. 다만, 긴급상황 등 불가피한 사유가 있는 경우에는 그러하지 아니하며, 그 사유를 제5조제3항에 따른 내역에 포함하여야 한다.
- ③ 공공시스템운영기관은 제5조제4항에 따른 계정을 발급할 때에는 개인정보 보호 교육을 실시하고, 보안 서약을 받아야 한다.
- ④ 공공시스템운영기관은 정당한 권한을 가진 개인정보취급자에게만 접근 권한이 부여·관리되고 있는지 확인하기 위하여 제5조제3항에 따른 접근 권한 부여, 변경 또는 말소 내역 등을 반기별 1회 이상 점검하여야 한다.
- ⑤ 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 "공공시스템이용기관"이라 한다)은 소관 개인정보취급자의 계정 발급 등 접근 권한의 부여·관리를 직접하는 경우 제2항부터 제4항까지의 조치를 하여야 한다.

제17조(공공시스템운영기관의 접속기록의 보관 및 점검) ① 공공시스템 접속기록 등을 자동화된 방식으로 분석하여 불법적인 개인정보 유출 및 오용·남용 시도를 탐지하고 그 사유를 소명하도록 하는 등 필요한 조치를 하여야 한다.

② 공공시스템운영기관은 공공시스템이용기관이 소관 개인정보취급자의 접속기록을 직접 점검할 수 있는 기능을 제공하여야 한다.

제18조(재검토 기한) 개인정보보호위원회는 「행정규제기본법」 제8조 및 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2023년 9월 15일을 기준으로 매 3년이 되는 시점(매 3년째의 9월 14일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2023-6호, 2023.09.22.>

이 고시는 발령한 날부터 시행한다. 다만, 다음 각 호의 개정규정은 각 호의 구분에 해당하는 개인정보처리자에 대해서는 2024년 9월 15일부터 시행한다.

1. 제5조제6항, 제7조제6항, 제8조제2항, 제11조의 개정규정 : 종전의 「(개인정보보호위원회) 개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회고시 제2021-3호) 적용대상인 개인정보처리자
2. 제7조제4항, 제12조제2항의 개정규정 및 제5조제6항 중 정보주체에 관한 개정규정 : 종전의 「(개인정보보호위원회) 개인정보의 안전성 확보조치 기준」(개인정보보호위원회고시 제2021-2호) 적용대상인 개인정보처리자
3. 제14조부터 제17조까지의 개정규정 : 공공시스템운영기관과 공공시스템이용기관

[시행 2024. 1. 4.] [개인정보보호위원회고시 제2024-1호, 2024. 1. 4., 일부개정]

제1장 총칙

제1조(목적) 이 지침은 「개인정보 보호법」(이하 "법"이라 한다) 제12조제1항에 따른 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정함을 목적으로 한다.

제2조(용어의 정의) 이 지침에서 사용하는 용어의 뜻은 다음과 같다.

1. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
2. "개인정보처리자"란 업무를 목적으로 법 제2조제4호에 따른 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 모든 공공기관, 법인·단체, 개인 등을 말한다.
3. "공공기관"이란 법 제2조제6호 및 「개인정보 보호법 시행령」(이하 "령"이라 한다) 제2조에 따른 기관을 말한다.
4. "친목단체"란 학교, 지역, 기업, 인터넷 커뮤니티 등을 단위로 구성되는 것으로서 자원봉사, 취미, 정치, 종교 등 공통의 관심사나 목표를 가진 사람간의 친목도모를 위한 각종 동창회, 동호회, 향우회, 반상회 및 동아리 등의 모임을 말한다.
5. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항 또는 제3항에 해당하는 자를 말한다.
6. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
7. "개인정보처리시스템"이란 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
8. "고정형 영상정보처리기기"란 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 영 제3조제1항에 따른 폐쇄회로 텔레비전 및 네트워크 카메라를 말한다.
- 8의2. "이동형 영상정보처리기기"란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(據置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 영 제3조제2항에 따른 착용형, 휴대형, 부착·거치형 장치를 말한다.
9. "개인영상정보"란 법 제2조제1호에 따른 개인정보 중 고정형 영상정보처리기기 또는 이동형 영상정보처리기기에 의하여 촬영·처리되는 영상 형태의 개인정보를 말한다.
10. "고정형영상정보처리기기운영자"란 법 제25조제1항 각 호에 따라 고정형 영상정보처리기기를 설치·운영하는 자를 말한다.

10의2. "이동형영상정보처리기기운영자"란 법 제25조의2제1항 각 호에 따라 업무를 목적으로 이동형 영상정보처리기기를 운영하는 자를 말한다.

11. "공개된 장소"란 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 또는 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.

제3조(적용범위) 이 지침은 전자적 파일과 인쇄물, 서면 등 모든 형태의 개인정보파일을 운용하는 개인정보처리자에게 적용된다.

제4조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성과 최신성을 유지하도록 하여야 하고, 개인정보를 처리하는 과정에서 고의 또는 과실로 부당하게 변경 또는 훼손되지 않도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 그에 상응하는 적절한 기술적·관리적 및 물리적 보호조치를 통하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차와 방법 등을 마련하여야 한다.

⑥ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하는 경우에도 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

⑦ 개인정보처리자는 개인정보를 적법하게 수집한 경우에도 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적 달성을 할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.

⑧ 개인정보처리자는 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제5조(다른 지침과의 관계) 중앙행정기관의 장이 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하는 경우에는 이 지침에 부합되도록 하여야 한다.

제2장 개인정보 처리 기준

제1절 개인정보의 처리

제6조(개인정보의 수집·이용) ① 개인정보의 "수집"이란 정보주체로부터 직접 이름,

주소, 전화번호 등의 개인정보를 제공받는 것뿐만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.

② 개인정보처리자는 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체로부터 사전에 동의를 받은 경우
2. 법률에서 개인정보를 수집·이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우
3. 법령에서 개인정보처리자에게 구체적인 의무를 부과하고 있고, 개인정보처리자가 개인정보를 수집·이용하지 않고는 그 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
4. 공공기관이 개인정보를 수집·이용하지 않고는 법령 등에서 정한 소관 업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우
5. 개인정보를 수집·이용하지 않고는 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 곤란한 경우
6. 명백히 정보주체 또는 제3자(정보주체를 제외한 그 밖의 모든 자를 말한다)의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
7. 개인정보처리자가 법령 또는 정보주체와의 계약 등에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집·이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니한 경우에 한한다.
8. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

③ 개인정보처리자는 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 "명함등"이라 함)를 제공받음으로써 개인정보를 수집하는 경우 명함등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

④ 개인정보처리자는 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 "인터넷 홈페이지등"이라 함)에서 개인정보를 수집하는 경우 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

⑤ 개인정보처리자는 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인의 개인정보를 수집·이용할 수 있다.

⑥ 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」에 따른 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집·이용할 수 있다.

제7조(개인정보의 제공) ① 개인정보의 "제공"이란 개인정보의 저장 매체나 개인정보가 담긴 출력물, 책자 등을 물리적으로 이전하거나 네트워크를 통한 개인정보의 전송,

개인정보에 대한 제3자의 접근권한 부여, 개인정보처리자와 제3자의 개인정보 공유 등 개인정보의 이전 또는 공동 이용 상태를 초래하는 모든 행위를 말한다.

- ② 법 제17조의 "제3자"란 정보주체와 정보주체에 관한 개인정보를 수집·보유하고 있는 개인정보처리자를 제외한 모든 자를 의미하며, 정보주체의 대리인(명백히 대리 범위 내에 있는 것에 한한다)과 법 제26조제2항에 따른 수탁자는 제외한다(이하 같다).
- ③ 개인정보처리자가 법 제17조제2항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

- 제8조(개인정보의 목적 외 이용·제공)** ① 개인정보처리자가 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다.
- ② 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 자는 해당 개인정보를 제공받는 자와 개인정보의 안전성 확보 조치에 관한 책임관계를 명확히 하여야 한다.
 - ③ 개인정보처리자가 법 제18조제3항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

- 제9조(개인정보 수집 출처 등 통지)** ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정당한 사유가 없는 한 정보주체의 요구가 있는 날로부터 3일 이내에 법 제20조제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
- 1. 통지를 요구하는 대상이 되는 개인정보가 법 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
 - 2. 통지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
- ② 개인정보처리자는 제1항 단서에 따라 제1항 전문에 따른 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 정보주체의 요구가 있는 날로부터 3일 이내에 그 거부의 근거와 사유를 정보주체에게 알려야 한다.

- 제10조(개인정보의 파기방법 및 절차)** ① 개인정보처리자는 개인정보의 보유 기간이 경과하거나 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5일 이내에 그 개인정보를 파기하여야 한다.
- ② 영 제16조제1항제1호의 '복원이 불가능한 방법'이란 현재의 기술수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말한다.

- ③ 개인정보처리자는 개인정보의 파기에 관한 사항을 기록·관리하여야 한다.
- ④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다.
- ⑤ 개인정보처리자 중 공공기관의 개인정보파일 파기에 관하여는 제55조 및 제56조를 적용한다.

제11조(법령에 따른 개인정보의 보존) ① 개인정보처리자가 법 제21조제1항 단서에 따라 법령에 근거하여 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 물리적 또는 기술적 방법으로 분리하여서 저장·관리하여야 한다.

- ② 제1항에 따라 개인정보를 분리하여 저장·관리하는 경우에는 개인정보 처리방침 등을 통하여 법령에 근거하여 해당 개인정보 또는 개인정보파일을 저장·관리한다는 점을 정보주체가 알 수 있도록 하여야 한다.

제12조(동의를 받는 방법 등) ① 개인정보처리자가 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 법 제22조제1항에 따라 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.

- ② 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 다음 각 호의 조건을 모두 충족해야 한다.

1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것
2. 동의를 받으려는 내용이 구체적이고 명확할 것
3. 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것
4. 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것

- ③ 개인정보처리자는 법 제22조제1항 각 호의 어느 하나에 해당하는 경우에는 동의 사항을 구분하여 각각 동의를 받아야 한다.

1. ~ 5. 삭제

- ④ 개인정보처리자는 제3항에 대하여 개인정보를 처리하고자 하는 경우에는 정보주체에게 동의 또는 동의 거부를 선택할 수 있음을 명시적으로 알려야 한다.

- ⑤ 개인정보처리자는 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보처리방침에 공개하거나 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(이하 "서면등의 방법"이라 한다)으로 정보주체에게 알려야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.

- ⑥ 개인정보처리자가 영 제17조제2항제2호의 규정에 따라 전화에 의한 동의와 관련하여 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.

- ⑦ 개인정보처리자가 친목단체를 운영하기 위하여 다음 각 호의 어느 하나에 해당하는 개인정보를 수집하는 경우에는 정보주체의 동의 없이 개인정보를 수집·이용할 수 있다.

1. 친목단체의 가입을 위한 성명, 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항
2. 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부현황에 관한 사항

3. 친목단체의 활동에 대한 구성원의 참석여부 및 활동내용에 관한 사항
4. 기타 친목단체의 구성원 상호 간의 친교와 화합을 위해 구성원이 다른
구성원에게 알리기를 원하는 생일, 취향 및 가족의 애경사 등에 관한 사항
- ⑧ 개인정보처리자가 정보주체의 동의를 받기 위하여 동의서를 작성하는 경우에는
개인정보 처리 동의 안내서를 준수하여야 한다.

제13조(법정대리인의 동의) ① 영 제17조의2제1항에 따라 개인정보처리자가
법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처,
법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다.

② 개인정보처리자는 법 제22조의2제2항에 따라 수집한 법정대리인의 개인정보를
법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의
거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 5일
이내에 파기해야 한다.

제14조(정보주체의 사전 동의를 받을 수 없는 경우) 개인정보처리자가 법
제15조제1항제5호 및 법 제18조제2항제3호에 따라 정보주체의 사전 동의 없이
개인정보를 수집·이용 또는 제공한 경우 해당 사유가 해소된 때에는 개인정보의
처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집·이용
또는 제공한 사실과 그 사유 및 이용내역을 알려야 한다.

제15조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보취급자를 업무상
필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리
범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.

② 개인정보처리자는 개인정보 처리시스템에 대한 접근권한을 업무의 성격에 따라
해당 업무수행에 필요한 최소한의 범위로 업무담당자에게 차등 부여하고 접근권한을
관리하기 위한 조치를 취해야 한다.

③ 개인정보처리자는 개인정보취급자에게 보안서약서를 제출하도록 하는 등 적절한
관리·감독을 해야 하며, 인사이동 등에 따라 개인정보취급자의 업무가 변경되는
경우에는 개인정보에 대한 접근권한을 변경 또는 말소해야 한다.

제2절 개인정보 처리의 위탁

제16조(수탁자의 선정 시 고려사항) 개인정보의 처리 업무를 위탁하는 개인정보처리자
(이하 "위탁자"라 한다)가 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라
한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등
개인정보 처리 및 보호 역량을 종합적으로 고려하여야 한다.

제17조(개인정보 보호 조치의무) 수탁자는 위탁받은 개인정보를 보호하기 위하여
「개인정보의 안전성 확보조치 기준 고시」에 따른 관리적·기술적·물리적 조치를
하여야 한다.

제3절 개인정보 처리방침 작성

제18조(개인정보 처리방침의 작성기준 등) ① 개인정보처리자가 개인정보 처리방침을 작성하는 때에는 법 제30조제1항 각 호 및 영 제31조제1항 각 호의 사항을 명시적으로 구분하되, 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.

② 개인정보처리자는 처리하는 개인정보가 개인정보의 처리 목적에 필요한 최소한이라는 점을 밝혀야 한다.

제19조(개인정보 처리방침의 기재사항) 개인정보처리자가 개인정보 처리방침을 작성할 때에는 법 제30조제1항에 따라 다음 각 호의 사항을 모두 포함하여야 한다.

1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목
3. 개인정보의 처리 및 보유 기간
4. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
5. 영 제14조의2제2항에 따라 개인정보의 추가적인 이용 또는 제공이 지속적으로 발생하는 경우 같은 조 제1항 각 호의 고려사항에 대한 판단 기준(해당되는 경우에만 정한다)
6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당되는 경우에만 정한다)
7. 개인정보의 파기절차 및 파기방법(법 제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
8. 법 제23조제3항에 따른 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정한다)
9. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
10. 법 제28조의2 및 제28조의3에 따른 가명정보의 처리 등에 관한 사항(해당되는 경우에만 정한다)
11. 영 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항
12. 개인정보 처리방침의 변경에 관한 사항
13. 법 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
14. 법 제31조의2제1항에 따라 국내대리인을 지정하는 경우 국내대리인의 성명, 주소, 전화번호 및 전자우편 주소(해당되는 경우에만 정한다)
15. 개인정보의 열람, 정정·삭제, 처리정지 요구권 등 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
16. 개인정보의 열람청구를 접수·처리하는 부서
17. 정보주체의 권익침해에 대한 구제방법

제20조(개인정보 처리방침의 공개) ① 개인정보처리자가 법 제30조제2항에 따라

개인정보 처리방침을 수립하는 경우에는 인터넷 홈페이지를 통해 지속적으로 게재하여야 하며, 이 경우 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

- ② 개인정보처리자가 인터넷 홈페이지를 운영하지 않는 경우 또는 인터넷 홈페이지 관리상의 하자가 있는 경우에는 영 제31조제3항 각 호의 어느 하나 이상의 방법으로 개인정보 처리방침을 공개하여야 한다. 이 경우에도 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.
- ③ 개인정보처리자가 영 제31조제3항제3호의 방법으로 개인정보 처리방침을 공개하는 경우에는 간행물·소식지·홍보지·청구서 등이 발행될 때마다 계속하여 게재하여야 한다.

제21조(개인정보 처리방침의 변경) 개인정보처리자가 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

제4절 개인정보 보호책임자

제22조(개인정보 보호책임자의 공개) ① 개인정보처리자가 개인정보 보호책임자를 지정하거나 변경하는 경우 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 공개하여야 한다.

- ② 개인정보처리자는 개인정보 보호책임자를 공개하는 경우 개인정보 보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개하여야 한다. 이 경우 개인정보 보호책임자와 개인정보 보호 업무를 처리하는 담당자의 성명, 부서의 명칭, 전화번호 등 연락처를 함께 공개할 수 있다.

제23조(개인정보 보호책임자의 교육) 영 제32조제4항에 따라 보호위원회가 개설 운영할 수 있는 개인정보 보호책임자에 대한 교육의 내용은 다음 각 호와 같다.

1. 개인정보 보호 관련 법령 및 제도의 내용
2. 법 제31조제3항 및 영 제32조제1항 각 호의 업무수행에 필요한 사항
3. 그 밖에 개인정보처리자의 개인정보 보호를 위하여 필요한 사항

제24조(교육계획의 수립 및 시행) ① 보호위원회는 매년 초 해당 연도 개인정보 보호책임자 교육계획을 수립하여 시행한다.

- ② 보호위원회는 제1항의 교육계획에 따라 개인정보 처리 및 보호에 관한 전문성을 갖춘 단체에 개인정보 보호책임자 교육을 실시하게 할 수 있다.
- ③ 보호위원회는 개인정보 보호책임자가 지리적·경제적 여건에 구애받지 않고 편리하게 교육을 받을 수 있는 여건 조성을 위해 노력하여야 한다.

제5절 개인정보 유출 통지 및 신고 등

제25조(개인정보의 유출등) 개인정보의 분실·도난·유출(이하 "유출등"이라 한다)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말한다.

제26조(유출등의 통지시기 및 항목) ① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 된 때에는 72시간 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다.

1. 유출등이 된 개인정보의 항목
 2. 유출등이 된 시점과 그 경위
 3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
 4. 개인정보처리자의 대응조치 및 피해구제절차
 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 지체 없이 정보주체에게 알릴 수 있다.
1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우
 2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우
- ③ 개인정보처리자는 제1항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.
1. 정보주체에게 유출등이 발생한 사실
 2. 제1항의 통지항목 중 확인된 사항
- ④ 개인정보처리자는 개인정보 유출등의 사고를 인지하지 못해 유출등의 사고가 발생한 시점으로부터 72시간 이내에 해당 정보주체에게 개인정보 유출등의 통지를 하지 아니한 경우에는 실제 유출등의 사고를 알게 된 시점을 입증하여야 한다.

제27조(유출등의 통지방법) ① 개인정보처리자는 정보주체에게 제26조제1항 각 호의 사항을 통지할 때에는 서면등의 방법을 통하여 정보주체에게 알려야 한다.

- ② 개인정보처리자는 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 법 제34조제1항 각 호 외의 부분 단서에 따라 같은 항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 30일 이상 게시하여야 한다.

제28조(개인정보 유출등의 신고) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 제26조제1항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 한국인터넷진흥원에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.

1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
2. 민감정보, 고유식별정보가 유출등이 된 경우
3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우

② 제1항에 따른 신고는 별지 제1호서식에 따른 개인정보 유출등 신고서를 통하여 하여야 한다.

③ 개인정보처리자는 개인정보 포털(www.privacy.go.kr)을 통하여 유출등 신고를 할 수 있다.

④ 개인정보처리자는 제1항에 따른 신고를 하려는 경우로서 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 신고해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다.

제29조(개인정보 유출등 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출등 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출등 대응 매뉴얼」을 마련하여야 한다.

1. 법 제2조제6호에 따른 공공기관
2. 그 밖에 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자

② 제1항에 따른 개인정보 유출등 대응 매뉴얼에는 유출등 통지·조회 절차, 영업점·인터넷회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 개인정보처리자는 개인정보 유출등에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

제30조(개인정보 침해 사실의 신고 처리 등) ① 개인정보처리자의 개인정보 처리로 인하여 개인정보에 관한 권리 또는 이익을 침해받은 사람은 법 제62조제2항에 따른 개인정보침해 신고센터에 침해 사실을 신고할 수 있다.

② 제1항에 따른 개인정보침해 신고센터는 다음 각 호의 업무를 수행한다.

1. 개인정보 처리와 관련한 신고의 접수·상담

2. 개인정보 침해 신고에 대한 사실 조사·확인 및 관계자의 의견 청취
3. 개인정보처리자에 대한 개인정보 침해 사실 안내 및 시정 유도
4. 사실 조사 결과가 정보주체의 권리 또는 이익 침해 사실이 없는 것으로 판단되는 경우 신고의 종결 처리
5. 법 제43조에 따른 개인정보 분쟁조정위원회 조정 안내 등을 통한 고충 해소 지원

제6절 정보주체의 권리 보장

제31조(개인정보 열람 연기 사유의 소멸) ① 개인정보처리자가 법 제35조제3항 후문에 따라 개인정보의 열람을 연기한 후 그 사유가 소멸한 경우에는 정당한 사유가 없는 한 사유가 소멸한 날로부터 10일 이내에 열람하도록 하여야 한다.

② 정보주체로부터 영 제41조제1항제4호의 규정에 따른 개인정보의 제3자 제공 현황의 열람청구를 받은 개인정보처리자는 국가안보에 긴요한 사안으로 법 제35조제4항제3호마목의 규정에 따른 업무를 수행하는데 중대한 지장을 초래하는 경우, 제3자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정할 수 있다.

제32조(개인정보의 정정·삭제) ① 개인정보처리자가 법 제36조제1항에 따른 개인정보의 정정·삭제 요구를 받았을 때는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 정보주체의 정정·삭제 요구가 법 제36조제1항 단서에 해당하는 경우에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 삭제를 요구할 수 없는 근거법령의 내용을 정보주체에게 알려야 한다.

제33조(개인정보의 처리정지) ① 개인정보처리자가 정보주체로부터 법 제37조제1항에 따라 개인정보처리를 정지하도록 요구받은 때에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 개인정보 처리의 일부 또는 전부를 정지하여야 한다. 다만, 법 제37조제2항 단서에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

② 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 정당한 사유가 없는 한 처리정지의 요구를 받은 날로부터 10일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치를 취하고 그 결과를 정보주체에게 알려야 한다.

제34조(권리행사의 방법 및 절차) ① 개인정보처리자는 정보주체가 법 제38조제1항에 따른 열람등요구를 하는 경우에는 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보의 수집시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구할 수 없다.

② 제1항의 규정은 영 제46조에 따라 본인 또는 정당한 대리인임을 확인하고자 하는 경우와 영 제47조에 따른 수수료와 우송료의 정산에도 준용한다.

제3장 영상정보처리기기 설치·운영

제1절 총칙

제35조(적용범위) 이 장은 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자가 설치·운영하는 고정형 영상정보처리기기 또는 이동형 영상정보처리기기와 그 기기를 통하여 처리되는 개인영상정보를 대상으로 한다.

제2절 고정형 영상정보처리기기의 설치

제36조(고정형 영상정보처리기기 운영·관리 방침) ① 고정형영상정보처리기기운영자가 법 제25조제7항에 따라 고정형 영상정보처리기기 운영·관리 방침을 마련하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

② 고정형영상정보처리기기운영자가 법 제30조에 따른 개인정보 처리방침을 정할 때 고정형 영상정보처리기기 운영·관리에 관한 사항을 포함시킨 경우에는 제1항에 따른 고정형 영상정보처리기기 운영·관리 방침을 마련하지 아니할 수 있다.

제37조(관리책임자의 지정) ① 고정형영상정보처리기기운영자는 개인영상정보의 처리에 관한 업무를 총괄해서 책임질 관리책임자를 지정하여야 한다.

② 제1항의 관리책임자는 법 제31조제3항에 따른 개인정보 보호책임자의 업무에 준하여 다음 각 호의 업무를 수행한다.

1. 개인영상정보 보호 계획의 수립 및 시행
2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
4. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인영상정보 보호 교육 계획 수립 및 시행
6. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
7. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무

③ 법 제31조에 따른 개인정보 보호책임자는 관리책임자의 업무를 수행할 수 있다.

제38조(사전의견 수렴) 고정형 영상정보처리기기의 설치 목적 변경에 따른 추가 설치 등의 경우에도 영 제23조제1항에 따라 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

제39조(안내판의 설치) ① 고정형영상정보처리기기운영자는 정보주체가 고정형 영상정보처리기기가 설치·운영 중임을 쉽게 알아볼 수 있도록 법 제25조제4항 본문에 따라 다음 각 호의 사항을 기재한 안내판 설치 등 필요한 조치를 하여야 한다.

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 연락처
4. 고정형 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의

명칭 및 연락처

- ② 제1항에 따른 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 판독할 수 있게 설치되어야 하며, 이 범위 내에서 고정형영상정보처리기기운영자가 안내판의 크기, 설치위치 등을 자율적으로 정할 수 있다.
- ③ 공공기관의 장이 기관 내 또는 기관 간에 고정형 영상정보처리기기의 효율적 관리 및 정보 연계 등을 위해 용도별·지역별 고정형 영상정보처리기기를 물리적·관리적으로 통합하여 설치·운영(이하 ‘통합관리’라 한다)하는 경우에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 제1항에 따른 안내판에 기재하여야 한다.

제3절 이동형 영상정보처리기기의 운영

제39조의2(이동형 영상정보처리기기의 촬영 사실 표시) ① 이동형 영상정보처리기기로

사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우에는 불빛, 소리, 안내판, 안내서면, 안내방송 또는 그 밖에 이에 준하는 수단이나 방법으로 정보주체가 촬영 사실을 쉽게 알 수 있도록 표시하고 알려야 한다.

- ② 드론을 이용한 항공촬영 등 촬영 방법의 특성으로 인해 정보주체에게 촬영 사실을 알리기 어려운 경우에는 보호위원회가 이동형 영상정보처리기기의 촬영 사실 표시를 지원하기 위하여 구축·운영하는 인터넷 사이트에 촬영 사실 및 목적, 촬영 일시 및 장소 등의 사항을 공지하는 방법으로 알릴 수 있다.

제39조의3(이동형 영상정보처리기기 운영·관리 방침) ①

이동형영상정보처리기기운영자는 법 제25조의2제4항에 따라 영 제25조제1항을 준용하여 다음 각 호의 사항이 포함된 이동형 영상정보처리기기 운영·관리 방침을 마련하여야 한다.

1. 이동형 영상정보처리기기의 운영 근거 및 운영 목적
 2. 이동형 영상정보처리기기의 운영 대수
 3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
 4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
 5. 이동형영상정보처리기기운영자의 영상정보 확인 방법 및 장소
 6. 정보주체의 영상정보 열람 등 요구에 대한 조치
 7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
 8. 그 밖에 이동형 영상정보처리기기의 설치·운영 및 관리에 필요한 사항
- ② 이동형영상정보처리기기운영자가 제1항에 따라 이동형 영상정보처리기기 운영·관리 방침을 마련하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.
 - ③ 이동형영상정보처리기기운영자가 법 제30조에 따른 개인정보 처리방침을 정할 때 이동형 영상정보처리기기 운영·관리에 관한 사항을 포함시킨 경우에는 제1항에 따른 이동형 영상정보처리기기 운영·관리 방침을 마련하지 아니할 수 있다.

제4절 개인영상정보의 처리

제40조(개인영상정보 이용·제3자 제공 등 제한 등) 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 다음 각 호의 경우를 제외하고는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하여서는 아니 된다. 다만 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체에게 동의를 얻은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 필요한 경우로서 법 제28조의2 또는 제28조의3에 따라 가명처리한 경우
5. 개인영상정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우
10. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

제41조(보관 및 파기) ① 고정형영상정보처리기기운영자 또는

이동형영상정보처리기기운영자는 고정형 영상정보처리기기 또는 이동형 영상정보처리기기 운영·관리 방침에 명시한 보관 기간이 경과하거나 개인영상정보의 처리 목적 달성, 법 제2조제1호에 따른 가명정보의 처리 기간 경과 등 그 개인영상정보가 불필요하게 되었을 때에는 지체 없이 그 개인영상정보를 파기하여야 한다. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러하지 아니하다.

② 고정형영상정보처리기기운영자가 그 사정에 따라 보유 목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30일 이내로 한다.

③ 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.

1. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
2. 전자기적(電磁氣的) 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제

제42조(이용·제3자 제공·파기의 기록 및 관리) ① 고정형영상정보처리기기운영자

또는 이동형영상정보처리기기운영자는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하는 경우에는 다음 각 호의 사항을 기록하고 이를 관리하여야 한다.

1. 개인영상정보 파일의 명칭
 2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭
 3. 이용 또는 제공의 목적
 4. 법령상 이용 또는 제공근거가 있는 경우 그 근거
 5. 이용 또는 제공의 기간이 정해져 있는 경우에는 그 기간
 6. 이용 또는 제공의 형태
 7. 이용 또는 제공한 개인영상정보의 업무처리 담당자
- ② 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자가 개인영상정보를 파기하는 경우에는 다음 사항을 기록하고 관리하여야 한다.
1. 파기하는 개인영상정보 파일의 명칭
 2. 개인영상정보 파기 일시 (사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 관한 확인 시기)
 3. 개인영상정보 파기 담당자

제43조(영상정보처리기기 설치 및 운영 등의 위탁) ① 고정형영상정보처리기기운영자가 영 제26조제1항에 따라 고정형 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽게 확인할 수 있도록 영 제24조에 따른 안내판 및 영 제25조에 따른 고정형 영상정보처리기기 운영·관리 방침에 수탁자의 명칭 등을 공개하여야 한다.

② 이동형영상정보처리기기운영자가 법 제25조의2제4항에 따라 영 제26조를 준용하여 이동형 영상정보처리기기의 운영에 관한 사무를 제3자에게 위탁하는 경우에는 제39조의2에 따른 이동형 영상정보처리기기 운영·관리 방침에 수탁자의 명칭 등을 공개하여야 한다.

③ 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자가 영 제26조제1항에 따라 고정형 영상정보처리기기 또는 이동형 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁할 경우에는 그 사무를 위탁받은 자가 개인영상정보를 안전하게 처리하고 있는지를 관리·감독하여야 한다.

제5절 개인영상정보의 열람등 요구

제44조(정보주체의 열람등 요구) ① 정보주체는 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자가 처리하는 개인영상정보에 대하여 열람 또는 존재확인(이하 "열람등"이라 한다)을 해당 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자에게 요구할 수 있다. 이 경우 정보주체가 열람등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보에 한한다.

② 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자가 공공기관인 경우에는 해당 기관의 장에게 별지 제2호서식에 따른 개인영상정보 열람·존재확인 청구서(전자문서를 포함한다)로 하여야 한다.

③ 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 제1항에 따른 요구를 받았을 때에는 지체 없이 필요한 조치를 취하여야 한다. 이때에

고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인하여야 한다.

- ④ 제3항의 규정에도 불구하고 법 제35조제4항 각 호의 어느 하나에 해당하는 경우에는 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 정보주체의 개인영상정보 열람등 요구를 제한하거나 거부할 수 있다. 이 경우 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 10일 이내에 서면 등으로 제한 또는 거부 사유를 정보주체에게 통지하여야 한다.

1. ~ 3. 삭제

- ⑤ 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 제3항 및 제4항에 따른 조치를 취하는 경우 다음 각 호의 사항을 기록하고 관리하여야 한다.

1. 개인영상정보 열람등을 요구한 정보주체의 성명 및 연락처
2. 정보주체가 열람등을 요구한 개인영상정보 파일의 명칭 및 내용
3. 개인영상정보 열람등의 목적
4. 개인영상정보 열람등을 거부한 경우 그 거부의 구체적 사유
5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유
6. 개인영상정보 열람등의 업무처리 담당자

- ⑥ 삭제

제45조(개인영상정보 관리대장) 제42조제1항 및 제2항, 제44조제5항에 따른 기록 및 관리는 별지 제3호서식에 따른 ‘개인영상정보 관리대장’을 활용할 수 있다.

제46조(정보주체 이외의 자의 개인영상정보 보호) 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 제44조제2항에 따른 열람등 조치를 취하는 경우, 만일 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해의 우려가 있는 경우에는 해당되는 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 보호조치를 취하여야 한다.

제6절 개인영상정보 보호 조치

제47조(개인영상정보의 안전성 확보를 위한 조치) 고정형영상정보처리기기운영자 또는 이동형영상정보처리기기운영자는 개인영상정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 법 제29조 및 영 제30조제1항에 따라 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행. 다만, 1만명 미만의 정보주체의 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.
2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 (네트워크 카메라의

- 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장시 비밀번호 설정 등)
4. 처리기록의 보관 및 위조·변조 방지를 위한 조치 (개인영상정보의 생성 일시 및 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리 조치 등)
 5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

제48조(개인영상정보처리기기의 설치·운영에 대한 점검) ① 공공기관의 장이 고정형 영상정보처리기기를 설치·운영하는 경우에는 이 지침의 준수 여부에 대한 자체점검을 실시하여 다음 해 3월 31일까지 그 결과를 보호위원회에게 통보하고 영 제34조제3항에 따른 시스템에 등록하여야 한다. 이 경우 다음 각 호의 사항을 고려하여야 한다.

1. 고정형 영상정보처리기기의 운영·관리 방침에 열거된 사항
 2. 관리책임자의 업무 수행 현황
 3. 고정형 영상정보처리기기의 설치 및 운영 현황
 4. 개인영상정보 수집 및 이용·제공·파기 현황
 5. 위탁 및 수탁자에 대한 관리·감독 현황
 6. 정보주체의 권리행사에 대한 조치 현황
 7. 기술적·관리적·물리적 조치 현황
 8. 고정형 영상정보처리기 설치·운영의 필요성 지속 여부 등
- ② 공공기관의 장은 제1항과 제3항에 따른 고정형 영상정보처리기기 설치·운영에 대한 자체점검을 완료한 후에는 그 결과를 홈페이지 등에 공개하여야 한다.
- ③ 공공기관 외의 고정형영상정보처리기기운영자는 고정형 영상정보처리기기 설치·운영으로 인하여 정보주체의 개인영상정보의 침해가 우려되는 경우에는 자체점검 등 개인영상정보의 침해 방지를 위해 적극 노력하여야 한다.

제4장 공공기관 개인정보파일 등록·공개

제1절 총칙

제49조(적용대상) 이 장의 적용대상은 다음과 같다.

1. 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
2. 「국가인권위원회법」에 따른 국가인권위원회
3. 「공공기관의 운영에 관한 법률」에 따른 공공기관
4. 「지방공기업법」에 따른 지방공사 및 지방공단
5. 특별법에 의하여 설립된 특수법인
6. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교

제50조(적용제외) 이 장은 다음 각 호의 어느 하나에 해당하는 개인정보파일에 관하여는 적용하지 아니한다.

1. 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속기관을 포함한다)에서 관리하는 개인정보파일
2. 법 제32조제2항에 따라 적용이 제외되는 다음 각목의 개인정보파일
 - 가. 국가안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
 - 나. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국 관리에 관한 사항을 기록한 개인정보파일
 - 다. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
 - 라. 회의 참석 수당 지급, 자료·물품의 송부, 금전의 정산 등 단순 업무 수행을 위해 운영되는 개인정보파일로서 지속적 관리 필요성이 낮은 개인정보파일
 - 마. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
 - 바. 다른 법령에 따라 비밀로 분류된 개인정보파일
 - 사. 그 밖에 일회적 업무 처리만을 위해 수집된 개인정보파일로서 저장되거나 기록되지 않는 개인정보파일
3. 법 제58조제1항제2호에 따라 적용이 제외되는 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일
 - 가. ~ 다. 삭제
4. 영상정보처리기를 통하여 처리되는 개인영상정보파일
5. 삭제
6. 「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관이 금융업무 취급을 위해 보유하는 개인정보파일

제2절 개인정보파일의 등록주체와 절차

제51조(개인정보파일 등록 주체) ① 개인정보파일을 운용하는 공공기관의 개인정보 보호책임자는 그 현황을 보호위원회에 등록하여야 한다.

- ② 중앙행정기관, 광역자치단체, 특별자치시도, 기초자치단체는 보호위원회에 직접 등록하여야 한다.
- ③ 교육청 및 각급 학교 등은 교육부를 통하여 보호위원회에 등록하여야 한다.
- ④ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관을 통하여 보호위원회에 등록하여야 한다.

제52조(개인정보파일 등록 및 변경 신청) ① 개인정보파일을 운용하는 공공기관의 개인정보취급자는 해당 공공기관의 개인정보 보호책임자에게 개인정보파일 등록을 신청하여야 한다.

- ② 개인정보파일 등록 신청 사항은 다음의 각 호와 같다. 신청은 「개인정보 처리 방법에 관한 고시」(이하 이 조에서 "고시"라 한다) 제3조제2항에 따른 별지

제2호서식의 ‘개인정보파일 등록·변경등록 신청서’를 활용할 수 있다.

1. 개인정보파일을 운용하는 공공기관의 명칭
 2. 개인정보파일의 명칭
 3. 개인정보파일의 운영 근거 및 목적
 4. 개인정보파일에 기록되는 개인정보의 항목
 5. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
 6. 개인정보의 처리 방법
 7. 개인정보의 보유 기간
 8. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
 9. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서
 10. 개인정보의 열람 요구를 접수·처리하는 부서
 11. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유
 12. 법 제33조제1항에 따른 개인정보 영향평가를 받은 개인정보파일의 경우에는 그 영향평가의 결과
- ③ 개인정보취급자는 등록한 사항이 변경된 경우에는 고시 제3조제2항에 따른 별지 제2호서식의 ‘개인정보파일 등록·변경등록 신청서’를 활용하여 개인정보 보호책임자에게 변경을 신청하여야 한다.

제53조(개인정보파일 등록 및 변경 확인) ① 개인정보파일 등록 또는 변경 신청을 받은 개인정보 보호책임자는 등록·변경 사항을 검토하고 그 적정성을 판단한 후 보호위원회에 등록하여야 한다.

- ② 교육청 및 각급 학교 등의 개인정보 보호책임자는 교육부에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 교육부의 확인을 받아 보호위원회에 등록하여야 한다.
- ③ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 상위 관리기관의 확인을 받아 보호위원회에 등록하여야 한다.
- ④ 제1항부터 제3항의 등록은 60일 이내에 하여야 한다.

제54조(개인정보파일 표준목록 등록과 관리) ① 특별지방행정기관, 지방자치단체, 교육기관(학교 포함) 등 전국적으로 단일한 공통업무를 집행하고 있는 기관은 각 중앙행정기관에서 제공하는 ‘개인정보파일 표준목록’에 따라 등록해야 한다.

- ② 전국 단일의 공통업무와 관련된 개인정보파일 표준목록은 해당 중앙행정기관에서 등록·관리해야 한다.

제55조(개인정보파일의 파기) ① 공공기관은 개인정보파일의 보유기간 경과, 처리 목적 달성 등 개인정보파일이 불필요하게 되었을 때에는 지체 없이 그 개인정보파일을 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지

아니하다.

- ② 공공기관은 개인정보파일의 보유기간, 처리 목적 등을 반영한 개인정보 파기계획을 수립·시행하여야 한다. 다만, 영 제30조제1항제1호에 따른 내부 관리계획이 수립되어 있는 경우에는 내부 관리계획에 개인정보 파기계획을 포함하여 시행할 수 있다.
- ③ 개인정보취급자는 보유기간 경과, 처리 목적 달성 등 파기 사유가 발생한 개인정보파일을 선정하고, 별지 제4호서식에 따른 개인정보파일 파기요청서에 파기 대상 개인정보파일의 명칭, 파기방법 등을 기재하여 개인정보 보호책임자의 승인을 받아 개인정보를 파기하여야 한다.
- ④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하고 별지 제5호서식에 따른 개인정보파일 파기 관리대장을 작성하여야 한다.

제56조(개인정보파일 등록 사실의 삭제) ① 개인정보취급자는 제55조에 따라

개인정보파일을 파기한 경우, 법 제32조에 따른 개인정보파일의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청해야 한다.

- ② 개인정보파일 등록의 삭제를 요청받은 개인정보 보호책임자는 그 사실을 확인하고, 지체 없이 등록 사실을 삭제한 후 그 사실을 보호위원회에 통보한다.

제57조(등록·파기에 대한 개선권고) ① 공공기관의 개인정보 보호책임자는

제53조제1항에 따라 검토한 개인정보파일이 과다하게 운용되고 있다고 판단되는 경우에는 개선을 권고할 수 있다.

- ② 교육청 및 각급 학교, 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관의 개인정보 보호책임자는 제53조제2항 및 제3항에 따라 검토한 개인정보파일이 과다하게 운용된다고 판단되거나, 등록되지 않은 파일이 있는 것으로 확인되는 경우에는 개선을 권고할 수 있다.
- ③ 보호위원회는 개인정보파일의 등록사항과 그 내용을 검토하고 다음 각 호의 어느 하나에 해당되는 경우에는 법 제32조제3항에 따라 해당 공공기관의 개인정보 보호책임자에게 개선을 권고할 수 있다.
 - 1. 개인정보파일이 과다하게 운용된다고 판단되는 경우
 - 2. 등록하지 않은 개인정보파일이 있는 경우
 - 3. 개인정보파일 등록 사실이 삭제되었음에도 불구하고 개인정보파일을 계속 보유하고 있는 경우
 - 4. 개인정보 영향평가를 받은 개인정보파일을 보유하고 있음에도 그 결과를 등록사항에 포함하지 않은 경우
 - 5. 기타 법 제32조에 따른 개인정보파일의 등록 및 공개에 위반되는 사항이 있다고 판단되는 경우
- ④ 보호위원회는 제3항에 따라 개선을 권고한 경우에는 그 내용 및 결과에 대하여 보호위원회의 심의·의결을 거쳐 공표할 수 있다.
- ⑤ 보호위원회는 공공기관의 개인정보파일 등록·파기 현황에 대한 점검을 실시할 수 있다.

제3절 개인정보파일의 관리 및 공개

제58조(개인정보파일대장 작성) 공공기관은 1개의 개인정보파일에 1개의 개인정보파일대장을 작성해야 한다.

제59조(개인정보파일 이용·제공 관리) 공공기관은 법 제18조제2항 각 호에 따라 제3자가 개인정보파일의 이용·제공을 요청한 경우에는 각각의 이용·제공 가능 여부를 확인하고 별지 제6호서식의 ‘개인정보 목적 외 이용·제공대장’에 기록하여 관리해야 한다.

제60조(개인정보파일 보유기간의 산정) ① 보유기간은 전체 개인정보가 아닌 개별 개인정보의 수집부터 삭제까지의 생애주기로서 보유목적에 부합된 최소기간으로 산정하되, 개별 법령의 규정에 명시된 자료의 보존기간에 따라 산정해야 한다.
② 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의 협의를 거쳐 기관장의 결재를 통하여 산정해야 한다. 다만, 보유기간은 별표 1의 개인정보파일 보유기간 책정 기준표에서 제시한 기준과 「공공기록물 관리에 관한 법률 시행령」 제25조에 따른 기록관리기준표를 상회할 수 없다.
③ 삭제

제61조(개인정보파일 현황 공개 및 방법) ① 공공기관의 개인정보 보호책임자는 개인정보파일의 보유·파기현황을 주기적으로 조사하여 그 결과를 해당 공공기관의 개인정보 처리방침에 포함하여 관리해야 한다.
② 보호위원회는 개인정보파일 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개할 수 있다.
③ 보호위원회는 전 공공기관의 개인정보파일 등록 및 삭제 현황을 종합하여 매년 공개해야 하며, 개인정보파일 현황 공개에 관한 업무를 전자적으로 처리하기 위하여 정보시스템을 구축·운영할 수 있다.

제62조 삭제

제63조 삭제

부칙 <제2024-1호, 2024.01.04.>

이 고시는 고시한 날부터 시행한다.

개인정보파일 보유기간 책정 기준표

보유기간	대상 개인정보파일
영구	<ol style="list-style-type: none"> 1. 국민의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	<ol style="list-style-type: none"> 1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일
30년	<ol style="list-style-type: none"> 1. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
10년	<ol style="list-style-type: none"> 1. 관계 법령에 따라 5년 이상 10년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
5년	<ol style="list-style-type: none"> 1. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
3년	<ol style="list-style-type: none"> 1. 행정업무의 참고 또는 사실 증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일(단 다른 법령에서 증명서 발급 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름)
1년	<ol style="list-style-type: none"> 1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일

개인정보 유출등 신고서

기관명					
유출등이 된 개인정보 항목 및 규모					
유출등이 된 시점과 그 경위					
유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등					
개인정보처리자의 대응 조치 및 피해 구제절차					
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처					
유출등 신고 담당자		성명	부서	직위	연락처
	개인정보 보호책임자				
	담당자				

유출등 신고 접수기관	기관명	담당자명	연락처

개인영상정보(<input type="checkbox"/> 존재확인 <input type="checkbox"/> 열람) 청구서				처리기한
※ 아래 유의사항을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.				10일 이내
청 구 인	성 명		전 화 번 호	
	생년월일		정보주체와의 관계	
	주 소			
정보주체의 인적사항	성 명		전 화 번 호	
	생년월일			
	주 소			
청구내용 (구 체 적 으 로 요청하지 않 으면 처리가 곤란할 수 있 음)	영상정보 기록기간	(예 : 2011.01.01 18:30 ~ 2011.01.01 19:00)		
	영상정보 처리기기 설치장소	(예 : 00시 00구 00대로 0 인근 CCTV)		
	청구 목적 및 사유			
「표준 개인정보 보호지침」 제44조에 따라 위와 같이 개인영상정보의 존재 확인, 열람을 청구 합니다.				
<div style="text-align: center;"> 년 월 일 </div> <div style="text-align: right;"> 청구인 (서명 또는 인) </div> <div style="text-align: center;"> ○ ○ ○ ○ 귀하 </div>				
담당자의 청구인에 대한 확인 서명				

개인영상정보 관리대장

번호	구분	일시	파일명/ 형태	담당자	목적/ 사유	이용· 제공받는 제3자 /열람등 요구자	이용· 제공 근거	이용· 제공 형태	기간
1	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
2	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
3	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
4	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
5	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
6	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
7	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								

개인정보파일 파기 요청서

작성일		작성자	
파기 대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보 보호책임자)	
파기 장소			
파기 방법			
파기 수행자		입회자	
폐기 확인 방법			
백업 조치 유무			
매체 폐기 여부			

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[] 목적외 이용 [] 제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의 경우)	담당 자	소속	성명
		전화번호	
제공받는 기관의 명칭 (제3자 제공의 경우)		성명	소속
	담당 자	전화번호	
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			

3

개인정보 보호책임자 경력 인정에 관한 고시

[시행 2024. 4. 2.] [개인정보보호위원회고시 제2024-5호, 2024. 4. 2., 제정]

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다) 제31조제9항 및 같은 법 시행령(이하 "령"이라 한다) 별표 1에 따라 개인정보 보호책임자의 경력 인정에 필요한 세부 사항을 정함을 목적으로 한다.

제2조(자격의 인정) 법 제31조제9항 및 영 별표 1에 따른 개인정보 보호책임자의 경력 인정을 위한 자격 요건은 별표와 같다.

제3조(경력 인정을 위한 교육) 개인정보 보호위원회(이하 "보호위원회"라 한다)가 법 제7조의8제7호에 따라 개인정보 보호책임자의 역량을 강화하기 위하여 실시하는 개인정보 보호책임자의 경력 개발 및 직무 수행과 관련된 교육과정(이하 "개인정보 보호책임자 교육과정"이라 한다)을 이수한 경우에는 최대 3개월의 범위에서 개인정보 보호책임자의 개인정보 보호 경력으로 인정한다. 다만, 개인정보 보호책임자 교육과정에는 다음 각 호의 사항이 포함되어야 한다.

1. 개인정보 관련 법률·정책·제도 및 최신 이슈
2. 개인정보 보호책임자의 역할 및 업무 수행에 필요한 사항
3. 개인정보 처리단계별 관리 방안
4. 개인정보 보호 기술
5. 개인정보 유출사고 대응
6. 개인정보 보호 우수사례
7. 그 밖에 개인정보처리자의 개인정보 보호를 위하여 필요한 사항 등

제4조(재검토 기한) 보호위원회는 「행정규제기본법」 제8조에 따라 이 고시에 대하여 2025년 1월 1일을 기준으로 2년마다(매 2년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2024-5호, 2024.04.02.>

제1조(시행일) 이 고시는 발령한 날부터 시행한다.

제2조(교육의 경력 인정에 관한 경과조치) 이 고시 시행 4년 전부터 이 고시 시행 전까지 「개인정보 보호법」 제7조의8제7호에 따라 보호위원회가 주관하거나 위탁한 기관이 운영하는 교육과정(이 고시 제3조 각 호의 내용을 포함한 개인정보 보호책임자 교육과정으로 한정한다)을 이수한 경우 이 고시 제3조의 규정에 따라 개인정보 보호 경력 인정요건을 갖춘 것으로 본다.

[별표]

< 개인정보 보호책임자 경력 인정 자격 >

구분	경력 인정 자격	인정기간
개인정보보호 경력	<ul style="list-style-type: none"> ○ 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 제14조에 따른 정보보호 및 개인정보보호 관리체계 인증심사원 ○ 개인정보 영향평가에 관한 고시 제5조제2항에 따른 개인정보 영향평가 전문인력 ○ 「변호사법」 제4조에 따른 변호사 자격 취득자 	1년
정보보호, 정보기술 경력	○ 정보관리기술사, 컴퓨터시스템응용기술사	1년
	○ 정보보안기사, 정보처리기사	6개월

※ 각각의 자격을 보유한 경우에는 구분된 경력 내(개인정보보호, 정보보호·정보기술)에서는 하나의 자격만 인정하며, 구분된 경력별로 중복 인정은 가능함

4

개인정보 보호법 위반에 대한 과징금 부과 기준

[시행 2023. 9. 15.] [개인정보보호위원회고시 제2023-3호, 2023. 9. 15., 제정]

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다) 제64조의2제6항, 같은 법 시행령(이하 "령"이라 한다) 제60조의2 및 [별표 1의5]에 따른 과징금 부과에 필요한 세부 기준을 정함을 목적으로 한다.

제2조(정의) 이 고시에서 사용하는 용어의 뜻은 다음과 같다.

1. "위반행위"란 법을 위반하여 법 제64조의2제1항 각 호에 따른 과징금 부과 대상이 되는 행위를 말한다.
2. "기준금액"이란 과징금 산정의 기초로서 영 제60조의2제1항에 따른 전체 매출액(이하 "전체 매출액"이라 한다)에서 같은 조 제3항에 따른 위반행위와 관련이 없는 매출액(이하 "위반행위와 관련이 없는 매출액"이라 한다)을 제외한 매출액에 영 [별표 1의5] 제2호가목 1)에서 위반행위의 중대성 별로 정한 부과기준율(이하 "부과기준율"이라 한다)을 곱하여 산출한 금액 또는 영 제60조의2제2항 및 [별표 1의5] 제2호가목 2)에서 정한 금액을 말한다.
3. "1차 조정"이란 위반행위의 기간 및 횟수, 위반행위로 인하여 취득한 이익의 규모, 개인정보처리자의 업무 형태 및 규모를 고려하여 기준금액의 100분의 90의 범위에서 가중하거나 감경하는 것을 말한다.
4. "2차 조정"이란 다음 각 목의 사항(법 제64조의2제4항 각 호의 사항 중 기준금액 산정 및 1차 조정 단계에서 고려된 사항은 제외한다)을 종합적으로 고려하여 1차 조정을 거친 금액의 100분의 50의 범위에서 가중하거나 감경하는 것을 말한다.
 - 가. 개인정보 보호위원회(이하 "보호위원회"라 한다)와의 협조 등 위반행위를 시정하기 위한 조치 여부
 - 나. 위반행위로 인한 피해의 회복 및 피해 확산 방지 조치의 이행 여부
 - 다. 개인정보 보호 인증, 자율적인 보호 활동 등 개인정보 보호를 위한 노력
 - 라. 위반행위의 주도 여부
 - 마. 위반행위자가 위반행위 사실의 자진신고 여부
5. "부과과징금의 결정"이란 기준금액에 1차 조정과 2차 조정을 거친 금액이 위반행위자의 현실적 부담능력 등을 종합적으로 고려하여 과중하다고 인정되는 경우 등에 2차 조정을 거친 금액을 그 금액의 100분의 90의 범위에서 감경하거나 면제하는 것을 말한다.

제3조(위반기간의 산정) ① 위반기간은 위반행위의 개시일부터 종료일까지의 기간을 말한다. 다만, 위반행위가 과징금 부과처분을 명하는 보호위원회의 심의종결일까지 종료되지 아니한 경우에는 해당 사건에 대한 보호위원회의 심의종결일을 위반행위의 종료일로 본다.

- ② 제1항에 따른 위반기간을 산정하면서 위반행위의 개시일 또는 종료일이 불분명한 경우에는 위반행위자의 영업·재무 관련 자료, 임직원·정보주체 등의 진술, 동종·유사 업종을 영위하는 다른 개인정보처리자의 영업 및 거래실태·관행 등을 고려하여 이를 산정할 수 있다.

제4조(과징금 부과 여부의 결정) ① 본인의 행위가 위법하지 않은 것으로 잘못 인식할 만한 정당한 사유가 있는 경우에는 과징금을 부과하지 않는다.

- ② 다음 각 호의 어느 하나에 해당하는 경우에는 과징금을 부과하지 않을 수 있다.

다만, 본문에 따라 과징금 부과처분을 받지 않은 자가 그 결정이 있는 날부터 3년 이내에 같은 위반행위를 하는 경우에는 그렇지 않다.

1. 위반행위의 내용·정도가 경미하거나 사소한 부주의나 오류로 인한 위반행위인 경우
2. 정보주체에게 피해가 발생하지 아니하였거나 경미한 경우로서 위반행위자가 위반행위를 시정하고 법 제34조에 따른 개인정보 유출 등의 통지·신고를 위반하지 않은 경우

제5조(과징금의 부과기준) ① 과징금 부과금액은 법 제64조의2제4항 각 호에 따른 고려 사항과 이에 영향을 미치는 행위를 종합적으로 고려하여 기준금액에 1차 조정, 2차 조정, 부과과징금의 결정을 순차적으로 거쳐 산정한다.

- ② 하나의 행위가 2 이상의 위반행위에 해당하는 경우에는 각 위반행위 별로 산정된 과징금 중 가장 큰 금액을 기준으로 과징금을 부과한다.

제6조(기준금액) ① 기준금액은 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액에 부과기준율을 곱한 금액으로 정한다.

- ② 영 제60조의2제2항 각 호의 어느 하나에 해당하여 제1항을 적용할 수 없는 경우에는 영 [별표 1의5] 제2호가목 2)에 따라 기준금액을 정한다.

- ③ 다음 각 호의 경우에는 영 제60조의2제2항 각 호의 어느 하나에 해당하여 매출액이 없거나 매출액의 산정이 곤란한 경우로 본다.

1. 공공기관, 비영리법인, 비영리단체 등으로서 매출액을 산정하지 않고, 「법인세법」 제4조제3항제1호에 따른 수익사업에서 생기는 소득이 없는 경우
2. 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 결과 산정된 매출액이 없는 경우

제7조(매출액 산정기준 판단 시 고려사항) ① 전체 매출액은 총매출액에서 부가가치세, 매출할인, 매출환입, 매출에누리 등을 차감한 순매출액(업종의 특성에 따라 매출액에 준하는 영업수익 등을 사용하는 경우에는 영업수익 등을 말한다)으로 한다.

- ② 영 제60조의2제1항 단서에서 정한 직전 3개 사업연도 또는 해당사업연도는 위반행위의 종료일을 기준으로 판정한다.

- ③ 영 제60조의2제3항에 따라 보호위원회가 위반행위와 관련이 없는 매출액으로 인정하는 매출액의 판단 시에는 다음 각 호의 사항을 종합적으로 고려할 수 있다.

1. 재화·서비스의 종류·성질, 공급 또는 제공 방식 등에 따른 독자성과 부속성의 정도
2. 재화·서비스를 이용하는 정보주체가 별개의 재화·서비스로 합리적으로 인식 가능한 정도

3. 위반행위의 대상이 된 개인정보의 범주·특성
 4. 개인정보파일·개인정보처리시스템의 관리·운영 방식의 분리 또는 연계 여부 등 독자성의 정도
 5. 개인정보 처리방침 또는 이용약관·약관 등에서 규정한 재화·서비스의 범위
 6. 통계청장이 고시하는 「한국표준산업분류」상 분류 또는 위반행위자의 품목별 또는 업종별 매출액 등의 회계단위
 7. 그 밖에 제1호부터 제6호까지에 준하는 사항
- ④ 재화·서비스의 유형·이용 방식 등이 유사하면 공급 또는 제공되는 지역·범위 등에 관계없이 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 재화·서비스로 볼 수 있다.
- ⑤ 재화·서비스에 대한 매출액은 회계자료를 참고하여 정하되, 위반행위자가 매출액 산정자료를 가지고 있지 않거나 정당한 사유로 제출하지 못하는 경우에는 위반행위자 및 동종 유사 업종을 영위하는 다른 개인정보처리자의 과거 실적, 사업계획, 그 밖에 시장상황 등을 종합적으로 고려하여 매출액을 산정할 수 있다.

제8조(중대성의 판단) ① 영 [별표 1의5] 제2호가목 1) 및 2)에 따른 위반행위의 중대성의 정도는 [별표] 위반행위의 중대성 판단기준을 기준으로 정한다.

- ② 제1항에도 불구하고 [별표]에서 고려되지 않거나 [별표]와 다르게 고려할 사유(해당 사유가 가중 또는 감면사유와 중복되는 경우는 제외한다)가 있는 경우에는 위반행위의 중대성의 정도를 달리 정할 수 있다. 이 경우 그 사유를 의결서에 명시하여야 한다.

제9조(1차 조정) ① 위반행위자가 다음 각 호의 어느 하나에 해당하는 경우에는 기준금액에 다음 각 호와 같이 과징금을 가산한다.

1. 위반기간이 1년을 초과하는 경우
 - 가. 위반기간이 1년 초과 2년 이내인 경우 : 기준금액의 100분의 25에 해당하는 금액을 가산
 - 나. 위반기간이 2년을 초과하는 경우 : 기준금액의 100분의 50에 해당하는 금액을 가산
 2. 최근 3년간 법 제64조의2제1항 같은 호에 해당하는 행위로 1회 이상 과징금 부과처분을 받은 경우. 이 경우 위반횟수 기간의 계산은 과징금 부과처분을 받은 날과 그 처분 후 다시 해당 위반행위를 하여 적발된 날을 기준으로 한다.
 - 가. 1회 과징금 부과처분을 받은 경우 : 기준금액의 100분의 15에 해당하는 금액을 가산
 - 나. 2회 이상 과징금 부과처분을 받은 경우 : 기준금액의 100분의 30에 해당하는 금액을 가산
- ② 위반행위자가 다음 각 호의 어느 하나에 해당하는 경우에는 기준금액에 다음 각 호와 같이 과징금을 감경한다.
1. 위반행위로 인하여 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 경우 : 기준금액의 100분의 30 이하에 해당하는 금액을 감경

2. 위반행위자가 공공기관, 비영리법인, 비영리단체 또는 「중소기업기본법」 제2조에 따른 중소기업자인 경우 등 위반행위자의 업무 형태 및 규모에 비해 과중하다고 인정되는 경우 : 기준금액의 100분의 50 이하에 해당하는 금액을 감경
- ③ 제1항에서 정한 가중사유 또는 제2항에서 정한 감경사유가 2개 이상 해당되는 경우에는 가중금액을 합산하여 가중하거나 감경금액을 합산하여 감경하되 각 가중·감경의 범위는 기준금액의 100분의 90을 초과할 수 없다.

제10조(2차 조정) ① 위반행위자가 다음 각 호의 어느 하나에 해당하는 경우에는 1차 조정을 거친 금액에 다음 각 호와 같이 추가적으로 과징금을 가산할 수 있다.

1. 위반행위자 및 그 소속 임직원이 법 제63조제1항 및 제2항에 따른 물품·서류의 제출요구 또는 검사를 거부하거나 증거인멸, 은폐, 조작, 허위의 정보제공 등의 방법으로 조사를 방해하거나 관련 정보주체 등에게 허위로 진술하도록 요청한 경우 : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 가산
2. 다수의 위반행위자가 관련된 상황에서 위반행위를 주도하거나 선도한 경우 : 1차 조정을 거친 금액의 100분의 20 이하에 해당하는 금액을 가산
- ② 위반행위자가 다음 각 호의 어느 하나에 해당하는 경우에는 1차 조정을 거친 금액에 다음 각 호와 같이 추가적으로 과징금을 감경할 수 있다.
 1. 보호위원회와의 협조 등 위반행위를 시정하기 위하여 조치한 경우로서 다음 각 목의 어느 하나에 해당하는 경우
 - 가. 과징금의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우 : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 감경
 - 나. 보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우 : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 감경
 2. 개인정보 분쟁조정, 민사조정 등을 통해 정보주체에게 발생한 피해에 대한 원상회복, 손해배상 또는 이에 상당하는 필요한 피해의 회복 및 피해 확산 방지 조치를 이행한 경우(다만, 법 제39조의7에 따른 손해배상책임의 이행을 위한 보험 등의 가입은 제외한다) : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 감경
 3. 개인정보 보호 인증, 자율적인 보호 활동 등 개인정보 보호를 위하여 노력한 경우로서 다음 각 목의 어느 하나에 해당하는 경우
 - 가. 개인정보 보호를 위해 보호위원회가 인정하는 인증을 받은 경우 : 1차 조정을 거친 금액의 100분의 50 이하에 해당하는 금액을 감경
 - 나. 개인정보 보호 자율규제 규약을 이행하는 등 개인정보 보호 활동을 성실히 수행한 것으로 확인된 경우 : 1차 조정을 거친 금액의 100분의 40 이하에 해당하는 금액을 감경
 - 다. 개인정보 처리방침의 평가 또는 개인정보 보호수준 평가의 결과가 상위 등급인 경우, 개인정보 영향평가(다만, 법 제33조제1항에 따라 개인정보

영향평가를 해야 하는 경우는 제외한다)를 하는 등 개인정보 보호 활동을 성실히 수행한 것으로 확인된 경우 : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 감경

4. 위반행위 사실을 자진신고(법 제34조제3항 전단에 따른 신고는 제외한다)한 경우 : 1차 조정을 거친 금액의 100분의 30 이하에 해당하는 금액을 감경

5. 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과징금을 줄일 필요가 있다고 인정되는 경우 : 1차 조정을 거친 금액의 100분의 10 이하에 해당하는 금액을 감경

③ 제1항에서 정한 가중사유 또는 제2항에서 정한 감경사유가 2개 이상 해당되는 경우에는 가중금액을 합산하여 가중하거나 감경금액을 합산하여 감경하되 각 가중·감경의 범위는 1차 조정을 거친 금액의 100분의 50을 초과할 수 없다.

제11조(부과과징금의 결정) ① 위반행위자의 현실적인 부담능력, 위반행위자가 속한 시장·산업 여건 등을 고려하여 제10조에 따라 산정된 과징금이 과중하다고 인정되는 경우에는 다음 각 호와 같이 해당 금액의 100분의 90 범위에서 감경할 수 있다.

1. 위반행위자의 자산, 자기자본 등 재무상황에 비추어 위반행위자가 과징금을 부담할 능력이 현저히 부족하다고 객관적으로 인정되는 경우
2. 경제위기 등으로 위반행위자가 속한 시장·산업 여건이 현저하게 변동되거나 지속적으로 악화된 상태인 경우

② 다음 각 호의 어느 하나에 해당하는 경우에는 제10조에 따라 산정된 과징금을 면제할 수 있다.

1. 위반행위자의 지급불능·지급정지 또는 자본잠식 등의 사유로 위반행위자가 객관적으로 과징금을 낼 능력이 없다고 인정되는 경우
2. 제10조에 따라 산정된 과징금이 다음 각 목의 어느 하나에 해당하는 경우

가. 2백만원 이하인 경우

나. 산정된 과태료 금액보다 적은 경우(위반행위가 법 제75조에 따른 과태료 부과 대상이 되는 행위인 경우에 한한다)

③ 제1항에 따른 위반행위자의 현실적인 부담능력과 관련한 감경은 다음 각 호의 경우에는 적용하지 아니한다.

1. 보호위원회로부터 부과받을 과징금 납부로 인해 단순히 자금 사정에 어려움이 예상되는 경우
2. 위반행위자가 현실적인 부담능력 입증과 관련된 객관적인 자료를 제출하지 않은 경우

④ 부과과징금이 법정 한도액을 넘는 경우에는 법정 한도액을 부과과징금으로 한다.

⑤ 부과과징금이 1억원 이상인 경우에는 1백만원 단위 미만의 금액을, 1억원 미만인 경우에는 1십만원 단위 미만의 금액을 버리는 것을 원칙으로 한다. 다만, 보호위원회는 부과과징금의 규모를 고려하여 적당하다고 생각되는 금액 단위 미만의 금액을 버리고 부과과징금을 결정할 수 있다.

- ⑥ 과징금 부과 기준이 되는 매출액 등이 외국환을 기준으로 산정되는 경우에는 해당 매출액 등 산정 기간의 평균환율을 적용하여 원화로 환산한 금액을 부과과징금으로 한다. 이 경우 환율은 하나은행이 최초로 고시하는 매매기준율에 따르며, 하나은행이 고시하지 않는 외국환의 경우에는 미국 달러화로 환산한 후 이를 원화로 다시 환산한다.

제12조(재검토 기한) 보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2023년 9월 15일을 기준으로 매 3년이 되는 시점(매 3년째의 9월 14일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2023-3호, 2023.09.15.>

제1조(시행일) 이 고시는 2023년 9월 15일부터 시행한다. 다만, 제10조제2항제2호 괄호 부분에 해당하는 개정규정 및 제10조제2항제3호다목의 개정규정은 2024년 3월 15일부터 시행한다.

제2조(시행일에 관한 경과조치) ① 부칙 제1조 단서에 따라 제10조제2항제2호 괄호 부분에 해당하는 개정규정이 시행되기 전까지는 해당 규정은 다음과 같이 규정된 것으로 본다. 다만, 법 제39조의9에 따른 손해배상책임의 이행을 위한 보험 등의 가입은 제외한다.

- ② 부칙 제1조 단서에 따라 제10조제2항제3호다목의 개정규정이 시행되기 전까지는 해당 규정 중 "개인정보 처리방침의 평가 또는 개인정보 보호수준 평가의 결과가"는 "개인정보 처리방침의 평가의 결과가"로 규정된 것으로 본다.

제3조(과징금의 산정기준에 관한 경과조치) 이 고시 시행 전의 위반행위로 종전 「개인정보보호 법규 위반에 대한 과징금 부과기준」 또는 「주민등록번호 유출 등에 대한 과징금 부과기준」에 따라 받은 행정처분은 제9조제1항제2호의 개정규정에 따른 위반행위의 횟수 산정에 포함한다.

[별표]

위반행위의 중대성 판단기준(제8조제1항 관련)

고려사항 \ 부과수준	상	중	하
고의·과실	위반행위가 위반행위자의 고의에 의한 경우 또는 중대한 과실에 의한 경우로서 특히 참작할 사유가 없는 경우	위반행위가 위반행위자의 중대한 과실에 의한 경우로서 특히 참작할 사유가 있는 경우	상 또는 중에 해당되지 않는 경우
위반행위의 방법	위반행위의 방법 및 수단을 고려할 때 부당성이 현저히 큰 경우	위반행위의 방법 및 수단을 고려할 때 부당성이 상당한 경우	상 또는 중에 해당되지 않는 경우
위반행위자가 처리하는 개인정보의 유형	위반행위의 대상이 된 개인정보가 민감정보 또는 고유식별정보인 경우	위반행위의 대상이 된 개인정보가 인증정보인 경우	상 또는 중에 해당되지 않는 경우
위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향	정보주체에게 현저한 피해를 입혔거나 입힐 가능성이 높은 경우	정보주체에게 상당한 피해를 입혔거나 입힐 가능성이 높은 경우	상 또는 중에 해당되지 않는 경우

비고

1. 위반행위의 중대성의 정도는 고려사항별 부과기준을 종합적으로 고려하여 판단한다.
2. 위반행위가 고려사항별 부과수준 중 두 가지 이상에 해당하는 경우에는 높은 부과수준을 적용한다.
3. 고려사항별 부과수준의 판단기준은 다음과 같다.

가. 고의·과실

위반행위의 목적, 동기, 당해 행위에 이른 경위, 영리 목적의 유무 등을 종합적으로 고려하여 판단한다.

나. 위반행위의 방법

안전성 확보 조치 이행 노력 여부, 개인정보 보호책임자 등 개인정보 보호 조직, 위반행위가 내부에서 조직적으로 이루어졌는지 여부, 사업주, 대표자 또는 임원의 책임·관여 여부 등을 종합적으로 고려하여 판단한다. 개인정보가 분실·도난·유출·위조·변조·훼손(이하 "유출등"이라 한다)된 경우에는 개인정보의 유출등과 안전성 확보 조치 위반행위와의 관련성을 포함하여 판단한다.

다. 위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향

피해 개인정보의 규모, 위반기간, 정보주체의 권리·이익이나 사생활 등에 미치는 영향 등을 종합적으로 고려하여 판단한다. 개인정보가 유출등이 된 경우에는 유출등의 규모 및 공중에 노출되었는지 여부를 포함하여 판단한다.

5

가명정보의 결합 및 반출 등에 관한 고시

[시행 2024. 1. 30.] [개인정보보호위원회고시 제2024-2호, 2024. 1. 30., 일부개정]

제1장 총칙

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다) 제28조의3과 「개인정보 보호법 시행령」(이하 "령"이라 한다) 제29조의2부터 제29조의4까지에 따른 결합전문기관 지정 및 가명정보의 결합·반출에 관한 기준·절차 등을 정함을 목적으로 한다.

제2조(정의) 이 고시에서 사용하는 용어의 정의는 다음과 같다.

1. "보호위원회등"이란 법 제28조의3제1항에 따라 전문기관을 지정할 수 있는 개인정보 보호위원회(이하 "보호위원회"라 한다) 또는 관계 중앙행정기관의 장을 말한다.
2. "결합키"란 결합 대상인 가명정보의 일부로서 해당 정보만으로는 특정 개인을 알아볼 수 없으나 다른 결합 대상 정보와 구별할 수 있도록 조치한 정보를 말한다.
3. "결합키연계정보"란 결합키가 동일한 정보를 결합할 수 있도록 서로 다른 결합신청자의 결합키를 연계한 정보를 말한다.
4. "결합전문기관"이란 법 제28조의3제1항에 따라 서로 다른 개인정보처리자 간의 가명정보 결합을 수행하기 위해 보호위원회등이 지정하는 전문기관을 말한다.
5. "결합키관리기관"이란 결합키연계정보를 생성하여 결합전문기관에 제공하는 등 가명정보의 안전한 결합을 지원하는 업무를 하는 한국인터넷진흥원을 말한다.

제2장 가명정보 결합체계 협의회 등

제3조(가명정보 결합체계 협의회) ① 가명정보의 결합체계와 관련하여 다음 각 호에 관한 사항을 협의하기 위해 영 제5조의2제4항에 따라 가명정보 결합체계 협의회(이하 "협의회"라 한다)를 보호위원회에 둔다.

1. 개인정보의 가명처리 및 가명정보 결합체계 연구·개선에 관한 사항
 2. 가명정보의 결합과 관련한 개인정보 보호 및 활용에 필요한 사항
 3. 결합전문기관의 지정·재지정 및 지정 취소에 관한 사항
 4. 결합전문기관의 관리·감독에 관한 사항
 5. 그 밖에 가명정보 제도 운영 등에 관하여 협의가 필요한 사항
- ② 협의회는 보호위원회 및 관계 중앙행정기관의 가명정보 결합 등에 관한 업무를 담당하는 부서의 장으로 구성한다.

제4조(보호위원회의 지원) ① 보호위원회는 결합신청자, 결합전문기관 및 결합키관리기관 간 결합 신청, 결합, 반출 등에 필요한 시스템을 구축하여 운영할 수 있다.

② 보호위원회는 반출심사의 전문성을 확보하기 위해 반출심사위원회 위원의 교육계획을 수립하여 운영할 수 있다.

- ③ 보호위원회는 지방자치단체와 공동으로 지역 가명정보 활용을 위한 지원센터를 구축하여 운영할 수 있다. 이 경우 지방자치단체가 지원센터를 운영한다.
- ④ 보호위원회는 결합신청자의 요청이 있는 경우 제1항의 시스템 또는 제3항의 지원센터를 통해 결합키 생성을 지원할 수 있다.

제3장 결합전문기관의 지정 등

제5조(결합전문기관의 지정 절차) ① 결합전문기관으로 지정받으려는 법인, 단체 또는 기관(이하 "지정신청자"라 한다)은 다음 각 호의 서류를 보호위원회등에게 제출하여야 한다. 다만, 「신용정보의 이용 및 보호에 관한 법률」 제26조의4에 따라 데이터전문기관으로 지정받은 기관인 경우 제3호 서류 중 일부를 생략할 수 있다.

1. 정관 또는 규약
 2. [별지 제1호서식]의 결합전문기관 지정신청서
 3. [별표1]의 결합전문기관 지정 기준 충족여부를 증빙할 수 있는 서류
- ② 지정신청자는 필요한 경우 제1항에 따른 지정 신청 전 보호위원회등에게 결합전문기관 사업계획서 또는 그에 준하는 서류를 제출하여 해당 내용이 [별표1]의 결합전문기관 지정 기준에 적합한지 여부를 확인받을 수 있다.
- ③ 보호위원회등은 제1항에 따른 신청을 받은 경우 [별표1]의 결합전문기관 지정 기준에 적합한지 여부를 결합전문기관 지정심사위원회(이하 "지정심사위원회"라 한다)를 구성하여 심사하여야 한다. 이 경우 지정심사위원회는 개인정보 보호에 관한 학식과 경험이 풍부한 5명의 위원으로 구성한다.
- ④ 보호위원회등은 제3항에 따른 심사 결과 [별표1]의 결합전문기관 지정 기준을 충족한다고 인정하는 경우 결합전문기관으로 지정할 수 있다. 이 경우 [별지 제2호서식]의 결합전문기관 지정서를 발급하여야 한다.
- ⑤ 보호위원회등은 제1항에 따른 신청을 받은 날의 다음날부터 2개월 이내에 결합전문기관 지정 여부를 결정하여야 하며, 부득이한 사정이 있는 경우 1개월의 범위에서 그 기간을 연장할 수 있다.
- ⑥ 결합전문기관으로 지정받은 자는 [별표1]의 결합전문기관 지정 기준에 해당하는 사실의 변경이 있는 경우 지체 없이 보호위원회등에게 변경된 사실을 알려야 한다. 이 경우 보호위원회등은 변경된 내용이 [별표1]의 결합전문기관 지정 기준을 충족하는지 여부를 변경사항의 통보를 받은 날의 다음날로부터 1개월 이내에 확인하여야 하며, 지정 기준을 충족하지 못한 때에는 해당 결합전문기관은 제8조에 따른 결합 신청을 접수하여서는 아니 된다.
- ⑦ 제5항 및 제6항에 따른 기간을 산정할 때에는 다음 각 호에 해당하는 기간은 심사기간에 산입하지 아니한다.
1. 지정신청자의 서류보완 등에 소요된 기간
 2. 법 또는 영에 따른 의무의 위반과 관련하여 지정신청자를 상대로 형사소송 절차가 진행되고 있거나 보호위원회등에 의한 조사·검사 등의 절차가 진행되고 있고, 그 소송이나 조사·검사 등의 내용이 지정심사에 중대한 영향을 미칠 수 있다고

인정되는 경우에는 그 소송이나 조사·검사 등의 절차가 끝날 때까지의 기간

제6조(결합전문기관의 재지정) ① 결합전문기관은 재지정을 받으려는 경우에는 지정기간 만료일 6개월 전부터 3개월 전까지 [별표1]의 결합전문기관 지정 기준에 부합함을 증명할 수 있는 서류를 갖추어 재지정을 신청할 수 있다. 이 경우 보호위원회등은 결합전문기관의 지정기간 만료일 6개월 전에 만료 사실을 알려줄 수 있다.

② 보호위원회등은 제1항에 따른 재지정 신청을 받은 때에는 [별표1]의 결합전문기관 지정 기준을 충족하고 있는지를 제5조제3항의 절차에 따라 심사하여 결합전문기관 지정기간 만료일 전까지 그 결과를 재지정을 신청한 결합전문기관에 통지하여야 한다. 심사 결과 보호위원회등이 재지정을 결정한 경우에는 [별지 제2호서식]의 결합전문기관 지정서를 발급하여야 한다.

제6조의2(결합전문기관의 지정취소) ① 보호위원회등은 결합전문기관의 지정 취소사유가 영 제29조의2제5항제3호부터 제5호까지에 해당하는 경우 결합전문기관에 시정·보완을 요구할 수 있다.

② 보호위원회등은 결합전문기관의 지정을 취소한 경우 해당 결합전문기관이 수행 중인 업무를 중단하도록 하고, 결합신청자와 협의하여 해당 업무를 다른 결합전문기관으로 이관하도록 하여야 한다.

제7조(결합전문기관 지정에 따른 고시 등) 보호위원회등은 결합전문기관을 지정, 재지정 또는 지정 취소하는 경우, 영 제29조의2제7항에 따라 다음 각 호의 사항을 관보에 공고하거나 보호위원회등의 홈페이지에 게시해야 한다. 이 경우 관계 중앙행정기관의 장은 다음 각 호의 사항을 보호위원회에 통보해야 한다.

1. 결합전문기관의 명칭 및 주소
2. 담당 부서 및 연락처
3. 지정 유효기간(지정 또는 재지정의 경우에 한정한다)
4. 취소 일시 및 취소 사유(지정 취소의 경우에 한정한다)

제4장 가명정보의 결합 신청 및 반출 등

제8조(가명정보의 결합 신청 접수 등) ① 결합전문기관은 영 제29조의3제1항에 따라 결합신청자로부터 [별지 제3호서식]의 결합신청서(전자문서를 포함한다.) 및 첨부 서류를 제출받은 경우 지체 없이 결합신청자에게 접수 사실을 통지하고, 서류의 누락 등 보완이 필요한 경우 보완을 요구하여야 한다. 다만, 결합전문기관은 결합신청자와 협의하여 결합 대상 가명정보의 가명처리 내역에 관한 서류를 가명정보 전송 시에 제출하도록 할 수 있다.

② 결합전문기관은 가명정보의 결합 일정 및 절차 등 결합에 필요한 사항을 결합신청자와 협의하여야 한다.

③ 결합기관관리기관은 결합키 생성에 필요한 사항을 결합신청자와 협의하여야 한다.

제9조(가명정보의 결합) ① 결합신청자는 제8조제3항에 따른 협의 결과에 따라 결합키와 결합에 필요한 일련번호를 결합기관관리기관에 전송하여야 하며, 결합기관관리기관은 이를

이용하여 지체 없이 결합키연계정보를 생성하여야 한다.

- ② 결합신청자는 결합 대상 정보가 확정된 경우 해당 정보를 가명처리하여 가명처리 내역, 결합에 필요한 일련번호와 함께 결합전문기관에게 전송하여야 한다. 이 경우 결합전문기관은 결합 대상 정보의 가명처리 수준을 확인한 후 필요한 경우 추가 처리를 요청할 수 있다.
- ③ 결합기관리기관은 결합전문기관이 가명정보 결합을 위해 결합키연계정보의 전송을 요청한 경우 지체 없이 결합키연계정보를 결합전문기관에 전송하여야 한다.
- ④ 결합전문기관은 결합기관리기관으로부터 결합키연계정보를 제공받아 가명정보의 결합을 완료하는 등으로 결합키연계정보가 불필요하게 된 때에는 이를 지체 없이 파기하여야 한다.
- ⑤ 결합전문기관이 별표1제1호가목 단서에 따라 제4조제3항의 지원센터를 담당조직으로 하는 경우에는 공익 목적의 결합 또는 다른 결합전문기관이 수행하는 것이 어려운 결합 등에 대해 보호위원회가 인정하는 경우에 한하여 결합을 수행할 수 있다.

제9조의2(가명정보의 결합률 확인 및 추출) ① 결합기관리기관은 결합신청자의 요청이 있는 경우 제9조제1항에 따른 결합키연계정보 생성과정에서 결합률을 확인하여 결합신청자에게 통보하여야 한다.

- ② 결합신청자는 제9조제2항에 따라 전송하는 정보를 최소화하기 위하여 결합기관리기관에 결합 대상 정보의 추출에 필요한 일련번호를 요청할 수 있으며, 이를 위해 필요한 자료를 제출하여야 한다.
- ③ 결합기관리기관은 제2항의 요청이 있는 경우 결합 대상 정보의 특성, 결합률 등을 고려하여 결합신청자에게 추출 가능 여부를 통지하여야 하며, 추출이 가능하다고 판단한 경우 결합 대상 정보의 추출에 필요한 일련번호를 결합신청자에게 전송하여야 한다.

제9조의3(가명정보의 모의결합) ① 결합신청자는 결합의 유용성을 미리 확인하기 위하여 제9조에 따른 결합을 수행하기 전에 결합전문기관과 협의하여 결합전문기관에 일부 가명정보의 결합(이하 ‘모의결합’이라 한다)을 요청할 수 있다. 이 경우 결합신청자는 제8조제3항에 따라 생성한 결합키 또는 제8조제3항에도 불구하고 모의결합을 위해 결합전문기관과 협의하여 생성한 모의결합키(이하 이 조에서 ‘결합키등’이라 한다)를 결합전문기관에 전송하여야 한다.

- ② 결합전문기관은 모의결합 대상 정보의 특성, 결합률 등을 고려하여 모의결합 가능 여부를 결합신청자에게 통지하여야 하며, 모의결합이 가능하다고 판단한 경우 모의결합 대상이 되는 정보의 결합키등을 선정하여 결합신청자에게 전송하여야 한다.
- ③ 결합신청자는 모의결합 대상이 되는 정보를 가명처리하여 가명처리 내역, 결합에 필요한 결합키등과 함께 결합전문기관에 전송하여야 한다. 이 경우 결합전문기관은 모의결합 대상 정보의 가명처리 수준을 확인한 후 필요한 경우 추가 처리를 요청할 수 있다.
- ④ 결합신청자는 결합전문기관으로부터 모의결합된 정보를 제공받아 영 제29조의3제3항에

다른 안전성 확보에 필요한 기술적·관리적·물리적 조치가 된 공간에서 분석할 수 있다.
단, 결합신청자는 분석한 정보 등 결과물을 결합전문기관 외부로 반출할 수 없다.

- ⑤ 결합전문기관은 제4항에 따라 모의결합된 정보를 제공하는 경우 결합키등은 삭제하여야 하며, 결합신청자가 분석을 마친 경우 모의결합에 사용된 모든 정보를 파기하여야 한다.

제9조의4(결합전문기관의 자체결합) ① 결합전문기관은 자신이 보유한 가명정보와 다른 개인정보처리자가 보유한 가명정보를 직접 결합(이하 "자체결합"이라 한다)할 수 있다.

- ② 결합전문기관은 제1항에 따라 자체결합을 하는 경우 다음 각 호의 사항을 준수하여야 한다. 다만, 결합전문기관이 가명정보의 결합을 신청하는 다른 개인정보처리자 등 제3자에게 제공하려는 경우에는 제5호 내지 제8호의 준수사항을 면제한다.

1. 결합전문기관과 이해관계가 없는 외부전문가가 다음 각목의 업무를 수행하도록 하여야 하며 이때 외부전문가는 제11조제2항 각 호에 해당하는 사람으로 할 것.
가. 제8조제1항의 결합신청서 및 첨부 서류의 확인과 보완 요구
나. 제9조제2항의 결합 대상 정보의 가명처리 수준 확인과 추가 처리 요청
2. 결합전문기관은 제11조 제2항에 따른 반출심사위원회를 결합전문기관과 이해관계가 없는 외부전문가로만 구성할 것
3. 결합전문기관에서 영 제29조의3제1항에 따른 결합신청자로서의 업무를 수행하는 담당자는 결합전문기관으로서의 업무에 참여하지 않을 것
4. 결합전문기관은 자신이 보유한 가명정보와 제1항에서 허용하는 바에 따라 결합한 가명정보를 물리적으로 분리하여 보관하고, 각 정보에 대한 접근권한을 통제·관리할 것
5. 결합전문기관이 결합된 정보를 이용하려는 경우에는 직전 분기까지 가명정보를 제3자에게 제공한 누적 실적범위에서 자체결합을 수행할 것
6. 제9조의4 제2항제2호에 따른 반출심사위원회는 유사분야의 다른 결합전문기관(데이터전문기관을 포함한다)의 임직원 또는 해당 기관에서 추천한 외부전문가로 구성할 것
7. 제6호에 따른 요건을 회피할 목적으로 타 기관과 교차하여 제9조의4 제2항제2호에 따른 반출심사위원회 구성을 의뢰하거나 수행하지 아니할 것
8. 제5호에 따른 자체결합에 관련한 각목의 사항을 자신이 구축한 인터넷 사이트에 공개할 것
가. 결합된 정보의 이용자 및 관리책임자
나. 결합된 정보의 활용 목적
다. 결합된 정보의 항목
라. 결합된 정보의 활용 기간

- ③ 결합전문기관은 제2항 각 호에 관한 사항을 기록하여 보관하여야 한다.

제10조(결합된 정보의 반출 전 처리) ① 결합신청자는 결합된 정보를 영 제29조의3제3항에 따른 안전성 확보에 필요한 기술적·관리적·물리적 조치가 된 공간에서 가명정보 또는 법 제58조의2에 해당하는 정보로 처리할 수 있다.

- ② 결합전문기관은 결합신청자의 요청이 있는 경우 결합신청자가 제1항의 공간에서

결합된 정보를 분석하도록 할 수 있다.

- ③ 결합신청자가 결합된 정보 또는 제1항과 제2항에 따라 처리한 정보를 반출하려는 경우 [별지 제4호서식]의 반출신청서와 다음 각 호의 첨부 서류를 결합전문기관에 제출하여야 한다.

1. 반출 대상 정보에 관한 서류(추가적인 서류 제출이 필요한 경우에 한함)
2. 반출 목적을 증명할 수 있는 서류(추가적인 서류 제출이 필요한 경우에 한함)
3. 반출 정보의 안전조치 계획 및 이를 증빙할 수 있는 서류

제11조(반출승인) ① 결합전문기관은 결합신청자가 반출을 요청하는 경우 영업일 기준 5일 이내에 반출심사위원회 구성 등 일정을 정하여 결합신청자에게 통지하고 구체적인 사항을 협의하여야 한다.

- ② 결합전문기관은 제1항에 따라 반출심사위원회를 구성하는 경우 개인정보 보호에 관하여 학식과 경험이 풍부한 사람으로서 다음 각 호에 해당하는 사람을 고루 포함하여 3명의 위원으로 구성하여야 한다. 다만, 반출심사를 위해 필요하다고 판단한 경우 다른 결합전문기관에 소속된 전문가를 추가로 포함할 수 있다.

1. 개인정보 보호와 관련한 업무 경력이 있거나 관련 단체로부터 추천을 받은 사람
2. 개인정보처리자로 구성된 단체에서 활동한 경력이 있거나 관련 단체로부터 추천을 받은 사람
3. 그 밖에 개인정보 보호와 관련한 경력과 전문성이 있는 사람

- ③ 반출심사위원회는 다음 각 호의 사항을 고려하여 반출심사를 하여야 한다.

1. 결합 목적과 반출 정보가 관련성이 있을 것
2. 특정 개인을 알아볼 가능성이 없을 것
3. 반출 정보에 대한 안전조치 계획이 있을 것

- ④ 결합신청자는 제3항에 따른 반출심사에 필요한 사항을 제출하고 이를 설명하여야 한다.

- ⑤ 결합신청자의 임직원 등 이해관계자는 반출심사위원회 위원으로 참여할 수 없다.

제11조의2(결합전문기관의 지원) ① 결합전문기관은 다음 각 호의 업무를 지원할 수 있다.

1. 결합 전 가명처리
2. 제10조제1항에 따른 처리 또는 같은 조 제2항에 따른 분석
3. 제11조에 따라 반출한 정보의 분석
4. 가명정보를 반출하려는 결합신청자에 대한 개인정보 보호 교육

- ② 제1항제1호부터 제3호까지의 업무를 수행하는 담당자는 제8조제1항, 제9조제2항, 제9조의3제3항에 따른 업무에 참여하여서는 아니 된다.

제5장 전문기관의 책무 및 전문기관에 대한 관리·감독

제12조(안전성 확보 등에 필요한 조치) ① 결합전문기관은 가명정보의 결합·반출 등으로 해당 가명정보의 결합·반출과정에서 제공받거나 생성한 정보가 불필요하게 된 때에는 이를 지체 없이 파기하여야 한다.

- ② 제1항에도 불구하고 결합전문기관은 매년 1월 1일부터 12월 31일까지 생성된 다음 각 호의 사항을 다음 연도 1월 31일까지 보호위원회에 제출하여야 한다.
1. 결합신청서 및 첨부 서류
 2. 반출심사에 대한 결과 및 심사위원 명단
 3. 결합된 정보 및 심사 대상 정보에 대한 파기 대장
- ③ 제1항과 제2항에도 불구하고 결합전문기관은 자체결합 관련 다음 각 호의 자료를 매 분기 마지막 달의 다음 달 말일까지 보호위원회에 제출하여야 한다.
1. 제2항 각 호의 서류
 2. 제9조의4제3항에 따라 보관하고 있는 기록
 3. 가명정보의 제3자 제공과 관련하여 다음 각 목의 사항을 확인할 수 있는 자료
 - 가. 제공받는 자
 - 나. 제공받는 자의 이용 목적
 - 다. 제공하는 항목
 - 라. 제공받는 자의 보유 및 이용기간
- ④ 결합기관리기관은 가명정보의 결합이 완료되는 등 결합기와 결합기연계정보가 불필요하게 된 때에는 지체 없이 파기하여야 한다.
- ⑤ 결합전문기관은 결합신청자가 정당한 사유 없이 제9조에 따른 가명정보의 결합이 완료된 날부터 14일 이상 제10조 제1항 또는 제2항에 따른 처리를 수행하지 않는 등 반출의 의사가 없다고 판단되면 결합 절차를 종료할 수 있다.

제12조의2(결합전문기관의 관리·감독) ① 결합전문기관은 영 제29조의4제2항제1호에 따른 가명정보의 결합 및 반출 실적 보고서를 작성할 때 제9조4제1항의 자체결합의 실적은 별도로 분리해서 작성하여야 한다.

- ② 결합전문기관은 매년 1월 1일부터 12월 31일까지 생성된 영 제29조의4제2항 각 호의 서류를 다음 연도 1월 31일까지 보호위원회등에 제출하여야 한다.

제6장 보칙

제13조(재검토기한) 보호위원회는 「행정규제기본법」 및 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2024년 1월 1일 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2024-2호, 2024.01.30.>

제1조(시행일) 이 고시는 발령한 날부터 시행한다.

제2조(자체결합에 관한 적용례)

제9조의4 제2항제5호 개정규정의 누적 실적은 2020년 8월 5일 이후 가명정보를 제3자에게 제공한 실적을 합산하여 적용한다.

결합전문기관 지정 기준

1. 담당 조직의 구성·운영

가. 결합전문기관 운영을 위해 제2호에 따른 전문가를 포함한 8명 이상의 담당 조직 구성. 다만, 고시 제4조제3항의 지원센터를 담당조직으로 구성하는 경우 3명 이상으로 구성할 수 있다.

나. 담당 조직에 대한 관리책임자 지정

다. 운영 인력에 대한 교육계획 수립

2. 제1호 가목의 담당 조직 구성 시 다음 각 목의 어느 하나에 해당하는 전문가를 3명 이상 상시

고용할 것(이 경우 기술·법률 전문가가 각 1명 이상 포함되도록 하여야 한다. 다만, 최대 1명(고시 제4조제3항의 지원센터를 담당조직으로 하는 경우 최대 3명)에 한하여 법인·단체·기관 내 다른 조직의 소속 직원을 겸임하게 할 수 있다.)

가. 기술 전문가

- 1) 「국가기술자격법」에 따른 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사 자격 취득 후 1년 이상 관련 경력(개인정보 보호, 데이터 가공·분석·활용, 데이터 가명·익명처리 및 적정성 평가 등 이하 가목에서 같다)이 있는 사람
- 2) 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제14조제1항에 따른 정보보호 및 개인정보보호 관리체계 인증심사원 자격(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」로 통합 이전 「정보보호 관리체계 인증 등에 관한 고시」와 「개인정보보호 관리체계 인증 등에 관한 고시」에 따른 인증심사원 자격을 포함한다)을 취득한 자로 4년 이상 관련 경력이 있는 사람
- 3) 정보시스템감사통제협회(Information Systems Audit and Control Association)의 공인정보시스템감사사(CISA) 자격 취득 후 5년 이상 관련 경력이 있는 사람
- 4) 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 공인정보시스템보호전문가(CISSP) 자격 취득 후 5년 이상 관련 경력이 있는 사람
- 5) 정보통신기사·정보처리기사 및 전자계산기조직응용기사, 정보보안기사 자격 취득 후 6년 이상 관련 경력이 있는 사람
- 6) 관련 분야(개인정보 보호, 정보보호, 정보통신, 정보기술, 데이터 분석, 컴퓨터공학, 통계학, 수학 등 이하 가목에서 같다)에서 박사학위 취득 후 1년 이상 관련 경력이 있는 사람
- 7) 관련 분야에서 석사학위 취득 후 4년 이상 관련 경력이 있는 사람
- 8) 관련 분야에서 학사학위 취득 후 6년 이상 관련 경력이 있는 사람
- 9) 정보보호, 정보통신, 정보기술, 데이터 분석, 컴퓨터 공학, 통계, 수학, 가명처리 관련 업무에 8년 이상 종사한 사람

나. 법률 전문가

- 1) 「변호사법」에 따른 변호사 자격 취득 후 1년 이상 관련 법률 경력(개인정보 보호(정보보호·정보보안 포함), 데이터 가공·분석·활용, 데이터 가명·익명처리 및 적정성 평가 등 관련 법률 자문 또는 지원 업무 이하 나목에서 같다)이 있는 사람
- 2) 법학 관련 박사학위 취득 후 1년 이상 관련 법률 경력이 있는 사람
- 3) 법학 관련 석사학위 취득 후 4년 이상 관련 법률 경력이 있는 사람
- 4) 법학 관련 학사학위 취득 후 6년 이상 관련 법률 경력이 있는 사람

- 5) 관련 법률 경력이 8년 이상 있는 사람
3. 다음 각 목에 따른 공간 및 시설 구축
 - 가. 결합, 가명정보 또는 법 제58조의2에 해당하는 정보로 처리(이하 '가명처리등'이라 한다), 반출심사를 위한 공간 및 시설
 - 나. 그 밖에 결합전문기관 업무 수행을 위한 공간 및 시설
 - 다. 가목 및 나목에 대한 물리적 안전조치
4. 다음 각 목의 기능을 수행하는 시스템 구축
 - 가. 가명정보 결합, 가명처리등, 반출심사에 필요한 기능
 - 나. 데이터 송신·수신에 필요한 기능
 - 다. 그 밖에 결합전문기관 업무를 위한 기능
5. 데이터 및 네트워크에 대한 보안조치 마련
 - 가. 데이터의 유출을 방지하기 위한 조치
 - 나. 결합, 가명처리등, 반출심사와 관련한 정보 및 시스템에 대한 접근 권한 관리
 - 다. 비인가자의 불법적인 접근 차단 및 침해사고 방지를 위한 조치
 - 라. 개인정보 암호화 및 데이터 송신·수신 시 암호화 적용을 위한 조치
 - 마. 접속기록 보관 및 위조·변조 방지 조치
 - 바. 악성프로그램 등 방지 조치
 - 사. <삭 제>
 - 아. 백업 및 복구를 위한 조치
 - 자. 데이터 파기를 위한 조치
 - 차. 결합전문기관으로서 처리하는 정보와 그 밖에 자신이 보유한 개인정보의 분리
6. 정책 및 절차 마련
 - 가. 결합, 가명처리등, 반출심사(심사위원 구성 방안 포함)를 위한 정책 및 절차
 - 나. 결합전문기관 업무를 위한 각 공간에 대한 출입 통제 정책 및 절차
 - 다. 데이터 반출·반입 통제 정책 및 절차
 - 라. 데이터 파기 및 기록·보관에 대한 정책 및 절차
 - 마. 개인정보의 안전성 확보조치 기준 제4조제1항제5호부터 제9호까지, 제11호, 제12호(접근권한 관리, 접근 통제, 개인정보 암호화, 접속기록 보관 및 점검, 악성프로그램 등 방지, 물리적 안전조치, 개인정보 유출사고 대응 계획) 및 제11조 각호(재해·재난 대비 안전조치)에 따른 조치
7. 자본금 50억원 이상(비영리법인의 경우 기본재산 또는 자본총계 50억원 이상)에 해당하는 재정 능력을 갖출 것. 다만, 다음 각 호에 해당하는 기관은 적용을 제외한다.
 - 가. 법 제2조제6호가목에 해당하는 공공기관
 - 나. 특별법에 따라 설립된 특수법인으로 기관의 사업과 운영에 필요한 비용을 중앙행정기관 또는 지방자치단체가 출연할 수 있도록 법률에서 정하고 있는 경우
 - 다. 공공 업무를 주 목적으로 설립된 비영리법인으로 기관의 사업과 운영에 필요한 비용을 중앙행정기관 또는 지방자치단체로부터 지급받고 소관 중앙행정기관의 장 또는 지방자치단체의 장의 요청에 따라 보호위원회가 인정한 경우
8. 최근 3년 이내(결합전문기관 지정 신청일 기준)에 법 제66조에 따라 공표된 적이 없을 것

결합전문기관 지정신청서

※ 색상이 어두운 난은 신청인이 작성하지 않습니다.

접수번호	접수일시	처리기간
지정 신청자	법인·단체·기관명	사업자등록번호 또는 법인등록번호
	대표자 성명	담당자 성명
	주소	담당자 전화번호
		담당자 전자우편 주소

「개인정보 보호법」 제28조의3제1항 및 같은 법 시행령 제29조의2제2항, 「가명정보의 결합 및 반출 등에 관한 고시」 제5조제1항에 따라 결합전문기관 지정을 위와 같이 신청합니다.

년 월 일

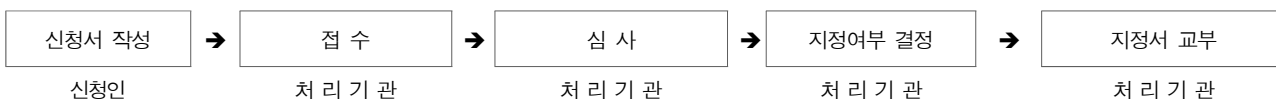
지정신청자(대표자)

(서명 또는 인)

개인정보보호위원회 귀중 (관계 중앙행정기관의 장 귀하)

첨부 서류 (각 3부)	1. 정관 또는 규약 2. [별표 1]에 따른 조직·인력, 시설·장비, 재정 능력 등 심사를 위하여 필요한 서류	수수료 없음
-----------------	---	-----------

처 리 절 차



210mm×297mm[(백상지(80g/㎡) 또는 중질지(80g/㎡)]

제 호

결합전문기관 지정서

1. 법인·단체·기관명 :
2. 대 표 자 :
3. 주 소 :
4. 유효기간 :

위의 법인·단체·기관을 「개인정보 보호법」 제28조의3제1항 및 같은 법 시행령 제29조의2에 따른 결합전문기관으로 지정합니다.

년 월 일

개인정보 보호위원회
/관계 중앙행정기관의 장

직인

240mm×340mm[한지백색 170g/㎡]

결합 신청서

신청번호	
접수번호	

결합신청자

기관명		사업자등록번호 또는 법인등록번호	
주소		대표자명	
담당자		담당자 연락처 (전화, e-mail)	
유형	<input type="checkbox"/> 개인 <input type="checkbox"/> 공공기관 <input type="checkbox"/> 비영리법인 <input type="checkbox"/> 민간기관		

결합 개요

전체 결합신청기관명	총 기관 수 []개 기관
	기관명
반복결합	[] 해당없음 [] 최초 [] 추가(결합접수번호 :)
추가절차 신청	결합률 확인 [] 가명정보 추출 [] 모의결합 []

가명정보 제공자

제출 방법	<input type="checkbox"/> 온라인 <input type="checkbox"/> 오프라인	
지원 요청 사항	<input type="checkbox"/> 결합 신청에 필요한 가명처리	
가명정보 제공 담당자	이름	연락처 (전화, e-mail)

결합정보 이용자

결합 목적	<input type="checkbox"/> 통계작성 <input type="checkbox"/> 과학적 연구 <input type="checkbox"/> 공익적 기록보존 등		
세부 결합 목적			
분석공간 이용	<input type="checkbox"/> 추가 가명처리 <input type="checkbox"/> 결합정보 분석 <input type="checkbox"/> 이용안함		
지원 요청 사항	<input type="checkbox"/> 반출 전 처리 <input type="checkbox"/> 분석		
결합정보 이용 담당자	이름	연락처 (전화, e-mail)	

「개인정보 보호법」 제28조의3제1항 및 같은 법 시행령 제29조의3제1항에 따른 결합을 위하여 결합전문기관에 결합신청서를 위와 같이 제출합니다.

이
의
리

결합신청기관 (서명 또는 인)

(결합전문기관명)의 장 귀하

첨부 서류	<ol style="list-style-type: none"> 1. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류 1부 2. 결합 목적을 증명할 수 있는 서류 1부(결합정보 이용자에 한함) 3. 결합 대상 가명정보에 관한 서류(전체 항목명, 가명처리 대상 항목명*, 가명처리 내역 등**) 1부(가명정보 제공자에 한함) <p>* 결합키 생성에 사용된 항목 제외 ** 결합 대상 정보가 확정된 이후에 제출</p>
----------	---

반출신청서

반출접수번호	
결합접수번호	

결합신청자			
기관명		사업자등록번호 또는 법인등록번호	
주소		대표자명	
담당자		담당자 연락처 (전화, e-mail)	

결합 유형			
반복결합	<input type="checkbox"/> 최초	<input type="checkbox"/> 추가	

반출 개요			
파일명			
반출 목적	<input type="checkbox"/> 통계작성	<input type="checkbox"/> 과학적 연구	<input type="checkbox"/> 공익적 기록보존 등
세부 반출 목적			
반출 정보 유형	<input type="checkbox"/> 가명정보	<input type="checkbox"/> 법 제58조의2에 해당하는 정보(익명정보)	
제공 받는 방법	<input type="checkbox"/> 온라인	<input type="checkbox"/> 오프라인	<input type="checkbox"/> 결합전문기관 내 분석공간
지원 요청 사항	<input type="checkbox"/> 반출된 정보의 분석	<input type="checkbox"/> 개인정보 보호 교육	

「개인정보 보호법」 제28조의3제2항 및 같은 법 시행령 제29조의3제3항·제6항, 「가명정보의 결합 및 반출 등에 관한 고시」 제10조제3항에 따라 결합된 정보를 반출하기 위하여 결합전문기관에 반출신청서를 위와 같이 제출합니다.

년 월 일

결합신청자

(서명 또는 인)

결합전문기관의 장 귀하

첨부 서류	1. 반출 대상 정보에 관한 서류 1부(추가적인 서류 제출이 필요한 경우에 한함) 2. 반출 목적을 증명할 수 있는 서류 1부(추가적인 서류 제출이 필요한 경우에 한함) 3. 반출 정보의 안전조치계획 및 이를 증빙할 수 있는 서류 1부
-------	---

6

개인정보 국외 이전 운영 등에 관한 규정

[시행 2023. 10. 16.] [개인정보보호위원회고시 제2023-11호, 2023. 10. 16., 제정]

제1장 총칙

제1조(목적) 이 고시는 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제5조, 제29조의8, 제29조의9, 제29조의11, 제29조의12에 따라 개인정보의 국외 이전에 관하여 필요한 사항을 정함을 목적으로 한다.

제2조(정의) 이 고시에서 사용하는 용어의 정의는 다음과 같다.

1. "국외이전전문위원회"는 영 제5조제1항에 따라 개인정보 보호 관련 전문가 등으로 구성된 개인정보 국외 이전 분야의 전문위원회를 말한다.
2. "개인정보 국외 이전 인증"이란 영 제29조의8제1항에 따라 개인정보 보호위원회(이하 "보호위원회"라 한다)가 고시하는 인증을 말한다.
3. "개인정보 보호 인증 전문기관"이란 영 제34조의6에 따른 개인정보 보호 인증 전문기관을 말한다.
4. "이전대상국등"이란 법 제28조의8제1항제5호에 따라 개인정보가 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 '이전'이라 한다)되는 국가 또는 국제기구를 말한다.

제2장 국외이전전문위원회 운영 등

제3조(국외이전전문위원회 위원 임기) 국외이전전문위원회 위원(이하 '위원'이라 한다)의 임기는 위촉된 날로부터 3년으로 하되 연임할 수 있다. 다만, 영 제5조제2항제1호에 해당하는 위원의 임기는 해당 직위에 재직하는 기간으로 한다.

제4조(국외이전전문위원회 운영) ① 국외이전전문위원회 회의는 보호위원회의 요청에 따라 국외이전전문위원회 위원장이 소집한다.

- ② 국외이전전문위원회 위원장이 부득이한 사유로 그 직무를 수행할 수 없는 때에는 국외이전전문위원회 위원장이 미리 지명한 위원이 그 직무를 대행한다.
- ③ 국외이전전문위원회는 재적위원 과반수의 출석으로 개최하고 출석위원 과반수의 찬성으로 의결한다.
- ④ 국외이전전문위원회는 필요한 경우 관계기관의 공무원 및 이해관계인에게 국외이전전문위원회 회의 출석 또는 의견 제출을 요청할 수 있다.
- ⑤ 국외이전전문위원회 회의는 공개하지 않는다. 다만, 다음 각 호의 사항을 포함한 회의록을 작성하여 보관하여야 하며, 국외이전전문위원회 위원장이 필요하다고 인정하면 녹음 또는 녹화를 할 수 있다.

1. 회의 일시 및 장소

2. 회의에 참석한 위원 명단

3. 회의 안건 및 내용

- ⑥ 국외이전전문위원회 위원장이 안건을 검토한 결과 사안이 긴급을 요하거나 토론을 요하지 아니한다고 판단되는 경우, 국외이전전문위원회 회의를 서면으로 개최할 수 있다.

제5조(간사 등) ① 국외이전전문위원회에 간사 1인을 두되, 간사는 보호위원회 사무처 소속 공무원 중에서 개인정보의 국외 이전 업무를 담당하는 부서의 장이 된다.

② 간사는 다음 각 호의 업무를 수행한다.

1. 국외이전전문위원회 위원장의 국외이전전문위원회 운영에 관한 보좌
2. 국외이전전문위원회 회의록 작성 및 보관
3. 국외이전전문위원회의 업무에 관한 사무처리 등

제6조(소위원회) 국외이전전문위원회 위원장은 국외이전전문위원회 업무를 효율적으로 수행하기 위하여 필요하다고 인정될 경우 일부 위원으로 구성되는 소위원회를 둘 수 있다.

제7조(위원의 제척 사유) 위원은 다음 각 호의 어느 하나에 해당하는 경우에는 해당 평가에 관여하지 못한다

1. 위원 본인과 직접적인 이해관계가 있는 사항
2. 위원 본인과 친족관계에 있거나 있었던 자와 관련된 사항
3. 위원이 해당 사안에 관하여 증언, 감정, 법률자문을 한 경우
4. 위원이 해당 사안에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우
5. 위원이나 위원이 속한 공공기관·법인 또는 단체 등이 조언 등 지원을 하고 있는 자와 이해관계가 있는 경우

제8조(위원의 해임 및 해촉) 보호위원회 위원장은 위원이 다음 각 호의 어느 하나에 해당하는 경우에는 해당 위원을 해임 또는 해촉할 수 있다.

1. 심신장애로 인하여 직무를 수행할 수 없게 된 경우
2. 직무와 관련된 비위사실이 있는 경우
3. 직무 태만, 품위 손상, 그 밖의 사유로 인하여 위원의 직을 유지하는 것이 적합하지 아니하다고 인정되는 경우
4. 위원 스스로 직무를 수행하는 것이 곤란하다고 의사를 밝히는 경우

제9조(수당과 여비) 국외이전전문위원회와 제6조에 따른 소위원회의 회의에 출석한 위원 등에게는 예산의 범위에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 그 소관 업무와 직접적으로 관련되어 출석하는 경우에는 그러하지 아니하다.

제10조(운영세칙) 국외이전전문위원회의 운영에 관하여 이 규정에서 정하지 아니한 세부적 사항은 국외이전전문위원회의 의결을 거쳐 국외이전전문위원회 위원장이 정한다.

제3장 개인정보 국외 이전 인증

제11조(인증에 대한 개인정보 보호 인증 전문기관의 평가) 개인정보 보호 인증 전문기관이 영 제29조의8제1항제1호에 따라 평가를 할 때에는 별표1의 기준에 따라 해당 인증의 개인정보 보호 수준, 정보주체의 권리 보호 적절성 등을 평가하고 그 내용을 보호위원회에 제출하여야 한다.

제12조(인증에 대한 국외이전전문위원회의 평가) 국외이전전문위원회가 영 제29조의8제1항제2호에 따라 평가를 할 때에는 별표1의 기준에 따라 해당 인증의 개인정보 보호 수준, 정보주체의 권리 보호 적절성 등을 평가하고 그 내용을 보호위원회에 제출하여야 한다.

제13조(인증에 대한 정책협의회의 협의) 보호위원회는 영 제29조의8제1항제3호에 따라 정책협의회를 개최하여 해당 인증에 대하여 관계기관과 협의하여야 한다.

제14조(인증에 대한 보호위원회 심의·의결) 보호위원회는 제11조에 따른 개인정보 보호 인증 전문기관 평가 내용, 제12조에 따른 국외이전전문위원회 평가 내용, 제13조에 따른 정책협의회 협의 내용 등을 종합적으로 고려하여, 보호위원회의 심의·의결을 거쳐 법 제28조의8제1항제4호에 따라 고시하는 인증을 정한다.

제15조(개인정보 국외 이전 인증) 제14조에 따라 보호위원회가 정하는 인증은 별표2와 같다.

제16조(유효기간과 갱신) ① 보호위원회는 영 제29조의8제2항에 따른 유효기간 만료 전에 해당 인증의 유효기간 갱신 여부를 심의하고, 이를 갱신할 수 있다.
② 제1항에 따른 심의를 하려는 경우 제11조부터 제14조까지의 절차를 거쳐야 한다.

제17조(인증의 제외) 보호위원회는 이 장에 따라 고시한 인증의 개인정보 보호 수준이 법 제32조의2에 따른 개인정보 보호 인증의 개인정보 보호 수준에 미치지 못한다고 판단하는 경우 해당 인증에 대해 제11조부터 제14조까지의 절차를 거쳐 해당 인증을 별표2에서 제외할 수 있다.

제4장 국가 등에 대한 개인정보 보호 수준 인정

제18조(이전대상국등 인정에 대한 국외이전전문위원회 평가) 국외이전전문위원회가 영 제29조의9제2항에 따라 평가를 할 때에는 영 제29조의9제1항 각 호의 사항에 따라 이전대상국등의 개인정보 보호 수준, 정보주체의 권리 보호 적절성 등을 평가하고 평가 내용을 보호위원회에 제출하여야 한다.

제19조(이전대상국등 인정에 대한 정책협의회의 협의) 보호위원회는 영 제29조의9제2항제2호에 따라 정책협의회를 개최하여 해당 이전대상국등 인정에 대해 관계기관과 협의하여야 한다.

제20조(이전대상국등 인정에 대한 보호위원회 심의·의결) 보호위원회는 제18조에 따른 국외이전전문위원회 평가 내용 및 제19조에 따른 정책협의회 협의 내용 등을 종합적으로 고려하여, 보호위원회의 심의·의결을 거쳐 법 제28조의8제1항제5호에 따라 이전대상국등의 인정 여부를 정한다.

제21조(이전대상국등 인정기간 및 갱신) ① 보호위원회는 영 제29조의9제3항에 따른 이전대상국등의 인정 기간 만료 전에 갱신 여부를 심의하고, 이를 연장할 수 있다.
② 제1항에 따른 심의를 하려는 경우 제18조부터 제20조까지의 절차를 거쳐야 한다.

제22조(이전대상국등 인정의 내용변경 및 취소 등) 보호위원회는 영 제29조9제5항에 따라 인정을 취소하거나 그 내용을 변경할 경우에는 해당 이전대상국등의 의견을 듣고 제18조부터 제20조까지의 절차를 거쳐야 한다.

제5장 개인정보 국외 이전 중지 명령

제23조(국외 이전 중지 명령에 대한 국외이전전문위원회 평가 등)

국외이전전문위원회가 영 제29조의11제2항에 따른 평가를 할 때에는 영 제29조의11제1항 각 호의 사항에 따라 법령 위반의 중대성, 피해의 심각성 등을 평가하고 평가 내용을 보호위원회에 제출하여야 한다.

제24조(국외 이전 중지 명령에 대한 보호위원회 심의·의결) ①

보호위원회는 국외이전전문위원회 평가 내용 등을 고려하여 보호위원회의 심의·의결을 거쳐 해당 개인정보처리자에 대한 개인정보 국외 이전 중지를 명한다.

② 보호위원회는 중지 명령 심의에 필요한 경우 해당 개인정보처리자에게 관련 자료를 요청할 수 있다.

제25조(국외 이전 중지 명령의 통보 등) 영 제29조의11제3항에 따라

개인정보처리자에게 국외 이전 중지를 명하는 문서는 별지 제1호 서식에 따른다.

제26조(국외 이전 중지 명령 이의 제기 등) ① 영 제29조의12제1항에 따라

보호위원회가 정하는 이의신청서는 별지 제2호의 서식에 따른다.

② 보호위원회는 제1항에 따른 중지 명령 이의제기를 받은 경우에는 30일 이내에 중지 명령 해제 여부를 결정하고 그 내용을 신청인에게 문서로 알려야 한다.

제27조(국외 이전 중지 명령의 해제) ①

보호위원회는 다음 각 호의 어느 하나에 해당하는 경우 개인정보의 국외 이전 중지 명령을 해제할 수 있다.

1. 보호위원회가 법 제28조의9제1항 각 호의 어느 하나에 해당하지 않는다고 인정하는 경우
2. 보호위원회가 개인정보처리자의 법 제28조의9제2항에 따른 이의제기가 정당하다고 인정하는 경우

3. 그 밖에 보호위원회가 필요하다고 인정하는 경우
- ② 법 제28조의9에 따라 국외 이전의 중지를 명령받은 개인정보처리자가 제1항제1호에 따라 중지 명령의 해제를 요청하려는 경우에는 별지 제3호의 서식과 이를 증명하는데 필요한 서류를 첨부하여 보호위원회에 제출하여야 한다.
- ③ 보호위원회는 제1항에 따라 중지 명령을 해제할 때에는 해당 개인정보처리자에게 문서로 알려야 한다.

제6장 보 칙

제28조(재검토기한) 보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2023년 9월 15일 기준으로 매 3년이 되는 시점(매 3년째의 9월 14일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2023-11호, 2023.10.16.>

이 고시는 공포한 날부터 시행한다.

개인정보 국외 이전 인증 평가 기준 (제11조~제14조 관련)

구분	세부 평가항목
가. 합법적인 처리근거	1) 수집 · 이용 · 제공 2) 목적 외 이용 · 제공 3) 가명정보의 처리
나. 최소처리	1) 사생활 침해 최소화, 가명처리 · 익명처리 2) 수집 제한 3) 보유기간 제한 4) 파기
다. 정보주체 권리	1) 열람 2) 정정 · 삭제 3) 처리정지 4) 전송요구권 5) 자동화된 결정에 대한 대응권 6) 피해구제 7) 손해배상 청구권
라. 투명성	1) 처리방침 공개 2) 출처 통지 3) 이용내역 확인
마. 책임성	1) 정확성 · 최신성 · 완전성 2) 영업양도 3) 영향평가 4) 보호책임자 지정 5) 위탁 6) 국내대리인 지정
바. 안전성	1) 관리적 보호조치 2) 기술적 보호조치 3) 물리적 보호조치 4) 노출된 개인정보의 삭제 · 차단
사. 특별한 보호가 요구되는 개인정보 처리	1) 아동 개인정보 2) 민감정보 3) 고유식별정보(주민등록번호 포함) 4) 영상정보(고정형, 이동형)
아. 침해대책 및 대응	1) 침해사고 예방 및 대응체계 구축 2) 침해사고 대응 및 복구 3) 유출 등의 통지 신고
자. 국외 이전	1) 이전 2) 재이전
차. 인증제도 운영	

개인정보 국외 이전 인증 (제15조 관련)

인증명	인증 유효기간	비고
1. ISMS-P	해당 없음	법 제32조의2에 따른 개인정보 보호 인증

개인정보 국외 이전 중지 명령서

중지 명령 확인번호	제 호	
상호(명칭)	상호(명칭)	사업자등록번호
	소재지	
대표자	성명	전화번호
중지 명령	명령의 내용	
	사유	
	이의제기 기간	

「개인정보 보호법」 제28조의9제1항 및 같은 법 시행령 제29조의11제3항에 따라 위와 같이 개인정보 국외 이전 중지를 명합니다.

년 월 일

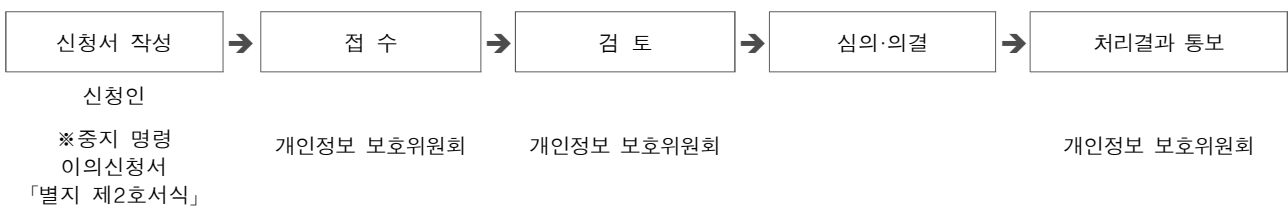
개인정보 보호위원회

직인

유의사항

「개인정보 보호법」 제28조의9 제1항에 따른 개인정보 국외 이전 중지 명령을 위반한 경우 같은 법 제64조의2제1항제8호에 따라 과징금을 부과받게 됩니다.

이의제기 절차 및 방법



210mm×297mm[백상지 80g/㎡(재활용품)]

개인정보 국외 이전 중지 명령 이의신청서

※ 바탕색이 어두운 칸은 신청인이 작성하지 않습니다.

접수번호	접수일		처리기간 30일
중지 명령 대상	상호(명칭)		사업자등록번호
	중지 명령이 있는(도달한) 날		중지 명령 확인번호
신청인 (대리인)	성명	생년월일	전화번호
이의신청	내용		
	사유		

「개인정보 보호법」 제28조의9제2항 및 같은 법 시행령 제29조의12제1항에 따라 개인정보 국외 이전 중지 명령 결정에 대하여 이의를 신청합니다.

년 월 일

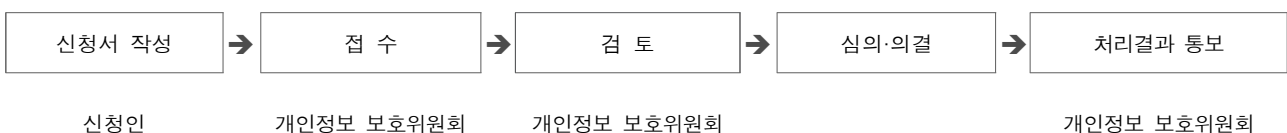
신청인

(서명 또는 인)

개인정보 보호위원회 귀중

첨부서류	1. 대리인인 경우 위임장 2. 이의신청 사유를 증명할 수 있는 자료(필요시 제출)	수수료 없음
------	---	-----------

절차 및 방법



210mm×297mm[백상지 80g/㎡(재활용품)]

개인정보 국외 이전 중지 명령 해제신청서

※ 바탕색이 어두운 칸은 신청인이 작성하지 않습니다.

접수번호	접수일	처리기간
중지 명령 대상	상호(명칭)	사업자등록번호
	중지 명령이 있는(도달한) 날	중지 명령 확인번호
신청인 (대리인)	성명	생년월일
		전화번호
해제신청	내용	

「개인정보 국외 이전 운영 등에 관한 규정」 제27조 제2항에 따라 개인정보 국외 이전 중지 명령 결정에 대하여 해제신청합니다.

년 월 일

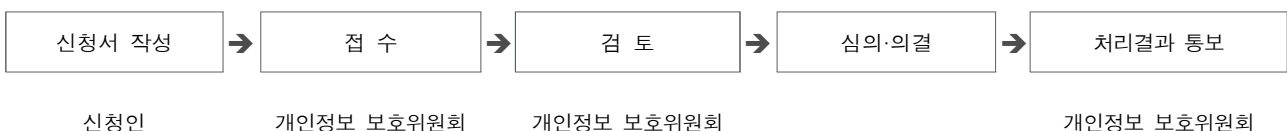
신청인

(서명 또는 인)

개인정보 보호위원회 귀중

첨부서류	1. 대리인인 경우 위임장 2. 법 제28조의9 제1항 제1호 상황에 해당하지 않음을 증명할 수 있는 자료	수수료 없음
------	--	-----------

절차 및 방법



210mm×297mm[백상지 80g/㎡(재활용품)]

[시행 2023. 10. 16.] [개인정보보호위원회고시 제2023-12호, 2023. 10. 16., 일부개정]

제1조(목적) 이 고시는 「개인정보 보호법」 제18조제4항·제22조제2항, 같은 법 시행령 제15조·제34조제1항·제41조제3항 및 제5항·제43조제3항·제44조제2항·제45조제2항에서 위임된 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(공공기관에 의한 개인정보의 목적 외 이용 또는 제3자 제공의 공고) 공공기관은 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공(이하 "목적외이용등"이라 한다)하는 경우에는 「개인정보 보호법」(이하 "법"이라 한다) 제18조제4항에 따라 개인정보를 목적외이용등을 **한 날부터 30일 이내에** 다음 각 호의 사항을 관보 또는 인터넷 홈페이지에 게재하여야 한다. 이 경우 인터넷 홈페이지에 게재할 때에는 **10일 이상 계속 게재**하여야 한다.

1. 목적외이용등을 한 날짜
2. 목적외이용등의 법적 근거
3. 목적외이용등의 목적
4. 목적외이용등을 한 개인정보의 항목(구성)

제3조(개인정보 보호업무 관련 장부 및 문서 서식) ① 법 제18조제2항과 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제15조에 따른 개인정보의 목적 외 이용 및 제3자 제공 대장은 별지 제1호서식과 같다.

- ② 법 제32조제1항과 영 제34조제1항에 따른 개인정보파일 등록 신청 및 변경등록 신청은 별지 제2호서식의 개인정보파일 등록·변경등록 신청서에 따른다.
- ③ 법 제35조제2항과 영 제41조제3항에 따른 개인정보 열람의 요구는 별지 제8호서식의 개인정보 열람 요구서에 따른다.
- ④ 법 제35조제5항과 영 제41조제5항에 따른 개인정보 열람 및 일부열람의 통지, 법 제35조제3항 후단과 영 제42조제2항에 따른 개인정보 열람연기의 통지, 법 제35조제4항과 영 제42조제2항에 따른 열람거절의 통지는 별지 제9호서식의 개인정보 열람, 일부열람, 열람연기, 열람거절 통지서에 따른다.
- ⑤ 법 제36조제6항과 영 제43조제3항에 따른 개인정보 정정·삭제 요구에 대한 결과의 통지, 법 제37조제6항과 영 제44조제2항에 따른 개인정보 처리정지 요구에 대한 결과의 통지는 별지 제10호서식의 개인정보 정정·삭제, 처리정지 요구에 대한 결과 통지서에 따른다.
- ⑥ 영 제45조제2항에 따른 정보주체의 위임장은 별지 제11호서식과 같다.

제4조(서면 동의 시 중요한 내용의 표시 방법) 법 제22조제2항에서 "보호위원회가 고시로

정하는 방법"이란 다음 각 호의 방법을 통해 종이 인쇄물, 컴퓨터 표시화면 등 서면 동의를 요구하는 매체의 특성과 정보주체의 이용환경 등을 고려하여 정보주체가 쉽게 알아볼 수 있도록 표시하는 방법을 말한다.

1. 글씨의 **크기, 색깔, 굵기 또는 밑줄** 등을 통하여 그 내용이 명확히 표시되도록 할 것
2. 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 **그 밖의 내용과 별도로 구분하여 표시**할 것

부칙 <제2023-12호, 2023.10.16.>

이 고시는 공포한 날부터 시행한다.

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[] 목적외 이용 [] 제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의 경우)		담당자	소 속
			성 명
			전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	성 명
			소 속
			전화번호
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			

210mm×297mm[인쇄용지(특급) 34g/㎡]

개인정보파일 (☐ 등록 ☐ 변경등록) 신청서

※ '변경정보 및 변경사유' 란은 변경등록시에만 작성합니다.

접수번호	접수일	처리기간	7일
------	-----	------	----

공공기관 명칭	주소	등록부서	전화번호
---------	----	------	------

등록항목	등록정보	변경정보 및 변경사유
개인정보파일 명칭		
개인정보파일의 운영 근거 및 목적		
개인정보파일에 기록되는 개인정보의 항목		
개인정보의 처리방법		
개인정보의 보유기간		
개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자		
개인정보파일을 운용하는 공공기관의 명칭		
개인정보파일로 보유하고 있는 개인정보의 정보주체 수		
해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서		
개인정보의 열람 요구를 접수·처리하는 부서		
개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유		

「개인정보 보호법」 제32조제1항과 같은 법 시행령 제34조제1항에 따라 위와 같이 개인정보파일 (☐ 등록 ☐ 변경등록) 을 신청합니다.

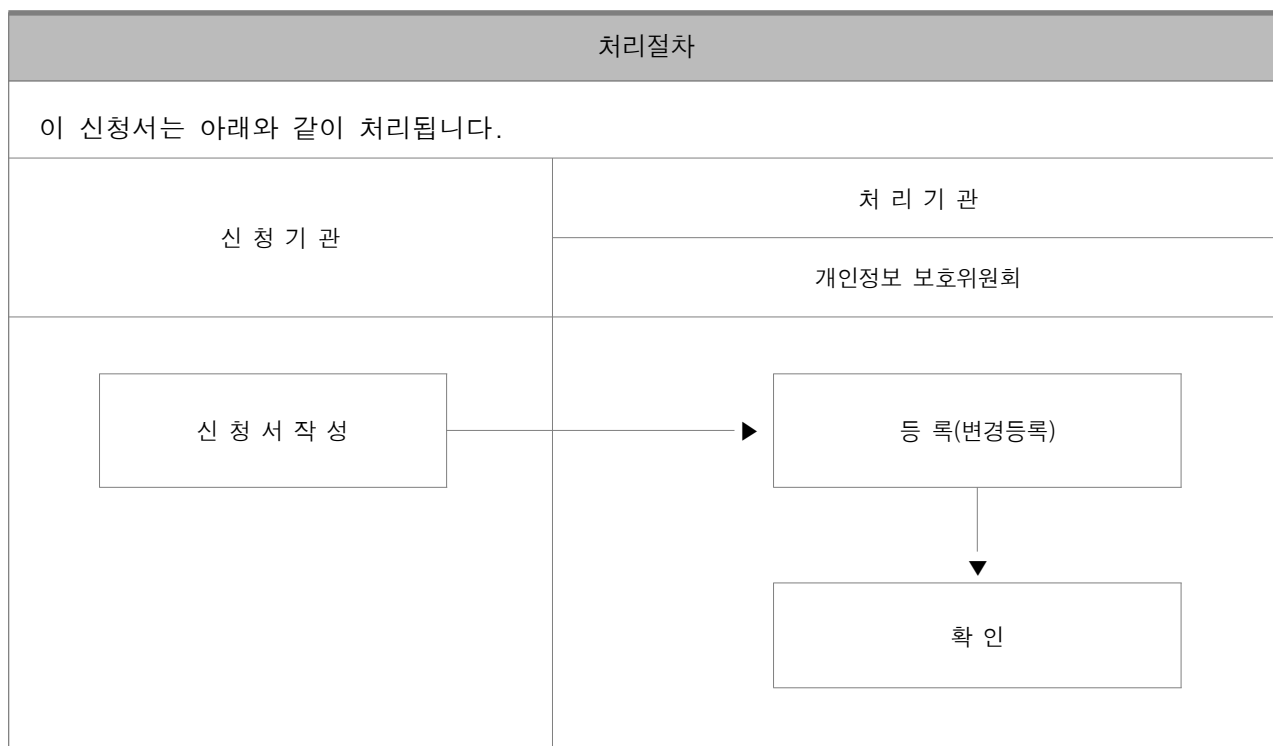
년 월 일

신청기관

(서명 또는 인)

개인정보 보호위원회 귀하

210mm×297mm[일반용지 70g/㎡(재활용품)]



개인정보 열람 요구서

※ 아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.

(앞 쪽)

접수번호	접수일	처리기간	10일 이내
정보주체	성 명	전 화 번 호	
	생년월일		
	주 소		
대리인	성 명	전 화 번 호	
	생년월일	정보주체와의 관계	
	주 소		
요구내용	[] 개인정보의 항목 및 내용 [] 개인정보 수집·이용의 목적 [] 개인정보 보유 및 이용 기간 [] 개인정보의 제3자 제공 현황 [] 개인정보 처리에 동의한 사실 및 내용		

「개인정보 보호법」 제35조제2항과 같은 법 시행령 제41조제3항에 따라 위와 같이 요구합니다.

년 월 일

요구인

(서명 또는 인)

개인정보 보호위원회 귀하

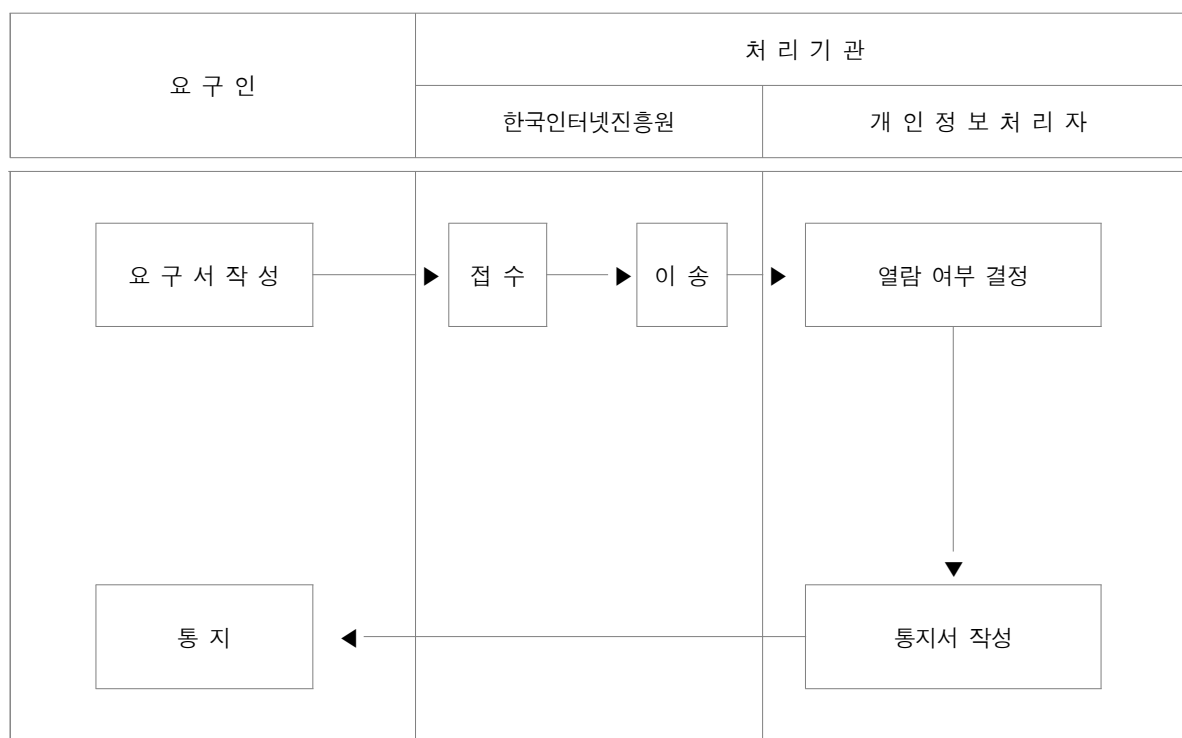
작성 방법

1. '대리인' 란은 대리인이 요구인일 때에만 적습니다.
2. '요구내용' 란은 열람하려는 사항을 선택하여 [√] 표시를 합니다. 표시를 하지 않은 경우에는 해당 항목의 열람을 요구하지 않은 것으로 처리됩니다.

210mm×297mm[백상지(80g/㎡) 또는 중질지(80g/㎡)]

처리절차

이 요구서는 아래와 같이 처리됩니다.



개인정보 (☐ 열람 ☐ 일부열람 ☐ 열람연기 ☐ 열람거절) 통지서

(앞 쪽)

수신자 (우편번호: , 주소:)

요구 내용			
열람 일시			열람 장소
통지 내용 (<input type="checkbox"/> 열람 <input type="checkbox"/> 일부열람 <input type="checkbox"/> 열람연기 <input type="checkbox"/> 열람거절)			
열람 형태 및 방법	열람 형태	<input type="checkbox"/> 열람·시청 <input type="checkbox"/> 사본·출력물 <input type="checkbox"/> 전자파일 <input type="checkbox"/> 복제물·인화물 <input type="checkbox"/> 기타	
	열람 방법	<input type="checkbox"/> 직접방문 <input type="checkbox"/> 우편 <input type="checkbox"/> 팩스 <input type="checkbox"/> 전자우편 <input type="checkbox"/> 기타	
납부 금액	①수수료	②우송료	계(①+②)
	원	원	원
	수수료 산정 명세		
사 유			
이의제기방법	※ 개인정보처리자는 이의제기방법을 적습니다.		

「개인정보 보호법」 제35조제3항·제4항 또는 제5항과 같은 법 시행령 제41조제5항 또는 제42조제2항에 따라 귀하의 개인정보 열람 요구에 대하여 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

210mm×297mm[신문용지 54g/㎡]

유의사항

1. 개인정보 열람 장소에 오실 때에는 이 통지서를 지참하여야 하며, 요구인 본인 또는 그 정당한 대리인임을 확인하기 위하여 다음의 구분에 따른 증명서를 지참하여야 합니다.
 - 가. 요구인 본인에게 공개할 때: 요구인의 신원을 확인할 수 있는 신분증명서(주민등록증 등)
 - 나. 요구인의 대리인에게 공개할 때: 대리인임을 증명할 수 있는 서류와 대리인의 신원을 확인할 수 있는 신분증명서
2. 수수료 또는 우송료는 다음의 구분에 따른 방법으로 냅니다.
 - 가. 국가기관인 개인정보처리자에게 내는 경우: 수입인지
 - 나. 지방자치단체인 개인정보처리자에게 내는 경우: 수입증지
 - 다. 국가기관 및 지방자치단체 외의 개인정보처리자에게 내는 경우: 해당 개인정보처리자가 정하는 방법

※ 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속 기관 또는 지방자치단체인 개인정보처리자에게 수수료 또는 우송료를 내는 경우에는 「전자금융거래법」 제2조제11호에 따른 전자지급수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 낼 수 있습니다.
3. 열람제한, 열람연기 또는 열람거절의 통지를 받은 경우에는 개인정보처리자가 이의제기방법란에 적은 방법으로 이의제기를 할 수 있습니다.

개인정보 ([] 정정·삭제, [] 처리정지) 요구에 대한 결과 통지서

수신자 (우편번호: , 주소:)

요구 내용	
<input type="checkbox"/> 정정·삭제 <input type="checkbox"/> 처리정지 조치 내용	
<input type="checkbox"/> 정정·삭제 <input type="checkbox"/> 처리정지 결정 사유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.

「개인정보 보호법」 제36조제6항 및 같은 법 시행령 제43조제3항 또는 같은 법 제37조제6항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

유의사항

개인정보의 정정·삭제 또는 처리정지 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.

위임장

위임받는 자	성명	전화번호
	생년월일	정보주체와의 관계
	주소	
위임자	성명	전화번호
	생년월일	
	주소	

「개인정보 보호법」 제38조제1항에 따라 위와 같이 개인정보의 (☐ 열람, ☐ 정정·삭제, ☐ 처리정지)의 요구를 위의 자에게 위임합니다.

년 월 일

위임자

(서명 또는 인)

0000 귀하

위임장

위임받는 자	성명	전 화 번 호
	생년월일	정보주체와의 관계
	주소	
위임자	성명	전화번호
	생년월일	
	주소	

「개인정보 보호법」 제38조제1항에 따라 위와 같이 개인정보의 (☐ 열람, ☐ 정정·삭제, ☐ 처리정지)의 요구를 위의 자에게 위임합니다.

년 월 일

위임자

(서명 또는 인)

0000 귀하

[시행 2024. 2. 20.] [개인정보보호위원회고시 제2024-3호, 2024. 2. 20., 제정]

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다)제30조의2와 같은법 시행령(이하 "영"이라 한다) 제31조의2에 따라 개인정보 처리방침 평가대상 선정과 평가절차 등에 관한 세부기준을 정함을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "개인정보 처리방침"(이하 "처리방침"이라 한다)이란 법 제30조에 따라 개인정보 처리 기준 및 보호조치 등에 관해 개인정보처리자가 수립하여 공개한 문서를 말한다.
2. "개인정보 처리방침 평가"(이하 "처리방침 평가"라 한다)란 개인정보보호위원회(이하 "보호위원회"라 한다)가 개인정보처리자의 처리방침이 법 제30조의2제1항 각 호의 기준에 부합하는지 여부를 평가하는 것을 말한다.
3. "평가 대상"이란 보호위원회가 법 제30조의2제1항에 따른 평가를 위하여 영 제31조의2 각 호의 사항을 종합적으로 고려하여 보호위원회가 선정한 처리방침을 말한다.

제3조(평가계획의 수립) ① 보호위원회는 법 제30조의2에 따른 처리방침 평가를 수행하는 경우 매년 평가 시작일을 기준으로 14일 전까지 평가 대상, 기준, 절차 및 일정 등을 정한 평가계획을 수립하여 심의·의결한다.
② 보호위원회는 제1항에 따라 평가계획을 의결한 경우 지체없이 보호위원회 홈페이지에 공개하여야 한다.

제4조(평가 대상) ① 영 제31조의2제1항에 따른 개인정보 처리방침의 평가 대상은 다음 각 호의 사항을 종합적으로 고려하여 처리방침 평가가 필요하다고 보호위원회가 심의·의결한 자로 한다.

1. 전년도(법인의 경우에는 전 사업연도를 말하며, 이하 이 조에서 같다)의 매출액이 1,500억원 이상이면서 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 정보주체의 수가 일일평균 100만명 이상일 것
2. 전년도 말 기준 직전 3개월간 법 제23조제1항에 따른 민감정보(이하 "민감정보"라 한다) 또는 법 제24조제1항에 따른 고유식별정보(이하 "고유식별정보"라 한다)가 저장·관리되고 있는 정보주체의 수가 일일평균 5만명(업무수행을 위해 처리되는 그에 소속된 임직원의 민감정보나 고유식별정보는 제외한다) 이상일 것
3. 개인정보 처리방침에 법 제22조제3항에 따라 정보주체의 동의 없이 처리할 수 있는 개인정보의 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하고 있지 않을 것
4. 법 제37조의2에 따라 완전히 자동화된 시스템(인공지능 기술을 적용한 시스템을 포함한다)으로 개인정보를 처리하거나, 그 밖에 새로운 기술을 이용한 개인정보

- 처리 방식으로 인하여 개인정보 침해 발생 우려가 있을 것
5. 최근 3년 간 다음 각 목의 어느 하나에 해당할 것
 - 가. 2회 이상 법 제34조에 따른 개인정보 유출등이 되었을 것
 - 나. 법 제62조의2에 따른 과징금을 부과 받았을 것
 - 다. 법 제75조에 따른 과태료를 부과 받았을 것
 6. 19세 미만 아동 또는 청소년을 주된 이용자로 하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제2호에 따른 정보통신서비스를 운영할 것
- ② 보호위원회는 필요한 경우 평가 대상을 선정하기 전에 개인정보처리자에게 제1항 각 호의 평가 대상에 해당하는지 여부에 대한 확인을 요청할 수 있다.

제5조(평가 절차) ① 처리방침 평가는 평가계획 수립 및 통지, 평가위원회 구성, 서류 검토 등 평가 수행, 평가 결과 통지 등의 절차에 따라 실시한다.

② 보호위원회는 제4조에 따라 선정된 평가 대상이 법 제30조의2제1항 각 호의 기준에 부합하는지 평가한다.

③ 보호위원회는 영 제31조의2제3항에 따라 개인정보처리자가 의견을 제출한 경우 그 내용의 타당성 등을 검토하여 평가에 반영할 수 있다.

④ 보호위원회는 영 제31조의2제4항에 따라 평가 결과를 지체없이 해당 개인정보처리자에게 통지하여야 한다.

제6조(평가위원회 구성 및 운영) ① 보호위원회는 처리방침 평가를 위해 처리방침 평가위원회(이하 "평가위원회"라 한다)를 구성·운영할 수 있다.

② 평가위원회는 위원장 1명을 포함하여 보호위원회가 위촉하는 20명 이상 50명 이내의 개인정보 보호에 관한 학식과 경험이 풍부한 외부 전문가로 다음 각 호의 경력을 가진 사람 중에서 구성한다.

1. 「고등교육법」제2조제1호·제2호 또는 제5호에 따른 학교나 공인된 연구기관에서 조교수 이상의 직 또는 이에 상당하는 직에 있거나 있었던 자로 개인정보 보호 연구경력이 3년 이상인 사람
2. 개인정보 보호 관련 업체, 기관 또는 단체(협회, 조합)에서 3년 이상 개인정보 보호 업무에 종사한 사람
3. 그 밖에 개인정보 안전한 활용, 정보보호·보안에 관한 학식과 경험이 풍부한 사람

③ 평가위원의 임기는 1년으로 하되 연임할 수 있으며, 위원장은 보호위원회 위원장이 위촉한다.

④ 평가위원은 업무에 직접 관여하는 등 직접적인 이해관계가 있거나 공정성을 기할 수 없는 현저한 사유가 있는 경우에는 해당 평가 대상의 평가에 관여할 수 없다.

⑤ 필요한 경우 평가위원회에 전문위원회를 둘 수 있다.

제7조(이의신청) ① 처리방침 평가를 받은 개인정보처리자는 제5조제4항에 따른 평가결과에 이의가 있는 경우 평가결과를 통보받은 날로부터 20일 이내에 별지 서식을 작성하여 보호위원회에 제출하여야 한다.

- ② 보호위원회는 제1항에 따른 이의신청을 받은 날로부터 30일 이내에 이의신청 내용을 검토하여 타당성이 인정되는 경우 평가 결과에 반영하여야 하며, 그 결과를 이의신청을 한 자에게 통지하여야 한다. 다만 부득이한 사정이 있는 경우 14일의 범위에서 그 기간을 연장할 수 있다.

- 제8조(평가결과의 활용 및 지원)** ① 보호위원회는 처리방침 평가 결과 개선이 필요한 경우 법 제61조제2항에 따른 개선권고를 할 수 있으며, 법 제66조에 따라 개선권고의 내용 및 결과에 대하여 공표하거나, 개선권고를 받은 자에게 개선권고를 받았다는 사실을 공표할 것을 명할 수 있다. 이 경우 공표 또는 공표명령의 기준은 별표와 같다.
- ② 제1항에 따라 개선권고를 받은 개인정보처리자는 그 조치결과를 보호위원회에 알려야 하며, 보호위원회는 이행 여부를 점검할 수 있다.
- ③ 보호위원회는 처리방침 평가 결과 우수한 개인정보처리자에 대하여 포상할 수 있다.
- ④ 보호위원회는 처리방침 평가 우수 사례를 홍보하거나 컨설팅 지원 등에 활용할 수 있다.
- ⑤ 보호위원회는 개인정보처리자의 개인정보 처리방침 작성 지침 준수를 위한 지원을 할 수 있다.

제9조(재검토기한) 보호위원회는 이 고시에 대하여 「행정규제기본법」 및 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2024년 1월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2024-3호, 2024.02.20.>

이 고시는 발령한 날부터 시행한다. 다만, 제4조제1항제4호의 개정규정은 2024년 3월 15일부터 시행한다.

[별표 1]

개인정보 처리방침 평가 결과의 공표 및 공표명령 기준(제8조제1항 관련)

1. 공표 및 공표명령 요건

가. 공표 요건

- 1) 처리방침 평가 결과 필수 작성항목을 미작성하거나, 그 작성 내용이 개인정보 보호 원칙에 비추어 부적정한 경우
- 2) 조치기한 내에 정당한 사유없이 개선권고를 불이행한 경우

나. 공표명령 요건

다수 정보주체의 권리에 중대한 침해가 발생할 우려가 있는 위반사항이 있거나, 권익구제 조치를 취할 수 있도록 알릴 필요가 있는 경우

2. 공표내용·방법 및 세부절차

가. 공표 및 공표명령의 내용 및 방법에 관한 사항은 보호위원회가 별도로 정하는 바에 따른다.

나. 의견청취 등 공표 절차에 관한 사항은 「개인정보 보호위원회의 조사 및 처분에 관한 규정」을 준용한다.

개인정보 처리방침 평가결과 이의신청서

이의신청자	기관·단체명	대표자 성명
	전화번호/FAX	전자우편
	주소	

이의신청 사유	<p>※ 증빙자료는 별도 첨부</p>
---------	----------------------

개인정보 처리방침 평가에 관한 고시 제7조제1항에 따라 위와 같이 개인정보 처리방침 평가결과에 대하여 이의를 신청합니다.

2024년 월 일

신청인

(서명 또는 인)

개인정보보호위원회 귀하

첨부서류	이의신청 사유를 증명하는 서류	
------	------------------	--

[시행 2024. 7. 24] [과학기술정보통신부 제2024-30호, 2024. 7. 24, 일부개정]
 [시행 2024. 7. 24.] [개인정보보호위원회고시 제2024-8호, 2024. 7. 24., 일부개정]

제1장 총칙

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다) 제47조제3항·제4항, 같은 법 시행령 제47조부터 제53조의2까지의 규정 및 같은 법 시행규칙 제3조에 따른 정보보호 관리체계 인증과, 「개인정보 보호법」 제32조의2, 같은 법 시행령 제34조의2부터 제34조의8까지의 규정에 따른 개인정보보호 인증의 통합 운영에 필요한 사항을 정하는 것을 목적으로 한다.

제2조(정의) 이 고시에서 사용하는 용어의 뜻은 다음 각 호와 같다.

1. "정보보호 및 개인정보보호 관리체계 인증"이란 인증 신청인의 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다) 또는 인증기관이 증명하는 것을 말한다.
2. "정보보호 관리체계 인증"이란 인증 신청인의 정보보호 관련 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 것을 말한다.
3. "인증기관"이란 인증에 관한 업무를 수행할 수 있도록 정보통신망법 제47조제6항, 「개인정보 보호법 시행령」제34조의6제1항제2호 및 제2항에 따라 과학기술정보통신부장관과 개인정보 보호위원회(이하 "보호위원회"라 한다)가 지정하는 기관을 말한다.
4. "심사기관"이란 인증심사 업무를 수행할 수 있도록 정보통신망법 제47조제7항, 「개인정보 보호법 시행령」제34조의6제1항제2호 및 제2항에 따라 과학기술정보통신부장관과 보호위원회가 지정하는 기관을 말한다.
5. "업무수행 요건·능력 심사"란 인증기관 또는 심사기관으로 지정받고자 신청한 법인 또는 단체의 업무수행 요건·능력을 심사하는 것을 말한다.
6. "인증심사"란 신청기관이 수립하여 운영하는 관리체계가 인증기준에 적합한지의 여부를 인터넷진흥원·인증기관 또는 심사기관(이하 "심사수행기관"이라 한다)이 서면심사 및 현장심사의 방법으로 확인하는 것을 말한다.
7. "인증위원회"란 인터넷진흥원 또는 인증기관의 장이 인증심사 결과 등을 심의·의결하기 위해 설치·운영하는 기구로서 위원장과 위원으로 구성된다.
8. "인증심사원"이란 인터넷진흥원으로부터 인증심사를 수행할 수 있는 자격을 부여받고 인증심사를 수행하는 자를 말한다.
- 8의2. "심사팀장"이란 인증심사를 수행하기 위해 구성한 팀의 책임자를 말한다.
9. "최초심사"란 처음으로 인증을 신청하거나 인증범위에 중요한 변경이 있어서 다시 인증을 신청한 때 실시하는 인증심사를 말한다.

10. "사후심사"란 인증(인증이 갱신된 경우를 포함한다)을 받고난 후 매년 사후관리를 위하여 실시하는 인증심사를 말한다.
11. "갱신심사"란 유효기간 만료로 유효기간 갱신을 위해 실시하는 인증심사를 말한다.

제3조(적용범위) 이 고시는 정보보호 및 개인정보보호 관리체계 인증, 정보보호 관리체계 인증에 공통으로 적용하되, 각 인증에 따로 적용되는 내용이 있는 경우 별도 조항으로 정한다.

제2장 정보보호 및 개인정보보호 관리체계 인증 협의회

- 제4조(협의회의 구성)** ① 과학기술정보통신부장관과 보호위원회는 정보보호 및 개인정보보호 관리체계 인증 운영에 관한 정책 사항을 협의하기 위하여 정보보호 및 개인정보보호 관리체계 인증 협의회(이하 "협의회"라 한다)를 운영한다.
- ② 협의회 위원은 과학기술정보통신부와 보호위원회 소속의 인증업무를 담당하는 부서의 장으로 한다.
- ③ 협의회 운영을 위하여 인터넷진흥원의 인증업무를 담당하는 부서의 장을 간사로 두며, 간사는 회의에 참석하여 발언할 수 있다.

제5조(협의회의 운영) ① 협의회는 정보보호 및 개인정보보호 관리체계 인증제도와 관련하여 다음 각 호의 사항을 협의한다.

1. 인증제도 연구 및 개선에 관한 사항
 2. 인증제도 운영을 위한 제반사항 검토 및 품질관리에 관한 사항
 3. 인증기관 및 심사기관의 지정·재지정 및 업무정지·지정 취소에 관한 사항
 4. 인증기관 및 심사기관의 관리·감독에 관한 사항
 5. 인증제도 운영에 따른 민원 처리 및 법적 분쟁에 관한 사항
 6. 그 밖에 협의회가 필요한 사항
- ② 협의회는 과학기술정보통신부장관 또는 보호위원회의 요구가 있거나 협의안건이 발생한 경우 개최할 수 있다.
- ③ 인터넷진흥원은 협의회 개최 및 제1항 각 호에 따른 협의회 운영 업무를 지원할 수 있다.
- ④ 협의회는 필요하다고 인정하는 때에는 관계기관의 공무원 및 임·직원, 그 밖의 전문가를 협의회에 참석하게 하여 그 의견을 들을 수 있다.
- ⑤ 협의회는 협의회의 운영을 위한 별도의 규정을 정할 수 있다.

제3장 인증기관 및 심사기관

- 제6조(지정공고)** ① 과학기술정보통신부장관과 보호위원회는 인증기관을 지정할 필요가 있는 때에는 협의회에서 지정대상 기관의 수, 업무의 범위, 신청방법 등을 미리 협의하고, 관보 또는 인터넷 홈페이지에 20일 이상 공고하여야 한다.
- ② 제1항에 따라 인증기관으로 지정받으려는 자는 다음 각 호의 서류를

과학기술정보통신부장관과 보호위원회에 제출하여야 한다.

1. 별지 제1호서식의 인증기관·심사기관 지정 신청서

2. 별지 제2호서식의 인증심사 업무를 수행하는 직원 보유현황과 이를 증명할 수 있는 서류

3. 별표 1의 업무수행 요건·능력 심사 제출서류

③ 심사기관 지정 신청일을 기준으로 다음 각 호의 어느 하나에 해당하는 자는 심사기관으로 지정받을 수 없다.

1. 최근 6개월 이내에 제7조제2항에 따른 심사에서 지정기준을 충족하지 못한 자

2. 최근 1년 이내에 정보통신망 제47조의2제1항에 따라 지정이 취소된 자

④ 과학기술정보통신부장관과 보호위원회는 인증기관 또는 심사기관의 지정, 재지정, 사후관리 등에 따른 업무를 인터넷진흥원에 위탁할 수 있다.

제7조(지정기준 및 지정절차) ① 인증기관 또는 심사기관의 업무수행 요건·능력 심사에 관한 세부기준은 별표 2와 같다.

② 과학기술정보통신부장관과 보호위원회는 제6조제2항에 따라 인증기관 또는 심사기관의 지정 신청을 받은 때에는 제1항에 따른 업무수행 요건·능력을 심사한다.

③ 과학기술정보통신부장관과 보호위원회는 제2항에 따른 심사 결과를 바탕으로 협의하여 인증기관 또는 심사기관으로의 지정여부를 최종 결정한다.

④ 과학기술정보통신부장관과 보호위원회는 인증기관으로 지정된 신청기관에 별지 제3호서식 정보보호 및 개인정보보호 관리체계 인증기관 지정서를, 심사기관으로 지정된 신청기관에 별지 제4호서식 정보보호 및 개인정보보호 관리체계 심사기관 지정서를 발급한다.

⑤ 과학기술정보통신부장관과 보호위원회는 제4항에 따라 지정서를 발급받은 자를 관보 또는 인터넷 홈페이지에 공고하여야 한다.

제8조(인증기관 및 심사기관의 사후관리) ① 인증기관과 심사기관은 매년 1월 31일까지 다음 각 호의 서류를 작성하여 과학기술정보통신부장관과 보호위원회에 제출하여야 한다.

1. 별지 제5호서식의 인증실적 보고서(해당 시)

2. 별지 제6호서식의 인증심사실적 보고서(해당 시)

② 과학기술정보통신부장관과 보호위원회는 필요한 경우 인증기관 또는 심사기관이 지정기준에 적합한지 여부의 확인을 위해 자료요청 또는 현장실사를 할 수 있다.

③ 과학기술정보통신부장관과 보호위원회는 제2항에 따른 지정기준의 충족여부 심사, 자료제출 요구 또는 현장심사에 관한 업무를 인터넷진흥원에 위탁할 수 있다.

④ 과학기술정보통신부장관과 보호위원회는 사후관리 결과 지정기준의 충족여부 등에 결격사유가 확인될 경우 보완을 요구할 수 있다.

제9조(인증기관 및 심사기관의 재지정) ① 인증기관 및 심사기관 지정의 유효기간은 3년이며 유효기간이 끝나기 전 6개월부터 끝나는 날까지 재지정을 신청을 할 수 있으며 제6조제2항 각 호의 서류를 과학기술정보통신부장관과 보호위원회에 제출하여야 한다. 이 경우 재지정의 신청에 대한 처리결과를 통지받을 때까지는 그 지정이 계속 유효한 것으로 본다.

- ② 과학기술정보통신부장관과 보호위원회는 제1항에 따른 재지정 신청을 받은 때에는 별표 2 업무수행 요건·능력 심사에 관한 세부기준에 따른 적합 여부를 심사하여 신청을 받은 날부터 3개월 이내에 그 결과를 신청기관에 통지하고, 인증기관 또는 심사기관으로 지정되는 신청기관에 제7조제4항의 지정서를 발급하여야 한다.
- ③ 인증기관 또는 심사기관이 재지정을 신청하지 않고 유효기간이 경과한 때에는 인증기관 또는 심사기관의 효력은 상실된다.

제10조(공정성 및 독립성 확보) 인증기관 및 심사기관은 인증심사의 공정성 및 독립성 확보를 위해 다음 각 호의 행위가 발생되지 않도록 노력하여야 한다.

- 1. 정보보호 및 개인정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하는 행위
- 2. 정당한 사유 없이 인증절차, 인증기준 등의 일부를 생략하는 행위
- 3. 조직의 이익 등을 위해 인증심사 결과에 영향을 주는 행위
- 4. 그 밖에 인증심사의 공정성 및 독립성을 훼손할 수 있는 행위

제11조(인증기관 및 심사기관의 지정취소 등) ① 인증기관 및 심사기관이 다음 각 호의 어느 하나에 해당하면 그 지정을 취소하거나 1년 이내의 기간을 정하여 해당 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호나 제2호에 해당하는 경우에는 그 지정을 취소하여야 한다.

- 1. 거짓이나 그 밖의 부정한 방법으로 인증기관 또는 심사기관의 지정을 받은 경우
- 2. 업무정지 기간 중에 인증 또는 인증심사를 한 경우
- 3. 정당한 사유 없이 인증 또는 인증심사를 하지 아니한 경우
- 4. 정보통신망법 제47조제11항 및 개인정보보호법 제32조의2제5항을 위반하여 인증 또는 인증심사를 한 경우
- 5. 정보통신망법 제47조제12항 및 개인정보보호법 시행령 제34조의6제1항제2호에 따른 지정기준에 적합하지 아니하게 된 경우

② 지정취소 및 업무정지에 대해서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(이하 "정보통신망법 시행령"이라 한다)」제54조에 따른 지정취소 및 업무정지에 관한 행정처분의 기준을 따른다.

③ 과학기술정보통신부장관과 보호위원회는 제1항에 따라 지정을 취소하거나 업무정지를 명한 사실을 관보 또는 인터넷 홈페이지에 공고 하여야 한다.

제4장 인증심사원

제12조(인증심사원의 자격 요건 등) 인증심사원은 심사원보, 심사원, 선임심사원으로 구분하며 등급별 자격 요건은 별표 3과 같다.

제13조(인증심사원 자격 신청) ① 인증심사원 자격을 신청하고자 하는 자는 별표 4의 인증심사원 자격 신청 요건을 갖추고 인터넷진흥원이 공고하는 신청기간 내에 별지 제7호 서식의 인증심사원 자격 신청서와 관련 서류를 제출하여야 한다.

- ② 인터넷진흥원은 제1항에 의해 제출한 신청서류가 자격 신청 요건에 적합한지를 검토하여야 한다.
- ③ 제2항에 따른 서류검토 결과 적합한 자는 인터넷진흥원이 시행하는 인증심사원 양성과정을 수료하여야 한다.

제14조(인증심사원 자격 발급 및 관리) ① 인터넷진흥원은 인증심사원 양성과정을 수료한 자에게 별지 제8호서식의 정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서를 발급하여야 한다.

- ② 인터넷진흥원은 인증심사원의 자격 증명서 발급, 심사원등급, 인증심사 업무경력 등을 관리하여야 한다.

제15조(인증심사원 자격 유지 및 갱신) ① 인증심사원의 자격 유효기간은 자격을 부여 받은 날부터 3년으로 한다.

- ② 인증심사원은 자격유지를 위해 자격 유효기간 만료 전까지 인터넷진흥원이 인정하는 보수교육을 수료하여야 한다.
- ③ 인터넷진흥원은 자격 유효기간 동안 1회 이상의 인증심사를 참여한 인증심사원에 대하여 제2항의 보수교육 시간 중 일부를 이수한 것으로 인정할 수 있다.
- ④ 인터넷진흥원은 인증정보를 제공하는 홈페이지에 제2항의 보수교육 운영에 관한 세부내용을 공지하여야 한다.
- ⑤ 인터넷진흥원은 제2항의 요건을 충족한 인증심사원에 한하여 별지 제8호서식의 정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서를 갱신하여 발급하고 자격 유효기간을 3년간 연장한다.
- ⑥ 제5항에도 불구하고 인터넷진흥원은 다음 각 호의 어느 하나에 해당하면 인증심사원 자격의 유효기간을 연장할 수 있다.
 1. 제29조제2항에 따른 인증위원회 위원으로 인정된 자
 2. 「재난 및 안전관리 기본법」 제3조에 따른 재난의 발생 등 협의회가 인정하는 불가피한 경우

제16조(인증심사원 자격 취소) ① 인터넷진흥원은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우 인증심사원의 자격을 취소할 수 있다.

1. 거짓이나 부정한 방법으로 인증심사원 자격을 부여 받은 경우
 2. 제15조제2항에 따른 자격 유지 기준을 충족하지 못한 경우
 3. 인증심사원으로서 객관적이고 공정한 인증심사를 수행하지 않은 경우
 4. 인증심사 과정에서 취득한 정보 또는 서류를 관련 법령의 근거나 인증신청인의 동의 없이 누설 또는 유출하거나 업무목적 외에 이를 사용한 경우
 5. 인증신청인으로부터 금전, 금품, 향응, 이익 등을 부당하게 수수하거나 요구한 경우
- ② 인터넷진흥원의 장은 제1항에 따른 자격 취소의 적합여부를 심의·의결하기 위하여 자격심의위원회를 개최하여야 하며, 자격심의위원회는 제29조의 인증위원회 위원 3인 이상을 포함하여 구성한다.

- ③ 제1항에 따른 자격 취소에 대하여 인증심사원은 30일 이내에 이의신청을 할 수 있다. 이 경우 인터넷진흥원은 해당 인증심사원의 자격을 제2항의 절차에 따라 재심의하여 처리결과를 통지하여야 한다.

제5장 인증심사의 신청 및 수수료 납부

제17조(신청인의 사전 준비사항) ① 정보보호 및 개인정보보호 관리체계 인증을 취득하고자 하는 자(이하 "신청인"이라 한다)는 인증을 신청하기 전에 인증기준에 따른 정보보호 및 개인정보보호 관리체계 또는 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다. 다만, 제18조의2제1항제1호에 따른 예비인증의 경우에는 그러지 아니한다.

- ② 신청인은 인증심사를 위하여 다음 각 호의 사항을 인증심사 실시 전에 준비하여야 한다.
1. 인증심사를 위한 문서 및 증거자료
 2. 인증심사 수행에 필요한 장소·시설·장비·기자재 등의 확보
 3. 그 밖에 인증심사를 원활하게 수행하기 위하여 심사수행기관이 요구하는 사항

제18조(인증 신청 등) ① 신청인은 다음 각 호의 인증을 선택하여 신청할 수 있다.

1. 정보보호 및 개인정보보호 관리체계 인증
 2. 정보보호 관리체계 인증
- ② 신청인은 제1항의 인증 선택에 따른 별지 제9호서식의 정보보호 및 개인정보보호 관리체계 인증 신청서를 심사수행기관에 제출하여야 한다.
- ③ 신청인은 인증범위 및 일정 등을 심사수행기관과 사전 협의하여 신청하여야 한다.
- ④ 심사수행기관은 제17조에 따른 신청인의 인증심사 사전준비사항을 확인할 수 있으며, 신청인의 준비가 미흡한 경우에는 신청인에 이를 보완할 것을 요구할 수 있다.
- ⑤ 심사수행기관은 인증범위의 변경이 필요한 경우에 이를 신청인과 협의하여 변경할 수 있다.

제18조의2(가상자산사업자에 대한 인증) ① 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제7조제1항에 따라 신고를 하려는 가상자산사업자(가상자산사업을 운영하려는 자를 포함한다. 이하 이 조에서 같다)에 대한 제18조제1항제2호의 인증은 다음 각 호로 구분한다.

1. 예비인증: 가상자산사업자 중 본인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 2개월 이상 운영하지 못한 자가 실제 서비스 운영 전 임시적으로 관련 시스템을 구축·운영(이하 "시험운영"이라 한다)하여 받는 인증으로서 제2호에 따른 본인증을 받기 위한 조건부 인증
2. 본인증: 예비인증을 취득한 자로서 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 2개월 이상 운영한 자를 대상으로 하는 인증

- ② 인터넷진흥원 또는 인증기관은 가상자산사업자에게 제1항제1호에 따른 예비인증을 부여할 때에는 다음 각 호의 조건을 붙여야 한다.
1. 예비인증 취득한 날부터 3개월 이내에 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제7조에 따른 신고를 할 것
 2. 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제7조에 따라 신고가 수리된 날부터 6개월 이내에 제1항제2호에 따른 본인증을 취득할 것(다만, 본인증 절차가 완료 될 때까지는 예비인증의 효력은 유효한 것으로 본다).
- ③ 예비인증 신청자가 제17조제2항에 따른 사전 준비사항을 준비하는 경우 정보보호 관리체계 구축 후에 시험운영 결과를 토대로 그 준비사항을 제출하여야 한다.
- ④ 인터넷진흥원 또는 인증기관은 제1항제1호에 따른 예비인증을 부여할 때에는 제32조에 따른 인증서 및 제34조에 따른 인증의 표시에 그 사실을 표기 및 표시하여야 한다.
- ⑤ 제1항제1호에 따른 예비인증은 제23조제1항제2호의 인증기준을 적용하되 시험운영을 통해 정보보호 관리체계가 적합한지에 대해 확인할 수 있는 범위로 한정한다.

제19조(정보보호 관리체계 인증 의무대상자) ① 정보보호 관리체계 인증

의무대상자(이하 "의무대상자"라 한다)란 정보통신망법 제47조제2항, 같은 법 시행령 제49조에 해당하는 자를 말한다.

- ② 제1항에 해당하는 자 중 집적정보통신시설 사업자가 마련한 시설의 일부를 임대하여 집적정보통신시설 사업을 하는 자에 대하여는 정보통신망법 시행령 제49조제2항의 기준을 준용한다.
- ③ 의무대상자는 제18조제1항제2호의 정보보호 관리체계 인증을 받아야 한다. 이때 의무대상자가 같은 항 제1호의 인증을 받은 경우에도 인증의무를 이행한 것으로 본다.
- ④ 의무대상자에 해당하는 자는 다음 해 8월 31일까지 인증을 받아야 한다.
- ⑤ 「재난 및 안전관리 기본법」제3조에 따른 재난의 발생 등 협의회가 인정하는 불가피한 사유로 제4항의 기한까지 인증을 받지 못한 경우 의무대상자의 인증 의무 이행 기한을 협의회가 정하는 바에 따라 연장할 수 있다.

제20조(인증심사의 일부 생략 신청 등) ① 제18조제1항 각 호의 어느 하나에

해당하는 인증을 신청한 자가 다음 각 호의 어느 하나에 해당하는 인증을 받거나 정보보호 조치를 취한 경우 별표 5의 인증심사 일부 생략의 범위 내에서 인증심사의 일부를 생략할 수 있다.

1. 국제인정협력기구에 가입된 인정기관이 인정한 인증기관으로부터 받은 ISO/IEC 27001 인증
 2. 「정보통신기반 보호법」제9조에 따른 주요정보통신기반시설의 취약점 분석·평가
- ② 제1항에 따라 인증심사의 일부를 생략하려는 경우에는 다음 각 호의 요건을 모두

충족하여야 한다.

1. 제18조제1항 각 호의 어느 하나에 해당하는 인증의 범위에 해당 국제표준 정보보호 인증 또는 정보보호 조치의 범위가 포함될 것
2. 제18조제1항 각 호의 어느 하나에 해당하는 인증 신청 및 심사 시에 해당 국제표준 정보보호 인증이나 정보보호 조치가 유효하게 유지되고 있을 것
- ③ 제1항에 따른 인증심사 일부 생략을 신청하고자 하는 자는 별지 제10호서식의 인증심사 일부 생략 신청서를 심사수행기관에 제출하여야 한다.
- ④ 심사수행기관은 별표 5의 인증심사 일부 생략의 범위를 생략하여 심사하고 인터넷진흥원 또는 인증기관이 인증을 부여할 때에는 그 사실을 인증서에 표기하여야 한다.
- ⑤ 정보통신망법 시행규칙 제3조제3항에서 "과학기술정보통신부장관이 고시하는 결과"란 「교육부 정보보안 기본지침」 제94조제1항에 따른 정보보안 수준에 대한 해당 연도의 평가결과가 만점의 100분의 80 이상인 것을 말한다.
- ⑥ 심사수행기관은 신청인의 인증범위 내에서 업무를 위탁받아 처리하는 자가 제18조제1항 각 호의 인증을 받은 범위의 현장심사를 생략할 수 있다.

제21조(수수료의 산정) ① 인증 수수료는 별표 6의 인증 수수료 산정 및 심사원 보수 기준을 적용하여 산정한다.

- ② 심사수행기관은 제1항에 따라 산정된 인증 수수료를 공지하여야 한다.
- ③ 심사수행기관은 신청인이 다음 각 호의 어느 하나에 해당하는 경우 수수료를 감면 또는 조정할 수 있다.
 1. 「중소기업기본법」제2조제2항에 따른 소기업
 2. 제20조에 따른 인증심사 일부 생략 신청을 하는 경우
 3. 「정보보호산업의 진흥에 관한 법률」제13조에 따라 정보보호 현황을 공시한 자
 4. 정보통신망법 제47조의7제1항 각 호의 어느 하나에 해당하는 자로서 제23조제3항 및 제4항에 따른 인증심사 기준을 적용받는 경우
 5. 그 밖에 신청인과 협의하여 수수료 조정이 필요하다고 판단되는 경우

제22조(수수료의 납부) 신청인은 최초심사, 사후심사 및 갱신심사 신청 시 인증 수수료를 청구 받은 날부터 인증심사 시작일 이전까지 심사수행기관에 납부하여야 하며, 수수료를 납부하지 않은 경우 심사수행기관은 인증심사를 실시하지 아니할 수 있다.

제6장 인증심사의 기준과 방법

제23조(인증심사 기준) ① 다음 각 호의 인증의 구분에 따라 별표 7의 인증기준을 적용한다.

1. 정보보호 및 개인정보보호 관리체계 인증 : 별표 7 가목부터 다목
2. 정보보호 관리체계 인증 : 별표 7 가목 및 나목
- ② 과학기술정보통신부장관과 보호위원회는 신청인과 협의를 통해 별표 7의 인증기준

내에서 인증범위, 업무특성, 기업규모 등을 고려하여 구체적인 확인사항을 관보 또는 인터넷 홈페이지에 공고할 수 있다.

- ③ 제1항에도 불구하고 정보통신망법 제47조의7제1항제1호 및 같은 법 시행령 제49조의2제1항제1호에 해당하는 자에 대해서는 다음 각 호의 인증의 구분에 따라 인증기준을 적용한다.

1. 정보보호 및 개인정보보호 관리체계 인증 : 별표 7의2 가목부터 다목
2. 정보보호 관리체계 인증 : 별표 7의2 가목(1.1.2. 항목 제외) 및 나목

- ④ 정보통신망법 시행령 제49조의2제1항제2호에 해당하는 자에 대해서는 다음 각 호의 인증의 구분에 따라 인증기준을 적용한다.

1. 정보보호 및 개인정보보호 관리체계 인증 : 별표 7의3 가목부터 다목
2. 정보보호 관리체계 인증 : 별표 7의3 가목 및 나목

제24조(인증심사팀 구성) ① 심사수행기관은 인증심사 일정이 확정된 때에는 인터넷진흥원에 심사원 모집을 요청하여 인증심사팀을 구성하여야 한다.

- ② 인증심사팀 구성 시 신청인의 인증범위, 사업유형, 기술의 다양성 등을 고려하여 심사팀원을 구성하여야 한다.

- ③ 인증심사원은 신청인의 정보보호 또는 개인정보보호 컨설팅에 참여하였거나 소속직원 등 신청인과 이해관계를 가지는 경우 사전에 소명하여야 하며, 심사수행기관은 인증심사원을 인증심사팀의 구성원에서 배제하여야 한다.

제25조(인증심사 방법 및 보완조치) ① 인증심사는 신청인을 방문하여 서면심사와 현장심사를 병행한다.

- ② 서면심사는 제23조에 따른 인증심사 기준에 적합한지에 대하여 정보보호 및 개인정보보호 관리체계 구축·운영 관련 정책, 지침, 절차 및 이행의 증거자료 검토, 정보보호대책 및 개인정보 처리단계별 요구사항 적용 여부 확인 등의 방법으로 관리적 요소를 심사한다.

- ③ 현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사한다.

- ④ 심사수행기관은 인증심사에서 발견된 결함에 대해 심사종료 다음날부터 최대 100일(재조치 요구 60일 포함) 이내에 보완조치를 완료하도록 신청인에게 요청할 수 있다.

- ⑤ 심사수행기관은 인증위원회 심의결과에 따라 인증위원회 종료 다음날부터 30일 이내에 신청인에게 추가 보완조치를 요구할 수 있다.

- ⑥ 제1항에도 불구하고 「재난 및 안전관리 기본법」 제3조에 따른 재난의 발생 등 협의회가 인정하는 불가피한 경우 원격심사를 병행할 수 있다.

제26조(심사중단) ① 심사수행기관은 다음 각 호의 사유가 발생한 경우에는 인증심사를 중단할 수 있다.

1. 신청인이 고의로 인증심사의 실시를 지연 또는 방해하거나 신청인의 귀책사유로 인하여 인증심사팀장이 인증심사를 계속 진행하기가 곤란하다고 판단하는 경우
 2. 신청인이 제출한 관련 자료 등을 검토한 결과 인증심사를 받을 준비가 되었다고 볼 수 없는 경우
 3. 인증심사 후 제25조제4항에 따른 보완조치를 최대 100일(재조치 요구 60일 포함) 이내에 완료하지 않은 경우
 4. 「재난 및 안전관리 기본법」제3조에 따른 재난의 발생 또는 경영환경 변화 등으로 인하여 인증심사 진행이 불가능하다고 판단되는 경우
- ② 심사수행기관은 제1항에 따라 인증심사를 중단하는 때에는 그 사유를 신청인에게 서면으로 통보하여야 한다.
- ③ 심사수행기관은 제1항의 인증심사 중단 사유가 해소되거나 제36조에 따른 이의신청 처리결과에 따라 인증심사를 재개하거나 종결할 수 있다.

제27조(사후관리) ① 인증을 취득한 자는 인증서 유효기간 중 연 1회 이상 심사수행기관에 사후심사를 신청하여야 한다.

② 사후심사는 제5장 및 제6장을 준용하여 진행한다.

③ 인증 취득한 범위와 관련하여 침해사고 또는 개인정보 유출사고가 발생한 경우 인터넷진흥원은 필요에 따라 인증관련 항목의 보안향상을 위한 필요한 지원 등을 할 수 있다.

제28조(인증의 갱신) ① 인증을 취득한 자는 인증서 유효기간 만료 3개월 전에 갱신심사를 신청하여야 한다.

② 갱신심사는 제5장 및 제6장을 준용하여 진행한다.

③ 인증을 취득한 자가 제1항에 따른 인증의 갱신을 신청하지 않고 인증의 유효기간이 경과한 때에는 인증의 효력은 상실된다.

제7장 인증위원회 구성과 운영

제29조(인증위원회의 구성) ① 인터넷진흥원 또는 인증기관의 장은 다음 각 호의 사항을 심의·의결하기 위하여 인증위원회를 설치·운영하여야 한다.

1. 최초심사 또는 갱신심사 결과가 인증기준에 적합한지 여부
2. 제35조제1항에 따른 인증의 취소에 관한 사항
3. 제36조에 따른 이의신청에 관한 사항
4. 그 밖에 정보보호 및 개인정보보호 관리체계 인증과 관련하여 위원장이 필요하다고 인정하는 사항

② 인증위원회는 35인 이내의 위원으로 구성하되, 위원은 정보보호 및 개인정보보호 관련 분야에 학식과 경험이 있는 자 중에서 인터넷진흥원 또는 인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

③ 위원장은 인증위원회의 업무를 통할하며 위원회를 대표한다.

④ 인터넷진흥원 또는 인증기관의 장은 위원이 법령 또는 이 규정을 위반한 때에는

해당 위원을 해촉할 수 있다.

- 제30조(인증위원회의 운영)** ① 인증위원회의 회의는 인터넷진흥원 또는 인증기관의 요구로 개최하되, 회의마다 위원장과 인증위원의 전문분야를 고려하여 6인 이상의 인증위원으로 구성한다. 단, 위원장이 부득이한 사유로 직무를 수행할 수 없는 경우 위원장이 사전에 지명한 위원이 위원장의 직무를 대행한다.
- ② 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의안을 검토하여 위원회 개최 5일 전까지 인증위원회에 제출한다. 다만, 긴급한 경우나 부득이한 사유가 있는 경우에는 그러하지 아니하다.
- ③ 인증위원회 위원장은 제29조제1항의 각 호의 사항에 대한 심의·의결 결과를 인터넷진흥원 또는 인증기관의 장에게 제출한다.
- ④ 인증위원회는 심의를 위하여 필요하다고 인정되는 경우에는 인증심사에 참여한 인증심사원 또는 관련 전문가로부터 그에 관한 의견을 들을 수 있다.
- ⑤ 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의·의결 결과를 제출받은 때에는 신청인에게 결과를 통보하여야 한다.

- 제31조(제척·기피·회피)** ① 인증위원회 위원은 신청인과 다음 각 호의 사항 중 어느 하나에 해당하는 때에는 심의·의결에 관여할 수 없다.
1. 위원 본인과 직접적인 이해관계가 있는 사항
 2. 위원 본인과 친족관계에 있거나 있었던 자와 관련된 사항
 3. 위원이 되기 전에 감사·수사 또는 조사에 관여한 사항
- ② 위원에게 심의·의결의 공정성을 기대하기 어려운 사정이 있는 경우 신청인은 기피신청을 할 수 있고, 위원회는 의결로 이를 결정한다.
- ③ 위원은 제척사유 또는 기피사유에 해당하는 경우에는 자기 스스로 심의·의결을 회피할 수 있다.

제8장 인증서의 발급·관리 및 홍보

- 제32조(인증서의 발급 등)** ① 인터넷진흥원 또는 인증기관의 장은 인증위원회에서 인증적합으로 판정된 경우 그 결과에 따라 신청인에게 별지 제11호서식의 정보보호 및 개인정보보호 관리체계 인증서 또는 별지 제12호서식의 정보보호 관리체계 인증서를 발급하여야 한다.
- ② 인증서 발급 시 인증번호는 별표 8의 인증의 표시를 따른다.
- ③ 제1항에 따른 인증서의 유효기간은 3년으로 한다.

- 제33조(인증서 관리 및 재발급)** ① 인터넷진흥원 또는 인증기관은 발급된 인증서의 인증번호, 발급일, 유효기간 등 인증서를 관리하여야 한다.
- ② 인증을 취득한 자는 인증서의 분실 등으로 인해 재발급을 받고자 할 경우 별지 제13호서식의 인증서 재발급 신청서를 인터넷진흥원 또는 인증기관에 제출하여야

한다.

- ③ 인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제14호서식의 인증서 변경 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

제34조(인증의 표시 및 홍보) ① 「개인정보 보호법 시행령」제34조의7 및 정보통신망법 시행령 제52조에 따른 인증의 표시는 별표 8과 같다.

- ② 제1항에 따른 인증의 표시를 사용하는 경우에는 인증범위 및 유효기간을 함께 표시하여야 한다.
- ③ 인터넷진흥원은 인증정보를 제공하는 홈페이지를 통해 인증현황을 공개하여야 한다.

제35조(인증의 취소) ① 인터넷진흥원 또는 인증기관은 다음 각 호의 사유를 발견한 때는 인증위원회 심의·의결을 거쳐 인증을 취소할 수 있다.

1. 거짓 혹은 부정한 방법으로 인증을 취득한 경우
 2. 제23조에 따른 인증기준에 미달하게 된 경우
 3. 인증을 취득한 자가 제27조제1항에 따른 사후심사 또는 제28조제1항에 따른 갱신심사를 받지 않았거나 제25조제4항에 따른 보완조치를 하지 않은 경우
 4. 인증 받은 내용을 홍보하면서 제34조제2항에 따른 인증범위 및 유효기간을 허위로 표기하거나 누락한 경우
 5. 인증을 취득한 자가 제27조 및 제28조에 따른 사후관리를 거부 또는 방해하는 경우
 6. 개인정보보호 관련 법령을 위반하고 그 위반사유가 중대한 경우
- ② 인터넷진흥원 또는 인증기관은 제1항에 따라 인증을 취소한 경우에 그 결과를 통지하고, 제32조에 따라 발급한 인증서를 회수한다.

제36조(이의신청) ① 신청인 또는 인증을 취득한 자가 인증심사 결과 또는 인증 취소처분에 관하여 이의가 있는 때에는 그 결과를 통보받은 날부터 15일 이내에 별지 제15호서식의 이의신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

- ② 인터넷진흥원 또는 인증기관은 제1항에 따른 이의신청이 이유가 있다고 인정되는 경우에는 인증위원회에 재심의를 요청할 수 있다.
- ③ 인터넷진흥원 또는 인증기관은 이의신청에 대한 처리결과를 신청인 또는 인증을 취득한 자에 통지하여야 한다.

제9장 인증업무 일반 등

제37조(비밀유지 등) ① 인터넷진흥원, 인증기관, 심사기관, 인증위원회 위원, 인증심사원 등 인증심사 업무에 종사하는 자 또는 종사하였던 자는 정당한 권한 없이 또는 허용된 권한을 초과하여 업무상 지득한 비밀에 관한 정보를 누설하거나 이를 업무 목적 이외에 사용하여서는 아니 된다.

- ② 인터넷진흥원, 인증기관, 심사기관, 인증위원회 위원, 인증심사원 등 인증심사업무에 종사하는 자 또는 종사하였던 자는 인증에 관련하여 일체의 금전, 금품, 이익 등을 부당하게 수수하여서는 아니 된다.

제38조(업무 지침 등) 인터넷진흥원, 인증기관 또는 심사기관은 인증 또는 심사업무 수행을 위해 필요한 경우 법령의 범위 내에서 인증 또는 심사업무에 관한 지침을 마련하여 시행할 수 있다.

제39조(재검토 기한) 과학기술정보통신부장관과 보호위원회는 「행정규제기본법」 및 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2019년 1월 1일을 기준으로 매3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2024-8호, 2024.07.24.>

이 고시는 발령한 날부터 시행한다.

[별표 1]

업무수행 요건·능력 심사 제출서류(제6조 관련)

구 분	제출서류
인증심사원 고용	1. 인증심사업무를 전담하는 심사원의 보유현황 2. 선임심사원 보유에 대한 증빙 서류
인증·심사의 공정성·독립성 확보	1. 정보보호 및 개인정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하지 않음을 확인할 수 있는 기업설명자료, 직제규정, 사업수행계획서 등 2. 인증신청인으로부터 독립성 확보 방안
재정 능력	1. 자본금 내역(공인회계사 또는 회계담당자가 서명 날인한 서류) 2. 신용평가서 3. 운영자금 보유 내역 및 피해보상 대책
시설	사무공간·인증심사 서류 보관 장소 및 보안설비·시설 증빙서류
인증 및 심사실적 (재지정만 해당)	인증 및 심사실적에 대한 증빙서류
업무수행 요건·능력 심사를 위하여 필요한 서류	[별표2] 업무수행 요건·능력 심사를 위한 세부기준 충족을 증빙할 수 있는 서류 1. 조직 및 전문성 관련 증빙서류 2. 신뢰도 관련 증빙서류 3. 업무수행 관련 증빙서류 4. 시설 및 보안 관련 증빙서류

업무수행 요건·능력 심사에 관한 세부기준 (제7조, 제9조 관련)

가. 업무수행 요건 심사 기준(필수)

평가 항목	세부평가 항목	세부 평가 기준 (인증기관 및 심사기관 모두 해당)
인력	인증심사원 고용	<ul style="list-style-type: none"> · 인증심사원 5명 이상 상시 고용 · 선임심사원 1명 이상 확보
공정성	객관성·공정성·독립성 확보	<ul style="list-style-type: none"> · 인증업무 또는 심사 업무의 독립성, 객관성, 공정성, 신뢰성을 확보할 수 있어야 하며 정보보호 및 개인정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하지 않아야 함

나. 업무수행 능력 심사 기준

평가 항목	세부평가 항목	평가 지표	인증 기관 배점	심사 기관 배점	세부 평가 기준
1. 조직 및 전문성	전담조직	등급	5	5	<ul style="list-style-type: none"> ○ 인증/심사 업무를 수행하는 전담조직 유무 · 전담조직 보유 : 배점의 100% · 전담조직 없음 : 0점
	전담인력	비율	5	5	<ul style="list-style-type: none"> ○ 심사 업무를 수행하는 전담 심사원의 수 · 10명 이상 : 배점의 100% · 10명 미만 : 배점의 $\chi\%$ ※ $\chi = (\text{전담 심사원 수} / 10\text{명}) \times 100$
	전문성	비율	5	5	<ul style="list-style-type: none"> ○ 최근 3년간 전담 심사원의 인증심사 참여일 수의 합 · 200일 이상 : 배점의 100% · 200일 미만 : 배점의 $\chi\%$ ※ $\chi = (\text{총 참여일수} / 200\text{일}) \times 100$
		비율	5	5	<ul style="list-style-type: none"> ○ 업무 전문성 강화를 위한 최근 3년간 교육 시간 · 전담 심사원 모두 100시간 이상의 교육을 받은 경우 : 배점의 100% · 전담 심사원 모두 100시간 이상의 교육을 받지 않은 경우 : 배점의 $\chi\%$ ※ $\chi = (100\text{시간 이상 교육을 받은 전담 심사원의 수} / \text{총 전담 심사원의 수}) \times 100$
2. 신뢰도	재정 능력	등급	5	5	<ul style="list-style-type: none"> ○ 신용평가등급 · AAA ~ A- : 배점의 100% · BBB+ ~ BBB- : 배점의 70% · BB+ ~ BB- : 배점의 50% · B+ ~ B- : 배점의 30% · CCC+ 이하 : 배점의 10%
		등급	3	3	<ul style="list-style-type: none"> ○ 자본금 보유 · 5억 이상 : 배점의 100% · 5억 미만 : 배점의 0%

	업무 지원 및 피해보상 대책	비계량	2	2	<ul style="list-style-type: none"> ○ 운영자금 법인통장 보유 및 유지 수준 ○ 지정취소, 부도·해산, 업무상 과실 등에 따른 피해 보상 관련 보험 가입 또는 이에 상응하는 대책 마련
3. 업무 수행	업무지침	비계량	4	4	<ul style="list-style-type: none"> ○ 인증/심사 업무 수행 지침 보유 ○ 업무지침의 타당성 및 준수여부 <ul style="list-style-type: none"> - 인증/심사 업무를 수행하는 직원의 의무와 책임 - 품질관리, 운영관리, 인증/심사업무, 문서관리, 시설관리, 보안관리 절차 및 방법
	품질관리	비계량	16	18	<ul style="list-style-type: none"> ○ 인증/심사의 품질 보증 및 관리를 위한 정보공유, 교육, 세미나 등의 활동 ○ 피심사기관으로부터 공정성, 객관성, 신뢰성, 독립성 확보방안 및 이행 ○ 인증/심사업무 참여자 및 업무 담당자의 공정성, 객관성, 신뢰성, 독립성 확보방안 및 이행 ○ 관계 법령 및 내부절차 준수, 청렴 등에 대한 독립적인 내부감사 실시 및 결과에 대한 조치 ○ 인증/심사 결과에 대한 처리절차 준수 등에 대한 책임자 검토 ○ 인증/심사 업무 관련 불만 및 이의제기에 대한 대응 절차마련 및 이행
	운영관리	비계량	8	12	<ul style="list-style-type: none"> ○ 업무 수행 방법 및 절차 등의 투명성 및 타당성 ○ 신청 접수, 수수료 산정방법 및 부과 ○ 심사 이후 자문료, 출장비 등의 지급의 적절한 이행 ○ 인증취득 희망기업에 특정 기관으로 부적절한 방법으로 심사를 종용하는 등 부당행위 방지대책
	인증관리	비계량	12	-	<ul style="list-style-type: none"> ○ 인증의 독립성·객관성·공정성 확보를 위한 인증위원 구성 및 인증위원회 운영 ○ 인증위원회 개최 정족수, 상정안건의 검토, 의결 등의 운영절차 마련 및 이행 ○ 인증서 관리 절차 마련 및 이행 ○ (재지정만 해당)인증실적 및 인증 내역
	심사관리	비계량	12	18	<ul style="list-style-type: none"> ○ 심사팀 구성 원칙마련 및 이행 ○ 심사원의 의무와 책임 준수, 보안관리 및 감독 방안 및 이행 ○ 심사 수행절차 준수 ○ 심사결과보고, 인증위원회 상정 등 사후 절차 준수 ○ 인증심사 수행 시 문서 및 정보의 유출 방지를 위한 시스템 도입 및 이행 ○ (재지정만 해당)심사 실적 및 인증심사원 참여 내역
	문서관리	비계량	10	10	<ul style="list-style-type: none"> ○ 업무의 기록 및 문서에 관한 관리절차 마련 및 준수 ○ 업무 담당자간 파일 송수신 및 문서 공유시 안전한 방식을 사용 ○ 업무 기록 및 문서에 권한이 없거나 불필요한 인원의 접근방지 대책 및 이행
4. 시설 및 보안	시설 및 보안	비계량	4	4	<ul style="list-style-type: none"> ○ 독립된 사무공간 및 회의공간 ○ 인증 및 심사 기록물의 안전한 보관을 위한 장소 ○ 사무공간 출입의 신원확인 및 출입통제 보안설비 운영 ○ 문서 분실, 도난 등 예방을 위한 보안시설 마련

	시스템 및 보안	비계량	4	4	<ul style="list-style-type: none"> ○ 인증 및 심사 관리를 위한 시스템 운영 및 사무관련 시스템 보유 ○ 인증 및 심사정보의 침해사고, 유출사고를 대비한 보안시스템 운영
5 감점	자격 취소 사실	계량	감점	감점	<ul style="list-style-type: none"> ○ 지정공고일 기준으로 10년 이내에 과학기술정보통신부, 개인정보 보호위원회가 부여한 정보보호 또는 개인정보보호 관련 업무 수행자격이 취소된 사실이 있는 경우 ※취소 1회 당 : 감점 10점
합계			100	100	

<비 고>

1. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 비계량 각 세부평가 점수 부여기준은 배점에 평가등급(계수)를 곱하여 계산한다.

평가요소별 비계량 평가	평가등급(계수)
우수	1.0
보통	0.6
미흡	0.2
미 제출	점수없음(0)

[별표 3]

인증심사원 등급별 자격 요건(제12조 관련)

등급	자격 기준
심사원보	o 인증심사원 자격 신청 요건을 만족하는 자로서 인터넷진흥원이 수행하는 인증심사원 양성과정 통과하여 자격을 취득한 자
심사원	o 심사원보 자격 취득자로서 인증심사에 4회 이상 참여하고 심사일수의 합이 20일 이상인 자
선임심사원	o 심사원 자격 취득자로서 정보보호 및 개인정보보호 관리체계 인증심사를 3회 이상 참여하고 심사일수의 합이 15일 이상인 자

※ 인터넷진흥원은 인증심사원의 인증심사 능력에 따라 매년 책임심사원을 지정할 수 있다.

인증심사원 자격 신청 요건(제13조 관련)

4년제 대학졸업 이상 또는 이와 동등학력을 취득한 자로서 정보보호 및 개인정보보호 경력을 각 1년 이상 필수로 보유하고 정보보호, 개인정보보호 또는 정보기술 경력을 합하여 6년 이상을 보유

가. "동등학력"이란 고등학교 졸업자는 4년 이상, 2년제 대학 졸업자는 2년 이상 업무경력을 말한다.

나. "정보기술 경력"이란 공공기관, 기업체, 교육 및 연구기관 등에서 정보통신서비스, 정보통신기기, 소프트웨어 및 컴퓨터 관련 서비스 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 경력 또는 관련 법률자문 경력을 말한다.

다. "정보보호 경력"이란 공공기관, 기업체, 교육 및 연구기관 등에서 정보보호를 위한 공통기반기술, 시스템·네트워크 보호, 응용서비스 보호, 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 경력 또는 관련 법률자문 경력을 말한다.

라. "개인정보보호 경력"이란 공공기관, 기업체, 교육 및 연구기관 등에서 개인정보보호 업무 수행, 개인정보보호 컨설팅, 개인정보보호 관련 법률자문 등의 업무를 수행한 경력을 말한다.

마. 변호사법에 따른 변호사의 경우에는 6년의 개인정보보호 유관경력을 보유한 것으로 본다.

바. 동일기간에 두 가지 이상 업무가 중복되는 경우에 하나의 경력만 인정하며, 모든 해당 경력은 신청일 기준 최근 10년 이내의 경력에 한해 인정한다.

사. 아래의 학위 또는 자격을 취득한 경우 정보보호 또는 개인정보보호 경력을 대체할 수 있으며 중복으로 인정하지 않는다.

<경력인정 요건-중복 인정 불가>

구 분	경력 인정 요건	인정기간
정보보호 경력	o “정보보호” 관련 박사 학위 취득자	2년
	o “정보보호” 관련 석사 학위 취득자	1년
	o 정보보안기사	
	o 정보시스템감사통제협회(ISACA)의 정보시스템감사사(CISA)	
	o 국제정보시스템보안자격협회(ISC ²)의 정보시스템보호전문가(CISSP)	
개인정보보호 경력	o “개인정보보호” 관련 박사 학위 취득자	2년
	o “개인정보보호” 관련 석사 학위 취득자	1년
	o 개인정보 영향평가에 관한 고시 제6조에 따른 개인정보 영향평가 전문인력	
	o 개인정보관리사(CPPG)	
정보기술 경력	o “정보기술” 관련 박사 학위 취득자	2년
	o 정보관리기술사, 컴퓨터시스템응용기술사	
	o 정보시스템감리사	
	o “정보기술” 관련 석사 학위 취득자	1년
	o 정보시스템감리원	
	o 정보처리기사, 전자계산기조직응용기사	

[별표 5]

인증심사 일부 생략의 범위(제20조 관련)

분야		항목	
2.1.	정책, 조직, 자산 관리	2.1.1	정책의 유지관리
		2.1.2	조직의 유지관리
		2.1.3	정보자산 관리
2.2.	인적 보안	2.2.1	주요 직무자 지정 및 관리
		2.2.2	직무 분리
		2.2.3	보안 서약
		2.2.4	인식제고 및 교육훈련
		2.2.5	퇴직 및 직무변경 관리
		2.2.6	보안 위반 시 조치
2.3.	외부자 보안	2.3.1	외부자 현황 관리
		2.3.2	외부자 계약 시 보안
		2.3.3	외부자 보안 이행 관리
		2.3.4	외부자 계약 변경 및 만료 시 보안
2.4.	물리 보안	2.4.1	보호구역 지정
		2.4.2	출입통제
		2.4.3	정보시스템 보호
		2.4.4	보호설비 운영
		2.4.5	보호구역 내 작업
		2.4.6	반출입 기기 통제
		2.4.7	업무 환경 보안
2.12.	재해복구	2.12.1	재해, 재난 대비 안전조치
		2.12.2	재해 복구 시험 및 개선

[별표 6]

인증 수수료 산정 및 심사원 보수 기준(제21조 관련)

1. 인증수수료 산정 기준

$\text{인증 수수료} = \text{직접인건비} + \text{제경비} + \text{기술료} + \text{직접경비}$
--

가. 직접인건비는 인증심사에 투입되는 인증심사원에 대한 인건비로 산정한다.

나. 제경비는 최대 (직접인건비×120%) 로 산정한다.

다. 기술료는 최대 {(직접인건비+제경비)×40%} 로 산정한다.

라. 직접경비는 인증심사업무의 수행에 따라 발생하는 교통비, 숙박비 및 식대 등 인증심사업무에 소요되는 직접적인 경비를 산정한다. 단, 신청인은 심사 현장 상황에 따라 직접경비를 인증 수수료와 별도로 지급할 수 있다.

2. 인증심사원 보수 및 출장비 지급기준

가. 인증심사원에 대한 보수 및 경비는 인터넷진흥원이 정하여 공고한다.

나. 인증심사원이 국내·외에서 출장업무를 수행하는 경우 심사 수행기관의 업무 지침에 따른 정액여비로 별도 지급할 수 있다.

인증기준(제23조 관련)

가. 관리체계 수립 및 운영

분야		항목		상세 내용
1.1.	관리체계 기반 마련	1.1.1	경영진의 참여	최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.
		1.1.2	최고책임자의 지정	최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.
		1.1.3	조직 구성	최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호 담당자로 구성된 협의체를 구성하여 운영하여야 한다.
		1.1.4	범위 설정	조직의 핵심 서비스와 개인정보 처리 현황 등을 고려하여 관리체계 범위를 설정하고, 관련된 서비스를 비롯하여 개인정보 처리 업무와 조직, 자산, 물리적 위치 등을 문서화하여야 한다.
		1.1.5	정책 수립	정보보호와 개인정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호와 개인정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
		1.1.6	자원 할당	최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다.
1.2.	위험 관리	1.2.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
		1.2.2	현황 및 흐름분석	관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
		1.2.3	위험 평가	조직의 대내외 환경분석을 통해 유형별 위험정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.
		1.2.4	보호대책 선정	위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.
1.3.	관 리 체 계 운영	1.3.1	보호대책 구현	선정한 보호대책은 이행계획에 따라 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.
		1.3.2	보호대책 공유	보호대책의 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여 지속적으로 운영되도록 하여야 한다.
		1.3.3	운영현황 관리	조직이 수립한 관리체계에 따라 상시적 또는 주기적으로

				수행하여야 하는 운영활동 및 수행 내역은 식별 및 추적 이 가능하도록 기록하여 관리하고, 경영진은 주기적으로 운영활동의 효과성을 확인하여 관리하여야 한다.
1.4.	관 리 체 계 점검 및 개선	1.4.1	법적 요구사항 준수 검토	조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법 적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준 수 여부를 지속적으로 검토하여야 한다.
		1.4.2	관리체계 점검	관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성 하여 연 1회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다.
		1.4.3	관리체계 개선	법적 요구사항 준수검토 및 관리체계 점검을 통해 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하며, 경영진은 개선 결과의 정 확성과 효과성 여부를 확인하여야 한다.

나. 보호대책 요구사항

분야		항목		상세 내용
2.1.	정책, 조직, 자산 관리	2.1.1	정책의 유지관리	정보보호 및 개인정보보호 관련 정책과 시행문서는 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경변화 등에 따라 주기적으로 검토하여 필요한 경우 제·개정하고 그 내역을 이력관리하여야 한다.
		2.1.2	조직의 유지관리	조직의 각 구성원에게 정보보호와 개인정보보호 관련 역할 및 책임을 할당하고, 그 활동을 평가할 수 있는 체계와 조직 및 조직의 구성원 간 상호 의사소통할 수 있는 체계를 수립하여 운영하여야 한다.
		2.1.3	정보자산 관리	정보자산의 용도와 중요도에 따른 취급 절차 및 보호대책을 수립·이행하고, 자산별 책임소재를 명확히 정의하여 관리하여야 한다.
2.2.	인적 보안	2.2.1	주요 직무자 지정 및 관리	개인정보 및 중요정보의 취급이나 주요 시스템 접근 등 주요 직무의 기준과 관리방안을 수립하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다.
		2.2.2	직무 분리	권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 불가피하게 직무 분리가 어려운 경우 별도의 보완대책을 마련하여 이행하여야 한다.
		2.2.3	보안 서약	정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 한다.
		2.2.4	인식제고 및 교육훈련	임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고 직무별 전문성을 확보할 수 있도록 연간 인식제고 활동 및 교육훈련 계획을 수립·운영하고, 그 결과에 따른 효과성을 평가하여 다음 계획에 반영하여야 한다.
		2.2.5	퇴직 및 직무변경 관리	퇴직 및 직무변경 시 인사·정보보호·개인정보보호·IT 등 관련 부서별 이행하여야 할 자산반납, 계정 및 접근권한 회수·조정, 결과확인 등의 절차를 수립·관리하여야 한다.
		2.2.6	보안 위반 시 조치	임직원 및 관련 외부자가 법령, 규제 및 내부정책을 위반한 경우 이에 따른 조치 절차를 수립·이행하여야 한다.
2.3.	외부자 보안	2.3.1	외부자 현황 관리	업무의 일부(개인정보취급, 정보보호, 정보시스템 운영 또는 개발 등)를 외부에 위탁하거나 외부의 시설 또는 서비스(집적정보통신시설, 클라우드 서비스, 애플리케이션 서비스 등)를 이용하는 경우 그 현황을 식별하고 법적 요구사항 및 외부 조직·서비스로부터 발생하는 위험을 파악하여 적절한 보호대책을 마련하여야 한다.
		2.3.2	외부자 계약 시 보안	외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우 이에 따른 정보보호 및 개인정보보호 요구사항을 식별하고, 관련 내용을 계약서 또는 협정서 등에 명시하여야 한다.
		2.3.3	외부자 보안 이행 관리	계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항에 따라 외부자의 보호대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야 한다.
		2.3.4	외부자 계약 변경 및	외부자 계약만료, 업무종료, 담당자 변경 시에는 제공한

			만료 시 보안	정보자산 반납, 정보시스템 접근계정 삭제, 중요정보 파괴, 업무 수행 중 취득정보의 비밀유지 약속서 징구 등의 보호대책을 이행하여야 한다.
2.4.	물리 보안	2.4.1	보호구역 지정	물리적·환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역·제한구역·접근구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립·이행하여야 한다.
		2.4.2	출입통제	보호구역은 인가된 사람만이 출입하도록 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
		2.4.3	정보시스템 보호	정보시스템은 환경적 위협과 유해요소, 비인가 접근 가능성을 감소시킬 수 있도록 중요도와 특성을 고려하여 배치하고, 통신 및 전력 케이블이 손상을 입지 않도록 보호하여야 한다.
		2.4.4	보호설비 운영	보호구역에 위치한 정보시스템의 중요도 및 특성에 따라 온도·습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영절차를 수립·운영하여야 한다.
		2.4.5	보호구역 내 작업	보호구역 내에서의 비인가행위 및 권한 오·남용 등을 방지하기 위한 작업 절차를 수립·이행하고, 작업 기록을 주기적으로 검토하여야 한다.
		2.4.6	반출입 기기 통제	보호구역 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제절차를 수립·이행하고 주기적으로 검토하여야 한다.
		2.4.7	업무환경 보안	공용으로 사용하는 사무용 기기(문서고, 공용 PC, 복합기, 파일서버 등) 및 개인 업무환경(업무용 PC, 책상 등)을 통해 개인정보 및 중요정보가 비인가자에게 노출 또는 유출되지 않도록 클린데스크, 정기점검 등 업무환경 보호대책을 수립·이행하여야 한다.
2.5.	인증 및 권한관리	2.5.1	사용자 계정 관리	정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다.
		2.5.2	사용자 식별	사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립·이행하여야 한다.
		2.5.3	사용자 인증	정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여야 한다.
		2.5.4	비밀번호 관리	법적 요구사항, 외부 위협요인 등을 고려하여 정보시스템 사용자 및 고객, 회원 등 정보주체(이용자)가 사용하는 비밀번호 관리절차를 수립·이행하여야 한다.
		2.5.5	특수 계정 및 권한 관리	정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.
		2.5.6	접근권한 검토	정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다.
2.6.	접근통제	2.6.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중

				요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.
		2.6.2	정보시스템 접근	서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.
		2.6.3	응용프로그램 접근	사용자별 업무 및 접근 정보의 중요도 등에 따라 응용프로그램 접근권한을 제한하고, 불필요한 정보 또는 중요정보 노출을 최소화할 수 있도록 기준을 수립하여 적용하여야 한다.
		2.6.4	데이터베이스 접근	테이블 목록 등 데이터베이스 내에서 저장·관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따른 접근통제 정책을 수립·이행하여야 한다.
		2.6.5	무선 네트워크 접근	무선 네트워크를 사용하는 경우 사용자 인증, 송수신 데이터 암호화, AP 통제 등 무선 네트워크 보호대책을 적용하여야 한다. 또한 AD Hoc 접속, 비인가 AP 사용 등 비인가 무선 네트워크 접속으로부터 보호대책을 수립·이행하여야 한다.
		2.6.6	원격접근 통제	보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.
		2.6.7	인터넷 접속 통제	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P2P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.
2.7.	암호화 적용	2.7.1	암호정책 적용	개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.
		2.7.2	암호키 관리	암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행하고, 필요 시 복구방안을 마련하여야 한다.
2.8.	정보시스템 도입 및 개발 보안	2.8.1	보안 요구사항 정의	정보시스템의 도입·개발·변경 시 정보보호 및 개인정보 보호 관련 법적 요구사항, 최신 보안취약점, 안전한 코딩 방법 등 보안 요구사항을 정의하고 적용하여야 한다.
		2.8.2	보안 요구사항 검토 및 시험	사전 정의된 보안 요구사항에 따라 정보시스템이 도입 또는 구현되었는지를 검토하기 위하여 법적 요구사항 준수, 최신 보안취약점 점검, 안전한 코딩 구현, 개인정보 영향 평가 등의 검토 기준과 절차를 수립·이행하고, 발견된 문제점에 대한 개선조치를 수행하여야 한다.
		2.8.3	시험과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소시키기 위하여 원칙적으로 분리하여야 한다.
		2.8.4	시험 데이터 보안	시스템 시험 과정에서 운영데이터의 유출을 예방하기 위하여 시험 데이터의 생성과 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립·이행하여야 한다.
		2.8.5	소스 프로그램 관리	소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리

				하고, 운영환경에 보관하지 않는 것을 원칙으로 하여야 한다.
		2.8.6	운영환경 이관	신규 도입·개발 또는 변경된 시스템을 운영환경으로 이관할 때는 통제된 절차를 따라야 하고, 실행코드는 시험 및 사용자 인수 절차에 따라 실행되어야 한다.
2.9.	시스템 및 서비스 운영관리	2.9.1	변경관리	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립·이행하고, 변경 전 시스템의 성능 및 보안에 미치는 영향을 분석하여야 한다.
		2.9.2	성능 및 장애관리	정보시스템의 가용성 보장을 위하여 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링하여야 하며, 장애 발생 시 효과적으로 대응하기 위한 탐지·기록·분석·복구·보고 등의 절차를 수립·관리하여야 한다.
		2.9.3	백업 및 복구관리	정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상, 주기, 방법, 보관장소, 보관기간, 소산 등의 절차를 수립·이행하여야 한다. 아울러 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
		2.9.4	로그 및 접속기록 관리	서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리하여야 한다.
		2.9.5	로그 및 접속기록 점검	정보시스템의 정상적인 사용을 보장하고 사용자 오·남용(비인가접속, 과다조회 등)을 방지하기 위하여 접근 및 사용에 대한 로그 검토기준을 수립하여 주기적으로 점검하며, 문제 발생 시 사후조치를 적시에 수행하여야 한다.
		2.9.6	시간 동기화	로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그 분석을 위하여 관련 정보시스템의 시각을 표준시각으로 동기화하고 주기적으로 관리하여야 한다.
		2.9.7	정보자산의 재사용 및 폐기	정보자산의 재사용과 폐기 과정에서 개인정보 및 중요정보가 복구·재생되지 않도록 안전한 재사용 및 폐기 절차를 수립·이행하여야 한다.
2.10	시스템 및 서비스 보안관리	2.10.1	보안시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.
		2.10.2	클라우드 보안	클라우드 서비스 이용 시 서비스 유형(SaaS, PaaS, IaaS 등)에 따른 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호대책을 수립·이행하여야 한다.
		2.10.3	공개서버 보안	외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행하여야 한다.
		2.10.4	전자거래 및 핀테크 보안	전자거래 및 핀테크 서비스 제공 시 정보유출이나 데이터 조작·사기 등의 침해사고 예방을 위해 인증·암호화 등의 보호대책을 수립하고, 결제시스템 등 외부 시스템과 연계할 경우 안전성을 점검하여야 한다.
		2.10.5	정보전송 보안	타 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 조직 간 합의를 통해 관리 책임, 전송방법, 개인정보 및 중요정보 보호를 위한 기술적 보호조치 등을 협약하고 이행하여야 한다.
		2.10.6	업무용 단말기기 보안	PC, 모바일 기기 등 단말기기를 업무 목적으로 네트워크에 연결할 경우 기기 인증 및 승인, 접근 범위, 기기 보안설정 등의 접근통제 대책을 수립하고 주기적으로 점검하여야 한다.
		2.10.7	보조저장매체 관리	보조저장매체를 통하여 개인정보 또는 중요정보의 유출이

				발생하거나 악성코드가 감염되지 않도록 관리 절차를 수립·이행하고, 개인정보 또는 중요정보가 포함된 보조저장매체는 안전한 장소에 보관하여야 한다.
		2.10.8	패치관리	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인한 침해사고를 예방하기 위하여 최신 패치를 적용하여야 한다. 다만 서비스 영향을 검토하여 최신 패치 적용이 어려울 경우 별도의 보완대책을 마련하여 이행하여야 한다.
		2.10.9	악성코드 통제	바이러스·웬·트로이목마·랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방·탐지·대응 등의 보호대책을 수립·이행하여야 한다.
2.11.	사고 예방 및 대응	2.11.1	사고 예방 및 대응체계 구축	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조체계를 구축하여야 한다.
		2.11.2	취약점 점검 및 조치	정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.
		2.11.3	이상행위 분석 및 모니터링	내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후조치는 적시에 이루어져야 한다.
		2.11.4	사고 대응 훈련 및 개선	침해사고 및 개인정보 유출사고 대응 절차를 임직원과 이해관계자가 숙지하도록 시나리오에 따른 모의훈련을 연 1회 이상 실시하고 훈련결과를 반영하여 대응체계를 개선하여야 한다.
		2.11.5	사고 대응 및 복구	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하여야 한다.
2.12.	재해복구	2.12.1	재해·재난 대비 안전조치	자연재해, 통신·전력 장애, 해킹 등 조직의 핵심 서비스 및 시스템의 운영 연속성을 위협할 수 있는 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 복구 목표시간, 복구 목표시점을 정의하고 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구체계를 구축하여야 한다.
		2.12.2	재해 복구 시험 및 개선	재해 복구 전략 및 대책의 적정성을 정기적으로 시험하여 시험결과, 정보시스템 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.

다. 개인정보 처리 단계별 요구사항

분야		항목		상세 내용
3.1.	개인정보 수집 시 보호조치	3.1.1	개인정보 수집 · 이용	개인정보는 적법하고 정당하게 수집 · 이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 14세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
		3.1.2	개인정보 수집 제한	개인정보를 수집하는 경우 처리 목적에 필요한 최소한의 개인정보만을 수집하여야 하며, 정보주체가 선택적으로 동의할 수 있는 사항 등에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하지 않아야 한다.
		3.1.3	주민등록번호 처리 제한	주민등록번호는 법적 근거가 있는 경우를 제외하고는 수집 · 이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.
		3.1.4	민감정보 및 고유식별정보의 처리 제한	민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체의 별도 동의를 받아야 한다.
		3.1.5	개인정보 간접수집	정보주체 이외로부터 개인정보를 수집하거나 제3자로부터 제공받는 경우에는 업무에 필요한 최소한의 개인정보를 수집하거나 제공받아야 하며, 법령에 근거하거나 정보주체의 요구가 있으면 개인정보의 수집 출처, 처리목적, 처리정지의 요구권리를 알려야 한다.
		3.1.6	영상정보처리기기 설치 · 운영	고정형 영상정보처리기기를 공개된 장소에 설치 · 운영하거나 이동형 영상정보처리기기를 공개된 장소에서 업무를 목적으로 운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항을 준수하고, 적절한 보호대책을 수립 · 이행하여야 한다.
		3.1.7	마케팅 목적의 개인정보 수집 · 이용	재화나 서비스의 홍보, 판매 권유, 광고성 정보전송 등 마케팅 목적으로 개인정보를 수집 · 이용하는 경우 그 목적을 정보주체가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다.
3.2.	개인정보 보유 및 이용 시 보호조치	3.2.1	개인정보 현황관리	수집 · 보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 하며, 공공기관의 경우 이를 법률에서 정한 관계기관의 장에게 등록하여야 한다.
		3.2.2	개인정보 품질보장	수집된 개인정보는 처리 목적에 필요한 범위에서 개인정보의 정확성 · 완전성 · 최신성이 보장되도록 정보주체에게 관리절차를 제공하여야 한다.
		3.2.3	이용자 단말기 접근 보호	정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 접근이 필요한 경우 이를 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받아야 한다.
		3.2.4	개인정보 목적 외 이용 및 제공	개인정보는 수집 시의 정보주체에게 고지 · 동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용 · 제공하려는 때에는 정

				보주체의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.
		3.2.5	가명정보 처리	가명정보를 처리하는 경우 목적제한, 결합제한, 안전조치, 금지의무 등 법적 요건을 준수하고 적정 수준의 가명처리를 보장할 수 있도록 가명처리 절차를 수립·이행하여야 한다.
3.3.	개인정보 제공 시 보호조치	3.3.1	개인정보 제3자 제공	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
		3.3.2	개인정보 처리 업무 위탁	개인정보 처리업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자 등 관련사항을 공개하여야 한다. 또한 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다.
		3.3.3	영업의 양도 등에 따른 개인정보 이전	영업의 양도·합병 등으로 개인정보를 이전하거나 이전받는 경우 정보주체 통지 등 적절한 보호조치를 수립·이행하여야 한다.
		3.3.4	개인정보 국외이전	개인정보를 국외로 이전하는 경우 국외 이전에 대한 동의, 관련 사항에 대한 공개 등 적절한 보호조치를 수립·이행하여야 한다.
3.4.	개인정보 파기 시 보호조치	3.4.1	개인정보 파기	개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.
		3.4.2	처리목적 달성 후 보유 시 조치	개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.
3.5.	정보주체 권리보호	3.5.1	개인정보 처리방침 공개	개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 정보주체가 알기 쉽도록 개인정보 처리방침을 수립하고, 이를 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화하여야 한다.
		3.5.2	정보주체 권리보장	정보주체가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 등 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.
		3.5.3	정보주체에 대한 통지	개인정보의 이용·제공 내역 등 정보주체에게 통지하여야 할 사항을 파악하여 그 내용을 주기적으로 통지하여야 한다.

인증기준(제23조제3항 관련)

가. 관리체계 수립 및 운영

분야		항목		상세 내용
1.1.	관리체계 기반 마련	1.1.1	경영진의 참여	최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.
		1.1.2	최고책임자의 지정	최고경영자는 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.
		1.1.3	조직 구성	최고경영자는 정보보호의 효과적 구현을 위한 실무조직을 구성하여 운영하여야 한다.(단, 정보보호 및 개인정보보호 관리체계 인증의 경우 ‘정보보호’를 ‘정보보호 및 개인정보보호’로 한다.)
		1.1.4	범위 설정	조직의 핵심 서비스를 고려하여 관리체계 범위를 설정하고, 관련된 서비스를 비롯하여 조직, 자산, 물리적 위치 등을 문서화하여야 한다.
		1.1.5	정책 수립	정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.(단, 정보보호 및 개인정보보호 관리체계 인증의 경우 ‘정보보호’를 ‘정보보호 및 개인정보보호’로 한다.)
1.2.	위험 관리	1.2.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
1.3.	관 리 체 계 운영	1.3.1	운영현황 관리	조직이 수립한 관리체계에 따라 상시적 또는 주기적으로 수행하여야 하는 운영활동 및 수행 내역은 식별 및 추적이 가능하도록 기록하여 관리하고, 경영진은 주기적으로 운영활동의 효과성을 확인하여 관리하여야 한다.
1.4.	관 리 체 계 점검 및 개선	1.4.1	관리체계 점검	관리체계가 내부 정책 및 시행문서에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하고, 경영진은 발견된 문제점에 대한 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.

나. 보호대책 요구사항

분야		항목		상세 내용
2.1.	인적 보안	2.1.1	보안 서약	정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 한다.
		2.1.2	인식제고 및 교육훈련	임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고 직무별 전문성을 확보할 수 있도록 연간 인식제고 활동 및 교육훈련 계획을 수립·운영하고, 그 결과에 따른 효과성을 평가하여 다음 계획에 반영하여야 한다.
2.2.	외부자 보안	2.2.1	외부자 계약 시 보안	외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우 이에 따른 정보보호 및 개인정보보호 요구사항을 식별하고, 관련 내용을 계약서 또는 협정서 등에 명시하여

				야 한다.
2.3.	물리 보안	2.3.1	보호구역 지정	내외부의 위협으로부터 주요 설비 및 자료 등을 보호하기 위하여 통제구역·제한구역·접건구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립하고 이행 여부를 주기적으로 검토하여야 한다.
		2.3.2	정보시스템 보호	정보시스템은 환경적 위협과 유해요소, 비인가 접근 가능성을 감소시킬 수 있도록 중요도와 특성을 고려하여 배치하고, 통신 및 전력 케이블이 손상을 입지 않도록 보호하여야 한다.
		2.3.3	반출입 기기 통제	보호구역 내에서의 비인가행위 및 권한 오·남용 등을 방지하기 위하여 작업 절차를 수립·이행하고, 반출입 이력을 주기적으로 검토하여야 한다.
		2.3.4	업무환경 보안	공용으로 사용하는 사무용 기기(문서고, 공용 PC, 복합기, 파일서버 등) 및 개인 업무환경(업무용 PC, 책상 등)을 통해 개인정보 및 중요정보가 비인가자에게 노출 또는 유출되지 않도록 클린데스크, 정기점검 등 업무환경 보호대책을 수립·이행하여야 한다.
2.4.	인증 및 권한관리	2.4.1	사용자 계정 관리	정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다.
		2.4.2	사용자 식별	사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립·이행하여야 한다.
		2.4.3	사용자 인증	정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여야 한다.
		2.4.4	비밀번호 관리	법적 요구사항, 외부 위협요인 등을 고려하여 정보시스템 사용자 및 고객, 회원 등 정보주체(이용자)가 사용하는 비밀번호 관리절차를 수립·이행하여야 한다.
2.5.	접근통제	2.5.1	네트워크 접근	유·무선 네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB 존, 개발존 등)와 접근통제를 적용하여야 한다.
		2.5.2	정보시스템 접근	서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.
		2.5.3	원격접근 통제	통제구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 보호대책을 수립·이행하여야 한다.
		2.5.4	인터넷 접속 통제	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P2P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접

				속 통제 정책을 수립·이행하여야 한다.
2.6.	암호화 적용	2.6.1	암호정책 적용	개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책 및 암호키 관리 절차를 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.
2.7.	정보시스템 도입 및 개발 보안	2.7.1	보안 요구사항 정의	정보시스템의 도입·개발·변경 시 정보보호 및 개인정보 보호 관련 법적 요구사항, 최신 보안취약점, 안전한 코딩 방법 등 보안 요구사항을 정의하고 적용하여야 한다.
		2.7.2	시험과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소시키기 위하여 원칙적으로 분리하여야 한다.
		2.7.3	시험 데이터 보안	시스템 시험 과정에서 운영데이터의 유출을 예방하기 위하여 시험 데이터의 생성과 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립·이행하여야 한다.
		2.7.4	소스 프로그램 관리	소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하고, 운영환경에 보관하지 않는 것을 원칙으로 하여야 한다.
2.8.	시스템 및 서비스 운영관리	2.8.1	변경관리	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립·이행하고, 변경 전 시스템의 성능 및 보안에 미치는 영향을 분석하여야 한다.
		2.8.2	백업 및 복구관리	정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상, 주기, 방법, 보관장소, 보관기간, 소산 등의 절차를 수립·이행하여야 한다. 아울러 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
		2.8.3	로그 및 접속기록 관리	서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리하며, 접근 및 사용에 대한 로그 검토기준에 따라 주기적으로 점검하여야 한다.
2.9.	시스템 및 서비스 보안관리	2.9.1	보안시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.
		2.9.2	클라우드 보안	클라우드 서비스 이용 시 서비스 유형(SaaS, PaaS, IaaS 등)에 따른 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호대책을 수립·이행하여야 한다.
		2.9.3	공개서버 보안	외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행하여야 한다.
		2.9.4	업무용 단말기기 보안	PC, 모바일 기기 등 단말기기를 업무 목적으로 네트워크에 연결할 경우 기기 인증 및 승인, 접근 범위, 기기 보안설정 등의 접근통제 대책을 수립하고 주기적으로 점검하여야 한다.
		2.9.5	보조저장매체 관리	보조저장매체를 통하여 개인정보 또는 중요정보의 유출이 발생하거나 악성코드가 감염되지 않도록 관리 절차를 수립·이행하고, 개인정보 또는 중요정보가 포함된 보조저장매체는 안전한 장소에 보관하여야 한다.
		2.9.6	패치관리	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인한 침해사고를 예방하기 위하여 최신 패치를 적용하여야 한다. 다만 서비스 영향을 검토하여 최신 패치 적용이 어려운 경우 별도의 보완대책을 마련하여 이행하여야 한다.
		2.9.7	악성코드 통제	바이러스·웬·트로이목마·랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방·탐지·대응 등의

				보호대책을 수립·이행하여야 한다.
2.10.	사고 예방 및 대응	2.10.1	사고 예방 및 대응체계 구축	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하게 대응할 수 있도록 외부기관 등과 협조체계를 구축하여야 한다.
		2.10.2	취약점 점검 및 조치	정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.
		2.10.3	사고 대응 및 복구	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하여야 한다.

다. 개인정보 처리 단계별 요구사항

분야		항목		상세 내용
3.1.	개인정보수집 시 보호조치	3.1.1	개인정보 수집·이용	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 14세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
		3.1.2	개인정보 수집 제한	개인정보를 수집하는 경우 처리 목적에 필요한 최소한의 개인정보만을 수집하여야 하며, 정보주체가 선택적으로 동의할 수 있는 사항 등에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하지 않아야 한다.
		3.1.3	주민등록번호 처리 제한	주민등록번호는 법적 근거가 있는 경우를 제외하고는 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.
		3.1.4	민감정보 및 고유식별정보의 처리 제한	민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체의 별도 동의를 받아야 한다.
		3.1.5	개인정보 간접수집	정보주체 이외로부터 개인정보를 수집하거나 제3자로부터 제공받는 경우에는 업무에 필요한 최소한의 개인정보를 수집하거나 제공받아야 하며, 법령에 근거하거나 정보주체의 요구가 있으면 개인정보의 수집 출처, 처리목적, 처리정지의 요구권리를 알려야 한다.
		3.1.6	영상정보처리기기 설치·운영	고정형 영상정보처리기기를 공개된 장소에 설치·운영하거나 이동형 영상정보처리기기를 공개된 장소에서 업무를 목적으로 운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항을 준수하고, 적절한 보호대책을 수립·이행하여야 한다.
		3.1.7	마케팅 목적의 개인정보 수집·이용	재화나 서비스의 홍보, 판매 권유, 광고성 정보전송 등 마케팅 목적으로 개인정보를 수집·이용하는 경우 그 목적을 정보주체가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다.

3.2.	개인정보 보유 및 이용 시 보호조치	3.2.1	개인정보 현황관리	수집·보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 하며, 공공기관의 경우 이를 법률에서 정한 관계기관의 장에게 등록하여야 한다.
		3.2.2	개인정보 품질보장	수집된 개인정보는 처리 목적에 필요한 범위에서 개인정보의 정확성·완전성·최신성이 보장되도록 정보주체에게 관리절차를 제공하여야 한다.
		3.2.3	이용자 단말기 접근 보호	정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 접근이 필요한 경우 이를 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받아야 한다.
		3.2.4	개인정보 목적 외 이용 및 제공	개인정보는 수집 시의 정보주체에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.
		3.2.5	가명정보 처리	가명정보를 처리하는 경우 목적제한, 결합제한, 안전조치, 금지의무 등 법적 요건을 준수하고 적정 수준의 가명처리를 보장할 수 있도록 가명처리 절차를 수립·이행하여야 한다.
3.3.	개인정보 제공 시 보호조치	3.3.1	개인정보 제3자 제공	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
		3.3.2	개인정보 처리 업무 위탁	개인정보 처리업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자 등 관련사항을 공개하여야 한다. 또한 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다.
		3.3.3	영업의 양도 등에 따른 개인정보 이전	영업의 양도·합병 등으로 개인정보를 이전하거나 이전받는 경우 정보주체 통지 등 적절한 보호조치를 수립·이행하여야 한다.
		3.3.4	개인정보 국외이전	개인정보를 국외로 이전하는 경우 국외 이전에 대한 동의, 관련 사항에 대한 공개 등 적절한 보호조치를 수립·이행하여야 한다.
3.4.	개인정보파기 시 보호조치	3.4.1	개인정보 파기	개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.
		3.4.2	처리목적 달성 후 보유 시 조치	개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.
3.5.	정보주체 권리보호	3.5.1	개인정보 처리방침 공개	개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 정보주체가 알기 쉽도록 개인정보 처리방침을 수립하고,

				이를 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화하여야 한다.
		3.5.2	정보주체 권리보장	정보주체가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 등 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.
		3.5.3	정보주체에 대한 통지	개인정보의 이용·제공 내역 등 정보주체에게 통지하여야 할 사항을 파악하여 그 내용을 주기적으로 통지하여야 한다.

인증기준(제23조제4항 관련)

가. 관리체계 수립 및 운영

분야		항목		상세 내용
1.1.	관리체계 기반 마련	1.1.1	경영진의 참여	최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.
		1.1.2	최고책임자의 지정	최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.
		1.1.3	조직 구성	최고경영자는 정보보호의 효과적 구현을 위한 실무조직을 구성하여 운영하여야 한다.(단, 정보보호 및 개인정보보호 관리체계 인증의 경우 ‘정보보호’를 ‘정보보호 및 개인정보보호’로 한다.)
		1.1.4	범위 설정	조직의 핵심 서비스를 고려하여 관리체계 범위를 설정하고, 관련된 서비스를 비롯하여 조직, 자산, 물리적 위치 등을 문서화하여야 한다.
		1.1.5	정책 수립	정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.(단, 정보보호 및 개인정보보호 관리체계 인증의 경우 ‘정보보호’를 ‘정보보호 및 개인정보보호’로 한다.)
1.2.	위험 관리	1.2.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 물리적 인프라를 제외한 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
		1.2.2	현황 및 흐름분석	관리체계 전 영역에 대한 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
1.3.	관 리 체 계 운영	1.3.1	운영현황 관리	조직이 수립한 관리체계에 따라 상시적 또는 주기적으로 수행하여야 하는 운영활동 및 수행 내역은 식별 및 추적이 가능하도록 기록하여 관리하고, 경영진은 주기적으로 운영활동의 효과성을 확인하여 관리하여야 한다.
1.4.	관 리 체 계 점검 및 개선	1.4.1	법적 요구사항 준수 검토	조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.
		1.4.2	관리체계 점검	관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다.
		1.4.3	관리체계 개선	법적 요구사항 준수검토 및 관리체계 점검을 통해 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하며, 경영진은 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.

나. 보호대책 요구사항

분야		항목		상세 내용
2.1.	정책, 조직, 자산 관리	2.1.1	정책의 유지관리	정보보호 및 개인정보보호 관련 정책과 시행문서는 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경변화 등에 따라 주기적으로 검토하여 필요한 경우 제·개정하고 그 내역을 이력관리하여야 한다.
		2.1.2	조직의 유지관리	조직의 각 구성원에게 정보보호와 개인정보보호 관련 역할 및 책임을 할당하고, 그 활동을 평가할 수 있는 체계와 조직 및 조직의 구성원 간 상호 의사소통할 수 있는 체계를 수립하여 운영하여야 한다.
		2.1.3	정보자산 관리	정보자산의 용도와 중요도에 따른 취급 절차 및 보호대책을 수립·이행하고, 자산별 책임소재를 명확히 정의하여 관리하여야 한다.
2.2	인적 보안	2.2.1	주요 직무자 지정 및 관리	개인정보 및 중요정보의 취급이나 주요 시스템 접근 등 주요 직무의 기준과 관리방안을 수립하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다.
		2.2.2	보안 서약	정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 한다.
		2.2.3	인식제고 및 교육훈련	임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고 직무별 전문성을 확보할 수 있도록 연간 인식제고 활동 및 교육훈련 계획을 수립·운영하고, 그 결과에 따른 효과성을 평가하여 다음 계획에 반영하여야 한다.
		2.2.4	퇴직 및 직무변경 관리	퇴직 및 직무변경 시 인사·정보보호·개인정보보호·IT 등 관련 부서별 이행하여야 할 자산반납, 계정 및 접근권한 회수·조정, 결과확인 등의 절차를 수립·관리하여야 한다.
2.3.	외부자 보안	2.3.1	외부자 계약 시 보안	외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우 이에 따른 정보보호 및 개인정보보호 요구사항을 식별하고, 관련 내용을 계약서 또는 협정서 등에 명시하여야 한다.
2.4.	물리 보안	2.4.1	출입통제	통제구역은 비인가자의 출입을 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
		2.4.2	업무환경 보안	공용으로 사용하는 사무용 기기(문서고, 공용 PC, 복합기, 파일서버 등) 및 개인 업무환경(업무용 PC, 책상 등)을 통해 개인정보 및 중요정보가 비인가자에게 노출 또는 유출되지 않도록 클린데스크, 정기점검 등 업무환경 보호 대책을 수립·이행하여야 한다.
2.5.	인증 및 권한관리	2.5.1	사용자 계정 관리	정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다.
		2.5.2	사용자 식별	사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립·이행하여야 한다.
		2.5.3	사용자 인증	정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여

				야 한다.
		2.5.4	비밀번호 관리	법적 요구사항, 외부 위협요인 등을 고려하여 정보시스템 사용자 및 고객, 회원 등 정보주체(이용자)가 사용하는 비밀번호 관리절차를 수립·이행하여야 한다.
2.6.	접근통제	2.6.1	네트워크 접근	관리자 및 사용자 등 업무목적에 따라 네트워크를 분리하고 IP관리, 단말인증 등 접근통제를 적용하여야 한다.
		2.6.2	정보시스템 접근	정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.
		2.6.3	원격접근 통제	통제구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 보호대책을 수립·이행하여야 한다.
		2.6.4	인터넷 접속 통제	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P2P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.
2.7.	암호화 적용	2.7.1	암호정책 적용	개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책 및 암호키 관리 절차를 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.
2.8.	정보시스템 도입 및 개발 보안	2.8.1	보안 요구사항 정의	정보시스템의 도입·개발·변경 시 안전한 코딩방법을 적용하여야 한다.
		2.8.2	시험 데이터 보안	시스템 시험 과정에서 운영데이터의 유출을 예방하기 위하여 시험 데이터의 생성과 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립·이행하여야 한다.
		2.8.3	소스 프로그램 관리	소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하여야 한다.
2.9.	시스템 및 서비스 운영관리	2.9.1	변경관리	정보시스템 관련 자산을 관리할 수 있도록 절차를 수립·이행하고, 변경 전 시스템의 성능 및 보안에 미치는 영향을 분석하여야 한다.
		2.9.2	백업 및 복구관리	정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상, 주기, 방법, 보관장소, 보관기간, 소산 등의 절차를 수립·이행하여야 한다. 아울러 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
		2.9.3	로그 및 접속기록 관리	정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리하여야 한다.
2.10.	시스템 및 서비스 보안관리	2.10.1	보안시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.
		2.10.2	업무용 단말기기 보안	PC, 모바일 기기 등 단말기기를 업무 목적으로 네트워크에 연결할 경우 기기 인증 및 승인, 접근 범위, 기기 보안설정 등의 접근통제 대책을 수립하고 주기적으로 점검하여야 한다.
		2.10.3	보조저장매체 관리	보조저장매체를 통하여 개인정보 또는 중요정보의 유출이 발생하거나 악성코드가 감염되지 않도록 관리 절차를 수립·이행하고, 개인정보 또는 중요정보가 포함된 보조저장매체는 안전한 장소에 보관하여야 한다.
		2.10.4	패치관리	정보시스템의 취약점으로 인한 침해사고를 예방하기 위하여 최신 패치를 적용하여야 한다. 다만 서비스 영향을 검토하여 최신 패치 적용이 어려울 경우 별도의 보완대책을

				마련하여 이행하여야 한다.
		2.10.5	악성코드 통제	바이러스·웜·트로이목마·랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방·탐지·대응 등의 보호대책을 수립·이행하여야 한다.
2.11.	사고 예방 및 대응	2.11.1	사고 예방 및 대응체계 구축	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하게 대응할 수 있도록 외부기관 등과 협조체계를 구축하여야 한다.
		2.11.2	취약점 점검 및 조치	정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.
		2.11.3	사고 대응 및 복구	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하여야 한다.

다. 개인정보 처리 단계별 요구사항

분야		항목		상세 내용
3.1.	개인정보수집 시 보호조치	3.1.1	개인정보 수집·이용	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 14세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
		3.1.2	개인정보 수집 제한	개인정보를 수집하는 경우 처리 목적에 필요한 최소한의 개인정보만을 수집하여야 하며, 정보주체가 선택적으로 동의할 수 있는 사항 등에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하지 않아야 한다.
		3.1.3	주민등록번호 처리 제한	주민등록번호는 법적 근거가 있는 경우를 제외하고는 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.
		3.1.4	민감정보 및 고유식별정보의 처리 제한	민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체의 별도 동의를 받아야 한다.
		3.1.5	개인정보 간접수집	정보주체 이외로부터 개인정보를 수집하거나 제3자로부터 제공받는 경우에는 업무에 필요한 최소한의 개인정보를 수집하거나 제공받아야 하며, 법령에 근거하거나 정보주체의 요구가 있으면 개인정보의 수집 출처, 처리목적, 처리정지의 요구권리를 알려야 한다.
		3.1.6	영상정보처리기기 설치·운영	고정형 영상정보처리기기를 공개된 장소에 설치·운영하거나 이동형 영상정보처리기기를 공개된 장소에서 업무를 목적으로 운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항을 준수하고, 적절한 보호대책을 수립·이행하여야 한다.
		3.1.7	마케팅 목적의 개인정보 수집·이용	재화나 서비스의 홍보, 판매 권유, 광고성 정보전송 등 마케팅 목적으로 개인정보를 수집·이용하는 경우 그 목

				적을 정보주체가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다.
3.2.	개인정보 보유 및 이용 시 보호조치	3.2.1	개인정보 현황관리	수집·보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 하며, 공공기관의 경우 이를 법률에서 정한 관계기관의 장에게 등록하여야 한다.
		3.2.2	개인정보 품질보장	수집된 개인정보는 처리 목적에 필요한 범위에서 개인정보의 정확성·완전성·최신성이 보장되도록 정보주체에게 관리절차를 제공하여야 한다.
		3.2.3	이용자 단말기 접근 보호	정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 접근이 필요한 경우 이를 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받아야 한다.
		3.2.4	개인정보 목적 외 이용 및 제공	개인정보는 수집 시의 정보주체에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.
		3.2.5	가명정보 처리	가명정보를 처리하는 경우 목적제한, 결합제한, 안전조치, 금지의무 등 법적 요건을 준수하고 적정 수준의 가명처리를 보장할 수 있도록 가명처리 절차를 수립·이행하여야 한다.
3.3.	개인정보 제공 시 보호조치	3.3.1	개인정보 제3자 제공	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
		3.3.2	개인정보 처리 업무 위탁	개인정보 처리업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자 등 관련사항을 공개하여야 한다. 또한 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다.
		3.3.3	영업의 양도 등에 따른 개인정보 이전	영업의 양도·합병 등으로 개인정보를 이전하거나 이전받는 경우 정보주체 통지 등 적절한 보호조치를 수립·이행하여야 한다.
		3.3.4	개인정보 국외이전	개인정보를 국외로 이전하는 경우 국외 이전에 대한 동의, 관련 사항에 대한 공개 등 적절한 보호조치를 수립·이행하여야 한다.
3.4.	개인정보파기 시 보호조치	3.4.1	개인정보 파기	개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.
		3.4.2	처리목적 달성 후 보유 시 조치	개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.

3.5.	정보주체 권리보호	3.5.1	개인정보 처리방침 공개	개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 정보주체가 알기 쉽도록 개인정보 처리방침을 수립하고, 이를 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화하여야 한다.
		3.5.2	정보주체 권리보장	정보주체가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 등 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.
		3.5.3	정보주체에 대한 통지	개인정보의 이용·제공 내역 등 정보주체에게 통지하여야 할 사항을 파악하여 그 내용을 주기적으로 통지하여야 한다.

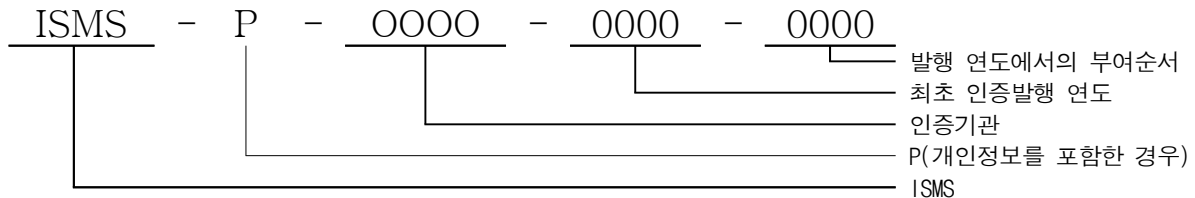
[별표 8]

인증의 표시(제32조, 제34조 관련)




1. 인증번호 부여

가. 인증번호는 유일성, 간결성, 관리의 용이성 등을 고려하여 최초심사, 갱신심사의 구분 없이 최초 발급 순서별로 부여한다.

나. 인증번호는 아래와 같은 형식으로 부여한다.



2. 도안모형

정보보호 및 개인정보보호 관리체계 인증	정보보호 관리체계 인증	정보보호 관리체계 예비인증
 <p>[인증범위] 000 시스템 운영 [유효기간] 2022.00.00 ~ 2025.00.00</p>	 <p>[인증범위] 000 시스템 운영 [유효기간] 2022.00.00 ~ 2025.00.00</p>	 <p>[인증범위] 000 시스템 운영(고시 제18조의2에 따른 예비인증) [유효기간] 2022.00.00 ~ 2025.00.00</p>

3. 인증 표시에 대한 유의사항

가. 인증 취득 사실의 홍보는 인증서를 발급받은 날부터 효력이 유지되는 동안에만 사용이 가능하다. 인증이 취소된 경우에는 인증에 대한 홍보, 인증서 사용을 중지하여야 한다.

나. 인증 표시를 사용하는 경우 유효기간, 인증범위를 함께 표시하여야 한다.

다. 인증을 취득한 자는 인증의 사실을 과장되거나 불명확한 표현을 사용하여 광고할 수 없다.

라. 고시 제18조의2에 따라 예비인증을 취득한 자는 예비인증 마크 사용과 함께 예비인증의 사실을 표시하여야 한다.

4. 인증 표시의 사용 방법

가. 인증 표시는 지정된 색상으로 사용할 수 있다. 또한 색상이 명확하게 나타날 수 있는 바탕색 위에 흑백으로 사용하거나 표시된 인쇄물의 주된 단일색상으로 사용할 수 있다.

나. 인증 표시의 크기는 표시물 대상의 크기나 표시장소의 여건에 따라 조정할 수 있으며, 같은 비율로 축소 또는 확대하여 표시할 수 있다.

다. 일반문서, 편지의 상단, 송장, 홍보 책자 등에 인증 취득 사실의 내용을 홍보할 수 있다.

5. 인증명판 제작 시 유의사항

가. 소재는 가급적 동판으로 제작한다.

나. 바탕색은 가급적 연마하지 않은 황동색으로 한다.

다. 도안 모형은 인증의 표지를 중앙에 둔다.

라. 글씨 및 도형은 양각으로 한다.

마. 크기는 사각형으로 하며 가로와 세로 비율을 3 : 2로 하여 일정 비율로 조정할 수 있다.

인증기관·심사기관 지정 신청서

※ 색상이 어두운 난은 신청인이 작성하지 아니하며, []에는 해당되는 곳에 √ 표를 합니다.

접수번호	접수일시	처리기간
신청인	업체명	사업자등록번호
	대표자	전화번호
	주소	
	전자우편 주소(e-mail)	
	총 직원 수	인증심사를 수행하는 직원 수
신청구분	[] 신규 [] 재지정	
기관구분	[] 인증기관 [] 심사기관	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제6항, 제7항 및 같은 법 시행령 제53조의2, 「개인정보 보호법」 제32조제5항 및 같은 법 시행령 제34조의6, 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제6조에 따라 정보보호 및 개인정보보호 관리체계 인증기관 또는 심사기관 지정을 위와 같이 신청합니다.

년 월 일

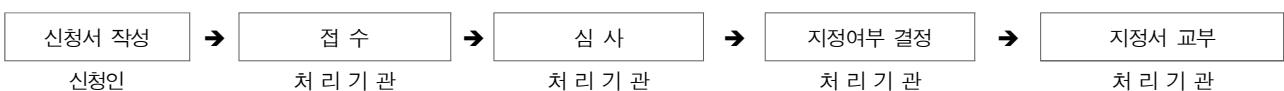
신청인(대표자)

(서명 또는 인)

과학기술정보통신부장관 귀하 개인정보 보호위원회 귀하

첨부서류 (각 3부)	1. 정관 또는 규약 2. 별지 제2호서식의 인증심사원의 보유현황과 이를 증명할 수 있는 서류 3. 별표 1에 따른 업무수행 요건·능력 심사를 위하여 필요한 서류 1부	수수료
담당공무원 확인사항	법인등기사항증명서	없음

처 리 절 차



210mm×297mm[(백상지(80g/㎡)또는 중질지(80g/㎡)]

인증심사 업무를 수행하는 직원 보유현황

신청인	업체명					
	대표자					
	전체 직원 수			인증심사 업무를 전담하는 직원의 수		

번호	성명	생년월일	입사일	소속부서 및 업무		고용형태
		인증심사원 자격번호	최초자격취득일	심사원 등급 ※ 신청서 제출 시점	인증심사 참여 일수 ※ 최근 3년 이내	비고
				
			. . .		일	
				
			. . .		일	
				
			. . .		일	
				
			. . .		일	
				
			. . .		일	

유의사항

1. 「심사원등급」란에는 심사원보, 심사원, 선임심사원 여부를 기재한다.
2. 인증심사원 자격 보유 및 인증심사 경력을 증빙할 수 있는 서류를 함께 제출하여야 한다.
3. 비고에 학위, 자격 등에 대한 사항을 추가로 기재한 경우 학위 및 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.

210mm×297mm[(백상지(80g/㎡)]

정보보호 및 개인정보보호 관리체계 인증기관 지정서

등록번호 : 유효기간 :
업 체 명 : 대 표 자 :
업무의 범위 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제6항 및 같은 법 시행령 제53조의2, 「개인정보 보호법」 제32조제5항 및 같은 법 시행령 제34조의6에 따라 위와 같이 정보보호 및 개인정보보호 관리체계 인증기관 (위 인증업무에 한함)으로 지정합니다.

년 월 일

과학기술정보통신부장관

직인

개인정보 보호위원회

직인

210mm×297mm[백상지 (150g/㎡)]

(제2쪽)

CERTIFICATE OF DESIGNATION AS Certification Body of Personal information & Information Security Management System

Registry Number : Period of Validity :
Name of Organization : Name of Representative :
Scope of Certification work :
:

This is to certify that the abovementioned organization is designated Certification Body of Personal information & Information Security Management System in accordance with Article 47, Paragraph 6 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act and in accordance with Article 32-2, Paragraph 5 of 「Personal Information Protection Act」 and Article 34-6 of the Enforcement Decree of the same Act.

Date of Issuance:

서 명 또는 직 인
Minister, Ministry of Science and ICT

서 명 또는 직 인
Personal Information Protection Commission

210mm×297mm[백상지 (150g/㎡)]

정보보호 및 개인정보보호 관리체계 심사기관 지정서

등록번호 : 유효기간 :
업 체 명 : 대 표 자 :
업무의 범위 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제7항 및 같은 법 시행령 제53조의2, 「개인정보 보호법」 제32조제5항 및 같은 법 시행령 제34조의6에 따라 위와 같이 정보보호 및 개인정보보호 관리체계 심사기관(위 심사업무에 한함)으로 지정합니다.

년 월 일

과학기술정보통신부장관

직인

개인정보 보호위원회

직인

210mm×297mm[백상지 (150g/㎡)]

(제2쪽)

CERTIFICATE OF DESIGNATION AS Examination Institution for Personal information & Information Security Management System

Registry Number : Period of Validity :
Name of Organization : Name of Representative :
Address :
Scope of Examination work :

This is to certify that the abovementioned organization is designated Examination Institution of Personal information & Information Security Management System in accordance with Article 47, Paragraph 7 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act and in accordance with Article 32-2, Paragraph 5 of 「Personal Information Protection Act」 and Article 34-6 of the Enforcement Decree of the same Act.

Date of Issuance:

서 명 또는 직 인
Minister, Ministry of Science and ICT

서 명 또는 직 인
Personal Information Protection Commission

210mm×297mm[백상지 (150g/㎡)]

인증실적 보고서

※ []에는 해당되는 곳에 √ 표를 합니다.

인증기관	업체명	
	대표자	사업자등록번호
	인증기관 등록번호	인증기관 지정일(유효기간)
	인증업무의 범위	

구분	세부	실적
정보보호 및 개인정보보호 관리체계 인증 실적	신규 인증 건수	건
	인증 취소 건수	건
	인증 유지 건수	건
정보보호 관리체계 인증 실적	신규 인증 건수	건
	인증 취소 건수	건
	인증 유지 건수	건
인증기관 지정요건 내역 변동사항	[] 없음	[] 있음

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제53조의4, 「개인정보 보호법 시행령」 제34조의6, 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제8조에 따라 정보보호 및 개인정보보호 관리체계 인증실적을 제출합니다.

년 월 일

신청인(대표자)

(서명 또는 인)

과학기술정보통신부장관 귀하 개인정보 보호위원회 귀하

첨부서류	1.인증실적 내역 2.인증기관 지정요건 내역 변동사항(해당되는 경우만 제출)
------	---

210mm×297mm[(백상지(80g/㎡))]

인증심사실적 보고서

※ []에는 해당되는 곳에 √ 표를 합니다.

심사기관	업체명	
	대표자	사업자등록번호
	심사기관 등록번호	심사기관 지정일(유효기간)
	심사업무의 범위	

구분	세부	실적
정보보호 및 개인정보보호 관리체계 인증심사 실적	최초심사	건
	갱신심사	건
	사후심사	건
정보보호 관리체계 인증심사 실적	최초심사	건
	갱신심사	건
	사후심사	건
심사기관 지정요건 내역 변동사항	[] 없음 [] 있음	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제53조의4, 「개인정보 보호법 시행령」 제34조의6, 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제8조에 따라 정보보호 및 개인정보보호 관리체계 인증심사실적을 제출합니다.

년 월 일

신청인(대표자)

(서명 또는 인)

과학기술정보통신부장관 귀하 개인정보 보호위원회 귀하

첨부서류	1. 인증심사실적 내역 2. 심사기관 지정요건 내역 변동사항(해당되는 경우만 제출)
------	---

210mm×297mm[(백상지(80g/㎡))]

인증심사원 자격 신청서

※ 색상이 어두운 난은 신청인이 작성하지 아니하며, []에는 해당되는 곳에 √ 표를 합니다.

접수번호		접수일시		처리기간		
신청자 인적사항	성명		생년월일		신청일부터 6개월 내에 촬영된 컬러사진 (3.5cm × 4.5cm)	
	소속					
	주소	(우:)				
	휴대전화					
	이메일					
학력사항	최종학력	[] 고졸 [] 전문대졸 [] 대졸 [] 석사 [] 박사				
경력사항 (※ 서류로 증명 가능한 내용만 기술)	경력 내역 (중복불가)	[] 정보보호 경력		총	년	개월
		[] 개인정보보호 경력		총	년	개월
		[] 정보기술 경력		총	년	개월
		총 합		총	년	개월
	경력인정 자격	자격증 또는 학위명(전공 또는 논문명)		취득일자		수여기관

정보보호 및 개인정보보호 관리체계 인증심사원 자격을 신청하기 위하여 이 신청서를 제출합니다.
본 신청서의 내용이 사실과 다르거나, 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 별표4의 인증심사원 자격 신청 요건에 해당하지 아니할 때에는 합격 또는 자격을 취소하여도 이의를 제기하지 않겠습니다.

년 월 일

신청자

(서명 또는 인)

한국인터넷진흥원장 귀하

첨부서류	1. 자격 신청 세부내역서 2. 응시요건에 충족함을 증빙하는 서류 ① 학력증명서 ② 부서이동 및 수행업무 내역이 구체적으로 기재된 상세 경력증명서 또는 재직증명서 ③ 기술실적증명서(해당 시) ④ 자격증명서(해당 시) 3. 정보보호 서약서 4. 개인정보 수집·이용 동의서 등
------	---

210mm×297mm[(백상지(80g/㎡) 또는 중질지(80g/㎡)]

정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서

1. 발급번호 :
2. 성 명 :
3. 생년월일 :
4. 유효기간 :
5. 등 급 :

위 사람은 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제14조에 따른 정보보호 및 개인정보보호 관리체계 인증심사원임을 증명합니다.

년 월 일

한국인터넷진흥원장

직인

정보보호 및 개인정보보호 관리체계 인증 신청서

※ 색상이 어두운 란은 신청인이 작성하지 아니하며, []에는 해당되는 곳에 √ 표를 합니다.

접수번호	접수일시	처리기간
신청인	업체명	사업자등록번호
	대표자	전화번호
	주소	
	전자우편(e-mail)	
정보보호 및 개인정보보호 관리체계 인증	심사구분	[]최초심사 []사후심사(차) []갱신심사
	인증범위	
	범위 내 개인정보	
	특례적용 대상 여부	[]대상 []비대상 ※ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의7에 따른 특례 대상자 여부
정보보호 관리체계 인증	심사구분	[]최초심사 []사후심사(차) []갱신심사
	인증범위	
	특례적용 대상 여부	[]대상 []비대상 ※ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의7에 따른 특례 대상자 여부

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 같은 법 시행령 제47조, 「개인정보 보호법」 제32조의2에 따라 위와 같이 인증을 신청합니다.

년 월 일

신청인(대표자)

(서명 또는 인)

00000(심사수행기관명)의 장 귀하

첨부서류	정보보호 및 개인정보보호 관리체계 명세서 1부 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의7에 따른 특례 대상 증빙서류 (해당 시)
------	--

처 리 절 차



210mm×297mm[(백상지(80g/㎡) 또는 종질지(80g/㎡)]

인증심사 일부 생략 신청서

접수번호	접수일시	처리기간
신청인	업체명	사업자등록번호
	대표자	전화번호
	주소	
	전자우편(e-mail)	
ISO/IEC 27001	인증번호 :	인증기관 :
	인증의 범위 :	
	인증유효기간 : . . . ~ . . .	
	최근 인증심사 수행기간 : . . . ~ . . .	
	보완조치 완료일 :	
「정보통신기반 보호법」 제9조에 따른 취약점의 분석·평가	기반시설 지정번호(공문번호) :	
	취약점 분석·평가 수행범위 :	
	취약점 분석·평가 수행기간 : . . . ~ . . .	
	수행주체 :	

「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제20조에 따라 위와 같이 인증 일부 심사 생략을 신청합니다.

년 월 일

신청인(대표자)

(서명 또는 인)

00000(심사수행기관명)의 장 귀하

첨부서류	1. 인증 일부 심사 생략 명세서 1부 2. 인증심사 일부기준 생략을 증명할 수 있는 서류
------	---

210mm×297mm[(백상지(80g/㎡) 또는 중질지(80g/㎡)]

정보보호 및 개인정보보호 관리체계 인증서

1. 인증번호 :
2. 업체명 :
3. 대표자 :
4. 인증의 범위 :
5. 유효기간 :
6. 심사수행기관 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항, 같은 법 시행령 제47조, 「개인정보 보호법」 제32조의2에 따라 위와 같이 정보보호 및 개인정보보호 관리체계를 인증합니다.

년 월 일

한국인터넷진흥원장
또는 인증기관의 장

직인

CERTIFICATE OF Personal information & Information Security Management System

1. Certificate Number :
2. Name of Organization :
3. Name of Representative :
4. Scope of Certification :
5. Period of Validity :
6. Examination Institution :

This is to certify that the abovementioned organization is compliant to the assessment standard for Personal information & Information Security Management System certification in accordance with Article 47, Paragraph 1 of 「Act on Information Network Utilization and Data Protection, etc.」 and Article 47 of the Enforcement Decree of the same Act and in accordance with Article 32-2 of 「Personal Information Protection Act」

Date of Issuance :

서 명 또는 직 인

한국인터넷진흥원장 또는 인증기관의 장 영문

210mm×297mm[백상지 (150g/㎡)]

정보보호 관리체계 인증서

1. 인증번호 :
2. 업체명 :
3. 대표자 :
4. 인증의 범위 :
※ 심사 생략 범위 :
5. 유효기간 :
6. 심사수행기관 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계를 인증합니다.

년 월 일

한국인터넷진흥원장
또는 인증기관의 장

직인

CERTIFICATE OF Information Security Management System

1. Certificate Number :
2. Name of Organization :
3. Name of Representative :
4. Scope of Certification :
 - ※ Scope of omitted certification examination :
5. Period of Validity :
6. Examination Institution :

This is to certify that the abovementioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 of 「Act on Information Network Utilization and Data Protection, etc.」 and Article 47 of the Enforcement Decree of the same Act.

Date of Issuance :

서 명 또는 직 인

한국인터넷진흥원장 또는 인증기관의 장 영문

210mm×297mm[백상지 (150g/㎡)]

인증서 재발급 신청서

접수번호	접수일시	처리기간
신청인	업체명	사업자등록번호
	대표자	전화번호
	주소	
	전자우편(e-mail)	
인증 정보	인증번호	
	인증범위	
재발급 사유		

위와 같이 인증서의 재발급을 신청합니다.

년 월 일

신청인(대표자)

(서명 또는 인)

한국인터넷진흥원 또는 인증기관의 장 귀하

210mm×297mm[(백상지(80g/㎡) 또는 중질지(80g/㎡)]

인증서 변경 신청서

접수번호	접수일시	처리기간
신청인	업체명	사업자등록번호
	대표자	전화번호
	주소	
	전자우편(e-mail)	
인증정보	인증번호	
	인증범위	
변경 내용	변경전	(국문)
		(영문)
	변경후	(국문)
		(영문)
변경사유		

위와 같이 인증서의 변경을 신청합니다.

년 월 일

신청인(대표자)

(서명 또는 인)

한국인터넷진흥원 또는 인증기관의 장 귀하

첨부서류	인증서 내용의 변경이 필요함을 증명할 수 있는 서류
------	------------------------------

210mm×297mm[(백상지(80g/㎡) 또는 중질지(80g/㎡)]

이의신청서

접수번호	접수일시	처리기간
신청인	업체명	사업자등록번호
	대표자	전화번호
	주소	
	전자우편(e-mail)	
통지사항	통지를 받은 날	
	통지된 사항	
이의신청 대상		
이의신청 사유		

위와 같이 이의신청합니다.

년 월 일

신청인(대표자)

(서명 또는 인)

한국인터넷진흥원 또는 인증기관의 장 귀하

첨부서류	이의신청 내용을 확인할 수 있는 증빙 자료
------	-------------------------

210mm×297mm[(백상지(80g/㎡) 또는 중질지(80g/㎡)]

[시행 2024. 3. 15.] [개인정보보호위원회고시 제2024-4호, 2024. 3. 15., 제정]

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다) 제11조의2와 같은 법 시행령(이하 "령"이라 한다) 제13조의2에 따라 개인정보 보호수준 평가를 위한 세부적인 평가 대상, 평가의 절차, 평가단의 구성·운영 방법, 평가 결과의 활용 등 필요한 세부 사항을 정함을 목적으로 한다.

제2조(평가 대상) ① 보호위원회는 매년 평가 대상이 되는 기관의 신설, 통·폐합, 제2항에 따른 신규 및 재지정 등을 반영하여 당해연도 개인정보 보호수준 평가 대상을 확정하여야 한다.

② 영 제13조의2제1항제3호에 따른 평가 대상은 특별법에 의하여 설립된 특수법인과 「고등교육법」 제2조에 따른 학교 중에 다음 각 호의 사항을 종합적으로 고려하여 보호수준 평가가 필요한 기관에 대해 보호위원회가 정할 수 있다.

1. 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보 또는 법 제24조제1항에 따른 고유식별정보를 처리하는 경우
2. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 경우
3. 최근 3년간 개인정보 유출 등 개인정보 침해사고가 2회 이상 발생하였거나, 보호위원회로부터 과징금 또는 과태료 처분 등을 1회 이상 받은 경우
4. 그 밖에 개인정보 처리 및 관리에 있어서 개인정보 침해 우려가 크다고 판단되는 경우

③ 제2항에 따라 지정된 평가 대상은 최초 평가를 위한 준비기간을 고려하여 차년도부터 평가를 실시할 수 있으며, 이 경우 최초 평가를 실시한 연도를 포함하여 3년간 평가를 실시한다.

제3조(평가계획의 수립) ① 보호위원회는 법 제11조의2에 따른 평가를 수행하는 경우 평가 대상, 평가 일정, 평가 기준 및 세부 평가방법, 평가지표 등을 포함하여 평가계획을 수립하여야 한다.

② 보호위원회는 제1항에 따라 매년 평가계획을 수립하여 평가 대상에게 통보하여야 하고, 평가계획을 보호위원회 누리집 등에 공개할 수 있다.

제4조(평가 절차) ① 개인정보 보호수준 평가는 평가계획 수립 및 통보, 평가단 구성, 평가자료 제출, 평가 수행, 평가 결과 통지 등의 절차에 따라 실시한다.

② 보호위원회는 제1항에 따라 평가 대상이 제출한 자료를 기준으로 평가한다. 이 경우 제출된 자료의 사실 여부 또는 추가적 사항의 확인 등을 위해 평가 대상에게 추가 자료의 제출을 요청할 수 있으며, 평가 대상은 관련 자료의 제출 요구에 성실히 응하여야 한다.

- ③ 보호위원회는 제2항에 따른 평가 결과를 차년도 상반기에 발표하며, 각 평가 대상에게 통지하여야 한다.
- ④ 평가 결과의 공개범위는 기관별 등급으로 하며, 평가 결과는 보호위원회 누리집 등에 공개할 수 있다. 다만, 기관별 세부 평가자료 및 점수는 공개하지 않는다.

제5조(평가단 구성 및 운영) ① 보호위원회는 개인정보 보호수준 평가의 전문성·공정성 확보를 위해 평가단을 구성하여 운영할 수 있다.

- ② 평가단은 단장 1명을 포함하여 보호위원회가 위촉하는 개인정보에 관한 경력과 전문지식이 풍부한 전문가로 다음 각호의 경력을 가진 사람 중에서 구성한다.
 - 1. 「고등교육법」제2조에 따른 학교에서 조교수 이상으로 재직하는 자로서 개인정보 보호 관련 경력 3년 이상인 사람
 - 2. 개인정보 보호 또는 정보 보호·보안 분야에서 3년 이상 업무 경력을 갖춘 사람
 - 3. 그 밖에 개인정보 관련 분야에 경력과 전문지식이 풍부하다고 보호위원회가 인정하는 사람
- ③ 평가단원의 임기는 위촉된 날부터 1년으로 하되 연임할 수 있으며, 단장 및 단원은 보호위원회 위원장이 위촉한다.
- ④ 평가단은 평가를 위해 다음 각호의 업무를 수행한다.
 - 1. 평가 대상 제출자료에 대한 검증, 평가 및 적정성 여부 판단
 - 2. 평가 대상 현장검증 및 자문
 - 3. 평가 결과 평정
 - 4. 그 밖에 개인정보 보호수준 평가의 효율적 수행 및 개선을 위한 지원
- ⑤ 평가단원은 업무에 직접 관여하는 등 직접적인 이해관계가 있거나 공정성을 기할 수 없는 현저한 사유가 있는 경우에는 해당 평가 대상의 평가에 관여할 수 없으며 평가단원이 그러한 사유가 있다고 판단하는 때에는 스스로 해당 평가 대상의 평가에서 회피할 수 있다.
- ⑥ 보호위원회는 평가단원이 다음 각호의 하나에 해당할 때는 해촉할 수 있다.
 - 1. 평가와 관련한 법령상 의무를 위반한 때
 - 2. 평가와 관련한 직무를 태만히 하거나 직무수행 능력이 부족하다고 인정될 때
 - 3. 그 밖에 평가단원으로서 품위를 손상하는 행위를 한 때
- ⑦ 보호위원회는 평가단에 대하여 예산의 범위 안에서 수당과 여비, 그 밖에 필요한 경비를 지급할 수 있다.

제6조(평가 결과에 따른 포상 등) ① 보호위원회는 개인정보 보호수준 평가 결과에 따라 선정한 우수기관 또는 소속 직원에 대하여 표창 수여, 포상금 지급 등의 우대조치를 할 수 있다.

- ② 평가 우수기관에 대한 포상금은 예산의 범위 내에서 지급한다.

제7조(평가 결과의 활용 및 지원) ① 보호위원회는 공공기관의 개인정보 보호수준을 향상시키기 위하여 개인정보 보호수준 평가 결과 우수사례 홍보 등에 활용할 수 있다.

- ② 보호위원회는 개인정보 보호수준 평가 결과 미흡기관에 대해 현장 컨설팅 및 실태점검을 실시할 수 있다.
- ③ 보호위원회는 중앙행정기관의 장 또는 지방자치단체의 장에게 소속 기관·단체 등 소관 분야 공공기관에 대해 컨설팅, 교육, 기술지원 및 주기적 점검 등의 필요한 사항을 지원하도록 요청할 수 있다.
- ④ 보호위원회는 개인정보 보호수준 평가 결과가 업무평가 등에 반영될 수 있도록 소관 기관의 장에게 평가 결과를 제공할 수 있다.

제8조(재검토기한) 보호위원회는 이 고시에 대하여 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2024년 1월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2024-4호, 2024.03.15.>

이 고시는 2024년 3월 15일부터 시행한다.

[시행 2024. 4. 3.] [개인정보보호위원회고시 제2024-7호, 2024. 4. 3., 일부개정]
2024. 10. 11 일부개정안 행정예고 내용은 파란색으로 표시

제1장 총칙

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다) 제33조와 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제36조, 제38조에 따른 평가기관의 지정 및 영향평가의 절차 등에 관한 세부기준을 정함을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "개인정보 영향평가(이하 "영향평가"라 한다)"란 법 제33조제1항에 따라 공공기관의 장이 영 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.
2. "대상기관"이란 영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 공공기관을 말한다.
3. "개인정보 영향평가기관(이하 "평가기관"이라 한다)"이란 영 제36조제1항 각 호의 요건을 모두 갖춘 법인으로서 공공기관의 영향평가를 수행하기 위하여 개인정보 보호위원회(이하 "보호위원회"라 한다)가 지정한 기관을 말한다.
4. "대상시스템"이란 영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 정보시스템을 말한다.
5. "개인정보 영향평가 관련 분야 수행실적(이하 "영향평가 관련 분야 수행실적"이라 한다)"이란 영 제36조제1항제1호에 따른 영향평가 업무 또는 이와 유사한 업무, 정보보호 컨설팅 업무 등을 수행한 실적을 말한다.

제2장 개인정보 영향평가기관의 지정

제3조(평가기관 지정절차) ① 영 제36조에 따른 평가기관의 지정절차는 지정신청 공고, 지정신청 서류 접수 및 검토, 현장실사, 종합심사의 순으로 진행된다.

② 보호위원회는 평가기관으로 지정받으려는 자가 지정 신청을 할 수 있도록 관보 등을 통해 15일 이상 지정신청공고를 하여야 한다.

③ 영 제36조제2항에 따라 평가기관으로 지정받으려는 자는 별지 제1호서식의 "개인정보 영향평가기관 지정신청서"와 함께 다음 각 호의 서류를 보호위원회에 제출한다.

1. 영 제36조제2항제1호부터 제3호까지의 규정에 따른 서류
2. 별지 제2호서식의 개인정보 영향평가 수행실적 명세서
3. 별지 제3호서식의 개인정보 영향평가 수행실적물 관리카드
4. 별지 제4호서식의 개인정보 영향평가 수행인력 보유현황
5. 별지 제5호서식의 개인정보 영향평가 수행인력의 경력 및 실적 증명서

6. 별지 제6호서식의 개인정보 영향평가 수행인력 관리카드
 7. 별지 제7호서식의 개인정보 영향평가 수행능력 세부 심사자료
 8. 별지 제8호서식의 개인정보 영향평가 관련 기술자산 보유목록
 9. 별지 제9호서식의 개인정보 영향평가 수행 관련 사무실 및 설비 보유 현황
 10. 영 제36조제1항제1호의 사실을 증명할 수 있는 서류
 11. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(영 제36조제3항 각 호 외의 부분 단서에 해당하는 경우에만 첨부한다)등 그 밖에 평가기관 지정을 위해 필요하다고 판단되는 서류
- ④ 보호위원회는 제3항에 따른 평가기관 지정신청을 받은 경우 지정기준의 적합여부를 심사하기 위하여 **개인정보 영향평가위원회(이하 “영향평가위원회”라 한다)**를 구성·운영한다.
 - ⑤ 보호위원회는 **영향평가위원회**의 심사결과를 검증한 후 평가기관 지정을 확정하고, 별지 제10호서식의 개인정보 영향평가기관 지정서를 교부한다.
 - ⑥ 평가기관의 유효기간은 보호위원회가 평가기관으로 지정한 날로부터 3년으로 한다.
 - ⑦ 평가기관의 유효기간을 연장하고자 하는 자는 유효기간 만료일 3개월 전까지 제3조제3항에 따른 서류를 보호위원회에 제출해야 한다.
 - ⑧ 영 제36조제6항에 따른 신고는 별지 제11호서식의 개인정보 영향평가기관 변경사항 신고서에 따른다.

제4조(지정심사위원회의 구성 및 운영) ① 제3조에 따른 지정심사위원회는 다음 각 호의 자격을 가진 자 중에서 보호위원회가 위촉하는 5인 이상 15인 이내의 위원으로 구성한다.

1. 「고등교육법」제2조제1호·제2호 또는 제5호에 따른 학교나 공인된 연구기관에서 조교수 이상의 직 또는 이에 상당하는 직에 있거나 있었던 자로 개인정보 보호 연구경력이 8년 이상인 사람
 2. 개인정보 보호 관련 업체, 기관 또는 단체(협회, 조합)에서 8년 이상 개인정보 보호 업무에 종사한 사람
 3. 그 밖에 개인정보 보호에 관한 학식과 경험이 풍부한 사람
- ② 지정심사위원회는 영 제36조제1항에 따른 신청한 법인의 자격 및 업무수행능력 등을 검토한다.
 - ③ 지정심사위원회의 위원 임기는 3년으로 하되, 연임할 수 있다.
 - ④ 지정심사위원회의 회의는 필요에 따라 보호위원회가 소집한다.

제4조(영향평가위원회의 구성 및 운영) ① 보호위원회는 다음 각 호의 사항을 심의하기 위하여 영향평가위원회를 구성·운영한다.

1. 영향평가기관 지정·지정 취소에 관한 사항
2. 영향평가제도 연구 및 개선에 관한 사항
3. 영향평가제도 운영을 위한 제반사항 검토 및 품질관리에 관한 사항
4. 영향평가기관의 관리 감독에 관한 사항
5. 그 밖에 영향평가제도 운영과 관련하여 보호위원회가 필요하다고 인정하는 사항

② 영향평가위원회는 다음 각 호의 자격을 가진 자 중에서 보호위원회가 위촉하는 5인 이상 15인 이내의 위원으로 구성한다.

1. 「고등교육법」제2조제1호·제2호 또는 제5호에 따른 학교나 공인된 연구기관에서 조교수 이상의 직 또는 이에 상당하는 직에 있거나 있었던 자로 개인정보 보호 연구경력이 3년 이상인 사람
2. 개인정보 보호 관련 업체, 기관 또는 단체(협회, 조합)에서 3년 이상 개인정보 보호 업무에 종사한 사람
3. 그 밖에 개인정보 보호에 관한 학식과 경험이 풍부한 사람

③ 영향평가위원회의 위원 임기는 2년으로 하되, 연임할 수 있으며, 위원장은 보호위원회 위원장이 위촉한다.

④ 영향평가위원회의 회의는 필요에 따라 보호위원회가 소집한다.

⑤ 영향평가위원회 위원은 영향평가기관과 직접적인 이해관계가 있거나 공정성을 기할 수 없는 현저한 사유가 있는 경우 등에는 해당 대상의 심의에 관여할 수 없으며 위원이 그러한 사유가 있다고 판단하는 때에는 스스로 해당 심의에서 회피할 수 있다.

제5조(영향평가 수행인력 자격) ① 영향평가 수행인력은 다음 각 호와 같이 일반수행인력과 고급수행인력으로 구분할 수 있다.

1. 일반수행인력의 자격은 다음 각 목과 같다.

가. 별표1에 따른 전문인력의 자격을 갖춘 사람

나. 한국CPO포럼이 시행하는 개인정보관리사 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야 수행실적이 있는 사람

2. 고급수행인력의 자격은 다음 각 목과 같다.

가. 제1호의 일반수행인력의 자격을 갖춘 후 5년 이상의 영향평가 관련 분야 수행실적이 있는 사람

나. 관련 분야 박사학위를 취득한 후 3년 이상의 영향평가 관련 분야 수행실적이 있는 사람
다. 「국가기술자격법 시행규칙」 제3조에 따른 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사 자격을 취득한 후 3년 이상의 영향평가 관련 분야 수행실적이 있는 사람

② 제1항에 따른 영향평가 수행인력은 제6조제2항에 따른 전문교육을 이수하고 제6조제3항에 따른 전문인력 인증서를 받은 경우에 영향평가를 수행할 수 있다.

제6조(영향평가 전문교육의 운영 및 실시) ① 보호위원회는 영향평가 전문인력 양성을 위한 세부 교육계획 수립 및 교육 운영 등의 업무를 효율적으로 추진하기 위하여 한국인터넷진흥원을 전문교육기관으로 지정한다.

② 전문교육기관의 장은 영향평가 전문인력 양성을 위한 세부 교육계획을 수립하여 전문교육 등을 실시하여야 한다.

③ 전문교육기관의 장은 전문교육 이수자에 대한 평가를 실시하고 그 결과에 따라 개인정보 영향평가 전문인력 인증서를 교부한다. 이 경우 인증서의 유효기간은 인증서를 교부받은 날로부터 3년으로 한다.

④ 전문교육기관의 장은 제3항에 따른 전문인력 인증서를 교부받은 날로부터 매 2년이 경과한 자에 대해 계속교육을 실시하여야 하며, 인증서를 교부받은 자는 자격 유지를 위해 인증서 유효기간 만료 전까지 계속교육을 이수하여야 한다.

⑤ 전문교육기관의 장은 제4항의 요건을 충족한 자에 한하여 제3항의 개인정보 영향평가 전문인력 인증서를 갱신하여 교부하고, 인증서의 유효기간을 인증서를 교부받은 날로부터 3년간 연장한다.

제7조(영향평가 기관 지정기준) ① 평가기관의 영향평가 업무수행 요건·능력 심사에 관한 세부 기준은 별표 2와 같다.

② 보호위원회는 영향평가 수행능력심사 세부평가기준에 따른 심사결과가 총점 75점 이상인 경우 신청한 법인을 평가기관으로 지정한다.

③ 평가기관의 유효기간을 연장하고자 하는 자에 대한 세부평가기준은 별표 3과 같다.

제8조(사후관리) ① 보호위원회는 평가기관이 영 제36조제1항의 평가기관 지정요건을 충족하는 지 여부와 영 제36조제6항에 따른 변경사항을 확인하기 위하여 현장실사, 관련 자료제출 요구 등을 할 수 있다.

② 평가기관은 다음 각 호를 포함한 보호대책을 별표 4와 같이 수립·시행하여야 하며, 보호위원회는 그에 대한 준수여부를 점검할 수 있다.

1. 영향평가 수행구역 및 설비에 대한 보호대책
2. 영향평가 수행 인력에 대한 보호대책
3. 문서 및 전산자료에 대한 보호대책
4. 일반 관리적 보호대책

③ 보호위원회는 평가기관이 법 제33조제7항제3호부터 제5호까지의 규정에 해당하는 경우에는 지정취소 이전에 시정 및 보완을 요구할 수 있다.

제3장 개인정보 영향평가의 절차 등

제9조(평가절차) 대상기관은 다음 각 호와 같이 사전 준비, 영향평가 수행, 이행 단계로 영향평가를 수행한다.

1. 사전 준비 단계에서는 영향평가 사업계획을 수립하여 예산을 확보하고 평가기관을 선정한다.

2. 영향평가 수행 단계에서는 평가기관이 개인정보 침해요인을 분석하고 개선계획을 수립하여 영향평가서를 작성한다.
3. 이행 단계에서는 영향평가서의 침해요인에 대한 개선계획이 반영되는 가를 점검한다.

제9조의2(영향평가 수행) ① 개인정보파일을 구축·운용 또는 변경하고자 하는 공공기관의 장은 별표 5의 필요한 사항이 반영될 수 있도록 설계완료 전에 영향평가를 수행하여야 한다.

② 공공기관의 장이 개인정보파일을 구축·운용 또는 변경하고자 할 때에는 제1항의 영향평가 결과를 반영한 조치를 이행 **하여야 한다**.

제9조의3(영향평가 개선계획 반영여부의 확인) 공공기관의 장은 개인정보 영향평가 수행 후, 영향평가 개선계획의 반영여부를 정보시스템 감리 시 확인하여야 한다. 단, 감리를 수행하지 않은 경우에는 정보시스템 테스트단계에서 영향평가 개선계획의 반영여부를 확인하여야 한다.

제10조(평가영역 및 평가분야) 영 제38조제1항의 영향평가기준에 따른 평가영역은 별표 5와 같다. 다만, 대상기관이 1년 이내에 다른 정보시스템의 영향평가를 받은 경우에는 대상기관의 개인정보 보호 관리체계에 대한 평가는 생략할 수 있다.

제11조(평가항목) ① 평가기관은 별표 5에 따라 적합한 평가항목을 선정하여 영향평가를 수행하여야 한다. 다만, 대상기관이 1년 이내에 이미 평가받은 항목은 그 변경이 없는 때에는 평가항목에서 제외된다.

② 별표 5에 명시되지 않은 특화된 **정보기술(IT)**을 적용하는 경우에는 해당 기술이 개인정보 보호에 미치는 영향에 대한 평가항목을 개발하여 영향평가 시 반영하여야 한다.

제12조(영향평가서의 제출 및 영향평가 개선사항 이행) ① 영 제38조제2항에 따라 영향평가서를 제출받은 대상기관의 장은 2개월 이내에 평가결과에 대한 내부승인 절차를 거쳐 영향평가서 및 그 요약본(요약본을 공개하려는 경우 해당 요약본을 포함한다)을 보호위원회에 제출하여야 한다.

② 영 제38조제2항에 따른 영향평가 결과 개선사항으로 지적받은 사항이 있는 경우에는 지적된 부분에 대한 이행결과 및 계획 등을 별지 제13호서식에 따라 제1항의 기간 내에 보호위원회에 제출하여야 한다. 다만, 동 기간 경과 후 조치한 사항에 대해서는 이행결과를 부득이한 사유가 없는 한 1년 이내에 보호위원회에 제출하여야 한다. (**제14조에서 이동**)

제12조의2(영향평가서 요약본의 공개) ① 공공기관의 장은 영 제38조제3항에 따라 개인정보 영향평가서를 요약한 내용을 공개하는 경우 공공기관의 정보공개에 관한 법률 등에 따라 해당 기관의 홈페이지에 공개할 수 있다. 이 경우 보호위원회는 공공기관의 장이 공개한 영향평가 요약본을 보호위원회가 구축하는 인터넷 사이트에

공개할 수 있다.

- ② 보호위원회는 공공기관의 영향평가 요약본 공개 실태에 대해 점검할 수 있으며, 점검 결과 필요한 경우 공공기관에 개선을 요청할 수 있다.

제13조(영향평가 수행안내서) 보호위원회는 영향평가에 필요한 세부기준 및 절차, 평가항목 등을 구체화하는 "영향평가 수행안내서"를 마련하여 제공할 수 있다.

제14조(재검토 기한) 보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2023년 10월 16일을 기준으로 매 3년이 되는 시점(매 3년째의 10월 15일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2024-7호, 2024.04.03.>

이 고시는 고시한 날부터 시행한다.

전문인력의 자격기준(제5조 관련)

1. 「국가기술자격법」에 따른 정보통신 직무분야의 국가기술자격 중 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 전자계산기조직응용기사, 정보처리기사, 정보보안기사 또는 정보통신기사 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
2. 「전자정부법」 제60조에 따른 감리원(ISA) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
3. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 공인정보시스템감사사(CISA) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
4. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 공인정보시스템보호전문가(CISSP) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
5. 「개인정보 보호법」 제32조의2제7항에 따른 심사원 자격을 취득한 사람

비고

"개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람"이란 공공기관, 법인 및 단체 등의 임직원으로 개인정보 보호를 위한 공통기반기술(암호기술, 인증기술 등을 말한다), 시스템·네트워크 보호(시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등을 말한다) 또는 응용서비스 보호(전자거래 보호, 응용서비스 보호, 정보보호 표준화 등을 말한다)에 해당하는 분야에서 계획, 분석, 설계, 개발, 운영, 유지·보수, 감리, 컨설팅 또는 연구·개발 업무 등을 수행한 경력이 있는 사람을 말한다.

개인정보 영향평가 업무수행 요건·능력 심사에 관한 세부기준

(제7조 관련)

가. 업무수행 요건 심사 기준(필수)

평가항목	세부평가항목	세부 평가 기준
수행실적	영향평가 및 관련 분야 수행실적	· 최근 5년간 영향평가 업무 및 관련 업무 수행의 대가로 받은 금액의 합계액이 2억원 이상
인력	전문인력 고용	· 전문인력 10명 이상 상시 고용
사무실 및 설비	사무실 및 설비 확보	· 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실 · 기록 및 자료의 안전한 관리를 위한 설비

나. 업무수행 능력 심사 기준

(제1쪽)

구분	평가항목	세부평가항목	배점	평가지표	세부 평가 기준
I. 정량 평가 (60)	1. 경험 (25)	최근 5년간 영향평가 관련 분야 수행실적	15	계약금액 총액	· 5억원 이상: 배점의 100% · 5억원 미만: 배점의 $\chi\%$ ※ $\chi = (\text{계약금액총액}/5\text{억원}) \times 100$
		최근 2년간 계약금액 1천만원 이상의 영향평가 관련 분야 수행실적	15	수행건수	· 5건 이상: 배점의 100% · 5건 미만: 배점의 $\chi\%$ ※ $\chi = (\text{수행건수}/5\text{건}) \times 100$
	2. 전문성 (25)	고급수행인력의 수	15	인원수	· 인원수 \times 1점(최대 15점)
		전담조직 유무	5	비율	· 전담조직 보유 : 배점의 100% · 전담조직 없음 : 0점
	3. 신뢰도 (10)	신용평가등급	10	등급	· 신용평가 등급에 근거하여 평가 ※ 개인정보 영향평가에 관한 고시 별표3의 붙임기준
	II. 정성 평가 (40)	영향평가 수행실적의 질적 평가	20	비계량	· 영향평가 품질제고 활동 · 영향평가 수행방법의 우수성 · 영향평가 수행 대상기관
		영향평가 수행인력의 자질 및 경험	10	비계량	※ 신청서류, 현장실사 등을 통해 평가

II. 정성 평가 (40)	영향평가 수행역량 (40)	지정신청법인의 자체 개인정보영향평가대책	10	비계량	<ul style="list-style-type: none">영향평가 수행구역 및 설비에 대한 보호대책영향평가 수행 인력에 대한 보호대책문서 및 전산자료에 대한 보호대책일반 관리직 보호대책
III. 기타		「벤처기업육성에 관한 특별 조치법」 제25조에 따라 벤 처기업으로 확인을 받은 기업	가점	확인여부	※ 벤처 확인기업: 가점 5점
		지방소재(수도권제외) 기업	가점	확인여부	※ 본사 위치가 수도권을 제외한 지방에 위치하는 경우 : 가점 5점
		최근 3년간 조달법령에 따라 부정당업자로 지정되어 입찰 참가 제한을 받은 기간	감점	입찰참가 제한월수	※ 제한월수 1월당: 감점 0.5점
<p>비 고</p> <p>1. 위 표 각 세부 평가항목별 점수는 소수점 이하 둘째 자리에서 반올림한다.</p> <p>2. 세부 평가기준 중 신뢰도 항목은 기업신용평가서 제출로 대체할 수 있으며 이에 대한 배점기준은 [붙임] 신용평가등급에 의한 평가기준에 따른다.</p> <p>3. ‘최근’의 기산일은 지정공고일자를 기준으로 한다.</p>					

【별표 3】

개인정보 영향평가기관 갱신 세부평가기준 (제7조 관련)

가. 업무수행 요건 심사 기준(필수)

평가항목	세부평가항목	세부 평가 기준
수행실적	영향평가 및 관련 분야 수행실적	· 최근 5년간 영향평가 업무 및 관련 업무 수행의 대가로 받은 금액의 합계액이 2억원 이상
인력	전문인력 고용	· 전문인력 10명 이상 상시 고용
사무실 및 설비	사무실 및 설비 확보	· 인원 확인 및 출입 통제를 위한 설비를 갖춘 사무실 · 기록 및 자료의 안전한 관리를 위한 설비

나. 업무수행 능력 심사 기준

(제1쪽)

구분	평가항목	세부평가항목	배점	평가지표	세부 평가 기준
I. 정량 평가 (60)	1.경험 (30)	최근 2년간 영향평가 수행실적	10	계약금액 총액	· 5억원 이상 : 배점의 100% · 5억원 ~ 2억원 : 배점의 $\chi\%$
		최근 2년간 영향평가 수행건수	10	수행건수	· 5건 이상: 배점의 100% · 5건 미만: 배점의 $\chi\%$ ※ $\chi = (\text{수행건수}/5\text{건}) \times 100$
		최근 2년간 영향평가 관련 분야 수행실적	5	계약금액 총액	· 5억원 이상 : 배점의 100% · 5억원 ~ 2억원 : 배점의 $\chi\%$ · 2억원 미만 : 자격미달(시행령 제36조 제1항 제1호) ※ $\chi = (\text{계약금액총액}/5\text{억원}) \times 100$
			5	수행건수	· 5건 이상: 배점의 100% · 5건 미만: 배점의 $\chi\%$ ※ $\chi = (\text{수행건수}/5\text{건}) \times 100$
	2.전문성 (20)	고급수행인력의 수	15	인원수	· 인원수×1점(최대 15점)
		전담조직 유무	5	비율	· 전담조직 보유 : 배점의 100% · 전담조직 없음 : 0점
	3. 신뢰도 (10)	신용평가등급	10	등급	· 신용평가 등급에 근거하여 평가 ※ 개인정보 영향평가에 관한 고시 별표3의 붙임기준
II. 정성 평가 (40)	1.영향 평가 수행 역량 (40)	영향평가 수행실적의 질적 평가	25	비계량	· 영향평가 품질제고 활동 · 영향평가 수행방법의 우수성 및 개선도 · 영향평가 수행 대상기관
		영향평가 수행인력의 자질 및 경험(인터뷰)	10	비계량	※ 신청서류, 현장실사 등을 통해 평가

II. 정성 평가 (40)	1.영향 평가 수행 역량 (40)	지정신청법인의 자체 개인정보 영향평가 대책	5	비계량	<ul style="list-style-type: none">영향평가 수행구역 및 설비에 대한 보호대책영향평가 수행 인력에 대한 보호대책문서 및 전산자료에 대한 보호대책일반 관리직 보호대책
III. 기타		「벤처기업육성에 관한 특별조치법」 제25조에 따라 벤처기업으로 확인을 받은 기업	가점	확인여부	※ 벤처 확인기업: 가점 5점
		지방소재 공공기관에 대한 영향평가 수행 건수	가점	확인여부	※ 수행 건수 당 : 가점 1점
		무자격자를 활용한 영향평가 수행 건수 (고시 제5조 위반 건수)	감점	확인여부	※ 수행 건수 당 : 감점 1점
		최근 3년간 조달법령에 따라 부정당업자로 지정되어 입찰참가 제한을 받은 기간	감점	입찰참가 제한월수	※ 제한월수 1월당: 감점 0.5점
<div>비 고</div> <div>1. 위 표 각 세부 평가항목별 점수는 소수점 이하 둘째 자리에서 반올림한다.</div> <div>2. 세부 평가기준 중 신뢰도 항목은 기업신용평가서 제출로 대체할 수 있으며 이에 대한 배점기준 은 [붙임] 신용평가등급에 의한 평가기준에 따른다.</div> <div>3. ‘최근’의 기산일은 지정공고일자를 기준으로 한다.</div>					

신용평가등급에 의한 평가기준

회사채에 대한 신용평가등급	기업어음에 대한 신용평가등급	기업신용평가 등급	평점(점)
			10점
AAA	—	AAA (회사채에 대한 신용평가등급 AAA에 준하는 등급)	10.0
AA+, AA0, AA-	A1	AA+, AA0, AA- (회사채에 대한 신용평가등급 AA+, AA0, AA-에 준하는 등급)	
A+	A2+	A+ (회사채에 대한 신용평가등급 A+에 준하는 등급)	
A0	A20	A0 (회사채에 대한 신용평가등급 A0에 준하는 등급)	
A-	A2-	A- (회사채에 대한 신용평가등급 A-에 준하는 등급)	
BBB+	A3+	BBB+ (회사채에 대한 신용평가등급 BBB+에 준하는 등급)	8.0
BBB0	A30	BBB0 (회사채에 대한 신용평가등급 BBB0에 준하는 등급)	
BBB-	A3-	BBB- (회사채에 대한 신용평가등급 BBB-에 준하는 등급)	
BB+, BB0	B+	BB+, BB0 (회사채에 대한 신용평가등급 BB+, BB0에 준하는 등급)	7.0
BB-	B0	BB- (회사채에 대한 신용평가등급 BB-에 준하는 등급)	
B+, B0, B-	B-	B+, B0, B- (회사채에 대한 신용평가등급 B+, B0, B-에 준하는 등급)	6.0
CCC+ 이하	C 이하	CCC+ 이하 (회사채에 대한 신용평가등급 CCC+에 준하는 등급)	3.0

개인정보 영향평가기관 보호대책의 주요 내용 (제8조 관련)

항 목	주 요 내 용
I. 영향평가 수행구역 및 설비에 대한 보호대책	1. 영향평가를 수행하는 구역을 지정하여야 한다. 이 구역은 해당 영향평가 수행인력이 아닌 자의 출입이 제한되어야 한다. 2. 영향평가 분석자료를 처리·전송·저장하는 정보통신망에 대하여 위험분석에 따른 통제대책을 강구하여야 한다. 이 경우 노트북 컴퓨터, 그 밖에 휴대용 정보처리 기기에 대한 통제대책을 포함하여야 한다.
II. 영향평가 수행인력에 대한 보호대책	3. 영향평가 수행인력이 관계법령에 따르는 비밀유지의무를 포함한 제반의무를 숙지하고 이의 준수를 확인하는 내용의 서약서를 작성하는 지침과 절차를 마련하여야 한다. 4. 영향평가 수행인력을 채용할 때의 적격 심사와 퇴직할 때의 퇴직자 관리를 위한 지침과 절차를 마련하여야 한다. 5. 영향평가 수행인력이 평가기관의 보안대책을 위반하는 경우의 제재 및 처리에 관한 내부규정을 마련하여야 한다. 6. 영향평가 수행인력을 포함한 임직원이 정기적으로 업체 내부 및 외부의 개인정보 영향평가 교육을 받을 수 있도록 하여야 한다.
III. 문서 및 전산자료에 대한 보호대책	7. 영향평가 분석자료(부수자료를 포함한다)를 보호하기 위하여 법 제12조의 표준개인정보 보호지침에 따른 보안대책을 마련하여야 한다. 8. 영향평가 수행인력이 아닌 자는 영향평가 분석자료에 접근·열람하거나 편집·반출·폐기하지 못하도록 통제대책을 강구하여야 한다. 9. 정보통신망을 통하여 처리·전송·저장하는 영향평가 분석자료에 대하여 위험분석에 따른 통제대책을 강구하여야 한다. 10. 서면, 도면, 마이크로필름·전산출력물 등 출력물 형태의 영향평가 분석자료에 대한 보관·복사·배포·폐기 등에 관한 통제대책을 강구하여야 한다.
IV. 일반 관리 대책	11. 영향평가에 관한 평가기관의 기본방침을 대표자가 서면으로 공표하고 영향평가 수행인력을 포함한 임직원이 이를 숙지하여야 한다. 12. 영향평가업무에 대한 위험분석 및 통제대책의 관리·운영실태를 주기적으로 점검·평가하여야 한다.

개인정보 영향평가의 평가영역 및 평가분야 (제9조~제11조 관련)

(제1쪽)

평가 영역	평가 분야	세부 분야
I. 대상기관 개인정보보 호 관리체계	1. 개인정보 보호 조직	개인정보보호책임자의 지정
		개인정보보호책임자 역할수행
	2. 개인정보 보호 계획	내부관리계획 수립
		개인정보보호 연간계획 수립
	3. 개인정보 침해대응	침해사고 신고 방법 안내
		유출사고 대응
	4. 정보주체권리보장	정보주체 권리보장 절차 수립
		정보주체 권리보장 방법 안내
II. 대상시스템 의 개인정보보 호 관리체계	5. 개인정보취급자 관리	개인정보취급자 지정
		개인정보취급자 관리·감독
	6. 개인정보파일 관리	개인정보파일대장 관리
		개인정보파일 등록
	7. 개인정보처리방침	개인정보처리방침의 공개
		개인정보처리방침의 작성
III. 개인정보처리 단계별 보호 조치	8. 수집	개인정보 수집의 적합성
		동의 받는 방법의 적절성
	9. 보유	보유기간 산정
	10.이용·제공	개인정보 제공의 적합성
		목적 외 이용·제공 제한
		제공시 안전성 확보
	11. 위탁	위탁사실 공개
		위탁 계약
		수탁사 관리·감독
	12. 파기	파기 계획 수립
		분리보관 계획 수립
		파기대장 작성

IV. 대상시스템의 기술적 보호 조치	13. 접근권한 관리	계정 관리
		인증 관리
		권한 관리
	14. 접근통제	접근통제 조치
		인터넷 홈페이지 보호조치
		업무용 모바일기기 보호조치
	15. 개인정보의 암호화	저장시 암호화
		전송시 암호화
	16. 접속기록의 보관 및 점검	접속기록 보관
		접속기록 점검
		접속기록 보관 및 백업
	17. 악성프로그램 등 방지	백신 설치 및 운영
		보안업데이트 적용
	18. 물리적 접근방지	출입통제 절차 수립
		반출·입 통제 절차 수립
	19. 개인정보의 파기	안전한 파기
	20. 기타 기술적 보호조치	개발 환경 통제
		개인정보처리화면 보안
		출력시 보호조치
	21. 개인정보처리구역보호	보호구역지정
V. 특정 IT기술 활용시 개인정보 보호	22. 고정형 영상정보 처리기기	고정형 영상정보 처리기기 설치 운영계획 수립
		고정형 영상정보 처리기기설치시 의견수렴
		고정형 영상정보 처리기기 설치 안내
		고정형 영상정보 처리기기 사용 제한
		고정형 영상정보 처리기기 설치 및 관리에 대한 위탁
	23. RFID	RFID 이용자 안내
		RFID 태그부착 및 제거
	24. 생체인식정보	원본정보 보관시 보호조치
	25. 위치정보	개인위치정보 수집 동의
		개인위치정보 제공시 안내사항
	26. 가명정보	가명정보의 처리
		가명정보의 안전조치의무 등
	27. 이동형 영상정보 처리기기	영상정보 촬영 및 안내
		영상정보 촬영 사용제한
		영상정보 촬영 및 관리에 대한 위탁
	28. 자동화된 결정	자동화된 결정에 대한 정보주체의 권리 등

개인정보 영향평가기관 지정신청서

접수번호	접수일	처리기간 2개월
신청인	법인명 및 대표자 성명	법인 설립일
	소재지(주소)	전화번호

개인정보 영향평가 수행인력의 수

명

「개인정보 보호법」 제33조제2항 및 「개인정보 보호법 시행령」 제36조제2항에 따라 개인정보 영향평가기관 지정을 위와 같이 신청합니다.

년 월 일

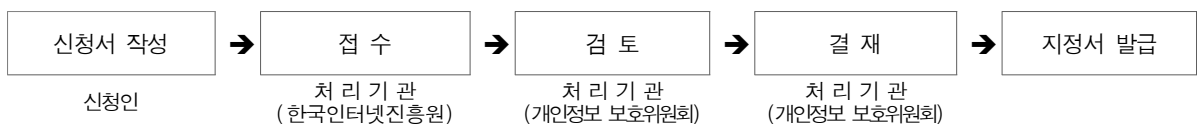
신청인

(서명 또는 인)

개인정보 보호위원회 귀하

첨부서류	<p>1. 「개인정보 보호법 시행령」 제36조제2항제1호 및 제3호의 규정에 따른 서류</p> <p>2. 「개인정보 보호법 시행령」 제36조제2항제4호에 따른 다음의 서류</p> <p>가. 「개인정보 영향평가에 관한 고시」 별지 제2호서식의 개인정보 영향평가 수행실적 명세서</p> <p>나. 「개인정보 영향평가에 관한 고시」 별지 제3호서식의 개인정보 영향평가 수행실적물 관리카드</p> <p>다. 「개인정보 영향평가에 관한 고시」 별지 제4호서식의 개인정보 영향평가 수행인력 보유현황</p> <p>라. 「개인정보 영향평가에 관한 고시」 별지 제5호서식의 개인정보 영향평가 수행인력의 경력 및 실적 증명서</p> <p>마. 「개인정보 영향평가에 관한 고시」 별지 제6호서식의 개인정보 영향평가 수행인력 관리카드</p> <p>바. 「개인정보 영향평가에 관한 고시」 별지 제7호서식의 개인정보 영향평가 수행능력 세부 심사자료</p> <p>사. 「개인정보 영향평가에 관한 고시」 별지 제8호서식의 개인정보 영향평가 관련 기술자산 보유목록</p> <p>아. 「개인정보 영향평가에 관한 고시」 별지 제9호서식의 개인정보 영향평가 수행관련 사무실 및 설비 보유 현황</p> <p>자. 「개인정보 보호법 시행령」 제36조제1항제1호의 사실을 증명할 수 있는 서류</p> <p>차. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(「개인정보보호법 시행령」 제36조제3항 각 호 외의 부분 단서에 해당하는 경우에만 첨부합니다)</p>
------	---

처리절차



210mm×297mm[백상지(80g/㎡) 또는 중질지(80g/㎡)]

개인정보 영향평가 관련 분야 수행실적 명세서

(제1쪽)

업체명						
기간						
수행실적 총계		외 건 (총 천원)				
일련 번호	프로젝트명 (대상기관 (기업)명)	수행기간 (총참여 M/M)	과제책임자	금액 (천원)	참여인력 (개인별 참여율 (M/M), 전문참여분야)	비고 (기반시설 여부, 영향평가 지분 등)
비고 1. 영향평가 관련 분야 수행실적은 개인정보 영향평가 수행실적, 정보보호컨설팅 수행실적, 정보시스템 및 정보보호시스템 구축실적 중 정보보호컨설팅 비율(별도 금액대비 %로 표기), 감리수행실적 중 정보보호컨설팅 비율(별도 금액대비 %로 표기) 등을 말한다. 2. 영향평가 관련 분야 수행실적 명세서는 영향평가 관련 분야를 수행하였던 대상기관에서 작성하되 부득이한 경우 대상기관과의 계약서, 사업완료보고서, 납품증명서, 준공조서 등으로 대체할 수 있다. 3. 영향평가 관련 분야 수행실적 세부사항은 영향평가 관련 분야 수행실적을 간략히 확인할 수 있도록 금액규모를 구분하여 영향평가 수행실적, 정보보호컨설팅 수행건수 및 금액(또는 정보시스템 및 정보보호시스템 구축실적 중 정보보호컨설팅 건수 및 금액비율, 감리수행실적 중 정보보호컨설팅 건수 및 금액 비율)을 표기한다.						

210mm×297mm[일반용지 60g/㎡(재활용품)]

영향평가 관련 분야 수행실적 세부사항						
영향평가 실적 금액규모	영향평가 관련 분야 수행건수 (합계)	영향평가 관련 분야 수행금액 (합계)	영향평가 수행건수	영향평가 수행금액	영향평가 건수비율	영향평가 금액비율
1억원 이상						
5천만원 이상						
3천만원 이상						
1천만원 이상						
계/평균비율						
<p>비고</p> <p>1. 영향평가 관련 분야 수행실적은 개인정보 영향평가 수행실적, 정보보호컨설팅 수행실적, 정보시스템 및 정보보호시스템 구축실적 중 정보보호컨설팅 비율(별도 금액대비 %로 표기), 감리수행실적 중 정보보호컨설팅 비율(별도 금액대비 %로 표기) 등을 말한다.</p> <p>2. 영향평가 관련 분야 수행실적 명세서는 영향평가 관련 분야를 수행하였던 대상기관에서 작성하되 부득이한 경우 대상기관과의 계약서, 사업완료보고서, 납품증명서, 준공조서 등으로 대체할 수 있다.</p> <p>3. 영향평가 관련 분야 수행실적 세부사항은 영향평가 관련 분야 수행실적을 간략히 확인할 수 있도록 금액규모를 구분하여 영향평가 수행실적, 정보보호컨설팅 수행건수 및 금액(또는 정보시스템 및 정보보호시스템 구축실적 중 정보보호컨설팅 건수 및 금액비율, 감리수행실적 중 정보보호컨설팅 건수 및 금액 비율)을 표기한다.</p>						

210mm×297mm[일반용지 60g/㎡(재활용품)]

[illegible]

210mm×297mm[일반용지60g/㎡(재활용품)]

개인정보 영향평가 수행인력 보유현황

[illegible]

210mm×297mm[일반용지 60g/㎡(재활용품)]

개인정보 영향평가 수행인력의 경력 및 실적 증명서

※ 이 서식은 「개인정보 보호법」 제33조 및 「개인정보 보호법 시행령」 제36조에 따른 개인정보 영향 평가기관 지정심사에 활용됨

인적 사항	성명 (한자)		생년월일		
	주소				
경력 사항	근무부서	근무기간	직위(직급)	담당업무 (구체적으로 기재)	
실적 사항	프로젝트명	수행기간	대상기관명	담당자	비고
				전화번호	

본 증명서의 기재 사항에 일체 허위사실이 없음을 확인하오며 허위 사실 기재로 인한 불이익에는 이의를 제기하지 않겠습니다.

년 월 일

신청인 (서명 또는 인)

개인정보 보호위원회 귀하

개인정보 영향평가 수행인력 관리카드

(제1쪽)

법인명					
성명		생년월일			
소속부서명					
주소					
입사일		인력등재일			
퇴사일		인력삭제일			
인력구분 : 일반 / 고급		등급 취득일 :		등급 변경기록 :	
학력 및 이력 사항	기관명(학교명)	기 간	소 속 부 서 (직위, 직책)	자 격 명 (취득일)	비고

210mm×297mm[일반용지 60g/㎡(재활용품)]

개인정보 영향평가 수행능력 세부 심사자료

1. 총매출액 대비 개인정보 영향평가 관련 분야 매출액의 비율

- (1) 지정신청직전 결산회기의 총매출액: 천원
- (2) 지정신청직전 결산회기의 개인정보영향평가 관련 분야의 매출액: 천원
- (3) 총매출액 대비 개인정보 영향평가 관련 분야 매출액의 비율: %

II. 부채비율 및 자기자본이익율

- (1) 부채비율 = (부채총계 / 자본총계) × 100 = %
- (2) 자기자본이익율 = (당기순이익 / 평균자기자본) × 100 = %

III. 기 타

- (1) 「벤처기업육성에 관한 특별조치법」에 따른 벤처기업 확인 여부 (○ , ×)
- (2) 조달관계법령에 따른 부정당업자 지정 경험 여부 (○ , ×)

비 고

1. Ⅰ항, Ⅱ항은 공인회계사 또는 지정신청업체 회계담당자가 서명날인한 계산내역을 첨부한다
(개인정보 영향평가 관련 분야 매출액을 정확하게 확정할 수 없는 경우에는 개산한 금액으로 한다).

210mm×297mm[일반용지60g/㎡(재활용품)]

[illegible]

210mm×297mm[일반용지60g/㎡(재활용품)]

개인정보 영향평가 수행 관련 사무실 및 설비 보유 현황

※ 아래의 작성방법을 읽고 작성하시기 바랍니다.

법인명 및 대표자 성명	
소재지(주소)	

① 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실

[] 있음 [] 없음

② 신원 확인 및 출입 통제 설비

명 칭	설비 등의 세부사항	수 량	비고

③ 기록 및 자료의 안전관리 설비

명 칭	설비 등의 세부사항	수 량	비 고

작성 방법

①의 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실이 있는 경우에는 '있음'란에 [√] 표시를 하고, 없는 경우에는 '없음'란에 [√] 표시를 합니다.

210mm×297mm[일반용지 60g/㎡(재활용품)]

제 호

개인정보 영향평가기관 지정서

1. 대 표 자:
2. 생년월일 또는 사업자등록번호:
3. 법 인 명:
4. 소재지(주소):
5. 전화번호:
6. 지정요건:

「개인정보 보호법」 제33조제2항과 같은 법 시행령 제36조제4항에 따라 위의 법인을 개인정보 영향평가기관으로 지정하였으므로 개인정보 영향평가기관 지정서를 발급합니다.

년 월 일

개인정보 보호위원회

직인

개인정보 영향평가기관 변경사항 신고서

접수번호	접수일자		처리기간 7일
신고인	법인명		
	대표자명	생년월일	
	소재지(주소) (전화번호 :)		
변경일			
구분	종 전	변 경	
수행 인력			
사무실 및 설비			
평가 기관 양도·양수 또는 합병 등	종 전 법인	법인명	
		대표자명	생년월일
		주소 (전화번호 :)	
	변 경 법인	법인명	
		대표자명	생년월일
		주소 (전화번호 :)	
법인명·창·주소·전화번호 및 대표자 변경			

「개인정보 보호법」 시행령 제36조제6항에 따라 평가기관의 변경사항을 위와 같이 신고합니다.

년 월 일
신고인 대표 (서명 또는 인)

개인정보 보호위원회 귀하

첨부서류	1. 양도·양수·합병 등의 경우 양도·양수 또는 합병 계약서 등 사본 1부 2. 그 밖의 변경사항 증명서류 각 1부
------	---

유의사항

위 변경사항과 관련하여 자세한 내용은 별지로 작성하거나 관련 서류를 첨부하여 제출할 수 있습니다.

210mm×297mm[일반용지 60g/㎡(재활용품)]

개인정보 영향평가서 개요						
공공기관 명						
평가대상시스템 개요	시스템명				추진 일정	
	추진개요 및 목적					
	추진성격	대상여부			추진예산	
		추진주체				
		추진근거			비고	
주요내용						
개인 정보 파일 개요	개인정보 수집 목적					
	평가대상 파일	파일명	정보주체수	파일 및 범위 설명		
				
주요 개인정보 수집 현황	○ 총 ()개 항목 : - 필수 수집 : - 선택 수집 :					
영향 평가 항목	주요 평가항목 변경 내역 (수행안내서 지표 활용 내역 기술)	구 분	주요내용			
		지표추가 항목	-			
		지표삭제 항목	-			
평가 결과 및 개선 계획	평가결과 및 개선사항	주요 내용	○			
		침해요인 도출건수	개선대책 도출건수	개선계획 수립건수	조치완료 건수	조치예정 건수
		건	건	건	건	건
	주요개선 계획 및 일정	○				
		○				
		○				
평가기관			평가기간			
			평가예산			

210mm×297mm[일반용지60g/㎡(재활용품)]

[illegible]

210mm×297mm[일반용지60g/m²(재활용품)]

2024. 9. 30 일부개정안 제정(안) 행정예고

제1장 총 칙

제1조(목적) 이 고시는 「개인정보 보호법」(이하 “법”이라 한다) 제35조의2부터 제35조의4 및 「개인정보 보호법 시행령」(이하 “영”이라 한다) 제42조의3, 제42조의5부터 제42조의13에 따른 전송 요구의 방법, 전송 방식, 개인정보관리 전문기관 지정 및 개인정보 전송 지원 플랫폼 등록 등에 관한 사항을 정하는 것을 목적으로 한다.

제2조(정의) 이 고시에서 사용하는 용어의 뜻은 다음과 같다.

1. “정보전송자”란 법 제35조의2제1항 및 제2항, 영 제42조의2에 따라 정보주체로부터 전송 요구받은 개인정보를 정보주체 본인 또는 제3자에게 전송하는 자를 말한다.
2. “일반수신자”란 법 제35조의2제2항제2호 및 영 제42조의3제1항에 따른 요건을 충족하는 자로서 고유의 업무를 수행하는 과정에서 수집한 정보의 진위 여부 등을 확인하기 위해 개인정보를 전송받는 자를 말한다.
3. “지정권자”란 법 제35조의3제1항에 따라 개인정보관리 전문기관을 지정할 수 있는 개인정보 보호위원회(이하 “보호위원회”라 한다) 또는 관계 중앙행정기관의 장을 말한다.
4. “중계 전문기관”이란 영 제42조의8제1항제1호에 해당하는 자로서 개인정보 전송 중계에 필요한 기능을 제공하고 관련 시스템을 운영하는 업무 및 정보전송자의 전송을 지원하는 업무를 수행하는 자를 말한다.
5. “일반 전문기관”이란 영 제42조의8제1항제2호에 해당하는 자로서 통합조회, 맞춤형 서비스, 연구, 교육 등을 위해 정보전송자로부터 전송받은 개인정보(영 제42조의4제1항제1호의 정보는 제외)를 관리·분석하는 업무를 수행하는 자를 말한다.
6. “특수 전문기관”이란 영 제42조의8제1항제3호에 해당하는 자로서 통합조회, 맞춤형 서비스, 연구, 교육 등을 위해 정보전송자로부터 전송받은 영 제42조의4제1항제1호의 개인정보를 관리·분석하는 업무를 수행하는 자를 말한다.

제2장 개인정보 전송 방법 등

제3조(일반수신자 시설 및 기술) 법 제35조의2제2항제2호 및 영 제42조의3제1항에 따른 “보호위원회가 정하여 고시하는 시설 및 기술”은 별표 1과 같다.

제4조(전송 요구의 방법) 정보주체는 법 제35조의2제2항에 따라 전송을 요구하는 경우 별지 제1호서식의 전송 요구서를 작성하여 정보전송자에게 제출하여야 한다.

제5조(전송 방식 등) ① 영 제42조의6제3항에서 “보호위원회가 정하여 고시하는 방식”이란 다음 각 호를 모두 충족하는 방식을 말한다. 다만, 제35조의2제1항에 따라 전송을 요구하는 경우에는 제1호에 한한다.

1. 정보 전송 시 안전한 암호 알고리즘으로 암호화하여 전송하는 방식
2. 정보전송자, 일반수신자, 개인정보관리 전문기관 사이에 미리 정한 방식
3. 정보전송자, 일반수신자, 개인정보관리 전문기관 간 상호 식별·인증할 수 있는 방식
4. 정보전송자, 일반수신자, 개인정보관리 전문기관 간 상호 확인할 수 있는 방식

② 영 제42조의6제8항 각 호 외의 부분에서 “보호위원회가 정하여 고시하는 방식”이란 같은 항 각 호의 접근수단을 다음 각 호의 어느 하나에 해당하는 방법을 통해 위임·대리·대행, 그 밖에 이와 유사한 방식으로 정보주체의 이름으로 열람하는 방식을 말한다.

1. 접근수단을 직접 보관하는 방법
2. 정보주체의 접근수단에 접근할 수 있는 권한을 확보하는 방법
3. 접근수단에 대한 지배권, 이용권 또는 접근권 등을 사실상 확보하는 방법

제3장 개인정보관리 전문기관 지정

제6조(지정기준) 영 제42조의9제1항제1호다목, 제2호다목 및 제3호다목에서 “보호위원회가 정하여 고시하는” 설비 및 기술 등 기준은 별표 2와 같다.

제7조(지정권자) ① 지정권자는 다음 각 호로 한다.

1. 중계 전문기관: 보호위원회 또는 관계 중앙행정기관의 장(단, 영 제42조의4제1항제1호에 해당하는 개인정보에 관한 중계 전문기관은 보건복지부장관이 지정한다)

2. 일반 전문기관: 보호위원회 또는 관계 중앙행정기관의 장

3. 특수 전문기관: 보건복지부장관

② 제1항제1호 및 제2호에 따라 개인정보관리 전문기관을 지정할 수 있는 관계 중앙행정기관의 장은 개인정보관리 전문기관으로 지정받고자 하는 기관·법인 또는 단체(이하 “지정신청자”라 한다)가 전송받고자 하는 정보와의 업무 관련성을 고려하여 정한다.

제8조(지정신청) ① 지정신청자는 법 제35조의3제1항 및 영 제42조의9에 따라 별지 제2호 서식의 개인정보관리 전문기관 지정신청서에 별표 3에 따른 신청서류를 첨부하여 제7조 제1항 각 호에 따른 지정권자에게 제출하여야 한다.

② 지정신청자가 일반 전문기관과 특수 전문기관의 업무를 모두 수행하고자 하는 경우에는 각 지정권자에게 제1항에 따른 지정신청을 각각 하여야 한다.

③ 제1항에 따른 지정신청을 받은 관계 중앙행정기관(이하 이 조문 안에서 “신청서 접수기관”이라 한다)의 장은 다음 각 호의 어느 하나에 해당하는 경우에는 보호위원회 및 다른 관계 중앙행정기관의 장과 협의하여 접수된 지정신청서류를 지체 없이 소관 기관에 이송하고, 그 사실을 지정신청자에게 통지하여야 한다.

1. 신청서 접수기관의 업무와 지정신청의 내용 간에 밀접한 관련성이 없는 경우

2. 신청서 접수기관이 해당 업무를 수행하기 어려운 정당한 사유가 있는 경우

④ 제3항에도 불구하고 보호위원회는 신청서 접수기관의 장이 개인정보관리 전문기관을 지정하는 것이 적정하지 않다고 판단되는 경우에는 신청서 접수기관의 장 및 다른 관계 중앙행정기관의 장과 협의하여 접수된 지정신청서류를 소관 기관에 이송하도록 할 수 있다. 이 경우 보호위원회는 그 사실을 지정신청자에게 통지하여야 한다.

제9조(지정절차) ① 법 제35조의3제1항 및 영 제42조의9에 따른 개인정보관리 전문기관의 지정절차는 서류심사, 현장심사, 종합심사의 순으로 진행된다.

② 지정권자는 제8조제1항에 따른 지정신청에 관하여 서류 등이 누락되거나 보완이 필요한 경우에는 지정신청자에게 기간을 정하여 보완을 요구할 수 있다.

③ 지정권자는 제8조제1항에 따른 지정신청을 받은 날의 다음날부터 4개월 이내(예비지정을 받은 경우에는 2개월 이내)에 개인정보관리 전문기관 지정 여부를 결정하여 그 결과를

지체없이 지정신청자에게 문서(지정신청자가 전자문서로 신청한 경우 전자문서를 포함한다. 이하 같다)로 통지하여야 한다. 다만, 부득이한 사정이 있는 경우 1개월의 범위에서 그 기간을 연장할 수 있다.

④ 제3항에 따른 심사기간을 산정할 때에는 다음 각 호에 해당하는 기간은 심사기간에 산입하지 아니한다.

1. 제8조제3항 및 제4항에 따라 개인정보관리 전문기관 지정권자의 확인 및 변경, 지정권자 협의 등에 소요되는 기간
2. 제2항에 따른 지정신청자의 신청서류 보완에 소요되는 기간
3. 법 또는 영에 따른 의무의 위반과 관련하여 지정신청자를 상대로 형사소송 절차가 진행되고 있거나 조사·검사 등의 절차가 진행되고 있고, 그 소송이나 조사·검사 등의 내용이 지정심사에 중대한 영향을 미칠 수 있다고 인정되는 경우에는 그 소송이나 조사·검사 등의 절차가 끝날 때까지의 기간
4. 지정심사 중 불가피한 사유, 대규모 사회재난, 천재지변 등 불가항력적인 사유로 인한 기간

⑤ 지정권자는 지정 여부를 결정하기 위하여 보호위원회 또는 전송 요구 정보와 관련된 관계 중앙행정기관 장의 의견을 들어야 한다.

⑥ 제8조제2항의 경우 지정권자는 사전에 다른 지정권자와 협의하여 지정 여부를 결정하여야 한다. 이 경우 지정권자는 다른 지정권자와 협의하여 지정심사(제9조제1항에 따른 서류심사, 현장심사 및 종합심사를 포함한다)를 공동으로 진행할 수 있다.

제10조(지정심사위원회 구성 등) ① 지정권자는 제8조제1항에 따른 신청을 받은 경우 법 제35조의3제2항 및 영 제42조의9제1항에 따른 개인정보관리 전문기관 지정요건을 충족하는지 여부를 개인정보관리 전문기관 지정심사위원회(이하 “지정심사위원회”라 한다)를 구성하여 심사하여야 한다.

② 지정심사위원회는 개인정보 보호, 정보보호, 회계 및 지정권자가 정하는 관계 분야 등 지정요건에 관하여 학식과 경험이 풍부한 전문가로 구성하되, 7명 이상 15명 이하로 한다.

③ 지정심사위원회는 제9조제1항에 따른 종합심사를 수행한 후 그 심사결과를 지정권자에게 보고하여야 한다.

④ 지정권자는 다음 각 호의 기관의 장에게 지정심사위원회의 구성·운영, 기술적인 사항의 자문 등 지정 여부를 결정하기 위하여 필요한 지원을 요청할 수 있다.

1. 한국인터넷진흥원

2. 업무 관련성 및 수행능력 등을 고려하여 지정권자가 적합하다고 인정하는 기관

제11조(지정 및 지정서 발급) ① 지정권자는 제10조제3항에 따른 지정심사위원회의 심사결과를 확인하여 지정이 적합하다고 인정하는 경우 지정신청자를 개인정보관리 전문기관으로 지정할 수 있다.

② 지정권자는 제1항에 따른 지정에 조건을 붙일 수 있다. 이 경우 지정권자는 그 이행 여부를 확인하여야 한다.

③ 지정권자는 제1항에 따라 개인정보관리 전문기관을 지정한 때에는 별지 제3호서식의 개인정보관리 전문기관 지정서를 지정신청자에게 발급하여야 한다.

제12조(예비지정) ① 영 제42조의9제5항에 따른 개인정보 관리 전문기관 예비지정(이하 “예비지정”이라 한다)을 받고자 하는 자는 별지 제2호서식의 개인정보관리 전문기관 예비지정신청서에 별표 3에 따른 신청서류를 첨부하여 보호위원회 또는 관계 중앙행정기관의 장에게 제출하여야 한다.

② 지정권자는 제1항에 따라 예비지정신청을 받은 경우에는 2개월 이내에 서류심사를 통해 예비지정 여부를 결정하여 그 결과를 지체없이 예비지정신청자에게 통지하여야 한다. 다만, 부득이한 사정이 있는 경우 1개월의 범위에서 그 기간을 연장할 수 있다.

③ 제1항에 따른 심사 결과 예비지정을 받은 자는 예비지정을 받은 날부터 6개월 이내에 예비지정의 내용(예비지정시 조건을 붙인 경우 그 조건을 포함한다)을 이행한 후 제9조에 따른 개인정보관리 전문기관 지정(이하 이 항에서 “본지정”이라 한다)을 신청하여야 한다. 다만, 지정권자의 예비지정 당시 본지정 신청기한을 따로 정하였거나 예비지정 후 본지정 신청기한의 연장에 대하여 지정권자의 승인을 받은 경우에는 그 기간을 달리 정할 수 있다.

④ 예비지정에 관하여 제1항부터 제3항까지에서 정한 사항을 제외하고는 제7조부터 제10조까지의 규정을 준용한다. 이 경우 “지정”은 “예비지정”으로 본다.

제13조(변경승인) ① 영 제42조의9제8항에 따라 변경승인을 받으려는 자는 별지 제4호서식의

개인정보관리 전문기관 변경승인신청서에 영 제42조의9제8항 각 호의 변경된 문서를 첨부하여 지정권자에게 제출하여야 한다.

② 지정권자는 제1항에 따라 제출된 변경승인신청서를 심사하고 승인 여부를 변경승인 신청자에게 통지하여야 한다.

③ 영 제42조의9제8항 단서에서 “보호위원회가 정하여 고시하는 경미한 사항”이란 자구(字句) 수정, 오타자 정정 등 단순한 변경에 관한 사항을 말한다.

④ 변경승인에 관하여 제1항부터 제3항까지에서 정한 사항을 제외하고는 제9조부터 제10조까지의 규정을 준용할 수 있다. 이 경우 “지정”은 “변경승인”으로 본다.

제14조(재지정) ① 개인정보관리 전문기관은 재지정을 받으려는 경우 유효기간 만료일 6개월 전까지 제8조제1항에 따른 개인정보관리 전문기관 지정신청서 및 신청서류를 갖추어 지정권자에게 제출하여야 한다. 이 경우 재지정 신청에 대한 처리결과를 통지받을 때까지는 그 지정은 계속 유효한 것으로 본다.

② 개인정보관리 전문기관 재지정 심사 및 절차에 관련하여서는 제8조부터 제11조, 제16조의 절차를 준용한다. 이 경우 “지정”은 “재지정”으로 본다.

제15조(지정취소) ① 지정권자는 개인정보관리 전문기관에 법 제35조의3제4항제2호의 사유 또는 영 제42조의10제1항제3호부터 제6호까지의 지정 취소사유가 발생하는 경우 그 지정을 취소하기 전에 해당 개인정보관리 전문기관에 시정·보완을 요구할 수 있다.

② 영 제42조의10제7항에서 “보호위원회가 정하여 고시하는 조치”는 다음 각 호와 같다.

1. 수행 중인 업무의 중단
2. 보유하고 있는 개인정보의 파기(다른 법령에 따라 보존하여야 하는 경우는 제외한다)
3. 업무의 중단 및 개인정보의 파기 시 해당 사실의 정보주체에 대한 통지
4. 수행 중인 업무를 다른 중계 전문기관으로 이전(중계 전문기관을 중지 또는 폐지, 취소하려는 경우에 한한다)

제16조(지정 등의 공고) ① 지정권자는 개인정보관리 전문기관을 지정, 재지정 또는 지정 취소한 경우 영 제42조의10제4항에 따라 다음 각 호의 사항을 관보에 공고하거나 지정권자의 홈페이지에 게시하여야 한다.

1. 개인정보관리 전문기관의 명칭 및 주소
 2. 담당 부서 및 연락처
 3. 지정 유효기간(지정 또는 재지정의 경우에 한한다)
 4. 취소일자 및 취소사유(지정 취소의 경우에 한한다)
- ② 보호위원회가 아닌 지정권자는 영 제42조의10제5항 본문의 사항을 결정하려는 경우 각 사유의 시행 예정일로부터 10일 전까지 제1항 각 호의 사항을 보호위원회에게 통지하여야 한다.

제4장 그 밖에 필요한 사항

제17조(일반수신자 개인정보 전송지원 플랫폼 등록 절차) ① 영 제42조의13제1항에 따라 일반수신자로서 정보를 전송받으려는 자는 별지 제5호서식의 일반수신자 등록신청서에 다음 각 호의 서류(「전자문서 및 전자거래 기본법」 제2조제1호에 따른 전자문서를 포함한다. 이하 같다)를 첨부하여 개인정보 전송지원 플랫폼(이하 “플랫폼”이라 한다)에 등록을 요청하여야 한다.

1. 개인정보 관리 계획서(고유의 업무 수행에 있어 전송받고자 하는 정보의 필요성 및 이용계획 포함)
 2. 별표 1에 따른 일반수신자 시설 및 기술을 갖추었음을 증명할 수 있는 서류
 3. 법 제29조에 따른 안전조치의무 이행을 증명할 수 있는 서류
- ② 보호위원회는 제1항에 따른 사항을 확인하여 법 제35조의2제2항제2호 및 별표 1에 따른 일반수신자 시설 및 기술 등을 충족하는 경우에는 해당 일반수신자를 플랫폼에 등록하여야 한다.

제18조(전문기관 등 개인정보 전송지원 플랫폼 등록 절차) ① 보호위원회는 지정권자가 제9조제3항에 따라 개인정보관리 전문기관을 지정한 경우 해당 개인정보관리 전문기관을 플랫폼에 등록하여야 한다.

- ② 보호위원회는 영 제42조의12제1항에 따라 법 제35조의2제2항에 따른 정보전송자임을 확인한 경우 해당 정보전송자를 플랫폼에 등록하여야 한다.

[별표 1]

일반수신자 시설 및 기술(제3조 관련)

구 분	시설 및 기술
1. 전송 요구 관련 제반 시스템	1) 표준 전송 절차 및 연계 방식, 전송 보안 기준을 충족하는 전송 요구 기능을 갖춘 시스템 - 정보주체 인증 및 전송요구서 관리 기능 - 개인정보 전송 내역 기록·보관 기능 - 전송받은 정보의 분리·보관 기능 2) 시스템의 운영 및 보호가 가능한 네트워크 구성
2. 보호체계	1) 일반수신자 업무 관련 정보의 안전성 확보를 위한 내부 관리계획 ※ 해킹 등 전자적 침해행위로부터 보호하기 위한 방안 포함 2) 개인정보 전송 내역의 기록·보관 및 점검 3) 시스템의 주요 정보를 안전하게 처리하기 위한 접근 권한의 관리 및 점검 체계 4) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 시스템, 업무용 단말 등에 대한 접근통제 체계

※ 그 외 법 제29조에 따라 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 함

[별표 2]

개인정보관리 전문기관 지정기준(제6조 관련)

1. 중계 전문기관 지정기준

구 분		지정기준
1. 설비 및 기술		1) 표준 전송 절차 및 연계 방식, 전송 보안 기준을 충족하는 전송 중계 및 전송 지원과 관련한 기능 <ul style="list-style-type: none"> - 전송요구서 관리, 전자서명 검증, 접근권한 인가 - 이용기관(제3자 대상 정보전송자, 일반수신자, 일반·특수전문기관) 연계 체계 - 개인정보 전송 지원 플랫폼과의 연계 체계 - 개인정보 전송 내역 기록·보관 기능 ※ 중계 전문기관 업무 관련 시스템과 그 외 개인정보 처리시스템의 분리 구축 2) 시스템의 운영 및 보호가 가능한 네트워크 구성 3) 중계 전문기관 업무의 가용성 및 연속성 보장을 위한 체계 <ul style="list-style-type: none"> - 주요 시스템 및 네트워크 이중화 구성 - 시스템 및 네트워크 모니터링 체계 - 시스템 장애, 오류 등으로 전송 중계 및 전송 지원이 불가능한 경우 보호위원회 및 지정권자, 이용기관(제3자 대상 정보전송자, 일반수신자, 일반·특수전문기관) 대상 통지 체계
2. 보호체계	가. 보호정책의 수립·시행 및 점검	1) 전문기관 업무 관련 정보의 안전성 확보를 위한 내부 관리계획 <ul style="list-style-type: none"> ※ 시스템에 대한 정기적인 취약점 점검 및 조치 방안, 해킹 등 전자적 침해행위로부터 보호하기 위한 방안 포함 2) 개인정보 전송 내역의 기록·보관 및 점검 방안
	나. 접근권한의 관리	3) 시스템의 주요 정보를 안전하게 처리하기 위한 접근 권한의 관리 및 점검 체계
	다. 접근통제	4) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 시스템, 업무용 단말 등에 대한 접근 통제 체계 5) 유출 및 해킹을 신속하게 탐지·대응할 수 있는 모니터링 체계

		6) 시스템에 접근할 수 있는 관리용 단말기를 지정·관리하고 추가인증을 적용하여 정당한 권한을 가진 자만 접속 가능하도록 조치 7) 시스템에 접속하는 개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단 조치
	라. 암호화	8) 정보의 송·수신 등을 위한 안전한 암호화 적용 9) 암호 키의 안전한 관리 체계(암·복호화 대상 시스템과 분리된 시스템 구축 등)
	마. 접속기록의 보관 및 점검	10) 시스템을 안전하게 관리하기 위한 접속기록의 보관 및 이상접속을 탐지하기 위한 조치
	바. 악성프로그램 등 방지	11) 악성프로그램 등을 예방·탐지·대응하기 위한 조치
	사. 물리적 안전조치	12) 정보를 안전하게 보관·관리하기 위한 물리적 안전조치
	아. 재해·재난 대비 안전 조치	13) 재난·재해 및 장애 등에 대비한 비상계획, 복구 계획 및 훈련실시 방안 14) 중계 전문기관 업무 관련 정보의 안전한 백업 및 복구 체계(소산 포함)
	자. 출력복사시 안전 조치	15) 개인정보, 전송요구서 등을 안전하게 이용·관리하기 위한 출력·복사시 안전 조치 방안
	차. 파기	16) 정보의 안전한 파기를 위한 조치
	카. 그 밖에 필요한 조치	17) 시스템 가용성 및 연속성 보장을 위한 주요 지표 마련 및 관리 방안 18) 시스템 정비 및 프로그램 변경·이행 절차 19) 중계 전문기관의 안정적 운영을 위한 전담조직 및 담당인력 지정
3. 보험 또는 공제 가입		최저가입금액 10억원 이상의 보험 또는 공제 가입 (다만, 지정신청자가 영 제42조의9제2항 각 호의 어느 하나에 해당하는 경우에는 법 제39조의7 및 영 제48조의7에서 정한 기준을 따른다.)

2. 일반 전문기관 지정기준

구 분		지정기준
1. 설비 및 기술		1) 표준 전송 절차 및 연계 방식, 전송 보안 기준을 충족하는 전송 요구 기능을 갖춘 시스템 - 정보주체 인증 및 전송요구서 관리 기능 - 중계 전문기관과의 연계 체계 - 개인정보 전송 지원 플랫폼과의 연계 체계 - 개인정보 전송 내역 기록·보관 기능 - 전송받은 정보의 분리·보관 기능 - 전송 내역, 전송받은 정보의 제3자 제공 동의내역의 개인정보 전송 지원 플랫폼 제출 기능 2) 시스템의 운영 및 보호가 가능한 네트워크 구성
2. 보호체계	가. 보호정책의 수립·시행 및 점검	1) 전문기관 업무 관련 정보의 안전성 확보를 위한 내부 관리계획 ※ 시스템에 대한 정기적인 취약점 점검 및 조치 방안, 해킹 등 전자적 침해행위로부터 보호하기 위한 방안 포함 2) 개인정보 전송 내역의 기록·보관 및 점검 3) 정보주체 대상 전송 내역의 통지 절차
	나. 접근권한의 관리	4) 시스템의 주요 정보를 안전하게 처리하기 위한 접근 권한의 관리 및 점검 체계
	다. 접근통제	5) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 시스템, 업무용 단말 등에 대한 접근 통제 체계
	라. 암호화	6) 정보의 송·수신 등을 위한 안전한 암호화 적용
	마. 접속기록의 보관 및 점검	7) 시스템을 안전하게 관리하기 위한 접속기록의 보관 및 점검 체계
	바. 악성프로그램 등 방지	8) 악성프로그램 등을 예방·탐지·대응하기 위한 조치

	사. 물리적 안전조치	9) 정보를 안전하게 보관·관리하기 위한 물리적 안전조치
	아. 재해·재난 대비 안전 조치	10) 재난·재해 및 장애 등에 대비한 비상계획, 복구 계획 및 훈련실시 방안 11) 정보의 안전한 백업 및 복구 체계
	자. 출력·복사시 안전 조치	12) 개인정보, 전송요구서 등을 안전하게 이용·관리하기 위한 출력·복사시 안전 조치 방안
	차. 파기	13) 정보의 안전한 파기를 위한 조치
3. 보험 또는 공제 가입		최저가입금액 10억원 이상의 보험 또는 공제 가입 (다만, 지정신청자가 영 제42조의9제2항 각 호의 어느 하나에 해당하는 경우에는 법 제39조의7 및 영 제48조의7에서 정한 기준을 따른다.)

3. 특수 전문기관 지정기준

구 분		지정기준
1. 설비 및 기술		1) 표준 전송 절차 및 연계 방식, 전송 보안 기준을 충족하는 전송 요구 기능을 갖춘 시스템 <ul style="list-style-type: none"> - 정보주체 인증 및 전송요구서 관리 기능 - 중계 전문기관과의 연계 체계 - 개인정보 전송 지원 플랫폼과의 연계 체계 - 개인정보 전송 내역 기록·보관 기능 - 전송받은 정보의 분리·보관 기능 - 전송 내역, 전송받은 정보의 제3자 제공 동의내역의 개인정보 전송 지원 플랫폼 제출 기능 2) 시스템의 운영 및 보호가 가능한 네트워크 구성
2. 보호체계	가. 보호정책의 수립·시행 및 점검	1) 전문기관 업무 관련 정보의 안전성 확보를 위한 내부 관리계획 ※ 시스템에 대한 정기적인 취약점 점검 및 조치 방안, 해킹 등 전자적 침해행위로부터 보호하기 위한 방안 포함 2) 개인정보 전송 내역의 기록·보관 및 점검 3) 정보주체 대상 전송 내역의 통지 절차
	나. 접근권한의 관리	4) 시스템의 주요 정보를 안전하게 처리하기 위한 접근 권한의 관리 및 점검 체계
	다. 접근통제	5) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 시스템, 업무용 단말 등에 대한 접근통제 체계 6) 유출 및 해킹을 신속하게 탐지·대응할 수 있는 모니터링 체계 7) 시스템에 접근할 수 있는 관리용 단말기를 지정·관리하고 추가인증을 적용하여 정당한 권한을 가진 자만 접속 가능하도록 조치 8) 시스템에 접속하는 개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단 조치
	라. 암호화	9) 정보의 송·수신 등을 위한 안전한 암호화 적용 10) 암호 키의 안전한 관리 체계(암·복호화 대상 시스템과 분리된 시스템 구축 등)

	마. 접속기록의 보관 및 점검	11) 시스템을 안전하게 관리하기 위한 접속기록의 보관 및 이상접속을 탐지하기 위한 조치
	바. 악성프로그램 등 방지	12) 악성프로그램 등을 예방·탐지·대응하기 위한 조치
	사. 물리적 안전조치	13) 정보를 안전하게 보관·관리하기 위한 물리적 안전조치
	아. 재해·재난 대비 안전 조치	14) 재난·재해 및 장애 등에 대비한 비상계획, 복구계획 및 훈련실시 방안 15) 정보의 안전한 백업 및 복구 체계
	자. 출력복사시 안전 조치	16) 개인정보, 전송요구서 등을 안전하게 이용·관리하기 위한 출력·복사시 안전 조치 방안
	차. 파기	17) 정보의 안전한 파기를 위한 조치
3. 보험 또는 공제 가입		최저가입금액 10억원 이상의 보험 또는 공제 가입 (다만, 지정신청자가 영 제42조의9제2항 각 호의 어느 하나에 해당하는 경우에는 법 제39조의7 및 영 제48조의7에서 정한 기준을 따른다.)

[별표 3]

개인정보관리 전문기관 지정 신청서류(제8조제1항, 제12조제1항 관련)

관련 규정	신청서류	
	예비지정	지정
1. 정관 또는 규약	정관 또는 규약(안)	정관 또는 규약
2. 사업계획서	사업계획서(안)	사업계획서 (증명 서류 포함)
3. 개인정보 관리 계획서	개인정보 관리 계획서(안)	개인정보 관리 계획서 (증명 서류 포함)
4. 과거 3개년간의 재무제표	과거 3개년간의 재무제표	과거 3개년간의 재무제표
5. 법 제35조의3제2항에 따른 지정요건을 충족하였음을 증명할 수 있는 서류		
가. 별표 2에 따른 설비 및 시설 증명 서류	별표 2에 따른 설비 및 시설 구축 계획	별표 2에 따른 설비 및 시설을 적정하게 갖췄는지 확인할 수 있는 자료
나. 법 제29조에 따른 안전조치의무 이행	안전조치 의무 이행 계획	안전조치 의무 이행을 확인할 수 있는 자료
다. 별표 2에 따른 보호 체계 증명 서류	별표 2에 따른 보호체계 이행 계획, 전문기관 업무 관련 내부 관리계획(안)	별표 2에 따른 보호체계를 적정하게 갖췄는지 확인할 수 있는 자료, 전문기관 업무 관련 내부관리계획
라. 자본금	자본금(기본재산 또는 자산총계) 증빙자료 또는 자본금 조달계획서	자본금(기본재산 또는 자산총계) 증빙자료
마. 보험 또는 공제 가입	-	별표 2에 따른 보험 또는 공제 가입을 확인할 수 있는 자료
6. 그 밖에 지정에 필요하 다고 인정하는 서류	지정권자가 지정에 필요하다고 별도로 정하는 서류(지정공고 사항 참고)	지정권자가 지정에 필요하다고 별도로 정하는 서류(지정공고 사항 참고)

개인정보 전송요구서

전송 요구 목적	
정보전송자 (전송 요구를 받는 자)	기관·법인·단체명(또는 명칭)
개인정보를 전송받는 자	기관·법인·단체명(또는 명칭)
전송을 요구하는 개인정보	
정기적 전송을 요구하는지 여부 및 그 주기	영 제42조의8제1항제2호 및 제3호에 해당하는 개인정보관리 전문기관으로 전송하는 경우에 한함
전송 요구의 종료 시점	
보유 및 이용기간	

「개인정보 보호법」 제35조의2제2항에 따라 개인정보 전송을 위와 같이 요구합니다.

년 월 일

신청자

(서명 또는 인)

210mm×297mm[(백상지(80g/㎡) 또는 중질지(80g/㎡)]

개인정보관리 전문기관 지정신청서

([] 지정 [] 예비지정)

지정 신청자	기관·법인·단체명 (또는 명칭)	사업자등록번호 또는 법인등록번호	
	대표자 성명		
	주소 (주된 사무소 소재지)		
	주요 설비 및 시설의 설치 장소		
	홈페이지 주소		
담당자	담당자 성명		
	담당자 연락처	전화번호	
		전자우편	
종전 지정사항	[] 예비지정 (예비지정을 받은 일시: 년 월 일)		
	[] 일반 전문기관 업무 [] 특수 전문기관 업무 (지정을 받은 일시: 년 월 일)		
지정받고자 하는 업무	[] 중계 전문기관 업무 [] 일반 전문기관 업무 [] 특수 전문기관 업무		

「개인정보 보호법」 제35조의3제1항 및 같은 법 시행령 제42조8제1항, 「개인정보 전송방법 및 개인정보관리 전문기관 지정 등에 관한 고시」 제8조제1항 또는 제12조제1항에 따라 개인정보관리 전문기관 지정을 위와 같이 신청합니다.

년 월 일

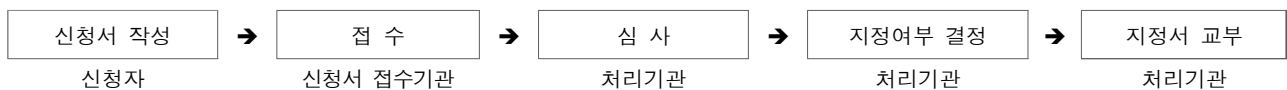
신청자

(서명 또는 인)

개인정보보호위원회 귀중 / 관계 중앙행정기관의 장 귀하

첨부 서류	별표 3에 따른 지정 신청서류	수수료 없음
-------	------------------	---------------

처 리 절 차



210mm×297mm[(백상지(80g/㎡) 또는 중질지(80g/㎡)]

제 호

개인정보관리 전문기관 지정서

1. 기관·법인·단체명(또는 명칭) :
2. 대 표 자 :
3. 주 소 :
4. 지정업무 :
5. 유효기간 :

위의 (기관·법인·단체)를 「개인정보 보호법」 제35조의3제1항 및 같은 법 시행령 제42조의9에 따라 개인정보관리 전문기관으로 지정합니다.

년 월 일

개인정보보호위원회/
관계 중앙행정기관의 장

직인

개인정보관리 전문기관 변경승인신청서

([] 중계 전문기관 [] 일반 전문기관 [] 특수 전문기관)

변경승인 신청자	기관·법인·단체명 (또는 명칭)	사업자등록번호 또는 법인등록번호	
	대표자 성명		
	주소 (주된 사무소 소재지)		
	홈페이지 주소		
담당자	담당자 성명		
	담당자 연락처	전화번호	
		전자우편	
변경사항	변경 사항	<input type="checkbox"/> 사업계획서 <input type="checkbox"/> 개인정보 관리 계획서	
	변경 내용	변경 전	
		변경 후	
	변경 사유		

「개인정보 보호법」 제35조의3 및 같은 법 시행령 제42조9제8항, 「개인정보 전송방법 및 개인정보 관리 전문기관 지정 등에 관한 고시」 제13조제1항에 따라 개인정보관리 전문기관 변경승인을 위와 같이 신청합니다.

년 월 일

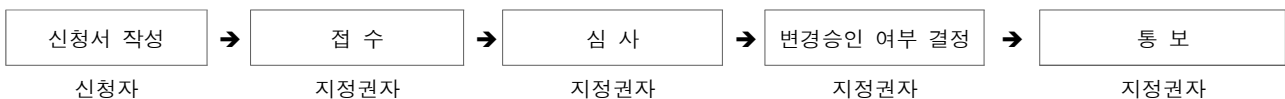
신청자

(서명 또는 인)

개인정보보호위원회 귀중 / 관계 중앙행정기관의 장 귀하

첨부 서류	1. 사업계획서(전송받고자 하는 정보의 추가 또는 변경을 포함) 2. 개인정보 관리 계획서	수수료
		없음

처 리 절 차



210mm×297mm[(백상지(80g/㎡)또는 중질지(80g/㎡)]

일반수신자 등록신청서

등록 신청자	기관·법인·단체명 (또는 명칭)		
	사업자등록번호 또는 법인등록번호		
	대표자 성명		
	주소 (주된 사무소 소재지)		
	주요 설비 및 시설의 설치 장소		
	홈페이지 주소		
담당자	담당자 성명		
	담당자 연락처	전화번호	
		전자우편	

「개인정보 보호법」 제35조의3제1항 및 같은 법 시행령 제42조13제1항, 「개인정보 전송방법 및 전문기관 지정 등에 관한 고시」 제17조제1항에 따라 일반수신자 등록을 위와 같이 신청합니다.

년 월 일

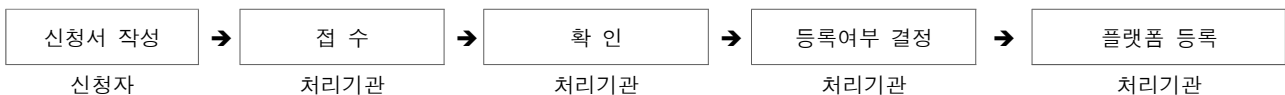
신청자

(서명 또는 인)

개인정보보호위원회 귀중

첨부 서류	1. 개인정보 관리 계획서 (고유의 업무 수행에 있어 전송받자 하는 정보의 필요성 및 이용계획 포함) 2. 별표 1에 따른 일반수신자 시설 및 기술을 갖추었음을 증명할 수 있는 서류 3. 법 제29조에 따른 안전조치의무 이행을 증명할 수 있는 서류	수수료 없음
-------	--	-----------

처 리 절 차



210mm×297mm[(백상지(80g/㎡) 또는 중질지(80g/㎡)]

2024. 10. 29 일부개정안 제정(안) 행정예고

제1조(목적) 이 고시는 「개인정보 보호법」 제35조의2제1항 내지 제2항, 「개인정보 보호법 시행령」(이하 “영”이라 한다) 제42조의2제1호 및 영 제42조의4제1항제1호에 따라 보건 의료 분야의 정보전송자 및 전송 요구 정보에 관한 사항을 정하는 것을 목적으로 한다.

제2조(정보전송자) 영 제42조의2제1호에서 “보건복지부장관과 협의하여 보호위원회가 정하여 고시하는 자”란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 질병관리청
2. 「국민건강보험법」 제13조에 따른 국민건강보험공단 및 같은 법 제62조에 따른 건강보험심사평가원

제3조(전송 요구 정보) 영 제42조의4제1항제1호에서 “보건복지부장관과 협의하여 보호위원회가 정하여 고시하는 정보”는 별표와 같다.

부 칙

이 고시는 2025년 3월 13일부터 시행한다.

[별표]

전송 요구의 대상이 되는 정보(제3조 관련)

정보 전송자	정보항목	세부항목	대상 범위
「의료법」 제3조의4에 따른 상급종합 병원	환자정보	성명, 성별, 생년월일	전송 요구 시점으로 부터 3년
	의료기관 정보	의료기관 종별 타입, 의료기관 명칭	
	진료의 정보	진료의 성명, 진료과	
	내원정보	내원 상태, 진료 구분, 내원 기간	
	진단정보	진단 상태, 진단 코드, 진단 및 주호소 정보, 진단 일시	
	약물처방 정보	약물 처방 상태, 약물 처방 의도, 지참약 여부, 처방 약물 정보, 약물 처방 일시, 약물 투여 방법	
	수술 및 처치내역	수술 및 처치 진행상태, 수술 및 처치 코드, 수술 및 처치 일시	
	진단검사, 기타검사	검사진행상태, 검사구분(진단, 기타), 검사 코드, 검사 일시, 검사 결과, 참고치	
	알레르기 및 불내성	알레르기 및 불내성 원인구분, 알레르기 및 불내성 원인코드, 알레르기 및 불내성 기록 일시, 알레르기 및 불내성 반응, 추가정보	
	영상검사, 병리검사	검사진행상태, 검사구분(영상, 병리), 검사 코드, 검사일시, 검사 소견	
질병관리청	예방접종 정보	접종자 현황(성명, 성별, 생년월일), 접종일자, 접종기관명, 접종차수, 접종코드	전체기간
국민건강 보험공단	건강검진 정보	건강검진 정보, 영유아건강검진 정보, 암건강 검진 정보	전송 요구 시점으로 부터 10년
	진료내용 정보	대상자 현황, 병의원/약국 명칭, 진료개시일, 진료형태, 방문입원일수, 처방횟수, 본인부담금, 병의원 소재지	전송 요구 시점으로 부터 1년
건강보험 심사평가원	투약이력 정보	조제일자, 조제기관, 약품코드, 약품명(제품명), 성분코드, 함량, 투약량, 투여횟수, 총투약일수	전송 요구 시점으로 부터 1년

※ 각 정보의 식별자는 기본 포함

※ 의료기관에 따라 해당 의료정보가 시스템에 존재하지 않는 경우 제공되지 않을 수 있음

Chapter

IV

교육분야 관련 서식 등 참고자료



[시행 2024. 2. 7.] [교육부훈령 제476호, 2024. 2. 7., 전부개정]

제1조(목적) 이 지침은 「개인정보 보호법」(이하 "법"이라 한다) 제12조제2항 및 「표준 개인정보 보호지침」에 따라 교육부 소관 분야의 개인정보보호에 필요한 세부적인 사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 지침은 전자적 처리 여부를 불문하고 수기문서를 포함한 모든 형태의 개인정보파일을 운용하는 교육부 및 그 소속기관, 시도교육청 및 그 소속기관, 교육부장관의 지도감독을 받는 공공기관 및 각급학교(이하 "교육기관"이라 한다.)에 적용한다.

제3조(용어의 정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
 - 가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
 - 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
 - 다. 가목 또는 나목을 제1호의 2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)
- 1의2. "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.
2. "각급학교"란 다음 각 호의 어느 하나에 해당하는 기관을 말한다.
 - 가. 「유아교육법」에 따른 학교
 - 나. 「초·중등교육법」에 따른 각급학교
 - 다. 「고등교육법」에 따른 각급학교
 - 라. 그 밖의 다른 법률에 따라 설치된 각급학교
3. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 제31조 및 「개인정보 보호법 시행령」(이하 "시행령"이라 한다) 제32조제2항에 따른 지위에 해당하는 자를 말한다.
5. "개인정보보호 업무 분야별책임자"(이하 "분야별책임자"라 한다)란 업무를 위하여 개인정보파일을 처리하는 부서의 장으로 개인정보 보호책임자가 지정한 자를 말한다.
6. "개인정보 보호담당자"란 교육기관의 실질적인 개인정보 보호업무를 담당하는 자로 개인정보처리자가 지정한 자를 말한다.

7. "개인정보취급자"란 개인정보처리자의 지휘감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직원, 파견근로자, 시간제근로자 등을 말한다.
8. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
9. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
10. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
11. "공공기관"이란 법 제2조제6호 및 시행령 제2조에 따른 기관을 말한다.
12. "고유식별정보"란 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호를 말한다.
13. "민감정보"란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보와 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 시행령 제18조 각 호의 정보를 말한다.

제4조(다른 지침과의 관계) ① 교육기관에서 처리하는 개인정보는 교육부 소관 다른 지침에 특별한 규정이 있는 경우를 제외하고는 이 지침에서 정하는 바에 따른다.

② 교육기관이 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하는 경우에는 이 지침에 부합하도록 해야 한다.

③ 이 지침에서 정하지 않은 사항은 「개인정보 보호법」 및 같은 법 시행령, 「표준 개인정보 보호지침」에 따른다.

제5조(개인정보 보호책임자의 지정) ① 개인정보처리자는 법 제31조제1항 및 시행령 제32조제2항에 따라 소관 개인정보의 보호 및 관리를 위하여 개인정보 보호책임자를 지정·운영하여야 한다.

② 개인정보처리자는 제1항에 따라 개인정보 보호책임자를 지정하려는 경우 다음 각 호의 구분에 따른다.

1. 교육부 : 고위공무원
2. 시·도교육청 : 3급 이상 공무원 또는 그에 상응하는 공무원
3. 교육지원청 : 4급 이상 공무원 또는 그에 상응하는 공무원(과단위 교육지원청은 5급 이상 공무원)
4. 유·초·중·고 : 원장 또는 교장
5. 대학 : 학무(교무)위원에 상당하는 행정사무를 총괄하는 사람
6. 그 외의 기관 : 개인정보 처리 관련 업무를 담당하는 부서의 장

제6조(개인정보 보호책임자의 업무 등) ① 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태의 정기적인 조사 및 개선

3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
 4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
 5. 개인정보 보호 교육 계획의 수립 및 시행
 6. 개인정보파일의 보호 및 관리·감독
 7. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
 8. 개인정보 보호 관련 자료의 관리
 9. 개인정보파일의 보유기간 산정
 10. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기
 11. 시행령 제14조의2제1항 각 호의 고려사항에 대한 판단 기준의 공개 여부에 대한 점검 및 해당 기준에 따른 개인정보의 추가적인 이용 또는 제공 여부의 점검
- ② 개인정보 보호책임자는 제1항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

제7조(분야별책임자의 지정) ① 개인정보 보호책임자는 주요 개인정보를 취급하는 부서의 장을 분야별책임자로 지정할 수 있다.

- ② 분야별책임자는 해당부서의 다음 각 호의 업무를 위임받아 수행할 수 있다.
1. 개인정보 처리 실태의 정기적인 조사 및 개선
 2. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
 3. 개인정보파일의 보호 및 관리·감독
 4. 개인정보 처리방침의 수립·변경 및 시행
 5. 개인정보 보호 관련 자료의 관리
 6. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기
 7. 그 밖에 해당부서의 개인정보 보호를 위해 필요한 사항 등

제8조 (개인정보보호 지원단 운영) ① 교육부장관은 교육기관의 개인정보 보호 활동을 효율적으로 수행하기 위하여 "개인정보보호 지원단"을 운영할 수 있다.

- ② 교육부장관은 개인정보보호 지원단 운영 시 필요하다고 인정하는 경우에 교육기관의 장에게 소속 공무원 및 전문요원의 파견(업무지원)을 요청할 수 있다.
- ③ 개인정보보호 지원단은 다음 각호의 업무를 수행한다.
1. 개인정보보호 업무를 위한 지침 및 계획 수립 지원
 2. 개인정보 영향평가 및 개인정보보호 수준진단 지원
 3. 개인정보 분실·도난·유출(이하 "유출등"이라 한다) 예방 점검 및 현장 확인·이행 조치 지원
 4. 개인정보 보호 역량 강화 지원을 위한 교육, 컨설팅 지원(정기, 특별)
 5. 그 밖에 개인정보보호 업무를 위하여 필요한 사항
- ④ 교육부장관 및 시·도교육감은 법 제61조제4항에 따라 교육기관에 대하여 개인정보 보호에 관한 의견을 제시하거나 지도·점검을 할 수 있다.

제9조(교육분야 개인정보보호 전문기관) ① 교육부장관은 교육분야 개인정보 보호 활동을

효율적으로 수행하기 위하여 한국교육학술정보원을 교육분야 개인정보보호 전문기관으로 지정한다.

- ② 교육부장관은 한국교육학술정보원에 개인정보보호 관련 다음 각 호의 업무를 위탁하고 관련 예산을 지원할 수 있다.
1. 개인정보보호 교육 및 컨설팅
 2. 개인정보보호 수준진단 운영
 3. 개인정보보호 지원단 운영
 4. 교육부 개인정보보호 포털 운영
 5. 개인정보 유출등 조사 지원 및 노출점검시스템 운영
 6. 가명처리지원시스템 운영 및 컨설팅
 7. 그 밖에 개인정보보호 업무를 위하여 필요한 사항

제10조(각급학교 폐교·통폐합에 따른 개인정보의 이전) ① 각급학교에서 폐교 및 통폐합 등 처리 시 불필요 개인정보파일은 삭제하는 것을 원칙으로 한다. 다만, 관련 법령 등에 의해 보관이 필요한 경우는 그러하지 아니하다.

- ② 각급학교의 폐교 및 통폐합 등으로 인한 개인정보파일의 이전은 교육부장관 및 시·도교육감이 지정한 개인정보처리자가 안전하게 이전될 수 있도록 처리하여야 한다.
- ③ 제2항에 따라 개인정보파일을 이전하려는 자 또는 받는 자는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 경우에는 사업장 등의 보기 쉬운 장소에 30일 이상 게시하여야 한다.
- ④ 학교 통·폐합과 관련하여 행정예고 등에 제2항의 개인정보파일 이전에 관한 사항을 포함하여 공고한 경우에는 제3항의 내용을 준수한 것으로 본다.

제11조(개인정보보호 교육) ① 개인정보처리자는 매년 당해 연도 개인정보보호를 위한 교육계획을 수립하여 시행하여야 한다.

- ② 제1항에 따라 개인정보 보호 교육계획을 수립할 때에는 다음 각 호의 사항이 포함되어야 한다.
1. 교육목적
 2. 교육대상
 3. 교육내용
 4. 교육일정
 5. 교육방법
 6. 그 밖에 개인정보 보호 교육을 위하여 필요한 사항
- ③ 교육부장관은 개인정보 보호책임자, 개인정보 보호담당자에게 개인정보보호에 필요한 교육을 실시하여야 한다. 다만, 유·초·중·고 등 소관 교육기관의 교육은 관할하는 시·도교육감이 실시한다.
- ④ 개인정보처리자는 개인정보취급자 등을 대상으로 개인정보보호에 필요한 교육을 실시하여야 한다.
- ⑤ 개인정보 보호책임자는 신규 채용자, 전입자에게 개인정보 보호 교육을 하여야 한다.

- ⑥ 개인정보 보호책임자는 개인정보 관련 전문기관 교육 및 기술 세미나 참석을 장려하고 신규로 지정된 개인정보 보호담당자가 신규 발령일로부터 1년 이내에 15시간 이상의 개인정보보호 교육(정보보안 교육을 포함하되 5시간을 초과할 수 없다)을 받도록 노력하여야 한다.

제12조(개인정보보호 수준진단) ① 교육부장관은 자율적인 개인정보 보호 활동을 촉진하고 지원하기 위하여 교육기관을 대상으로 개인정보보호 수준진단을 실시할 수 있다.
 ② 시·도교육감은 소관 교육기관을 대상으로 개인정보보호 수준진단을 실시할 수 있다.
 ③ 교육부장관 및 시·도교육감은 소관 교육기관의 수준진단 결과에 따라 제8조제4항에 따라 지도·점검을 할 수 있다.

제13조(개인정보 유출등의 신고) ① 개인정보처리자는 1명이라도 정보주체에 관한 개인정보의 유출등이 발생한 것을 알게 되었을 때에는 유출등 내용 및 조치결과를 72시간 내에 상급기관을 경유하여 교육부에 신고하여야 한다. 다만 다음 각 호의 어느 하나에 해당하는 경우에는 72시간 내에 상급기관을 경유하여 교육부 신고와 동시에 개인정보 보호위원회(이하 "보호위원회"라 한다) 또는 시행령 제40조제3항의 전문기관에 신고하여야 한다.

1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
 2. 민감정보, 고유식별정보가 유출등이 된 경우
 3. 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우
- ② 제1항에도 불구하고 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.
- ③ 제1항에 따른 신고는 별지 제5호서식에 따른 개인정보 유출등 신고서를 통하여 하여야 한다.
- ④ 개인정보처리자는 전자우편, 모사전송 또는 교육부 개인정보보호 포털(privacy.moe.go.kr) 및 개인정보 포털(www.privacy.go.kr)을 통하여 유출등 신고를 할 시간적 여유가 없거나 그 밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 법 제34조제1항 각 호의 사항을 신고한 후, 별지 제5호서식에 따른 개인정보 유출등 신고서를 제출할 수 있다.
- ⑤ 개인정보처리자는 개인정보 유출등 신고를 하려는 경우에 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 신고하고 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다.

제14조(개인정보의 유출등 조사) ① 개인정보처리자는 개인정보 유출등이 발생되었을 경우 유출등의 원인을 조사하고 다음 각 호의 사항을 준수해야 한다.

1. 유출등의 원인 보완 및 재발방지 조치계획 수립·이행
 2. 개인정보취급자(전직원) 대상 사례 전파 및 재발방지 교육
 3. 그 밖에 개인정보의 유출등 방지를 위해 필요하다고 판단되는 사항
- ② 교육부장관 및 시·도교육감은 소관 교육기관으로부터 개인정보 유출등 신고를 받고

필요하다고 판단되는 경우 관련 자료제출을 요구하거나 해당 기관, 해당 유출등의 원인 및 그와 관련한 관계인에 대해 제9조에 따른 전문기관과 함께 조사를 실시하고 법 제34조제1항 각 호에 따른 사항을 요구할 수 있다. 해당 요구를 받은 개인정보처리자 등은 특별한 사정이 없으면 이에 응하여야 한다.

- ③ 개인정보의 유출등 조사를 위해서는 정보주체 및 유출등 사고 관련자의 사생활 침해를 최소화하는 방법(익명처리 등)으로 처리될 수 있도록 노력하여야 한다.

제15조(개인정보파일의 등록 주체) ① 개인정보파일을 운용하는 교육기관의 개인정보 보호책임자는 그 현황을 보호위원회 개인정보보호 종합지원시스템에 등록하여야 한다.

- ② 교육부는 보호위원회에 직접 등록하여야 한다.

- ③ 교육기관은 상급기관을 통하여 보호위원회에 등록하여야 한다.

제16조(개인정보파일 등록 및 변경 확인) 개인정보파일의 등록 또는 변경 신청을 받은 상급기관은 보호위원회 개인정보보호 종합지원시스템을 확인하여 60일 이내에 처리하여야 한다.

제17조(개인정보파일 표준목록 등록과 관리) 개인정보 보호책임자가 제15조제1항에 따라 개인정보파일을 등록하는 때에는 교육부가 제공하는 ‘개인정보파일 표준목록’에 따라 등록하여야 한다.

제18조(개인정보파일대장 작성) 교육기관은 1개의 개인정보파일에 1개의 개인정보파일대장을 작성하여야 한다.

제19조(개인정보파일 이용·제공 관리) 교육기관은 법 제18조제2항 각 호에 따라 제3자가 개인정보파일의 이용·제공을 요청한 경우에는 각각의 이용·제공 가능 여부를 확인하고 별지 제8호서식의 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하여 관리하여야 한다.

제20조(개인정보파일 현황 공개 및 방법) 교육기관의 개인정보 보호책임자는 개인정보파일의 보유·파기 현황을 주기적으로 조사하여 그 결과를 해당 기관의 개인정보 처리방침에 반영하여 관리해야 한다.

제21조(등록·파기에 대한 개선권고 및 점검) ① 교육기관의 개인정보 보호책임자는 제20조에 따라 개인정보파일의 보유·파기 현황을 조사한 결과 개인정보파일이 과다하게 운용되고 있다고 판단하거나 제17조에 따라 교육부가 제공하는 개인정보 파일 표준목록에 따라 등록되지 않은 파일이 있는 것으로 확인되는 경우에는 그 개선을 권고할 수 있다.

- ② 교육부장관 및 시·도교육감은 소관 교육기관의 개인정보파일의 등록사항과 그 내용을 검토하고 다음 각 호의 어느 하나에 해당되는 경우에는 법 제32조제3항에 따라 교육기관의 개인정보 보호책임자에게 개선을 권고할 수 있다.

1. 개인정보파일이 과다하게 운용된다고 판단되는 경우
2. 등록하지 않은 개인정보파일이 있는 경우

3. 개인정보파일 등록 사실이 삭제되었음에도 불구하고 개인정보파일을 계속 보유하고 있는 경우
 4. 개인정보 영향평가를 받은 개인정보파일을 보유하고 있음에도 그 결과를 등록사항에 포함시키지 않은 경우
 5. 그 밖에 법 제32조에 따른 개인정보파일의 등록 및 공개에 위반되는 사항이 있다고 판단되는 경우
- ③ 교육부장관 및 시·도교육감은 소관 교육기관의 개인정보파일 등록·파기 현황에 대한 점검을 실시할 수 있다.

제22조(개인정보의 파기 방법 및 절차) 개인정보 보호책임자는 개인정보 파기 절차, 파기 여부의 확인 등을 포함하는 파기계획을 수립하고 주기적으로 점검하는 등 필요한 조치를 하여야 한다. 단, 분야별책임자를 지정한 경우에는 분야별책임자가 개인정보 보호책임자의 승인을 득한 후 이를 수행할 수 있다.

제23조(재검토기한) 교육부장관은 이 훈령에 대하여 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2023년 12월 1일 기준으로 매 3년이 되는 시점(매 3년째의 11월 30일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제476호, 2024.02.07.>

이 훈령은 발령한 날부터 시행한다.

교육분야 개인정보 유출등 사고 대응 매뉴얼

2024. 3.

**KERIS****한국교육학술정보원**
KOREA EDUCATION AND RESEARCH INFORMATION SERVICE

목 차

1. 개요

1.1 목적	1
1.2 법적 근거	1
1.3 용어 정의	1
1.4 단계별 프로세스(업무 절차)	3
1.5 유출등 대응 업무수행 체계	4

2. 개인정보 유출등 사고 대응 조치 및 피해 구제 방법

2.1 유출등 통지 절차	6
2.2 유출등 신고 절차 및 방법	8
2.3 현장 혼합 최소화 조치	10
2.4 정보주체 민원 대응 조치	11
2.5 정보주체 불안 해소 조치	11
2.6 피해자 구제 조치	12

3. 개인정보 유출등 원인별 보호 조치

3.1 해킹	13
3.2 내부자 유출	11
3.3 이메일 오발송	12
3.4 개인정보 노출	12

4. 개인정보 유출등 사고 재발방지 조치

4.1 유출등 원인 보완 및 재발방지 조치 계획 수립·이행	15
4.2 재발방지 교육 및 사례 전파	15

【참고자료】

〔붙임 1〕 개인정보 유출등 신고서 (양식)	16
〔붙임 2〕 개인정보 유출등 신고 조치확인서 (양식)	18
〔붙임 3〕 개인정보 유출등에 따른 2차 피해유형 및 대응요령	24
〔붙임 4〕 교육부 개인정보보호 포털 유출등 신고 절차	27
〔붙임 5〕 유관기관 관련 연락처	32

- 본 매뉴얼은 「개인정보 보호법」의 적용을 받는 개인정보처리자를 대상으로 합니다.

적용대상

업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통해 개인정보를 처리하는 교육기관의 모든 개인정보처리자

교육기관 즉, 교육부(소속기관 포함), 교육청(직속기관 포함), 교육지원청, 초·중·고(각급학교 포함), 대학, 국·공립대학병원, 교육부 산하 공공기관이 대상입니다.

- 본 매뉴얼은 「표준 개인정보 보호지침」(개인정보보호위원회 고시 제2024-1호, 2024.1.4.) 제29조(개인정보 유출등 사고 대응 매뉴얼 등)에 따라,
 - 개인정보 유출등 사고와 관련하여 신속한 대응과 그 피해를 최소화하기 위한 최소한의 사항을 안내하고 있습니다.

관계법령

표준 개인정보 보호지침

제29조(개인정보 유출등 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출등 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출등 대응 매뉴얼」을 마련하여야 한다.

1. 법 제2조제6호에 따른 공공기관
2. 그 밖에 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자

② 제1항에 따른 개인정보 유출등 대응 매뉴얼에는 유출등 통지·조치 절차, 영업점·인터넷회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 개인정보처리자는 개인정보 유출등에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

- 따라서 각 교육기관은 본 매뉴얼을 조직의 특성 및 환경에 맞게 보완하여 사용하시기 바랍니다.

개인정보 유출등 대응 절차(요약)

1. 개인정보 유출등 대응 체계 구축

개인정보 유출등 사고 대응팀	개인정보 보호책임자	개인정보 유출등 대응 총괄 지휘, 개인정보 유출등 사고 대응팀 구성·운영
	개인정보 보호담당자	정보주체에게 개인정보 유출 통지, 교육부 또는 개인정보위에 개인정보 유출 신고
	정보보호 담당자	교육부 및 과기정통부에 침해사고 신고, 사고경위 분석, 시스템 복구 등 침해대응
	담당·지원 부서	정부, 언론사, 이용자 민원 대응, 이용자 피해구제 분쟁조정 기구 안내

2. 피해 최소화 및 긴급 조치

유형	대응 방안
해킹	시스템 분리/차단 조치, 로그 등 증거자료 확보, 유출 원인 분석, 정보주체 및 개인정보취급자 비밀번호 변경 등
내부자	유출 경로 확인, 유출에 활용된 컴퓨터/USB/이메일/출력물 등 확보, 취급자의 접근권한 확인, 비정상 접근 경로 차단 등
이메일	발송 이메일 즉시 회수, 수신자에게 오발송 메일 삭제 요청, 대용량 메일 서버 운영자에게 파일 삭제 요청, 파일 전송시 암호화 등
노출	검색엔진 : 노출된 개인정보 삭제 요청, 로봇(크롤링 등)배제 규칙 적용 등 시스템 오류 : 소스 코드, 서버 설정 등 원인 파악 및 수정 등

3. 개인정보 유출등 통지 및 신고

근거법률		개인정보 보호법	교육부 개인정보 보호지침
		제34조(개인정보 유출 등의 통지·신고)	제13조(개인정보 유출등의 신고)
유출 통지	규모	1명 이상	
	시점	72시간 이내(유출등이 되었음을 알게 되었을 때)	
	방법	홈페이지, 서면 등의 방법으로 개별 통지	
	항목	① 유출등이 된 개인정보의 항목, ② 유출등이 된 시점과 그 경위 ③ 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법, ④ 개인정보처리자의 대응조치 및 피해구제 절차, ⑤ 피해 신고·상담 부서 및 연락처 등	
유출 신고	규모	① 1천명 이상 ② 1명 이상 민감정보, 고유식별정보 유출 등 ③ 외부로부터의 불법적인 접근에 의한 개인정보 유출 등	1명 이상
	시점	72시간 이내(유출등이 되었음을 알게 되었을 때)	
	기관	개인정보보호위원회 또는 한국인터넷진흥원 (privacy.go.kr)	교육부 또는 한국교육학술정보원 (privacy.moe.go.kr)

4. 피해 구제 및 재발 방지

정보주체 피해 구제	<ul style="list-style-type: none"> - 홈페이지 등을 통한 유출여부 조회 기능 제공 - 유출로 인한 피해 신고, 접수, 상담, 문의 등 각종 민원대응 방안 마련 - 유출 대응 현장 혼란 최소화 방안 강구 - 보이스피싱 등 2차 피해 방지를 위한 유의 사항 안내 - 피해 보상 계획 마련 및 관련 제도 안내 등
재발 방지 대책 마련	<ul style="list-style-type: none"> - 개인정보 유출 원인 등에 대한 개선방안 마련 - 취급자 대상 개인정보보호 교육 실시 - 홈페이지 취약점 제거 등 개인정보 안전조치 강화 등

1 개요

1.1 목적

- ‘개인정보 유출등 사고 대응 매뉴얼’은 교육기관이 ‘개인정보 보호법’ 및 시행령, 관련 지침 따라 개인정보 유출등 관련 사고에 대하여 신속하고 체계적인 대응을 목적으로 한다.

※ 관련근거 : 표준 개인정보 보호지침 제29조(개인정보 유출등 사고 대응 매뉴얼 등)

1.2 법적 근거

- 개인정보 보호법 및 시행령
- 표준 개인정보 보호지침, 개인정보의 안전성 확보조치 기준
- 교육부 개인정보 보호지침

1.3 용어 정의

개인정보 유출의 개념	
표준 개인정보 보호지침 제25조(개인정보의 유출등) 개인정보의 분실·도난·유출(이하 "유출등"이라 한다)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말한다.	

용 어	정 의
유출등 사고 대응팀	•개인정보 유출등 사고 발생에 따른 사고의 분석, 처리지원, 사후 복구, 사후 예방조치 등을 주요 업무로 하는 개인정보보호 담당부서를 말함
개인정보 보호책임자	•개인정보 보호법 제31조에 근거하여 개인정보 처리 업무를 총괄하는 자 •개인정보 보호담당자를 임명하여 유출등 사고 발생 시 본 절차에 따라 대응토록 함
개인정보 보호담당자	•개인정보 보호책임자의 지정을 받아 개인정보 보호업무를 수행하는 자
분야별 책임자	•개인정보 보호책임자의 지휘·감독을 받아 각 업무부서의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자를 말함
분야별 담당자	•개인정보보호 분야별 책임자의 지정을 받아 개인정보 보호업무를 수행하는 자
개인정보취급자	•개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말함

대법원 2014. 5. 16. 선고 2011다24555, 24562판결

개인정보의 누출이란 개인정보가 해당 정보통신서비스 제공자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 의미하는바, 어느 개인정보가 정보통신서비스 제공자의 관리·통제하에 있고 그 개인정보가 제3자에게 실제 열람되거나 접근되지 아니한 상태라면, 정보통신서비스 제공자의 기술적·관리적 보호조치에 미흡한 점이 있어서 제3자가 인터넷상 특정 사이트를 통해 정보통신서비스 제공자가 보관하고 있는 개인정보에 접근할 수 있는 상태에 놓여 있었다고 하더라도 그것만으로 바로 개인정보가 정보통신서비스 제공자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 되었다고 할 수는 없다.

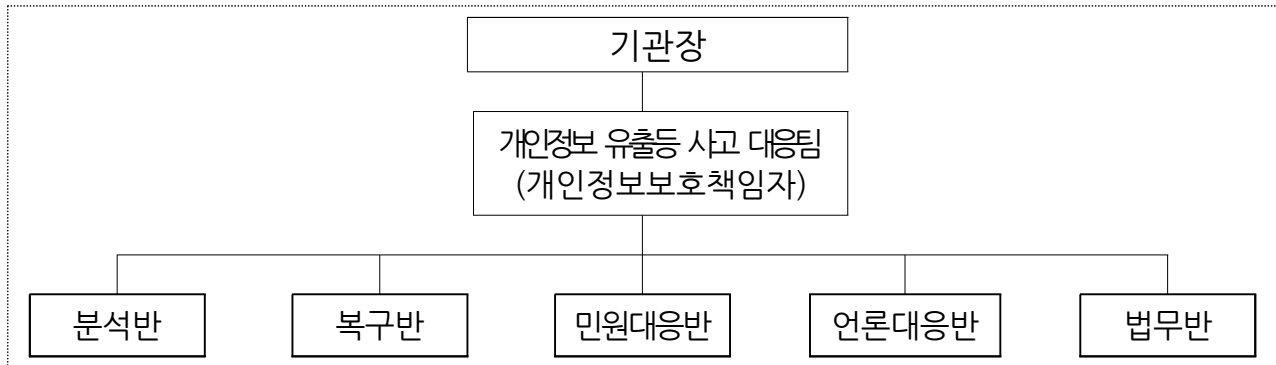
1.4 단계별 프로세스(업무 절차)

- 기관의 개인정보 처리 형태에 따라 조직체계, 업무분장, 비상연락체계가 상이하므로 본 양식을 참고하여 작성(다음 예시가 의무사항은 아님)

단계	상세 업무	비고
사고인지 및 긴급조치	<ul style="list-style-type: none"> ○ 개인정보 유출등 사고 인지 및 신고 접수 <ul style="list-style-type: none"> - 유출등 사고 발생이 의심되는 경우, 지체없이 개인정보 보호담당자에게 신고 ○ 개인정보 보호담당자는 사고 내용 등에 대해 개인정보 보호책임자에게 보고 ○ 유출등 사고 대응반 소집 및 유관기관 협조체계 확인 ○ 피해 최소화를 위한 긴급조치 수행 <ul style="list-style-type: none"> - 유출등이 된 개인정보 비공개 또는 삭제 조치 - 유출등 접속 경로 차단, 취약점 점검·보완 등 긴급조치, 재발방지 조치 등 	
정보주체 유출등 통지	<ul style="list-style-type: none"> ○ 정보주체에게 개인정보 유출등 사실 통지(72시간 이내) <ul style="list-style-type: none"> - 유출등이 된 개인정보의 항목, 유출등이 된 시점과 그 경위, 피해 구제절차 등 	세부내용 2.1 참고
개인정보 유출등 신고	<ul style="list-style-type: none"> ○ 1명 이상의 개인정보 유출등 발생 시 교육부(privacy.moe.go.kr)에 유출 신고 ○ ①1천명 이상 유출등이 발생하거나, ②민감정보·고유식별정보 1건 이상 또는 ③외부로부터의 불법적인 접근에 의해 1건 이상 유출등 발생 시 교육부 및 개인정보보호위원회(한국인터넷진흥원, privacy.go.kr)에 유출 신고 	세부내용 2.2 참고
사고분석	<ul style="list-style-type: none"> ○ 유출등 사고 대응반의 조사 및 분석 <ul style="list-style-type: none"> - 사고 원인 분석, 유출등 규모 확인, 사고 원인에 대한 조치 등 	
민원대응	<ul style="list-style-type: none"> ○ 민원대응을 위한 별도의 온·오프라인 창구 개설·운영 <ul style="list-style-type: none"> - 피해자 구제방안, 수사 진행상황 등에 대한 답변 방향 결정 및 응대 - 2차 피해 방지를 위한 조치방법 안내 등 고객 불안 해소 조치 및 피해구제 절차 안내 	세부내용 2.4~2.6 참고
유출등 사고 결과보고	<ul style="list-style-type: none"> ○ 개인정보 유출등 사고 결과보고서 작성 및 보고 	
개선 및 이행점검	<ul style="list-style-type: none"> ○ 개인정보 유출등 사고 사례 전파 교육 및 개선 대책 시행(재발방지) 	

1.5 유출등 대응 업무수행 체계

○ 조직체계(예시)



○ 업무분장

조직	담당 업무
기관장	<ul style="list-style-type: none"> 유출등 대응 관련 방향성 제시 등 의사 결정
개인정보보호 책임자	<ul style="list-style-type: none"> 유출등 사고 대응 총괄 지휘 및 사고 대응팀 구성·운영
개인정보 유출등 사고 대응팀	<ul style="list-style-type: none"> 유출등 사고 인지, 접수, 전파 유출등 사고 대응 절차 수립 정보주체에게 유출등 사실 통지 교육부 및 개인정보위에 유출등 신고
분석반	<ul style="list-style-type: none"> 유출등 사실 확인, 조사 및 원인 분석 사고내용 세부조사
복구반	<ul style="list-style-type: none"> 외부요인에 의한 유출의 경우, 유관 기관과 협조하여 사고 처리 지원 시스템 복구 및 백업(유지보수/협력업체 포함)
민원대응반 (온라인, 오프라인)	<ul style="list-style-type: none"> 개별 통지문 안내에 따른 후속업무(민원 등) 진행 상담센터, 소비자보호 방안 마련(필요시 유관부서와 협조)
언론대응반	<ul style="list-style-type: none"> 유출등 사고 관련 대외기관(언론사 등) 대응 유출등 사고 안내문 문구 최종 검토
법무반	<ul style="list-style-type: none"> 법률상 대응방안, 의사결정 사항 등 정책적 판단사항 검토 및 결정 유출등 사고 관련 수사기관 경과사항 대응 및 대책반 공유

○ 비상연락망

- 개인정보 유출등 사고 대응팀

조직별	담당자	전화번호	이메일
개인정보보호책임자	성함, 직책 명시	02-000-0000 (010-000-0000)	000@ooo.kr
분석반	○○팀장	02-000-0000 (010-000-0000)	000@ooo.kr
복구반	○○팀장	02-000-0000 (010-000-0000)	000@ooo.kr
민원대응반	○○팀장	02-000-0000 (010-000-0000)	000@ooo.kr
언론대응반	○○팀장	02-000-0000 (010-000-0000)	000@ooo.kr
법무반	○○팀장	02-000-0000 (010-000-0000)	000@ooo.kr

- 협력업체/유지보수업체

업체명	담당 시스템	담당자	전화번호	이메일
○○기업	○○시스템	성함, 직책 명시	00-000-0000 (010-000-0000)	000@ooo.kr
○○기업	○○시스템	성함, 직책 명시	00-000-0000 (010-000-0000)	000@ooo.kr
○○기업	○○시스템	성함, 직책 명시	00-000-0000 (010-000-0000)	000@ooo.kr
○○기업	○○시스템	성함, 직책 명시	00-000-0000 (010-000-0000)	000@ooo.kr
○○기업	○○시스템	성함, 직책 명시	00-000-0000 (010-000-0000)	000@ooo.kr

2 개인정보 유출등 사고 대응 조치 및 피해 구제 방법

2.1 유출등 통지·조치 절차

가이드

- 개인정보처리자는 「개인정보 보호법」 제34조제1항에 따른 통지 절차를 마련하고 이에 대한 내용을 기술
- 개인정보처리자는 개인정보 유출등 사고 규모에 따라 신고 관련 절차를 마련하고 이에 대한 내용을 기술
- 개인정보처리자는 정보주체가 홈페이지 등을 통해 자신의 개인정보가 유출등이 되었는지 확인할 수 있는 절차를 만들고 이에 대한 내용을 기술
- 개인정보 처리 업무 위탁 시, 1차적인 유출등 신고 및 통지 의무는 위탁자에게 있으므로, 유출등 사고 발생 시 수탁자와의 대응 절차를 마련하고 이에 대한 내용을 기술

- 개인정보 유출등 사고 대응팀은 유출등이 된 규모 및 관련 사항을 확인하여 유출등 통지 방법*에 따라 정보주체들에게 개인정보 유출등 통지

* 본 매뉴얼 내 [개인정보 유출등 대응 절차(요약) - 3. 개인정보 유출등 통지 및 신고] 참고

- 통지 항목 : ① 유출등이 된 개인정보의 항목, ② 유출등이 된 시점과 그 경위, ③ 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법, ④ 개인정보처리자의 대응조치 및 피해구제 절차, ⑤ 피해 신고·상담 부서 및 연락처 등

- 수탁사업자가 수탁 업무를 처리하는 과정에서 개인정보가 유출등이 된 경우 즉시 위탁자에게 보고하도록 표준 개인정보처리위탁 계약서에 명시하고, 수탁사업자로부터 보고 받은 시점에서 지체 없이 유출 통지

- 1명 이상 개인정보 유출등이 되었음을 알게 되었을 때에는 서면 등의 방법으로 72시간 이내에 유출등 통지 항목 5개를 정보주체에게 안내

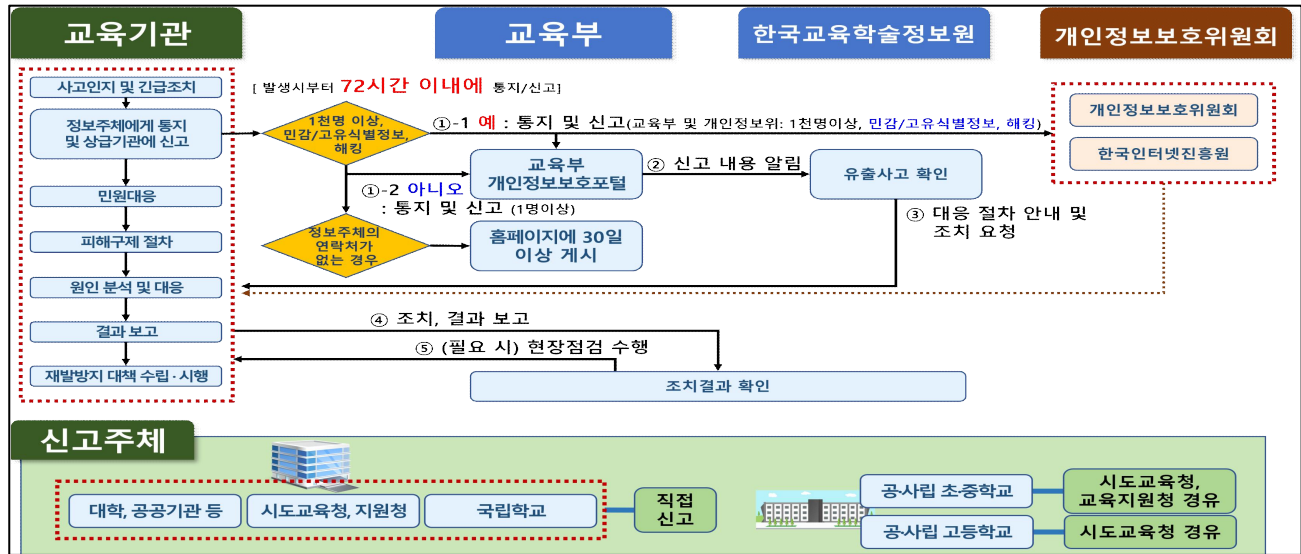
- 정보주체의 연락처를 알 수 없는 경우 인터넷 홈페이지에 통지항목 5개를 30일 이상 게시하는 것으로 정보주체 유출등 통지 의무를 갈음할 수 있음

개인정보 유출등 통지문(예시)

통지문(예시)	작성 준수사항
<p style="text-align: center;">개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.</p> <p>❶ 고객님의 개인정보는 ○○○○년 ○○월 ○○일 해커에 의한 홈페이지 내 악성코드가 삽입되어 ○○건이 유출된 것으로 확인되었습니다. 유출된 정확한 일시는 에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.</p> <p>❷ 유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 휴대전화번호 총 5개 항목입니다.</p> <p>❸ 유출 사실을 인지한 후 해당 악성코드는 즉시 삭제하였으며, 해커가 접속한 해당 IP와 우회 접속한 IP를 차단하고, 추가적인 홈페이지 취약점 점검과 보완 조치를 하였습니다. 더불어 침입방지시스템을 추가 도입하여 24시간 모니터링을 수행하고 있습니다.</p> <p>❹ 이번 사고로 인해 유출된 개인정보를 이용하여 웹사이트 명의도용, 보이스피싱, 파밍 등 2차 피해의 우려가 있으므로 혹시 모를 피해를 막기 위하여 고객님의 비밀번호를 변경하여 주시기 바랍니다.</p> <p>❺ 비밀번호 변경하기</p> <p>❻ 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 아래 피해 등 접수 담당부서로 연락해주시기 바랍니다.</p> <p>▶ 피해 등 접수 담당부서: ○○○○팀 (000-123-0000)</p> <p>▶ 피해 등 접수 e-메일: ○○○○@oooo.co.kr</p> <p style="text-align: right;">○○○교육기관</p> <p>⑦ 개인정보 유출 여부 조회하기</p>	<p>❶ 개인정보 유출 등이 발생한 시점과 확인한 유출 건수를 누구나 이해할 수 있게 상세하게 설명 ☞ 잘못된 사례: '회원정보 일부' 등</p> <p>❷ 유출된 개인정보 항목은 누락없이 모두 나열하여야 함 ☞ 잘못된 사례: '등'으로 생략하거나, 회사 전화 번호, 집전화번호를 '전화번호'로 통칭</p> <p>❸ 개인정보처리자 등의 대응조치 내용 접속경로 차단 등 예시된 항목 외에도 망분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근통제, 시스템 모니터링 강화 등 조치한 사항을 설명</p> <p>❹ 이용자가 취할 수 있는 조치 방법 유출된 개인정보, 경로 등에 따라 발생할 수 있는 피해를 추정하여 가능한 피해예방 조치를 모두 안내(예: 보이스피싱, 피싱메일, 불법TM, 스팸문자 등)</p> <p>❺ 이용자의 비밀번호 변경페이지로 연결</p> <p>❻ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처 전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내</p> <p>⑦ 이용자가 자신의 개인정보 유출여부를 조회할 수 있도록 절차를 마련</p>

2.2 유출등 신고 절차 및 방법

○ 유출등 신고 절차



○ 유출등 신고 방법

구분	내용
신고대상	<ul style="list-style-type: none"> ▶ 개인정보가 1천명 이상 유출등이 됐거나, 민감정보·고유식별정보 및 외부로부터의 불법적인 접근에 의해 1건이라도 유출등이 된 경우는 교육부 및 개인정보위 (또는 한국인터넷진흥원)에 신고 ▶ 1명 이상 유출등이 된 경우 상급기관을 경유하여 교육부에 신고 <ul style="list-style-type: none"> ※ 공·사립 초등학교·중학교는 교육지원청, 교육청, 교육부에 신고 ※ 고등학교, 교육지원청, 교육청 직속기관 등은 교육청, 교육부에 신고 ※ 국립학교, 대학, 교육청, 공공기관 등은 교육부에 신고
신고시기	<ul style="list-style-type: none"> ▶ 유출등이 되었음을 알게 된 후 72시간 이내 <ul style="list-style-type: none"> ※ 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있음
신고방법	<ul style="list-style-type: none"> ▶ 교육부(privacy.moe.go.kr) 및 개인정보보호위원회(privacy.go.kr) 홈페이지를 통해 유출등 신고서 제출 <ul style="list-style-type: none"> ※ 부득이한 경우 전자우편 등을 통해 개인정보 유출 신고서 제출 ▶ 시간적 여유가 없거나 특별한 사정이 있는 경우 상급기관과 교육부에 동시에 신고하며 유출등 신고서 제출
신고내용	<ul style="list-style-type: none"> ▶ 기관명, 통지여부, 유출등이 된 개인정보 항목·규모, 유출등 시점·경위, 유출 등 피해 최소화 대책·조치 및 결과, 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차, 담당부서·담당자 연락처 등 <ul style="list-style-type: none"> ※ 정보주체에 대한 유출등 통지 결과 및 피해 최소화를 위한 긴급 조치 내용이 포함되도록 해야 함
신고양식	▶ [붙임 1] 개인정보 유출등 신고서 (양식)

※ **조치결과**는 교육부 개인정보 보호지침 제14조(개인정보의 유출등 조사)에 따라 [붙임2] 개인정보 유출등 신고 조치확인서 작성 및 제출(moeprivacy@○○○대학교.or.kr)

개인정보 유출등 신고서 작성 방법

유출 등 신고서 양식	작성 방법
❶ 유출등이 된 개인정보 항목	<ul style="list-style-type: none"> - 유출 등이 된 개인정보 항목을 모두 기재해야 하며, ‘등’과 같이 일부 생략하거나 휴대전화번호와 집 전화번호를 ‘전화번호’로 기재하여서는 안됨 - 유출 등이 된 개인정보의 모든 항목을 적어야 하며, 유출 등 규모도 현 시점에서 파악된 내용을 모두 작성
❷ 유출등이 된 시점과 그 경위	<ul style="list-style-type: none"> - 유출 등 시점, 인지시점을 명확히 구분하여 날짜 및 시간 모두 작성해야 하며, 유출 등 경위와 인지경위를 포함
❸ 정보주체가 취할 수 있는 피해 최소화 조치	<ul style="list-style-type: none"> - 개인정보 유출 등으로 발생 가능한 스팸 문자, 보이스피싱, 금융사기와 같은 2차적인 피해 방지를 위해 이용자가 할 수 있는 조치를 기재(예: 비밀번호 변경 등)
❹ 개인정보처리자 대응조치 및 피해 구제절차	<ul style="list-style-type: none"> - 유출 등 사실을 안 후 긴급히 조치한 내용과 향후 이용자의 피해구제를 위한 계획 및 절차를 기재 ex) 경찰에 신고, 일시적 홈페이지 로그인 차단(홈페이지 해킹일 경우) 등
❺ 정보주체가 피해 신고·상담 등을 접수할 수 있는 부서 및 연락처	<ul style="list-style-type: none"> - 실제 신고 접수 및 상담이 가능한 전담 처리부서와 해당 담당자 연락처를 기재
❻ 기타	<ul style="list-style-type: none"> - 유출 등이 된 기관명, 사업자번호, 사업자 주소, 웹사이트 주소 등 기재

2.3 현장 혼잡 최소화 조치

가이드

- 유출 대응 현장에서의 긴급·돌발 상황 발생 등에 따른 현장 혼잡 최소화를 위한 절차를 마련하고 이에 대한 내용을 기술

- 개인정보 유출등 사고 대응팀은 0층 00회의실에 오프라인 창구를 개설
 - 전화, 메일, 홈페이지, SNS 등 한 가지 이상의 채널을 선택하여 단일화된 민원대응 창구를 구축

구분	채널	상세 내용
오프라인	3층 00회의실	
온라인 중 택 1	전화	02-000-0000
	메일	privacy@ooo.ooo
	홈페이지	https://ooo.ooo
	SNS	#0000

- 정보주체가 개인정보 유출 여부 등을 확인가능 하도록 별도의 홈페이지 등을 제공
 - ※ 개인정보 유출 결과는 전체 공지가 아닌 핸드폰 인증 등을 통해 정보주체가 개별 본인 확인 후 개인정보 유출 결과 조회 지원
- 복구반은 유출등이 된 시스템의 이용을 제한하고 별도의 임시 시스템 구축을 통하여 기관의 업무 혼잡 방지
 - ※ 현장에서 물리적 시스템 장애, 파괴 그리고 불필요한 인력 등으로 인하여 개인정보가 분실, 도난, 훼손되지 않도록 주의
- 분석반은 대외 수사 기관에 협조할 수 있는 전담 인력 구성 및 대응
- 시스템 오류 등 서비스 장애로 인한 정보주체의 민원 발생 시 유관부서와 협의하여 해결

2.4 정보주체 민원 대응 조치

가이드

- 개인정보처리자는 정보주체 민원을 처리할 수 있는 체계를 만들고 이에 대한 내용을 기술

- 민원대응반은 유관부서(언론대응반, 법무반)와 협의하여 피해자 구제방안, 수사 진행상황 등에 대한 외부 질의 답변 방향 결정
- 협의 방안을 토대로 민원대응 매뉴얼 작성 및 배포
- 민원대응 전담 인력·회선 확보 및 대응 매뉴얼 교육
- 대외적 접촉창구는 민원대응반으로 단일화하여 기관 및 대민 000홈페이지(<http://ooo.com>)에 공지하고 타 팀에서 외부로부터 개인정보 유출등 관련 질문을 받으면 최대한 민원대응반으로 연결
- 기본적으로 민원대응반을 통해서 1차 민원 대응을 하되, 별도 대응이 필요한 경우 해당 부서에서 응대하도록 안내

문의별	담당부서
유출 확인 문의 대응	00 팀 or 00반
피해구제 관련 문의 대응	00 팀 or 00반
기타(000)	00 팀 or 00반

2.5 정보주체 불안 해소 조치

가이드

- 개인정보처리자는 정보주체가 유출등이 된 개인정보로 인한 불안을 해소할 수 있는 체계를 마련하고 이에 대한 내용을 기술

- 000홈페이지(<http://ooo.com>)에 유출등 피해 최소화를 위해 현재 기관에서 실시하고 있는 노력에 대한 사항 공지(1일 1회 이상 업데이트)
- 비밀번호, 신용카드번호 등 유출 시 비밀번호 변경, 카드 재발급 등

을 할 수 있도록 유출 통지 시 함께 안내

※ 불법스팸대응센터(☎118, spam.kisa.or.kr)를 통하여 불법스팸신고 및 차단 등을 구체적으로 안내

[개인정보 유출 항목별 2차 피해 예방을 위한 안내사항]

항목	세부 안내 사항
아이디, 비밀번호	- 비밀번호 변경 안내
카드번호	- 카드 재발급 절차 안내
다량의 개인정보	- 보이스피싱 등 2차 피해 예방 안내

- (정보주체 요청이 있을 시) 회원 탈퇴 방법 안내 및 정보주체의 개인정보 삭제 조치

2.6 피해자 구제 조치

가이드

- 개인정보처리자는 정보주체가 피해를 구제할 수 있는 절차를 마련하고, 이에 대한 내용을 기술

- 정보주체에게 개인정보 유출등 피해에 대한 피해구제, 상담 등을 문의 할 수 있음을 안내
- 개인정보를 유출당한 사람은 누구든지 개인정보 분쟁조정위원회에 분쟁조정을 신청할 수 있음을 안내(「개인정보 보호법」 제43조제1항)
- 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있음을 안내

3 개인정보 유출등 원인별 보호 조치

3.1 해킹

- 개인정보가 유출된 사실을 알게 된 경우에는 개인정보 추가 유출 방지를 위한 대책을 마련하고 피해를 최소화할 수 있는 조치를 강구하여야 함
 - 유출된 시스템 분리·차단 조치, 관련 로그 등 증거자료 확보, 유출 원인 분석, 이용자 및 개인정보취급자 비밀번호 변경* 등 기술적 보호 조치 강화, 시스템 변경, 기술지원 의뢰 및 복구 등과 같은 긴급 조치를 시행하여야 함
 - * 일방향 암호화되지 않은 비밀번호가 유출되었거나, 해커 등이 이용자의 비밀번호를 알고 있다고 판단되는 경우에는 이용자가 비밀번호를 변경하지 않으면 이용할 수 없도록 하고, 일방향 암호화된 비밀번호가 유출된 경우에도 비밀번호 변경을 유도하여 추가 피해 예방 방지
 - 사고원인 조사 등 조치가 완료된 이후에는 개인정보 유출의 직·간접적인 원인을 즉시 제거하고, 미비한 보호조치 부분을 파악하기 위한 취약점 점검·개선 조치 등을 수행하여야 함

3.2 내부자 유출

- 개인정보 유출자가 개인정보처리시스템에 접속한 이력 및 개인정보 열람·다운로드 등 내역을 확인하여야 함
- 개인정보 유출자의 개인정보처리시스템에 대한 접근·접속 경로 등을 확인하고, 비정상적인* 접속인 경우 접속경로를 확인하여 차단하여야 함
 - * 비인가된 개인정보 처리, 대량의 개인정보에 대한 조화·정정·다운로드·삭제·출력 등
- 개인정보취급자의 개인정보처리시스템 접속계정, 접속권한, 접속기록 등을 검토하여 추가적인 유출 여부를 확인하여야 함
- 개인정보 유출에 활용된 단말기(PC, 스마트폰 등)와 매체(USB, 이메일, 출력물 등)를 회수하고, 필요시 수사기관 등과 협조하여 유출된 개인정보를 회수하기 위한 모든 방법을 강구하여야 함

3.3 이메일 오발송

- 이메일 회수가 가능한 경우에는 즉시 회수 조치하고, 불가능한 경우에는 이메일 수신자에게 오발송 메일의 삭제를 요청*하여야 함
 - * 삭제 요청시 가능한 삭제되었음을 확인할 수 있는 증빙자료 첨부률 같이 요청 (예: 삭제전 목록화면과 삭제후 목록화면을 받음)
- 메일서버 외 첨부파일서버(대용량 메일 등)를 이용하는 경우 첨부파일서버 운영자에게 관련 파일의 삭제를 요청하여야 함

3.4 개인정보 노출

- (외부 검색엔진을 통한 노출의 경우) 노출된 사업자의 웹페이지 삭제를 검토하고, 검색엔진에 노출된 개인정보 삭제를 요청하여야 하며, 필요시 로봇배제 규칙*을 적용하여 외부 검색엔진의 접근을 차단하여야 함
 - * 홈페이지 공개 원칙에 벗어나지 않는 범위 내에서 로봇배제 적용 필요
- (관리자 페이지에 접속하여 노출된 경우) 관리자의 접속 IP를 제한하고, 소스코드를 수정하여 사용자 인증 절차를 추가하여야 함
- (개인정보취급자 부주의로 인한 노출의 경우) 게시글 및 첨부파일 내 개인정보 노출 부분을 삭제 또는 마스킹 처리하여 필요한 경우 다시 게시하여야 함
- (상용 오피스 취약점으로 노출된 경우) S/W버전은 항상 최신버전*으로 이용하며 홈페이지 첨부파일 탑재 시 엑셀 문서는 PDF 등으로 변환**하여 탑재
 - * 엑셀2003 이하에서는 외부링크 취약점이 존재하여 엑셀2007 이상 버전 사용 (관련문서: 교육부 교육정보화과-4027(2017.08.04.))
 - ** 엑셀은 OLE개체, 열·행·시트 숨김, 치환함수, 피벗테이블 등의 다양한 기능으로 사용자가 인지하지 못하는 개인정보 등 노출 발생 가능성 높음

4 개인정보 유출등 사고 재발방지 조치

4.1 유출등 원인 보완 및 재발방지 조치 계획 수립·이행

- 개인정보 유출등 원인별 긴급 보호조치를 취한 이후 보완대책 점검 및 보완 실시
- 중장기 보완대책을 위해 재발방지 계획을 수립하고 수립된 계획에 따라 이행 실시*
- * 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2023-6호)에 따라 개인정보보호 책임자가 내부관리계획의 이행실태를 연 1회 이상 점검·관리할 때 이행 여부 점검 권고

4.2 재발방지 교육 및 사례 전파

- 기관내 구성원 재발방지 교육 실시
 - 개인정보 유출등과 관련된 부서내 모든 취급자는 필수적으로 재발방지 교육 실시
- 개인정보 유출등 사례를 내부공지 등을 통해 기관내 구성원에게 사례를 전파*
 - * 사례전파 시 또 다른 개인정보 유출등이 발생하지 않도록 주의 필요
 - 사례 전파의 구성(예시)

구분	구성 내용
사고 개요	<ul style="list-style-type: none"> • 0년 0월 0일 개인정보 취급자가 홈페이지 게시판 관리 중 개인정보가 포함된 파일을 게시판에 탑재함 • 개인정보가 포함된 파일(엑셀)을 00으로부터 0년 0월 0일 인지하여 해당파일 삭제 조치함 • 개인정보 00건, 포함된 개인정보 항목은 00을 포함한 총 00개가 유출됨
사고 처리 절차	<ul style="list-style-type: none"> • 정보주체에게 유출통지를 하였으며, 홈페이지에 관련 내용을 탑재하여 전파 • 피해 구제 방안 등 정보주체 민원 대응반 구축 • 재발방지대책(교육 등)을 수립
기관 보완 조치 내용	<ul style="list-style-type: none"> • 개인정보 취급자 대상 개인정보 교육 실시 • 개인정보 웹 필터링 시스템 도입으로 개인정보 파일 검출 • 기관 개인정보 체계 강화를 위한 홍보자료 및 사례 전파 실시
향후 기관의 보완 방향	<ul style="list-style-type: none"> • 개인정보 필터링 시스템 등 개인정보 체계 강화를 위한 시스템 구축 • 매년 개인정보 취급자 대상 개인정보 교육 실시
관련 변경 지침	<ul style="list-style-type: none"> • 내부관리 계획 수립 시 개인정보 유출등 재발방지 계획 포함

개인정보 유출등 신고서

기관명					
유출등이 된 개인정보 항목 및 규모					
유출등이 된 시점과 그 경위					
유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등					
개인정보처리자의 대응 조치 및 피해 구제절차					
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처					
유출등 신고(보고) 담당자		성명	부서	직위	연락처
	개인정보 보호책임자				
	담당자 (취급자)				

유출등 신고 접수기관	기관명	담당자명	연락처

개인정보 유출등 신고서(작성 사례)

기관명	교육 고등학교				
유출등이 된 개인정보 항목 및 규모	<ul style="list-style-type: none"> ■ 유출규모: 1,150명(중복제거 후 1,100명) - 교육부 신고(2024.3.22. 13:00), 개인정보위 신고여부(2024.3.22. 12:00) ■ 유출항목: 이름, ID, 비밀번호, 주소, 핸드폰번호, 이메일 				
유출등이 된 시점과 그 경위	<ul style="list-style-type: none"> ■ 사고발생 인지경위(인지시점 포함) - 2024.3.21 10:00 월별 개인정보처리시스템 접속로그 점검 시 특정 IP로부터 다량의 개인정보 다운로드 기록 확인 - 2024.3.21 11:00 개인정보처리시스템의 로그 확인 결과 알 수 없는 개인정보 압축 파일 발견 - 2024.3.21 12:00 IP Table, NAC 등을 확인하여 개인정보를 다운로드한 특정 IP의 PC(용역업체 개인 PC) 확인 ■ 유출 시점 및 경위 - 2024.3.4 20:00 용역업체 A씨는 개인정보처리시스템에 접속하여 다량의 개인정보파일을 생성 후 PC로 다운로드 - 2024.3.4 21:00 PC내 보안 솔루션(NAC 등)에 의하여 상용 이메일 접근 불가 확인 후 개인 이메일 서버로 파일 전송 				
유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등	<ul style="list-style-type: none"> ■ 정보주체가 할 수 있는 피해최소화 방법 ① 2차 피해 방지를 위하여 개인정보 유출 여부 조회(학교 홈페이지 등) ② 유출사고 발생 후 홈페이지 로그인시 개인정보 유출에 따른 비밀번호 변경 ■ 사고발생 후 조치사항 ① 기관 개인정보 유출사고 대응 매뉴얼에 따라 유출사고 대응반 구축 ② 개인정보 유출 접수 창구 및 민원 대응 창구 구축 ③ 유출 항목 및 발생 상황 인지 후 유출 통지문 작성 및 관련 내용 통지, 교육부 개인정보 유출 신고 ④ 유출 원인에 따른 개인정보처리시스템에 대한 접근권한 관리체계 강화 ⑤ 재발방지 대책을 위한 보안강화 계획(안) 수립 				
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처	<ul style="list-style-type: none"> ① 2차 피해 접수를 위한 피해 접수 담당 창구 운영(02-124-2345, abcd@efgf.co.kr) ② 개인정보 유출 관련 개인정보 분쟁조정 신청 창구 안내(1833-6972) 				
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자	김영희	총무과	총무과장	044-123-1234
	개인정보 취급자	홍길동	총무과	담당자	044-123-1234

유출등 신고 접수기관	기관명	담당자명	연락처
	한국교육학술정보원 및 00시도교육청	김철수	044-234-5678

개인정보 유출등 신고 조치확인서(양식)

※ 6하 원칙에 따라 사실 관계를 명확하게 작성(moeprivacy@○○○대학교.or.kr로 제출).

기관명		00학교
정보주체 통지 여부	통지일시	2024.00.00. 12:00
	통지방법	(예시) 전화, 이메일, 서면, 팩스, 홈페이지 공개* 등 * 정보주체의 연락처를 알 수 없는 경우

	필수통지항 목	필수 통지 항목 5가지		포함 여부 확인(O, X)
		① 유출등이 된 개인정보의 항목		○ 또는 X
		② 유출등이 된 시점과 및 그 경위		○ 또는 X
		③ 피해 최소화를 위한 정보주체가 할 수 있는 방법		○ 또는 X
		④ 기관의 대응조치 및 피해구제 절차		○ 또는 X
		⑤ 피해 신고·상담 부서 및 연락처 등		○ 또는 X
		(예시) 이메일, 팩스, 홈페이지 공개 등 내용 이미지 캡처 등 증빙자료 포함		

발생(인지) 일자	2024.00.00.	
발생(인지) 경로	(예시) - 2024.00.00 00:00 KISA에서 통보 - 정보주체가 해당 학과에 신고, ECSC 사고 신고, 민원인 신고 등	

<p>유출등 사실 인지 이후 후속 조치 경과 (유출등 피해 최소화 대책·조치 및 결과)</p>	<p>개인정보 유출등 발생시 아래 사항 준수</p> <ol style="list-style-type: none"> 1. 개인정보 유출등 대응 매뉴얼 구비 <ul style="list-style-type: none"> ※ 법령에 기반하여 최신화 되어있는지 확인 및 개선, 유출등 발생시 매뉴얼대로 즉시 신고 등 대응 2. 유출등 원인 보완 및 재발방지 조치계획 수립·이행 3. 개인정보취급자(전직원) 대상 사례 전파 및 재발방지 교육 <ul style="list-style-type: none"> ※ 개인정보보호 관련 전직원 교육 실시, 특히 신규 직원은 업무 투입 전 개인정보보호 기본 교육 실시 후 투입 4. 그 밖의 개인정보의 유출등 방지를 위해 필요하다고 판단되는 사항 <p>(예시)</p> <ul style="list-style-type: none"> - 2024.00.00 00:00 해당 게시글 삭제 - 2024.00.00 00:00 정보주체에게 메일, 문자로 안내 - 2024.00.00 00:00 홈페이지취약점 점검 수행 - 2024.00.00 00:00 홈페이지에 유출 건 내용 게시 - 2024.00.00 00:00 재발방지대책 수립 - 2024.00.00 00:00 전직원 대상 개인정보 관련 교육
--	---

		- 개인정보 파일 삭제, 오발송된 이메일 회수, 사례전파, 교육실시 등 증빙자료 포함	
교육부 신고 일시 (1명 이상 유출등)		2024. 0. 00. 12:00	[교육부 신고] 유출등 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 신고(교육부 개인정보보호 포털(privacy.moe.go.kr))
개인정보보호위원회 신고 일시 (1천명 이상, 민감정보·고유식별정보, 외부로부터의 불법적인 접근으로 유출등)		2024. 0. 00. 12:00	[교육부 및 개인정보보호위원회 신고] 유출등 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 신고하고(교육부 개인정보보호 포털, 개인정보보호위원회(또는 한국인터넷진흥원, www.privacy.go.kr)에 신고
유출등이된 개인정보	규모(명)	00명	(중복제거) 00명
	항목	이름, 핸드폰번호 ,,,,,	
유출등이 된 시점과		(예시)	

그 경위	<ul style="list-style-type: none"> - 2024.00.00 00:00 메일 잘못 발송, 실수로 개인정보 파일 첨부함 - 2024.00.00 00:00 유출 확인
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차	(예시) 피해구제절차 안내 등

진행사항 또는 향후계획	(예시) 자체 내부 감사 수행, 상위기관 현장 컨설팅 수행, 개인정보보호위원회 점검 예정 등
--------------	--

※ 유출등 신고 후 1주일 이내 조치 확인서를 작성하여 교육부 개인정보보호 포털-유출신고
내역을 수정하여 제출하거나 메일(moeprivacy@○○○대학교.or.kr)로 반드시 제출

개인정보 유출등 신고 조치 확인서(작성 사례)

※ 6하 원칙에 따라 사실 관계를 명확하게 작성(moeprivacy@○○○대학교.or.kr로 제출).

기관명		교육 고등학교													
정보주체 통지 여부	통지일시	2024. 3. 22. (화) 13:00													
	통지방법	이메일 및 유선 전화													
	필수통지항 목	<table><tr><th>필수 통지 항목 5가지</th><th>포함 여부 확인(O, X)</th></tr><tr><td>① 유출등이 된 개인정보의 항목</td><td>○</td></tr><tr><td>② 유출등이 된 시점과 및 그 경위</td><td>○</td></tr><tr><td>③ 피해 최소화를 위한 정보주체가 할 수 있는 방법</td><td>○</td></tr><tr><td>④ 기관의 대응조치 및 피해구제 절차</td><td>○</td></tr><tr><td>⑤ 피해 신고·상담 부서 및 연락처 등</td><td>○</td></tr></table>		필수 통지 항목 5가지	포함 여부 확인(O, X)	① 유출등이 된 개인정보의 항목	○	② 유출등이 된 시점과 및 그 경위	○	③ 피해 최소화를 위한 정보주체가 할 수 있는 방법	○	④ 기관의 대응조치 및 피해구제 절차	○	⑤ 피해 신고·상담 부서 및 연락처 등	○
		필수 통지 항목 5가지	포함 여부 확인(O, X)												
		① 유출등이 된 개인정보의 항목	○												
② 유출등이 된 시점과 및 그 경위		○													
③ 피해 최소화를 위한 정보주체가 할 수 있는 방법		○													
④ 기관의 대응조치 및 피해구제 절차		○													
⑤ 피해 신고·상담 부서 및 연락처 등	○														
<p>개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.</p> <p>고객님의 개인정보는 2023년 3월 4일 00용역업체 직원에 의하여 외부 유출된 사실을 확인하였고, 2차 피해 예방을 위해 경찰청에 즉시 조사를 의뢰하여 수사진행 중입니다.</p> <p>유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 핸드폰번호, 주소 총 6개 항목입니다.</p> <p>유출 사실을 인지한 후 즉시 접속 경로를 차단하고, 취약점 점검과 보완 조치를 완료 하였습니다.</p> <p>현재까지 확인한 바로는 경찰청에서 00용역업체 직원이 외부로 유출된 개인정보는 제3자에게 2차 전달하거나 판매하지 않는 것으로 확인 되었습니다.</p> <p>혹시 모를 피해를 최소화하기 위하여 00시스템과 동일한 ID 및 비밀번호를 사용하고 있는 웹사이트가 있다면, 귀하의 계정정보(ID/비밀번호)를 변경하여 주시기 바랍니다.</p> <p>아울러 피해가 발생하였거나 기타 궁금하신 사항은 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해 드리고, 필요한 조치를 거쳐 손해배상 등의 구제절차를 진행하도록 하겠습니다.</p> <p>앞으로 해당 서비스에 대한 보안 및 개인정보보호 조치 강화 등 개인정보에 대한 관리체계를 개선하고, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.</p> <p>귀하께 실례를 끼쳐 드리게 되어 거듭 진심으로 사과드립니다.</p> <p>▶ 피해 등 접수 담당부서: 0000팀(00-0000-0000) ▶ 피해 등 접수 메일:0000@0000.kr</p> <p>00교육기관 000</p>															
발생(인지) 일자		2024.3.21.													

발생(인지) 경로		<ul style="list-style-type: none"> - 2024.3.21 10:00 월별 개인정보처리시스템 접속로그 점검 시 특정 IP로부터 다량의 개인정보 다운로드 기록 확인 - 2024.3.21 10:30 정보보안 솔루션(방화벽, IPS 등) 로그 분석 결과 외부 해킹 공격은 없음 - 2024.3.21 11:00 개인정보처리시스템의 로그 확인 결과 알 수 없는 개인정보 압축 파일 발견 - 2024.3.21 12:00 IP Table, NAC 등을 확인하여 개인정보를 다운로드한 특정 IP의 PC(용역업체 개인 PC) 확인 - 2024.3.21 13:00 해당 PC 점검 및 유출 내용 확인 	
유출등 사실 인지 이후 후속 조치 경과 (유출등 피해 최소화 대책·조치 및 결과)		<ul style="list-style-type: none"> - 2024.3.21. 12:00 기관 개인정보 유출사고 대응 매뉴얼에 따라 유출사고 대응반 구축 - 2024.3.21. 13:30 개인정보 유출 접수 창구 및 민원 대응 창구 구축 - 2024.3.21. 14:00 유출 항목 및 발생 상황 인지 후 유출 통지문 작성 및 관련 내용 통지, 개인정보보호위원회 및 교육부 개인정보 유출 신고 - 2024.3.21. 14:30 유출 원인에 따른 개인정보처리시스템에 대한 접근권한 관리체계 강화 - 2024.3.21. 15:00 유출 피해 최소화를 위해 추가 확인 정보 공지 및 관련 내용 현행화 실시 - 2024.3.21. 15:30 재발방지 대책을 위한 보안강화 계획(안) 수립 <ul style="list-style-type: none"> 1) 보안 솔루션 도입 2) 전 직원대상 사례 전파 교육 및 개인정보 교육 3) 모든 개인정보처리시스템 대상 안전성 확보 조치 방안 점검 	
교육부 신고 일시 (1명 이상 유출등)		2024. 3. 22. 14:00	[교육부 신고] 유출등 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 신고(교육부 개인정보보호 포털(privacy.moe.go.kr))
개인정보보호위원회 신고 일시 (1천명 이상, 민감정보·고유식별정보, 외부로부터의 불법적인 접근으로 유출등)		2024. 3. 22. 14:00	[교육부 및 개인정보보호위원회 신고] 유출등 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 신고하고(교육부 개인정보보호 포털), 개인정보보호위원회(또는 한국인터넷진흥원, www.privacy.go.kr)에 신고
유출등이 된 개인정보	규모(명)	1,150명	(중복제거) 1,100명(학생 600명, 학부모 200명, 교직원 300명)
	항목	이름, ID, 비밀번호, 주소, 핸드폰번호, 이메일	
유출등이 된 시점과 그 경위		<ul style="list-style-type: none"> - 2024.3.4 20:00 용역업체 A씨는 개인정보처리시스템에 접속하여 다량의 개인정보파일을 생성 후 PC로 다운로드 - 2024.3.4 21:00 PC내 보안 솔루션(NAC 등)에 의하여 상용 이메일 접근 불가 확인 후 개인 이메일 서버로 파일 전송 	
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차		<ul style="list-style-type: none"> ■ 정보주체가 할 수 있는 피해최소화 방법 <ul style="list-style-type: none"> ① 2차 피해 방지를 위하여 개인정보 유출 여부 조회(학교 홈페이지 등) ② 유출사고 발생 후 홈페이지 로그인시 개인정보 유출에 따른 비밀번호 변경 ■ 피해자 구제절차 <ul style="list-style-type: none"> ① 2차 피해 접수를 위한 피해 접수 담당 창구 운영 	

	(02-124-2345, abcd@efgf.co.kr) ② 개인정보 유출 관련 개인정보 분쟁조정 신청 창구 안내(1833-6972)
진행사항 또는 향후계획	① 개인정보 파일 운영 강화를 위한 보안 솔루션 도입(DLP, DRM 등) ② 용역업체(유지보수 등)가 접속할 수 있는 별도의 계정 생성 ③ 개인정보취급자 대상 개인정보보호 교육 강화 ④ 모든 개인정보처리시스템 대상 개인정보 보호법 등 관련 법률에 따라 개인정보 안전성 확보 조치 이행사항 확인 및 관련 내용 점검

※ 유출등 신고 후 1주일 이내 조치 확인서를 작성하여 교육부 개인정보보호 포털-유출신고 내역을 수정하여 제출하거나 메일(moeprivacy@○○○대학교.or.kr)로 반드시 제출

붙임3

개인정보 유출등에 따른 2차 피해유형 및 대응요령

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
금전적	온라인 사기쇼핑	주민등록번호, 카드번호, 유효기간 등	① 카드번호, 유효기간으로 온라인 결제가 가능한 국내외 홈쇼핑 사이트에 접속 ② 홈쇼핑 홈페이지, ARS를 통한 온라인 사기 결제주문	• 신용카드 정지 및 재발급 신청 ※ 신고기관 : 각 카드사, 한국소비자원 소비자상담센터(☎1372) 등
	명의도용을 통한 통신서비스 가입	이름, 주소, 주민등록번호 등	① 유출된 개인정보를 이용하여 휴대전화, 인터넷전화 등 가입 ※ 통신서비스 가입 시 본인확인절차가 있으므로 주민등록증 위조 등 추가적인 불법 행위 수반이 예상됨 ② 불법 가입한 전화번호로 스팸을 발송하여 금전적 이익을 취득함 ※ 명의를 도용당한 사람은 서비스 이용제한을 당하거나 명의도용 소명절차를 밟는 등 피해를 당함	• 한국정보통신진흥협회(KAIT)의 명의도용방지서비스(M-Safer)를 통한 불법 통신서비스 신규가입 여부 확인 ※ 신고기관 : 통신민원조정센터(msafer.or.kr) ※ 명의도용방지서비스(M-Safer) : 통신서비스 신규가입시 이메일·문자로 가입여부 통보
	명의도용을 통한 신용카드 복제	이름, 신용카드 번호, 유효기간 등	① 유출된 개인정보를 이용하여 신용카드 불법 복제 ※ 특수장비를 이용하여 카드번호, 유효기간, 이름 등으로 복제 가능 ② 불법 복제된 카드를 국내외에서 활용하여 상품 결제 등에 악용 ※ 국내외 POS단말기의 경우 마그네틱 부분만을 이용하여 결제 가능	• 신용카드 정지 및 재발급 신청, 이용내역 통지 서비스 가입 ※ 신고기관 : 각 카드사, 경찰, 금융감독원(☎1332)

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
	스미싱	휴대전화번호	① '정보유출 확인 안내' 등 금융기관을 사칭하는 문자메시지에 악성코드(인터넷주소)를 삽입하여 발송 ② 금융기관 사칭 메시지를 받은 피해자가 인터넷주소(URL)를 클릭하면 악성코드에 감염되어 소액결제 피해 및 개인·금융정보 탈취	<ul style="list-style-type: none"> 수상한 문자메시지 삭제 및 메시지 상 링크 클릭하지 않기 또는 카드사 공지 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118)
비금전적	보이스피싱	신용카드번호, 휴대전화, 집전화번호, 집주소 등	① 경찰, 금융감독당국 또는 금융회사 직원을 사칭하여 전화 ② 금융관련 업무 목적 사칭을 통한 개인정보·금융정보 탈취(비밀번호, 보안카드번호 등) ③ 유출된 금융사를 사칭, 개인정보 유출 확인을 빙자하여 ARS를 통해 계좌번호/비밀번호 등 금융정보 입력 요청	<ul style="list-style-type: none"> 수상한 전화 거부 및 각 카드사에서 공지한 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118)
	명의도용을 통한 온라인회원 가입	이름, 이메일, 연락처 등	① 유출된 개인정보를 이용하여 웹사이트 가입 ※ 일부 홈페이지의 경우 이름, 이메일, 연락처만으로 회원가입 가능 ② 명의도용을 통해 본인도 모르는 수십여개의 웹사이트 가입하여 개인정보 불법 이용	<ul style="list-style-type: none"> e프라이버시 클린서비스(www.eprivacy.go.kr)를 활용한 해당 사이트 탈퇴 요청 ※ 신고기관 : 경찰, 불법스팸대응센터(☎118) ※ 국내 사이트로 주민번호 사용 내역이 있는 경우만 가능하며, 주민번호 미사용시 서비스 불가
	휴대전화/이메일 스팸발송	휴대전화 번호, 이메일 주소 등	① 유출된 개인정보를 이용해 불특정 다수에게 스팸 발송 ※ 유출된 모든 휴대전화, 이메일로	<ul style="list-style-type: none"> 지능형 스팸차단서비스를 이용한 스팸 차단, 수신 스팸 적극 신고 ※ 신고기관 : 카드사, 경찰,

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
			<p>도박 등 스팸 무작위 발송 가능</p> <p>※ 신용정보, 연소득 등 활용 대출 스팸 발송, 자동차 보유여부를 활용한 보험 스팸 발송 등 특정유형의 개인에 대한 타겟 마케팅 가능</p> <p>② 휴대전화, 이메일 서비스 이용자는 원치 않는 홍보·마케팅 광고 수신</p>	<p>불법스팸대응센터(☎118)</p> <p>※ 지능형 스팸차단서비스 : 발신·회신번호 등 발송패턴을 분석하여 스팸을 차단해주는 서비스</p>
	사회공학적 기법을 활용한 악성코드 유포메일 발송	이메일주소 등	<p>① 해커가 특정 대상을 목표로 스팸/피싱 시도용 첨부파일이 포함되어 있거나 연결을 유도 URL이 포함된 이메일 발송</p> <p>② 수신자들이 이메일에 포함된 첨부파일 및 URL을 클릭</p> <p>③ 해커가 수신자의 PC를 장악하여 기밀 및 개인정보를 빼냄</p>	<ul style="list-style-type: none"> • 의심가는 이메일을 받은 경우 함부로 열람하지 않고 바로 삭제 • 사용자 PC의 바이러스 백신을 항상 최신버전으로 유지 및 정기적 검사 수행 <p>※ 신고기관 : 경찰, 불법스팸대응센터(☎118)</p>

붙임4

교육부 개인정보보호 포털 유출등 신고 절차

□ 유출등 신고 절차

[1단계] 교육부 개인정보보호 포털(<https://privacy.moe.go.kr>) 사이트 접속 →

① [개인정보 유출 등 신고] 선택



[2단계] EPKI 로그인 및 SNS(카카오, 네이버, 구글) 계정으로 로그인 실시

회원정보

EPKI 갱신

회원가입

아이디 찾기

개인정보재동의

로그인

로그인

사이트 방문을 환영합니다.
로그인을 하시면 다양한 서비스를 이용하실 수 있습니다.

- ▶ 회원가입 시, EPKI(교육부 행정전자서명 인증서)를 등록하지 않을 경우 회원가입이 불가합니다.
- ▶ EPKI(교육부 행정전자서명 인증서)는, 회원가입 시 등록하신 후 별도의 등록절차 없이 사용이 가능합니다.
- ▶ (* EPKI가 변경된 경우 EPKI 갱신메뉴에서 갱신된 인증서를 등록하신 후 이용해주시면 됩니다.)
- ▶ 개인정보보호 소개 메뉴 이외에는 회원가입 시, EPKI(교육부 행정전자서명 인증서)를 등록하신 후 이용이 가능합니다.
- ▶ EPKI 이외의 인증서 (GPKI, 은행용 인증서 및 범용 공인 인증서)는 이용하실 수 없습니다.

보안모듈다운로드

EPKI 로그인

EPKI 갱신

EPKI 안내

아이디 찾기 | 회원가입

SNS 계정으로 로그인 하기

카카오 로그인

네이버 로그인

구글 로그인

제Ⅳ편 교육분야 관련 서식 등 참고자료 441

[3단계] ① [개인정보 유출 등 신고] 선택

[4단계] ① [유출신고 관련 내용 작성] → ② [확인] 완료

※ 유출 등 신고서 내용은 정확한 정보(이메일, 연락처 등)로 입력하여 작성

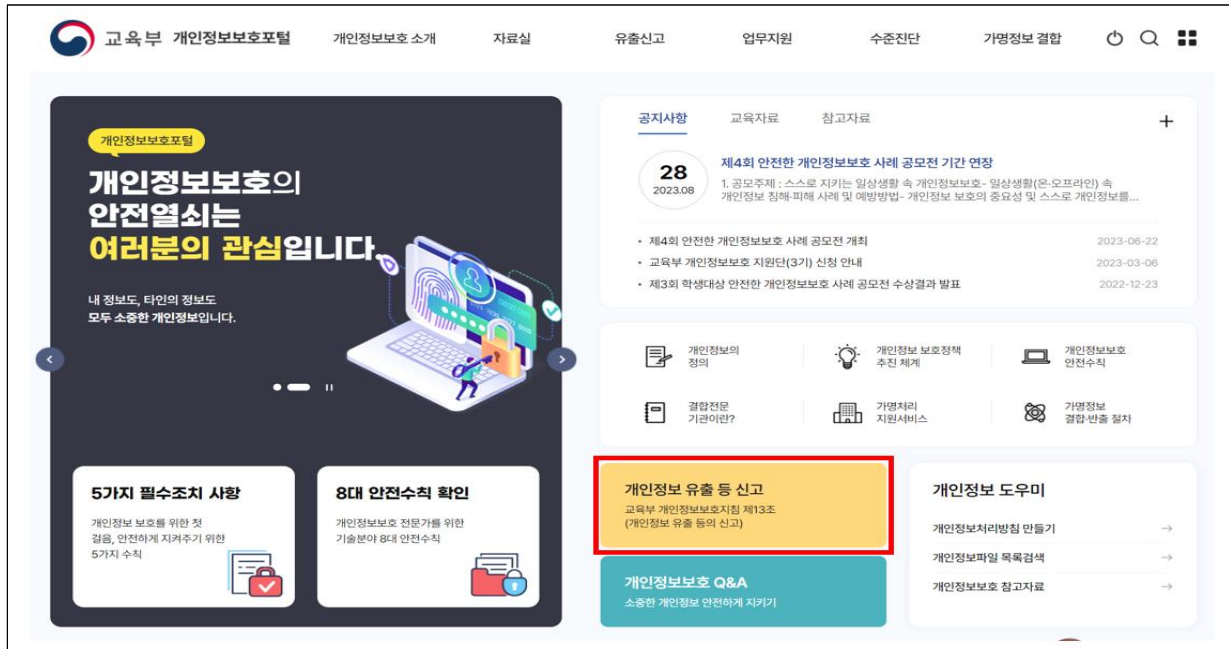
[5단계] 교육부 개인정보 보호지침 제13조에 따른 개인정보 유출 등 신고서(붙임1)를 첨부파일로 제출

※ 개인정보 유출 등 신고 완료 후 1주일 이내 개인정보 유출 등 신고 조치 확인서(붙임2)를 작성 후 교육부 개인정보보호 포털-유출신고 내역 수정하여 제출하거나 메일(moeprivacy@o.o.o대학교.or.kr)로 전달

□ 유출등 신고내역 수정(조치 확인서 제출 등) 절차

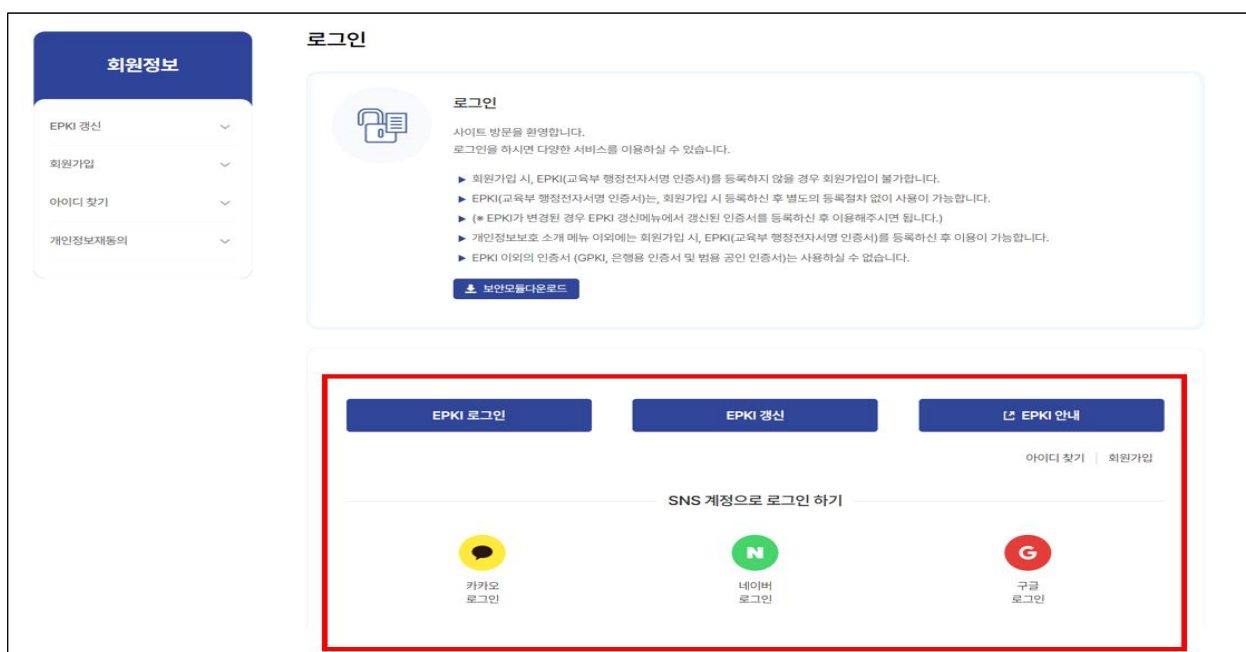
[1단계] 교육부 개인정보보호 포털(<https://privacy.moe.go.kr>) 사이트 접속 →

① [개인정보 유출 등 신고] 선택



[2단계] EPKI 로그인 및 SNS(카카오, 네이버, 구글) 계정으로 로그인 실시

※ 개인정보 유출등 신고한 계정과 동일 계정으로 로그인(동일한 계정 아닐 경우 수정 불가)



[3단계] ① [개인정보 유출 등 신고내역] 선택

교육부 개인정보보호포털

개인정보보호 소개 자료실 유출신고 업무지원 수준진단 가명정보 결합

유출신고 > 개인정보 유출 등 신고

유출신고

개인정보 유출 등 신고

개인정보 유출 등 신고 내역

개인정보 유출 등 신고

개인정보 유출신고 안내

개인정보의 분실·도난·유출(이하 "유출 등")은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말합니다.

▶ 교육부 개인정보 보호지침 제13조(개인정보 유출 등의 신고)

1. 1명 이상 정보주체에 관한 개인정보의 유출 등이 발생한 경우 72시간 내에 교육부로 신고

단, 각 호에 해당하는 경우 교육부와 개인정보보호위원회 동시 신고

1. 1천명 이상의 정보주체 관한 개인정보가 유출등이 된 경우
2. 민감정보, 고유식별정보가 1명 이상 유출등이 된 경우
3. 외부로부터의 불법적인 접근에 의해 유출등이 된 경우

개인정보 유출 등 신고

개인정보 유출 등 신고내역

[4단계] ① 유출 등 신고 내역 확인 후 수정할 유출 등 신고 내역 선택

유출신고

개인정보 유출 등 신고

개인정보 유출 등 신고 내역

개인정보 유출 등 신고

검색

번호	신고기관	신고인 성명	항목 및 규모	파일	신청일시	처리상태
1	한국교육학술정보원	TEST	test		2024-03-12	접수대기

<< < 1 > >>

신청하기

[5단계] ① [수정] 선택 후 내용 수정

유출신고

개인정보 유출 등 신고

개인정보 유출 등 신고 내역

개인정보 유출 등 신고

신고기관

한국교육학술정보원

정보주체 통지여부

통지

신고기준

1천명 이상의 정보주체에 관한 개인정보가 유출됨이 된 경우

신고인

성명

TEST

연락처

010-1234-1234

이메일

abcd@keris.or.kr

웹사이트 주소

moe.privacy.go.kr

유출된 개인정보의 항목 및 규모

test

유출된 시점과 그 경위

test

유출피해 최소화 대책, 조치 및 결과

test

정보주체가 할 수 있는 피해 최소화 방법 및 구제절차

test

파일첨부

분류	성명	부서	직위	연락처	이메일
개인정보보호 책임자	TEST	test	test	test	test
개인정보보호 담당자	test	test	test	test	test

수정

삭제

목록

[6단계] ① 유출등 신고 내역 수정 후 [확인] 선택

한국교육학술정보원

통지

비통지

1천명 이상의 정보주체에 관한 개인정보가 유출됨이 된 경우

1명 이상의 인명정보가 유출됨이 된 경우

1명 이상의 고유식별정보가 유출됨이 된 경우

개인정보처리시스템 또는 개인정보처리자에게 이용되는 정보기기에 대한 위양률(위)의 불법적인 접근에 의해 개인정보가 유출됨이 된 경우

기타(신고기준에 대한 구체적인 내용을 확인하지 못하여 우선 신고하는 경우 등)

성명

TEST

연락처

010-1234-1234

이메일

abcd@keris.or.kr

웹사이트 주소

moe.privacy.go.kr

유출된 개인정보 항목 및 규모

test

유출됨이된 시점과 그 경위

test

유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등

test

정보주체가 할 수 있는 피해 최소화 방법 및 구제절차

test

파일첨부

첨가

확인

구분	성명	부서	직위	연락처	이메일
개인정보 보호책임자	TEST	test	test	test	test
개인정보 보호담당자	test	test	test	test	test

확인

취소

※ 개인정보 유출등 신고서(붙임1), 개인정보 유출등 신고 조치 확인서(붙임2)를 작성하여 붙임파일로 제출

붙임5**유관기관 관련 연락처**☐ 개인정보 유출등 신고

기 관 명	전화번호	인터넷사이트
교육부	-	https://privacy.moe.go.kr/ (교육부 개인정보보호 포털)
개인정보보호위원회 (한국인터넷진흥원)	118	https://privacy.go.kr/ (개인정보보호 포털)

☐ 관련기관 연락처

기 관 명	전화번호	인터넷사이트
대검찰청	1301	https://www.spo.go.kr/
경찰청	182	https://ecrm.cyber.go.kr

3

[학년초] 개인정보 처리 유의사항

실질적인 정보주체 권리 보장을 위해 개정된 개인정보 보호법('23.9.15)을 명확히 준수하며 학생, 학부모 등의 개인정보 수집·이용이 집중되는 시기에 불필요한 개인정보 수집 방지 및 개인정보 유출 예방을 위한 유의사항 안내

① 최소정보 수집

- 개인정보를 수집하는 경우 업무처리 목적에 필요한 최소한의 정보만 수집하고 그 목적에 맞는 용도로만 활용(개인정보 보호법(이하 '법') 제16조)
※ 「각급학교 개인정보 수집업무 길잡이」 참고 (교육부 개인정보보호 포털, '24.2.)

◎ 법 위반사례

☞ 학사업무와 무관한 학부모의 직업, 학력 등 개인정보를 과도하게 수집

☞ 채용 계약과 관련 없는 가족사항, 신체사항 등 불필요한 개인정보 수집

※ 채용 이후에 필요한 개인정보를 입사지원 시에 수집하는 것은 최소수집 원칙에 위배 소지

* 가족수당 지급에 필요한 가족관계 정보 등

② 개인정보 수집 · 이용

- 정보주체의 동의, 법령상 의무 준수, 공공기관의 소관 업무 수행 등을 위해 개인정보 수집·이용 가능(법 제15조)
 - (필수 고지사항) 개인정보의 ①수집 목적, ②수집 항목, ③이용 기간, ④동의 거부권과 그에 따른 불이익 내용 고지 후 동의
 - (별도 동의) 민감정보, 고유식별정보(주민등록번호 제외) 등의 수집·이용 동의는 다른 개인정보의 동의와 구분하여 별도 동의 필요
 - (주민등록번호 처리 제한) 주민등록번호는 정보주체의 동의가 있어도 법률, 시행령에 근거가 없으면 수집 불가
 - (만14세 미만 아동의 개인정보 처리) ①법정대리인의 동의 ②법정대리인의 동의여부 확인 ③만 14세 미만의 아동에게 이해하기 쉬운 양식과 명확하고 알기쉬운 언어로 안내(법 제22조의2)

- 개인정보는 처리 목적에 따라 필요한 최소한의 정보만 수집하고, 목적에 맞는 용도로 활용(법 제3조, 제16조)
- 업무처리 과정에서 얻은 개인정보를 이용하여 법령에서 금지하는 행위를 하는 경우 처벌될 수 있음을 유의

◎ 법 위반사례

- ☞ (최소수집 위반) 학사업무와 무관한 학부모의 직업, 학력, 생년월일 등 개인정보를 과도하게 수집하는 사례
- ☞ (개인정보 미동의) 현장학습, 우유급식, 스쿨뱅킹, 졸업앨범 등의 경우 개인정보 수집을 위한 별도의 법적 근거가 없음에도 정보주체의 동의 없이 개인정보를 수집하는 사례
- ☞ (필수 고지사항 누락) 온라인(홈페이지 등), 오프라인(종이문서) 등을 통해 동의를 받을 때 4가지 항목* 중 일부 항목만 동의를 받는 사례

* ①수집 목적, ②수집 항목, ③이용 기간, ④동의 거부권과 그에 따른 불이익 내용

③ 개인정보처리시스템, 홈페이지 등에서의 개인정보 처리

- 개인정보처리시스템 및 개인정보 처리 업무와 관련된 접근권한은 법령 또는 업무규정 등에 따라 업무수행에 필요한 최소한의 범위로 부여
- ※ 권한없는 자(사회복무요원 등)에게 접근권한 임의로 양도 또는 대여 금지
- 홈페이지 파일(한글, PDF 등) 탑재, 강당·벽면·교내 게시판에 자료 공지 시 개인정보 포함 여부 반드시 확인

◎ 개인정보 유출사례

- ☞ 반 편성 정보를 알리는 과정에서 다수에게 공개되지 않아도 될 성적 등 불필요한 개인정보가 포함된 자료 게시
- ☞ 정보공개청구에 따른 정보공개 시, 제공한 파일에 개인정보가 없음을 육안으로 확인했음에도 엑셀의 다양한 기능(숨기기, 개체 삽입 등)에 의해 개인정보가 발견되어 유출
- ☞ 학사정보시스템의 업무담당자가 전출로 인해 접근권한이 말소되어야 함에도 해당 시스템에 접속 가능하여 학사정보를 유출하는 사례

○ 홈페이지 첨부파일 엑셀문서 탑재 금지 권고(☞PDF변환 게시)

※ 부득이하게 엑셀파일 탑재 시 비밀번호를 설정하고 숨기기 처리된 행·열 사전 확인 필수

※ 엑셀 외부링크 연결 기능으로 다른 파일의 개인정보가 포함될 가능성이 있어 점검·삭제 필요

4 이메일, 메신저 등을 이용한 개인정보 처리

○ 이메일을 이용하여 개인정보가 포함된 파일을 전송할 경우, **메일 수신자(개인·단체) 및 파일 암호설정 여부 반드시 확인**

○ 상호 간에 실시간 정보공유가 가능한 기관 **메신저** 등을 이용하여 업무정보를 주고받는 경우, **개인정보 탑재 지양**

○ 공문(붙임파일 포함)에 개인정보가 포함된 경우, 문서보안(보안 결재), 열람범위 지정 및 열람제한 기능을 활용

◎ 개인정보 유출사례

- ☞ 개인정보취급자가 개인정보가 포함된 파일을 **이메일을 통하여 다수의 사용자에게 무분별하게 발송**
- ☞ SNS 단체 대화방, 메신저 등을 통해 직원이 다수 학생에게 공지사항을 안내하며 개인정보 포함된 자료를 공유
- ☞ 주소 변경 등을 이유로 다수 학생의 개인정보를 공유
- ☞ 합격결과 통보, 학사일정 안내, 교육프로그램 홍보 등을 다수의 학생에게 **집단메일로 발송하여 타인의 이메일 정보 노출**(☞개별발송 기능 사용)
- ☞ 대학원 졸업과 관련된 이메일을 본인외 **다른사람의 개인정보가 담긴** 자료를 포함하여 발송
- ☞ 업무담당자가 개인정보가 포함된 파일을 **이메일을 통하여 다수의 사용자에게 무분별하게 발송**
- ☞ 학교 **비상연락망**이 유출되어 보호자가 구청 담당자를 사칭한 보이스피싱 전화 수신(☞비상연락망에 대한 철저한 관리 필요)

⑤ 개인정보 제3자 제공 · 위탁

- (제3자 제공) 개인정보를 목적內 또는 목적外로 이용·제공할 경우 제공받는 자는 개인정보 안전성 확보 조치 마련
 - (목적內) 정보주체 동의*, 타 법률에 규정, 공공기관 소관 업무 수행 등의 경우 수집목적의 범위 내에서 제3자 제공 가능(법 제17조)
 - * (동의 시 고지사항) ①제공받는 자, ②제공받는 자의 이용 목적, ③제공 항목, ④제공받는 자의 보유 및 이용 기간, ⑤동의 거부권 및 불이익 내용
 - (목적外) 정보주체 동의, 타 법률에 규정(국정감사 등), 범죄 수사, 법원 재판 등의 경우 수집목적 외의 용도로 제3자 제공 가능(법 제18조)
- ※ 제3자에게 제공한 날로부터 30일 이내, 10일 이상 홈페이지 또는 관보 등에 게재
- (위탁) 개인정보처리 위탁 시 문서(표준 개인정보처리위탁 계약서)로 계약을 체결하고, 홈페이지 개인정보 처리방침에 포함하여 공개
 - ※ 수탁자가 재위탁시 위탁자의 동의 필수, 재위탁받은 수탁자도 개인정보 처리방침에 공개
 - ※ 수학여행, 졸업앨범 제작 등을 위해 업체 위탁 시 수탁자 관리·감독 철저

◎ 법 위반사례

- ☞ 학사업무를 목적으로 수집한 학생의 개인정보를 홍보·마케팅 등 수집 목적 범위를 초과하여 이용하거나 제3자에게 제공
- ☞ 민원업무로 알게 된 민원인의 성명, 연락처 등의 개인정보를 정당한 이유 없이 피민원기관에 제공
- ☞ 민원인이 선생님의 핸드폰번호를 요구하여, 해당 선생님의 동의 없이 핸드폰번호 제공

⑥ 개인정보 파기

- 개인정보의 보유기간 경과, 처리목적 달성한 경우, 별도의 보관기간이 규정되어 있지 않다면 지체 없이(5일 이내) 파기(법 제21조)
 - ※ 고정형 영상정보처리기기(CCTV)영상의 경우 보관기간 미설정시 30일 동안 보관후 파기

- 개인정보 파기는 절차와 방법에 따라 기술적, 물리적으로 복원이 불가능하게 파기하여야 하며 파기 후 결과 보고 및 대장 관리 필요

◎ 파기 참고사례

- ☞ 부득이하게 개인정보를 포함한 파일을 (업무용)PC에 저장할 경우 암호화하여 저장하고 목적 달성 시 즉시 파기 조치
- ☞ 개인정보가 포함된 인쇄물 등은 이면지로 활용해서는 안 되며, 복원할 수 없도록 파기 처리
- ☞ 재학생의 사진 등이 홈페이지 등에 게재된 경우 별도의 동의가 없다면 졸업 후에는 반드시 삭제 처리

7 고정형 영상정보처리기기(CCTV 등) 운영

- (공개된 장소) 공개된 장소에서의 고정형 영상정보처리기기 설치는 원칙적으로 금지되고 예외적으로 개인정보 보호법 제25조에서 정하는 사유에 해당하는 경우에만 고정형 영상정보처리기기 설치·운영 가능

【 고정형 영상정보처리기기 설치·운영 허용 】

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설의 안전 및 화재 예방을 위하여 정당한 권한을 가진 자가 설치 운영 한 경우
4. 교통단속을 위하여 정당한 권한을 가진 자가 설치 운영 한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치 운영 한 경우
6. 촬영된 영상정보를 저장하지 아니하는 경우로서 대통령령으로 정하는 경우
 - 가. 출입자 수 등 통계값 산출을 위해 필요한 경우
 - 나. 성별, 연령대 등 통계적 특성값을 도출하기 위해 필요한 경우
 - 다. 그 밖에 이에 준하는 경우로서 보호위원회의 심의 의결을 거친 경우

※ 정당한 권한 없이 임의로 CCTV를 설치하여 공개된 장소를 촬영하는 행위 금지

- 단, 불특정 다수가 이용하여 현저히 사생활 침해 우려가 있는 장소 (목욕실, 화장실, 발한실, 탈의실 등)는 고정형 영상정보처리기기 설치·운영 금지

※ [참고] “공개된 장소” 예시

- ☞ 누구나 출입, 접근 또는 통행이 허용되는 장소(학교 운동장, 학교 복도* 등)

* 학교 건물이 엄격하게 출입통제 및 관리되는 경우 비공개 장소로 볼 수 있음

- (비공개된 장소) 비공개 장소에 업무를 목적으로 고정형 영상정보 처리기기를 설치하는 경우에는 **개인정보 보호법 제15조**(개인정보의 수집·이용)에 따라 설치·운영 가능

※ [참고] “비공개된 장소” 예시

☞ 학생, 교사 등 학교 관계자만 출입이 가능한 학교시설(교실, 실험실 등)

- (안내판 설치) 고정형 영상정보처리기기 운영자는 다음의 필수사항이 모두 포함된 안내판 설치 필요

안내판 필수사항	
① 설치목적 및 장소	② 촬영범위 및 시간
③ 관리책임자의 연락처	④ 고정형 영상정보처리기기 설치·운영 사무 위탁하는 경우, 수탁자의 명칭 및 연락처

- (열람 등 요구 절차) “10일 이내” 처리 필요

열람대상	열람 등의 청구	본인 또는 정당한 대리인 여부 확인
1. 정보주체 2. 명백히 정보주체의 급박한 생명·신체, 재산의 이익을 위해 필요한 경우	⇒ 정보주체의 개인영상정보 열람 또는 존재확인 요청	⇒
열람 여부 결정	열람 조치	열람 기록·관리
※ (열람 거부 사유) 1. 법률에 따라 제한된 경우 2. 타인의 생명·신체를 해하거나 재산 등을 침해할 우려가 있는 경우 3. 다음에 해당하는 업무 수행 시 중대한 지장을 초래하는 경우 - 조세의 부과징수 또는 환급에 관한 업무 - 각급학교 평생교육시설 고등교육면에서의 성적평가 또는 입학자 선별에 관한 업무 - 채용에 관한 시험 자격심사에 관한 업무 - 보상금급부금 산정 등에 관한 업무 - 감사 및 조사에 관한 업무	⇒ 비식별조치가 가능한 경우 정보주체 외 묘자이크 처리 비식별조치가 어려운 경우 타 정보주체의 제3자 제공 동의 징구	⇒ 개 인 영 상 정 보 관리대장 기록 및 관리

◎ 법 위반사례

☞ (과태료 처분) 00고등학교 화장실에 학생 흡연 및 학교 폭력 방지를 위한 목적으로 고정형 영상정보처리기기(CCTV) 설치

⑧ 개인정보처리자의 주요업무

○ 개인정보 내부관리계획에 따라 안전조치의무(법 제29조) 이행사항을 주기적으로 철저하게 관리

- 접속기록(매월 점검, 특히 다운로드 사유 확인), 접근권한 부여 및 관리 등
- 개인정보처리 위탁계약 시 수탁자의 업무 관리·감독 등
- 안전한 접속수단 및 인증수단 적용, 아이들 타임아웃(Idle Timeout)* 설정, 웹 취약점 점검 및 보완 조치 등 접근통제 강화
 - * 최대 접속시간 제한 설정 등
- 전산실·자료보관실의 출입통제 철저 및 서류·보조저장매체 등을 안전한 장소에 보관

※ 영리를 목적으로 개인정보를 유출한 사건과 유사한 사례가 발생하지 않도록 개인정보취급자에 대한 접근권한 최소화, 접속기록 점검 등 관리 강화 필요

※ 시험지 유출 사고 등 PC 보안, 출입 통제 미흡에 따른 개인정보 침해사고가 증가함에 따라 접근통제 강화 필요

※ 홈페이지 및 시스템 취약점 점검 등 해킹사고 예방을 위한 안전조치 강화

○ 개인정보 업무담당자, 정보주체 등을 대상으로 개인정보 보호 교육 실시

- 개인정보의 적정한 취급을 보장하기 위하여 개인정보 보호담당자 및 개인정보취급자에게 정기적(연1회 이상)으로 필요한 교육 실시(법 제28조)
 - ※ 교육부 정보보호교육센터(<https://sec.keris.or.kr>) 등의 개설 교육과정 활용
- 원격수업을 실시하는 경우 학생, 교사 등을 대상으로 개인정보의 유출 예방 및 정보주체의 권리 보호를 위한 사전 유의사항 안내
 - ※ 원격수업 중 불법적인 녹음, 녹화 등으로 인한 교육활동 침해 예방(교원지위법 제15조)

○ 기관별 개인정보 관련 변경사항 발생 시 개인정보파일 (변경)등록, 개인정보 처리방침 및 내부관리계획 현행화 등 추진

○ 1명 이상의 개인정보 유출 시 상급기관 경유하여 교육부 개인정보보호 포털(<https://privacy.moe.go.kr>)에 보고하고 신속한 조치*

* 교육분야 개인정보 유출사고 대응 매뉴얼, 개인정보보호 업무사례집 참고

※ 1천명 이상의 유출 시, 교육부와 개인정보보호위원회에 신고

※ ①민감정보, 고유식별정보가 유출된 경우 및 ②외부로부터 불법적인 접근에 의해 개인정보가 유출된 경우에도 교육부와 개인정보보호위원회 동시 신고(72시간 이내)

《 교육부와 개인정보보호위원회* 신고사항(72시간 이내) 》

- ① 1천명 이상 유출등
- ② 민감정보·고유식별정보 1건 이상 유출등
- ③ 외부로부터의 불법적인 접근에 의해 1건 이상 유출등

9] 참고사항

○ 개인정보보호 교육 일정, 업무 관련 자료*는 **교육부 개인정보보호 포털** (<https://privacy.moe.go.kr>) **참고** (* 별도 로그인 없이 사용 가능)

* **자료실> 참고자료**에 개인정보 보호 법령·고시 및 지침 해설서, 업무 사례집, 매뉴얼, 각급학교 수집업무 길잡이(표준개인정보파일목록 포함) 등 탑재

○ 「개인정보 보호법», 「교육부 개인정보 보호지침」 등 **관계 법령 및 행정규칙**은 **국가법령정보센터(law.go.kr)**에서 확인 가능

4

개인정보보호 현장 실태점검 체크리스트

교육기관

개인정보보호 현장실태점검
체크리스트

202 . . .

[기본 정보 작성]

기관명		주 소	
작성자의 성명		작성자의 부서 및 직책	
작성자의 전화번호		작성자의 팩스	

※ 이 조사표는 ‘개인정보보호법’ 제63조 제1항에 따라 귀 기관의 개인정보 관리 현황을 검사하기 위해 요구되는 자료입니다. 정기/수시로 기관의 개인정보 유출사고 예방 및 [교육부/개인정보위] 개인정보 현장실태점검 대응 등의 자료로 조사표를 활용하시기 바랍니다.

[교육부/개인정보위] 개인정보 현장실태점검의 경우, 자료제출 불응 또는 허위자료 제출 시 1천만원 이하의 과태료를 부과할 수 있습니다.

※ 제출된 자료는 동법 제63조 제4항에 따라 제3자에게 제공하거나 일반에게 공개하지 않습니다.

※ 현황 작성 기준일은 2023년 12월 05일입니다.

▶ 자료작성 관련 문의 : 교육분야 개인정보보호 전문기관 한국교육학술정보원(○○○대학교)
- 개인정보보호부 문의

▶ 예시된 사항을 참고하여 작성하시기 바랍니다.

《 개인정보 관리 현황 》

정보주체 건 수	000,000명
개인정보 파일 수	00개
개인정보처리시스템 수	00식
고유식별정보 보유 현황	<input type="checkbox"/> 주민번호 <input type="checkbox"/> 여권번호 <input type="checkbox"/> 외국인등록번호 <input type="checkbox"/> 운전면허
비 고	전체 정보주체 건 수 000개

☐ 개인정보파일 보유 현황

개인정보 파일명(DB명)	정보주체 수 (명)	수집하는 개인정보 항목 ※ 필수/선택 구분	민감정보 및 고유식별정보 수집 여부 ※ 수집시 해당 항목 명시	취급부서	취급 자(명)
TM 고객정보	5,000,999건 (100,999명)	(필수) 고객명, 연락처 등 (선택) 주소, 건강	·민감정보(건강) 수집	·TM 센터	50
홈페이지회원 정보	건수 확인불가 (100,999명)	(필수) 이름, 성명, 아이디, 비밀번호 CI (선택) 자택주소	·수집하지 않음	·마케팅팀	50
비회원 구매내역	1,000,999건 (10,999명)	(필수) 이름, 성명, 카드번호, 주소, 이메일주소, 연락처	·고유식별정보(주민등록 번호) 수집	·구매팀	30
예약정보	건수 확인불가 5,999,999명	(필수) 영문이름, 한글이름, 연락처, 여권번호, 주민번호 (선택) 건강	·고유식별정보(여권정 보, 주민등록번호) 수집	·예약팀	30

☐ 개인정보처리시스템 현황

개인정보 처리시스템명	보유개인정보파일명	소프트웨어 아키텍처 ※ web, c/s 중 하나 이상 택일	개발업체	유지보수 업체
TM시스템	·TM고객정보	·web방식	A정보통신	A정보통신
대표홈페이지시스템	·홈페이지회원정보	·web방식	A정보통신	B정보통신
예약관리시스템	·홈페이지회원정보 ·예약정보	·web방식, c/s방식	자체개발	자체유지보수

□ 의무대상 파일 개인정보 영향평가 실시 현황

개인정보처리 시스템명	개인정보파 일명	고유식별/ 민감정보	개인정보 보유량	연계시스템 여부	영향평가 실시	비고
TM시스템	·TM고객정보	해당사항 없음	1,787,070	해당사항 없음	영향평가 실시 2012년 12월 31일	-
대표홈페이지 시스템	·홈페이지 회원정보	주민등록번호	3,244,148	유치원입학관 리시스템과 연동	영향평가 실시 2018년 9월 3일 (2015년 10월 31일) ※ 일부 운영체제 변경으로 2018년도 영향평가 수행	-
예약관리시스템	·홈페이지회 원정보 ·예약정보	주민등록번호 외국인등록 번호	6,999,377	유치원입학관 리시스템과 연동	영향평가 미실시	2022년도 실시 예정

개인정보 최소 수집 · 이용 · 제공 점검

개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.(법 제3조, 제16조)

개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다. (법 제3조)

이를 위하여 공공기관은 업무 관련 법령(법, 시행령, 시행규칙), 고시, 훈령, 예규, 자치단체 조례·시행규칙, 기관 내규 등의 각종 서식에 대하여 개인정보 기재 항목이 반드시 필요한 지를 검토하고 업무수행에 필요 없는 개인정보는 다른 정보로 변경하거나 삭제하여야 한다.

신규로 개인정보를 수집·이용·제공하고자 할 경우 해당 업무수행 및 목적달성에 필요한 최소한의 개인정보가 어떠한 것들이 있는지 검토하여 수집·제공 여부를 결정해야 한다.

개인정보 수집 · 이용 · 제공 항목 점검표

※ 개인정보처리업무(서비스 등)별 모두 작성

□ 개인정보처리 서비스/업무명 []

순번	개인정보 항목	수집·제공 이유(근거 등 필요성)	구분	적정성검토
1	예) 이름	서비스 제공을 위한 본인식별	수집	양호
2	예) 소속	연계 서비스 제공(기관별 서비스 상이)	수집	양호
3	예) 주민등록번호	00법 제0조, 00시행령 제0조	수집	양호
4	예) 부모 학력	관련법령 및 수집 근거가 없음	수집	개선 필요
5	예) 연락처	00법 제0조, 00시행령 제0조	제공	양호
6	예) 학력	관련법령 및 제공 근거가 없음	제공	개선 필요
7				
8				
9				

NO.1-2

개인정보 수집 · 이용 · 제공 · 동의 절차 준수여부 점검

법 제15조 제1항, 법 제17조 제1항, 법 제18조 제2항, 법 제23조 제1항, 법 제24조 제1항에 따라 개인정보 수집·제공 등 처리에 대한 동의로 받을 때에는 각각의 고시 사항을 고지하여야 하고 법 제22조 및 시행령 제17조에서 정한 동의를 받는 방법을 준수하여야 한다.

개인정보 수집 · 이용 · 제공 · 동의 절차 준수여부 점검표

※ 개인정보처리업무(서비스 등)별 모두 작성

☐ 개인정보처리 서비스/업무명 ()

점검 항목	법 조항	세부 점검 내용	예	아니오	해당 없음
1	제15조	개인정보 수집 시(회원가입, 게시판 등), 정보주체의 동의를 받고 있는가?			
		(증빙자료)			
2	제23조, 제24조	① 민감정보, 고유식별정보(주민등록번호 제외) 수집 시, 별도로 개인정보 주체의 동의 혹은 법령에 근거하여 수집하고 있는가? ② 주민등록번호 수집 시, 법률에 근거하여 수집하고 있는가? ③ 서비스를 제공하는 과정에서 공개되는 정보에 민감정보가 포함되어 사생활 침해 위험성이 있는 경우 서비스 제공 전에 민감정보의 공개 가능성 및 비공개 선택하는 방법을 정보주체가 알아보기 쉽게 알리고 있는가?			
		(증빙자료)			

점검 항목	법 조항	세부 점검 내용	예	아니오	해당 없음
3	제22조, 제22조의2	① 만 14세 미만 아동의 개인정보 수집 시, 법정대리인에게 동의를 받고 있는가? ② 법정대리인이 동의하였는지를 확인하고 있는가?			
		(증빙자료)			
4	제15조	개인정보 수집 시, 필수 고지항목(4개)을 명확하게 고지하는가? ① 개인정보의 수집·이용 목적 ② 수집하려는 개인정보의 항목 ③ 개인정보의 보유 및 이용 기간 ④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용			
		(증빙자료)			

점검 항목	법 조항	세부 점검 내용	예	아니오	해당 없음
5		홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보를 구분하여 동의를 받고 있는가?			
		(증빙자료)			
6	제22조	선택항목 및 홍보 권유 정보의 미 동의를 이유로 재화 또는 서비스 제공 거부를 하지 않는가?			
		(증빙자료)			

점검 항목	법 조항	세부 점검 내용	예	아니오	해당 없음
7		제3자 제공에 관한 사항을 정보주체에게 알리고 동의를 받는가?			
		(증빙자료)			
8	제17조	제3자 제공에 관한 동의를 받을 시, 필수고지항목(5개)을 명확하게 고지하는가? ① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용			
		(증빙자료)			

점검 항목	법 조항	세부 점검 내용	예	아니오	해당 없음
9	제20조	정보주체 이외로부터 수집한 개인정보가 대통령령으로 정하는 기준(5만명 이상의 민감정보(또는 고유식별정보)이거나 100만명 이상의 개인정보일 경우, 개인정보의 수집·출처 등을 정보 주체에게 알리고 있는가? ① 개인정보의 수집 출처 ② 개인정보의 처리 목적 ③ 개인정보 처리의 정지를 요구할 권리가 있다는 사실			
		(증빙자료)			
10	제22조	개인정보의 동의를 서면으로 받을 경우, 대통령령으로 정하는 중요한 내용(재화나 서비스의 홍보 또는 판매 권유 등으로 정보주체에게 연락할 수 있다는 사실, 민감정보 또는 고유식별정보, 보유 및 이용기간, 제공받는 자 및 이용목적)을 보호위원회가 고시로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하고 있는가?			
		(증빙자료)			

점검 항목	법 조항	세부 점검 내용	예	아니오	해당 없음
11	제22조	<p>정보주체의 동의없이 처리할 수 있는 개인정보에 대하여 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 공개하거나 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법으로 정보주체에게 알리고 있는가?</p> <p>(증빙자료)</p>			
12	제15조, 제17조, 제18조, 제23조, 제24조	<p>정보주체의 동의가 적법하기 위한 정보주체에 따라 다음 조건을 모두 충족하는가?</p> <ol style="list-style-type: none"> 1. 정보주체가 자유로운 의사에 따라 동의여부를 결정할 수 있음 2. 동의 내용이 구체적이고 명확함 3. 평이하고 이해하기 쉬운 문구를 사용함 4. 정보주체에게 동의 여부에 대한 의사를 명확하게 표시할 수 있는 방법을 제공함 <p>(증빙자료)</p>			

<별첨1>

개인정보 수집 · 동의 서식

※ 개인정보처리업무(서비스 등)별 모두 제출

☐ 개인정보처리 서비스/업무명 ()

(증빙자료)

※ 반드시 부서별 사용하는 개인정보 수집·동의 서식 “모두” 제출

교육 대상별 개인정보보호 교육 계획 수립 및 운영

개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.(법 제28조)

개인정보 보호 교육의 목적은 개인정보가 안전하게 관리될 수 있도록 개인정보 보호에 대한 인식을 제고시키고 개인정보 보호 대책의 필요성을 이해시키는 것이다.

교육대상(개인정보 보호책임자, 개인정보 보호담당자, 개인정보취급자/일반직원)에 따라 교육내용을 차별화하고 일정 및 방법 등 구체적 사항을 명시해야 한다. 내부관리계획 또는 “00년 개인정보보호 교육계획(안)”과 같은 문서를 통해 관리하여야 한다.

점검 항목	법 조항	세부 점검 내용	예	아니오	해당 없음
1	제28조	교육 대상별(개인정보보호책임자, 개인정보보호담당자, 개인정보취급자/임직원) 차별화된 교육계획을 수립하였는가? (증빙자료)			
2	제28조	교육 대상별(개인정보보호책임자, 개인정보보호담당자, 개인정보취급자/임직원) 목적에 맞게 구분하여 교육을 실시하였는가? (증빙자료)			

개인정보처리시스템 자율 점검

개인정보처리시스템에 불법적인 접근 및 침해사고 방지 등을 위해 접근 제한 및 접근 통제를 위한 접근통제를 위한 시스템을 구축·운영하거나, 개인정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보호조치를 하여야 한다.(법 제29조, 시행령 제30조, 개인정보의 안전성 확보조치 기준 제6조)

개인정보를 정보통신망을 통하여 송신 또는 보조저장매체를 통해 전달하는 경우에는 암호화 등을 하여야 하고, DB 또는 파일 등으로 저장하는 경우에는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장·관리하여야 한다.(법 제29조, 시행령 제30조, 개인정보의 안전성 확보조치 기준 제7조)

개인정보처리시스템별 안전성확보에 필요한 필수 요건 사항을 점검한다.

개인정보처리시스템 자율 점검표

□ 개인정보처리자(공통항목)

점검 항목	법 조항	세부 점검 내용	양호	개선 필요	해당 없음	개선 기한 (개선필요 해당 시)
1	제26조	① 업무 위탁 계약문서에 필수 반영사항(7개)이 포함되어있는지 여부 ※ 법 제26조 제1항 및 시행령 제28조 제1항 참조 ② 수탁자가 제3자에게 다시 위탁하는 경우 위탁자의 동의를 받도록 하는지 포함 여부				
2	제29조	내부관리계획수립·시행여부 [필수 15개 항목] ※ 개인정보의 안전성 확보조치 기준 제4조 제1항 참조				
3	제30조	개인정보처리방침의 공개 및 필수 사항 포함 여부 ※ 법 제30조 제1항 및 시행령 제31조 제1항 참조				
4	제32조	개인정보파일을 운용하는 경우 개인정보보호 종합지원시스템(intra.privacy.go.kr)에 등록여부				
5	제17조 제18조	개인정보 제3자 제공 절차 수립 및 전파하고 개인정보보호책임자 확인 하에 이행준수 여부				
6	제21조	개인정보 파기절차 수립 및 전파하고 개인정보보호책임자 확인 하에 이행준수 여부				

□ 개인정보처리시스템명 (서비스명) ※ 개인정보처리시스템(서비스)별 모두 작성

점검 항목	법 조항	세부 점검 내용	양호	개선 필요	해당 없음	개선 기한 (개선필요 해당 시)
7		개인정보 수집 시 정보주체의 동의 여부				
8	제15조	개인정보 수집에 따른 정보주체의 동의 여부 및 동의를 받을 때 필수 사항(4개) 고지 및 내용의 적정성 여부				
9	제22조	만 14세 미만 아동의 개인정보 처리 시 법정 대리인(부모 등)의 동의 여부				
10	제17조	제3자에게 개인정보 제공시 법률 근거 여부, 정보주체의 동의 여부 및 동의를 받을 때 필수 사항(5개) 고지 및 내용의 적정성 여부				
11	제23조 제24조	민감정보, 고유식별정보 수집에 따른 법령 근거 유무 또는 별도의 동의를 받고 있는지 여부				
12	제24조 의2	법령에 근거하지 않고 주민등록번호를 수집 및 처리하고 있는지 여부				
13	제21조	보유기간 경과, 처리 목적(제공받은 경우 제공 받은 목적) 달성 후 지체 없이 영구 삭제하고 있는지 여부				
14		접근 권한 관리 정책서 보유 여부[필수 사항 반영 여부] <div style="border: 1px dotted black; padding: 5px; margin: 5px 0;"> ① 접근 권한 정의 및 업무분장, 책임 및 역할 ② 권한 부여 기준(업무담당자별(1인 1계정) 차등 부여, 말소 기준 등) ③ 권한 부여·변경·말소 절차 및 방법 </div>				
15		접근 권한의 부여·변경·말소 내역을 기록 및 관리하고, 최소 3년간 보관하는지 여부				
16		안전한 비밀번호 작성규칙을 수립 및 적용하는지 여부				
17		일정 횟수 이상 인증에 실패한 경우 개인정보 처리시스템에 대한 접근을 제한하는 등의 기술적 조치 여부				

점검 항목	법 조항	세부 점검 내용	양호	개선 필요	해당 없음	개선 기한 (개선필요 해당 시)
18	제29조	개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하거나 접속한 IP주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응 여부 ※ 관리자페이지 외부 노출 여부				
19		고유식별정보를 처리하는 경우 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점 점검여부				
20		개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하는지 여부				
21		고유식별정보, 비밀번호, 생체인식정보를 정보통신망을 통하여 송신하거나, 보조저장매체 등을 통하여 전달하거나, 저장하는 경우 안전한 암호 알고리즘으로 암호화 적용 여부				
22		비밀번호 암호화 저장 시 일방향 암호화(해쉬 함수) 알고리즘 적용 여부				
23		고유식별정보를 인터넷과 내부망의 중간지점(DMZ) 및 내부망에 저장하는 경우 암호화 조치 적용 여부				
24		안전한 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차의 수립·시행 여부 ※ 10만명 이상의 개인정보를 보유한 공공기관(강화유형)만 해당				
25		개인정보취급자의 접속기록을 최소 1년 이상 보관 및 관리하고, 도난 및 분실되지 않도록 안전하게 보관 및 관리하는지 여부 * 5만명 이상 또는 주민번호나 민감정보의 경우, 2년 이상 보관				
26	제29조	개인정보취급자의 접속이력 기록 시 필수 항목(5개)을 기록하고 있는지 여부 ※ 계정/접속일시/접속지정보/수행업무/처리한 정보주체의 정보				
27		월 1회 이상 접속기록 점검 여부(다운로드가 있을 경우 사유 확인 여부)				

점검 항목	법 조항	세부 점검 내용	양호	개선 필요	해당 없음	개선 기한 (개선필요 해당 시)
28		보안 프로그램(백신)을 정당한 사유가 없는 한 자동 업데이트 또는 1일 1회 이상 업데이트 하여 최신의 상태로 유지하고 있는지 여부				
29		관리용 단말기에 대한 안전조치 여부				
30		개인정보 침해사고 대응 절차서[필수 4가지 사항 반영 여부] 수립 및 전파여부 ① 개인정보 침해 유형별 정의(유출, 노출 등) ② 업무 절차(침해사고 인지, 경위 조사, 확산 방지 등) ③ 업무 분장(개인정보 보호책임자, 개인정보 보호 담당자, 개인정보취급자 등) ④ 신고 및 피해구제 방법(유출 신고, 통지 등)				
31		재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차 마련·점검 및 전파 여부 ※ 10만명 이상의 개인정보를 보유한 공공기관 (강화유형)만 해당 ① 개인정보처리시스템 구성 요소(개인정보 보유량, 종류·중요도, 시스템 연계 장비·설비 등) ② 재해·재난 등에 따른 파급효과(개인정보 유출, 손실, 훼손 등) 및 초기대응 방안 ③ 개인정보처리시스템 백업 및 복구 우선순위, 목표시점·시간 ④ 개인정보처리시스템 백업 및 복구 방안(복구 센터 마련, 백업계약 체결, 비상가동 등) ⑤ 업무분장, 책임 및 역할 ⑥ 실제 발생 가능한 사고에 대한 정기적 점검, 사후처리 및 지속관리 등				
32		재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획 마련 여부 ※ 10만명 이상의 개인정보를 보유한 공공기관 (강화유형)만 해당				

<별첨2>

전자결재

개인정보처리시스템 접근권한 관리 정책서

□ 개인정보처리시스템명 ()

※ 개인정보처리업무(서비스 등)별 모두 제출

(증빙자료)

※ 기안문 및 첨부파일(정책서)

※ 전결권자 전자결재 필수

NO.4

업무용PC, 모바일 기기 등에 대한 관리 점검

개인정보취급자들이 사용하는 업무용 컴퓨터 등에 불필요한 개인정보가 보관되거나, 암호화되지 않은 상태로 보관되는 등 저장된 개인정보가 유·노출되지 않도록 정기적으로 점검 프로그램을 수행하거나 인터넷 홈페이지, P2P, 공유폴더, 무선랜 등 비인가 접근 경로를 차단하여야 한다. 또한, 개인정보를 기재한 문서에 대한 보안관리를 취하여야 한다.(법 제 29조, 시행령 제30조, 고시 제6조)

업무용PC 개인정보 관리 점검표

점검 항목	법 조항	세부 점검 내용	예	아니오	해 당 없 음
1	제29조	공유폴더 내 개인정보 저장되어 업무용PC 등을 통해 공유되고 있지 않은가?			
		(증빙자료)			
2	제29조	업무용PC 내 개인정보를 암호화 하지 않고 저장하고 있지 않은가?			
		(증빙자료)			

점검 항목	법 조항	세부 점검 내용	예	아니오	해당 없음
3	제29조	업무용PC로부터 상용 웹메일, P2P, 웹하드, 메신저, SNS서비스 등을 통한 개인정보 유·노출 방지 조치가 되어 있는가?			
		(증빙자료)			
4	제29조	업무용PC 및 모바일 기기 사용 시 비밀번호 설정 등의 보호조치 및 관리가 되고 있는가?			
		(증빙자료)			
5	제29조	업무용PC 내 PMS(개인정보관리솔루션) 등의 개인정보 관리를 위한 보안프로그램이 설치되어 운영 및 점검·관리되고 있는가?			
		(증빙자료)			

개인정보처리업무 위탁 관리 점검

기관은 개인정보 처리업무 위탁 현황을 제대로 파악하고 있는지 점검하고 법의무사항을 문서화하여야 한다. (법 제26조, 시행령 제28조)

기관은 개인정보 처리업무를 위탁하는 경우, 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고 수탁자의 개인정보 처리현황 및 실태, 목적 외 이용·제공 여부, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 관리·감독하여야 한다.

개인정보 처리업무 위탁업체 현황

※ 홈페이지 내 개인정보처리방침에 게재된 “개인정보처리 위탁” 확인”

No	점검대상	위탁사	위탁업무 내용	위탁기간
1	나이스대국민서비스(예시)	코리아크레딧뷰로 (KCB)	회원정보관리를 위한 본인확인	“18.5.2 ~ 19.5.1”
		(주)한국사이버결제	응시료결제	“17.5.2 ~ 19.5.1”
2	OOO서비스			
3	OOO서비스			
4				
5				
6				
7				

개인정보 처리업무 위탁 표준계약서

※ 개인정보처리시스템(서비스)별 모두 제출

<개인정보 처리업무 위탁 계약서 필수항목>이 모두 포함된 계약서 첨부

※ 갱신 계약인 경우, **“최초계약서와 갱신계약서”** 함께 제출

※ 위·수탁 업체의 인감·서명 날인 등이 포함된 자료

<개인정보 처리업무 위탁 계약서 필수항목>

- ① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- ② 개인정보의 기술적·관리적 보호조치에 관한 사항
- ③ 위탁업무의 목적 및 범위
- ④ 재위탁 제한에 관한 사항 (재위탁시 반드시 위탁자 승인 필수)
- ⑤ 개인정보에 대한 접근 권한 제한 등 안전성 확보 조치에 관한 사항
- ⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
- ⑦ 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 책임에 관한 사항

NO.5-3

개인정보파일 처리업무 위탁업체 교육확인서

※ 개인정보처리시스템(서비스)별 모두 제출

※ 교육목적, 일시, 시간, 장소, 교육내용, 교육참석확인서 등이 포함된 교육확인 증빙 자료
(결과보고, 참석자 명단 등)

개인정보 수탁기관 관리실태 점검표

※ 서명 날인한 스캔본 첨부

□ 개인정보 수탁업체 명 :

○ 개인정보 처리시스템 : 000

※ 개인정보처리시스템(서비스)별 모두 제출

점검자 : (인) 확인자 : 개인정보 보호책임자 (인)

분야	점검 항목	점검결과		개선기한 (2021년 0월 00일한)
		양호 (해당없음)	개선 필요	
1. 업무위탁 계약	1. 필수 반영사항(7개*)이 포함된 개인정보처리 위탁계약서 작성 여부 * 필수사항 : ①위탁업무 수행 목적외 처리금지, ②기술·관리적 보호조치, ③목적범위, ④재위탁 제한, ⑤접근제한 등 안전조치, ⑥관리·감독사항, ⑦손해배상 등 책임에 대한 사항			
	2. 개인정보처리 위탁계약서 이행 여부			
2. 개인정보의 안전성 확보조치	3. PC에 저장된 개인정보의 암호화 여부			
	4. 개인정보 처리시스템에 대한 접근권한 부여 시 필요 최소한의 범위로 업무 담당자에 따라(1인 1계정) 차등 부여 여부			
	5. 개인정보 처리시스템에 대한 접근권한을 3년 이상 보관 여부			
	6. 개인정보 처리시스템에 대한 접속 비밀번호 규칙 준수 여부(최소 9자리 이상 : 영문+숫자+특수문자)			
	7. 저장매체 등 물리적 접근방지 조치 적용 여부			
	8. 개인정보 처리시스템 접속기록 1년 이상 보관 여부 * 5만명 이상 또는 주민번호나 민감정보의 경우, 2년 이상 보관			
	9. 개인정보 처리시스템에 대한 접속기록의 주기적인 점검(월1회) 여부 * 개인정보를 다운로드한 경우, 사유 확인 여부 必			
	10. 취급자의 접속이력 기록 시 필수항목(5개*)을 기록하고 있는지 여부 * 필수항목 : ①ID, ②날짜 및 시간, ③접속지 정보(접속자의 단말기 정보, IP주소) ④수행 업무(열람, 수정, 삭제, 인쇄, 입력 등) ⑤ 처리한 정보주체 정보			
	11. 비인가 프로그램 및 유해사이트 접속 차단 여부			
	12. 개인정보취급자가 외부에서 정보통신망을 통한 접속 시 가상사설망(VPN), 전용선 등 안전한 접속수단을 제공하고 있는지 여부			
	13. 보안 프로그램(백신)을 정당한 사유가 없는 한 자동 업데이트 또는 1일 1회 이상 업데이트 하여 최신의 상태로 유지하고 있는지 여부			
	14. 비밀번호의 내부 저장 시 일방향 암호화(해쉬함수) 알고리즘을 적용하고 있는지 여부			
3. 수탁자 교육	15. 수탁자 자체 교육실시 여부 * 자체 교육계획을 수립 및 교육 실시 후 결과 보고			

NO.6

기관 보유 개인정보처리시스템별 개인정보처리방침 적정성 검토 및 보완

공공기관은 관리하는 개인정보파일에 대해 개인정보처리방침을 수립하여 정보주체가 언제든지 확인할 수 있도록 인터넷 홈페이지 등을 통해 공개하여야 한다.(법 제30조, 시행령 제31조)

개인정보처리방침을 변경하는 경우에는 변경 및 시행시기, 변경된 내용을 인터넷 홈페이지 등을 통해 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

개인정보처리서비스별 개인정보처리방침 점검표

No	점검대상	개인정보의 처리목적	처리 및 보유기간	제3자 제공 (현행화포함)	개인정보 처리위탁 (현행화포함)	정보주체의 권리 (법정대리인 포함)	개인정보 항목 (자동수집 운영 등 포함)	개인정보의 파기	안전성 확보 조치	개인정보 보호책임자 (현행화포함)	개인정보 열람창구	권익침해구 제방법 (현행화포함)	개인정보처 리방침변경 관리
1	나이스대국민서비스(예 시)	적용	적용	적용 (현행화)	적용 (현행화)	적용	적용	적용	적용	적용 (현행화)	적용	적용(현행화) ※○○○대학 교대표홈페이 지참조	적용
2	○○○서비스												
3	○○○서비스												
4													
5													

5

표준 내부관리계획 및 연간 활동 일정표 [샘플]

본 문서는 법령상 의무 및 권고사항까지 모두 포함된 문서입니다.

각 교육기관은 기관의 유형 및 규모에 따라 포함하지 않아도 되는 내용이 있으므로 알맞게 적용하시기 바랍니다.

파란색·빨간색으로 표시된 내용은 2023년에 개정된 내용을 반영한 것입니다.

○○○대학교 개인정보 내부관리계획(안)

202 . . .

입학처

목 차

제1장 총칙	00
제1조(목적)	00
제2조(적용범위)	00
제3조(용어정의)	00
제4조(개인정보 보호 원칙)	00
제5조(다른 지침과의 관계)	00
제2장 내부관리계획의 수립 및 시행	00
제6조(내부관리계획의 수립 및 승인)	00
제6조의2(공공시스템운영기관의 내부 관리계획의 수립·시행)	00
제7조(내부관리계획의 공표)	00
제3장 개인정보보호에 관한 조직 및 역할	00
제1절 ○○○대학교 개인정보 보호위원회	00
제8조(○○○대학교 개인정보 보호위원회)	00
제2절 개인정보 보호책임자 및 분야별 책임자·취급자	00
제9조(개인정보 보호책임자 및 가명정보 관리책임자)	00
제10조(개인정보 보호책임자 및 가명정보 관리책임자의 역할)	00
제11조(개인정보보호 분야별 책임자)	00
제12조(개인정보보호 분야별 책임자의 역할)	00
제13조(개인정보취급자의 범위 및 역할)	00
제4장 개인정보의 처리	00
제1절 개인정보의 수집, 생성, 이용 및 제공	00
제1관 개인정보의 수집, 생성 및 목적 내 이용, 제공	00
제14조(개인정보의 수집)	00
제15조(개인정보의 생성)	00
제16조(개인정보의 수집·생성 제한)	00
제17조(개인정보의 이용)	00
제17조의2(개인정보의 추가적인 이용·제공)	00
제18조(개인정보의 제공)	00
제2관 개인정보의 목적 외 이용 및 제공	00
제19조(개인정보의 목적 외 이용 및 제공)	00
제20조(개인정보의 목적 외 이용 및 제공 시 조치)	00
제3관 개인정보의 수집, 생성, 이용 후 조치	00
제21조(정보주체의 사전 동의가 없었던 경우의 개인정보 수집, 생성, 이용 후 조치)	00
제22조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)	00
제22조의2(개인정보 이용·제공 내역의 통지)	00

제4관 개인정보의 파기	00
제23조(개인정보의 파기)	00
제2절 개인정보의 수집, 이용, 제공을 위한 고지 및 동의	00
제1관 개인정보의 수집, 이용, 제공을 위한 고지 및 동의	00
제24조(동의가 필요한 경우의 고지의무)	00
제25조(동의가 필요한 개인정보와 동의가 필요하지 않은 개인정보의 구분 등)	00
제26조(동의를 받는 방법)	00
제2관 개인정보의 목적 외 이용, 목적 외 제3자 제공을 위한 고지 및 동의	00
제27조(개인정보의 목적 외 이용, 목적 외 제3자 제공 시의 고지의무)	00
제28조(개인정보의 목적 외 이용, 목적 외 제3자 제공 시 동의를 받는 방법)	00
제3관 아동의 개인정보 보호	00
제29조(아동의 개인정보)	00
제4관 동의의무의 예외	00
제30조(친목단체에 대한 동의의무의 예외)	0
제3절 민감정보와 고유식별정보의 처리	00
제1관 민감정보의 처리	00
제31조(민감정보의 정의)	00
제32조(민감정보의 수집, 생성, 이용 및 제공)	00
제33조(민감정보의 목적 외 이용, 목적 외 제3자 제공)	00
제2관 고유식별정보 및 주민등록번호의 처리	00
제34조(고유식별정보의 정의)	00
제35조(고유식별정보의 수집, 이용, 제공)	00
제35조의2(주민등록번호 처리의 제한)	00
제36조(고유식별정보의 목적 외 이용, 목적 외 제3자 제공)	00
제36조의2(주민등록번호의 목적 외 이용, 목적 외 제3자 제공)	00
제37조(홈페이지 회원가입을 위한 고유식별정보 대체수단 제공)	00
제4절 민감정보와 고유식별정보의 처리를 위한 고지 및 동의	00
제38조(민감정보와 고유식별정보의 수집, 이용, 제공 시의 고지의무 등)	00
제39조(민감정보와 고유식별정보의 수집, 이용, 제공 시 동의를 받는 방법)	00
제40조(민감정보와 고유식별정보의 목적 외 이용 및 목적 외 제3자 제공 시의 고지의무)	00
제41조(민감정보와 고유식별정보의 목적 외 이용 및 목적 외 제3자 제공 시 동의를 받는 방법)	00
제5절 영상정보처리기기	00
제42조(고정형 영상정보처리기기의 설치 및 운영)	00
제42조의2(이동형 영상정보처리기기의 운영 제한)	00
제6절 개인정보처리업무의 위탁	00
제43조(개인정보처리업무의 위탁)	00
제44조(정보주체를 위한 위탁사실의 게재)	00
제45조(위탁자와 수탁자의 의무)	00
제7절 개인정보취급자에 대한 관리 및 감독	00
제46조(개인정보취급자에 대한 관리 및 감독)	00

제8절 가명정보의 처리에 관한 특례	00
제46조의2(가명정보의 처리 등)	00
제46조의3(가명정보의 결합 제한)	00
제46조의4(가명정보 및 추가정보에 대한 안전조치의무 등)	00
제46조의5(가명정보 처리 시 금지의무 등)	00
제46조의6(가명정보 또는 추가정보의 분야별 관리책임자 지정 및 역할)	00
제46조의7(가명정보의 적용범위)	00
제5장 개인정보의 안전한 관리	00
제1절 총설	00
제47조(개인정보의 안전성 확보 조치)	00
제47조의2(공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등)	00
제2절 개인정보의 안전성 확보를 위한 관리적 조치	00
제1관 개인정보처리방침의 수립, 변경 및 공개	00
제48조(개인정보처리방침의 수립 및 공개)	00
제49조(개인정보처리방침의 작성기준)	00
제50조(개인정보처리방침의 변경 및 공개)	00
제2관 개인정보파일의 등록 및 관리	00
제51조(개인정보파일의 등록)	00
제52조(개인정보파일의 등록의 예외)	00
제53조(개인정보파일의 등록 및 공개 절차)	00
제54조(개인정보파일대장 작성, 삭제)	00
제55조(개인정보파일의 목적 외 이용·목적 외 제3자 제공 관리)	00
제56조(개인정보파일 보유기간의 산정)	00
제57조(개인정보파일의 파기)	00
제58조(개인정보파일 등록사실의 삭제)	00
제59조(개인정보파일 보유·파기현황의 공개 및 방법)	00
제3관 개인정보 영향평가의 실시	00
제60조(개인정보 영향평가)	00
제4관 개인정보 유출등 사고 대응 계획 수립 및 시행	00
제61조(개인정보의 유출등)	00
제61조의2(개인정보의 유출등 사고 대응 계획 수립)	00
제62조(개인정보의 유출등 통지시기 및 항목)	00
제63조(개인정보 유출등의 통지방법)	00
제64조(개인정보 유출등의 신고 및 절차)	00
제3절 개인정보의 안전성 확보를 위한 기술적·물리적 조치	00
제65조(접근권한의 관리)	00
제65조의2(공공시스템운영기관의 접근권한의 관리)	00
제66조(접근통제)	00
제67조(개인정보의 암호화)	00
제68조(접속기록의 보관 및 점검)	00

제68조의2(공공시스템운영기관의 접속기록 보관 및 점검)	00
제69조(악성프로그램 등 방지)	00
제70조(물리적 접근 방지)	00
제71조(위험도 분석 및 대응 방안)	00
제72조(재해 및 재난 안전조치)	00
제73조(출력·복사시 안전조치)	00
제74조(개인정보보호담당부서의 지원)	00
제6장 정보주체의 권리보장	00
제75조(개인정보의 열람)	00
제76조(열람의 제한·거절)	00
제77조(개인정보의 정정·삭제)	00
제78조(개인정보의 처리정지)	00
제78조의2(자동화된 결정에 대한 정보주체의 권리 등)	00
제79조(이의신청)	00
제80조(권리행사 방법 등의 공개)	00
제81조(대리인의 범위 등)	00
제7장 개인정보보호 교육	00
제82조(개인정보보호 교육 계획의 수립)	00
제83조(개인정보보호 교육의 실시)	00
제8장 정기적인 자체 감사	00
제84조(자체 감사 주기 및 절차)	00
제85조(자체 감사 결과 반영)	00
제9장 보 칙	00
제86조(적용의 일부제외)	00
제86조의2(적용제외)	00
제87조(권한의 위임)	00
제88조(금지행위)	00
제89조(비밀유지 등)	00
제90조(의견제시 및 개선권고)	00
제91조(처리중인 개인정보에 대한 경과조치)	00
[별표] 1. 개인정보파일 보유기간 책정 기준표	00
2. 과징금의 산정기준과 산정절차	00
3. 과태료의 부과기준	00
[별지] 별지 제1호 ~ 별지 제19호	00
[붙임] 1. ○○○대학교 영상정보처리기기 표준 지침	00
2. ○○○대학교 「개인정보처리방침」 표준가이드	00
3. 동의획득 예시	00
4. 만 14세 미만 아동의 개인정보 수집 예시	00
5. 표준 개인정보처리위탁 계약서(안)	00
6. 개인정보 처리(등록, 파기 포함) 요구 절차	00
7. 개인정보 목적 외 이용 및 제3자 제공 절차	00

8. ○○○대학교 개인정보 유출등 사고 대응 절차서	00
9. ○○○대학교 개인정보 재해·재난 대비 개인정보처리시스템 위기대응 절차	00
10. ○○○대학교 가명·익명처리 절차서	00

제1장 총 칙

제1조(목적) ○○○대학교 개인정보보호 내부관리계획은 「개인정보 보호법」(이하“법”이라 한다) 제29조(안전조치의무) 내부관리계획의 수립 및 시행 의무에 따라 제정된 것으로 ○○○대학교가 준수하여야 하는 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 내부관리계획은 전자적 처리 여부를 불문하고 수기문서를 포함한 모든 형태의 수집, 이용, 제공 또는 관리되는 개인정보에 대해서 적용되며, 이러한 개인정보를 취급하는 ○○○대학교 임직원(임시직, 파견근로자, 시간제근로자 포함) 및 계약에 의한 외부업체 직원인 개인정보취급자에게 적용된다. 다만, 교육부 등 외부기관의 위탁에 따라 해당 개인정보파일의 관리감독 책임이 외부기관에 있을 경우에는 예외로 한다.

제3조(용어정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다. 또한, 제1호의 2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보를 말한다. (이하 “가명정보”라 한다.)

- 개인정보 : 성명, 주소, 연락처, 소득, 학력, 성적, 직업, 전자우편, 영상, 통화 내용, 신용, 부채, 인터넷 접속 IP 등 객관적 사실에 관한 정보와 개인에 대한 제3자의 의견이나 평가 등 주관적 정보 포함
- 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
- 민감정보 : 사상, 신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 정보, 유전정보, 범죄경력정보 등

- 1의2 “가명처리”란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.
2. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
3. “처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
4. “개인영상정보”란 「개인정보 보호법」(이하“법”이라 한다) 제2조제1호에 따른 개인정보 중 고정형 영상정보처리기기 또는 이동형 영상정보처리기기에 의하여 촬영·처리되는 영상 형태의 개인정보를 말한다.

5. “개인정보 보호책임자”란 ○○○대학교의 개인정보 처리에 관한 업무를 총괄해서 책임 지거나 업무처리를 최종적으로 결정하는 자로서 「개인정보 보호법 시행령」(이하“시행령”이라 한다) 제32조제2항 또는 제3항에 따른 지위에 해당하는 자를 말한다.
6. “개인정보보호 분야별 책임자”란 개인정보 보호책임자의 지휘·감독을 받아 각 업무부서의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자를 말한다.
7. “개인정보취급자”란 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말하며 개인정보 처리 시 안전조치를 이행해야 한다.
8. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
9. “개인정보파일 보유”란 업무처리를 위해 개인정보파일을 생성 및 제공받아 가지고 있거나, 해당 개인정보파일에 대한 접근권한이 있어 개인정보를 처리하여 저장할 수 있는 경우를 말한다.
10. “개인정보처리시스템”이란 개인정보를 처리할 수 있도록 체계적으로 구성된 데이터 베이스시스템을 말한다.
11. “내부망”이란 인터넷망 차단, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
12. “생체정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
- 12의2. “생체인식정보”란 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
13. “보조저장매체”란 이동형 하드디스크(HDD), 유에스비(USB)메모리 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 분리할 수 있는 저장매체를 말한다.
14. “비밀번호”란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
15. “안전한 암호화 알고리즘”이란 미국 NIST, 일본 CRYPTREC, 유럽 ECRYPT 등의 외국 및 국내외 암호 연구기관에서 권고하는 알고리즘을 말한다.
16. “고정형 영상정보처리기기”란 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 시행령 제3조 제1항에 따른 폐쇄회로 텔레비전 및 네트워크 카메라를 말한다.
- 16의2. “이동형 영상정보처리기기”란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(據置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 시행령 제3조제2항에 따른 착용형, 휴대형, 부착·거치형 장치를 말한다.
17. “공개된 장소”란 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 또는 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.

18. “영상정보처리기기운영자”란 법 제25조제1항 각호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.
18. “고정형영상정보처리기기운영자”란 법 제25조제1항 각호에 따라 고정형 영상정보처리기기를 설치·운영하는 자를 말한다.
- 18의2. “이동형영상정보처리기기운영자”란 법 제25조의2제1항 각 호에 따라 업무를 목적으로 이동형 영상정보처리기기를 운영하는 자를 말한다.
19. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
20. “접속기록”이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 처리한 정보주체 정보, 수행 업무 등 접속한 사실을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
21. “모바일 기기”라 함은 무선망을 이용할 수 있는 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
22. “공개된 무선망”이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
23. “개인정보보호 대상”이란 종이, 정보시스템, PC, 영상정보처리기기 등에서 업무상 필요에 의하여 처리되고 있는 개인정보를 말한다.
24. “소속기관”이란 ○○○대학교 소속 조직 및 부속시설 등을 말한다.
25. “과학적 연구”란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다.
26. “익명처리”란 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없도록 처리하는 것을 말한다.
27. “인증정보”란 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속을 요청하는 자의 신원을 검증하는데 사용되는 정보를 말한다.

제4조(개인정보 보호 원칙) ① 업무부서는 정보주체의 동의 또는 관련 법률·규정에 근거하여 개인정보 및 개인영상정보를 처리하여야 한다.

② 업무부서는 개인정보를 수집할 당시 수집목적에 명확히 특정하여야 하며, 그 특정된 목적을 달성하기 위하여 직접적으로 필요한 범위 내에서만 개인정보 및 개인영상정보를 처리하여야 한다.

③ 업무부서는 개인정보의 내용이 처리 당시의 사실에 부합하도록 정확하고 최신의 상태를 유지하여야 하며, 개인정보의 처리과정에서 고의 또는 과실로 개인정보 및 개인영상정보가 부당하게 변경 또는 훼손되지 않도록 하여야 한다.

④ 업무부서는 정보주체의 권리가 침해받을 가능성과 위험의 정도에 상응하는 적절한 관리적·기술적 및 물리적 보안조치를 통하여 개인정보를 안전하게 관리하여야 한다.

⑤ 업무부서는 법 제30조에 따른 개인정보처리방침 등 개인정보의 처리에 관한 사항을 일반적으로 공개하여야 하며, 열람청구권 등 정보주체의 열람, 정정·삭제 요구 등 권리가 보장될 수 있도록 합리적인 절차를 마련하여야 한다.

⑥ 업무부서는 처리 목적에 필요한 범위에서 개인정보를 처리하는 경우에도 가능한 한 정보 주체의 사생활 침해를 최소화하는 방법을 선택하여야 한다.

⑦ 업무부서는 개인정보를 가명 또는 익명으로 처리하여도 개인정보 수집목적 달성을 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.

제5조(다른 지침과의 관계) 개인정보보호에 관하여는 다른 지침에 특별한 규정이 있는 경우를 제외하고는 이 내부관리계획에서 정하는 바에 따른다.

제2장 내부관리계획의 수립 및 시행

제6조(내부관리계획의 수립 및 승인) ① 개인정보 보호담당자는 매년 2월말까지 개인정보보호와 관련한 법령 및 관련 규정을 준수하여 ○○○대학교의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 작성한다.

② 개인정보 보호책임자는 개인정보 보호담당자가 작성한 제1항의 내부관리계획의 타당성을 검토하여 개인정보보호를 위한 내부관리계획을 승인한다.

③ 개인정보 보호담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 3월말까지 내부관리계획의 개정안을 작성하여 개인정보 보호책임자에게 보고하고 개인정보 보호 책임자의 승인을 받아야 한다.

④ 개인정보 보호책임자는 내부관리계획의 사항에 중요한 변경이 있는 경우 이를 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

⑤ 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리 계획의 이행 실태를 연1회 이상으로 점검·관리하고 그 결과에 따라 적절한 조치를 취하여야 한다.

제6조의2(공공시스템운영기관의 내부 관리계획의 수립·시행) 공공시스템운영기관은 공공시스템 별로 다음 각 호의 사항을 포함하여 내부 관리계획을 수립하여야 한다.

1. 제47조의2에 따른 관리책임자(이하“관리책임자”라 한다)의 지정에 관한 사항
2. 관리책임자의 역할 및 책임에 관한 사항
3. 개인정보취급자의 역할 및 책임에 관한 사항
4. 제12조제1호, 제65조, 제66조, 제68조에 관한 사항
5. 제65조의2, 제68조의2에 관한 사항

제7조(내부관리계획의 공표) ① 개인정보 보호책임자는 제6조에 따라 승인한 내부관리계획을 매년 3월말까지 ○○○대학교 전 임·직원에게 공표한다.

② 내부관리계획은 임·직원 및 외부업체 직원인 개인정보취급자가 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보 보호에 관한 조직 및 역할

제1절 ○○○대학교 개인정보 보호위원회

제8조(○○○대학교 개인정보 보호위원회) ① ○○○대학교의 개인정보보호에 관한 다음의 사항을 심의·의결하기 위하여 ○○○대학교 개인정보 보호위원회(이하 “○○○대학교 보호위원회”라 한다.)를 둘 수 있다.

1. ○○○대학교 개인정보 보호계획
2. 개인정보 보호와 관련된 규정의 제·개정에 관한 사항
3. 개인정보의 처리에 관한 부서 간의 의견 조정에 관한 사항
4. 개인정보와 관련한 정보주체의 권리보장에 관한 사항
5. 제79조에 따른 이의신청에 관한 사항
6. 그 밖에 ○○○대학교내 개인정보 보호와 관련된 사항

② ○○○대학교 보호위원회는 위원장(개인정보 보호책임자 당연직) 1명을 포함하여 10명 이내의 위원(개인정보보호 분야별 책임자 당연직)으로 구성하여 운영한다.

③ ○○○대학교 보호위원회는 ○○○대학교의 개인정보보호 관련 주요 사안의 의결이 필요한 경우 개인정보 보호책임자가 소집할 수 있다.

④ 개인정보 보호책임자는 ○○○대학교 보호위원회를 별도 구성하지 않을 경우, ○○○대학교 「보안업무규정」 제3조의 보안심사위원회에 그 역할을 대신하게 할 수 있다.

제2절 개인정보 보호책임자 및 분야별 책임자·취급자

제9조(개인정보 보호책임자 및 가명정보 관리책임자) ① ○○○대학교는 법 제31조 및 동법 시행령 제32조제2항에 따라 개인정보보호 업무를 총괄하는 부서의 장을 개인정보 보호책임자로 한다.

② 개인정보 보호책임자의 성명, 소속, 전화번호 등 연락처를 ○○○대학교 대표 인터넷 홈페이지에 공개하여야 하고, 개인정보 보호책임자가 변경되는 경우에도 같은 방법으로 공개하여야 한다.

③ 개인정보 보호책임자가 지정·변경되는 경우 개인정보 보호책임자는 교육부로 해당 내용을 통보해야 하며, 변경사항을 개인정보보호 종합지원시스템(intra.privacy.go.kr)에 등록하여야 한다.

④ 개인정보 보호책임자는 개인정보 보호담당자를 지정하여 개인정보 보호업무를 담당하게 할 수 있다.

⑤ ○○○대학교는 가명정보를 총괄하는 부서의 장을 가명정보 관리책임자로 한다.

제10조(개인정보 보호책임자 및 가명정보 관리책임자의 역할) ① 개인정보 보호책임자는 ○○○대학교의 개인정보 보호와 관련하여 다음 각 호의 업무를 수행한다.

1. ○○○대학교 개인정보 보호계획의 수립 및 시행
2. ○○○대학교 개인정보 보호 관련 내부 지침 제·개정
3. ○○○대학교 업무부서의 개인정보 처리 실태 및 관행의 점검 및 개선 권고
4. ○○○대학교 개인정보 보호 관련 교육계획의 수립 및 시행

5. ○○○대학교 개인정보 유출 및 오·남용 방지를 위한 내부통제시스템의 구축
6. 개인정보처리방침의 수립·변경 및 시행
7. 개인정보파일의 보호 및 관리·감독[개정, 2017. 2.]
8. 개인정보보호 분야별 책임자의 개인정보 보호 업무에 관한 지휘 및 감독
9. ○○○대학교 개인정보 처리와 관련한 불만 처리 및 피해 구제
10. 개인정보파일 및 대장 등록·파기 승인, 관리 감독
11. 가명정보 또는 추가정보의 관리·감독 책임자(이하 가명정보 관리책임자) [신설, 2021. 3.]
12. 그 밖에 ○○○대학교 개인정보보호를 위해 필요한 사항

② 가명정보 관리책임자는 다음 각 호의 업무를 수행한다.[신설, 2022. 3.]

1. 가명정보 내부관리계획의 수립·시행
2. 내부관리계획의 이행실태 점검 및 관리
3. 가명처리 및 적정성 검토 현황 관리
4. 가명정보 및 추가정보에 대한 관리·감독
5. 가명정보 처리 현황 및 관련 기록 관리
6. 가명정보 교육계획의 수립 및 시행
7. 가명처리 및 가명정보 처리 위탁 사항에 대한 관리·감독(해당 시)
8. 가명정보에 대한 재식별 모니터링 및 재식별 시 처리 방안
9. 그 밖의 가명정보 처리에 대한 보호에 관한 사항

제11조(개인정보보호 분야별 책임자) ① 개인정보 보호책임자의 업무를 효율적으로 수행하기 위하여 ○○○대학교 각 업무부서의 장을 개인정보보호 분야별 책임자로 한다. 다만, 제47조의2에 따라 공공시스템운영기관에 해당하게 될 경우 해당 시스템을 운영하는 업무부서의 장을 제47조의2제4항에 따른 관리책임자로 지정한다.

② 업무부서는 개인정보보호 분야별 책임자의 성명, 소속, 전화번호 등 연락처를 업무부서가 운영·관리하는 인터넷 홈페이지에 공개하여야 하고, 개인정보보호 분야별 책임자가 변경되는 경우에도 같은 방법으로 공개하여야 한다.

③ 업무부서가 인터넷 홈페이지를 운영하지 않는 등 제2항의 내용을 업무부서 또는 대표 인터넷 홈페이지에 공개할 수 없는 사정이 있는 경우에는 다음 각 호의 어느 하나 이상의 방법을 이용하여 공개하여야 한다.

1. 업무부서가 위치한 건물의 보기 쉬운 장소에 게시하는 방법
2. 관보나 ○○○대학교가 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목, 다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 실는 방법
3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 실는 방법(이 방법으로 개인정보 처리방침을 공개하는 경우에는 간행물·소식지·홍보지 또는 청구서 등이 발행될 때마다 계속하여 게재하여야 한다.)
4. 재화나 용역을 제공하기 위하여 ○○○대학교와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

④ 개인정보보호 분야별 책임자가 변경되는 경우 변경된 개인정보보호 분야별 책임자는 개인정보 보호책임자에게 변경 내용을 통보하여야 한다.

⑤ 개인정보보호 분야별 책임자는 개인정보보호 분야별 담당자를 지정하여 개인정보 보호업무를 담당하게 할 수 있다.

제12조(개인정보보호 분야별 책임자의 역할) 개인정보보호 분야별 책임자는 업무부서의 개인정보 보호와 관련하여 다음 각 호의 업무를 수행한다.

1. 업무부서의 개인정보취급자 지정·관리·감독·교육
2. 업무부서의 개인정보파일 지정·관리·보호·파기
3. 업무부서의 공개대상 개인정보파일 등록·공개
4. 업무부서의 공개대상 개인정보파일의 처리방침 수립·시행 및 공개
5. 업무부서의 영상정보처리기기 운영·관리 방침 수립·시행
6. 업무부서의 개인정보보호 관련 자료 관리 및 제출
7. 업무부서의 개인정보 처리와 관련한 요구 처리 및 피해 구제
8. 업무부서의 개인정보 관련 개선 권고 및 시정 조치사항 이행
9. 업무부서의 개인정보보호를 위해 필요한 관리적·기술적 및 물리적 보호조치 수행
10. 업무부서의 가명정보 또는 추가정보의 관리·감독

제13조(개인정보취급자의 범위 및 역할) ① 개인정보취급자는 개인정보처리자의 지휘 감독을 받아 개인정보를 처리하는 자로서, 모든 임직원 및 임시직, 파견근로자, 시간제근로자 및 계약에 의한 외주용역 직원 등을 포함한다.

② 개인정보취급자는 다음 각 호의 업무를 수행한다.

1. 개인정보보호 법적 준수 항목 이행 및 보호 활동 참여
2. 내부관리계획의 준수 및 이행
3. 개인정보의 기술적·관리적 보호조치 기준 이행
4. 개인정보 보호책임자에게 개인정보의 파일 등록·변경·삭제 신청
5. 개인정보파일의 파기
6. 개인정보 파기 시 개인정보파일의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청
7. 소속 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등
8. 기타 정보주체의 개인정보보호를 위해 필요한 사항의 이행

제4장 개인정보의 처리

제1절 개인정보의 수집, 생성, 이용 및 제공

제1관 개인정보의 수집, 생성 및 목적 내 이용, 제공

제14조(개인정보의 수집) ① 개인정보의 “수집”이란, 정보주체로부터 직접 성명, 주소, 전화번호 등의 정보를 제공받는 것뿐만 아니라, 정보주체 이외의 자로부터 개인정보를 취득하는 것 및 공개된 정보에서 개인정보를 취득하는 것 등 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.

② 업무부서는 다음 각 호의 경우에 개인정보를 수집할 수 있다.

1. 정보주체로부터 **동의를 받은 경우**
2. 법률에서 구체적으로 명시하거나 허용하고 있는 경우
3. 개인정보를 수집, 이용하지 않고는 법령 등에서 정한 소관 업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우
4. **체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우**
5. **명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우**
6. **업무부서의** 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 업무부서의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.
7. 정보주체로부터 명함 등을 제공받아 수집하는 경우, 정보주체가 동의의사를 표시하거나 명함 등을 제공하는 정황에 비추어 사회통념상 동의의사가 있었다고 인정되는 범위 내에서만 이용
8. 인터넷 홈페이지 등 공개된 곳에서 개인정보를 수집하는 경우, 본인의 개인정보를 인터넷 홈페이지 등에 게시하거나 게시에 대한 정보주체의 동의가 있거나 인터넷 홈페이지 등의 표시내용에 비추어 사회통념상 동의의사가 있었다고 인정되는 범위 내에서만 이용
9. 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우, 대리인의 대리권 확인을 위한 목적으로만 대리인의 개인정보를 수집·이용 가능
10. 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」 제2조제5호의 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집·이용
11. **공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우**

③ 제2항에 필요한 고지 및 동의의 방법은 이 장 제2절에 따른다.

제15조(개인정보의 생성) 업무부서가 그 업무 수행을 위하여 정보주체에 관한 개인정보를 생성하는 경우, 생성된 개인정보를 처리할 때에는 수집된 개인정보와 마찬가지로 취급하여야 한다.

제16조(개인정보의 수집·생성 제한) ① 업무부서는 그 목적에 필요한 최소한의 개인정보만을 수집·생성하여야 한다.

② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.

③ 업무부서는 정보주체가 **필요한 최소한의 정보 외의 개인정보 수집에 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니된다.**

제17조(개인정보의 이용) ① 개인정보를 수집·생성한 업무부서는 그 정보를 수집·생성한 목적범위 내에서 그 개인정보를 이용할 수 있다.

② 제1항 이외의 소속부서도 제1항의 업무부서가 수집·생성한 목적범위 내에서 그 개인정보를 이용할 수 있다.

③ 제1항 및 제2항의 업무부서(소속부서 포함)는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다.

제17조의2(개인정보의 추가적인 이용·제공) ① ○○○대학교는 당초 수집 목적과 합리적으로 관련된 범위 내에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 제2항 각 호의 기준에 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용하거나 제공할 수 있다.

② ○○○대학교는 법 제15조제3항 또는 법 제17조4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공하는 경우에는 다음 각 호의 사항을 고려해야 한다.

1. 당초 수집 목적과 관련성이 있는지 여부
2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부
3. 정보주체의 이익을 부당하게 침해하는지 여부
4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

③ ○○○대학교는 개인정보의 추가적인 이용 또는 제공이 지속적으로 발생하는 경우에는 제2항의 각 호의 고려사항에 대한 판단 기준을 법 제30조 제1항에 따른 개인정보처리방침에 **공개하고**, 법 제31조 제1항에 따른 개인정보 보호책임자가 해당 기준에 따라 개인정보의 추가적인 이용 또는 제공을 하고 있는지 여부를 점검해야 한다.

④ 제3항에 따라 업무부서는 개인정보의 추가적인 이용 또는 제공에 대한 관리대장을 작성 관리해야 한다.

제18조(개인정보의 제공) ① 개인정보의 “제공”이란 개인정보의 저장매체 또는 개인정보가 담긴 출력물이나 책자 등의 물리적 이전, 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제3자의 접근권한 부여, 제3자와의 개인정보 공유 등 제3자에게 개인정보를 이전하거나 제3자가 개인정보를 공동으로 이용할 수 있도록 하는 모든 행위를 말한다.

② 제1항에서의 “제3자”란 정보주체와 정보주체 또는 그의 법정대리인으로부터 개인정보를 수집·보유한 ○○○대학교를 제외한 모든 자를 의미하며 수탁자는 제외한다.

③ 업무부서는 다음 각 호의 경우에 개인정보를 수집·생성한 목적 범위 내에서 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

1. 정보주체로부터 사전에 별도의 동의를 받은 경우
2. 제14조제2항제2호, 제3호, 제5호, **제6호, 제11호**에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

④ 제3항에 필요한 고지 및 동의의 방법은 이 장 제2절에 따른다.

⑤ 개인정보를 제공받는 자에게 이용 목적, 방법, 기간, 형태 등을 제한하거나 개인정보 안전성 확보조치를 마련하도록 문서로 요청하여야 한다.

⑥ 업무부서는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다.

제2관 개인정보의 목적 외 이용 및 제공

제19조(개인정보의 목적 외 이용 및 제공) ① 업무부서는 개인정보를 수집·생성한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 개인정보를 제공하여서는 아니 된다. 단 제2항의 경우에는 그러하지 아니하다.

② 업무부서는 다음 각 호의 경우에는 개인정보를 목적 외의 용도로 이용하거나 목적 외의 용도로 제3자에게 제공할 수 있다. 단, 정보주체 또는 타인의 이익을 부당하게 침해할 우려가 있을 때를 제외한다.

1. 정보주체로부터 별도의 동의를 받은 경우
 2. 다른 법률에 특별한 규정이 있는 경우
 3. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
 4. 개인정보를 목적 외의 용도로 이용하거나 목적 외의 용도로 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 법 제7조의9에 따른 개인정보 보호위원회의 심의·의결을 거친 경우
 5. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
 6. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
 7. 법원의 재판업무 수행을 위하여 필요한 경우
 8. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우
 9. **공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우**
- ③ 제2항에 필요한 고지 및 동의의 방법은 이 장 제2절에 따른다.

제20조(개인정보의 목적 외 이용 및 제공 시 조치) ① 업무부서가 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 제3자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 소속기관에 문서로 알려야 한다.

② 업무부서가 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우, 개인정보를 제공하는 소속기관과 개인정보를 제공받는 자는 개인정보의 안전성에 관한 책임관계를 명확히 정하여야 한다.

③ 업무부서가 개인정보를 목적 외의 용도로 이용하거나 목적 외의 용도로 제3자에게 제공하는 경우에는 다음 각 호의 사항을 별지 제2호서식의 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리하여야 한다.

1. 이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭
2. 이용기관 또는 제공받는 기관의 명칭
3. 이용 목적 또는 제공받는 목적
4. 이용 또는 제공의 법적 근거
5. 이용하거나 제공하는 개인정보의 항목

6. 이용 또는 제공의 날짜, 주기 또는 기간

7. 이용하거나 제공하는 형태

8. 제1항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용

④ 업무부서가 정보주체의 동의 없이 개인정보를 목적 외의 용도로 이용하거나 목적 외의 용도로 제3자에게 제공하는 경우에는, 다음 각 호의 사항을 목적 외 이용 등을 한 날부터 30일 이내에 인터넷 홈페이지에 10일 이상 계속 게재하여야 한다.

1. 이용 또는 제공의 일자

2. 이용 또는 제공의 법적 근거

3. 이용 또는 제공의 목적

4. 이용 또는 제공하는 개인정보의 항목

⑤ 업무부서가 인터넷 홈페이지를 운영하지 않는 등 제4항의 내용을 인터넷 홈페이지에 게재할 수 없는 사정이 있는 경우에는 제11조제3항의 규정을 준용한다.

⑥ 개인정보처리자는 법적근거에 의하여 개인정보를 제3자에 제공하고 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 되며, 이 외의 경우 개인정보를 재 제공한 자에게 개인정보처리자가 개인정보 제공을 중단 할 수 있다.

1. 정보주체로부터 별도의 동의를 받은 경우

2. 다른 법률에 특별한 규정이 있는 경우

⑦ 개인정보 재 제공 중단절차는 다음 각 호의 순서를 따른다.

1. 개인정보취급자는 개인정보 재 제공사실을 확인한 후 개인정보 보호담당자에게 알린다.

2. 개인정보취급자는 개인정보 재 제공 즉시 중지를 요청한다.

3. 개인정보취급자는 개인정보 재 제공 사실에 대한 소명접수(공문 접수)를 요청한다.

4. 개인정보 보호담당자는 위반사항에 대한 조치방안을 수립하여 개인정보 보호책임자에게 보고한다.

5. 개인정보 보호책임자는 개인정보 보호담당자가 보고한 사항을 검토하여 그 적정성을 판단한 후 승인 여부를 결정한다.

6. 개인정보취급자는 조치방안에 대한 후속조치를 취하고 그 결과를 개인정보보호 담당자에게 알린다.

제3관 개인정보의 수집, 생성, 이용 후 조치

제21조(정보주체의 사전 동의가 없었던 경우의 개인정보 수집, 생성, 이용 후 조치) 업무부서가 제14조제2항제5호, 제18조제3항제2호, 제19조제2항제3호에 따라 정보주체의 사전 동의 없이 개인정보를 수집·이용 또는 제공한 경우, 당해 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집·이용 또는 제공한 사실 및 그 사유와 이용내역을 알려야 한다.

제22조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 통지) ① 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 요구가 있는 날로부터 3일 이내에 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.

1. 개인정보의 수집 출처

2. 개인정보의 처리 목적

3. 제78조에 따른 개인정보 처리의 정지를 요구하거나 동의를 철회할 권리가 있다는 사실

② 제1항에도 불구하고 다음 각 호에 해당하는 업무부서는 제1항 각 호의 모든 사항을 서면·전화·문자전송·전자우편 등 정보주체가 쉽게 알 수 있는 방법 또는 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법으로 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알려야 한다.

1. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 업무부서(3개월 간 일일 평균 기준)

2. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 업무부서(3개월 간 일일 평균 기준)

③ 제2항의 경우로 제24조제2항제1호로부터 제4호까지의 사항에 대하여 제18조제3항제1호에 따라 정보주체의 동의를 받아 연 2회 이상 주기적으로 개인정보를 제공받아 처리하는 경우에는 개인정보를 제공받은 날로부터 3개월 이내에 정보주체에게 알리거나 그 동의를 받은 날부터 가산하여 연 1회 이상 정보주체에게 알려야 한다.

1. 서면·전자우편·전화·문자전송 등 정보주체가 통지 내용을 쉽게 확인할 수 있는 방법

2. 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법

④ 제1항과 제2항 본문은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 정보주체의 권리보다 명백히 우선하는 경우에 한한다.

1. 고지를 요구하는 대상이 되는 개인정보가 제52조 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우

2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

⑤ 업무부서는 다음 각 호의 어느 하나에 해당하고, 각 호가 보호하고자 하는 법익을 정보주체의 권리보다 명백히 우선하여 보호할 필요가 있는 경우에는 제1항의 요구를 거부할 수 있다.

1. 통지를 요구하는 대상이 되는 개인정보가 제52조에 해당하는 개인정보파일에 포함되어 있는 경우

2. 통지로 인하여 타인의 생명·신체를 해할 우려가 있거나 타인의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

⑥ 업무부서는 정당한 사유가 없는 한 요구가 있는 날로부터 3일 이내에 제1항에서 정한 사항 또는 제5항에 따른 거부의 근거와 사유를 정보주체에게 알려야 한다.

⑦ 업무부서는 제2항에 따라 개인정보의 수집 출처 등에 관한 사항을 알리는 것과 제22조의 제1항에 따른 이용·제공 내역의 통지를 함께 할 수 있다.

⑧ 제1항 각 호의 어느 하나에 해당하는 업무부서는 제2항에 따라 알린 경우 다음 각 호의 사항을 제23조 또는 제78조제5항에 따라 해당 개인정보를 파기할 때까지 보관·관리하여야 한다.

1. 정보주체에게 알린 사실

2. 알린 시기

3. 알린 방법

제22조의2(개인정보 이용·제공 내역의 통지) ① 다음 각 호에 어느 하나에 해당하는 업무부서는 수집한 개인정보의 이용·제공 내역이나 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 주기적으로 정보주체에게 통지하여야 한다. 다만, 연락처 등 정보주체에게 통지할 수 있는 개인정보를 수집·보유하지 아니한 경우에는 통지하지 아니할 수 있다.

1. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자(3개월 간 일일 평균 기준)
2. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자(3개월 간 일일평균 기준)

② 제1항에 따른 통지의 대상이 되는 정보주체는 다음 각 호의 정보주체를 제외한 정보주체로 한다.

1. 통지에 대한 거부 의사 표시한 정보주체
2. 개인정보처리자가 업무수행을 위해 그에 소속된 임직원의 개인정보를 처리한 경우 해당 정보주체
3. 개인정보처리자가 업무수행을 위해 다른 공공기관, 법인, 단체의 임직원 또는 개인의 연락처 등의 개인정보를 처리한 경우 해당 정보주체
4. 법률에 특별한 규정이 있거나 법령 상 의무를 준수하기 위하여 이용·제공한 개인정보의 정보주체
5. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 이용·제공한 개인정보의 정보주체

③ 제1항에 따라 정보주체에게 통지해야 하는 정보는 다음 각 호와 같다.

1. 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목
2. 개인정보를 제공받은 제3자와 그 제공 목적 및 제공한 개인정보의 항목. 다만, 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 제외한다.

④ 제1항에 따른 통지는 다음 각 호의 어느 하나에 해당하는 방법으로 연1회 이상 해야 한다.

1. 서면·전자우편·전화·문자전송 등 정보주체가 통지 내용을 쉽게 확인할 수 있는 방법
2. 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법(제1항에 따른 개인정보의 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 통지하는 경우로 한정한다)

제4관 개인정보의 파기

제23조(개인정보의 파기) ① 업무부서는 보유기간의 경과, 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과, 해당서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 5일 이내에 그 개인정보를 파기하여야 한다. 단, 「공공기록물 관리에 관한 법률」등 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니한다. **[개정 2024.2.]**

② 업무부서가 제1항 본문에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 다음 각 호의 구분에 따른 방법으로 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

③ 업무부서가 개인정보의 일부만을 파기하는 경우, 제2항의 방법으로 파기하는 것이 어려운 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독

2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

④ 업무부서가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보를 다른 개인정보와 분리하여서 저장·관리하여야 하며, 법령에 따라 해당 개인정보를 보존한다는 점을 분명히 표시하여야 한다.

⑤ 업무부서는 개인정보의 파기에 관한 사항을 기록·관리하여야 하며, 이를 받기 1회 이상 개인정보보호 분야별 책임자에게 보고하여야 한다.

⑥ 개인정보보호 분야별 책임자는 개인정보의 보유 기간 만료 등에 따른 구체적 파기 시점·방법 등을 반영한 개인정보 파기계획을 수립·시행하고 파기계획은 개인정보처리방침에 포함하여 시행하여야 하며 개인정보의 파기 결과를 확인하여야 한다.

제2절 개인정보의 수집, 이용, 제공을 위한 고지 및 동의

제1관 개인정보의 수집, 이용 및 제공을 위한 고지 및 동의

제24조(동이가 필요한 경우의 고지의무 및 개인정보 이전 고지) ① 업무부서가 정보주체의 동의를 받아 개인정보를 수집·이용하고자 하는 경우 다음 각 호의 사항을 정보주체에게 알려야 한다.

1. 개인정보의 수집·이용 목적

2. 수집하려는 개인정보의 항목

3. 개인정보의 보유 및 이용 기간

4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

② 업무부서가 정보주체의 동의를 받아 개인정보를 제공하고자 하는 경우 다음 각 호의 사항을 정보주체에게 알려야 한다.

1. 개인정보를 제공받는 자(제공받는 자의 성명과 연락처를 포함한다)

2. 개인정보를 제공받는 자의 개인정보 이용 목적

3. 제공하는 개인정보의 항목

4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 업무부서는 제1항 또는 제2항 각 호의 어느 하나의 사항을 변경하는 경우에도 정보주체에게 이를 알리고 동의를 받아야 한다.

④ 업무부서가 개인정보를 국외의 제3자에게 제공할 때에도 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 내부관리계획을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

⑤ 업무부서는 ○○○대학교 이외의 다른 사람에게 개인정보를 이전 시에는 다음 각 호의 사항을 통지 내용에 포함하여야 한다.

1. 개인정보를 이전하려는 사실

2. 이전받는 자의 성명(또는 법인의 명칭), 주소, 전화번호 및 그 밖의 연락처
 3. 정보주체가 개인정보의 이전을 원하지 않는 경우 조치할 수 있는 방법 및 절차
- ⑥ 업무부서는 다른 사람에게 개인정보를 이전 통지 시 그 방법은 다음 각 호의 사항에 따라 실시하여야 한다.
1. 서면 등의 방법으로 정보주체에게 직접 통지
 2. 서면 등의 방법으로 직접 통지가 어려운 경우 인터넷 홈페이지에 30일 이상 게시하고 인터넷 홈페이지에 게재할 수 없는 정당한 사유가 있는 경우에는 다음 각 목의 어느 하나의 방법으로 제5항의 각 호를 정보주체에게 알릴 수 있다. [개정, 2021. 3.]
- 가) 이전받는 자의 사업장등의 보기 쉬운 장소에 30일 이상 게시하는 방법
- 나) 이전받는 자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 또는 같은 조 제2호에 따른 일반일간신문·일반주간신문 또는 인터넷신문에 실는 방법

제25조(동의가 필요한 개인정보와 동의가 필요하지 않은 개인정보의 구분) ① 업무부서가 이 내부관리계획이 규정하는 바에 따라 정보주체의 동의 없이도 정보주체의 개인정보를 수집·이용 및 제공할 수 있는 경우, 업무부서는 본 내부관리계획에서 달리 정하는 바를 제외하고는 원칙적으로 정보주체에 대하여 어떠한 고지의무도 부담하지 않는다.

② 업무부서가 이 내부관리계획이 규정하는 바에 따라 정보주체의 동의를 얻어 정보주체의 개인정보를 수집·이용 및 제공하고자 하는 경우, 우선 업무부서가 수집·이용 및 제공하고자 하는 개인정보에 정보주체의 동의가 필요한 개인정보와 그렇지 않은 개인정보가 혼재되어 있는지 검토하여야 한다.

③ 제2항의 검토 결과 정보주체의 동의가 필요한 개인정보와 그렇지 않은 개인정보가 혼재되어 있는 경우, 업무부서는 동의가 필요한 개인정보와 그렇지 않은 개인정보를 명확히 구분하여야 한다.

④ 제3항의 경우 업무부서는 제1항에도 불구하고 정보주체의 동의가 필요한 개인정보에 대하여 제24조의 고지의무를 이행하는 과정에서 정보주체의 동의가 필요하지 않은 개인정보에 대하여도 다음 각 호의 사항을 정보주체에게 함께 알려야 한다.

1. 정보주체의 동의를 받아 수집·이용 및 제공하는 개인정보와는 별도로 정보주체의 동의 없이 수집·이용 및 제공할 수 있는 개인정보가 있다는 점과 그 대상
2. 수집·이용 및 제공 사유

⑤ 제2항의 검토 결과 정보주체의 동의가 필요한 개인정보와 그렇지 않은 개인정보가 혼재되어 있지 않은 경우 업무부서는 제3항과 제4항의 의무를 이행하지 아니하여도 된다.

제26조(동의를 받는 방법) ① 업무부서는 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다. 이 경우 다음 각 호의 동의 사항을 구분하여 각각 동의를 받아야 한다.

1. 제14조제2항제2호에 따라 동의를 받는 경우
2. 제18조제3항제1호에 따라 동의를 받는 경우
3. 제19조제2항제1호에 따라 동의를 받는 경우
4. 개인정보 제공받는 자가 정보주체로부터 별도의 동의를 받은 경우

5. 제32조제2항에 따라 동의를 받는 경우

6. 제35조제1항제1호에 따라 동의를 받는 경우

7. 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 경우

8. 그 밖에 정보주체를 보호하기 위하여 동의 사항을 구분하여 동의를 받아야 할 필요가 있는 경우

② 개인정보처리자는 제1항의 동의를 서면(「전자문서 및 전자거래 기본법」 제2조제1호에 따른 전자문서를 포함한다)으로 받을 때에는 개인정보의 수집·이용 목적, 수집·이용하려는 개인정보의 항목 등 다음 각 호에서 정하는 중요한 내용을 개인정보보호위원회(이하 “보호위원회”라고도 한다.)가 고시로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다.

1. 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실

2. 처리하려는 개인정보의 항목 중 다음 각 목의 사항

가. 민감정보

나. 제34조제2호부터 제4호까지의 규정에 따른 여권번호, 운전면허의 면허번호 및 외국인등록번호

3. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)

4. 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

③ 업무부서는 정보주체의 동의를 받을 때에는 다음 각 호의 조건을 모두 충족해야 한다.

1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것

2. 동의를 받으려는 내용이 구체적이고 명확할 것

3. 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것

4. 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것

④ 업무부서는 개인정보의 처리에 대하여 다음 각 호의 어느 하나에 해당하는 방법으로 정보주체의 동의를 받아야 한다.

1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 직접 서명하거나 날인한 동의서를 받는 방법

2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법

3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷 주소 등을 통하여 동의내용을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의 의사표시를 확인하는 방법

4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법

5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편 및 이에 준하는 전자적 확인을 받는 방법

6. 그 밖에 제1호부터 제5호까지의 규정에 따른 법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

⑤ 제4항제2호에 따라 전화에 의한 동의와 관련하여 업무부서가 통화내용을 녹취할 때에는 녹취 사실을 정보주체에게 알려야 한다.

제2관 개인정보의 목적 외 이용, 목적 외 제3자 제공을 위한 고지 및 동의

제27조(개인정보의 목적 외 이용, 목적 외 제3자 제공 시의 고지의무) ① 업무부서가 정보주체의 별도의 동의를 받아 개인정보를 수집·생성한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공하고자 하는 경우 제24조제2항 각 호의 사항을 정보주체에게 알려야 한다.

② 업무부서는 제1항 각 호의 어느 하나의 사항을 변경하는 경우에도 정보주체에게 이를 알리고 동의를 받아야 한다.

제28조(개인정보의 목적 외 이용, 목적 외 제3자 제공 시 동의를 받는 방법) 업무부서가 정보주체의 별도의 동의를 받아 개인정보를 수집·생성한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공하고자 하는 경우 제25조와 제26조를 준용한다. 이 경우 제25조의 “제24조의 고지의무”는 “제27조의 고지의무”로 보며, 제25조와 제26조의 “수집·이용 및 제공”과 “제공”은 “목적 외 이용·목적 외 제3자 제공”으로 본다.

제3관 아동의 개인정보 보호

제29조(아동의 개인정보) ① 업무부서가 만 14세 미만 아동의 개인정보를 처리하기 위하여 **개인 정보 보호법**에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 하며, 법정대리인이 동의하였는지를 확인하는 경우에는 다음 각 호의 어느 하나에 해당하는 방법으로 해야 한다.

1. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 개인정보처리자가 그 동의 표시를 확인했음을 법정대리인의 휴대전화 문자메시지로 알리는 방법
 2. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법
 3. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 휴대전화 본인인증 등을 통하여 본인 여부를 확인하는 방법
 4. 동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나 우편 또는 팩스를 통하여 전달하고, 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법
 5. 동의 내용이 적힌 전자우편을 발송하고 법정대리인으로부터 동의의 의사표시가 적힌 전자우편을 전송받는 방법
 6. 전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 받거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 받는 방법
 7. 그 밖에 제1호부터 제6호까지의 규정에 준하는 방법으로서 법정대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법
- ② 제1항에도 불구하고 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보로서 성명, 연락처에 관한 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있으며, 이 경우 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다.
- ③ 업무부서는 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우에는 인터넷주소 또는 사업장 전화번호 등 동의 내용을 확인할 수 있는 방법을 법정대리인에게 안내할 수 있다.

제4관 동의의무의 예외

제30조(친목단체에 대한 동의의무의 예외) 개인정보취급자가 친목단체의 운영을 위하여 다음 각 호의 어느 하나에 해당하는 개인정보를 수집·이용하는 경우에는 정보주체에 대한 동의의무를 부담하지 않는다.

1. 친목단체의 가입을 위한 성명, 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항
2. 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부현황에 관한 사항
3. 친목단체의 활동에 대한 구성원의 참석여부 및 활동내용에 관한 사항
4. 기타 친목단체의 구성원 상호간의 친교와 화합을 위해 구성원이 다른 구성원에게 알리기를 원하는 생일, 취향 및 가족의 애경사에 관한 사항

제3절 민감정보와 고유식별정보의 처리

제1관 민감정보의 처리

제31조(민감정보의 정의) ① “민감정보”란 정보주체의 사생활을 현저히 침해할 우려가 있는 개인 정보로서 다음 각 호의 어느 하나에 해당하는 정보를 말한다.

1. 개인의 사상이나 신념에 관한 정보
 2. 노동조합 혹은 정당에의 가입이나 탈퇴에 관한 정보
 3. 개인의 정치적 견해에 관한 정보
 4. 개인의 건강이나 성생활 등에 관한 정보
 5. 유전자검사 등의 결과로 얻어진 유전정보
 6. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보
 7. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보
 8. 인종이나 민족에 관한 정보
- ② 업무부서가 제19조제2항제5호부터 제9호까지의 규정에 따라 제1항제5호부터 제8호까지의 정보를 처리하는 경우의 해당 정보는 민감정보로 보지 않는다

제32조(민감정보의 수집, 생성, 이용 및 제공) ① 업무부서는 민감정보를 수집·생성·이용 및 제공 하여서는 아니 된다. 단, 제2항과 제3항의 경우에는 그러하지 아니하다.

② 정보주체에게 제38조1항 및 2항의 각 호의 사항을 알리고 개인정보의 처리에 대한 별도의 동의를 받은 경우 민감정보를 수집·생성·이용 및 제공할 수 있다.

③ 업무부서는 법령에서 민감정보의 수집·생성·이용 및 제공을 요구하거나 허용하는 경우에는 정보주체의 별도의 동의가 없더라도 민감정보를 수집·생성·이용 및 제공할 수 있다.

④ 업무부서는 제2항과 제3항에 따라 민감정보를 수집·생성·이용 및 제공하는 경우, 필요한 최소한의 한도 내에서만 민감정보를 수집·생성·이용 및 제공하여야 한다.

⑤ 업무부서는 제2항과 제3항에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 하여야 한다.

⑥ 제2항에 필요한 고지 및 동의의 방법은 이 장 제4절에 따른다.

⑦ 개인정보처리자는 재화 또는 서비스를 제공하는 과정에서 공개되는 정보에 정보주체의 민감정보가 포함됨으로써 사생활 침해의 위험성이 있다고 판단하는 때에는 재화 또는 서비스의 제공 전에 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 정보주체가 알아보기 쉽게 알려야 한다.

제33조(민감정보의 목적 외 이용, 목적 외 제3자 제공) ① 업무부서는 민감정보를 수집·생성한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공하여서는 아니 된다. 단, 제2항과 제3항의 경우에는 그러하지 아니하다.

② 업무부서는 정보주체로부터 민감정보의 목적 외 이용, 목적 외 제3자 제공에 대한 별도의 동의(제32조제2항의 동의와는 별개의 동의를 말한다)를 받은 경우에는 민감정보를 수집·생성한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공할 수 있다. 단, 정보주체 또는 타인의 이익을 부당하게 침해할 우려가 있을 때를 제외한다.

③ 업무부서는 법령에서 민감정보의 목적 외 이용, 목적 외 제3자 제공을 요구하거나 허용하는 경우에는 정보주체의 동의가 없더라도 민감정보를 수집·생성한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공할 수 있다. 단, 정보주체 또는 타인의 이익을 부당하게 침해할 우려가 있을 때를 제외한다.

④ 업무부서가 민감정보를 수집·생성한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공할 경우 준수하여야 할 구체적인 사항에 관하여는 제20조를 준용한다. 이 경우 “개인정보”는 “민감정보”로 본다.

⑤ 제2항에 필요한 고지 및 동의의 방법은 이 장 제4절에 따른다.

제2관 고유식별정보 및 주민등록번호의 처리

제34조(고유식별정보의 정의) ① “고유식별정보”란 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 다음 각 호의 어느 하나에 해당하는 정보를 말한다.

1. 「주민등록법」 제7조의2제1항에 따른 주민등록번호
2. 「여권법」 제7조제1항제1호에 따른 여권번호
3. 「도로교통법」 제80조에 따른 운전면허의 면허번호
4. 「출입국관리법」 제31조제5항에 따른 외국인등록번호

② 업무부서가 제19조제2항제5호부터 제9호까지의 규정에 따라 정보를 제1항 각 호의 정보를 처리하는 경우의 해당 정보는 고유식별정보로 보지 않는다.

제35조(고유식별정보의 수집, 이용, 제공) ① 업무부서는 다음 각 호의 경우를 제외하고는 고유식별정보를 수집·이용 및 제공하여서는 아니 된다.

1. 정보주체에게 제38조 1항 및 2항의 각 호의 사항을 알리고 개인정보의 처리에 대한 별도의 동의를 받은 경우
2. 업무부서는 법령에서 구체적으로 고유식별정보의 수집·이용 및 제공을 요구하거나 허용하는 경우

② 업무부서는 제1항에 따라 고유식별정보를 수집·이용 및 제공하는 경우 필요한 최소한의 한도 내에서만 고유식별정보를 수집·이용 및 제공하여야 한다.

③ 업무부서는 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 등 안전성 확보에 필요한 조치를 하여야한다.

④ 제1항에 필요한 고지 및 동의의 방법은 이 장 제4절에 따른다.

제35조의2(주민등록번호 처리의 제한) ① 제35조제1항에도 불구하고 업무부서는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 수집·이용 및 제공하여서는 아니 된다.

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
 3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우
- ② 업무부서는 제35조제3항에도 불구하고 주민등록번호가 분실·도난·유출·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 「개인정보 보호법 시행령」으로 정한다.
- ③ 업무부서는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

제36조(고유식별정보의 목적 외 이용, 목적 외 제3자 제공) ① 업무부서는 정보주체의 고유식별정보를 수집한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공하여서는 아니 된다. 단, 다음 각 호의 경우에는 그러하지 아니하다.

1. 정보주체로부터 고유식별정보의 목적 외 이용·목적 외 제3자 제공에 대한 별도의 동의(제35조제1항의 동의와는 별개의 동의를 말한다)를 받은 경우(단, 정보주체 또는 타인의 이익을 부당하게 침해할 우려가 있을 때를 제외한다.)
 2. 법령에서 고유식별정보의 목적 외 이용·목적 외 제3자 제공을 요구하거나 허용하는 경우(단, 정보주체 또는 타인의 이익을 부당하게 침해할 우려가 있을 때를 제외한다.)
- ② 업무부서가 고유식별정보를 수집한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공할 경우 준수하여야 할 구체적인 사항에 관하여 제20조를 준용한다. 이 경우 “개인정보”는 “고유식별정보”로 본다.
- ③ 제1항에 필요한 고지 및 동의의 방법은 이 장 제4절에 따른다.

제36조2 (주민등록번호의 목적 외 이용, 목적 외 제3자 제공) ① 업무부서는 정보주체의 주민등록번호를 수집한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공하여서는 아니 된다. 단, 다음 각 호의 경우에는 그러하지 아니하다.

1. 법령에서 주민등록번호의 목적 외 이용·목적 외 제3자 제공을 요구하거나 허용하는 경우(단, 정보주체 또는 타인의 이익을 부당하게 침해할 우려가 있을 때를 제외한다.)
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우

② 업무부서가 주민등록번호를 수집한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공할 경우 준수하여야 할 구체적인 사항에 관하여 제20조를 준용한다. 이 경우 “개인정보”는 “주민등록번호”로 본다.

③ 제1항에 필요한 고지 및 동의의 방법은 이 장 제4절에 따른다. [신설, 2017. 2.]

제37조(홈페이지 회원가입을 위한 고유식별정보 대체수단 제공) ① 업무부서는 정보주체가 업무부서의 인터넷 홈페이지를 통하여 회원으로 가입하는 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 대체수단을 제공하여야 한다.

② 업무부서는 제1항의 경우 정보주체가 주민등록번호가 아닌 대체수단을 사용하여서도 회원으로 가입할 수 있다는 점을 회원가입을 위한 화면에서 명시적으로 알아볼 수 있도록 필요한 조치를 취하여야 한다.

③ 업무부서는 제2항의 경우 주민등록번호를 이용한 회원가입 방법과 대체수단을 이용한 회원가입 방법을 하나의 화면을 통하여 제공하여야 한다.

제4절 민감정보와 고유식별정보의 처리를 위한 고지 및 동의

제38조(민감정보와 고유식별정보의 수집, 이용, 제공 시의 고지의무 등) ① 업무부서는 정보주체의 별도의 동의를 받아 민감정보 또는 고유식별정보를 수집·이용하고자 하는 경우 다음 각 호의 사항을 정보주체에게 알려야 한다.

1. 민감정보 또는 고유식별정보의 수집·이용 목적
2. 수집하려는 민감정보 또는 고유식별정보의 항목
3. 민감정보 또는 고유식별정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

② 업무부서는 정보주체의 별도의 동의를 받아 민감정보 또는 고유식별정보를 제공하고자 하는 경우 다음 각 호의 사항을 정보주체에게 알려야 한다.

1. 민감정보 또는 고유식별정보를 제공받는 자(제공받는 자의 성명(법인, 단체일 경우 그 명칭)과 연락처를 포함한다)
2. 민감정보 또는 고유식별정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 민감정보 또는 고유식별정보의 항목
4. 민감정보 또는 고유식별정보를 제공받는 자의 개인정보보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 업무부서는 제1항 또는 제2항 각 호의 어느 하나의 사항을 변경하는 경우에도 정보주체에게 이를 알리고 동의를 받아야 한다.

④ 업무부서는 민감정보 또는 고유식별정보를 국외의 제3자에게 제공할 때에도 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 내부관리계획을 위반하는 내용으로 민감정보 또는 고유식별정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

⑤ 정보주체에게 고유식별정보·민감정보 처리에 대해 별도로 동의를 받거나, 법령에서 처리를 요구하거나 허용하는 경우에 한하여 사용하되 원칙적으로 수집, 이용 및 제공은 금지한다.

⑥ 인터넷 홈페이지에서 회원가입시 주민등록번호를 필요로 하는 경우 공공 아이디 등 주민등록번호 대체수단을 제공하여야 하며, 주민등록번호와 대체수단에 의한 가입 방법을 같은 화면에서 제공되어야 한다.

⑦ 주민등록번호는 반드시 개인정보 보호책임자 승인 후에 보유하도록 한다.

제39조(민감정보와 고유식별정보의 수집, 이용, 제공 시 동의를 받는 방법) 업무부서가 정보주체의 별도의 동의를 받아 민감정보 또는 고유식별정보를 수집·이용 및 제공하고자 하는 경우 제25조, 제26조, 제29조를 준용한다. 이 경우 제25조의 “제24조의 고지의무”는 “제38조의 고지의무”로 보며, 제25조, 제26조, 제29조의 “개인정보”는 “민감정보 또는 고유식별정보”로 본다.

제40조(민감정보와 고유식별정보의 목적 외 이용 및 목적 외 제3자 제공 시의 고지의무)

① 업무부서가 정보주체의 별도의 동의를 받아 민감정보 또는 고유식별정보를 수집·생성한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공하고자 하는 경우 제24조 제2항의 각 호의 사항을 정보주체에게 알려야 한다.

② 업무부서는 제1항 각 호의 어느 하나의 사항을 변경하는 경우에도 정보주체에게 이를 알리고 동의를 받아야 한다.

제41조(민감정보와 고유식별정보의 목적 외 이용, 목적 외 제3자 제공 시 동의를 받는 방법) 업무부서가 정보주체의 별도의 동의를 받아 민감정보 또는 고유식별정보를 수집·생성한 목적의 범위를 초과하여 이용하거나 그러한 이용을 위해 제3자에게 제공하고자 하는 경우 제25조, 제26조, 제29조를 준용한다. 이 경우 제25조의 “제24조의 고지의무”는 “제40조의 고지의무”로 보며, 제25조, 제26조, 제29조의 “개인정보”는 “민감정보 또는 고유식별정보”로, “수집·이용 및 제공”과 “제공”은 “목적 외 이용·목적 외 제3자 제공”으로 본다.

제5절 영상정보처리기기

제42조(고정형 영상정보처리기기의 설치 및 운영) ① ○○○대학교의 고정형 영상정보처리기기에 의해 처리되는 개인영상정보는 관련 법령 및 이 내부관리계획에 의해 보호되어야 한다.

② 업무부서가 고정형 영상정보처리기기를 설치·운영하고자 할 때에는 [붙임 1]의 ‘○○○대학교 고정형 영상정보처리기기 표준 지침’에 따라야 한다.

③ 업무부서가 고정형 영상정보처리기기를 설치·운영하는 경우에는 제2항의 지침의 준수 여부에 대한 자체점검을 실시한 후 개인정보보호위원회 개인정보보호 종합지원시스템(intra.privacy.go.kr)에 등록하고 그 결과를 개인정보 보호책임자에게 제출하여야 한다.

제42조의2(이동형 영상정보처리기기의 운영 제한) ① ○○○대학교의 이동형 영상정보처리기기에 의해 처리되는 개인영상정보는 관련 법령 및 이 내부관리계획에 의해 보호되어야 하며, 업무를 목적으로 이동형 영상정보처리기기를 운영하려는 업무부서는 다음 각 호의 경우를 제외하고는 공개된 장소에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상(개인정

보에 해당하는 경우로 한정한다. 이하 같다)을 촬영하여서는 아니 된다.

1. 제14조제2항 각 호의 어느 하나에 해당하는 경우
 2. 촬영 사실을 명확히 표시하여 정보주체가 촬영 사실을 알 수 있도록 하였음에도 불구하고 촬영 거부 의사를 밝히지 아니한 경우. 이 경우 정보주체의 권리를 부당하게 침해할 우려가 없고 합리적인 범위를 초과하지 아니하는 경우로 한정한다.
 3. 그 밖에 제1호 및 제2호에 준하는 경우로서 범죄, 화재, 재난 또는 이에 준하는 상황에서 인명의 구조·구급 등을 위하여 사람 또는 그 사람과 관련된 사물의 영상(개인정보에 해당하는 경우로 한정한다. 이하 같다)의 촬영이 필요한 경우
- ② 업무부서가 이동형 영상정보처리기를 설치·운영하고자 할 때에는 [붙임 1]의 ‘○○○대학교 고정형 영상정보처리기기 표준 지침’을 준용하여 다음 각 호의 사항이 포함된 이동형 영상정보처리기기 운영·관리 방침을 마련하여야 한다.
1. 이동형 영상정보처리기기의 운영 근거 및 운영 목적
 2. 이동형 영상정보처리기기의 운영 대수
 3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
 4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
 5. 이동형영상정보처리기기운영자의 영상정보 확인 방법 및 장소
 6. 정보주체의 영상정보 열람 등 요구에 대한 조치
 7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
 8. 그 밖에 이동형 영상정보처리기기의 설치·운영 및 관리에 필요한 사항
- ③ 업무부서가 제2항에 따라 이동형 영상정보처리기기 운영·관리 방침을 마련하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

제6절 개인정보처리업무의 위탁

제43조(개인정보처리업무의 위탁) ① 업무부서는 ○○○대학교 이외의 자에게 다음 각 호의 내용이 포함된 문서에 의하여 개인정보의 처리 업무를 위탁할 수 있다. 이 경우 ○○○대학교를 “위탁자”라 한다.
[개정, 2017. 2.]

1. 위탁업무의 목적 및 범위
 2. 재위탁 제한에 관한 사항
 3. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
 4. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
 5. 법 제26조제2항에 따른 수탁자(이하 “수탁자”라 한다)가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항
 6. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
 7. 개인정보의 기술적·관리적 보호조치에 관한 사항
- ② 위탁자는 인력과 물적 시설, 재정 능력, 기술력, 책임능력 등을 종합적으로 고려하여 개인정보를 안전하게 처리할 수 있는 수탁자를 선정하여야 한다. 손해배상책임에 대해 수탁자는 위탁기관의 직원으로 본다.

③ 수탁자는 위탁받은 개인정보의 처리 업무를 제3자에게 다시 위탁하는 경우에는 위탁자의 동의를 받아야 한다.

제44조(정보주체를 위한 위탁사실의 게재) ① 위탁자는 위탁하는 업무의 내용과 수탁자에 관한 정보를 정보주체가 언제든지 쉽게 확인할 수 있도록 위탁자의 인터넷 홈페이지에 지속적으로 게재하여야 한다.

② 위탁자가 인터넷 홈페이지를 운영하지 않는 등 제1항의 내용을 인터넷 홈페이지에 게재할 수 없는 사정이 있는 경우에는 제11조 제3항의 규정을 준용한다.

제45조(위탁자와 수탁자의 의무) ① 위탁자는 수탁자가 개인정보의 처리 업무를 수행하는 경우 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고 처리 현황을 점검하는 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

② 위탁자는 수탁자에 대한 감독을 통해 개인정보 처리 업무의 지연, 처리 업무와 관련 없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 종합적으로 검토하여 이를 방지하기 위하여 필요한 조치를 마련하여야 한다.

③ 수탁자는 위탁받은 개인정보를 보호하기 위하여 개인정보의 안전성 확보조치 기준에 따라 조치를 취해야한다. 또한 위탁자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 안 된다.

④ 수탁자에 관하여는 개인정보 보호법 제15조부터 제18조까지, 제21조, 제22조, 제22조의2, 제23조, 제24조, 제24조의2, 제25조, 제25조의2, 제27조, 제28조, 제28조의2부터 제28조의5까지, 제28조의7부터 제28조의11까지, 제29조, 제30조, 제30조의2, 제31조, 제33조, 제34조, 제34조의2, 제35조, 제35조의2, 제36조, 제37조, 제37조의2, 제38조, 제59조, 제63조, 제63조의2 및 제64조의2를 준용한다. 이 경우 “개인정보처리자”는 “수탁자”로 본다.

제7절 개인정보취급자에 대한 관리 및 감독

제46조(개인정보취급자에 대한 관리 및 감독) ① 업무부서는 개인정보취급자를 업무부서의 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.

② 업무부서는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 적절한 관리·감독을 하여야 한다.

제8절 가명정보의 처리에 관한 특례

제46조의2(가명정보의 처리 등) ① 업무부서는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

② 업무부서는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.

③ 업무부서는 가명 처리한 가명정보가 개인정보를 포함하고 있는지 적정성 검토를 거친 후에 가명정보를 처리할 수 있다. 적정성 검토와 관련된 주요 사항은 교육분야 가명·익명정보 처리 가이드라인을 준용한다.

제46조의3(가명정보의 결합 제한) ① 업무부서는 통계작성, 과학적 연구, 공익적 기록보존 등을 위해 가명정보의 내부결합을 할 수 있다.

② 제1항의 경우에도 불구하고 업무부서가 다른 업무부서가 보유한 가명정보와의 결합을 하려는 경우에는 개인정보보호 담당부서를 통해 결합을 수행하여야 한다.

③ 업무부서가 보유하는 가명정보와 다른 개인정보처리자가 보유한 가명정보를 결합하려는 경우에는 결합전문기관에 요청하여 결합을 수행해야 한다.

④ 제3항의 경우에도 불구하고 제3자 제공을 목적으로 하거나 다른 개인정보처리자에게 제공하는 것을 목적으로 결합하려는 경우에는 본원의 결합전문기관에서 결합 및 반출 등을 처리할 수 있다.

⑤ 업무부서에서 가명정보를 취급하는 자는 가명처리 전 개인정보를 취급했거나 취급권한을 가진 자와는 업무를 분리하거나 배제해야 한다.

제46조의4(가명정보 및 추가정보에 대한 안전조치의무 등) ① 업무부서는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 가명정보 및 추가정보에 대하여 다음 각 호의 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

1. 개인정보 보호법 시행령 제30조에 따른 안전성 확보 조치

2. 가명정보와 추가정보의 분리 보관. 추가정보는 특별한 이유가 없는 한 생성 즉시 삭제하며, 단, 시계열 분석 등 보관이 필요한 경우에는 가명정보와 분리·보관하고 저장 시 암호화하여 저장하여야 한다.

2의2. 개인정보, 가명정보 및 추가정보는 물리적으로 분리 보관하는 것을 원칙으로 하며, 물리적 보관이 어려운 경우 추가적인 접근통제를 통해 논리적인 분리를 시행할 수 있다.

3. 가명정보와 추가정보에 대한 접근 권한의 분리. 단, 접근 권한은 최소한의 인원으로 통제하며, 업무에 따라 차등적으로 부여해야 한다.

4. 가명정보 또는 추가정보에 대한 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하도록 하고 이 기록은 최소 3년간 보관하여야 한다.

② 업무부서는 제46조의2 또는 제46조의3에 따라 가명정보를 처리하는 경우 처리목적 등을 고려하여 가명정보의 처리 기간을 별도로 정할 수 있다.

③ 업무부서는 제46조의2 또는 제46조의3에 따라 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자, 가명정보의 처리 기간(제2항에 따라 처리 기간을 별도로 정한 경우에 한한다) 등 가명정보 처리 내용을 관리하기 위하여 다음 각 호의사항에 대한 관련 기록을 작성하여 보관하여야 하며, 가명정보를 파기한 경우에는 파기한 날로부터 3년 이상 보관하여야 한다.

1. 가명정보 처리의 목적

2. 가명정보 처리 및 보유기간(제46조의4제2항에 따라 가명정보의 처리 기간을 별도로 정한 경우로 한정한다)

3. 가명처리한 개인정보의 항목

4. 가명정보의 이용내역
5. 제3자 제공 시 제공받는 자
6. 추가 정보의 이용 및 파기 등에 관한 사항 등
7. 그 밖에 가명정보의 처리 내용을 관리하기 위하여 개인정보보호위원회가 필요하다고 인정하여 고시하는 사항

제46조의5(가명정보 처리 시 금지의무 등) ① 제46조의2 또는 제46조의3에 따라 가명정보를 처리하는 자는 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다.

② 업무부서는 제46조의2 또는 제46조의3에 따라 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고 지체 없이 회수·파기하여야 한다. 이 경우, 제3자에게 제공한 가명정보도 관련 절차에 따라 파기하여야 한다.

③ 가명정보를 처리하는 경우 처리 목적을 벗어나서 가명정보를 오·남용해서는 아니 된다.

제46조의6(가명정보 또는 추가정보의 분야별 관리책임자 지정 및 역할) ① 가명정보 관리책임자의 업무를 효율적으로 수행하기 위하여 ○○○대학교 각 업무부서의 장을 가명정보 또는 추가정보의 분야별 관리책임자로 한다.

② 가명정보 또는 추가정보의 분야별 관리책임자는 다음 각 호의 업무를 수행한다.

1. 가명정보 또는 추가정보의 접근권한 관리정책 수립 및 운영
2. 가명정보 또는 추가정보의 접근권한에 대한 관리·감독
3. 개인정보 및 가명정보, 추가정보의 별도 분리 보관
4. 가명정보 재식별 금지를 위한 내부통제시스템 구축
5. 가명정보 재식별 발생시 가명정보의 처리 중단·회수·삭제(파기)
6. 가명정보 및 추가정보에 대한 물리적 안전 조치

제46조의7(가명정보의 적용범위) 제46조의2 또는 제46조의3에 따라 처리된 가명정보는 제22조, 제22조의2, 제62조 제2항, 제63조 제2항, 제75조부터 78조까지의 규정을 적용하지 아니한다.

제5장 개인정보의 안전한 관리

제1절 총설

제47조(개인정보의 안전성 확보조치) 업무부서는 보유하고 있는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 접속기록 보관 등 보호위원회 고시 「개인정보의 안전성 확보조치 기준」에서 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적·물리적 조치를 하여야 한다.

제47조의2(공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등) ① 개인정보의 처리 규모, 접근권한을 부여받은 개인정보취급자의 수 등 보호위원회가 고시하는 기준에 해당하는 개인정보처리시스템(이하 이 조에서 “공공시스템”이라 한다)을 운영하는 공공기관(이하 이 조에서 “공공시스템 운영기관”이라 한다)은 제47조의 안전성 확보 조치 외에 다음 각 호의 조치를 추가로 해야 한다.

1. 제6조에 따른 내부 관리계획에 공공시스템별로 작성한 안전성 확보 조치를 포함할 것
 2. 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 이 조에서 “공공시스템이용기관”이라 한다)이 정당한 권한을 가진 개인정보취급자에게 접근 권한을 부여·변경·말소 등을 할 수 있도록 하는 등 접근 권한의 안전한 관리를 위해 필요한 조치
 3. 개인정보에 대한 불법적인 접근 및 침해사고 방지를 위한 공공시스템 접속기록의 저장·분석·점검·관리 등의 조치
- ② 공공시스템운영기관 및 공공시스템이용기관은 정당한 권한 없이 또는 허용된 권한을 초과하여 개인정보에 접근한 사실이 확인되는 경우에는 지체 없이 정보주체에게 해당 사실과 피해 예방 등을 위해 필요한 사항을 통지해야 한다. 이 경우 다음 각 호의 어느 하나에 해당하는 경우에는 통지를 한 것으로 본다.
1. 제62조제2항에 따라 정보주체에게 개인정보의 분실·도난·유출에 대하여 통지한 경우
 2. 다른 법령에 따라 정보주체에게 개인정보에 접근한 사실과 피해 예방 등을 위해 필요한 사항을 통지한 경우
- ③ 공공시스템운영기관(공공시스템을 개발하여 배포하는 공공기관이 따로 있는 경우에는 그 공공기관을 포함한다. 이하 이 조에서 같다)은 해당 공공시스템의 규모와 특성, 해당 공공시스템이용기관의 수 등을 고려하여 개인정보의 안전한 관리에 관련된 업무를 전담하는 부서를 지정하여 운영하거나 전담인력을 배치해야 한다.
- ④ 공공시스템운영기관은 공공시스템별로 해당 공공시스템을 총괄하여 관리하는 부서의 장을 관리책임자로 지정해야 한다. 다만, 해당 공공시스템을 총괄하여 관리하는 부서가 없을 때에는 업무관련성 및 수행능력 등을 고려하여 해당 공공시스템운영기관의 관련 부서의 장 중에서 관리책임자를 지정해야 한다.
- ⑤ 공공시스템운영기관은 공공시스템의 안전성 확보 조치 이행상황 점검 및 개선에 관한 사항을 협의하기 위하여 다음 각 호의 기관으로 구성되는 공공시스템운영협의회를 공공시스템별로 설치·운영해야 한다. 다만, 하나의 공공기관이 2개 이상의 공공시스템을 운영하는 경우에는 공공시스템운영협의회를 통합하여 설치·운영할 수 있다.
1. 공공시스템운영기관
 2. 공공시스템의 운영을 위탁하는 경우 해당 수탁자
 3. 공공시스템운영기관이 필요하다고 인정하는 공공시스템이용기관
- ⑥ 보호위원회는 공공시스템운영기관이 개인정보의 안전성 확보 조치를 이행하는데 필요한 지원을 할 수 있다.
- ⑦ 제1항부터 제6항까지에서 규정한 사항 외에 공공시스템운영기관 등의 개인정보의 안전성 확보 조치에 필요한 사항은 보호위원회가 정하여 고시한다.

제2절 개인정보의 안전성 확보를 위한 관리적 조치

제1관 개인정보처리방침의 수립, 변경 및 공개

제48조(개인정보처리방침의 수립 및 공개) ① 개인정보 보호책임자는 ○○○대학교의 개인정보 처리방침을 수립하고 ○○○대학교에서 운영하는 인터넷 홈페이지를 통해 인터넷 홈페이지 첫 화면 또는 첫 화면과의 연결화면에 지속적으로 게재하여야 한다.

② 개인정보보호 분야별 책임자는 업무부서의 개인정보처리방침을 수립하고 업무부서의 인터넷 홈페이지를 통해 인터넷 홈페이지 첫 화면 또는 첫 화면과의 연결화면에 지속적으로 게재하여야 한다.

③ 업무부서가 인터넷 홈페이지를 운영하지 않는 등 개인정보보호 분야별 책임자가 제2항에 따라 수립한 개인정보처리방침을 인터넷 홈페이지에 게재할 수 없는 사정이 있는 경우에는 제 11조 제3항의 규정을 준용한다.

④ 제1항 내지 제3항에 따라 개인정보처리방침을 게재하는 경우에는“개인정보처리방침”이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

제49조(개인정보 처리방침의 작성기준) ① 제48조에 따라 개인정보 처리방침을 작성하는 경우에는 [붙임 2]의 ‘○○○대학교 개인정보 처리방침 표준가이드’를 참조하여 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.

② 제48조에 따라 개인정보 처리방침을 작성하는 경우에는 개인정보 처리방침에서 명시하는 개인정보 항목이 개인정보의 처리목적에 필요한 최소한의 개인정보라는 점을 밝혀야 한다.

③ 개인정보 처리방침에 반드시 포함되어야 할 사항은 다음 각 호와 같다.

1. 개인정보의 처리 목적

2. 개인정보의 처리 및 보유 기간

3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)

3의2. 개인정보의 파기절차 및 파기방법(제23조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다.)

3의3. 제32조의7항에 따른 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당하는 경우에만 정한다)

4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)

4의2. 제46조의2 및 제46조의3에 따른 가명정보의 처리 등에 관한 사항(해당되는 경우에만 정한다)

5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항

6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)

7. 처리하는 개인정보의 항목

8. 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처

9. 개인정보의 안전성 확보조치에 관한 사항

10. 개인정보 처리방침의 변경에 관한 사항

11. 추가적인 이용·제공 관련 영 제14조의2 제1항 각 호의 고려사항에 대한 판단기준(해당되는

경우에만 정한다)

12.가명정보를 처리하는 경우 가명정보 처리에 관한 사항(해당되는 경우에만 정한다)

- 가명정보의 처리 목적, 가명정보의 처리 및 보유기간, 가명정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다), 가명정보 처리의 위탁에 관한 사항(해당되는 경우에만 정한다), 처리하는 가명정보의 항목, 법 제28조의4에 따른 가명정보의 안전성 확보조치에 관한 사항

13. 개인정보의 열람청구를 접수·처리하는 부서

14. 정보주체의 권익침해에 대한 구제방법

15. 국내대리인을 지정한 경우 국내대리인의 성명(법인의 경우 그 명칭 및 대표자의 성명), 주소(법인의 경우 영업소 소재지), 전화번호 및 전자우편 주소(해당되는 경우에만 정한다)

16. 영상정보처리기기 운영·관리에 관한 사항(법 제25조7항에 따른 ‘영상정보처리기기 운영·관리방침’을 개인정보 처리방침에 포함하여 정하는 경우)

17. 그 밖에 개인정보처리자가 개인정보 처리 기준 및 보호조치 등에 관하여 자율적으로 개인정보 처리방침에 포함하여 정한 사항

제50조(개인정보 처리방침의 변경 및 공개) ① 개인정보 보호책임자 또는 개인정보보호 분야별 책임자가 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 인터넷 홈페이지 등에 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

② 업무부서가 인터넷 홈페이지를 운영하지 않는 등 개인정보보호 분야별 책임자가 제1항의 내용을 인터넷 홈페이지에 공개할 수 없는 사정이 있는 경우에는 제11조제3항의 규정을 준용한다.

제2관 개인정보파일의 등록 및 관리

제51조(개인정보파일의 등록) 업무부서는 개인정보파일(제52조에 따른 개인정보파일은 제외한다. 이하 이 조에서 같다)을 보유한 날부터 60일 이내에 별지 제1호서식의 개인정보파일(등록·변경)신청서 및 파일을 개인정보보호위원회 개인정보보호 종합지원시스템(<http://intra.privacy.go.kr>)에 등록하여야 한다. 등록된 항목 중 하나라도 변경된 경우에도 60일 이내 재등록하여야 하며 단, 생성·변경이 상시적으로 이루어지는 경우에는 1년 1회 변경 등록이 가능하다.

제52조(개인정보파일의 등록의 예외) 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 제51조를 적용하지 아니한다. 다만 등록 예외사항에 해당되는 개인정보파일은 개인정보보호 분야별 책임자의 관리·감독 하에 안전하게 관리하여야 한다.

1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일
3. 「조세범처벌법」이나 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
4. 「공공기록물관리에 관한 법률」 제33조(비밀 기록물의 관리), 「보안업무규정」 제4조(비밀의 구분) 등 다른 법령에서 비밀로 분류된 개인정보파일

5. 회의 참석 수당 지급, 자료·물품의 송부, 금전의 정산 등 단순 업무 수행을 위해 운영되는 개인정보파일로서 지속적 관리 필요성이 낮은 개인정보파일
6. 제86조1항2호에 따라 적용이 제외되는 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일
7. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
8. CCTV 등 영상정보처리기를 통하여 처리되는 개인영상정보파일
9. 그 밖에 일회적 업무 처리만을 위해 수집된 개인정보파일로서 저장되거나 기록되지 않는 개인정보파일
10. [삭제, 2024. 2.]

제53조(개인정보파일의 등록 및 공개 절차) ① 개인정보취급자가 개인정보파일의 현황을 등록할 경우에는 개인정보보호 분야별 책임자의 승인을 받아야 한다.

② 개인정보보호 분야별 책임자는 개인정보취급자가 등록할 사항을 검토하여 그 적정성을 판단한 후 승인 여부를 결정하여야 한다.

③ 개인정보보호 분야별 책임자가 개인정보파일의 현황의 등록을 승인한 경우에는 개인정보 보호책임자에게 그 사실을 보고하고 개인정보 보호책임자의 승인을 받아야 한다.

④ 개인정보 보호책임자는 개인정보보호 분야별 책임자가 승인한 사항을 검토하여 그 적정성을 판단한 후 승인 여부를 결정하여야 한다.

제54조(개인정보파일대장 작성) ① 업무부서는 1개의 개인정보파일에 1개의 개인정보파일대장을 작성하여야 한다.

② 업무부서는 법 제18조제2항 각 호에 따라 제3자가 개인정보파일의 이용·제공을 요청한 경우에는 이용·제공 가능 여부를 확인하고 별지 제2호서식의 개인정보 목적 외 이용 및 제3자 제공 대장에 기록하여 관리하여야 한다.

제55조(개인정보파일의 목적 외 이용·목적 외 제3자 제공 관리) 업무부서는 제19조 제2항 각 호에 따라 제3자가 개인정보파일의 목적 외 이용·목적 외 제3자 제공을 요청한 경우에는 각각의 이용·제공 가능 여부를 확인하고 별지 제2호 서식의 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하여 관리해야 한다.

제56조(개인정보파일 보유기간의 산정) ① 보유기간은 전체 개인정보가 아닌 개별 개인정보의 수집부터 삭제까지의 생애주기로서 보유목적에 부합된 최소기간으로 산정하되, 개별 법령의 규정에 명시된 자료의 보존기간에 따라 산정해야 한다.

② 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보보호 분야별 책임자가 개인정보 보호책임자와의 협의를 거쳐 그 보유기간을 산정해야 한다. 단, 보유기간은 [별표 1]의 '개인정보파일 보유기간 책정 기준표'에서 제시한 기준과 「공공기록물 관리에 관한 법률 시행령」 제25조에 따른 기록관리기준표를 상회할 수 없다.

제57조(개인정보파일의 파기) ① 업무부서는 개인정보파일의 보유기간 경과, 처리목적 달성 등 개인정보파일이 불필요하게 되었을 때에는 5일 이내에 그 개인정보파일을 파기하여야 한다. 단, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 제1항 본문에 따라 개인정보파일을 파기하는 경우에는 제23조제2항 및 제3항을 준용한다.

③ 제1항 단서에 따라 개인정보파일을 파기하지 아니하고 보존하는 경우에는 제23조제4항을 준용한다.

④ 개인정보취급자는 개인정보파일을 파기하는 경우 보유기간 경과, 처리목적 달성 등 파기 사유가 발생한 개인정보파일을 선정하고, 별지 제3호서식의 개인정보파일 파기요청서에 파기 대상 개인정보파일의 명칭, 파기방법 등을 기재하여 개인정보보호 분야별 책임자의 승인을 받아야 한다.

⑤ 개인정보보호 분야별 책임자는 개인정보파일의 파기 시행 후 파기 결과를 확인하고 별지 제4호서식의 개인정보파일 파기 관리대장을 작성하여야 한다.

⑥ 개인정보파일 파기 절차는 다음 각 호에 따라 실시한다.

1. 개인정보보호 분야별 책임자는 개인정보파일 파기 요청서를 작성하여 개인정보 보호책임자에게 제출
2. 개인정보 보호책임자는 파기 요청서를 검토 후 승인여부를 결정하여 분야별 책임자에게 통보
3. 승인을 받지 못한 경우 명시한 보완조치를 취한 후 다시 파기 요청을 하며, 승인을 받은 경우 분야별 책임자는 개인정보파일을 즉시 파기하고 그 결과를 개인정보 보호책임자에게 보고
4. 최종 결과를 받은 개인정보 보호책임자는 공개된 개인정보파일 등록을 삭제하고 교육부 개인정보 보호책임자에게 개인정보파일 파기결과를 보고

제58조(개인정보파일 등록사실의 삭제) ① 업무부서가 제57조에 따라 개인정보파일을 파기한 경우에는 제51조에 따른 개인정보파일의 등록사실을 삭제하여야 한다.

② 업무부서가 개인정보파일의 등록사실을 삭제하는 경우에는 제53조를 준용한다.

제59조(개인정보파일 보유·파기현황의 공개 및 방법) ① 개인정보보호 분야별 책임자는 개인정보파일의 보유·파기현황을 주기적으로 조사하여 그 결과를 업무부서 또는 대표 홈페이지의 개인정보 처리방침에 포함하여 관리해야 한다.

제3관 개인정보 영향평가의 실시

제60조(개인정보 영향평가) ① 개인정보 보호책임자는 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 “영향평가”라 한다)를 실시하고 그 결과를 교육부 장관 및 보호위원회에게 제출하여야 한다. 이 경우 개인정보 보호책임자는 영향평가를 보호위원회가 지정하는 기관(이하 “평가기관”이라 한다) 중에서 의뢰하여야 하며 세부내용은 개인정보 영향평가에 관한 고시를 참조한다.

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 ○○○대학교 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일

3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
 4. 영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일(이 경우 영향평가 대상은 변경된 부분으로 한정한다.)
- ② 개인정보보호 분야별 책임자는 운용하는 개인정보파일이 제1항의 경우에 해당하는 때에는 해당 개인정보파일에 대한 영향평가를 실시하고 그 결과를 개인정보 보호책임자에게 제출하여야 한다.
- ③ 업무부서는 영향평가를 실시한 개인정보파일을 제52조에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.

제4관 개인정보 유출등 사고 대응 계획 수립 및 시행

제61조(개인정보의 유출등) ① 개인정보의 분실·도난·유출(이하 "유출등"이라 한다)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말한다.

제61조의2(개인정보의 유출등 사고 대응 계획) ① 개인정보 보호책임자는 ○○○대학교에 대한 개인정보 유출등 사고 대응 계획 수립하고 시행하여야 한다.

② 개인정보 보호책임자는 아래의 내용이 포함될 수 있도록 개인정보 유출등 사고 대응 계획을 수립하여야 하며, 피해복구 조치 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

1. 유출등 통지·조회 절차
2. 고객 민원 대응 조치
3. 현장 혼잡 최소화조치, 고객 불안 해소 조치
4. 대응조치 및 피해자 구제조치(정보주체에게 유출사실 통지, 유출 신고 등)

제62조(개인정보 유출등 통지시기 및 항목) ① 개인정보취급자는 개인정보가 유출등이 되었음을 확인한 때에는 지체 없이 개인정보보호 분야별 책임자에게 이를 보고하여야 한다.

② 개인정보보호 분야별 책임자는 제1항의 보고를 받은 경우 지체 없이 개인정보 보호책임자에게 이를 보고하고, 유출등이 되었음을 알게 된 때에는 72시간 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다.

1. 유출등이 된 개인정보의 항목
 2. 유출등이 된 시점과 그 경위
 3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
 4. 업무부서의 대응조치 및 피해구제절차
 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- ③ 개인정보보호 분야별 책임자는 제2항 각 호의 구체적인 내용을 확인하지 못한 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출등이 발생한 사실
2. 제1항의 통지항목 중 확인된 사항

- ④ 업무부서는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.
- ⑤ 개인정보 보호책임자는 제2항에 따른 보고를 받는 즉시 ○○○대학교 침해·유출사고 대응절차에 따라 조치를 취하여야 한다.
- ⑥ 개인정보보호 분야별 책임자는 개인정보 유출등의 사고를 인지하지 못해 유출등의 사고가 발생한 시점으로부터 72시간 이내에 해당 정보주체에게 개인정보 유출등의 통지를 하지 아니한 경우에는 실제 유출등의 사고를 알게 된 시점을 입증하여야 한다.

제63조(개인정보 유출등의 통지방법) ① 개인정보보호 분야별 책임자는 정보주체에게 제62조제2항 각 호의 사항을 통지할 때에는 서면등의 방법을 통하여 정보주체에게 알려야 한다.

② 개인정보보호 분야별 책임자는 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 제62조제2항 각 호 외의 부분 단서에 따라 같은 항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 아니하는 경우에는 사업장등의 보기 쉬운 장소에 제62조제2항 각 호의 사항을 30일 이상 게시하여야 한다.

제64조(개인정보 유출등의 신고 및 절차) ① 개인정보 보호책임자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 제26조제1항 각 호의 사항을 서면등의 방법으로 **교육부 신고와 동시에** 보호위원회 또는 한국인터넷진흥원에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.

1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
2. 1명 이상의 민감정보, 고유식별정보가 유출등이 된 경우
3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 1명 이상의 개인정보가 유출등이 된 경우

② 제1항에 따른 신고는 별지 제7호서식에 따른 개인정보 유출등 신고서를 통하여 하여야 한다.

③ 정보주체에 관한 개인정보가 1명이라도 유출된 경우에는 교육부로 개인정보 유출신고서를 통하여 보고하여야 하며, 제62조제5항에 따른 조치를 취해야 한다.

④ 제64조 1항에 따라 신고하는 경우 개인정보 포털(privacy.go.kr)과 교육부 개인정보보호 포털(privacy.moe.go.kr)을 통하여 유출등 신고를 하여야 한다.

⑤ 제64조3항에 따라 신고하는 경우 교육부 개인정보보호 포털(privacy.moe.go.kr)을 통하여 유출등 신고를 하여야 한다.

⑥ 개인정보 보호책임자는 제1항 및 제3항에 따른 신고를 하려는 경우로서 제62조제2항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때 까지 확인된 내용 및 같은 항 제3호부터 5호까지의 사항을 서면등의 방법으로 우선 신고해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다.

제3절 개인정보의 안전성 확보를 위한 기술적·물리적 조치

제65조(접근권한의 관리) ① 업무부서는 개인정보취급자에게 개인정보처리시스템에 대한 접근권한을 개인정보취급자에게만 업무수행에 필요한 최소한의 범위로 차등 부여하고, 사용자별 개인정보 접근권한을 관리하기 위한 조치를 취해야 한다.

② 업무부서는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 해당 개인정보취급자의 개인정보처리시스템에 대한 접근권한을 변경 또는 말소하여야 한다.

③ 업무부서는 별지 제13호서식의 개인정보처리시스템 접근권한 관리대장에 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 업무부서는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 업무부서는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 하며 비밀번호를 설정하여 이행할 경우 다음 각 호의 사항을 포함하여 비밀번호작성규칙을 수립하여 적용하여야 한다.

1. 영문, 숫자, 특수문자 등을 조합하여 구성
2. 연속적인 숫자나 생일, 전화번호 등을 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고
3. 비밀번호 변경은 반기 1회 이상 정기적으로 변경하고 제3자에게 노출되었을 경우 즉시 새로운 비밀번호로 변경

⑥ 업무부서는 정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수(5번) 이상 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

⑦ 개인정보취급자의 정보시스템 이용권한을 추가, 변경할 경우 해당 부서장은 별지 제14호서식의 정보시스템 접근권한 신청서와 별지 제15호서식의 개인정보보호 보안서약서를 작성하여 정보시스템 운영부서의 장 또는 접근권한 책임부서의 장에게 신청한다.

⑧ 정보시스템 운영부서의 장 또는 접근권한 책임부서의 장은 접근권한 부여 시 정보시스템 이용 또는 활용목적의 정당성, 이용범위의 적정성, 신청내용의 타당성 등을 심사하여 최소한의 접근권한을 부여한다.

⑨ 정보시스템 운영부서의 장은 분기별로 인사발령·업무분장 변경에 따른 사용자 권한삭제 및 사용중지 조치여부, 시스템별 접근권한 오·남용 여부 등을 점검하고, 접근권한 변경 등 필요한 조치를 하여야 한다.

⑩ 정보시스템관련 유지보수 업체나 외주용역 업체 직원이 운영상 불가피한 사유로 시스템 접근이 필요한 때에는 아래사항의 보안대책을 마련한 다음 접근을 승인하며 정기적으로 관리·감독하여야 한다.

1. 보안서약서의 징구
2. 접근 허용기간 설정 또는 연장
3. 접근 허용기간이 종료되었거나 사용목적을 달성한 경우 접근차단
4. 최소범위의 접근권한 설정
5. 비인가자의 불법적인 접근 및 서비스 중단 등을 예방하기 위해 업무적으로 불필요하거나, 침해의 위협이 있는 네트워크 서비스를 사용금지

6. 그 밖의 정보시스템 또는 개인정보보호를 위해 필요하다고 판단되는 사항

제65조의2(공공시스템운영기관의 접근권한의 관리) ① 공공시스템운영기관은 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소하려는 때에는 인사정보와 연계하여야 한다.

② 공공시스템운영기관은 인사정보에 등록되지 않은 자에게 제65조제4항에 따른 계정을 발급해서는 안된다. 다만, 긴급상황 등 불가피한 사유가 있는 경우에는 그러하지 아니하며, 그 사유를 제65조제3항에 따른 내역에 포함하여야 한다.

③ 공공시스템운영기관은 제65조제4항에 따른 계정을 발급할 때에는 개인정보 보호 교육을 실시하고, 보안 서약을 받아야 한다.

④ 공공시스템운영기관은 정당한 권한을 가진 개인정보취급자에게만 접근 권한이 부여·관리되고 있는지 확인하기 위하여 제65조제3항에 따른 접근 권한 부여, 변경 또는 말소 내역 등을 반기별 1회 이상 점검하여야 한다.

⑤ 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 “공공시스템이용기관”이라 한다)은 소관 개인정보취급자의 계정 발급 등 접근 권한의 부여·관리를 직접하는 경우 제2항부터 제4항까지의 조치를 하여야 한다.

제66조(접근통제) ① 업무부서는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지 및 대응

② 업무부서는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.

③ 업무부서는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 다음 각 호의 조치를 취하여야 한다.

1. 인터넷 홈페이지의 취약점으로 인한 노출 방지
2. 개인정보취급자의 부주의로 인한 개인정보 및 개인정보파일 인터넷 홈페이지 게시 방지
3. P2P 프로그램·공유 폴더 사용 원칙적 금지, 부득이한 경우 전체 또는 불필요한 폴더 공유 금지, 공유폴더에 개인정보 파일의 포함 여부 정기적 점검

④ 업무부서는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.

⑤ 업무부서는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

⑥ 업무부서는 홈페이지를 통한 개인정보 노출방지를 위해 다음 각 호의 내용에 따라 조치하여야 한다.

1. 홈페이지 게시내용에 대해 책임부서 지정, 부서장 결재 후 내용을 게시
2. 게시판 등 글쓰기 화면에 개인정보 노출 경고메시지를 안내
3. 개인정보 노출 가능성이 있는 페이지에 대하여 검색 로봇 배제 기능을 설정

4. 홈페이지 개인정보 노출 차단을 위한 주기적 모니터링 등

제67조(개인정보의 암호화) ① **인증정보 관련** 암호화하여야 하는 개인정보는 **비밀번호** 및 생체인식 정보 등을 말한다.

② 업무부서는 제1항에 따른 개인정보를 정보통신망을 통하여 인터넷망 구간을 송·수신하는 경우에는 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 업무부서는 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.

1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우

2. 내부망에 고유식별정보를 저장하는 경우 다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용 여부 및 적용범위를 정하여 시행할 수 있다.

가. 제60조에 따른 개인정보 영향평가의 대상이 되는 서비스의 경우에는 해당 개인정보 영향평가의 결과

나. 암호화 미적용시 위험도 분석에 따른 결과

④ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 업무부서는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립 시행하고, 별지 제16호서식의 개인정보처리시스템 암호키 관리대장과 별지 제17호서식의 개인정보처리시스템 암호키 백업대장에 기록·관리하여야 한다.

⑤ 업무부서는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

⑥ 업무부서는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 이 항은 2024년 9월 15일부터 시행한다.

제68조(접속기록의 보관 및 점검) ① 업무부서는 개인정보취급자의 개인정보처리시스템에 대한 접속 기록을 최소 1년 이상 보관·관리하여야 하며, 개인정보보호 분야별 책임자는 이를 정기적으로 확인·감독 하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

② 업무부서는 개인정보의 오·남용, 분실·도난·유출·위조·변조·훼손 등에 대응하기 위하여 따라 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하고 별지 제5호서식의 개인정보처리시스템 접속기록 점검대장에 기록·관리하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 개인정보처리시스템별로 기준을 정하여 다음 각 호에 따라 그 사유를 반드시 확인하여야 한다.

1. (다운로드 정보주체의 수) 개인정보처리시스템의 일평균 개인정보 처리 건 수 대비하여 개인정보취급자가 다수의 정보주체에 대한 개인정보를 다운로드 한 경우 사유 확인
2. (일정기간 내 다운로드 횟수) 개인정보취급자가 단시간에 수차례에 걸쳐 개인정보를 다운로드 한 행위에 대한 사유 확인
3. (업무시간 외 다운로드 수행) 새벽시간, 휴무일 등 업무시간 외 개인정보를 다운로드 한 경우 사유 확인

③ 업무부서는 제1항의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 다음 각 호에 따라 안전하게 보관하여야 한다. 세부 사항은 개인정보의 안전성 확보조치 기준을 참조한다.

1. 정기적인 접속기록(식별자, 접속일시, 접속지 IP 정보, 처리한 정보주체 정보, 수행 업무 등) 백업
2. 별도의 보조저장 매체나 별도의 저장장치에 보관
3. 접속기록에 대한 위·변조를 방지하기 위해 CD-ROM 등과 같은 덮어쓰기 방지 매체를 사용
4. 접속기록을 수정 가능한 매체(HDD 또는 테이프 등)에 백업하는 경우 위·변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관·관리할 수 있음
5. 종이 등의 물리적 매체를 이용한 개인정보자료는 시건장치로 안전하게 보관하고 유실방지를 위하여 대장 작성 및 주기적 점검 등의 관리를 실시

제68조의2(공공시스템운영기관의 접속기록의 보관 및 점검) ① 공공시스템 접속기록 등을 자동화된 방식으로 분석하여 불법적인 개인정보 유출 및 오용·남용 시도를 탐지하고 그 사유를 소명하도록 하는 등 필요한 조치를 하여야 한다.

② 공공시스템운영기관은 공공시스템이용기관이 소관 개인정보취급자의 접속기록을 직접 점검할 수 있는 기능을 제공하여야 한다.

제69조(악성프로그램 등 방지) ① 업무부서는 악성 프로그램 등을 방지·치료할 수 있는 보안프로그램을 의무적으로 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안프로그램을 항상 최신 버전으로 업데이트하기 위해 자동 업데이트 기능 설정하거나, **정당한 사유가 없는 한 일 1회 이상 업데이트** 실시하여 최신의 상태로 유지
2. 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

② 업무부서는 개인정보보호를 위해 구성원을 대상으로 보안프로그램 설치 등의 보안정책을 적용할 필요가 있는 경우에는 보안심사위원회 등의 심의를 거치고 그 결정사항을 일괄 적용할 수 있다. 단, 보안정책을 수행함에 있어 수집되는 개인정보(IP, 맥주소, PC이름, 보안패치이력 등)는 법 제15조(개인정보의 수집·이용)에 의하여 합리적인 범위 내에서 수집 이용할 수 있으며, 훼손, 멸실, 변경, 위조 또는 유출하여서는 아니 된다.

제70조(물리적 접근 방지) ① 업무부서는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 업무부서는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제71조(위험 분석 및 대응 방안) ① 업무부서는 기관이 보유한 개인정보파일을 대상으로 내부망 또는 인터넷망 구간 및 인터넷망 구간과 내부망의 중간지점(DMZ)에 고유식별번호를 저장하는 경우 암호화의 적용 여부 및 적용 범위를 정하는 위험 분석을 실시하고 대응 방안을 마련하여야 한다.

② 제1항의 위험 분석을 수행하는 경우에는 『개인정보보호위원회, 개인정보 위험도 분석 기준 및 해설서』를 참고하여 실시한다.

③ 고유식별정보를 모두 안전한 암호화 알고리즘으로 암호화하는 경우 위험 분석을 생략할 수 있다.

제72조(재해 및 재난 안전조치) ① 업무부서는 정보시스템 운영부서와의 협조를 통해 화재, 홍수, 단전 등의 재해 재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

② 업무부서는 정보시스템 운영부서와의 협조를 통해 재해 재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

제73조(출력·복사시 안전조치) ① 업무부서는 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면 표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.

② 업무부서는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다. 다만, 이 항은 2024년 9월 15일부터 시행한다.

제74조(개인정보보호담당부서의 지원) ○○○대학교 개인정보 보호책임자가 소속된 부서를 개인정보보호담당부서로 하며, 각 부서에 대하여 이 절에서 규정하는 개인정보의 안전성 확보를 위한 기술적·물리적 조치에 관한 업무를 지원한다.

제6장 정보주체의 권리보장

제75조(개인정보의 열람) ① 정보주체는 별지 제8호서식의 개인정보 열람 요구서등 개인정보처리자가 마련한 방법을 통하여 해당 개인정보를 처리하는 소속기관에게 다음 각 호에 대한 열람을 요구할 수 있다.

1. 개인정보의 항목 및 내용
2. 개인정보의 수집·이용의 목적
3. 개인정보 보유 및 이용 기간
4. 개인정보의 제3자 제공 현황
5. 개인정보 처리에 동의한 사실 및 내용

② 제1항의 요구를 받은 업무부서는 개인정보 열람요구를 받은 날부터 10일 이내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 이 경우 해당 기간 내에 열람하게 할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 그 날로부터 10일 이내에 열람하게 하여야 한다.

③ 업무부서는 제3자 제공현황에 대한 열람청구를 받은 경우 해당 열람청구가 국가안보의 중요한 사안으로 다른 법률에 따라 진행중인 감사 및 조사에 관한 업무를 수행하는 데 중대한 지장을 초래하는 경우에는 제3자에게 열람청구에 관련한 의견을 조회하여 결정할 수 있다.

제76조(열람의 제한·거절) ① 제75조 제1항의 요구를 받은 업무부서는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있으며, 열람이 제한되는 사항을 제외한 부분은 열람할 수 있도록 하여야 한다.

1. 법률에 따라 열람이 금지되거나 제한되는 경우
2. 타인의 생명·신체를 해할 우려가 있거나 타인의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 다음 각 목의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우
 - 가. 조세의 부과·징수 또는 환급에 관한 업무
 - 나. 「초·중등교육법」 및 「고등교육법」에 따른 각급학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무
 - 다. 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무
 - 라. 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
 - 마. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무

② 제75조 제2항에 따라 열람을 연기하거나 제1항에 따라 열람을 제한·거절하려는 업무부서는 열람요구를 받은 날부터 10일 이내에 별지 제10호서식의 열람의 연기·일부열람·거절통지서 등 업무부서가 마련한 방법을 통하여 연기 또는 제한이나 거절의 사유 및 이의제기방법을 해당 정보주체에게 알려야 한다.

제77조(개인정보의 정정·삭제) ① 정보주체는 자신의 개인정보를 처리하는 소속기관에게 별지 제8호 서식의 개인정보 정정·삭제 요구서 등 개인정보처리자가 마련한 방법을 통해 그 개인정보에 대한 정정 또는 삭제를 요구할 수 있다. 단, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다. [개정, 2018. 3.]

② 제1항의 요구를 받은 업무부서는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 다음 각 호 중 하나의 조치를 한 후 그 사실을 별지 제11호서식의 개인정보 정정·삭제 요구에 대한 결과통지서 등을 통하여 해당 정보주체에게 알려야 한다. [개정, 2018. 3.]

1. 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 사실
2. 정보주체의 정정·삭제 요구가 제1항 단서에 해당하는 경우에는 삭제 할 수 없다는 사실과 삭제를 요구할 수 없는 근거법령의 내용 및 이의제기방법

③ 개인정보취급자가 제2항의 조치를 취하기 위하여 그 개인정보를 조사할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.

④ 개인정보취급자가 제2항에 따라 개인정보를 삭제할 때에는 그 개인정보가 복구 또는 재생되지 아니하도록 조치하여야 한다.

제78조(개인정보의 처리정지) ① 정보주체는 자신의 개인정보를 처리하는 업무부서에 별지 제8호 서식의 개인정보 처리정지 요구서 등 개인정보처리자가 마련한 방법을 통하여 그 개인정보 처리의 정지를 **요구하거나 개인정보 처리에 대한 동의를 철회할 수 있다.**

② **제1항에 따른 처리정지** 요구를 받은 업무부서는 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 단, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

1. ~4. (생략)

③ 업무부서는 정보주체가 제1항에 따라 동의를 철회한 때에는 지체 없이 수집된 개인정보를 복구·재생할 수 없도록 파기하는 등 필요한 조치를 하여야 한다. 다만, 제2항 각 호의 어느 하나에 해당하는 경우에는 동의 철회에 따른 조치를 하지 아니할 수 있다.

④ 제1항의 요구를 받은 업무부서는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 다음 각 호 중 하나의 조치를 한 후 그 사실을 별지 제11호서식의 개인정보 처리정지 요구에 대한 결과통지서 등으로 해당 정보주체에게 알려야 한다.

1. 처리정지 조치를 한 사실

2. 정보주체의 처리정지 요구가 제2항 단서에 해당하는 경우에는 처리정지 할 수 없다는 사실 및 이유와 이의제기 방법

⑤ 업무부서는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.[개정, 2024. 2.]

제78조의2(자동화된 결정에 대한 정보주체의 권리 등) ① 정보주체는 완전히 자동화된 시스템(인공지능 기술을 적용한 시스템을 포함한다)으로 개인정보를 처리하여 이루어지는 결정(「행정기본법」 제20조에 따른 행정청의 자동적 처분은 제외하며, 이하 이 조에서 “자동화된 결정”이라 한다)이 자신의 권리 또는 의무에 중대한 영향을 미치는 경우에는 해당 개인정보처리자에 대하여 해당 결정을 거부할 수 있는 권리를 가진다. 다만, 자동화된 결정이 제14조제2항제1호·제2호 및 제4호에 따라 이루어지는 경우에는 그러하지 아니하다.

② 정보주체는 개인정보처리자가 자동화된 결정을 한 경우에는 그 결정에 대하여 설명 등을 요구할 수 있다.

③ 개인정보처리자는 제1항 또는 제2항에 따라 정보주체가 자동화된 결정을 거부하거나 이에 대한 설명 등을 요구한 경우에는 정당한 사유가 없는 한 자동화된 결정을 적용하지 아니하거나 인적 개입에 의한 재처리·설명 등 필요한 조치를 하여야 한다.

④ 개인정보처리자는 자동화된 결정의 기준과 절차, 개인정보가 처리되는 방식 등을 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

⑤ 제1항부터 제4항까지에서 규정한 사항 외에 자동화된 결정의 거부·설명 등을 요구하는 절차 및 방법, 거부·설명 등의 요구에 따른 필요한 조치, 자동화된 결정의 기준·절차 및 개인정보가 처리되는 방식의 공개 등에 필요한 사항은 대통령령으로 정한다.

제79조(이의신청 등) ① 정보주체는 개인정보 열람·정정·삭제·처리정지 요구(이하 “열람등 요구”라 한다)에 대한 해당 업무부서의 결과 통지에 대하여 불복이 있는 때에는 해당 업무부서로부터 통지를 받은 날부터 30일 이내에 개인정보 보호책임자에게 서면 등 개인정보처리자가 마련한 방법으로 이의신청을 할 수 있다.

② 개인정보 보호책임자는 제1항의 이의신청을 받은 즉시 그 사실을 해당 업무부서에게 통지하여야 하며, 해당 업무부서의 개인정보보호 분야별 책임자는 3일 이내에 개인정보 보호책임자에게 이에 대한 의견을 제출하여야 한다.

③ 개인정보 보호책임자는 제1항의 이의신청을 받은 날로부터 10일 이내에 해당 정보주체와 해당 업무부서에게 이의신청 처리의 결과를 서면으로 통지하여야 한다. 이 경우 개인정보 보호

책임자는 사안의 성질상 필요하다고 판단되면 이를 ○○○대학교 보호위원회에 회부하여 심의하게 할 수 있다.

④ 해당 업무부서는 제3항의 통지를 받은 경우 지체 없이 그 내용에 따른 처리를 하여야 한다.

⑤ 정보주체는 「개인정보 보호법」 위반행위로 인한 손해배상 청구가 가능하며 개인정보보호 분야별 책임자는 고의 또는 과실이 없음을 입증할 책임이 있으며 법 의무사항 준수 등 개인정보 보호를 성실히 수행한 경우 감경이 가능하다.

제80조(권리행사 방법 등의 공개) ① 업무부서는 정보주체가 소속기관에게 자신의 개인정보에 대한 열람 등 요구를 할 수 있다는 점과 이에 관한 업무부서의 조치에 대한 이의신청절차 및 그 방법을 공개하여야 한다. 이 경우 열람 등 요구의 방법과 절차는 해당 개인정보의 수집 방법과 절차보다 어렵지 아니하도록 하여야 한다.

② 업무부서는 정보주체가 열람 등 요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

③ 개인정보에 관한 권리 또는 이익을 침해받은 사람은 개인정보침해신고센터로 신고할 수 있도록 개인정보침해신고센터(한국인터넷진흥원, 국번없이 118)에 대한 정보를 알기 쉬운 방법으로 공개하여야 한다.

제81조(대리인의 범위 등) ① 정보주체는 자신의 개인정보에 대한 열람 등 요구를 다음 각 호의 대리인을 통하여 할 수 있다. 이 경우 대리인은 해당 소속기관에게 별지 제12호서식의 위임장을 제출하여야 한다.

1. 정보주체의 법정대리인

2. 정보주체로부터 위임을 받은 자

② 만 14세 미만 아동의 법정대리인은 해당 아동의 개인정보를 처리하는 소속기관에게 그 아동의 개인정보 열람 등 요구를 할 수 있다.

③ 개인정보보호 분야별 책임자는 개인정보 처리 요구자가 본인이거나 정당한 대리인인지를 반드시 확인하여야 한다.

④ 열람 등을 요구하는 자에게 수수료와 우송료(사본의 우송을 청구하는 경우)를 필요한 실비의 범위 내에서 청구가 가능하며 해당 수수료는 「공공기관의 정보공개에 관한 법률 시행규칙」을 준용하도록 하되, 열람 등 요구를 하게 된 사유가 ○○○대학교에 있는 경우에는 제외한다.

제7장 개인정보보호 교육

제82조(개인정보보호 교육 계획의 수립) ① 개인정보 보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 매년 수립하여야 한다.

1. 교육목적 및 대상

2. 교육내용

3. 교육 일정 및 방법

4. 그밖에 개인정보보호 교육을 위하여 필요한 사항

② 개인정보 보호책임자는 수립한 개인정보보호 교육 계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

제83조(개인정보보호 교육의 실시) ① 개인정보 보호책임자는 ○○○대학교 내 모든 개인정보 취급자에 대하여 이 내부관리계획을 포함하여 업무상 취급하는 개인정보의 안전한 관리를 위하여 필요한 사항에 대한 교육을 매년 1회 이상 정기적으로 실시하여야 한다.

② 개인정보 보호책임자 및 개인정보 보호담당자는 연 1회 이상 개인정보보호 교육에 참석하여야 하며, **개인정보 보호책임자는 신규로 지정된 개인정보 보호담당자가 15시간 이상의 개인정보보호 교육(정보보안 교육을 포함한다)을 받도록 노력하여야 한다.**

③ 업무부서는 개인정보취급자로 하여금 제1항에 따른 교육을 이수하도록 하여야 한다.

④ 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시한다.

⑤ 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보 보호책임자 및 개인정보보호 분야별 책임자는 부서 회의 등을 통해 수시 교육을 실시할 수 있다.

⑥ 개인정보보호 교육에 포함되는 내용은 아래와 같다.

1. 개인정보보호(가명정보 포함)의 중요성 설명 [개정, 2021. 3.]
2. 내부관리계획의 준수 및 이행
3. 개인정보·가명정보의 기술적·관리적 보호조치 기준 [개정, 2021. 3.]
4. 개인정보보호 유출 시 대응방안
5. 개인정보보호 라이프사이클에 따른 업무절차
6. 「개인정보 보호법」에서 규정하는 위반 항목, 준수사항 이행 관련 절차 등

제8장 정기적인 자체 검사

제84조(자체 감사 주기 및 절차) ① 개인정보 보호책임자는 개인정보보호를 위한 내부관리계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지를 정기적으로 감사 또는 점검하여야 한다.

② 개인정보 보호책임자는 개인정보 자체감사를 위한 감사대상, 감사절차 및 방법 등 감사의 실시에 관하여 필요한 별도의 계획을 수립할 수 있다.

③ 개인정보보호 자체감사는 매년 1회 이상 실시한다.

제85조(자체 감사 결과 반영) ① 개인정보 보호책임자는 개인정보보호를 위한 자체감사 실시 결과, 개인정보의 관리·운영상의 문제점을 발견하거나 관련 개인정보취급자가 본 계획의 내용을 위반할 때에는 시정·개선 등 필요한 조치를 취하여야 한다.

② 개인정보 보호책임자는 개인정보 위반사실에 대한 시정·개선 조치가 이행되지 않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 되는 경우 개인정보취급자 등에 대하여 인사위원회 심의 요구 등 필요한 추가 조치를 취할 수 있다.

제9장 보 칙

제86조(적용의 일부제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제4장부터 제6장까지를 적용하지 아니한다.

1. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보
- ② 제42조에 따라 공개된 장소에 **고정형** 영상정보처리기를 설치·운영하여 처리되는 개인정보에 대하여는 **제14조, 제17조, 제24조 제1항과 제3항, 제25조 내지 제26조, 제29조에서 규정한 고지의무 및 동의를 받는 방법, 제63조 및 제78조를 적용하지 아니한다.**
- ③ 업무부서는 제1항 각 호에 따라 개인정보를 처리하는 경우에도 그 목적을 위하여 필요한 범위에서 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치, 개인정보의 처리에 관한 고충처리, 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하여야 한다.

제86조의2(적용제외) 이 내부관리계획은 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보에는 적용하지 아니한다.

제87조(권한의 위임) ① 각 업무부서의 개인정보보호 분야별 책임자는 이 내부관리계획에 따른 권한의 일부를 담당할 분야별 담당자를 지정하여 그 업무를 위임할 수 있다.

- ② 제1항에 따라 권한을 위임받은 분야별 담당자는 위임받은 업무의 처리결과를 개인정보보호 분야별 책임자에게 보고하여야 한다.

제88조(금지행위) 개인정보취급자 혹은 개인정보취급자였던 자는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위
2. 업무상 알게 된 개인정보를 누설하거나 권한 없이 타인이 이용하도록 제공하거나 직무상 목적 외의 용도로 사용하는 행위
3. 정당한 권한 없이 또는 허용된 권한을 초과하여 타인의 **개인정보를 이용**, 훼손, 멸실, 변경, 위조 또는 유출하는 행위

제89조(비밀유지 등) 다음 각 호의 업무에 종사하거나 종사하였던 자는 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적 외의 용도로 이용하여서는 아니 된다. 단, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.

1. 제8조에 따른 ○○○대학교 보호위원회의 업무
2. 제60조에 따른 영향평가 업무
3. **제46조의3에 따른 전문기관의 지정 업무 및 전문기관의 업무**

제90조(의견제시 및 개선권고) ① ○○○대학교 정보보안 담당부서는 ○○○대학교「보안업무 규정」제4조에 따른 정보보안담당관의 기본활동을 수행함에 있어 필요하다고 인정하면 이 내부관리계획 상의 개인정보의 안전한 관리를 위한 기술적·물리적 조치와 관련하여 각 업무부서에 의견을 제시할 수 있다.

② ○○○대학교 개인정보 보호책임자는 개인정보보호를 위하여 필요하다고 인정하면 각 업무부서에 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 업무부서는 이를 이행하기 위하여 성실하게 노력하여야 한다.

제91조(처리중인 개인정보에 대한 경과조치) ① 법 시행('11년 9월 30일) 전에 근거법령 없이 개인정보를 수집한 경우 당해 개인정보를 보유하는 것은 적법한 처리로 본다. 단, 법 시행 이후 기존의 수집목적 범위 내에서 이용하는 경우를 제외하고 개인정보를 새롭게 처리하는 경우에는 법, 시행령, 고시 및 이 내부관리계획에 따라야 한다.

② 법 시행 전에 법률의 근거 또는 정보주체의 동의 없이 정보주체 이외의 자로부터 개인정보를 수집하여 목적 외의 용도로 이용하고 있는 업무부서는 정보주체의 동의를 받아야 한다.

③ 법 시행 전에 개인정보를 수집한 업무부서는 기존의 수집목적 범위에도 불구하고 제1항 단서 및 제2항을 준수하기 위하여 새롭게 정보주체의 동의를 받을 목적으로 법 시행 전에 수집한 개인정보를 이용할 수 있다.

④ 개인정보 영향평가 대상 규모의 개인정보파일을 운용하고 있는 업무부서는 법 시행일로부터 5년 이내('16년 9월 29일)에 영향평가를 실시하고 그 조치를 완료하여야 한다.

부 칙

제1조(시행일) 이 내부관리계획은 ○○○대학교 총장의 승인을 받은 날로부터 시행한다.

제2조(경과조치) 부칙 제1조에도 불구하고 이 내부관리계획 시행일 이전에 시행된 사항은 이 내부관리계획에 의하여 처리된 것으로 본다.

개인정보파일 보유기간 책정 기준표

보유기간	대상 개인정보파일
영구	<ol style="list-style-type: none"> 1. 국민의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	<ol style="list-style-type: none"> 1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일
30년	<ol style="list-style-type: none"> 1. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
10년	<ol style="list-style-type: none"> 1. 관계 법령에 따라 5년 이상 10년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
5년	<ol style="list-style-type: none"> 1. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
3년	<ol style="list-style-type: none"> 1. 행정업무의 참고 또는 사실 증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일(단 다른 법령에서 증명서 발급 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름)
1년	<ol style="list-style-type: none"> 1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일

과징금의 산정기준과 산정절차(제60조의2제6항 관련)

1. 과징금의 산정단계

과징금은 법 제64조의2제4항 각 호에 따른 고려 사항과 이에 영향을 미치는 행위를 종합적으로 고려하여 제2호가목에 따라 산정된 기준금액에 같은 호 나목에 따른 1차 조정, 같은 호 다목에 따른 2차 조정, 같은 호 라목에 따른 부과과징금 결정을 순차적으로 거쳐 산정한다. 다만, 가중하는 경우에도 법 제64조의2제1항 각 호 외의 부분에 따른 과징금 금액의 상한을 넘을 수 없다.

2. 과징금의 산정단계에 따른 산정방식과 고려 사유

가. 기준금액의 산정

- 1) 기준금액은 제60조의2제1항에 따른 전체 매출액에서 같은 조 제3항에 따른 위반행위와 관련이 없는 매출액을 제외한 매출액에 위반행위의 중대성에 따라 다음과 같이 구분된 과징금의 산정비율(이하 “부과기준율”이라 한다)을 곱하여 산출한 금액으로 한다.

위반행위의 중대성	부과기준율
매우 중대한 위반행위	2.1% 이상 2.7% 이하
중대한 위반행위	1.5% 이상 2.1% 미만
보통 위반행위	0.9% 이상 1.5% 미만
약한 위반행위	0.03% 이상 0.9% 미만

- 2) 제60조의2제2항 각 호의 어느 하나에 해당하는 경우에는 1)에도 불구하고 위반행위의 중대성에 따라 기준금액을 다음과 같이 한다.

위반행위의 중대성	기준금액
매우 중대한 위반행위	7억원 이상 18억원 이하
중대한 위반행위	2억원 이상 7억원 미만
보통 위반행위	5천만원 이상 2억원 미만
약한 위반행위	5백만원 이상 5천만원 미만

- 3) 위반행위의 중대성은 다음의 사항을 종합적으로 고려하여 판단한다.

가) 위반행위의 내용 및 정도

나) 암호화 등 안전성 확보 조치 이행 노력

다) 개인정보가 분실·도난·유출·위조·변조·훼손된 경우 위반행위와의
관련성 및 분실·도난·유출·위조·변조·훼손의 규모

라) 개인정보처리자가 처리하는 개인정보의 유형과 정보주체에게 미치는 영향

마) 위반행위로 인한 정보주체의 피해 규모

나. 1차 조정

위반행위의 기간 및 횟수, 위반행위로 인하여 취득한 이익의 규모, 개인정보
처리자의 업무 형태 및 규모를 고려하여 가목에 따른 기준금액의 100분의 90의
범위에서 보호위원회가 정하여 고시하는 기준에 따라 가중하거나 감경할 수 있다.

다. 2차 조정

다음의 사항(법 제64조의2제4항 각 호의 사항 중 가목에 따른 기준금액 산정
및 나목에 따른 1차 조정 단계에서 고려된 사항은 제외한다)을 종합적으로
고려하여 1차 조정을 거친 금액의 100분의 50의 범위에서 보호위원회가
정하여 고시하는 기준에 따라 가중하거나 감경할 수 있다.

- 1) 보호위원회와의 협조 등 위반행위를 시정하기 위한 조치 여부
- 2) 위반행위로 인한 피해의 회복 및 피해 확산 방지 조치의 이행 여부
- 3) 개인정보 보호 인증, 자율적인 보호 활동 등 개인정보 보호를 위한 노력
- 4) 위반행위의 주도 여부
- 5) 위반행위 사실의 자진신고 여부

라. 부과과징금의 결정

- 1) 다음의 사항을 고려하여 다목에 따라 산정된 과징금이 과중하다고 인정되는
경우에는 해당 금액의 100분의 90 범위에서 감경할 수 있다.

가) 위반행위자의 현실적인 부담능력

나) 경제위기 등으로 위반행위자가 속한 시장·산업 여건이 현저하게 변동
되거나 지속적으로 악화된 상태인지 여부

- 2) 법 제64조의2제5항 각 호의 어느 하나에 해당하는 경우에는 과징금을
부과하지 않을 수 있다.

3. 세부 기준

매출액의 산정에 관한 세부 기준, 위반행위의 중대성 판단 기준, 1차 조정 및
2차 조정을 위한 세부 기준, 부과과징금의 결정을 위한 세부 기준과 그 밖에
과징금의 부과에 필요한 사항은 보호위원회가 정하여 고시한다.

과태료의 부과기준(제63조 관련)

1. 일반기준

가. 위반행위의 횟수에 따른 과태료의 가중된 부과기준은 최근 3년간 같은 위반행위로 과태료 부과처분을 받은 경우에 적용한다. 이 경우 기간의 계산은 위반행위에 대하여 과태료 부과처분을 받은 날과 그 처분 후 다시 같은 위반행위를 하여 적발된 날을 기준으로 한다.

나. 가목에 따라 가중된 부과처분을 하는 경우 가중처분의 적용 차수는 그 위반행위 전 부과처분 차수(가목에 따른 기간 내에 과태료 부과처분이 둘 이상 있었던 경우에는 높은 차수를 말한다)의 다음 차수로 한다.

다. 부과권자는 다음의 어느 하나에 해당하는 경우에는 제2호의 개별기준에 따른 과태료 금액을 줄이거나 면제할 수 있다. 다만, 과태료를 체납하고 있는 위반행위자에 대해서는 그렇지 않다.

- 1) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우
- 2) 위반의 내용·정도가 경미하다고 인정되는 경우
- 3) 위반행위자가 「중소기업기본법」 제2조에 따른 중소기업자인 경우 등 위반행위자의 업무 형태 및 규모에 비해 과중하다고 인정되는 경우
- 4) 위반행위자가 법 위반상태를 시정하거나 해소하기 위하여 노력한 것이 인정되는 경우
- 5) 위반행위자가 위반행위로 인한 피해의 회복 및 피해 확산 방지 조치를 이행한 경우
- 6) 위반행위자가 법 제32조의2에 따른 개인정보 보호 인증을 받거나 자율적인 보호 활동을 하는 등 개인정보 보호를 위하여 노력한 것이 인정되는 경우
- 7) 위반행위자가 위반행위 사실을 자진신고한 경우
- 8) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료 금액을 줄이거나 면제할 필요가 있다고 인정되는 경우

라. 부과권자는 다음의 어느 하나에 해당하는 경우에는 제2호의 개별기준에 따른 과태료의 2분의 1 범위에서 그 금액을 늘려 부과할 수 있다. 다만, 늘려 부과하는 경우에도 법 제75조제1항부터 제4항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.

- 1) 위반의 내용·정도가 중대하여 정보주체 등에게 미치는 피해가 크다고 인정되는 경우
- 2) 그 밖에 위반행위의 정도·기간, 위반행위의 동기와 그 결과 등을 고려하여 과태료 금액을 늘릴 필요가 있다고 인정되는 경우

2. 개별기준

(단위: 만원)

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
가. 법 제11조의2제2항을 위반하여 정당한 사유 없이 자료를 제출하지 않거나 거짓으로 제출한 경우 1) 자료를 제출하지 않은 경우 2) 자료를 거짓으로 제출한 경우	법 제75조 제4항제1호	100 200	200 400	400 800
나. 법 제16조제3항·제22조제5항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 재화 또는 서비스의 제공을 거부한 경우	법 제75조 제2항제1호	600	1,200	2,400
다. 법 제20조제1항·제2항을 위반하여 정보주체에게 같은 조 제1항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제2호	600	1,200	2,400
라. 법 제20조의2제1항을 위반하여 개인정보의 이용·제공 내역이나 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 통지하지 않은 경우	법 제75조 제2항제3호	600	1,200	2,400
마. 법 제21조제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제4호	600	1,200	2,400
바. 법 제21조제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 분리하여 저장·관리하지 않은 경우	법 제75조 제4항제2호	200	400	800
사. 법 제22조제1항부터 제3항까지(법 제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 동의를 받은 경우	법 제75조 제4항제3호	200	400	800
아. 법 제23조제2항·제24조제3항·제25조제6항(법 제25조의2제4항에 따라 준용되는 경우를 포함한다)·	법 제75조 제2항제5호	600	1,200	2,400

제28조의4제1항·제29조(법 제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우				
자. 법 제23조제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 알리지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
차. 법 제24조의2제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 주민등록 번호를 처리한 경우	법 제75조 제2항제7호	600	1,200	2,400
카. 법 제24조의2제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 암호화 조치를 하지 않은 경우	법 제75조 제2항제8호	600	1,200	2,400
타. 법 제24조의2제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체가 주민등록번호를 사용하지 않을 수 있는 방법을 제공하지 않은 경우	법 제75조 제2항제9호	600	1,200	2,400
파. 법 제25조제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보 처리기기를 설치·운영한 경우	법 제75조 제2항제10호	600	1,200	2,400
하. 법 제25조제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 고정형 영상정보 처리기기를 설치·운영한 경우	법 제75조 제1항제1호	1,000	2,000	4,000
거. 법 제25조의2제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 사람 또는 그 사람과 관련된 사물의 영상을 촬영한 경우	법 제75조 제2항제11호	600	1,200	2,400
너. 법 제25조의2제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영한 경우	법 제75조 제1항제2호	1,000	2,000	4,000
더. 법 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서로 하지 않은 경우	법 제75조 제4항제4호	200	400	800

러. 법 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 않은 경우	법 제75조 제4항제5호	200	400	800
머. 법 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조 제2항제12호	600	1,200	2,400
버. 법 제26조제6항을 위반하여 위탁자의 동의를 받지 않고 제3자에게 다시 위탁한 경우	법 제75조 제3항제1호	400	800	1,600
서. 법 제27조제1항·제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 않은 경우	법 제75조 제4항제6호	200	400	800
어. 법 제28조의4제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 관련 기록을 작성하여 보관하지 않은 경우	법 제75조 제4항제7호	200	400	800
저. 법 제28조의5제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인을 알아볼 수 있는 정보가 생성되었음에도 이용을 중지하지 않거나 이를 회수·파기하지 않은 경우	법 제75조 제2항제13호	600	1,200	2,400
처. 법 제28조의8제4항(법 제26조제8항 및 제28조의 11에 따라 준용되는 경우를 포함한다)을 위반하여 보호조치를 하지 않은 경우	법 제75조 제2항제14호	600	1,200	2,400
커. 법 제30조제1항 또는 제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리방침을 정하지 않거나 이를 공개하지 않은 경우	법 제75조 제4항제8호	200	400	800
터. 법 제31조제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 보호책임자를 지정하지 않은 경우	법 제75조 제4항제9호	200	400	800
퍼. 법 제31조의2제1항을 위반하여 국내대리인을 지정하지 않은 경우	법 제75조 제3항제2호	2,000		
허. 법 제32조의2제6항을 위반하여 인증을 받지 않았음에도 거짓으로 인증의 내용을 표시하거나 홍보한 경우	법 제75조 제2항제15호	600	1,200	2,400

고. 법 제33조제1항을 위반하여 영향평가를 하지 않거나 그 결과를 보호위원회에 제출하지 않은 경우	법 제75조 제2항제16호	600	1,200	2,400
노. 법 제34조제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 같은 항목 호의 사실을 알리지 않은 경우	법 제75조 제2항제17호	600	1,200	2,400
도. 법 제34조제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 보호위원회 또는 전문기관에 신고하지 않은 경우	법 제75조 제2항제18호	600	1,200	2,400
로. 법 제35조제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 열람을 제한하거나 거절한 경우	법 제75조 제2항제19호	600	1,200	2,400
모. 법 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제4항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조 제4항제10호	200	400	800
보. 법 제35조의3제1항에 따른 지정을 받지 않고 같은 항 제2호의 업무를 수행한 경우	법 제75조 제2항제20호	600	1,200	2,400
소. 법 제35조의3제3항을 위반한 경우	법 제75조 제2항제21호	600	1,200	2,400
오. 법 제36조제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정정·삭제 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제22호	600	1,200	2,400
조. 법 제37조제3항 또는 제5항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제23호	600	1,200	2,400
초. 법 제37조의2제3항(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 정당한 사유 없이 정보주체의 요구에 따르지 않은 경우	법 제75조 제2항제24호	600	1,200	2,400
코. 법 제45조제1항에 따른 자료를 정당한 사유 없이 제출하지 않거나 거짓으로 제출한 경우	법 제75조 제4항제11호			

1) 자료를 제출하지 않은 경우		100	200	400
2) 자료를 거짓으로 제출한 경우		200	400	800
토. 법 제45조제2항에 따른 출입·조사·열람을 정당한 사유 없이 거부·방해 또는 기피한 경우	법 제75조 제4항제12호	200	400	800
포. 법 제63조제1항(법 제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 관계 물품·서류 등 자료를 제출하지 않거나 거짓으로 제출한 경우	법 제75조 제2항제25호			
1) 자료를 제출하지 않은 경우		300	600	1,200
2) 자료를 거짓으로 제출한 경우		600	1,200	2,400
호. 법 제63조제2항(법 제26조제8항에 따라 준용되는 경우를 포함한다)에 따른 출입·검사를 거부·방해 또는 기피한 경우	법 제75조 제2항제26호	600	1,200	2,400
구. 법 제64조제1항에 따른 시정조치 명령에 따르지 않은 경우	법 제75조 제2항제27호	600	1,200	2,400

[별지 제1호 서식]

개인정보파일 ([] 등록 [] 변경등록) 신청서

※ '변경정보 및 변경사유' 란은 변경등록시에만 작성합니다.

접수번호	접수일	처 리 7일 기간	
공공기관 명칭	주소	등록부서	전화번호
등록항목	등록정보	변경정보 및 변경사유	
개인정보파일 명칭			
개인정보파일의 운영 근거 및 목적			
개인정보파일에 기록되는 개인정보의 항목			
개인정보의 처리방법			
개인정보의 보유기간			
개인정보를 통상적 또는 반복적으 로 제공하는 경우 그 제공받는 자			
개인정보파일을 운용하는 공공기관의 명칭			
개인정보파일로 보유하고 있는 개인정보의 정보주체 수			
해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서			
개인정보의 열람 요구를 접수· 처리하는 부서			
개인정보파일에서 열람을 제한 하거나 거절할 수 있는 개인정보의 범위 및 그 사유			

「개인정보 보호법」 제32조제1항과 같은 법 시행령 제34조제1항에 따라 위와 같이
개인정보파일 ([] 등록 [] 변경등록)을 신청합니다.

년 월 일

신청기관

(서명 또는 인)

개인정보보호위원회 귀하

[별지 제2호 서식]

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	<input type="checkbox"/> 목적 외 이용 <input type="checkbox"/> 제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의 경우)		담당자	소 속
			성 명 (서명)
			전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	소 속
			성 명 (서명)
			전화번호
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			
제공 승인일		승인자 (개인정보보호(분야별)책임자)	

개인정보파일 파기 요청서

작성일		작성자	
파기 대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보(분야별)보호책임자)	
파기 장소			
파기 방법			
파기 수행자		입회자	
폐기 확인 방법			
백업 조치 유무			
매체 폐기 여부			

[별지 제4호 서식]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

개인정보처리시스템 접속기록 점검 대장

□ 개인정보처리시스템 접속기록 점검표(예시) 점검자 :

시스템명	항목	점검내용	점검결과	비 고
○○ 시스템	계정	접근권한이 없는 계정 접속 행위 분석		
		- 승인 없는 권한 상승	정상/비정상	
		- 비인가 계정 접속	정상/비정상	
		- 알 수 없는 계정 생성	정상/비정상	
		- 우회경로를 통한 접속	정상/비정상	
		- 그 외 비정상적인 접속 행위	정상/비정상	
	접속일시	업무시간 외 접속 행위 분석		
		- 출근시간 전	정상/비정상	
		- 퇴근시간 후	정상/비정상	
		- 새벽시간	정상/비정상	
		- 휴무일	정상/비정상	
		- 그 외 비정상적 시간 접속	정상/비정상	
	접속지 정보	비인가 단말기 또는 IP 접속 행위 분석		
		- 비인가 단말기 접속 행위 분석	정상/비정상	
		- 비인가 IP 접속 행위 분석	정상/비정상	
	처리한 정보주체 정보	특정 정보주체 과도한 조회, 다운로드 등의 행위 분석		
		- 기간 내 특정 정보주체 조회 ○건 이상	정상/비정상	
		- 기간 내 특정 정보주체 다운로드 ○건 이상	정상/비정상	
	수행업무	대량의 개인정보 조회, 정정, 다운로드, 삭제 행위 분석		
		- 기간 내 개인정보 조회 건 수 ○건 이상	정상/비정상	
		- 기간 내 개인정보 정정 건 수 ○건 이상	정상/비정상	
		- 기간 내 개인정보 다운로드 건 수 ○건 이상	정상/비정상	
		- 기간 내 개인정보 삭제 건 수 ○건 이상	정상/비정상	
	기타	단시간 동일계정으로 다 수 IP로 접속한 행위 분석		
		- ○시간 내 ○개 이상의 IP로 접속한 행위 분석	정상/비정상	

※ 개인정보처리시스템의 특성 및 중요도, 이용자 통계 등을 고려하여 접속기록 점검 결과 비정상 행위가 탐지되었을 경우, (분야별) 개인정보 보호책임자에게 보고하여 적절한 대응조치를 취해야 함

비정상 행위에 대한 후속조치(해당시)	점검·분석 결과 이상이 있을 경우, 조치 및 결과 작성 (이상이 없을 경우, “ 해당 없음 ” 명시)
-------------------------	--

□ 다운로드 사유 확인 점검표(예시)

점검자 :

시스템명	항목	점검내용	점검결과 (해당여부)	비 고
○○시스템	다운로드 정보주체 수	기간 내 ○명 이상의 개인정보를 다운로드 한 경우	유/무	
	기간 내 다운로드 횟수	○시간 내 다운로드 횟수가 ○건 이상인 경우	유/무	
	업무시간 외 다운로드 수행	새벽시간 및 휴무일 등의 업무시간 외 다운로드 한 경우	유/무	
	기 타	그 외 다운로드 사유 확인이 필요하다고 판단되는 경우	유/무	

※ 해당사항이 있을 경우, 다운로드 사유를 반드시 확인하고 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것으로 확인이 되었다면 개인정보취급자가 다운로드 한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 함

다운로드 사유 확인 대상에 대한 후속조치(해당시)	다운로드 사유 확인이 필요한 대상 건에 대한 조사 및 조치 내용 작성 (다운로드 사유 확인 대상 건이 없을 경우, “ <u>해당 없음</u> ” 명시)
-----------------------------------	---

〔별지 제6호 서식〕

개인정보시스템 접속기록 백업 관리대장(예시)

[illegible]

[별지 제7호 서식]

개인영상정보 관리대장

번호	구분	일시	파일명/ 형태	담당자	목적/ 사유	이용· 제공받는 제3자 /열람등 요구자	이용· 제공 근거	이용·제공 형태	이용·제공 기간 및 파기 예정 일자	파기 여부 등 결과 및 처리 일자	안전관리 요청 내용 및 결과
1	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기										
2	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기										
3	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기										
4	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기										
5	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기										
6	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기										

개인정보 유출등 신고서

기관명					
유출등이 된 개인정보 항목 및 규모					
유출등이 된 시점과 그 경위					
유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등					
개인정보처리자의 대응 조치 및 피해 구제절차					
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처					
유출등 신고(보고) 담당자		성명	부서	직위	연락처
	개인정보 보호책임자				
	담당자 (취급자)				

유출등 신고 접수기관	기관명	담당자명	연락처

[별지 제9호 서식]

개인정보(☐ 열람 ☐ 정정·삭제 ☐ 처리정지 ☐ 동의철회) 요구서

※ 아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.

(앞 쪽)

접수번호	접수일	처 리 기 10일 이내 간
정보주체	성 명	전 화 번 호
	생년월일	
	주 소	
대리인	성 명	전 화 번 호
	생년월일	정보주체와의 관계
	주 소	
요구내용	<input type="checkbox"/> 열람	<input type="checkbox"/> 개인정보의 항목 및 내용 <input type="checkbox"/> 개인정보 수집·이용의 목적 <input type="checkbox"/> 개인정보 보유 및 이용 기간 <input type="checkbox"/> 개인정보의 제3자 제공 현황 <input type="checkbox"/> 개인정보 처리에 동의한 사실 및 내용
	<input type="checkbox"/> 정정·삭제	※ 정정·삭제하려는 개인정보의 항목과 그 사유를 적습니다.
	<input type="checkbox"/> 처리정지	※ 개인정보의 처리정지를 원하는 대상·내용 및 그 사유를 적습니다.
	<input type="checkbox"/> 동의철회	※ 개인정보의 동의철회를 원하는 대상·내용 및 그 사유를 적습니다.

「개인정보 보호법」 제35조제1항·제2항, 제36조제1항 또는 제37조제1항과 같은 법 시행령 제41조제1항, 제43조제1항 또는 제44조제1항에 따라 위와 같이 요구합니다.

년 월 일

요구인

(서명 또는 인)

0000 귀하

작 성 방 법

1. '대리인'란은 대리인이 요구인일 때에만 적습니다.
2. 개인정보의 열람을 요구하려는 경우에는 '열람' 란에 ☒ 표시를 하고 열람하려는 사항을 선택하여 ☒ 표시를 합니다. 표시를 하지 않은 경우에는 해당 항목의 열람을 요구하지 않은 것으로 처리됩니다.
3. 개인정보의 정정·삭제를 요구하려는 경우에는 '정정·삭제' 란에 ☒ 표시를 하고 정정하거나 삭제하려는 개인정보의 항목과 그 사유를 적습니다.
4. 개인정보의 처리정지를 요구하려는 경우에는 '처리정지' 란에 ☒ 표시를 하고 처리정지 요구의 대상·내용 및 그 사유를 적습니다.
5. 개인정보의 동의철회를 요구하려는 경우에는 '동의철회' 란에 ☒ 표시를 하고 동의철회 요구의 대상·내용 및 그 사유를 적습니다.

[별지 제10호 서식]

개인영상정보(□ 열람 □ 존재확인) 청구서				처리기한
※ 아래 유의사항을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.				10일 이내
청 구 인	성 명		전 화 번 호	
	생년월일		정보주체와의 관계	
	주 소			
정보주체의 인적사항	성 명		전 화 번 호	
	생년월일			
	주 소			
청구내용 (구 체 적 으 로 요청하지 않 으면 처리가 곤란할 수 있 음)	영상정보 기록기간	(예 : 2018.01.01 18:30 ~ 2018.01.01 19:00)		
	영상정보 처리기기 설치장소	(예 : 00시 00구 00대로 0 인근 CCTV)		
	청구 목적 및 사유			
「표준 개인정보 보호지침」 제44조에 따라 위와 같이 개인영상정보의 열람, 존재 확인을 청구합니다.				
<div style="text-align: center;"> 년 월 일 </div> <div style="text-align: right;"> 청구인 (서명 또는 인) </div> <div style="text-align: center;"> ○ ○ ○ ○ 귀하 </div>				
담당자의 청구인에 대한 확인 서명				

[별지 제11호 서식]

개인정보 (☐ 열람 ☐ 일부열람 ☐ 열람연기 ☐ 열람거절) 통지서

(앞 쪽)

수신자 (우편번호: , 주소:)

요구 내용			
열람 일시			열람 장소
통지 내용 (<input type="checkbox"/> 열람 <input type="checkbox"/> 일부열람 <input type="checkbox"/> 열람연기 <input type="checkbox"/> 열람거절)			
열람 형태 및 방법	열람 형태	<input type="checkbox"/> 열람·시청 <input type="checkbox"/> 사본·출력물 <input type="checkbox"/> 전자파일 <input type="checkbox"/> 복제물·인화물 <input type="checkbox"/> 기타	
	열람 방법	<input type="checkbox"/> 직접방문 <input type="checkbox"/> 우편 <input type="checkbox"/> 팩스 <input type="checkbox"/> 전자우편 <input type="checkbox"/> 기타	
납부 금액	①수수료	②우송료	계(①+②)
	원	원	원
	수수료 산정 명세		
사 유			
이의제기방법	※ 개인정보처리자는 이의제기방법을 적습니다.		

「개인정보 보호법」 제35조제3항·제4항 또는 제5항과 같은 법 시행령 제41조제5항 또는 제42조제2항에 따라 귀하의 개인정보 열람 요구에 대하여 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

[별지 제12호 서식]

개인정보 ([] 정정·삭제, [] 처리정지, [] 동의철회) 요구에 대한 결과 통지서

수신자 (우편번호: , 주소:)

요구 내용	
<input type="checkbox"/> 정정·삭제 <input type="checkbox"/> 처리정지 <input type="checkbox"/> 동의철회 조치 내용	
<input type="checkbox"/> 정정·삭제 <input type="checkbox"/> 처리정지 <input type="checkbox"/> 동의철회 결정 사유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.

「개인정보 보호법」 제36조제6항 및 같은 법 시행령 제43조제3항 또는 같은 법 제37조제6항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

유의사항

개인정보의 정정·삭제 또는 처리정지, 동의철회 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.

위임장

위임받는 자	성명	전화번호
	생년월일	정보주체와의 관계
	주소	
위임자	성명	전화번호
	생년월일	
	주소	

「개인정보 보호법」 제38조제1항에 따라 위와 같이 개인정보의 (☐ 열람, ☐ 정정·삭제, ☐ 처리정지, ☐ 동의철회)의 요구를 위의 자에게 위임합니다.

년 월 일

위임자

(서명 또는 인)

0000 귀하

OO개인정보처리시스템 접근권한 관리대장(예시)

소속(부서)	성명	계정	업무	접근권한 (권한명, 내역 등)	지정일자	해제일자	처리자
인재경영실	홍길동	qidmlsk55	인사관리	인사정보(입력, 조회, 수정)	20223-08-01		홍부장

개인정보처리시스템 접근권한 신청서(예시)

신청일 : 20 년 월 일

1. 신청인	부서		직급		성명	
2. 담당업무						
3. 이용업무명						
4. 비고						

<신청시 유의사항>

- 본인의 업무를 해당 시스템을 통하여 처리하고자 하는 경우에만 접근권한을 신청하여야 하며, 소관업무 이외의 업무처리를 위해 접근권한을 신청하거나, 업무이외의 용도로 해당 시스템을 이용하여서는 안됩니다.

<기재요령>

1. 신청인 : 신청인의 소속부서, 직급, 직위 및 성명을 기재합니다.
2. 담당업무 : 신청인의 소속부서에서 담당하고 있는 업무를 기재합니다.
3. 이용업무명 : 신청인이 시스템에서 이용하고자 하는 업무를 기재합니다.
4. 비고 : 신청하는 업무를 일시적으로만 처리하기 위해 신청하는 경우에는 그 기간, 그 외 특기사항이 있는 경우 그 내용을 기재합니다.

부서장	부서		직급		성명	(서명)
-----	----	--	----	--	----	------

개인정보보호 보안서약서(예시)

본인은 개인정보를 처리·취급하는 업무에 있어 다음과 같은 행동 수칙을 성실히 준수하겠습니다.

1. 상당한 사유 없이 다른 사람의 개인정보를 열람하거나 처리하지 않는다.
2. 업무상 알게된 개인정보를 누설하거나 다른 사람에게 제공하지 않는다.
3. 개인정보가 포함된 자료를 외부에 전송할 때는 반드시 안전한 비밀번호를 설정하고, 설정한 비밀번호는 다른 연락 수단을 활용하여 수신자에게 알려 준다.
4. 개인정보가 포함된 자료를 가급적 개인용 컴퓨터에 저장하지 않는다. 업무상 불가피하게 저장하는 경우에는 문서를 암호화하여 저장한다.
5. 개인정보가 담긴 서류 또는 보조저장매체는 안전한 장소에 보관한다.
6. 개인정보처리시스템 계정 로그인 정보를 다른 취급자와 공유하지 않는다. 특히 권한 없는 제3자가 나의 계정을 사용하게 하지 않는다.
7. 전보나 휴직 등으로 사용하던 개인정보처리시스템과 관련한 업무처리권한이 없어진 경우 해당 시스템을 사용하지 않는다.
8. 비밀번호는 알파벳 대문자·소문자, 숫자, 특수기호 등을 활용하여 최소 8자리 이상으로 안전하게 설정 하고, 주기적으로 변경한다.

본인은 본 서약서의 내용을 충분히 검토하고 자유로운 의사에 따라 이에 서명함을 확인하며, 위 각 사항을 준수하지 않음으로 인하여 발생하는 모든 책임은 본인에게 있음을 인정하고, ○○○대학교에서 정하는 규정 등에 의해 처리됨을 동의합니다.

20 년 일 일

소속 :

성명 : (서명)

○○○대학교 원장

개인정보처리시스템 암호키 관리대장(예시)

[illegible]

개인정보처리시스템 암호키 백업대장(예시)

백업대상	백업 주기	백업일자	키백업 패스워드 관리여부	완료확인	
				점검자	부서장
ex) 관리대상 암호키	<input type="checkbox"/> 연간 <input type="checkbox"/> 반기		ex) 보관형식(이동매체, 파일 등) 기술		

개인정보 수탁기관 관리실태 점검표(예시)

□ 개인정보 수탁업체 명 :

○ 개인정보 처리시스템 : 000

점검자 : (인) 확인자 : 개인정보 보호책임자(인)

분야	점검 항목	점검결과		개선기한 (2024년 0월 00일한)
		양호 (해당없음)	개선 필요	
1. 업무위탁 계약	1. 필수 반영사항(9개*)이 포함된 개인정보처리 위탁계약서 작성 여부 * 필수사항 : ①목적·범위 ②위탁기간 ③재위탁 제한 ④접근제한 등 기술·관리적 안전조치 ⑤위탁업무 수행 목적외 처리금지 ⑥관리·감독사항 ⑦정보주체 권리보장 ⑧개인정보 파기 ⑨손해배상 등 책임에 대한 사항			
	2. 개인정보처리 위탁계약서 이행 여부			
2. 개인정보의 안전성 확보조치	3. PC에 저장된 개인정보의 암호화 여부			
	4. 개인정보 처리시스템에 대한 접근권한 부여시 필요 최소한의 범위로 업무 담당자에 따라(1인 1계정) 차등 부여 여부			
	5. 개인정보 처리시스템에 대한 접근권한을 3년이상 보관 여부			
	6. 개인정보 처리시스템에 대한 접속 비밀번호 규칙 준수 여부(영문+숫자+특수문자)			
	7. 저장매체 등 물리적 접근방지 조치 적용 여부			
	8. 개인정보 처리시스템 접속기록 1년 이상 보관 여부 * 5만명 이상 또는 고유식별정보나 민감정보의 경우, 2년 이상 보관			
	9. 개인정보 처리시스템에 대한 접속기록의 주기적인 점검 여부			
	10. 취급자의 접속이력 기록시 필수항목(5개*)을 기록하고 있는지 여부 * 필수항목 : ①ID, ②날짜 및 시간, ③접속자 IP주소, ④수행 업무(열람, 수정, 삭제, 인쇄, 입력 등) ⑤처리한 정보주체 정보			
	11. 비인가 프로그램 및 유해사이트 접속 차단 여부			
	12. 개인정보취급자가 외부에서 정보통신망을 통한 접속 시 가상사설망(VPN), 전용선 등 안전한 접속수단을 제공하고 있는지 여부			
	13. 보안 프로그램(백신)을 자동 업데이트 또는 1일 1회 이상 업데이트 하여 최신의 상태로 유지하고 있는지 여부			
	14. 비밀번호의 내부 저장 시 일방향 암호화(해쉬함수) 알고리즘을 적용하고 있는지 여부			
3. 수탁자 교육	15. 수탁자 자체 교육실시 여부 * 자체 교육계획을 수립 및 교육 실시 후 결과 보고			

[별지 제20호 서식]

가명정보 관리대장(예시)

번호	기간	목적	항목	처리 및 보유기간	제공받는 자 등	위탁사항	제한사항	처리구분	기타 (추가정보)	가명처리 수행자	책임자

2024년 00시스템(00파일) 개인정보 파기 계획(안)

(2025.00.00., 정보보호총괄부)

□ 추진 근거

- 개인정보 보호법 제21조(개인정보의 파기) 및 동법시행령 제16조 (개인정보의 파기방법)
- 정보보호총괄부-0(2025.03.00.)호, '2024년도 개인정보보호 업무 추진 계획(안)'

□ 추진 내용

- (대상) 개인정보 보유기간 경과, 처리 목적 달성 등에 따른 00시스템(00파일)의 개인정보(이름, 생년월일, 휴대폰번호, 주소)

구분	00시스템(00파일)	구분	00시스템(00파일)	구분	00시스템(00파일)	구분	00시스템(00파일)
1월	1,200건	4월	1,200건	7월	1,200건	10월	1,200건
2월	1,300건	5월	1,300건	8월	1,300건	11월	1,300건
3월	1,500건	6월	1,500건	9월	1,500건	12월	1,500건

※ 개인정보 보유기간을 기준으로 예상 파기 건수를 측정하였으며, 실제 파기 규모는 변동될 수 있음

- (일시) 매월 00일 00:00
- (방법) 복원이 불가능한 방법으로 완전 삭제

※ 개인정보(파일) 파기는 기관 개인정보보호 담당자 입회하여 진행(입회가 불가능한 경우 파기 후 완전 삭제 여부 점검)

- (결과) 매월 개인정보 파기 후(완전 삭제 여부 점검) 개인정보 파기 관리대장 기록·관리

□ 향후 계획

- 최종 개인정보(파일) 파기 후 파기 결과를 개인정보 보호책임자 보고(12월)

※ 보고 완료된 개인정보(파일)는 개인정보보호 종합지원시스템(intra.privacy.go.kr)을 통하여 현행화

개인정보 반환 · 파기 여부 확인서(예시)

개인정보가 안전하게 반환 · 파기되었음을 다음과 같이 확인합니다.

위탁기관	○○○대학교	위탁업무	
수탁업체			
반환·파기 대상 개인정보		반환·파기 사유	ex) 위탁업무 종료
반환·파기 일자	ex) 위탁계약 종료일로부터 5일 이내 파기	파기 장소	
반환·파기 처리자	ex) 반환 시 개인정보를 전달 받은 사람 ex) 파기 시 파기를 수행 한 사람	입회자 (파기 시)	ex) ○○○대학교 업무 담당자
파기 방법	ex) 복원이 불가능한 방법으로 개인정보 완전 삭제		
백업 유무	(O, X)	특이사항	

20 년 월 일

수탁업체	업체명	
	담당자	(서명)
위탁업체(○○○대학교)	확인자	(서명)

○○○대학교 원장

○○○대학교 영상정보처리기기 표준 지침

제1장 총 칙

제1조(목적) 이 표준지침은 「개인정보 보호법」에 의거 ○○○대학교(이하 “○○○대학교”라 한다)에서 고정형 영상정보처리기기운영자 또는 이동형 영상정보처리기기 운영자가 설치·운영하는 고정형 영상정보처리기기 또는 이동형 영상정보처리기기와 그 기기를 통하여 처리되는 개인 영상정보를 대상으로 한다.

제2조(정의) 이 표준지침에서 사용하는 용어의 정의는 다음과 같다.

1. “소속기관”이라 함은 ○○○대학교 행정조직 및 부속시설 등을 말한다.
2. “개인정보”라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하거나 다른 정보와 결합하여 당해 개인을 식별할 수 있는 정보를 말하며, 이를 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보도 포함한다.
- 2의2. “개인영상정보”라 함은 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.
3. “처리”라 함은 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
4. “개인정보파일”이라 함은 컴퓨터 등에 의하여 처리할 수 있도록 체계적으로 구성된 개인정보의 집합물로서 자기테이프·자기디스크 등 전자적인 매체에 기록된 것을 말한다.
5. “처리정보”라 함은 개인정보파일에 기록되어 있는 개인정보를 말한다.
6. “영상정보처리기기”라 함은 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치로서 시행령 제3조에 따른 폐쇄회로텔레비전(CCTV) 및 네트워크카메라를 말한다.
- 6의2. “폐쇄회로 텔레비전(CCTV)”이라 함은 다음 각 목의 어느 하나에 해당하는 장치를 말한다.
 - 가. 일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송하는 장치
 - 나. 가목에 따라 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치
- 6의 3. “네트워크 카메라”이라 함은 일정한 공간에 지속적으로 설치된 기기로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치를 말한다.
- 6의 4. “영상정보처리기기운영자”이라 함은 법 제25조제1항 각호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.

7. “보유”라 함은 개인정보파일을 작성 또는 취득하거나 유지·관리하는 것(개인정보의 처리를 다른 기관·단체 등에 위탁하는 경우를 포함하되, 다른 기관·단체 등으로부터 위탁받은 경우를 제외한다)을 말한다.

8. “보유기관”이라 함은 개인정보파일을 보유하는 기관을 말한다.

9. “정보주체”라 함은 처리정보에 의하여 식별되는 자로서 당해 정보의 주체가 되는 자를 말한다.

제3조(적용범위) ① 업무부서가 범죄예방·증거확보·시설안전·화재예방·교통정보제공·법규위반 단속 등 공익을 위하여 필요한 경우에 설치·운영하는 영상정보처리기는 다른 법령에 특별한 규정이 있는 경우를 제외하고는 이 지침에 따른다.

② 허가를 받은 사람만 출입이 허용되는 건물 내부공간은 ‘비공개 장소’로 영상정보처리 기기 규정 대상에서 제외한다. 다만, 비공개된 장소에 설치된 영상정보처리기는 개인정보 보호법 제25조(영상정보처리기기의 설치·운영 제한)가 적용되지 않으나 이를 통해 수집되는 영상정보는 개인정보에 해당하므로 개인영상정보의 안전한 관리를 위하여 개인정보 보호법 제25조를 준용토록 한다.

③ 목욕실, 화장실, 탈의실 등 개인 사생활 침해가 우려되는 장소의 내부에서는 설치·운영을 하여서는 안된다. 다만, 구금·보호시설, 정신보건시설 등 법령에 근거하여 구금·보호하는 시설은 제외한다.

제4조(영상정보처리기기의 보호원칙) ① 업무부서의 장은 영상정보처리기기의 설치목적에 부합하는 필요소한의 범위 안에서 정보를 수집하여야 한다.

② 업무부서의 장은 제1항의 설치목적에 정보주체가 명확히 인식할 수 있도록 하여야 하며, 영상정보를 그 목적 이외의 용도로 활용하여서는 아니 된다.

③ 업무부서의 장은 영상정보의 정확성 및 최신성을 확보하여 이를 안전하게 관리하도록 노력하여야 한다.

④ 업무부서의 장은 영상정보의 취급에 관한 일반사항을 공개하고, 영상정보에 대한 정보주체의 권리를 보장하여야 한다.

제2장 영상정보처리기기 설치 시 준수사항

제1절 고정형 영상정보처리기기 운영

제5조(규정의 수립 등) 업무부서의 장은 고정형 영상정보처리기기를 설치할 경우 고정형 영상정보처리기기 운영·관리 방침을 마련하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

제6조(관리책임자의 지정) ① 고정형 영상정보처리기기운영자는 개인영상정보의 처리에 관한 업무를 총괄해서 책임질 관리책임자를 지정하여야 한다.

② 영상정보처리기기의 관리책임자는 다음 각 호의 업무를 수행한다.

1. 개인영상정보 보호 계획의 수립 및 시행
2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
4. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인영상정보 보호 교육 계획 수립 및 시행

6. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독

7. 그밖에 개인영상정보의 보호를 위하여 필요한 업무

제7조(사전의견수렴) ① 고정형 영상정보처리기를 설치하려는 업무부서의 장은 다음 각 호의 구분에 따른 방법으로 관련 전문가 및 이해관계인의 의견을 수렴하여야 한다.

1. 「행정절차법」에 따른 행정예고(20일 이상)의 실시 또는 의견청취
2. 해당 영상정보처리기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회·설문조사 또는 여론조사

② 법 제25조제2항 단서에 따른 시설에 영상정보처리기를 설치·운영하려는 자는 다음 각 호의 사람으로부터 의견을 수렴하여야 한다.

1. 관계 전문가
2. 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

③ 영상정보처리기의 설치 목적 변경에 따른 추가 설치 등의 경우에도 제1항에 따라 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

제8조(안내판의 설치) ① 업무부서의 장은 고정형 영상정보처리기를 설치할 경우 정보주체가 이를 쉽게 인식할 수 있도록 다음 각 호의 사항을 기재한 안내판을 설치하는 등 필요한 조치를 취하여야 한다.

1. 설치목적 및 장소

2. 촬영범위 및 시간

3. 관리책임자의 연락처

4. 고정형 영상정보처리기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처

② 제1항에 따른 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 판독할 수 있게 설치되어야 하며, 이 범위 내에서 고정형 영상정보처리기 운영자가 안내판의 크기, 설치위치 등을 자율적으로 정할 수 있다.

③ 제2항에도 불구하고 건물 안에 다수의 고정형 영상정보처리기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 고정형 영상정보처리기 설치 지역임을 표시하는 안내판을 설치할 수 있다.

④ 업무부서의 장이 기관 내 또는 기관 간에 고정형 영상정보처리기의 효율적 관리 및 정보연계 등을 위해 용도별·지역별 고정형 영상정보처리기를 물리적·관리적으로 통합하여 설치·운영(‘통합관리’라 한다)하는 경우에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 안내판에 기재하여야 한다.

제9조(안내판의 설치의 예외) ① 제8조제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우에는 안내판 설치에 갈음하여 인터넷 홈페이지에 제8조1항의 각 호의 사항을 게재할 수 있다.

1. 원거리 촬영, 과속·신호위반 단속 또는 교통흐름조사 등의 목적으로 영상정보처리기를 설치하는 경우로서 개인정보침해의 위험이 적은 경우

2. 산불감시용 영상정보처리기 등 장소적 특성으로 인하여 안내판을 설치하는 것이 불가능하거나 안내판을 설치하더라도 정보주체가 이를 쉽게 알아볼 수 없는 경우

② 업무부서는 다음 각 호의 어느 하나에 해당하는 시설에 설치하는 영상정보처리기에 대하여는 안내판을 설치하지 아니할 수 있다.

1. 「군사시설보호법」 제2조에 따른 군사시설

2. 「통합방위법」 제2조제13호에 따른 국가중요시설
3. 「보안업무규정」 제32조에 따른 국가보안시설

제2절 이동형 영상정보처리기기 운영

제9조의2(이동형 영상정보처리기기의 촬영 사실 표시) ① 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우에는 불빛, 소리, 안내판, 안내서면, 안내방송 또는 그 밖에 이에 준하는 수단이나 방법으로 정보주체가 촬영 사실을 쉽게 알 수 있도록 표시하고 알려야 한다.

② 드론을 이용한 항공촬영 등 촬영 방법의 특성으로 인해 정보주체에게 촬영 사실을 알리기 어려운 경우에는 보호위원회가 이동형 영상정보처리기기의 촬영 사실 표시를 지원하기 위하여 구축·운영하는 인터넷 사이트에 촬영 사실 및 목적, 촬영 일시 및 장소 등의 사항을 공지하는 방법으로 알릴 수 있다.

제9조의3(이동형 영상정보처리기기의 운영·관리 방침) ① 이동형영상정보처리기기운영자는 법 제25조의2제4항에 따라 영 제25조제1항을 준용하여 다음 각 호의 사항이 포함된 이동형 영상정보처리기기 운영·관리 방침을 마련하여야 한다.

1. 이동형 영상정보처리기기의 운영 근거 및 운영 목적
 2. 이동형 영상정보처리기기의 운영 대수
 3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
 4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
 5. 이동형영상정보처리기기운영자의 영상정보 확인 방법 및 장소
 6. 정보주체의 영상정보 열람 등 요구에 대한 조치
 7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
 8. 그 밖에 이동형 영상정보처리기기의 설치·운영 및 관리에 필요한 사항
- ② 이동형영상정보처리기기운영자가 제1항에 따라 이동형 영상정보처리기기 운영·관리 방침을 마련하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.
- ③ 이동형영상정보처리기기운영자가 법 제30조에 따른 개인정보 처리방침을 정할 때 이동형 영상정보처리기기 운영·관리에 관한 사항을 포함시킨 경우에는 제1항에 따른 이동형 영상정보처리기기 운영·관리 방침을 마련하지 아니할 수 있다. 동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우에는 불빛, 소리, 안내판, 안내서면, 안내방송 또는 그 밖에 이에 준하는 수단이나 방법으로 정보주체가 촬영 사실을 쉽게 알 수 있도록 표시하고 알려야 한다.

제3장 개인영상정보의 처리 시 준수사항

제10조(개인영상정보의 수집제한) 고정형 영상정보처리기기운영자 또는 이동형 영상정보처리기기 운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추어서는 아니 되며, 녹음기능을 사용할 수 없다.

제11조(개인영상정보 이용·제3자 제공 제한 등) ① 고정형 영상정보처리기기운영자 또는 이동형 영상정보처리기기 운영자는 다음 각 호의 경우를 제외하고는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하여서는 아니 된다.

1. 정보주체에게 동의를 얻은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인영상정보를 제공하는 경우
5. 개인영상정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 개인정보 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우
10. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

제12조(보관 및 파기) ① 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자는 고정형 영상정보처리기기 또는 이동형 영상정보처리기기 운영·관리 방침에 명시한 보관기간이 경과하거나 개인영상정보의 처리 목적 달성, 법 제2조제1호에 따른 가명정보의 처리기간 경과 등 그 개인영상정보가 불필요하게 되었을 때에는 지체 없이 그 개인영상정보를 파기하여야 한다. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러하지 아니하다.

② 고정형 영상정보처리기기 운영자가 그 사정에 따라 보유 목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30일 이내로 한다.

③ 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.

1. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
2. 전자기적(電磁氣的) 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제

제13조(개인영상정보 관리대장) ① 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하는 경우에는 다음 각 호의 사항을 「개인영상정보 관리대장」에 기록하고 이를 관리하여야 한다.

1. 개인영상정보 파일의 명칭
2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭
3. 이용 또는 제공의 목적
4. 법령상 이용 또는 제공근거가 있는 경우 그 근거
5. 이용 또는 제공의 기간이 정해져 있는 경우에는 그 기간

6. 이용 또는 제공의 형태

7. 이용 또는 제공한 개인영상정보의 업무처리 담당자

② 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자가 개인영상정보를 파기하는 경우에는 다음 사항을 「개인영상정보 관리대장」에 기록하고 관리하여야 한다.

1. 파기하는 개인영상정보 항목
2. 개인영상정보 파기일시 (사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 관한 확인 시기)
3. 개인영상정보 파기 담당자

제14조(영상정보처리기기 설치 및 관리 등의 위탁) ① 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 이 경우 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁하는 사무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 영상정보에 대한 접근제한 등 안전성 확보조치에 관한 사항
4. 영상정보의 관리현황 점검에 관한 사항
5. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

② 고정형 영상정보처리기기 운영자가 제1항에 따라 고정형 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽게 확인할 수 있도록 고정형 영상정보처리기기 운영·관리방침 및 안내판에 수탁자의 명칭 등을 공개하여야 한다.

② 이동형 영상정보처리기기 운영자가 제1항에 따라 이동형 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 제9조의제2에 따라 이동형 영상정보처리기기 운영·관리방침에 수탁자의 명칭 등을 공개하여야 한다.

③ 고정형 영상정보처리기기 운영자가 또는 이동형 영상정보처리기기 운영자는 제1항에 따라 고정형 영상정보처리기기 또는 이동형 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁할 경우에는 그 사무를 위탁받은 자가 개인영상정보를 안전하게 처리하고 있는지를 관리·감독하여야 한다.

제15조(정보주체의 열람등 요구) ① 정보주체는 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자가 처리하는 자신의 개인영상정보에 대하여 열람 및 존재확인(이하 “열람등”이라 한다)을 해당 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자에게 요구할 수 있다. 다만, 영상정보처리기기 운영자가 공공기관인 경우에는 해당 기관의 장에게 [별지 제9호 서식]에 따른 개인영상정보 열람·존재확인 청구서(전자문서를 포함한다)로 하여야 한다.

② 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자는 제1항에 따른 요구를 받았을 때에는 지체없이 필요한 조치를 취하여야 한다. 이때에 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자는 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인하여야 한다.

③ 제2항의 규정에도 불구하고 법 제35조제4항 각 호의 어느 하나에 해당하는 경우에는 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자는 정보주체의 개인영상정보 열람등 요구를 제한하거나 거부할 수 있다. 이 경우 고정형 영상정보처리기기 운영자

또는 이동형 영상정보처리기기 운영자는 10일 이내에 서면 등으로 거부 사유를 정보주체에게 통지하여야 한다.

④ 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자는 제2항 및 제3항에 따른 조치를 취하는 경우에, 다음 각 호의 사항을 [별지 제6호 서식]의 「개인영상정보 관리 대장」에 기록하고 관리하여야 한다.

1. 개인영상정보 열람 등을 요구한 정보주체의 성명 및 연락처
2. 정보주체가 열람 등을 요구한 개인영상정보 파일의 명칭 및 내용
3. 개인영상정보 열람 등의 목적
4. 개인영상정보 열람 등을 거부한 경우 그 거부의 구체적 사유
5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유
6. 개인영상정보 열람등의 업무처리 담당자

제16조(정보주체 이외의 자의 개인영상정보 보호) 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자는 열람등 필요한 조치를 취할 경우에 해당 개인영상정보 내에 정보주체 이외의 자의 개인영상정보가 포함되어 있는 때에는 해당 제3자의 개인영상정보를 식별할 수 없도록 보호조치를 취하여야 한다. [개정, 2024. 2.]

제17조(개인영상정보의 안전성 확보를 위한 조치) 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 법 제29조 및 시행령 제30조제1항에 따라 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 (네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일에 대한 비밀번호 설정 등)
4. 처리기록의 보관 및 위조·변조 방지를 위한 조치 (개인영상정보의 생성 일시, 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리를 개인영상정보 관리대장에 조치)
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

제18조(개인영상정보처리기기의 설치·운영에 대한 점검) ① 업무부서의 장이 고정형 영상정보 처리기기를 설치·운영하는 경우에는 이 지침의 준수 여부에 대한 자체점검을 실시하여 매년 그 결과를 개인정보 보호책임자에게 통보하고, 시행령 제34조제3항에 따른 시스템에 등록하여야 한다. 이 경우 다음 각 호의 사항을 점검하고 고려하여야 한다.

1. 고정형 영상정보처리기기의 운영·관리 방침에 열거된 사항
2. 관리책임자의 업무 수행 현황
3. 고정형 영상정보처리기기의 설치·운영 현황
4. 개인영상정보 수집 및 이용·제공·파기, 정보주체 권리행사 조치 현황
5. 위탁 및 수탁자에 대한 관리·감독 현황
6. 정보주체의 권리행사에 대한 조치 현황
7. 기술적·관리적·물리적 조치 현황
8. 고정형 영상정보처리기 설치·운영의 필요성 지속 여부 등

② 업무부서의 장은 제1항과 3항에 따른 고정형 영상정보처리기기 설치·운영에 대한 자체 점검을 완료한 후에는 그 결과를 홈페이지 등에 공개하여 한다.

제19조(교육) 업무부서의 장은 영상정보처리기기에 대하여 접근권한을 부여 받은 자로 하여금 정보주체의 개인정보보호를 위한 교육을 이수할 수 있도록 하여야 한다.

제4장 보칙

제20조(비밀유지의무) 영상정보처리기기를 처리하거나 처리하였던 자는 직무상 알게 된 정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용 하여서는 아니 된다.

고정형 영상정보처리기기 운영·관리 방침(예시)

_____ (이하 당 기관이라 함)는 고정형 영상정보처리기기 운영·관리 방침을 통해 본 기관에서 처리하는 영상정보가 어떠한 용도와 방식으로 이용·관리되고 있는지 알려드립니다.

1. 고정형 영상정보처리기기 설치 근거 및 설치 목적

본 기관은 개인정보 보호법 제25조 제1항에 따라 다음과 같은 목적으로 고정형 영상정보처리기기를 설치·운영합니다.

- 시설안전 및 화재 예방, 고객의 안전을 위한 범죄 예방, 차량도난 및 파손방지(주차장에 설치하는 경우)
- ※ 주차대수 30대를 초과하는 규모의 경우 「주차장법 시행규칙」 제6조제1항을 근거로 설치·운영 가능

2. 설치 대수, 설치 위치 및 촬영범위

설치 대수	설치 위치 및 촬영 범위
00대	건물로비, 주차장 입구

3. 관리책임자 및 접근권한자

귀하의 개인영상정보를 보호하고 개인영상정보와 관련한 불만을 처리하기 위하여 아래와 같이 개인영상정보 보호책임자 및 접근권한자를 두고 있습니다.

	이름	직위	소속	연락처
관리책임자	홍길동		0000팀	00-0000-0000
접근권한자				

4. 개인영상정보 촬영시간, 보관기간, 보관장소 및 처리방법

촬영시간	보관기간	보관장소
24시간	촬영일로부터 30일	000실 (보관시설 명)

- 처리방법 : 개인영상정보의 목적외 이용, 제3자 제공, 파기, 열람 등 요구에 관한 사항을 기록·관리하고, 보관기간 만료시 복원이 불가능한 방법으로 영구 삭제(출력물의 경우 파쇄 또는 소각)합니다.

5. 고정형 영상정보처리기기 설치 및 관리 등의 위탁에 관한 사항 [해당하는 경우만]

당 기관은 아래와 같이 고정형 영상정보처리기기 설치 및 관리 등을 위탁하고 있으며, 관계 법령에 따라 위탁계약 시 개인정보가 안전하게 관리될 수 있도록 필요한 사항을 규정하고 있습니다.

수탁업체	담당자	연락처
OO시스템	홍길동	02) 000-0000

6. 개인영상정보 확인 방법 및 장소에 관한 사항

- 확인 방법 : 개인영상정보 관리책임자에게 미리 연락하고 본사를 방문하시면 확인 가능합니다.
- 확인 장소 : OO부서 OO팀

7. 정보주체의 개인영상정보 열람 등 요구에 대한 조치

귀하는 개인영상정보에 관하여 열람 또는 존재확인 · 삭제를 원하는 경우 언제든지 고정형 영상정보 처리기기 운영자에게 요구하실 수 있습니다. 단, 귀하가 촬영된 개인영상정보에 한정됩니다.

본 기관은 개인영상정보에 관하여 열람 또는 존재확인 · 삭제를 요구한 경우 지체없이 필요한 조치를 하겠습니다.

8. 개인영상정보의 안전성 확보조치

본 기관에서 처리하는 개인영상정보는 암호화 조치 등을 통하여 안전하게 관리되고 있습니다. 또한 본 기관은 개인영상정보보호를 위한 관리적 대책으로서 개인정보에 대한 접근 권한을 차등부여하고 있고, 개인영상정보의 위 · 변조 방지를 위하여 개인영상정보의 생성 일시, 열람시 열람 목적 · 열람자 · 열람 일시 등을 기록하여 관리하고 있습니다. 이 외에도 개인영상정보의 안전한 물리적 보관을 위하여 잠금장치를 설치하고 있습니다.

9. 고정형 영상정보처리기기 운영 · 관리방침 변경에 관한 사항

이 고정형 영상정보처리기기 운영 · 관리방침은 2000년 0월 00일에 제정되었으며 법령 · 정책 또는 보안기술의 변경에 따라 내용의 추가 · 삭제 및 수정이 있을 시에는 시행하기 최소 7일 전에 본 기관 홈페이지를 통해 변경사유 및 내용 등을 공지하도록 하겠습니다.

- 공고일자 : 2000년 0월 00일 / 시행일자 : 2000년 0월 00일

○○○대학교 「개인정보 처리방침」 표준가이드

[개인정보 처리방침] 게재 안내

1. 대상 : 회원가입 등 개인정보를 보유한 홈페이지
2. 위치 : 홈페이지 하단에 잘 보이도록 게재(글 색깔 및 크기도 구분되게)
3. 내용 : 아래 내용을 참고하여 단위조직 상황에 맞게 수정

[개인정보 처리방침] 기재 사항 점검표

개인정보 처리방침 기재 항목	
① 제목 및 서문(필수)	
② 개인정보의 처리목적(필수)	
③ 개인정보의 처리 및 보유 기간(필수)	
④ 처리하는 개인정보의 항목(필수)	
⑤ 개인정보의 파기절차 및 파기방법(필수)	
⑥ 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항(필수)	
⑦ 개인정보의 안전성 확보조치에 관한 사항(필수)	
⑧ 개인정보 보호책임자의 성명 또는 개인정보보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처(필수)	
⑨ 개인정보의 열람청구를 접수·처리하는 부서(필수)	
⑩ 정보주체의 권익침해에 대한 구제방법(필수)	
⑪ 개인정보 처리방침의 변경에 관한 사항(필수)	
⑫ 개인정보파일 등록 현황(해당시 필수)	
⑬ 개인정보의 제3자 제공에 관한 사항(해당시 필수)	
⑭ 개인정보처리의 위탁에 관한 사항(해당시 필수)	
⑮ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당시 필수)	
⑯ 가명정보를 처리하는 경우 가명정보 처리에 관한 사항(해당시 필수)	
⑰ 추가적인 이용·제공 관련 판단기준(해당시 필수)	
⑱ 개인정보 영향평가 수행결과(권장)	
⑲ 개인정보 관리수준평가 결과(권장)	
⑳ 영상정보처리기기 운영·관리에 관한 사항(권장)	
㉑ 그 밖에 개인정보 처리기준 및 보호조치 등에 관해 자율적으로 정한 사항(권장)	

부록 1 | 개인정보 처리방침 예시 (기본형)

- 하단 예시는 일반적인 사항으로 공공기관에 해당하는 개인정보처리자는 자신의 처리 현황에 맞게 주요 개인정보 처리 표시 및 개인정보 처리방침 본문을 수정하여 반영하여야 함

〈공공기관명〉 개인정보 처리방침

〈공공기관명〉은(는) 정보주체의 자유와 권리 보호를 위해 「개인정보 보호법」 및 관계 법령이 정한 바를 준수하여, 적법하게 개인정보를 처리하고 안전하게 관리하고 있습니다. 이에 「개인정보 보호법」 제30조에 따라 정보주체에게 개인정보 처리에 관한 절차 및 기준을 안내하고, 이와 관련한 고충을 신속하고 원활하게 처리할 수 있도록 하기 위하여 다음과 같이 개인정보 처리방침을 수립·공개합니다.

[주요 개인정보 처리 표시(라벨링)]



※ 기호에 마우스 커서를 대시면 세부 사항을 확인할 수 있으며, 자세한 내용은 아래의 개인정보 처리방침을 확인하시기 바랍니다.

목 차

- | | |
|---|--|
| <ul style="list-style-type: none"> • 개인정보의 처리 목적 • 처리하는 개인정보 항목 • 개인정보 영향평가의 수행 결과 • 개인정보처리의 위탁 • 정보주체와 법정대리인의 권리·의무 및 행사방법 • 개인정보 자동 수집 장치의 설치·운영 및 거부에 관한 사항 • 개인정보 보호책임자 • 권익침해 구제방법 • 영상정보처리기기 설치·운영 | <ul style="list-style-type: none"> • 개인정보의 처리 및 보유기간 • 개인정보파일 등록 현황 • 개인정보의 제3자 제공 • 개인정보의 파기 • 개인정보의 안전성 확보조치 • 가명정보의 처리 • 개인정보 열람청구 • 개인정보 관리수준진단 결과 • 개인정보 처리방침 변경 |
|---|--|

■ 개인정보의 처리목적

① <공공기관명>은(는) 다음의 목적을 위하여 개인정보를 처리합니다. 처리하고 있는 개인정보는 다음의 목적 이외의 용도로는 이용되지 않으며, 이용 목적이 변경되는 경우에는 「개인정보 보호법」 제18조에 따라 별도의 동의를 받는 등 필요한 조치를 이행할 예정입니다.

1. 회원 가입 및 관리회원 가입의사 확인, 회원제 서비스 제공에 따른 본인 식별·인증, 회원자격 유지·관리, 제한적 본인확인제 시행에 따른 본인확인, 서비스 부정이용 방지, 만 14세 미만 아동의 개인정보 처리시 법정대리인의 동의여부 확인, 각종 고지·통지 등을 목적으로 개인정보를 처리합니다.

2. 민원사무 처리

민원인의 신원 확인, 민원사항 확인, 사실조사를 위한 연락·통지, 처리결과 통보 등의 목적으로 개인정보를 처리합니다.

3. 개인정보파일의 등록 및 공개

「개인정보 보호법」 제32조에 따라 등록·공개하는 개인정보파일의 처리목적·보유기간 및 항목은 아래와 같습니다.

개인정보파일의 명칭	운영근거 / 처리목적	개인정보파일에 기록되는 개인정보의 항목	보유기간
국가인재DB	국가공무원법 제19조의3 공직후보자 정보의 체계적 수집·관리	성명, 연령, 전문분야, 연락처, 전·현직 직위, 학력, 경력, 상훈 등	준영구

개인정보파일의 명칭	운영근거 / 처리목적	개인정보파일에 기록되는 개인정보의 항목	보유기간
전자민원 신청이력	공공기록물 관리에 관한 법령 최근 3년간 전자민원 신청이력 정보제공	성명, 주민번호, 전화번호, 주소	3년
주민등록정보	주민등록법 제28조, 제30조 주민등록전산정보 관리, 주민등록증 발급 등	주민등록번호, 성명, 주소사항, 세대사항, 주민등록증 발급사항 등 (5개 분야 10개 사항 161개 세부항목)	영구
○○○	○○○	○○○	

4. <기타 공공기관의 개인정보 처리업무>

<개인정보 처리업무에 따른 처리목적>으로 개인정보를 처리합니다.

■ 개인정보의 처리 및 보유기간

- ① <공공기관명>은(는) 법령에 따른 개인정보 보유·이용 기간 또는 정보주체로부터 개인정보를 수집 시 동의 받은 개인정보 보유·이용기간 내에서 개인정보를 처리합니다.
- ② 각각의 개인정보 처리 및 보유 기간은 다음과 같습니다.
 1. 홈페이지 회원 가입 및 관리 : <공공기관명> 홈페이지 탈퇴시까지
다만, 다음의 사유에 해당하는 경우에는 해당 사유 종료시까지
 - 1) 관계 법령 위반에 따른 수사·조사 등이 진행중인 경우에는 해당 수사, 조사 종료시까지
 - 2) 홈페이지 이용에 따른 채권, 채무관계 잔존시에는 해당 채권, 채무관계 정산시까지
 - 3) <예외 사유> 시에는 <보유기간> 까지
 2. 민원사무 처리 : 민원처리 종료 후 3년
 3. 「OO에 관한 법률」 제0조에 따른 개인정보 처리·보유 : 00년
 4. <개인정보 처리업무> : <보유기간>

■ 처리하는 개인정보 항목

<공공기관명>은(는) 다음의 개인정보 항목을 처리하고 있습니다.

1. 홈페이지 회원 가입 및 관리
 - 필수항목 : 성명, 생년월일, 아이디, 비밀번호, 주소, 전화번호, 성별, 이메일주소, 아이핀번호
 - 선택항목 : 결혼여부, 관심분야

2. 민원사무 처리

- 필수항목 : 성명, 주민등록번호, 전화번호, 주소
- 선택항목 : 이메일주소

3. <개인정보 처리업무>

- 필수항목 : <처리항목>
- 선택항목 : <처리항목>

4. 인터넷 서비스 이용과정에서 아래 개인정보 항목이 자동으로 생성되어 수집될 수 있습니다. (자동으로 생성·수집되는 개인정보항목이 있는 경우)

- IP주소, 쿠키, MAC주소, 서비스 이용기록, 방문기록, 불량 이용기록

■ 개인정보파일 등록 현황

<공공기관명>이(가) 「개인정보 보호법」 제32조에 따라 등록·공개하는 개인정보파일의 처리목적·보유기간 및 항목은 아래와 같습니다.

개인정보파일의 명칭	운영근거 / 처리목적	개인정보파일에 기록되는 개인정보의 항목	보유기간
국가인재DB	국가공무원법 제19조의3 공직후보자 정보의 체계적 수집·관리	성명, 연령, 전문분야, 연락처, 전·현직 직위, 학력, 경력, 상훈	준영구
전자민원 신청이력	공공기록물 관리에 관한 법령 최근 3년간 전자민원 신청이력 정보제공	성명, 주민번호, 전화번호, 주소	3년
주민등록정보	주민등록법 제28조, 제30조 주민등록전산정보 관리, 주민등록증 발급 등	주민등록번호, 성명, 주소사항, 세대사항, 주민등록증 발급사항 (5개 분야 10개 사항 161개 세부항목)	영구
○○○	○○○	○○○	

■ 개인정보 영향평가의 수행 결과

① <공공기관명>은 운영하고 있는 개인정보 처리시스템이 정보주체의 개인정보파일에 미칠 영향에 대해 조사, 분석, 평가하기 위해 「개인정보 보호법」 제33조에 따라 “개인정보 영향평가”를 받고 있습니다.

② <공공기관명>은 다음 개인정보파일에 대해 영향평가를 수행하였습니다.

개인정보파일의 명칭	개인정보파일에 기록되는 개인정보의 항목	영향평가 수행연도
국가인재DB	성명, 연령, 전문분야, 연락처, 현·전직 직위, 학력, 경력, 상훈	2021

■ 개인정보의 제3자 제공

- ① <공공기관명>은(는) 정보주체의 동의, 법률의 특별한 규정 등 「개인정보 보호법」 제17조 및 제18조에 해당하는 경우에만 개인정보를 제3자에게 제공합니다.
- ② <공공기관명>은(는) 법률에 따라 다음과 같이 개인정보를 제공합니다.

제공받는 자	제공목적	제공항목	보유 및 이용기간	관련 근거
<제3자명>	<제공목적>	<제공항목>	<제공받는 자의 보유 및 이용기간>	<관련 근거>
<제3자명>	<제공목적>	<제공항목>	<제공받는 자의 보유 및 이용기간>	<관련 근거>

- ③ <공공기관명>은(는) 원활한 서비스 제공을 위해 다음의 경우 정보주체의 동의를 얻어 필요 최소한의 범위로만 제공합니다.

제공받는 자	제공목적	제공항목	보유 및 이용기간
<제3자명>	<제공목적>	<제공항목>	<제공받는 자의 보유 및 이용기간>

■ 개인정보처리의 위탁

- ① <공공기관명>은(는) 원활한 개인정보 업무처리를 위하여 다음과 같이 개인정보 처리업무를 위탁하고 있습니다.

위탁받는 자(수탁자)	위탁업무
<수탁자명>	<위탁하는 업무>

- ② <공공기관명>은(는) 위탁계약 체결 시 「개인정보 보호법」 제26조에 따라 위탁업무 수행목적 외 개인정보 처리금지, 안전성 확보조치, 재위탁 제한, 수탁자에 대한 관리·감독, 손해배상 등 책임에 관한 사항을 계약서 등 문서에 명시하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하고 있습니다.
- ③ 위탁업무의 내용이나 수탁자가 변경될 경우에는 지체없이 본 개인정보 처리방침을 통하여 공개하도록 하겠습니다.

■ 개인정보의 파기

- ① <공공기관명>은(는) 개인정보 보유기간의 경과, 처리목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체없이 해당 개인정보를 파기합니다.
- ② 정보주체로부터 동의받은 개인정보 보유기간이 경과하거나 처리목적이 달성되었음에도

불구하고 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우에는, 해당 개인정보(또는 개인정보파일)를 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존합니다.

③ 개인정보 파기의 절차 및 방법은 다음과 같습니다.

1. 파기절차

〈공공기관명〉은(는) 파기하여야 하는 개인정보(또는 개인정보파일)에 대해 개인정보 파기계획을 수립하여 파기합니다. 〈공공기관명〉은(는) 파기 사유가 발생한 개인정보(또는 개인정보파일)를 선정하고, 〈공공기관명〉의 개인정보 보호책임자의 승인을 받아 개인정보(또는 개인정보파일)를 파기합니다.

2. 파기방법

〈공공기관명〉은(는) 전자적 파일 형태로 기록·저장된 개인정보는 기록을 재생할 수 없도록 파기하며, 종이 문서에 기록·저장된 개인정보는 분쇄기로 분쇄하거나 소각하여 파기합니다.

■ 정보주체와 법정대리인의 권리·의무 및 행사방법

① 정보주체는 〈공공기관명〉에 대해 언제든지 개인정보 열람·정정·삭제·처리정지 요구 등의 권리를 행사할 수 있습니다.

※ 만 14세 미만 아동에 관한 개인정보의 열람등 요구는 법정대리인이 직접 해야 하며, 만 14세 이상의 미성년자인 정보주체는 정보주체의 개인정보에 관하여 미성년자 본인이 권리를 행사하거나 법정대리인을 통하여 권리를 행사할 수도 있습니다.

② 권리 행사는 〈공공기관명〉에 대해 「개인정보 보호법」 시행령 제41조 제1항에 따라 서면, 전자우편, 모사전송(FAX) 등을 통하여 하실 수 있으며, 〈공공기관명〉은(는) 이에 대해 지체없이 조치하겠습니다.

③ 권리 행사는 정보주체의 법정대리인이나 위임을 받은 자 등 대리인을 통하여 하실 수도 있습니다. 이 경우 “개인정보 처리 방법에 관한 고시(제2020-7호)” 별지 제11호 서식에 따른 위임장을 제출하셔야 합니다.

④ 개인정보 열람 및 처리정지 요구는 「개인정보 보호법」 제35조 제4항, 제37조 제2항에 의하여 정보주체의 권리가 제한 될 수 있습니다.

⑤ 개인정보의 정정 및 삭제 요구는 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없습니다.

⑥ 〈공공기관명〉은(는) 정보주체 권리에 따른 열람의 요구, 정정·삭제의 요구, 처리정지의 요구 시 열람 등 요구를 한 자가 본인이거나 정당한 대리인인지를 확인합니다.

■ 개인정보의 안전성 확보조치

〈공공기관명〉은(는) 개인정보의 안전성 확보를 위해 다음과 같은 조치를 취하고 있습니다.

1. 관리적 조치 : 내부관리계획 수립·시행, 정기적 직원 교육
2. 기술적 조치 : 개인정보처리시스템 등의 접근권한 관리, 접근통제시스템 설치, 고유식별정보 등의 암호화, 보안프로그램 설치
3. 물리적 조치 : 전산실, 자료보관실 등의 접근통제

〈공공기관명〉은(는) 개인정보의 안전성을 확보하기 위하여 법령에서 규정하고 있는 사항 이외에도 다음과 같은 활동을 시행하고 있습니다.

1. 개인정보보호 활동: 개인정보보호 관련 블로그·유튜브 운영, 투명성 보고서 발간(연 1회), 공동규제 및 자율규약 참여 현황, 자율규제단체 활동
2. 국내외 개인정보보호 인증 획득: ISO/IEC 27701, ISMS-P

■ 개인정보 자동 수집 장치의 설치·운영 및 거부에 관한 사항

① 〈공공기관명〉은(는) 이용자에게 개별적인 맞춤서비스를 제공하기 위해 이용 정보를 저장하고 수시로 불러오는 '쿠키(cookie)'를 사용합니다.

② 쿠키는 웹사이트를 운영하는데 이용되는 서버(http)가 이용자의 컴퓨터 브라우저에게 보내는 소량의 정보이며 이용자들의 PC 컴퓨터내의 하드디스크에 저장되기도 합니다.

가. 쿠키의 사용목적 : 이용자가 방문한 각 서비스와 웹 사이트들에 대한 방문 및 이용형태, 인기 검색어, 보안접속 여부 등을 파악하여 이용자에게 최적화된 정보 제공을 위해 사용됩니다.

나. 쿠키의 설치·운영 및 거부 : 웹브라우저 상단의 도구>인터넷 옵션>개인정보 메뉴의 옵션 설정을 통해 쿠키 저장을 거부 할 수 있습니다.

다. 쿠키 저장을 거부할 경우 맞춤형 서비스 이용에 어려움이 발생할 수 있습니다.

■ 가명정보의 처리

〈공공기관명〉은(는) 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 수집한 개인정보를 특정 개인을 알아볼 수 없도록 가명처리하여 다음과 같이 처리하고 있습니다.

▶ 가명정보의 처리에 관한 사항

구분	처리 목적	처리항목	보유 및 이용기간
△△△ 연구	연령대별 △△ 분석	휴대전화번호, △△일시, △△유형	결합데이터 분석 완료시까지

▶ 가명정보의 제3자 제공에 관한 사항(해당되는 경우에만 작성)

제공받는 자	제공받는 자의 이용 목적	제공하는 항목	제공받는 자의 보유 및 이용기간
제공받는 자의 법인명 또는 명칭	연령대별 △△ 분석	휴대전화번호, △△일시, △△유형	○○년 ○월까지

▶ 가명정보 처리의 위탁에 관한 사항(해당되는 경우에만 작성)

위탁받는 자(수탁자)	위탁업무	보유 및 이용기간
제공받는 자의 법인명 또는 명칭	연령대별 △△ 분석	○○년 ○월까지

▶ 법 제28조의4(가명정보에 대한 안전조치 의무 등)에 따른 가명정보의 안전성 확보조치에 관한 사항

- 관리적 조치 : 내부관리계획 수립·시행, 정기적 직원 교육
- 기술적 조치 : 개인정보처리시스템 등의 접근권한 관리, 접근통제시스템 설치, 고유식별정보 등의 암호화, 보안프로그램 설치
- 물리적 조치 : 전산실, 자료보관실 등의 접근통제

■ 개인정보 보호책임자

- ① <공공기관명>은(는) 개인정보 처리에 관한 업무를 총괄해서 책임지고, 개인정보 처리와 관련한 정보주체의 불만처리 및 피해구제 등을 위하여 아래와 같이 개인정보 보호책임자를 지정하고 있습니다.

▶ 개인정보 보호책임자

성명 : ○○○

직책 : ○○○ 실장

직급 : 3급

연락처 : <전화번호>, <이메일>, <팩스번호>

※ 개인정보보호 담당부서로 연결됩니다.

▶ 개인정보보호 담당부서

부서명 : ○○○ 팀

담당자 : ○○○

연락처 : <전화번호>, <이메일>, <팩스번호>

- ② 정보주체는 <공공기관명>의 서비스(또는 사업)를 이용하시면서 발생한 모든 개인정보보호 관련 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자 및 담당부서로 문의할 수 있습니다. <공공기관명>은(는) 정보주체의 문의에 대해 지체없이 답변 및 처리해드릴 것입니다.

■ 개인정보 열람청구

정보주체는 「개인정보 보호법」 제35조에 따른 개인정보의 열람 청구를 아래의 부서에 할 수 있습니다.

〈공공기관명〉은(는) 정보주체의 개인정보 열람청구가 신속하게 처리되도록 노력하겠습니다.

• 개인정보 열람청구 접수·처리 부서

부서명 : ○○○

담당자 : ○○○

연락처 : 〈전화번호〉, 〈이메일〉, 〈팩스번호〉

■ 권익침해 구제방법

정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청할 수 있습니다. 이 밖에 기타 개인정보침해의 신고, 상담에 대하여는 아래의 기관에 문의하시기 바랍니다.

1. 개인정보분쟁조정위원회 : (국번없이) 1833-6972 (www.kopico.go.kr)
2. 개인정보침해신고센터 : (국번없이) 118 (privacy.kisa.or.kr)
3. 대검찰청 : (국번없이) 1301 (www.spo.go.kr)
4. 경찰청 : (국번없이) 182 (ecrm.cyber.go.kr)

「개인정보 보호법」 제35조(개인정보의 열람), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등)의 규정에 의한 요구에 대 하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판법이 정하는 바에 따라 행정심판을 청구할 수 있습니다.

- 중앙행정심판위원회 : (국번없이) 110 (www.simpan.go.kr)

■ 개인정보 관리수준진단 결과

- ① 〈공공기관명〉은 정보주체의 개인정보를 안전하게 관리하기 위해 「개인정보 보호법」 제11조에 따라 매년 개인정보보호위원회에서 실시하는 “공공기관 개인정보 관리수준진단”을 받고 있습니다.
- ② 〈공공기관명〉은 ‘20XX년도 개인정보 관리수준진단 평가에서 ‘양호’ 등급을 획득하였습니다.
- ③ 〈공공기관명〉은 20XX년도 개인정보 관리수준진단 결과에 따라 다음과 같이 개선 조치하였습니다.
 - (예시) 개인정보처리시스템 웹 취약점 점검 실시 또는 방화벽 구축
 - (예시) 개인정보보호 조례 제정 등

■ 영상정보처리기기 설치·운영

① <공공기관명>은(는) 아래와 같이 영상정보처리기기를 설치·운영하고 있습니다.

1. 영상정보처리기기 설치근거·목적 : <공공기관명>의 시설안전, 화재예방
2. 설치 대수, 설치 위치, 촬영 범위 : 사옥 로비·전시실 등 주요시설물에 00대 설치, 촬영범위는 주요시설물의 전 공간을 촬영
3. 관리책임자, 담당부서 및 영상정보에 대한 접근권한자 : 0000 팀 0000 과장
4. 영상정보 촬영시간, 보관기간, 보관장소, 처리방법
 - 촬영시간 : 24시간 촬영
 - 보관기간 : 촬영 시부터 30일
 - 보관장소 및 처리방법 : 0000팀 영상정보처리기기 통제실에 보관, 처리
5. 영상정보 확인 방법 및 장소 : 관리책임자에게 요구 (0000팀)
6. 정보주체의 영상정보 열람 등 요구에 대한 조치 : 개인영상정보 열람·존재 확인 청구서로 신청하여야 하며, 정보주체 자신이 촬영된 경우 또는 명백히 정보주체의 생명·신체·재산의 이익을 위해 필요한 경우에 한해 열람을 허용함
7. 영상정보 보호를 위한 기술적·관리적·물리적 조치 : 내부관리계획 수립, 접근통제 및 접근권한 제한, 영상정보의 안전한 저장·전송기술 적용, 처리기록 보관 및 위·변조 방지조치, 보관시설 마련 및 잠금장치 설치
8. 영상정보처리기기 설치 및 관리 등의 위탁에 관한 사항
 <공공기관명>은(는) 아래와 같이 영상정보처리기기 설치 및 관리 등을 위탁하고 있으며, 관계 법령에 따라 위탁계약 시 개인정보가 안전하게 관리될 수 있도록 필요한 사항을 규정하고 있습니다.

기관명/부서	수탁업체	담당자	연락처
000	000	000	000

9. 영상정보처리기기 운영·관리 방침의 변경에 관한 사항
 이 영상정보처리기기 운영·관리 방침은 0000년 0월 0일에 제정되었으며, 법령·정책 또는 보안기술의 변경에 따라 내용의 추가·삭제 및 수정이 있을 시에는 지체 없이 본 기관 홈페이지를 통해 변경사유 및 내용을 공지하도록 하겠습니다.

■ 개인정보 처리방침의 변경

- ① 이 개인정보 처리방침은 20XX. X. X부터 적용됩니다.
- ② 이전의 개인정보 처리방침은 아래에서 확인하실 수 있습니다.
 - 20XX. X. X ~ 20XX. X. X 적용 (클릭)
 - 20XX. X. X ~ 20XX. X. X 적용 (클릭)
 - 20XX. X. X ~ 20XX. X. X 적용 (클릭)

동의획득 예시

1. 개인정보 수집·이용 동의서 Check-List

개인정보 수집·이용 동의서 Check-List	Y	N
① 처리하고자 하는 업무에 반드시 필요한 최소한의 개인정보인가요?	●	
② 정보주체의 동의가 필요한가요? 정보주체의 동의가 필요하지 않은 경우 인지 확인하였나요? <<동의 없이 개인정보 수집 이용이 가능한 경우(보호법 제 15조)>> 1. 법률에 특별한 규정이 있거나 법령상 의무 준수를 위해 불가피한 경우 2. 공공기관이 법령 등에서 정하는 소관업무 수행을 위해 불가피한 경우 3. 정보주체와의 계약의 체결 및 이행을 위해 불가피하게 필요한 경우 4. 정보주체 또는 법정대리인이 의사표시를 질 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체해 또는 3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 5. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한함 <<동의 없이 제3자 제공에 가능한 경우(보호법 제 17조)>> 1. 법률에 특별한 규정이 있거나 법령상 의무 준수를 위해 불가피한 경우 2. 공공기관이 법령 등에서 정하는 소관업무 수행을 위해 불가피한 경우 3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 ※ 국외 제3자에게 제공 시에는 정보주체의 동의 필요 <<동의 없이 수집 목적 외로 개인정보를 이용하거나 제3자 제공이 가능한 경우(보호법 제 13조)>> 1. 다른 법률에 특별한 규정이 있는 경우 2. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 3. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우 4. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국내 기구에 제공하기 위하여 필요한 경우 5. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우 6. 법원의 재판업무 수행을 위하여 필요한 경우 7. 형(形) 및 감호, 보호처분의 집성을 위하여 필요한 경우	●	

▶ 개인정보 처리 위탁의 경우, 위탁사실, 위탁하는 업무의 내용, 수탁자 등을 홈페이지 등에 게시		
▶ 정보주체의 동의 없이 개인정보를 처리하는 경우에는 처리 근거를 작성하여 안내		
<p>③ 동의서의 목적과 내용을 쉽게 이해할 수 있도록 동의서 제목을 작성하였나요? 수집·이용과 함께 제3자 제공도 하려는 경우에 이데 대한 사실도 제목에 기재하였나요?</p> <p>※ 예시) ○○이벤트를 위한 개인정보 수집 이용 동의서, ○○회원 가입을 위한 개인정보 수집 이용 및 제3자 제공 동의서</p>	●	
<p>④ 처리하려는 개인정보의 항목, 목적, 처리내용, 이용 및 보유기간 등의 내용을 작성하였나요?</p> <p>i) 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게</p> <p>ii) 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시</p> <p>iii) 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시</p> <p style="text-align: center;"><<동의서의 중요한 사항></p> <p>1. 개인정보의 수집 이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실</p> <p>2. 처리하려는 개인정보 항목 중 민감정보, 고유식별정보(여권번호, 운전면허번호 및 외국인등록번호)</p> <p>3. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간)</p> <p>4. 개인정보를 제공받는 자와 제공받는 자의 개인정보 이용 목적</p>	●	
<p>⑤ 민감정보, 고유식별정보 처리에 대한 동의 여부를 확인하였나요?</p> <p>• 민감정보나 고유식별정보를 처리하기 위하여 정보주체의 동의가 필요한 경우, 동의서를 별도로 작성하여야 함</p> <p>※ 법령의 근거 등으로 동의가 불필요한 경우, 그 내용을 안내하는 것이 바람직함</p> <p>• 민감정보나 고유식별정보 처리의 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익 내용을 기재</p> <p>※ 주민등록번호는 반드시 법령의 근거에 따라 수집 가능(정보주체의 동의로 수집 불가)</p>	●	
<p>⑥ 개인정보 처리 주체를 기재하였나요? 정보주체의 동의의사를 확인하였나요?</p> <p>• 동의서 하단에는 개인정보 처리 주체를 명시</p> <p>• 동의의사를 서명이나 날인 등으로 확인</p> <p>• 정보주체가 만 14세 미만의 아동이라면 법정대리인의 동의 확인</p>	●	
<p>⑦ 동의 거부권 및 동의 거부에 따른 불이익을 안내하였나요?</p> <p>• 개인정보 처리에 관한 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익 내용을 기재</p> <p>※ 예시) 위 개인정보 수집 이용 동의를 거부할 권리가 있습니다. 동의를 거부하는 경우 동의 시에 제공하는 00서비스를 제공받을 수 없습니다.</p>	●	

2. 정보주체의 동의를 얻어 개인정보를 수집·이용하는 경우

[개인정보의 수집·이용 목적]

ㅇㅇㅇ대학교 ○○○은 다음과 같은 이유로 귀하의 개인정보를 수집·이용합니다.
아래의 개인정보 수집·이용에 대한 내용을 자세히 읽어 보신 후 동의 여부를 결정하여 주시기 바랍니다.

1. ○○○ 인터넷 홈페이지 회원관리

- 회원제 서비스 이용 및 제한적 본인 확인제에 따른 본인확인
- 불량회원의 부정 이용방지와 비인가 사용방지
- 가입의사 확인, 가입 및 가입횟수 제한
- 분쟁 조정을 위한 기록보존, 불만처리 등 민원처리, 고지사항 전달

2. ○○○을 위한 ○○○

[수집하는 개인정보의 항목]

1. 성명, 생년월일, 성별, 아이디, 비밀번호, 연락처(이메일, 휴대전화 중 택일)
2. ○○○에 관한 정보

[자동 수집하는 개인정보의 항목]

ㅇㅇㅇ대학교 ○○○은 귀하의 동의를 얻어 개인정보를 수집하는 과정에서, 다음과 같은 개인정보의 경우 ○○○를 위한 목적으로 귀하의 동의없이 수집·이용할 수 있습니다.

1. ○○○에 관한 법률에 근거한 ○○○에 관한 정보
2. ○○○에 근거한 ○○○에 관한 정보

[개인정보의 보유 및 이용기간]

귀하의 개인정보는 원칙적으로 개인정보의 수집 및 이용목적이 달성되면 지체없이 파기합니다. 단, 다음의 정보에 대해서는 아래의 이유로 명시한 기간 동안 보존합니다.

1. ㅇㅇㅇ대학교 ○○○의 내부 방침에 의한 정보보유 사유

- 부정이용기록
보존 이유 : 부정 이용 방지

보존 기간 : ○년

2. 관련법령에 의한 정보보유 사유

- ○○○에 관한 법률 등 관계법령의 규정에 의하여 보존할 필요가 있는 경우 관계 법령에서 정한 일정한 기간 동안 회원정보를 보관합니다.
- ○○○에 관한 기록
보존 근거 : ○○○에 관한 법률

보존 기간 : ○년

[개인정보 수집·이용에 대한 동의를 거부할 권리]

귀하가 ○○○대학교 ○○○에 이상의 정보를 제공하기 원하지 않을 경우 귀하는 개인 정보의 수집·이용에 대한 동의를 거부할 수 있으며, 미동의로 인해 어떠한 불이익도 발생하지 않습니다. (미동의를 ○○○상의 불이익이 발생할 수 있습니다.)

개인정보의 수집 및 이용목적에 동의하십니까? ☐ 동의함 ☐ 동의하지 않음

3. 정보주체의 동의를 얻어 개인정보를 제3자에게 제공하는 경우

[개인정보를 제공받는 자]

○○○대학교 ○○○은 수집한 귀하의 개인정보를 다음과 같은 자에게 제공합니다. 아래의 개인정보에 대한 내용을 자세히 읽어 보신 후 동의 여부를 결정하여 주시기 바랍니다.

1. ○○○에 관한 법률 제○조에 의한 ○○○기관

2. 주식회사 ○○○

[개인정보를 제공받는 자의 개인정보 이용 목적]

1. ○○○에 관한 서비스

2. ○○○에 관한 업무

[제공하는 개인정보의 항목]

1. ○○○에 관한 정보
2. ○○○에 관한 정보

[자동 제공하는 개인정보의 항목]

○○○대학교 ○○○은 귀하의 동의를 얻어 개인정보를 ○○○에 제공하는 과정에서, 다음과 같은 개인정보의 경우 ○○○를 위한 목적으로 귀하의 동의없이 제공할 수 있습니다.

1. ○○○에 관한 법률에 근거한 ○○○에 관한 정보
2. ○○○에 근거한 ○○○에 관한 정보

[개인정보를 제공받는 자의 개인정보 보유 및 이용기간]

○○○○에 제공된 귀하의 개인정보는 원칙적으로 개인정보의 수집 및 이용목적이 달성되면 지체없이 파기합니다. 단, 다음의 정보에 대해서는 아래의 이유로 명시한 기간 동안 보존합니다.

1. ○○○의 내부 방침에 의한 정보보유 사유

- ○○○○에 관한 정보

보존 이유 : ○○○○

보존 기간 : ○년

[개인정보의 제공 대한 동의를 거부할 권리]

귀하가 ○○○○에 이상의 정보를 제공하기 원하지 않을 경우 귀하는 개인정보의 제공에 대한 동의를 거부할 수 있으며, 미동의로 인해 어떠한 불이익도 발생하지 않습니다. (미동의를 ○○○○상의 불이익이 발생할 수 있습니다.)

개인정보의 제공목적에 동의하십니까?

☐ 동의함

☐ 동의하지 않음

4. 정보주체의 동의를 얻어 고유식별정보를 수집·이용하는 경우

[고유식별정보의 수집·이용 목적]

○○○대학교 ○○○○은 다음과 같은 이유로 귀하의 고유식별정보를 수집·이용합니다. 아래의 개인정보 수집·이용에 대한 내용을 자세히 읽어 보신 후 동의 여부를 결정하여 주시기 바랍니다.

1. ○○○○ 인터넷 홈페이지 회원관리

- 회원제 서비스 이용 및 제한적 본인 확인제에 따른 본인확인
- 불량회원의 부정 이용방지와 비인가 사용방지
- 가입의사 확인, 가입 및 가입횟수 제한

2. ○○○○을 위한 ○○○○

[수집하는 고유식별정보의 항목]

1. ○○○○의 경우 : 운전면허번호, 여권번호 중 하나

※ 고유식별정보 : 여권번호, 운전면허번호, 외국인등록번호

[고유식별정보의 보유 및 이용기간]

귀하의 고유식별정보는 원칙적으로 고유식별정보의 수집 및 이용목적이 달성되면 지체 없이 파기합니다. 단, 다음의 정보에 대해서는 아래의 이유로 명시한 기간 동안 보존합니다.

1. ○○○○대학교 ○○○○의 내부 방침에 의한 정보보유 사유

- ○○○○번호

보존 이유 : 부정 이용 방지

보존 기간 : ○년

2. 관련법령에 의한 정보보유 사유

- ○○○에 관한 법률 등 관계법령의 규정에 의하여 보존할 필요가 있는 경우 관계 법령에서 정한 일정한 기간 동안 회원정보를 보관합니다.

- ○○○번호

보존 근거 : ○○○에 관한 법률

보존 기간 : ○년

[고유식별정보의 제공 대한 동의를 거부할 권리]

귀하가 ○○○대학교 ○○○에 이상의 고유식별정보를 제공하기 원하지 않을 경우 귀하는 고유식별정보의 수집·이용에 대한 동의를 거부할 수 있으며, 미동의로 인해 어떠한 불이익도 발생하지 않습니다. (미동의를 ○○○상의 불이익이 발생할 수 있습니다.)

고유식별정보의 수집·이용목적에 동의하십니까? ☐ 동의함 ☐ 동의하지 않음

만 14세 미만 아동의 개인정보 수집 예시

[인터넷 홈페이지를 통한 회원가입의 경우]

Step 1. 어린이 회원 가입(선택)

일반회원 (만 14세 이상의 개인회원) >> 가입하기	어린이 회원 (만 14세 미만 개인회원) >> 가입하기
---	--

Step 2. 보호자 인증

만 14세 미만 아동은 회원 가입 시 보호자(법정대리인)의 동의가 있어야 가능합니다. 회원가입시에는 보호자가 함께 해 주시기 바라며, 보호자는 아래 인증수단 중 하나를 선택해 주시기 바랍니다.

<휴대폰 인증> 보호자 명의의 휴대폰으로 인증하실 수 있습니다. >> 인증하기	<i-PIN 인증> 보호자의 아이핀(i-PIN)으로 인증하실 수 있습니다. >> 인증하기	<신용카드> 보호자 명의의 신용카드로 인증하실 수 있습니다. >> 인증하기
--	--	--

Step 3. 만 14세 미만 아동의 개인정보의 수집·이용에 대한 보호자의 동의

표준 개인정보처리위탁 계약서(안)

본 표준 개인정보처리위탁 계약서는 「개인정보 보호법」 제26조제1항에 따라 위탁 계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 최소한의 사항을 표준적으로 제시한 것으로서, 위탁계약이나 위탁업무의 내용 등에 따라 세부적인 내용은 달라질 수 있습니다.

개인정보처리업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

2024년부터 개정된 개인정보 보호법으로 인하여 재위탁이 발생 할 경우 반드시 위탁자에게 동의 받은 후 재위탁을 할 수 있습니다.

표준 개인정보처리위탁 계약서(안)

○○○(이하 “위탁자”이라 한다)과 △△△(이하 “수탁자”이라 한다)는 “위탁자”의 개인정보 처리업무를 “수탁자”에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 “위탁자”가 개인정보처리업무를 “수탁자”에게 위탁하고, “수탁자”는 이를 승낙하여 “수탁자”의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는 「개인정보 보호법」, 같은 법 시행령 및 고시, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2023-6호) 및 「표준 개인정보 보호지침」(개인정보보호위원회 고시 제2024-1호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) “수탁자”는 계약이 정하는 바에 따라 () 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.¹⁾

- 1.
- 2.
- 3.

제4조 (위탁업무 기간) 이 계약서에 의한 개인정보 처리업무를 기간은 다음과 같다.
계약 기간 : 년 월 일 ~ 년 월 일

1) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

제5조 (재위탁 제한) ① “수탁자”는 “위탁자”의 사전 승낙을 얻은 경우를 제외하고 “위탁자”와의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② “수탁자”가 다른 제3의 회사와 수탁계약을 할 경우에는 “수탁자”는 해당 사실을 “위탁자”에게 동의를 받아야 한다.

제6조 (개인정보의 안전성 확보조치) “수탁자”는 「개인정보 보호법」 제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2023-6호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제7조 (개인정보의 처리제한) ① “수탁자”는 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② “수탁자”는 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법」 시행령 제16조 및 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2023-6호)에 따라 즉시 파기하거나 “위탁자”에게 반납하여야 한다.

③ 제2항에 따라 “수탁자”가 개인정보를 파기한 경우 지체없이 “위탁자”에게 그 결과를 통보하여야 한다.

제8조 (수탁자에 대한 관리·감독 등) ① “위탁자”는 “수탁자”에 대하여 다음 각 호의 사항을 감독할 수 있으며, “수탁자”는 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② “위탁자”는 “수탁자”에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, “수탁자”는 특별한 사유가 없는 한 이행하여야 한다.

③ “위탁자”는 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 ()회 “수탁자”를 교육할 수 있으며, “수탁자”는 이에 응하여야 한다.2)

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 “위탁자”는 “수탁자”와 협의하여 시행한다.

2) 「개인정보 안전성 확보조치 기준 고시」(개인정보보호위원회 고시 제2023-6호) 및 「개인정보 보호법」 제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

제9조 (정보주체 권리보장) ① “수탁자”는 정보주체의 개인정보 열람, 정정·삭제, 처리
정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제10조 (개인정보의 파기) ① “수탁자”는 제4조의 위탁업무기간이 종료되면 특별한 사
유가 없는 한 지체 없이 개인정보를 파기하고 이를 “위탁자”에게 확인받아야 한다.

제11조 (손해배상) ① “수탁자” 또는 “수탁자”의 임직원 기타 “수탁자”의 수탁자가 이
계약에 의하여 위탁 또는 재위탁 받은 업무를 수행함에 있어 이 계약에 따른 의무를
위반하거나 “수탁자” 또는 “수탁자”의 임직원 기타 “수탁자”의 수탁자의 귀책사유로
인하여 이 계약이 해지되어 “위탁자” 또는 개인정보주체 기타 제3자에게 손해가 발
생한 경우 “수탁자”는 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 “위탁자”가
전부 또는 일부를 배상한 때에는 “위탁자”는 이를 “수탁자”에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “위탁자”와 “수탁자”가
서명 또는 날인한 후 각 1부씩 보관한다.

20 . . .

위탁자

주 소 :

기관(회사)명 :

대표자 성명 : (인)

수탁자

주 소 :

기관(회사)명 :

대표자 성명 : (인)

개인정보 처리(등록, 파기 포함) 요구 절차

□ 개인정보 열람, 정정, 삭제, 처리정지 절차



※ 개인정보보호 포털(www.privacy.go.kr)을 통해서도 요구 가능

□ 개인정보파일 등록·변경등록 절차

1. 담당자별 역할(법 제32조, 영 제33조~제34조, 개인정보 처리 방법에 관한
고시 제3조, 표준지침 제51조~제57조)

구분	역할	처리 담당자
개인정보 보호책임자	- 개인정보파일 등록·변경등록 신청	정보보호본부장
교육부 장관	- 개인정보파일 경유·예비검토	소속·산하기관 ->교육부
개인정보보호위원회	- 개인정보파일 공개	-

2. 개인정보파일 등록·변경등록 절차

구분	내용	담당자	비고
1	등록·변경등록신청서 작성 및 제출 (별지1호 참조, 내부결재)	개인정보보호 분야별 담당자 개인정보보호 분야별 책임자	개인정보보호 담당자(순차협조)
2	등록요청 승인·반려 처리	개인정보 보호책임자	
3	승인시 개인정보보호위원회 등록 처리	개인정보 보호책임자	https://intra. privacy.go.kr
4	개인정보파일 공개	개인정보보호위원회	

□ 개인정보파일 파기 절차

1. 담당자별 역할(법 제31조, 영 제32조, 표준지침 제22조, 제55조~56조)

구분	역할	담당자
개인정보 보호책임자	- 개인정보파일 등록·파기 승인, 관리 감독 - 파기 시, 보호위원회에 사실 통보	정보보호본부장
개인정보보호 분야별 책임자	- 개인정보파일 지정·관리·보호·파기 - 공개 대상 개인정보파일 등록·공개 - 공개 대상 개인정보파일 처리방침 수립·시행 및 공개	본부별 부서장
원내 개인정보 보호담당자	- 개인정보파일 등록·파기 지도 검사	개인정보보호담당자
개인정보취급자	- 파기 수행 후 개인정보 보호책임자에게 등록 사실 삭제요청	시스템별 취급담당자

2. 개인정보파일 파기(법 제21조, 영 제16조, 표준지침 제11조, 제55조, 제56조)

○ 파기절차

구분	내용	담당자	비고
1	파기요청서 작성 및 제출 (별지4호 참조, 내부결재)	개인정보취급자	
2	파기요청 지도 검사	개인정보 보호담당자	순차협조
3	파기검토 및 승인·반려 처리	개인정보보호 분야별 책임자 개인정보 보호책임자	
4	승인시, 개인정보 파일 파기 실시 (접속로그 기록 확인)	개인정보취급자	
5	개인정보파일 파기결과 보고(협조전)	개인정보보호 분야별 책임자	
6	개인정보파일 파기결과 등록	개인정보보호 분야별 담당자	https://intra.privacy.go.kr
7	공개된 개인정보파일 등록 삭제	개인정보 보호책임자	등록내역 확인 후
8	파기결과 보고	개인정보 보호책임자	교육부 보고

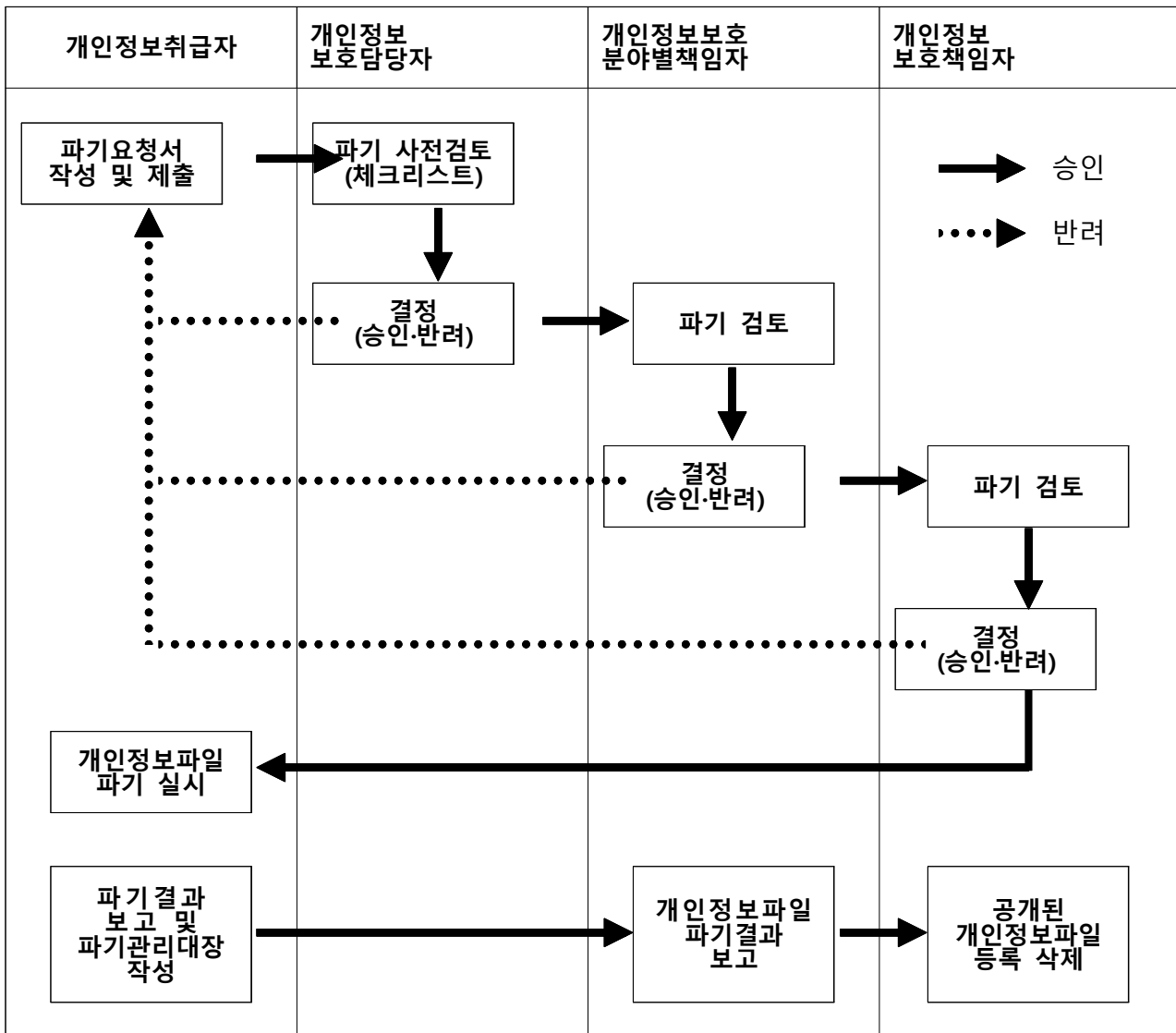
※ 개인정보파일 등록·삭제 뿐 만 아니라 일부 파기(변경등록) 일 경우에도 동일하게 교육부에 보고

※ 교육부에 보고 시 개인정보보호 분야별 담당자가 직접 개인정보보호위원회 개인정보보호 종합지원 시스템(<https://intra.privacy.go.kr>)을 통해 등록하면 개인정보 보호책임자가 승인 후 교육부 보고

※ 개인정보 보유목적 달성 및 보유기간이 지난 경우 (자동으로) 일부 파기가 가능하며, 이 경우 개인정보보호 분야별 책임자는 시스템(반드시 별지4호 서식 항목 모두 포함) 또는 파기관리 대장에 그 결과를 등록하여 관리한다.

※ 개인정보를 (자동으로) 일부 파기를 하는 경우, 연간 파기계획을 수립(파기방법, 파기절차 등)하여 파기에 관한 사항은 기록 관리 하여야 한다.

○ 개인정보파일 파기절차 흐름도



○ 파기 사전검토 체크리스트

구분	내용	확인(Y/N)
필수	1. 파기 요청서의 내용과 공개된 개인정보파일 등록된 내용이 동일한가?(개인정보파일명, 보관건수)	
	2. 파기사유가 구체적으로 작성되어있는가?	
	3. 파기일정이 명확하게 지정되어있는가?	
	4. 파기하지 않고 보존해야 하는 파일에 대한 법적 근거가 명시되어 있는가?	
	5. 개인보관 자료(PC)와 서버자료의 유무를 취급자에게 확인하였는가?	
	6. 파기장소와 방법이 명확한가?	
	7. 파기 수행자와 입회자가 지정되어 있는가?	
	8. 폐기 확인 방법이 명시되어 있는가?	
	9. 백업 조치에 대한 사유가 명시되어 있는가?	
	10. 매체 폐기를 하지 않을 경우, 사유가 상세히 기술되어 있는가?	
선택	※ 민원처리 관련 개인정보파일이 있는가? (있는 경우 10년간 보관해야 함)	

개인정보 목적 외 이용 및 제3자 제공 절차서

□ 기본 원칙 및 제공 기준

1. 기본 원칙

구분	역할
자료제공 판단 기준	<ul style="list-style-type: none"> - 목적의 정당성 : 구체적으로 어떠한 목적을 위하여 당해 개인정보가 필요한지? - 수단의 적정성 : 개인정보를 제공함으로써 공익목적 달성을 할 수 있는 것인지? - 피해의 최소화 : 목적달성을 위하여 필요한 최소한의 정보는 어디까지인지? - 법익의 균형성 : 제공에 따른 이익과 정보주체가 받을 수 있는 예상피해를 비교하여 전자가 우월하다고 할 수 있는지 여부 판단 <p>☞ 목적의 정당성, 수단의 적정성, 피해의 최소화, 법익의 균형성에 대하여 종합적으로 검토한 후 필요한 최소한의 범위 내에서 제공</p>
적격 여부 확인	<ul style="list-style-type: none"> - 요청 기관의 개별법에 자료요청의 근거조항이 구체적으로 명시된 경우 제공 가능 - 요청 기관의 개별법에 자료요청 근거법이 없는 경우 정보주체의 동의가 있었는지 여부 등 예외적 제공가능 사항에 해당되는지 확인한 후 제공 여부 결정
제공항목 판단	<ul style="list-style-type: none"> - ○○○대학교가 직접 수집·생산한 정보가 아닌 경우 자료제공 불가 ※단, 정보주체의 별도 동의가 있는 경우 제공 가능 - 요청 목적에 부합하는 최소 항목만 제공(개인정보 최소 제공 원칙) - 고유식별정보 및 민감정보는 법령(법률, 시행령, 고시)에 고유식별정보 및 민감정보의 처리를 요구(허용)하도록 규정되어 있는 경우만 제공

2. 개인정보의 제공기준

구분	역할
수집목적 범위 내 (개인정보보호법 제17조)	<ul style="list-style-type: none"> - 정보주체의 동의를 받은 경우 - 법 제15조제1항 제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우
수집목적 이외 용도 (개인정보보호법 제18조)	<ul style="list-style-type: none"> - 정보주체로부터 별도의 동의를 받은 경우 - 다른 법률에 특별한 규정이 있는 경우 - 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소 불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 - 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우 - 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 - 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우 - 법원의 재판업무 수행을 위하여 필요한 경우 - 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

□ 업무처리 기준

1. 목적 외 이용 및 제3자 제공 절차

절 차	주요내용	비고
1	법적근거 검토 - 목적 외 이용·제3자 제공이 가능한 경우에 해당하는지 법적근거 검토	개인정보취급자 (담당 부서)
↓		
2	동의절차 이행 - 법적 근거가 없는 경우 정보주체로부터 별도의 동의를 받아야 함 ※ 동의서는 [내부관리계획-동의획득 예시]의 표준양식 참조	개인정보취급자 (담당 부서)
↓		
3	제공 승인 획득 - 개인정보 보호책임자로부터 목적 외 이용·제공 승인 절차 진행(내부결재) ※ 기관 개인정보 보호담당자(순차협조), 기관 개인정보 보호책임자(전결)	개인정보취급자 기관 개인정보 보호담당자 기관 개인정보 보호책임자
↓		
4	대장 기록·관리 - '개인정보의 목적 외 이용 및 제3자 제공 대장'을 기록·관리하여야 함 ※ 목적 외 이용·제공 대장은 [별지] 서식 참조	개인정보취급자 (담당 부서)
↓		
5	보호조치 요구 - 제3자 제공시에는 이용목적, 이용방법, 이용기간, 이용형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 조치("안전성 확보 조치" 참조)를 마련하도록 문서로 요청 ※ 공문 발송 시 관련 내용을 명시하여 발송	개인정보취급자 (담당 부서)
↓		
6	조치결과 제출 - 안전성 확보조치 요청을 받은 자는 그에 따른 조치를 취한 후, 그 결과를 개인정보를 제공한 ○○○대학교에게 문서로 알려야 함	제공받는 자 (제공받는 기관)
↓		
7	주요 내용 공개 - (정보주체의 동의가 없는 경우)30일 이내에 관보 또는 인터넷 홈페이지에 10일 이상 계속 게재 ※ 동의를 받았거나 수사 목적인 경우는 예외	개인정보취급자 (담당 부서)

2. 세부 업무 처리 기준

가. 요청절차의 적절성 확인

○ 문서접수 방법

- 개인정보 제공 요청은 요청 기관의 장으로부터 문서로 접수
- 문서는 전자문서 접수를 원칙으로 하되, 법원 문서 등 불가피한 경우는 예외
※ 우편 또는 팩스 등 오프라인으로 접수한 경우 원본서류 스캔하여 공문접수
- 제공요청 문서 접수 시 확인할 필수 사항
※ 요청하는 법률 근거, 요청 목적, 요청하는 개인정보 항목, 이용기간, 파기계획

○ 신청인 확인 방법

- 전자문서 : 신청인 확인 절차 생략
- 내 원 : 신분증 확인 및 요청 기관 근무여부 확인
- 팩스, 우편 등 : 담당자 신분증 사본 접수 및 요청 기관 근무 여부 확인

나. 자료제공 항목 판단

○ ○○○대학교가 수집한 정보여부 확인

- ○○○대학교가 직접 수집·생산한 정보에 한하여 제공
- ○○○대학교가 다른 기관(교육부, 교육청 등)으로부터 입수·활용하는 정보는 제공 불가

※ 단, 정보주체로부터 별도의 동의를 받았거나 다른 법률에 특별한 규정이 있는 경우에는 제공 가능

○ 요청 목적에 부합하는 최소 항목만 제공(개인정보 최소 제공의 원칙)

- 자료제공 요청 항목이 요청 목적과 부합하지 않거나 과도하다고 판단되는 경우 해당 항목은 제외하고 필요한 최소 범위 내 제공
- 자료요청 개별 근거법에서 제공 항목을 열거하고 있는 경우 해당 항목에 한해 제공

○ 다른 기관으로부터 위탁받은 업무인 경우 위탁받은 업무 범위를 초과하여 자료제공 불가

다. 자료제공 여부 및 범위 판단(법적근거 검토 및 동의절차 이행)

○ 정보주체의 동의를 받은 경우(법 제18조 제2항 제1호)

- 반드시 정보 주체의 동의를 받아야 하므로 배우자 등 가족의 개인정보까지 요청하는 경우 가족 개개인의 동의 여부 확인
- 제3자 제공에 대한 동의를 받아야 하는 시점에 특별한 제한은 없으나 최초 수집할 당시 제3자 제공에 대한 동의를 받는 경우에는 수집 · 이용에 대한 동의와 별도로 구분해서 동의를 받아야 함

< 제3자 제공에 따른 고지 및 동의(예시) >

제공받는 기관	제 공 목 적	제 공 하 는 항 목	보유기간
00군 부 대	현장체험학습장 출입자 신분확인	학생의 성명, 학년, 반, 전화번호	1년

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 원활한 현장체험학습에 제한을 받을 수 있습니다.

☐ 위와 같이 귀하의 개인정보를 제3자에게 제공하는 데 동의하십니까?

동의함	<input type="checkbox"/>	동의하지 않음	<input type="checkbox"/>
-----	--------------------------	---------	--------------------------

- 요청 기관이 정보주체의 동의를 받은 경우 요청 기관으로부터 동의서를 전수 제출받아 확인 후 제공
 - ※ 동의서에 기재된 자료제공 항목 범위 내에서 제공
- 정보주체의 동의를 받아 제공하는 경우 「개인정보 보호법」 제18조 제3항에 따른 의무사항 반드시 준수
 - ※ ○○○대학교에서 정보주체의 동의를 받아 제공하는 경우에는 정보주체에게 제공받는 자, 이용 목적, 이용 기간 등 법 제18조 제3항에 따른 필수 고지사항을 알려주어야 함
 - ※ 요청 기관에서 정보주체의 동의서를 받아 제공하는 경우 동의서에 법 제18조 제3항에 따른 필수 고지사항 기재 여부 반드시 확인 후 제공

< 법 제18조 제3항에 따른 필수 고지사항 >

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 내용

- 다른 법률에 특별한 규정이 있는 경우(법 제18조 제2항 제2호)
 - 요청 기관의 개별 법률을 근거로 자료제공 요청하는 경우
 - ※ 요청 기관의 예 : 국회, 감사원, 법원, 경찰청 등
 - 자료제공 근거법 유무 확인
 - ※ 요청 기관의 개별법에 이용기관, 이용목적, 이용하는 개인정보의 항목 등을 구체적으로 명시한 특별한 규정이 있는 경우 제공
 - ※ 개별법에 “법령상 의무이행”과 같이 포괄적으로 규정되어 있거나, 시행령, 시행규칙에만 규정이 있는 경우는 제공 불가(단, 법률에 위임근거가 있고, 이에 따라 시행령, 시행규칙에 관련 규정이 있으면 제공 가능)

- ※ 다른 법률의 특별한 규정에 해당된다는 보호위원회 질의회신 문서를 첨부하는 경우 요청 목적 등 확인 후 제공 가능
 - 요청 목적의 적정 여부 확인
 - ※ 개별 법령에서 정한 이용목적 및 요청항목과 요청 목적이 부합하지 않는 경우 제공 불가(개별 법령에 이용목적이 한정되어 있거나 제공항목을 열거 하고 있는 경우에는 해당 목적 및 항목에 한해 제공 가능)
 - 그 이외의 이유로 인한 제3자 제공 여부 판단(법 제18조 제2항 제3호부터 제9호까지)
 - 개인정보의 제공 목적, 내용, 형태, 관련 근거법 등을 고려하여 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없는지 여부 등을 종합적으로 판단하여 제공
 - 수사 등의 목적으로 개인정보 제공을 요청받은 경우에도 무조건 제공해야 하는 것은 아니므로 영장, 사건번호, 접수번호 등을 확인한 후 자료제공 여부를 판단
 - ※ 범죄의 형태와 경중, 정보주체가 받을 불이익의 정도 등을 제반사정을 종합적으로 고려하여 개인정보 이용이 없는 수사 목적을 달성할 수 없는 경우에 한하여 제한적으로 제공
- < 참고사항 >**

 1. 불특정 다수의 개인정보를 제공할 경우 정보주체, 또는 제3자의 권익(인권)이 부당하게 침해될 소지가 있음
 - ☞ 수사기관에서 영장을 제시하거나 법원에서 요청하는 경우에는 영장의 구속력에 따라 제공 가능하나 자료 요청기관과 협의하여 최소한의 범위로 자료 제공
 2. 수사, 공소제기 및 유지를 위한 경우의 예외 및 한계 필요성
 - ☞ 범죄수사 등을 위한 경우라 하더라도 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있는 경우에는 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공할 수 없음
- 법원의 문서제출명령서, 사실조회, 문서송부촉탁 등에 의해 정보 주체의 동의 없이 목적 외로 제공 가능

라. 자료제공 업무처리 기준

- 업무처리 절차 : 개인정보 보호책임자로부터 목적 외 이용 및 제3자 제공 승인 획득
- 자료제공 처리 기준
 - 개인정보 자료 제공은 부득이한 경우를 제외하고는 전자결재에 의한 문서 회신을 원칙으로 함(회신 문서에는 다음 사항을 반드시 기재)

- < 회신문서의 필수 기재사항 >**

 1. 이용목적, 이용방법, 이용기간, 이용형태의 제한사항
 2. 개인정보의 안전성 확보를 위해 필요한 구체적인 조치사항

- 자료제공 내역을 ‘개인정보의 목적 외 이용 및 제3자 제공 대장’ (별지 서식)에 반드시 기록 · 관리하고, 관련 시스템에 등록
 - ※ 제공 건수가 없는 경우라도 ‘목적 외 이용 및 제3자 제공 대장’ 관리
- 관련업무 처리 후 PC에 개인정보 자료가 저장된 경우 지체없이 삭제
- 자료제공 방법

- 전자결재 문서에 의한 전자통신망을 이용해 제공하는 경우
 - ※ 개인정보를 엑셀 등 첨부파일 형태로 제공하되, 반드시 암호화 조치하여 송부하고 암호는 유선 등의 방법으로 별도 통보(문서 본문에 개인정보 및 비밀번호를 표기하여 제공하는 것을 금지)
- 엑셀 등 문서 출력물에 의해 직접 전달하는 경우
 - ※ 자료 제공 시 요청 기관의 담당자 또는 직상급자에게 직접 전달
- 보조기억매체(USB, CD, 디스켓 등)를 이용하여 제공하는 경우
 - ※ 제공되는 개인정보 자료는 반드시 암호화 조치, 자료 전달 완료 후 반출된 보조기억매체에 저장된 자료는 즉시 삭제
 - ※ 보조기억매체(USB, CD, 디스켓 등) 반·출입 절차에 대해서는 매체제어시스템 등록 후 처리
- 기타의 방법에 의해 자료제공이 필요한 경우는 안전성 조치 등에 대해 개인정보 보호담당자와 협의를 거쳐 제공

○ 개인정보의 목적 외 이용 또는 제3자 제공의 공고

- 개인정보 자료를 목적 외의 용도로 외부기관 등에 제공한 부서는 제공한 날부터 30일 이내에 ○○○대학교 홈페이지 혹은 해당 서비스 홈페이지에 반드시 10일 이상 계속 게시
- ○○○대학교 홈페이지 내 공지사항 및 해당 서비스 홈페이지 공지사항 게시
 - ※ (필수 기재사항) 제공한 날짜, 법적 근거, 제공 목적, 제공한 개인 정보 항목
 - ※ 정보주체에 대한 고지의무 위반 시 5천만원 이하의 과태료(제75조 제2항 제1호)

< 개인정보의 목적 외 이용 또는 제3자 제공 공고(예시)>

『개인정보 보호법』 제18조(개인정보의 목적 외 이용·제공 제한) 및 『개인정보 처리 방법에 관한 고시』 제2조(공공기관에 의한 개인정보의 목적 외 이용 또는 제3자 제공의 공고)에 의거 ○○○에서 개인정보의 목적 외 이용 또는 제3자 제공한 내역을 아래와 같이 공고합니다.

1. 관리부서 :
2. 개인정보파일명 :
3. 공고기간 : 게재일로부터 10일 이상
4. 공고 장소 : ○○○ 홈페이지 (고시/공고)
5. 개인정보 목적 외 이용 또는 제3자 제공일 :
6. 개인정보 목적 외 이용 또는 제3자 제공 법적근거 :
7. 개인정보 목적 외 이용 또는 제3자 제공 목적 :
8. 개인정보 목적 외 이용 또는 제3자 제공 항목 :

○ 안전성 확보 조치

- 개인정보 자료 제공은 문서로 시행되어야 하며, 문서에 제공 목적 이외의 이용금지, 사용 목적 달성 후 폐기, 사후관리 실태 확인 등의 안전성 확보 조치 문구를 표기하여 시행
 - ※ 개인정보 보호법 시행령 제30조, 개인정보의 안전성 확보조치 기준

교육기관을 위한 개인정보 보호 법령 요약집

본 모음집 중 1장의 내용은 원칙적으로 상업적 용도로 무단 복제를 금합니다.

오타 등이 있는 경우 ywkim@keris.or.kr 로 제보 받습니다.

내용을 가공·인용할 때에는 출처를 밝혀 주시기 바랍니다.

최신 자료 다운로드 : 교육부 개인정보보호 포털(privacy.moe.go.kr)

교육기관

개인정보 보호 법령 모음집



KERIS

한국교육학술정보원

개인정보보호부