

의안번호	제 호	의결사항
의결 연월일	2023. . . (제 회)	

개인정보보호법시행령
일부개정령안

제출자	국무총리 (개인정보보호위원회 소관)
제출연월일	2023. . .

법제처 심사 전

1. 의결주문

개인정보 보호법 시행령 일부개정령안을 별지와 같이 의결한다.

2. 제안이유

개인정보 보호법 개정(2023.3.14.공포)에 따라 2024년 3월 15일 시행 예정인 일부 조항에 대해 기준 및 절차 등에 관한 사항을 시행령 개정을 통해 구체화하는 내용으로, 일반적인 개인정보 처리 과정에서의 열람 및 정정·삭제, 처리정지 등 요구권으로 보장되고 있는 정보주체의 권리와 함께, 디지털 전환의 변화된 상황에 맞추어 ‘완전히 자동화된 시스템’으로 개인정보를 처리하는 특수한 영역에서도 동일하게 정보주체의 권리가 보장될 수 있도록 법에서 위임한 사항을 구체화하려는 것임

또한, 개인정보처리자의 개인정보 보호 역량을 강화하기 위해 개인정보 보호 보호책임자의 전문성과 독립성을 보장할 수 있도록 개인정보 보호책임자의 자격 요건 및 의무 대상을 구체화하고, 공공기관 개인정보 보호 수준 평가에 대한 세부 절차를 마련하는 한편, 손해배상책임 보장제도가 정보통신서비스제공자에서 개인정보처리자로 변경됨에 따라 의무대상자의 범위 및 기준을 합리적으로 정비하려는 것임

3. 주요내용

가. 개인정보 보호수준 평가의 대상 및 기준·방법·절차(영 제13조의2) 법 제11조의2 신설에 따른 공공기관의 ‘개인정보 보호수준 평가’를 위

해 하위 법령에 위임된 평가대상, 평가기준 및 절차, 자료제출 범위 등의 기준 및 절차 규정을 마련

나. 고유식별정보 관리실태 정기조사(영 제21조)

정기조사의 기간을 합리적으로 조정(매 2년 → 3년)하고, ‘개인정보 보호수준 평가’ 및 ‘개인정보보호인증’ 대상 등 유사한 조사·점검이 있는 경우 제외 규정을 마련

다. 개인정보 처리방침의 내용 및 공개방법(영 제31조제1항)

개인정보를 국외에서 수집하여 처리하는 경우에 그 사실과 해당 국가에 관한 사항, 국외 이전 시 법적 근거 등을 처리방침에 기재하도록 규정

라. 개인정보 보호책임자의 지정 및 협의회(영 제32조, 제32조의2)

개인정보 보호책임자의 전문성과 독립성을 강화할 수 있도록 법 제31조가 개정됨에 따라 시행령에 위임된 개인정보 보호책임자 자격요건 및 적용대상의 기준 등을 규정하고, 법 제31조에서 위임한 개인정보 보호책임자 협의회가 수행하는 공동사업의 범위 구체화

마. 자동화된 결정에 대한 정보주체의 권리(영 제44조의2~제44조의4)

자동화된 결정에 대한 정보주체의 거부·설명 등 요구권 신설(법 제37조의2)에 따라 시행령에 위임된 요구절차 및 방법, 개인정보처리자의 조치사항 및 공개사항 등 세부절차를 규정

바. 손해배상책임 보험 등 가입 대상자의 범위·기준(영 제48조의7)

법 제39조의7 개정으로 손해배상책임 보장 의무가 부여되는 대상이 변경됨에 따라 의무대상의 범위 및 기준을 합리적으로 정비

사. 규제의 재검토(영 제62조의3)

규제개혁위원회 재검토기한 심사결과에 따라 ‘개인정보처리자 간 가명정보의 결합’의 재검토 기한을 2년에서 3년으로 변경

4. 주요토의과제

없 음

5. 참고사항

가. 관계법령 : 생 략

나. 예산조치 : 별도조치 필요 없음

다. 합 의 : 관계부처 의견 조화 중

라. 기 타 : 1) 신·구조문대비표, 별첨

2) 입법예고(2023. 11. 23. ~ 2024. 1. 2.) 진행 중

3) 행정규제 : 규제개혁위원회와 협의 중

개인정보 보호법 시행령 일부개정령안

개인정보 보호법 시행령 일부를 다음과 같이 개정한다.

제13조의2를 다음과 같이 신설한다.

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

법 제11조의2제1항의 “그 밖에 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 보호위원회가 공공기관의 개인정보 처리 업무의 특성 등을 고려하여 개인정보 보호수준 평가가 필요하다고 인정하는 공공기관

② 법 제11조의2제5항에 따른 개인정보 보호수준 평가 기준은 다음 각 호와 같다.

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 법 및 이 영에 따른 필요한 조치 사항의 준수 여부

③ 보호위원회는 개인정보 보호수준 평가를 시행하기 전에 평가대상,

평가기준·방법 및 평가지표 등을 포함한 평가계획을 마련하여 평가 대상 기관의 장에게 통보하여야 한다.

④ 보호위원회는 평가를 효율적으로 실시하기 위하여 개인정보 보호에 관한 전문적인 지식과 경험이 풍부한 전문가로 평가단을 구성하여 운영할 수 있다.

⑤ 보호위원회는 평가대상 기관의 장이 평가계획에 따라 제출한 자료를 기준으로 평가를 진행하되, 평가자료에 대한 사실 확인이 필요한 경우에는 현장 방문 또는 대면 평가의 방법을 병행하여 평가를 실시할 수 있다.

⑥ 법 제11조의2제5항에 따른 자료제출 범위는 다음 각 호와 같다. 이 경우 사실확인 등 최소한의 범위로 한정한다.

1. 평가계획에 따른 평가지표별 점검결과 및 증빙자료
2. 제1호의 평가지표별 증빙자료의 검증에 필요한 자료
3. 그 밖에 평가에 필요한 사항

⑦ 보호위원회는 중앙행정기관의 장 또는 지방자치단체의 장에게 소속 기관·단체 등 소관 분야 공공기관의 평가준비 또는 평가결과에 따른 개인정보 보호 조치를 위해 필요한 사항을 지원하도록 요청할 수 있다. 이 경우 지원 요청을 받은 중앙행정기관의 장 또는 지방자치단체의 장은 특별한 사유가 없는 한 요청 사항을 지원하기 위하여 성실하게 노력하여야 한다.

⑧ 제1항부터 제7항까지에서 규정한 사항 외에 개인정보 보호수준 평

가를 위한 세부적인 평가대상, 평가의 절차, 평가단의 구성·운영 방법, 평가결과의 활용 등은 보호위원회가 정하여 고시한다.

제21조제2항제1호를 다음과 같이 하고, 같은 항 제2호를 제3호로 하며, 같은 항에 제2호를 다음과 같이 신설하고, 같은 조 제3항 중 “필요한 조치를 하였는지를 2년”을 “필요한 조치를 하였는지를 3년”으로 하며, 같은 조 제4항 및 제5항을 각각 제5항 및 제6항으로 하고, 같은 조에 제4항을 다음과 같이 신설한다.

1. 1만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 공공기관
2. 제1호에 해당하지 않는 공공기관의 경우로서 보호위원회가 법 위반 이력 및 내용·정도, 고유식별정보 처리의 위험성 등을 고려하여 조사가 필요하다고 인정하는 공공기관
- ④ 제3항에도 불구하고 보호위원회는 법 제11조의2에 따른 개인정보 보호수준 평가, 법 제32조의2에 따른 개인정보 보호 인증 등에 따라 고유식별정보의 안전성 확보에 필요한 조치에 대한 정기적인 확인이 이루어진 경우에는 정기적인 조사에 갈음할 수 있다.

제31조제1항에 제4호 및 제5호를 각각 다음과 같이 신설한다.

4. 정보주체로부터 개인정보를 국외에서 수집하여 처리하는 경우 개인정보가 국외에서 처리된다는 사실과 해당 국가에 관한 사항(해당되는 경우에만 정한다)
5. 개인정보를 국외로 이전하는 경우 국외 이전의 근거와 법 제28조의

8제2항 각 호의 사항(해당되는 경우에만 정한다)

제32조제3항을 삭제하고, 같은 조 제1항, 제2항 및 제4항을 각각 제2항, 제3항 및 제5항으로 하며, 같은 조에 제1항 및 제4항을 각각 다음과 같이 신설한다.

① 법 제31조제1항단서에서 “종업원 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 「소상공인기본법」 제2조제1항에 따른 소상공인에 해당하는 개인정보처리자를 말한다.

④ 다음 각 호의 어느 하나에 해당하는 개인정보처리자(법 제2조제6호에 따른 공공기관의 경우에는 이 영 제2조제2호부터 제5호에 해당하는 경우에 한한다)는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 별표 1에서 정하는 자격요건을 갖춘 자를 지정하여야 한다.

1. 연간 매출액 또는 수입 등이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자

가. 제15조의2제1항 각 호의 어느 하나에 해당하는 자

나. 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교

2. 「의료법」 제3조의4에 따른 상급종합병원

3. 제30조의2제1항에 따라 보호위원회가 고시하는 기준에 해당하는 개인정보처리시스템을 운영하는 공공기관

제32조제2항(중전의 제1항)제2호를 다음과 같이 한다.

2. 개인정보 처리와 관련된 인적·물적 자원 및 정보의 관리

제32조제2항(종전의 제1항) 각 호 외의 부분 중 “법 제31조제2항제7호”를 “법 제31조제3항제7호”로 하고, 같은 조 제3항(종전의 제2항)제1호바목 중 “공무원 또는”을 “이상 공무원 또는”으로 하며, 같은 호 사목에 단서를 다음과 같이 신설한다.

다만, 제4항제1호나목에 해당하는 경우에는 소속 임직원 중에서 지정할 수 있다.

제32조제5항(종전의 제4항) 중 “제31조제2항”을 “제31조제3항”으로 하고, 같은 조에 제6항을 다음과 같이 신설한다.

⑥ 개인정보처리자(법 제31조제2항에 따라 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우는 제외한다)는 개인정보 보호책임자가 개인정보 보호 관련 업무에 대한 종합적 이해와 전문가적 역량을 갖추고 법 제31조제3항의 업무를 독립적으로 수행할 수 있도록 다음 각 호의 사항을 준수하여야 한다.

1. 개인정보 처리와 관련된 모든 정보에 대한 접근 보장
2. 수행하는 업무계획, 집행, 결과 등에 관하여 연 1회 이상 정기적으로 대표자 및 이사회(이사회가 없는 경우에는 대표자에 한한다)에 직접 보고할 수 있는 체계의 구축
3. 업무 수행에 적합한 조직체계의 마련 및 인적·물적 자원의 제공
4. 부당한 지시에 대한 불이행을 이유로 한 불이익의 금지

제32조의2를 제32조의3으로 하고, 제32조의2 및 제44조의2부터 제44조

의4까지를 각각 다음과 같이 신설한다.

제32조의2(개인정보 보호책임자 협의회의 사업 범위) 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 위하여 필요한 사업

② 보호위원회는 예산의 범위에서 개인정보 보호책임자 협의회 운영과 사업에 필요한 행정적·재정적 지원을 할 수 있다.

제44조의2(자동화된 결정의 거부·설명 등을 요구하는 절차 및 방법) 정보주체는 법 제37조의2제1항 또는 제2항에 따라 자동화된 결정에 대한 거부·설명 등을 요구하려면 개인정보처리자가 마련하여 제44조의4제1항제5호에 따라 공개한 방법과 절차에 따라 요구하여야 한다. 이

경우 개인정보처리자가 자동화된 결정에 대한 거부·설명 등을 요구하는 방법과 절차를 마련할 때에는 제41조제2항을 준용하되, “열람”은 “거부·설명 등”으로 본다.

제44조의3(자동화된 결정의 거부·설명 등의 요구에 따른 조치) ① 개인정보처리자는 법 제37조의2제1항 본문에 따라 정보주체가 해당 자동화된 결정이 생명·신체·재산의 이익 등 자신의 권리 또는 의무에 중대한 영향을 미치는 경우에 해당하여 자동화된 결정을 거부한 경우 해당 자동화된 결정을 적용하지 않는 조치를 해야 한다. 이 경우 정보주체가 인적 개입에 의한 재처리를 요구한 경우에는 그에 따른 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 개인정보처리자는 법 제37조의2제2항에 따라 정보주체가 자동화된 결정에 대한 설명 등을 요구한 경우 다음 각 호의 사항을 포함한 간결하고 의미있는 설명을 정보주체가 이해하기 쉽도록 제공해야 한다. 다만, 해당 자동화된 결정이 법 제37조의2제1항 본문에 따른 정보주체의 권리 또는 의무에 중대한 영향을 미치는 경우가 아닌 때에는 제44조의4제1항 각 호의 사항을 알리는 방법으로 설명 등을 할 수 있다.

1. 해당 자동화된 결정의 결과
2. 해당 자동화된 결정에 사용된 주요 개인정보의 유형과 해당 유형의 개인정보가 자동화된 결정에 미친 영향 등 자동화된 결정의 주요 기준
3. 해당 자동화된 결정에 사용된 주요 개인정보의 처리 과정 등 자동

화된 결정이 이루어지는 절차

③ 개인정보처리자는 법 제37조의2제2항에 따라 자동화된 결정에 대하여 이의를 제기한 경우에는 그 내용을 고려하여 필요한 조치를 한 후 정보주체에게 그 결과를 알려야 한다.

④ 개인정보처리자는 법 제37조의2제3항에 따른 정보주체의 거부 또는 설명 등 요구에 대하여 정당한 사유가 있어 필요한 조치를 하지 않은 경우에는 정보주체에게 그 사실 및 이유와 이의제기방법을 지체 없이 서면등의 방법으로 알려야 한다.

⑤ 개인정보처리자는 제1항부터 제3항까지의 규정에 따라 정보주체에게 해당 사실을 알리거나 설명 등의 조치를 하려는 때에는 정보주체의 요구를 받은 날부터 30일 이내에 서면등의 방법으로 해야 한다. 다만, 30일 이내에 처리하기 어려운 정당한 사유가 있는 경우에는 정보주체에게 그 사유를 알리고 60일 이내의 범위에서 연장할 수 있다.

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 사전에 서면등의 방법으로 정보주체에게 알려야 한다.

1. 자동화된 결정이 이루어진다는 사실과 그 목적 및 대상이 되는 정보주체의 범위
2. 자동화된 결정에 사용되는 주요 개인정보의 유형과 자동화된 결정

의 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. 법 제37조의2제1항 및 제2항에 따른 자동화된 결정에 대하여 정보주체가 거부 또는 설명 등을 요구할 수 있다는 사실과 거부·설명 등의 요구 방법과 절차

② 개인정보처리자는 제1항 각 호의 사항을 공개할 때에는 정보주체가 해당 내용을 쉽게 알 수 있도록 표준화·체계화된 용어를 사용해야 한다. 이 경우 정보주체가 쉽게 이해할 수 있도록 동영상·그림·도표 등 시각화된 방법 등을 활용할 수 있다.

제48조의7제1항 각 호 외의 부분을 다음과 같이 한다.

법 제39조의7제1항에서 “대통령령으로 정하는 기준에 해당하는 자”란 다음 각 호의 요건을 모두 갖춘 자를 말한다.

제48조의7제1항제1호 중 “전 사업연도”를 “직전 사업연도”로, “5천만원”을 “10억원”으로 하고, 같은 호에 단서를 다음과 같이 신설한다.

다만, 매출액을 산정하지 않는 경우 「법인세법」 제4조제3항제1호에 따른 수익사업에서 생기는 소득을 매출액으로 본다.

제48조의7제1항제2호 중 “이용자”를 “정보주체(제15조의3제2항2호에 해당하는 임직원은 제외한다)의”로, “1천명”을 “1만명”으로 하고, 같은 호

에 단서를 다음과 같이 신설한다.

다만, 영업의 전부 또는 일부의 양수, 분할·합병 등으로 개인정보를 이전받은 경우 이전받은 시점 기준으로 정보주체의 수가 1만명 이상인 경우로 한다.

제48조의7제2항을 제4항으로 하고, 같은 조에 제2항을 다음과 같이 신설하며, 같은 조 제4항(중전의 제2항) 본문 중 “가입 대상 개인정보처리자(제1항 각 호의 요건을 모두 갖춘 정보통신서비스 제공자 및 그로부터 이용자의 개인정보를 법 제17조제1항제1호에 따라 제공받는 자를 말한다. 이하 이 조에서 같다)”를 “법 제39조의7제1항 및 제2항에 따른 가입 대상 개인정보처리자”로 하고, 같은 조 제3항을 다음과 같이 한다.

② 법 제39조의7제2항제1호에서 “대통령령으로 정하는 공공기관과 비영리법인 및 단체”란 다음 각 호의 기관을 말한다.

1. 법 제2조제6호에 따른 공공기관. 다만, 제32조제4항 각 호에 해당하는 공공기관은 제외한다.
2. 「공익법인의 설립·운영에 관한 법률」에 따라 설립 허가된 법인
3. 「비영리민간단체 지원법」에 따라 등록된 단체

③ 법 제39조의7제2항제2호에서 “대통령령으로 정하는 자”란 다음 각 호의 요건을 모두 갖춘 자를 말한다.

1. 법 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 취한 자

2. 「소상공인기본법」 제2조제1항에 따른 소상공인으로부터 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인정보의 저장·관리 업무를 위탁받은 자

제62조의3제1항에 제4호를 다음과 같이 신설하고, 같은 조 제2항제1호를 삭제한다.

4. 제29조의3에 따른 개인정보처리자 간 가명정보의 결합: 2024년 1월 1일

별표 1을 별지와 같이 신설한다.

별표 1의4 중 “5천만원”을 “10억원”으로 하고, 같은 표 중 “5천만원”을 “10억원”으로 하며, 같은 표 800억원 초과부터 5천만원 이상 50억원 이하까지 중 “1천명”을 “1만명”으로 하고, 같은 표 중 “5천만원”을 “10억원”으로 한다.

부 칙

이 영은 2024년 3월 15일부터 시행한다.

개인정보 보호책임자의 자격(제32조제4항 관련)

개인정보보호 경력을 3년 이상 필수로 보유하고 개인정보보호, 정보보호, 정보기술 경력을 합하여 6년 이상을 보유

가. “개인정보보호 경력”이란 공공기관, 기업체, 교육 및 연구기관 등에서 개인정보보호 업무 수행, 개인정보보호 컨설팅, 개인정보 보호 관련 법률자문, 개인정보 영향평가, 정보보호 및 개인정보 보호 관리체계 인증심사 등의 업무를 수행한 경력을 말한다.

나. “정보보호 경력”이란 공공기관, 기업체, 교육 및 연구기관 등에서 정보보호를 위한 공통기반기술, 시스템·네트워크 보호, 응용 서비스 보호, 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 경력 또는 관련 법률자문 경력을 말한다.

다. “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 업무를 수행한 경력 또는 관련 법률자문 경력을 말한다.

라. 동일 기간에 두 가지 이상 업무가 중복되는 경우에 하나의 경력만 인정한다.

마. 아래의 학위 또는 자격을 취득한 경우 개인정보보호, 정보보호, 정보기술 경력을 대체할 수 있고, 중복으로 인정하지 않는다.

바. 그 밖의 자격 및 보호위원회가 인정하는 교육 이수 등 경력인정 요건에 대하여는 보호위원회 위원장이 정하여 고시한다.

<경력인정 요건>

구분	경력 인정 요건	인정 기간
개인정보 보호경력	○ 개인정보보호 관련 박사학위 취득자	3년
	○ 개인정보보호 관련 석사학위 취득자 ○ 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 제14조에 따른 정보보호 및 개인정 보보호 관리체계 인증심사원 ○ 개인정보 영향평가에 관한 고시 제5조에 따른 개인정보 영향평가 전문인력	2년
	○ 개인정보보호 관련 학사학위 취득자	1년
정보보호, 정보기술 경력	○ 정보보호, 정보기술 관련 박사학위 취득자	2년
	○ 정보보호, 정보기술 관련 석사학위 취득자	1년
	○ 정보보호, 정보기술 관련 학사학위 취득자	6개월

신 · 구조문대비표

현 행	개 정 안
<u><신 설></u>	<u>제13조의2(개인정보 보호수준 평가의 대상 및 기준·방법·절차 등) ① 법 제11조의2제1항의 “그 밖에 대통령령으로 정하는 기관”이란 다음 각 호의 기관을 말한다.</u> <u>1. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관</u> <u>2. 「지방공기업법」에 따른 지방공사와 지방공단</u> <u>3. 그 밖에 보호위원회가 공공기관의 개인정보 처리 업무의 특성 등을 고려하여 개인정보 보호수준 평가가 필요하다고 인정하는 공공기관</u> <u>② 법 제11조의2제5항에 따른 개인정보 보호수준 평가 기준은 다음 각 호와 같다.</u> <u>1. 개인정보 보호 정책·업무 수행실적 및 개선 정도</u> <u>2. 개인정보 관리체계의 적정성</u> <u>3. 정보주체 권리보장을 위한 조치사항 및 이행 정도</u>

4. 개인정보 침해방지 조치사항
및 안전성 확보 조치 이행 정
도

5. 그 밖에 법 및 이 영에 따른
필요한 조치 사항의 준수 여
부

③ 보호위원회는 개인정보 보호
수준 평가를 시행하기 전에 평
가대상, 평가기준·방법 및 평
가지표 등을 포함한 평가계획을
마련하여 평가대상 기관의 장에
게 통보하여야 한다.

④ 보호위원회는 평가를 효율적
으로 실시하기 위하여 개인정보
보호에 관한 전문적인 지식과
경험이 풍부한 전문가로 평가단
을 구성하여 운영할 수 있다.

⑤ 보호위원회는 평가대상 기관
의 장이 평가계획에 따라 제출
한 자료를 기준으로 평가를 진
행하되, 평가자료에 대한 사실
확인이 필요한 경우에는 현장
방문 또는 대면 평가의 방법을
병행하여 평가를 실시할 수 있
다.

⑥ 법 제11조의2제5항에 따른

자료제출 범위는 다음 각 호와 같다. 이 경우 사실확인 등 최소한의 범위로 한정한다.

1. 평가계획에 따른 평가지표별 점검결과 및 증빙자료

2. 제1호의 평가지표별 증빙자료의 검증에 필요한 자료

3. 그 밖에 평가에 필요한 사항

⑦ 보호위원회는 중앙행정기관의 장 또는 지방자치단체의 장에게 소속 기관·단체 등 소관 분야 공공기관의 평가준비 또는 평가결과에 따른 개인정보 보호 조치를 위해 필요한 사항을 지원하도록 요청할 수 있다. 이 경우 지원 요청을 받은 중앙행정기관의 장 또는 지방자치단체의 장은 특별한 사유가 없는 한 요청 사항을 지원하기 위하여 성실하게 노력하여야 한다.

⑧ 제1항부터 제7항까지에서 규정한 사항 외에 개인정보 보호 수준 평가를 위한 세부적인 평가대상, 평가의 절차, 평가단의 구성·운영 방법, 평가결과의 활용 등은 보호위원회가 정하여

제21조(고유식별정보의 안전성 확보 조치) ① (생 략)

② 법 제24조제4항에서 “대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다.

1. 공공기관

<신 설>

2. (생 략)

③ 보호위원회는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에 대하여 법 제24조제4항에 따라 안전성 확보에 필요한 조치를 하였는지를 2년마다 1회 이상 조사해야 한다.

<신 설>

고시한다.

제21조(고유식별정보의 안전성 확보 조치) ① (현행과 같음)

② -----

-----.

1. 1만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 공공기관

2. 제1호에 해당하지 않는 공공기관의 경우로서 보호위원회가 법 위반 이력 및 내용·정도, 고유식별정보 처리의 위험성 등을 고려하여 조사가 필요하다고 인정하는 공공기관

3. (현행 제2호와 같음)

③ -----

----- 필요한 조치를 하였는지를 3년-----
-----.

④ 제3항에도 불구하고 보호위원회는 법 제11조의2에 따른 개

④ · ⑤ (생략)

제31조(개인정보 처리방침의 내용 및 공개방법 등) ① 법 제30조 제1항제8호에서 “대통령령으로 정한 사항”이란 다음 각 호의 사항을 말한다.

1. ~ 3. (생략)

<신설>

<신설>

② · ③ (생략)

인정보 보호수준 평가, 법 제32조의2에 따른 개인정보 보호 인증 등에 따라 고유식별정보의 안전성 확보에 필요한 조치에 대한 정기적인 확인이 이루어진 경우에는 정기적인 조사에 갈음할 수 있다.

⑤ · ⑥ (현행 제4항 및 제5항과 같음)

제31조(개인정보 처리방침의 내용 및 공개방법 등) ① -----

-----.

1. ~ 3. (현행과 같음)

4. 정보주체로부터 개인정보를 국외에서 수집하여 처리하는 경우 개인정보가 국외에서 처리된다는 사실과 해당 국가에 관한 사항(해당되는 경우에만 정한다)

5. 개인정보를 국외로 이전하는 경우 국외 이전의 근거와 법 제28조의8제2항 각 호의 사항(해당되는 경우에만 정한다)

② · ③ (현행과 같음)

제32조(개인정보 보호책임자의 업무 및 지정요건 등) <신 설>

① 법 제31조제2항제7호에서 “대통령령으로 정한 업무”란 다음 각 호와 같다.

1. (생략)

2. 개인정보 보호 관련 자료의 관리

3. (생략)

② 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다.

1. 공공기관: 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등
가. ~ 마. (생략)

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① 법 제31조제1항단서에서 “종업원 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 「소상공인기본법」 제2조제1항에 따른 소상공인에 해당하는 개인정보처리자를 말한다.

② 법 제31조제3항제7호-----
-----.

1. (현행과 같음)

2. 개인정보 처리와 관련된 인적·물적 자원 및 정보의 관리

3. (현행과 같음)

③ -----

--.

1. -----

가. ~ 마. (현행과 같음)

바. 시·군 및 자치구: 4급 공무원 또는 그에 상당하는 공무원

사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람 <단서 신설>

아. (생략)

2. (생략)

<신설>

바. ----- 의 상 공무원 또는 -----

사. -----

-----. 다만, 제4항제1호나목에 해당하는 경우에는 소속 임직원 중에서 지정할 수 있다.

아. (현행과 같음)

2. (현행과 같음)

④ 다음 각 호의 어느 하나에 해당하는 개인정보처리자(법 제2조제6호에 따른 공공기관의 경우에는 이 영 제2조제2호부터 제5호에 해당하는 경우에 한한다)는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 별표 1에서 정하는 자격요건을 갖춘 자를 지정하여야 한다.

1. 연간 매출액 또는 수입 등이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자

가. 제15조의2제1항 각 호의

③ 제2항에도 불구하고 개인정보
 보처리자가 「소상공인기본
 법」 제2조에 따른 소상공인에
 해당하는 경우에는 별도의 지정
 없이 그 사업주 또는 대표자를
 개인정보 보호책임자로 지정한
 것으로 본다. 다만, 개인정보처
 리자가 별도로 개인정보 보호책
 임자를 지정한 경우에는 그렇지
 않다.

④ 보호위원회는 개인정보 보호
 책임자가 법 제31조제2항의 업
 무를 원활히 수행할 수 있도록
 개인정보 보호책임자에 대한 교
 육과정을 개설·운영하는 등 지

어느 하나에 해당하는 자
 나. 직전연도 12월 31일 기준
 으로 재학생 수가 1만명
 이상인 「고등교육법」 제
 2조에 따른 학교
 2. 「의료법」 제3조의4에 따른
 상급종합병원
 3. 제30조의2제1항에 따라 보호
 위원회가 고시하는 기준에 해
 당하는 개인정보처리시스템을
 운영하는 공공기관

<삭 제>

⑤ -----
 ----- 제31조제3항-----

원을 할 수 있다.

<신 설>

<신 설>

-----.

⑥ 개인정보처리자(법 제31조제2항에 따라 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우는 제외한다)는 개인정보 보호책임자가 개인정보 보호 관련 업무에 대한 종합적 이해와 전문가적 역량을 갖추고 법 제31조제3항의 업무를 독립적으로 수행할 수 있도록 다음 각 호의 사항을 준수하여야 한다.

1. 개인정보 처리와 관련된 모든 정보에 대한 접근 보장
 2. 수행하는 업무계획, 집행, 결과 등에 관하여 연 1회 이상 정기적으로 대표자 및 이사회(이사회가 없는 경우에는 대표자에 한한다)에 직접 보고할 수 있는 체계의 구축
 3. 업무 수행에 적합한 조직체계의 마련 및 인적·물적 자원의 제공
 4. 부당한 지시에 대한 불이행을 이유로 한 불이익의 금지
- 제32조의2(개인정보 보호책임자 협의회의 사업 범위) ① 법 제3

1조제7항에서 “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 위하여 필요한 사업

② 보호위원회는 예산의 범위에서 개인정보 보호책임자 협의회 운영과 사업에 필요한 행정적·재정적 지원을 할 수 있다.

제32조의2 (생략)

<신설>

<신설>

제32조의3 (현행 제32조의2와 같음)

제44조의2(자동화된 결정의 거부

· 설명 등을 요구하는 절차 및 방법) 정보주체는 법 제37조의2 제1항 또는 제2항에 따라 자동화된 결정에 대한 거부·설명 등을 요구하려면 개인정보처리자가 마련하여 제44조의4제1항 제5호에 따라 공개한 방법과 절차에 따라 요구하여야 한다. 이 경우 개인정보처리자가 자동화된 결정에 대한 거부·설명 등을 요구하는 방법과 절차를 마련할 때에는 제41조제2항을 준용하되, “열람”은 “거부·설명 등”으로 본다.

제44조의3(자동화된 결정의 거부

· 설명 등의 요구에 따른 조치)
① 개인정보처리자는 법 제37조의2제1항 본문에 따라 정보주체가 해당 자동화된 결정이 생명·신체·재산의 이익 등 자신의 권리 또는 의무에 중대한 영향을 미치는 경우에 해당하여 자동화된 결정을 거부한 경우 해

당 자동화된 결정을 적용하지 않는 조치를 해야 한다. 이 경우 정보주체가 인적 개입에 의한 재처리를 요구한 경우에는 그에 따른 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 개인정보처리자는 법 제37조의2제2항에 따라 정보주체가 자동화된 결정에 대한 설명 등을 요구한 경우 다음 각 호의 사항을 포함한 간결하고 의미있는 설명을 정보주체가 이해하기 쉽도록 제공해야 한다. 다만, 해당 자동화된 결정이 법 제37조의2제1항 본문에 따른 정보주체의 권리 또는 의무에 중대한 영향을 미치는 경우가 아닌 때에는 제44조의4제1항 각 호의 사항을 알리는 방법으로 설명 등을 할 수 있다.

1. 해당 자동화된 결정의 결과
2. 해당 자동화된 결정에 사용된 주요 개인정보의 유형과 해당 유형의 개인정보가 자동화된 결정에 미친 영향 등 자동화된 결정의 주요 기준

3. 해당 자동화된 결정에 사용
된 주요 개인정보의 처리 과
정 등 자동화된 결정이 이루
어지는 절차

③ 개인정보처리자는 법 제37조
의2제2항에 따라 자동화된 결정
에 대하여 이의를 제기한 경우
에는 그 내용을 고려하여 필요
한 조치를 한 후 정보주체에게
그 결과를 알려야 한다.

④ 개인정보처리자는 법 제37조
의2제3항에 따른 정보주체의 거
부 또는 설명 등 요구에 대하여
정당한 사유가 있어 필요한 조
치를 하지 않은 경우에는 정보
주체에게 그 사실 및 이유와 이
의제기방법을 지체 없이 서면등
의 방법으로 알려야 한다.

⑤ 개인정보처리자는 제1항부
터 제3항까지의 규정에 따라 정
보주체에게 해당 사실을 알리거
나 설명 등의 조치를 하려는 때
에는 정보주체의 요구를 받은
날부터 30일 이내에 서면등의
방법으로 해야 한다. 다만, 30일
이내에 처리하기 어려운 정당한

<신 설>

사유가 있는 경우에는 정보주체에게 그 사유를 알리고 60일 이내의 범위에서 연장할 수 있다.

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 사전에 서면등의 방법으로 정보주체에게 알려야 한다.

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 아동

제48조의7(손해배상책임의 이행
을 위한 보험 등 가입 대상자의
범위 및 기준 등) ① 다음 각 호
의 요건을 모두 갖춘 정보통신
서비스 제공자(「정보통신망 이
용촉진 및 정보보호 등에 관한
법률」 제2조제1항제3호에 해
당하는 자를 말한다. 이하 이 조
에서 같다) 및 그로부터 이용자

의 개인정보를 처리하는 경우
그 목적 및 처리하는 개인정
보의 구체적인 항목

5. 법 제37조의2제1항 및 제2항
에 따른 자동화된 결정에 대
하여 정보주체가 거부 또는
설명 등을 요구할 수 있다는
사실과 거부·설명 등의 요구
방법과 절차

② 개인정보처리자는 제1항 각
호의 사항을 공개할 때에는 정
보주체가 해당 내용을 쉽게 알
수 있도록 표준화·체계화된 용
어를 사용해야 한다. 이 경우 정
보주체가 쉽게 이해할 수 있도
록 동영상·그림·도표 등 시각
화된 방법 등을 활용할 수 있다.

제48조의7(손해배상책임의 이행
을 위한 보험 등 가입 대상자의
범위 및 기준 등) ① 법 제39조
의7제1항에서 “대통령령으로
정하는 기준에 해당하는 자”란
다음 각 호의 요건을 모두 갖춘
자를 말한다.

(같은 법 제2조제1항제4호에 해당하는 자를 말한다. 이하 이 조에서 같다)의 개인정보를 법 제17조제1항제1호에 따라 제공받은 자는 법 제39조의9제1항에 따라 보험 또는 공제에 가입하거나 준비금을 적립해야 한다.

1. 전년도(법인의 경우에는 전 사업연도를 말한다)의 매출액이 5천만원 이상일 것 <단서 신설>

2. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 1천명 이상일 것 <단서 신설>

<신 설>

1. ----- 직전 사업연도-----
-- 10억원 ----- . 다만, 매출액을 산정하지 않는 경우 「법인세법」 제4조제3항제1호에 따른 수익사업에서 생기는 소득을 매출액으로 본다.

2. -----
----- 정보주체(제15조의3제2항2호에 해당하는 임직원은 제외한다)의 --- 1만명 --- . 다만, 영업의 전부 또는 일부의 양수, 분할·합병 등으로 개인정보를 이전받은 경우 이전받은 시점 기준으로 정보주체의 수가 1만명 이상인 경우로 한다.

② 법 제39조의7제2항제1호에

② 가입 대상 개인정보처리자 (제1항 각 호의 요건을 모두 갖춘 정보통신서비스 제공자 및 그로부터 이용자의 개인정보를 법 제17조제1항제1호에 따라 제공받는 자를 말한다. 이하 이 조에서 같다)가 보험 또는 공제에 가입하거나 준비금을 적립할 경우 최저가입금액(준비금을 적립하는 경우 최소적립금액을 말한다. 이하 이 조에서 같다)의 기준은 별표 1의4와 같다. 다만, 가입 대상 개인정보처리자가 보험 또는 공제 가입과 준비금 적

서 “대통령령으로 정하는 공공기관과 비영리법인 및 단체”란 다음 각 호의 기관을 말한다.

1. 법 제2조제6호에 따른 공공기관. 다만, 제32조제4항 각 호에 해당하는 공공기관은 제외한다.

2. 「공익법인의 설립·운영에 관한 법률」에 따라 설립 허가된 법인

3. 「비영리민간단체 지원법」에 따라 등록된 단체

④ 법 제39조의7제1항 및 제2항에 따른 가입 대상 개인정보처리자-----

립을 병행하는 경우에는 보험 또는 공제 가입금액과 준비금 적립금액을 합산한 금액이 별표 1의4에서 정한 최저가입금액의 기준 이상이어야 한다.

③ 가입 대상 개인정보처리자가 다른 법률에 따라 법 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립한 경우에는 법 제39조의9 제1항에 따른 보험 또는 공제에 가입하거나 준비금을 적립한 것으로 본다.

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 검

-----.

③ 법 제39조의7제2항제2호에서 “대통령령으로 정하는 자”란 다음 각 호의 요건을 모두 갖춘 자를 말한다.

1. 법 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 취한 자

2. 「소상공인기본법」 제2조제1항에 따른 소상공인으로부터 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인정보의 저장·관리 업무를 위탁받은 자

제62조의3(규제의 재검토) ① ---

토하여 개선 등의 조치를 해야 한다. 1. ~ 3. (생략) <u><신설></u> 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. 1. <u>제29조의3에 따른 개인정보 처리자 간 가명정보의 결합: 2022년 1월 1일</u> 2. (생략)	----- ----. 1. ~ 3. (현행과 같음) 4. <u>제29조의3에 따른 개인정보 처리자 간 가명정보의 결합: 2024년 1월 1일</u> ② ----- ----- ----- ----- ----- ----- -----. <u><삭제></u> 2. (현행과 같음)
---	---

〈 의안 소관 부서명 〉

개인정보보호위원회 개인정보보호정책과	
연 락 처	(02) 2100 - 3057