개인정보 보호법 및 2차 시행령 개정사항 안내

2024. 3. 12.

개인정보보호위원회

차 례

「개인정보 보호법」 개정('23.3.14.공포)에 따라 개정 조문의 시행 시기에 맞춰 시행령을 개정하고 있으며, 작년 1차 시행령 개정('23.9.15.시행)에 이어 올해 3월 15일 시행되는 사항에 대한 시행령 개정(2차)이 완료됨에 따라 현장에서의 이해를 돕기 위해 안내서를 마련하였습니다.

첫째, 그동안 법적 근거가 명확하지 않았던 공공기관의 개인정보 관리 수준 진단 결과의 신뢰성 확보를 위해 '개인정보 보호수준 평가'에 대한 법적 근거를 신설하였습니다.

둘째, 개인정보 보호책임자(CPO)가 전문성과 독립성을 기반으로 개인정보 보호 업무를 수행할 수 있도록 CPO 자격 요건을 강화하고, CPO 협의회 신설을 통해 CPO 상호 간 협력이 긴밀하게 이루어질 수 있도록 하였습니다.

셋째, 인공지능(AI) 등 사람의 개입 없이 이루어지는 '완전히 자동화된 결정'에 대해 정보주체가 설명 또는 검토 요구를 할 수 있도록 하고, 정보주체인 국민의 권리 또는 의무에 중대한 영향을 미치는 경우에는 거부할 수 있도록 근거도 마련하였습니다.

넷째, 정보주체에 대한 손해배상책임 이행 의무대상이 전체 개인정보처리자로 변경됨에 따라 매출액, 개인정보 보유량 기준과 의무면제 기준을 정비하였습니다.

끝으로, 고유식별정보 관리실태 정기조사의 기간을 3년으로 조정하고, 국외 이전 또는 국외에서 국내 정보주체의 개인정보를 직접 수집·처리하는 경우에도 개인정보 처리방침에 관련 내용을 공개하도록 하였습니다.

안내서는 개인정보 보호법 개정 취지를 설명하고 개인정보처리자가 유의해야 할 사항 등을 안내함으로써 제도의 안정적인 정착과 수범자들의 이해도를 높이기 위한 목적으로 마련되었습니다.

안내서에 대한 자세한 사항은 아래에 기재된 개인정보보호위원회의 관련 제도 담당부서로 문의하여 주시기 바랍니다.

< 관련 제도 담당 부서 >

총괄, 자동화된 결정	개인정보보호정책과	02-2100-3055, 3057, 3047
보호수준 평가, CPO 지정	자율보호정책과	02-2100-3080, 3084
손해배상책임 보장	분쟁조정과	02-2100-3142
고유식별정보 실태조사	조사총괄과	02-2100-3161, 3164
국외 수집·이전 공개	국제협력담당관	02-2100-2482, 2485

1 공공기관 개인정보 보호수준 평가(법 제11조의2)

1. 개정 개요

□ 종전 '공공기관 관리수준 진단'은 평가대상 선정, 평가절차, 진단결과 및 개선·이행조치 등에 대한 명확한 법적 근거가 없어 진단결과를 환류하는 데 어려움이 있었다.

□ 이에, 공공기관의 개인정보 보호 수준을 매년 평가하고 그 결과를 바탕으로 우수기관에 대한 포상과 미흡기관에 대한 개선권고를 실시함으로써 공공기관의 개인정보 보호수준 역량강화로 환류하고자, '개인정보 보호수준 평가'의 법적 근거를 마련하였다.

2. 개정 법령

법률	**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.
시행령	**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.

3. 개정내용 해설

□ 개인정보 보호수준 평가의 대상이 되는 공공기관은 다음과 같다.

○ 중앙행정기관 및 그 소속기관, 지방자치단체(시·도 교육청, 교육지원청 포함)
(법 제11조의2제1항)

○「공공기관의 운영에 관한 법률」제4조에 따른 공공기관,「지방공기업법」에 따른 지방공사와 지방공단(영 제13조의2제1항제1~2호)

○ 그 밖에 영 제2조제4호 및 제5호에 따른 공공기관 중 공공기관의 개인정보 처리 업무의 특성 등을 고려하여 보호위원회가 고시하는 기준에 해당하는 기관(영 제13조의2제1항제3호)

- 이 중 '공공기관의 개인정보 처리 업무의 특성 등을 고려하여 보호위원회가 고시하는 기준에 부합하는 기관'(영 제13조의2제1항제3호)은 공공기관 중 민감정보 또는 대규모 개인정보 처리여부, 개인정보 유출사고 발생 여부 등을 종합적으로 고려하여 보호위원회가 정함(고시 제2조제2항)

평가 대상 선정 세부 기준(고시* 제2조제2항)

② 영 제13조의2제1항제3호에 따른 평가 대상은 특별법에 의하여 설립된 특수법인과「고등교육법」제2조**에 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

** 대학, 산업대학, 교육대학, 전문대학, 방송대학·통신대학·방송통신대학 및 사이버대학, 기술대학, 각종학교

* 개인정보 보호수준 평가에 관한 고시('24.3.15. 시행)

□ 평가 기준은 개인정보 보호 정책·업무의 수행실적 및 개선정도, 개인정보 관리체계의 적정성, 정보주체 권리보장을 위한 조치사항 및 이행 정도, 개인정보 침해방지 조치사항 및 안전성 확보 조치 이행 정도 등을 기준으로 하며, 각 기준별 세부 평가지표를 마련하여 평가할 계획이다.(영 제13조의2제2항)

○ 평가 기준에 따른 세부 평가지표는 평가계획 공개 시 함께 공개할 예정이다.

□ 평가에 필요한 자료제출의 범위, 평가 방법 및 절차 등 구체적인 사항은 다음과 같다.

○ 평가는 평가계획 수립 및 통보, 평가단 구성, 평가자료 제출, 평가 수행, 평가결과 통지 등의 절차에 따라 실시한다.

○ 보호위원회는 평가를 시행하기 전에 평가 대상, 평가일정, 평가기준 및 세부 평가방법, 평가지표 등을 포함한 평가계획을 수립하여 평가대상 기관의 장에게 통보하고 평가를 실시할 계획이다.(영 제13조의2제3항)

○ 보호위원회는 보호수준 평가에 필요한 ①평가대상기관이 개인정보 보호수준을 자체적으로 점검한 경우 그 결과 및 증명자료, ②증명자료의 검증에 필요한 자료, ③그 밖에 개인정보의 안전한 관리 여부 등 개인정보 보호수준을 평가하기 위해 필요한 자료 등을 평가대상에게 요청할 수 있다.(영 제13조의2제5항)

- 또한 보호위원회는 평가대상기관의 장이 제출한 자료를 기준으로 평가를 진행하거나 평가대상기관을 방문하여 평가할 수 있다.(영 제13조의2제6항)

○ 평가 대상이 정당한 사유 없이 자료를 제출하지 아니하거나 거짓으로 제출한 경우에는 1천만원 이하의 과태료를 부과할 수 있다.(법 제75조제4항제1호)

○ 평가 결과는 차년도 상반기에 발표하며 각 평가대상에게 통지하고, 인터넷 홈페이지 등을 통하여 공개할 계획이다.(법 제11조의2제3항, 고시 제4조제3항)

□ 보호위원회는 평가를 위해 개인정보 보호에 관한 전문적인 지식과 경험이 풍부한 전문가를 포함하여 평가단을 구성·운영할 수 있다.(영 제13조의2제4항, 고시 제5조)

○ 평가단은 개인정보 보호수준 평가의 전문성, 공정성 확보를 위해 다음의 기준에 적합한 전문가로 구성하며, 임기를 1년으로 하되 연임할 수 있다.

- 「고등교육법」 제2조에 따른 학교에서 조교수 이상으로 재직하는 자로서 개인정보 보호 관련 경력 3년 이상인 사람
- 개인정보 보호 또는 정보보호·보안 분야에서 3년 이상 업무 경력을 갖춘 사람
- 그 밖에 개인정보 관련 분야에 경력과 전문지식이 풍부하다고 보호위원회가 인정하는 사람

□ 보호위원회는 평가 결과에 따라 우수기관 및 그 소속직원에 대하여 포상할 수 있으며, 개인정보 보호를 위하여 필요하다고 인정하면 해당 공공기관의 장에게 개선을 권고할 수 있고, 권고를 받은 공공기관의 장은 그 조치 결과를 보호위원회에 알려야 한다.(법 제11조의2제4항)

○ 보호위원회는 평가 결과 우수기관 또는 소속직원에 대하여 표창 수여, 포상금 지급 등의 우대조치를 할 계획이다.

○ 보호위원회는 개인정보 보호수준 평가 결과 미흡기관에 대해 현장 컨설팅 및 실태점검을 실시할 수 있으며, 개인정보 보호수준 평가 결과가 업무평가 등에 반영될 수 있도록 소관 기관의 장에게 평가 결과를 제공할 수 있다.(고시 제7조)

○ 보호위원회는 중앙행정기관의 장 또는 지방자치단체의 장에게 관리·감독 권한이 있는 소속기관, 산하기관·단체 등 소관 분야 평가대상 공공기관의 평가 준비 또는 결과에 따른 개인정보보호 조치 지원을 위해 자문(컨설팅), 교육, 기술지원 및 주기적 점검 등 필요한 사항을 지원하도록 요청할 수 있다.

- 위 요청을 받은 중앙행정기관의 장 또는 지방자치단체의 장은 소속기관 등 평가대상 공공기관에 대해 필요한 사항 지원을 하기 위해 노력해야 한다.(영 제13조의2제7항)

※ '관리수준 진단제'와 '보호수준 평가제' 비교

구분	공공기관 관리수준 진단	공공기관 보호수준 평가
도입	2008년	2024년
법적 근거	· 개인정보 보호법 제11조(자료제출 요구 등) 준용	· 개인정보 보호법 제11조의2(개인정보 보호수준 평가)
대상	중앙행정기관, 광역 및 기초자치단체, 공공기관(공기업, 지방공사·공단 등)	중앙행정기관 및 소속기관, 광역 및 기초자치단체, 시·도교육청 및 교육지원청, 공공기관(공기업, 지방공사·공단 등)
결과 환류	· 미흡기관 현장컨설팅 및 기획점검 시행 (※ 법적 근거 없음)	· 평가 결과 우수기관 및 우수직원 포상 · 개선 권고 및 조치결과 요구 등 · 미흡기관 현장컨설팅 및 실태점검 시행
제재 조치	· 없음	· 자료 미제출·부실 제출에 대한 과태료 부과

◈ 공공기관 개인정보 보호수준 평가에 대한 세부 절차·기준 등은 추진계획 수립 및 별도 안내서를 마련하여 안내할 예정임(~'24.4월)

4. 개인정보처리자 유의사항

□ 법 제11조의2제2항에 따라 평가대상 공공기관은 개인정보 보호수준 평가에 필요한 자료를 보호위원회에 제출하여야 하며, 이를 위반할 경우 제75조제4항제1호에 따라 과태료를 부과받을 수 있다.

5. 제재 규정

위반행위	제재 내용
정당한 사유 없이 자료를 제출하지 아니하거나 거짓으로 제출한 자(법 제11조의2제2항 위반)	1천만원 이하 과태료 (법 제75조제4항제1호)

6. 질의 응답

□ 개인정보 보호수준 평가 시 기존 수준진단과 달라진 점은?

⇨ 평가대상 공공기관이 확대됨. 기존 관리수준 진단 대상에 중앙행정기관의 소속기관, 시·도 교육청·교육지원청 등이 추가되고, 고시에 따라 민감정보 및 대규모 개인정보를 처리하거나 유출사고가 발생한 공공기관 등 보호수준 평가가 필요하다고 판단되는 기관도 평가대상에 포함될 수 있음

⇨ 평가 결과 우수기관 및 소속 직원에게는 표창 및 포상금을 지급하고, 미흡기관에는 개선 권고와 함께 실태점검을 시행할 예정임

⇨ 평가자료 제출에 대한 제재 조치가 도입되어, 정당한 사유 없이 자료를 제출하지 아니하거나 거짓으로 제출한 경우 1천만원 이하의 과태료를 부과받을 수 있음

□ 개인정보 보호수준 평가 대상을 선정하기 위한 세부 기준은?

⇨ 법 제11조의2제1항 및 영 제13조의2제1항에 따라 중앙행정기관 및 그 소속기관, 지방자치단체, 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관, 「지방공기업법」에 따른 지방공사와 지방공단은 별도 선정없이 매년 평가대상이 됨

⇨ 영 제13조의2제1항제3호에 따라 개인정보 보유규모, 민감정보 처리여부, 개인정보 유출사고 발생여부 등을 고려하여 평가대상 선정 및 평가계획에 포함하여 발표할 예정임

□ 개인정보 보호수준 평가 일정은?

⇨ 개인정보 보호수준 평가의 자세한 일정은 '24. 4월 중 평가계획을 수립하여 공개할 예정

□ 개인정보 보호수준 평가 안내서(편람)는 언제 배포되는지?

⇨ 개인정보 보호수준 평가 안내서(편람)는 '24. 4월 평가계획 수립 후 배포 예정임

참고 **개인정보 보호수준 평가에 관한 고시(제정안, 3.15.시행)**

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다) 제11조의2와 같은 법 시행령(이하 "영"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.

부 칙

이 고시는 2024년 3월 15일부터 시행한다.

2 개인정보 보호책임자 제도 개선(법 제31조)

1 개인정보 보호책임자 전문성 강화를 위한 자격요건 도입

1. 개정 개요

□ 개인정보 보호책임자에게는 개인정보 보호 계획의 수립 및 시행, 개인정보 처리실태 조사, 개인정보 관련 고충처리 등 조직 내 개인정보 처리에 관한 업무를 총괄해서 책임지는 핵심적인 역할이 요구되므로 개인정보 보호책임자의 전문성 강화가 필요하다는 지적이 제기되어 왔다.

○ 이에, 시행령 개정을 통해 개인정보 보호책임자의 자격요건을 도입하고 자격요건을 갖춘 개인정보 보호책임자를 지정해야 하는 개인정보처리자의 범위를 명확히 하였다.

2. 개정 법령

법률	**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. ② 제1항 단서에 따라 개인정보 보호책임자를 지정하지 아니하는 경우에는 개인정보처리자의 사업주 또는 대표자가 개인정보 보호책임자가 된다. ③ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다. 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 정하는 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. ⑤ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속기관 또는 단체의 장에게 개선조치를 보고하여야 한다. 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. 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. ⑧ 보호위원회는 제7항에 따른 개인정보 보호책임자 협의회의 활동에 필요한 지원을 할 수 있다. ⑨ 제1항에 따른 개인정보 보호책임자의 자격요건, 제3항에 따른 업무 및 제6항에 따른 독립성 보장 등에 필요한 사항은 매출액, 개인정보의 보유 규모를 고려하여 대통령령으로 정한다.
시행령	**제32조(개인정보 보호책임자 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. ② 법 제31조제3항제7호에서 "대통령령으로 정한 업무"란 다음 각 호와 같다. 1. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행 2. 개인정보 처리와 관련된 인적·물적 자원 및 정보의 관리 3. 처리목적이 달성되거나 보유기간이 지난 개인정보의 파기 ③ 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. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관: 고위공무원단에 속하는 공무원(이하 "고위공무원"이라 한다) 또는 그에 상당하는 공무원 나. 가목 외에 정무직공무원을 장으로 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(소속기관을 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 시·군 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. 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.

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.

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 위하여 필요한 사업

② 보호위원회는 법 제31조제8항에 따라 예산의 범위에서 개인정보 보호책임자 협의회의 운영과 사업에 필요한 행정적·기술적 지원을 할 수 있다.

부 칙

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 보호법 시행령 [별표 1]**

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 인증 심사 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 공통 기반기술, 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.

3. 개정내용 해설

□ 기존 법령에서는 공공기관의 경우에는 최소 4급 이상 공무원 또는 개인정보 처리 관련 업무를 담당하는 부서의 장을, 공공기관 이외의 개인정보처리자는 사업주 또는 대표자나 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)을 개인정보 보호책임자로 지정하도록 직위요건을 규정하고 있었다.

□ 이번 시행령 개정을 통해 개인정보 보호책임자의 전문성 강화를 목적으로 매출액, 개인정보의 보유 규모를 고려하여 일정기준 이상 개인정보처리자*는 개인정보보호 경력 등 자격요건**을 갖춘 개인정보 보호책임자를 지정하도록 하였다.

* ① 연간 매출액 또는 수입이 1,500억원 이상인 자로서 [1]5만명 이상 민감·고유식별정보를 처리하거나 [2]100만명 이상의 개인정보를 처리하는 자 ② 직전 연도 12월 31일 기준 재학생 수(대학원 재학생 수를 포함)가 2만명 이상인 대학 ③ 상급종합병원 ④ 공공시스템운영기관

** 개인정보보호 경력, 정보보호 경력, 정보기술 경력을 합하여 총 4년 이상 보유하고 그 중 개인정보보호 경력을 최소 2년 이상 보유할 것

□ 또한, 학위 및 자격을 취득하거나 보호위원회가 주관하는 교육을 이수한 경우에는 일정기간을 개인정보 보호책임자의 경력으로 인정하는 제도를 함께 도입하였다.

※ 「개인정보 보호책임자 경력 인정에 관한 고시」를 통해 개인정보 보호책임자의 경력에 산입할 수 있는 자격의 종류 및 경력 인정기간을 명시하고, 보호위원회가 주관하는 교육에 대해서는 최대 3개월의 범위 내에서 개인정보보호 경력을 인정할 수 있는 근거를 마련하였음

< 개인정보 보호책임자 경력 인정 요건 >

구 분		경력 인정 요건	인정기간
시행령 별표1	개인정보보호 경력	ㅇ 개인정보보호 관련 박사학위 취득자	2년
		ㅇ 개인정보보호 관련 석사학위 취득자	1년
		ㅇ 개인정보보호 관련 학사학위 취득자	6개월
	정보보호 경력	ㅇ 정보보호 관련 박사학위 취득자	2년
		ㅇ 정보보호 관련 석사학위 취득자	1년
		ㅇ 정보보호 관련 학사학위 취득자	6개월
	정보기술 경력	ㅇ 정보기술 관련 박사학위 취득자	2년
		ㅇ 정보기술 관련 석사학위 취득자	1년
		ㅇ 정보기술 관련 학사학위 취득자	6개월
고시 별표1	개인정보보호 경력	ㅇ 정보보호 및 개인정보보호 관리체계 인증 등에 고시 제14조에 따른 정보보호 및 개인정보보호 관리체계 인증심사원 ㅇ 개인정보 영향평가에 관한 고시 제5조제2항에 따른 개인정보 영향평가 전문인력 ㅇ「변호사법」제4조에 따른 변호사 자격 취득자	1년
	정보보호, 정보기술 경력	ㅇ 정보관리기술사, 컴퓨터시스템응용기술사	1년
		ㅇ 정보보안기사, 정보처리기사	6개월

※ 고시 별표1에서 각각의 자격을 보유한 경우에는 구분된 경력 내(개인정보보호, 정보보호·정보기술)에서는 하나의 자격만 인정하며, 구분된 경력별로 중복 인정은 가능함

4. 개인정보처리자 유의사항

□ 개정 시행령 시행일은 2024년 3월 15일로 하되, 영 제30조의2제1항에 따라 보호위원회가 고시하는 기준에 해당하는 개인정보처리시스템(공공시스템)을 운영하는 기관에 대해서는 시행일을 2024년 9월 15일로 정하였다.

* 영 제30조의2제1항 개정규정 시행일 : 2024.9.15.

□ 시행령 시행 당시 개인정보처리자가 종전 규정에 따라 지정한 개인정보 보호책임자에 대하여는 영 시행 후 2년 이내에 제32조제3항 및 별표 1의 개정규정에 따른 자격요건을 갖추도록 하여 준비기간을 부여하였다.

○ 다만, 공공시스템운영기관이 제32조제4항제1호의 요건에도 해당되는 경우에는 2024년 3월 15일부터 2년 이내에 개정규정에 따른 자격요건을 갖추어야 한다.

◈ 개인정보 보호책임자 자격요건 인정에 대한 세부 절차 및 기준 등은 별도 안내서 마련 예정(~'24.6월)

5. 제재 규정

위반행위	제재 내용
법 제31조제1항을 위반하여 개인정보 보호 책임자를 지정하지 아니한 자	1천만원 이하의 과태료 (법 제75조제4항제9호)
이 법 위반행위에 대해 법 제64조제1항에 따라 시정조치 명령을 받은 후 시정조치 명령에 따르지 아니한 자	3천만원 이하 과태료 (법 제75조제2항제27호)

6. 질의 응답

□ 개인정보 보호책임자의 자격요건 준수를 위해서는 총 경력 4년을 충족하여야 하는데, 개인정보보호 경력과 정보보호·정보기술 경력을 필수로 모두 보유하여야 하는지?

⇨ 개인정보 보호책임자의 자격요건을 충족하기 위해서는 개인정보보호·정보보호·정보기술 경력을 합산한 총 경력을 4년 이상 보유하되, 그 중 개인정보보호 경력을 2년 이상 보유하여야 함. 다만, 각각의 경력을 모두 보유하여야 하는 것은 아니며, 개인정보보호 경력으로만 4년 이상 보유한 경우에도 자격요건의 충족은 가능함

□ 학위 및 자격 취득을 통한 개인정보 보호책임자의 경력은 중복으로 인정 가능한지?

⇨ 학위 및 자격 취득, 교육 이수를 통한 개인정보 보호책임자의 경력은 중복으로 인정할 수 있음. 다만, 개인정보 보호법 시행령 별표 1에서 규정하고 있는 학위 취득을 통한 경력 인정의 경우, 여러 개의 학위를 취득한 경우라도 하나의 학위만 인정이 가능하며, 관련 고시 별표 1에서 규정하고 있는 자격을 취득한 경우, 경력 내(개인정보보호, 정보보호·정보기술)에서는 하나의 자격만 인정하고 경력별로는 중복 인정이 가능함

□ 직전 연도 12월 31일 기준 재학생 수(대학원 재학생 수를 포함)가 2만명 이상인 대학의 경우 개인정보 보호책임자로 지정할 수 있는 구체적인 범위는?

⇨ 해당 학교의 행정사무를 총괄하는 사람을 포함하여 「고등교육법」 제14조에 따른 교원과 직원을 개인정보 보호책임자로 지정할 수 있음

□ 자격요건을 갖춘 개인정보 보호책임자를 지정하여야 하는 민간기업은 임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장을 개인정보 보호책임자로 지정할 수 있는데 "임원이 없는 경우"를 어떻게 해석해야 하는지?

⇨ 전체 조직에 임원이 없는 경우로 해석하는 것이 타당하며, "임원이 없는 경우"를 "개인정보 처리 관련 업무를 담당하는 임원이 없는 경우" 또는 "자격요건을 충족하는 임원이 없는 경우"로 축소 해석하는 것은 제도의 취지에 반할 우려가 있음

□ 민간기업의 정보보호 최고책임자가 부서장인 경우, 개인정보 보호책임자와 겸직이 가능한지?

⇨ 공공기관 외의 개인정보처리자는 정보보호 최고책임자와의 겸직 여부와 관계없이 사업주, 대표자 또는 임원을 개인정보 보호책임자로 지정하여야 하며, 임원이 있음에도 부서장을 개인정보 보호책임자로 지정한 경우 법 제31조제1항의 개인정보 보호책임자 지정 의무를 준수하지 않은 것으로 판단됨

※ 정보보호 최고책임자는 「개인정보 보호법」 제31조제2항에 따른 개인정보 보호책임자의 업무를 겸할 수 있음(정보통신망법 제45조의3제4항제2호라목)

□ 자격요건을 갖춘 개인정보 보호책임자 지정 의무 대상 기준에서 정보주체의 개인정보 수를 산정할 때, 임직원 개인정보나 분리·보관된 개인정보도 포함해야 하는지?

⇨ 개인정보 처리규모(5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보, 100만명 이상의 정보주체에 관한 개인정보)를 산정할 때, 개인정보처리자가 보유하고 있는 임직원 개인정보 및 분리·보관된 개인정보도 포함하는 것이 타당함

참고 개인정보 보호책임자 경력 인정에 관한 고시(안)

* 안내서에서 제시하고 있는 '고시안'은 현재 제정 절차가 진행 중이므로 변경될 수 있음

제1조(목적) 이 고시는 「개인정보 보호법」(이하 "법"이라 한다) 제31조제9항 및 같은 법 시행령(이하 "영"이라 한다) 별표 1에 따라 개인정보 보호책임자의 경력 인정에 필요한 세부 사항을 정함을 목적으로 한다.

제2조(자격의 인정) ① 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

부 칙

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 인정 요건을 갖춘 것으로 본다.

■ 개인정보 보호책임자 자격 인정에 관한 고시 [별표]

< 개인정보 보호책임자 경력 인정 자격 >

구분	경력 인정 자격	인정기간
개인정보 보호 경력	o 정보보호 및 개인정보보호 관리체계 인증 등에 고시 제14조에 따른 정보보호 및 개인정보보호 관리체계 인증심사원 o 개인정보 영향평가에 관한 고시 제5조제2항에 따른 개인정보 영향평가 전문인력 o「변호사법」제4조에 따른 변호사 자격 취득자	1년
정보보호, 정보기술 경력	o 정보관리기술사, 컴퓨터시스템응용기술사	1년
	o 정보보안기사, 정보처리기사	6개월

※ 각각의 자격을 보유한 경우에는 구분된 경력 내(개인정보보호, 정보보호 · 정보기술)에서는 하나의 자격만 인정하며, 구분된 경력별로 중복 인정은 가능함

2 개인정보 보호책임자 독립성 보장 및 협력체계 구축

1. 개정 개요

□ 법 개정을 통해 개인정보처리자에게 개인정보 보호책임자가 업무를 독립적으로 수행할 수 있도록 보장하여야 할 의무를 부과함에 따라, 이를 위해 시행령에 개인정보처리자가 준수하여야 할 사항을 구체적으로 규정하였다.

□ 또한, 법에 개인정보 보호책임자 간 교류협력을 활성화하기 위한 개인정보 보호책임자 협의회의 구성·운영 근거 및 보호위원회의 지원 근거가 마련됨에 따라, 시행령에 위임된 개인정보 보호책임자 협의회의 사업 범위를 규정하였다.

2. 개정 법령

법률	**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. ② 제1항 단서에 따라 개인정보 보호책임자를 지정하지 아니하는 경우에는 개인정보처리자의 사업주 또는 대표자가 개인정보 보호책임자가 된다. ③ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다. 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 정하는 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. ⑤ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속기관 또는 단체의 장에게 개선조치를 보고하여야 한다. 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. 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. ⑧ 보호위원회는 제7항에 따른 개인정보 보호책임자 협의회의 활동에 필요한 지원을 할 수 있다. ⑨ 제1항에 따른 개인정보 보호책임자의 자격요건, 제3항에 따른 업무 및 제6항에 따른 독립성 보장 등에 필요한 사항은 매출액, 개인정보의 보유 규모를 고려하여 대통령령으로 정한다.

시행령	**제32조(개인정보 보호책임자 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. ② 법 제31조제3항제7호에서 "대통령령으로 정한 업무"란 다음 각 호와 같다. 1. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행 2. 개인정보 처리와 관련된 인적·물적 자원 및 정보의 관리 3. 처리목적이 달성되거나 보유기간이 지난 개인정보의 파기 ③ 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. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관: 고위공무원단에 속하는 공무원(이하 "고위공무원"이라 한다) 또는 그에 상당하는 공무원 나. 가목 외에 정무직공무원을 장으로 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(소속기관을 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 시·군 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. 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. 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. 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 위하여 필요한 사업 ② 보호위원회는 법 제31조제8항에 따라 예산의 범위에서 개인정보 보호책임자 협의회의 운영과 사업에 필요한 행정적·기술적 지원을 할 수 있다.

3. 개정내용 해설

□ 개인정보처리자가 개인정보 보호책임자의 독립성을 보장하기 위해 준수하여야 할 사항*을 시행령에 구체화하여 규정하였다.

* ① 개인정보 처리 관련 정보에 대한 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 업무수행에 적합한 조직체계 마련 및 인적·물적 자원의 제공

□ 아울러, 개인정보 보호책임자 협의회가 수행하는 공동사업에 대한 범위*를 규정하고, 보호위원회가 행정적·기술적으로 지원할 수 있도록 하였다.

* 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 개인정보보호 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

4. 개인정보처리자 유의사항

□ 개인정보처리자는 법 제31조제2항에 따라 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우를 제외하고 개인정보 보호책임자의 독립성 보장을 위한 의무사항을 이행하여야 한다.

◈ 개인정보 보호책임자의 독립성 보장을 위한 세부 기준 등은 별도 안내서 마련 예정(~'24.6월)

5. 제재 규정

위반행위	제재 내용
법 제31조제1항을 위반하여 개인정보 보호 책임자를 지정하지 아니한 자	1천만원 이하의 과태료 (법 제75조제4항제8호)
이 법 위반행위에 대해 법 제64조제1항에 따라 시정조치 명령을 받은 후 시정조치 명령에 따르지 아니한 자	3천만원 이하 과태료 (법 제75조제2항제27호)

6. 질의 응답

□ 개인정보 보호책임자가 대표자 또는 이사회에 정기적으로 직접 보고할 수 있는 체계를 구축하도록 하고 있는데 구체적으로 어떻게 마련하면 되는지?

⇨ 조직 내 개인정보보호 관련 사항에 대한 전사적 차원의 관심을 제고하고, 개인정보 보호책임자가 개인정보 처리에 관한 책임자로서 실질적 역할을 수행할 수 있도록 개인정보 보호 계획의 수립·시행 및 그 결과에 관하여 이사회 또는 대표자에게 최소 연 1회 이상 정기적으로 보고할 수 있는 체계를 구축하되, 이사회가 있는 경우에는 이사회 보고를 우선으로 하는 것이 바람직함

□ 개인정보 보호책임자가 대표자 또는 이사회에 정기적으로 직접 보고할 수 있는 체계를 구축하도록 하고 있는데 보고 방식이 정해져 있는 것인지?

⇨ 개인정보 보호책임자의 보고 체계를 특정 방식으로 한정하고 있지 않으므로 기관의 개인정보 보호 계획*, 내부 관리계획** 등을 활용하여 조직 상황에 따라 보고 방법을 정할 수 있음

* 개인정보 보호책임자의 업무 : 개인정보 보호 계획의 수립 및 시행(법 제31조제3항제1호)

** 내부 관리계획 포함사항 : 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항 (개인정보의 안전성 확보조치 기준 제4조제1항제3호)

□ 영 제32조제6항을 위반한 경우 제재규정이 있는지?

⇨ 보호위원회는 법 제61조에 따라 개인정보처리자에게 개인정보 처리실태의 개선을 권고할 수 있고 법 제64조 및 제75조제2항제27호에 근거하여 보호위원회의 시정조치 명령에 따르지 않은 자는 3천만원 이하의 과태료 부과 대상이 될 수 있음

□ 개인정보 보호책임자 협의회의 역할은?

⇨ 개인정보처리자가 개인정보의 안전한 처리 및 보호, 정보의 교류, 공동사업 등을 수행하기 위해 협의회를 구성·운영할 수 있으며, 협의회를 통해 개인정보 보호책임자의 권한과 책임을 보장하여 정부와의 정책 소통의 창구로써 그 기능을 수행할 수 있음

3 자동화된 결정에 대한 정보주체의 권리(법 제37조의2)

1. 개정 개요

□ 인공지능(AI)의 복잡한 처리 과정, '블랙박스'로 표현되는 불투명성으로 인해 정보주체인 국민과 개인정보처리자 간의 '정보 비대칭' 문제가 제기됨에 따라,

□ 법 개정('23.3.14.공포)을 통해 자동화된 결정에 대해 정보주체가 설명을 요구하거나 의견 제출을 통한 검토 요구를 할 수 있도록 하여 투명성을 보장하였으며,

○ 정보주체의 권리 또는 의무에 중대한 영향을 미치는 경우에는 일정한 조건이 충족될 경우에는 거부할 수 있도록 규정을 신설하였다.

2. 개정 법령

법률	**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.
시행령	**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.

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.

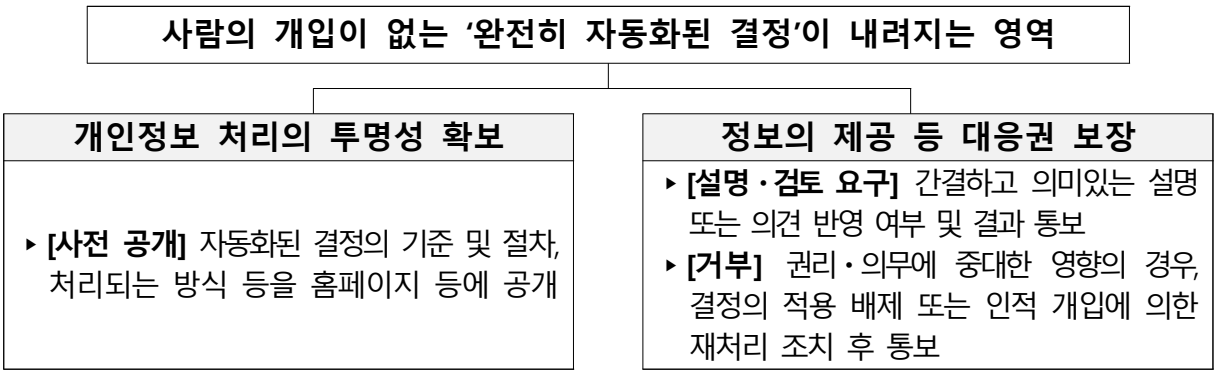
⑥ 제1항부터 제5항까지의 규정에 따른 정보주체의 거부·설명등요구에 따른 조치에 관한 세부사항은 보호위원회가 정하여 고시한다.

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.

3. 개정내용 해설



① 정보주체의 권리가 인정되는 대상 : '자동화된 결정'

□ '자동화된 결정'이란 사람의 개입 없이 완전히 자동화된 시스템으로, 개인정보를 분석하는 등 처리하는 과정을 거쳐, 개인정보처리자가 정보주체의 권리 또는 의무에 영향을 미치는 최종적인 결정을 한 경우를 말한다.

○ 따라서, 결정이 이루어지는 과정에서 정당한 권한을 가진 사람에 의한 실질적인 개입이 없거나, 단순 결재 등 형식적인 절차만을 운영하고 있다면 사실상 사람의 개입 없이 이루어진 결정이므로 완전히 자동화된 결정에 해당될 수 있다.

사례 **완전히 자동화된 시스템 : "실질적이고 의미있는 인적 개입이 있는지 여부"**

- **(해당)** 인공지능(AI) 면접만을 통해서 응시자의 개인정보를 분석하여 불합격 결정을 하는 경우
- **(제외)** 권한이 있는 인사위원회를 통해 실질적으로 채용 여부를 결정하는 절차를 운영하고, 인공지능(AI) 등 자동화된 시스템에 의해 산출된 자료를 참고하는 경우

□ 정보주체인 사람의 개인정보자기결정권을 보호하고자 하는 취지이므로 해당 정보주체의 개인정보를 처리하여 이루어지는 결정이어야 한다.

○ '분석·가공 등 실질적인 자동화 처리 과정을 거쳐 의미 있는 정보를 추출하여 이루어지는 결정'을 의미하며, 기계적으로 대입하여 분류하거나 단순 산출 과정을 거치는 경우를 의미하는 것은 아니라는 점에 유의해야 한다.

○ 따라서, ①개인정보 처리와 무관한 사업자 정보, 상품 정보 등을 처리하는 경우, ②개인정보를 단순 난수 처리하거나 무작위 추출하는 경우 등은 해당되지 않는다.

사례 **'개인정보의 처리' 사례**

- **(해당)** AI 배차 플랫폼을 운영하면서 플랫폼 이용사업자의 이용기록 및 패턴(행태정보)을 분석하여 이용계정 중지 여부를 결정하는 경우
- **(제외)** 쇼핑 플랫폼에서 이용사업자의 상품 노출 순서를 자동으로 결정하는 경우에 이용사업자의 개인정보가 아닌 사업자정보 및 상품정보만을 활용하는 경우

□ 정보주체인 국민의 권리 또는 의무에 영향을 미치는 최종적인 결정인 경우에는 자동화된 결정의 범위에 포함된다. 다만, 개인정보처리자가 추천하고 정보주체가 선택·결정하는 맞춤형 광고·뉴스 추천, 본인 확인 등 사실의 확인과 같은 경우는 자동화된 결정에 해당하지 않는다.

사례 **개인정보처리자가 정보주체의 권리 또는 의무에 영향을 미치는 최종적 결정**

- **(해당)** 개인정보처리자가 AI배차 등 분야에서 부정거래탐지시스템을 통한 개인정보 분석 등 처리 과정을 거쳐 계약해지 등 불이익을 주는 최종적 결정을 한 경우
- **(제외)** 맞춤형 광고, 뉴스 추천 등과 같이 개인정보처리자가 추천하고 이용여부에 대한 결정은 정보주체가 하는 경우로서 권리 또는 의무에 영향을 미치지 않는 경우

□ 「행정기본법」의 '자동적 처분'에 관하여 개별 법률에서 규정하고 있는 경우에는 자동화된 결정에서 제외된다.

○ 「행정기본법」 제20조에 따른 '자동적 처분'의 경우에는 행정청의 처분에 재량이 있는 경우에는 자동적 처분을 제한하고 있고, 개별 법률의 규정에 따라 자동적 처분에 대한 근거규정이 명확한 경우에만 허용하고 있다.

사례 **「행정기본법」 제20조에 따라 개별 법률에서 규정한 '자동적 처분'**

- **「행정기본법」 제20조(자동적 처분)** 행정청은 법률로 정하는 바에 따라 완전히 자동화된 시스템(인공지능 기술을 적용한 시스템을 포함한다)으로 처분을 할 수 있다. 다만, 처분에 재량이 있는 경우는 그러하지 아니하다.
- **「수입식품안전관리 특별법」 제20조의2(수입신고 수리의 자동화)** ① 제20조제1항에 따른 수입신고 중 국민건강에 미치는 위해발생의 우려가 낮고 반복적으로 수입되는 수입식품등의 수입신고는 「행정기본법」 제20조에 따라 제39조의2의 수입식품통합정보시스템에 의하여 완전히 자동화된 방식으로 수리할 수 있다.

○ 공공분야의 경우에도 「행정기본법」 제20조의 자동적 처분에 해당하지 않는 자동화된 결정에 대하여는 「개인정보 보호법」의 자동화된 결정 규정이 적용되므로 자동화된 결정에 대한 정보주체의 권리를 보장해야 한다.

□ 다른 법률에 자동화된 결정과 관련한 특별한 규정이 있는 경우에는 해당 법률의 규정이 적용된다.

○ 「신용정보의 이용 및 보호에 관한 법률」에 따른 자동화평가와 같이 해당 분야의 특수성을 반영하여 자동화된 결정과 관련하여 별도의 권리 규정을 두고 있는 때에는 해당 법률의 규정이 적용된다.

사례 「신용정보의 이용 및 보호에 관한 법률」에 따른 '자동화평가'

· **제2조(정의)** 14. **"자동화평가"**란 제15조제1항에 따른 신용정보회사등의 종사자가 평가 업무에 관여하지 아니하고 컴퓨터 등 정보처리장치로만 개인신용정보 및 그 밖의 정보를 처리하여 개인인 신용정보주체를 평가하는 행위를 말한다.

· **제36조의2(자동화평가 결과에 대한 설명 및 이의제기 등)** ① 개인인 신용정보주체는 개인신용평가회사 및 대통령령으로 정하는 신용정보제공·이용자(이하 이 조에서 "개인신용평가회사등"이라 한다)에 대하여 다음 각 호의 사항을 설명하여 줄 것을 요구할 수 있다.

1. ~ 2. (생략)

② 개인인 신용정보주체는 개인신용평가회사등에 대하여 다음 각 호의 행위를 할 수 있다.

1. 해당 신용정보주체에게 자동화평가 결과의 산출에 유리하다고 판단되는 정보의 제출
2. 자동화평가에 이용된 기초정보의 내용이 정확하지 아니하거나 최신의 정보가 아니라고 판단되는 경우 다음 각 목의 어느 하나에 해당하는 행위
   가. 기초정보를 정정하거나 삭제할 것을 요구하는 행위
   나. 자동화평가 결과를 다시 산출할 것을 요구하는 행위

③·④ (생략)

② 설명 및 검토 요구 : '자동화된 결정이 있는 경우'

□ 정보주체인 국민은 자동화된 결정이 자신의 권리 또는 의무에 영향을 미치는 경우에는 개인정보처리자에게 해당 결정에 대한 설명 또는 검토해 줄 것을 요구할 수 있다.

□ 정보주체의 설명 요구를 받은 개인정보처리자는 해당 결정의 기준 및 처리 과정 등에 대해 설명해야 한다.

○ 이 때의 '설명'은 결정의 주요 기준(개인정보의 유형 및 영향), 결정의 절차(개인정보의 처리 과정) 등의 사항*에 대해 일반적으로 이해할 수 있는 간결하고 의미있는 정보를 제공하는 것을 말한다.

* ①해당 자동화된 결정의 결과, ②해당 자동화된 결정에 사용된 주요 개인정보의 유형, ③해당 유형의 개인정보가 자동화된 결정에 미친 영향 등 자동화된 결정의 주요 기준, ④해당 자동화된 결정에 사용된 주요 개인정보의 처리 과정 등 자동화된 결정이 이루어지는 절차

○ 설명할 때에는 데이터 처리기술, 알고리즘이나 머신러닝의 작동방식 등 개인정보 처리의 복잡도를 고려하여 정보주체가 이해하기 쉬운 방식으로 간략하게 제시하여야 하고, 정보주체의 입장에서 개인정보자기결정권 행사에 도움이 될 수 있는 의미 있는 정보를 선별하여 제공하여야 한다.

※ (취지) 알고리즘이나 머신러닝의 작동과정에서 개인정보 처리에 대한 복잡한 수학적 설명 대신 간결하고 의미있는 정보를 정보주체에게 제공하도록 하려는 것임

□ 이와 함께, 개인정보처리자는 정보주체가 개인정보를 추가적으로 반영해 줄 것을 요구하는 등 의견을 제출하는 경우에는 해당 의견을 반영할 필요가 있는지 검토하고 반영 여부와 그 결과를 지체 없이 알려야 한다.

③ 자동화된 결정에 대한 거부 : '중대한 영향을 미치는 경우'

□ 정보주체는 자동화된 결정이 자신의 권리 또는 의무에 법적인 영향을 미치는 경우로서 그 영향의 정도가 정보주체의 권리 또는 의무의 본질적인 부분을 제한하거나 박탈하는 등 중대한 영향을 미치는 경우에는 해당 결정에 대해 거부할 수 있다.

기준 정보주체의 권리 또는 의무에 중대한 영향을 미치는지 여부의 판단기준

· 정보주체의 권리 또는 의무에 중대한 영향을 미치는 경우에 해당하는지 여부를 판단할 때에는 ①사람의 생명, 신체의 안전 및 기본권의 보호와의 관련성이 있는지, ②정보주체의 권리가 박탈되거나 권리의 행사가 불가능하게 되는지, ③정보주체가 수인하기 어려운 의무가 발생하는지, ④정보주체의 권리 또는 의무에 지속적인 제한이 발생하는지, ⑤해당 영향이 미치기 전의 상태로 회복하거나 해당 영향을 회피할 수 있는 가능성이 있는지 등을 종합적으로 고려하여 판단하여야 함

○ 이 경우 개인정보처리자는 ①해당 결정을 적용하지 않는 조치를 하거나 ②인적 개입에 의한 재처리를 하고 그 결과를 정보주체에게 알려야 한다.

사례 정보주체가 거부한 경우 조치방법

· 공공기관이 복지수당 지급 후 'AI 부정수급자 탐지시스템'만으로 수급자의 개인정보를 분석하는 처리과정을 통해, 해당 정보주체에 대한 복지수당 지급을 취소하는 최종 결정을 한 경우로서 정보주체가 해당 결정을 거부하면, ①복지수당 지급 취소 결정을 적용(실행)하지 않는 조치를 하거나 ②사람이 실질적으로 개입하여 재처리한 후 그 결과를 정보주체에게 30일 이내에 알려야 함

· 완전히 자동화된 AI 부정거래탐지시스템을 통하여 정보주체의 계정을 '영구적으로 박탈'하는 최종 결정을 한 경우 정보주체가 해당 결정을 거부하면, '영구적으로 계정을 박탈'하는 조치를 적용(실행)하지 않거나 사람이 실질적으로 개입하여 재처리한 후 그 결과를 정보주체에게 30일 이내에 알려야 함

□ 다만, 자동화된 결정이 정보주체의 권리 또는 의무에 중대한 영향을 미치는 경우라고 하더라도, 자동화된 결정이 이루어진다는 사실에 대해 정보주체가 명확히 알 수 있도록 동의, 계약 등을 통해 미리 알렸거나 법률에 명확히 규정이 있는 경우에는 거부권은 인정되지 않고, 자동화된 결정에 대한 설명 요구 또는 의견제출을 통한 검토 요구만 가능하다.

④ 개인정보처리자의 거절사유 : '정당한 사유'

□ 개인정보처리자는 다른 사람의 생명·신체·재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 등 정당한 사유가 있는 경우에는, 거부 또는 설명 등 요구에 대해 거절할 수 있고, 거절하는 경우에는 그 사유를 정보주체에게 지체 없이 알려야 한다.

○ 정당한 사유가 있는지 여부는 ①자동화된 결정에 대한 정보주체의 권리 성립 요건을 충족하는지, ②법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우인지, ③다른 사람의 생명·신체·재산과 그 밖의 이익을 부당하게 침해할 우려가 있는지, ④개인정보처리자 또는 제3자의 재산상 권리를 부당하게 침해할 우려가 있는 경우로서 정보주체의 자동화된 결정에 대한 권리보다 우선하는지 등을 종합적으로 고려하여 이익형량 과정을 거쳐 판단해야 한다.

□ 거부 또는 설명 등 요구에 대해 거절 등 조치를 할 경우 정보주체가 이의를 제기할 수 있는 절차를 마련하고 안내해야 하고(법 제38조제5항),

○ 정보주체가 해당 절차에 따라 이의를 제기한 경우에는 그 내용을 검토한 후 그 결과를 정보주체에게 알려야 한다.

⑤ 자동화된 결정의 기준 및 절차 등 공개

□ 개인정보처리자가 완전히 자동화된 결정을 하는 경우에는 그 기준과 절차, 개인정보가 처리되는 방식 등을 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지 등에 공개하도록 하여 투명성 확보와 함께 정보주체의 권리 행사가 가능하도록 하였다.

○ 다만, 인터넷 홈페이지 등을 운영하지 않거나 지속적으로 알려야 할 필요가 없는 경우에는 미리 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(서면 등의 방법)으로 정보주체에게 알릴 수 있다.

< 인터넷 홈페이지 등에 공개해야 하는 사항 >

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

□ 아울러, 공개할 때에는 정보주체가 해당 내용을 쉽게 알 수 있도록 표준화·체계화된 용어를 사용해야 하고, 정보주체가 쉽게 이해할 수 있도록 동영상·그림·도표 등 시각적인 방법 등을 활용할 수 있다.

⑥ 처리기간 및 고지방법

□ 개인정보처리자는 정보주체의 요구를 받은 날부터 30일 이내에 정보주체에게 거부에 따른 조치 사실을 알리거나 설명 등의 조치를 하여야 한다.

○ 다만, 정당한 사유가 있는 경우 정보주체에게 그 사유를 알리고 30일 이내 범위에서 연장할 수 있으며, 그 횟수는 2회에 한정된다.

□ 고지 방법은 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(서면등의 방법)으로 알려야 한다.

⑦ 정보주체의 요구 절차 및 방법

□ 개인정보처리자는 정보주체가 열람등요구*를 할 수 있는 구체적인 방법과 절차를 마련하고 이를 정보주체가 알 수 있도록 공개해야 하고, 이 경우 열람등요구의 방법과 절차는 해당 개인정보의 수집 방법과 절차보다 어렵지 않도록 해야 한다. (법 제38조제4항, 영 제41조제2항)

* 열람등요구 : 법 제35조에 따른 열람, 제35조의2에 따른 전송, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지 및 동의 철회, 제37조의2에 따른 거부·설명 등의 요구

□ 정보주체는 자동화된 결정에 대해 거부하는 경우에는 개인정보처리자가 마련하여 영 제44조의4제1항제5호에 따라 공개하는 방법과 절차에 따라야 한다.

□ 정보주체는 자동화된 결정에 대해 개인정보처리자에게 해당 자동화된 결정의 기준 및 처리 과정 등에 대한 설명을 요구하거나, 정보주체가 개인정보 추가 등의 의견을 제출하여 개인정보처리자가 해당 의견을 자동화된 결정에 반영할 수 있는지에 대한 검토를 요구할 수 있다.

○ 이 경우 정보주체의 설명 또는 검토 요구는 개인정보처리자가 마련하여 영 제44조의4제1항제5호에 따라 공개하는 방법과 절차에 따라야 한다.

4. 개인정보처리자 유의사항

□ 자동화된 결정에 대한 '설명'의 경우 자동화된 결정에 사용된 주요 개인정보가 자동화된 결정에 미치는 영향 등에 대한 간결하고 의미 있는 설명을 의미하므로,

○ 알고리즘의 공개나 복잡한 기술적 작동원리 등을 나열하는 등의 설명을 하도록 한 것은 아니고, 정보주체의 입장에서 의미 있는 설명을 간결하게 제공하여 정보주체가 이해할 수 있도록 한 것임에 유의해야 한다.

□ 개인정보처리자는 법 제38조제4항에 따라 자동화된 결정에 대한 거부 및 설명 등 요구 방법과 절차를 마련하여 공개해야 하고,

○ 정보주체는 개인정보처리자가 마련하여 공개한 방법과 절차에 따라 거부·설명 등을 요구할 수 있다.

◈ 자동화된 결정에 대한 세부 절차·기준 등은 별도 안내서(~3월) 및 고시 마련 예정(~'24.상반기)

5. 제재 규정

위반행위	제재 내용
법 제37조의2제3항을 위반하여 정당한 사유 없이 정보주체의 요구에 따르지 아니한 자	3천만원 이하 과태료 (법 제75조제2항제24호)
이 법 위반행위에 대해 법 제64조제1항에 따라 시정조치 명령을 받은 후 시정조치 명령에 따르지 아니한 자	3천만원 이하 과태료 (법 제75조제2항제27호)

6. 질의 응답

□ 인공지능(AI)을 활용한 채용 절차를 진행하게 되면 무조건 자동화된 결정에 대한 권리 행사의 대상에 해당하는 것인지?

⇨ 인공지능(AI)을 활용한 채용 절차라고 하더라도 모두 동일하게 권리 행사의 대상이 되는 것이 아니며, 채용심사 과정에 실질적인 인적 개입이 있는지, 자동화된 시스템에 의한 개인정보 처리와 결정 사이에 실질적인 관련성이 있는지 등의 구체적이고 개별적인 맥락을 고려해야 함 (① 정보주체의 권리가 인정되는 대상 : '자동화된 결정' 부분 24쪽 참조)

□ 인공지능(AI)만으로 채용을 진행하는 경우 지원자가 거부권을 행사할 수 있는지?

⇨ 해당 결정을 '거부'할 수 있는 권리는 정보주체의 권리·의무에 중대한 영향을 미치는 결정의 적용을 유보함으로서 정보주체에게 발생하는 피해를 막고, 해당 결정에 오류가 없는지, 처리한 개인정보는 정확한지 등을 인적 개입을 통해 확인하는 기회를 부여하는 것임

⇨ 따라서, 인공지능(AI)을 활용한 면접만으로 '불합격 결정'을 한 경우, 자동화된 결정에 대한 거부권은 불합격 결정의 적용을 유보하고 인적 개입을 통해 오류 등을 확인하고 재처리하는 조치 의무가 발생하고, '합격 결정'을 해야 하거나 사람이 개입하는 채용절차를 별도로 마련해야 하는 의무가 발생하는 것은 아님

□ 정보주체는 자동화된 결정에 대한 ‘설명 요구’를 해야만 추가 의견 제출을 할 수 있는 것인지?

> ⇨ 법 제37조의2제2항에서는 설명 등을 요구할 수 있도록 하고 있으므로, 자동화된 결정에 대한 설명 요구 없이도 추가 의견을 제출하고 해당 사항에 대한 검토를 요구할 수 있음. 다만, 자동화된 결정에 대한 설명을 제공받은 후 처리 과정에 개인정보를 추가해 줄 것을 요청하는 등의 의견을 제출하여 구체적으로 검토를 요구하는 것이 바람직함

□ 영 제44조의3제3항에 따라 정보주체가 의견을 제출하면 개인정보처리자는 검토를 해야 하는데, 특별한 사정(잘못된 개인정보에 대한 오류 정정, 최신 개인정보의 반영 등)이 없음에도 시스템을 통해 재처리를 해주어야 하는지?

> ⇨ 정보주체가 잘못된 개인정보에 대한 오류 정정이나 최신 개인정보의 반영 등 특별한 사유 없이 재처리를 요구하는 경우에는 정보주체가 제출한 의견(재처리)을 반영할 것인지 여부를 검토한 후 그 검토 결과를 알리는 조치를 할 수 있음

□ 정보주체에게 자동화된 결정에 대한 설명을 했음에도 불구하고, 이해가 되지 않는다는 사유를 들어 알고리즘이나 영업비밀에 해당하는 내용까지 추가로 설명을 요구하는 경우에 그 내용을 설명해야 하는지?

> ⇨ 자동화된 결정에 대한 ‘설명’은 정보주체가 이해하지 못하는 AI 알고리즘에 대한 복잡한 작동 원리나 기술적인 설명을 요구하는 것이 아니며, 개인정보처리자의 영업비밀 또는 기타 재산상의 권리를 부당하게 침해할 우려가 있는 경우 정당한 사유가 있는 것으로 보아 설명 요구를 거절할 수 있음

□ 현재 고객민원 창구를 통해 개인정보 열람이나 정정·삭제, 동의철회 등의 고객민원 처리를 통합하여 운영하고 있는 경우에 별도의 절차를 마련해야 하는 것인지?

> ⇨ 자동화된 결정에 대한 거부·설명 등의 요구절차는 개인정보처리자가 기존에 운영하고 있는 고객민원 처리 절차에 통합하여 운영할 수 있음. 다만, 영 제44조의4제1항에 따라 거부·설명 등을 할 수 있다는 사실과 방법 및 절차를 정보주체가 쉽게 확인할 수 있도록 공개해야 함

□ 자동화된 결정에 대한 공개 사항을 개인정보처리방침에 같이 공개해도 되는 것인지?

> ⇨ 공개사항은 인터넷 홈페이지 등을 통해 공개해야 하므로, 개인정보처리자가 기존에 인터넷 홈페이지에 공개하고 있는 개인정보처리방침에 자동화된 결정의 기준 및 절차 등의 내용을 포함하여 함께 공개할 수 있음

참고 개인정보처리자를 위한 "자동화된 결정" 자율진단표

개인정보처리자를 위한
"자동화된 결정" 자율진단표

「행정기본법」 제20조에 따른 행정청의 **자동적 처분** 및
「신용정보의 이용 및 보호에 관한 법률」 제36조의2에 따른 **자동화평가**는 대상에서 제외됨

Q. '완전히' 자동화된 시스템에 의한 것인지?
※ 인적개입이 형식적 절차에 불과하면 'Yes' 해당
No → 대상 아님 (예시) 실질적인 인적 개입이 있는 경우
Yes ↓

Q. 개인정보를 '처리'하는지?
No → 대상 아님 (예시) 해당 결정 정보주체의 개인정보와 무관한 정보의 처리
Yes ↓

Q. 정보주체의 권리 또는 의무에 영향을 주는 '개인정보처리자'에 의한 '결정'인지?
No → 대상 아님 (예시) 추천에 따라 정보주체가 선택·결정하는 자동화된 맞춤형 광고나 추천 서비스
Yes ↓

Q. 개인정보처리자에 의한 '최종적 결정'인지?
※ 단계적 결정이라도 각 단계에서의 최종적 결정이면 'Yes' 해당
No → 대상 아님 (예시) 최종 결정의 확정 전에 실질적인 인적개입 절차가 존재하는 경우
Yes ↓

'자동화된 결정'에 해당 ↓

조치사항	홈페이지 등에 '기준·절차 및 처리되는 방식 등' 공개
조치사항	정보주체가 ❶'설명 요구'시 간결하고 의미있는 설명 제공 또는 ❷'검토 요구'시 반영 여부·결과 통보

↓

Q. 정보주체의 권리 또는 의무에 '중대한 영향'을 미치는지?
No → 거부권 대상 아님 (예시) 정보주체의 권리 또는 의무에 대해 본질적인 제한이나 박탈 등의 영향이 없는 경우
Yes ↓

Q. 자동화된 결정이 동의, 법률, 계약에 근거한 경우가 아닌지?
No → 거부권 대상 아님 (예시) 자동화된 결정에 대해 동의나 계약 등을 통해 미리 알렸거나 법률에 명확히 규정이 있는 경우
Yes ↓

조치사항	정보주체가 '거부'시 ❶자동화된 결정을 적용하지 않거나 ❷인적 개입에 의한 재처리 후 결과 통보

4 손해배상책임 보장 의무대상자의 범위(법 제39조의7)

1. 개정 개요

□ 「개인정보 보호법」 개정('23.3.14.공포)으로 정보통신서비스 제공자등을 대상으로 하던 '손해배상의 보장' 특례규정(법 제39조의9)이 삭제되고 일반 규정으로 변경됨에 따라,

○ 손해배상책임의 보장 의무 대상이 개인정보처리자로 변경되어 손해배상책임 보장을 위한 보험(공제) 가입 및 준비금 적립 등 의무대상을 조정하였다.

2. 개정 법령

법률	**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. ② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 조치를 하지 아니할 수 있다. 1. 대통령령으로 정하는 공공기관, 비영리법인 및 단체 2.「소상공인기본법」제2조제1항에 따른 소상공인으로서 대통령령으로 정하는 자에게 개인정보처리를 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.
시행령	**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. 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. 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.

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.

■ 개인정보 보호법 시행령 [별표 1의4]

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.

3. 개정내용 해설

□ 손해배상책임의 이행 의무대상이 ‘정보통신서비스 제공자등’에서 모든 ‘개인정보처리자’로 변경되면서,

○ 매출액 및 개인정보 보유 규모의 기준을 현행 ‘매출액 5천만 원’ 및 ‘이용자 수 1천 명’ 이상에서 ‘매출액 10억 원’ 및 ‘정보주체 수 1만 명’ 이상으로 조정하였다.

□ 또한, 법 제39조의7에서의 의무가 면제되는 공공기관, 비영리법인 및 단체, 소상공인으로서 개인정보 처리를 위탁한 자 등에 대한 구체적인 기준을 시행령에 마련하였다.

○ 첫째, 개인정보 보호법상의 공공기관의 경우 원칙적으로 의무적용을 면제하되, 시행령 제2조제2호부터 제5호까지에 해당하는 공공기관으로서 제32조제4항 각 호*의 적용을 받는 공공기관의 경우에는 의무를 적용하도록 하였다.

***시행령 제32조제4항 각 호**

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

○ 둘째,「공익법인의 설립·운영에 관한 법률」제2조에 따른 공익법인,「비영리민간단체 지원법」제4조에 따라 등록한 단체는 의무적용을 면제하였다.

○ 셋째,「소상공인기본법」제2조제1항에 따른 소상공인으로서 아래의 요건을 모두 갖춘 자에게 개인정보 저장·관리업무를 위탁한 경우에 의무를 면제하도록 하였다.

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

○ 넷째, 다른 법률에 따라 법 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립한 개인정보처리자의 경우 의무적용 대상에서 제외하였다.

- 이 경우, 법 제39조의7제1항제3호에 따른 손해배상책임의 이행을 보장하는 경우에 해당하는지 여부는 다른 법률에 따라 가입한 보험 등이 법 제39조 및 제39조의2에 따른 손해배상책임을 담보(보상)하는지, 시행령 별표 1의4에서 정한 최저가입금액기준(최저적립금액기준)을 준수하고 있는지 등을 고려하여 개별적으로 판단하여야 한다.

<손해배상책임 보장 의무대상자 범위>

<table>
<tr><td>일반 기준</td><td colspan="2">①전년도 매출액등이 10억원 이상 + ②정보주체 수 1만명 이상 모두 충족</td></tr>
<tr><td colspan="2">[적용 제외(의무면제)]</td><td>[적용(의무대상)]</td></tr>
<tr><td colspan="2">1. 공공기관
※ 영 제32조제4항에 따라 CPO 지정시 자격요건 의무대상 공공기관*은 제외</td><td rowspan="5">* CPO 지정시 자격요건 의무대상인 공공기관은 손해배상책임 보장 의무적용 대상임
- 시행령 제2조제2호부터 제5호까지에 해당하는 공공기관으로서 시행령 제32조제4항 각 호에 해당하는 공공기관은 적용대상에 포함됨

<시행령 제32조제4항 각 호>
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</td></tr>
<tr><td colspan="2">2. 공익법인의 설립·운영에 관한 법률 제2조에 따른 공익법인</td></tr>
<tr><td colspan="2">3. 비영리민간단체 지원법 제4조에 따라 등록한 단체</td></tr>
<tr><td colspan="2">4. 다음 각호의 요건을 모두 갖춘 자에게 개인정보 처리를 위탁한 「소상공인기본법」 제2조제1항에 따른 소상공인
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</td></tr>
<tr><td colspan="2">5. 다른 법률에 따라 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립한 개인정보처리자</td></tr>
</table>

4. 개인정보처리자 유의사항

□ 시행령 개정으로 의무대상 개인정보처리자의 기준이 변경되었으므로 변경된 기준에 해당하는지 여부를 확인할 필요가 있다.

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

○ 전년도(법인의 경우 직전 사업연도)의 매출액등*이 10억원 이상인 개인정보처리자로서,

* 매출액등 : 매출액과 매출액을 산정하지 않는 경우에는 「법인세법」 제4조제3항제1호에 따른 수익사업에서 생기는 소득을 말함(시행령 제31조의2제1항제1호)

- 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 정보주체(소속 임직원인 정보주체는 제외)의 수가 일일평균 1만명 이상이어야 한다.

- 다만, 해당 연도에 영업의 전부 또는 일부의 양수, 분할·합병 등으로 개인정보를 이전받은 경우에는 이전받은 시점을 기준으로 정보주체의 수를 산정한다.

○ '정보주체 수'는 개인정보처리자가 개인정보를 "저장·관리"하는 정보주체 수를 기준으로 산정한다.

* 정보주체 수 일일평균 = 10월·11월·12월 전체 일일 정보주체 수의 총합 ÷ 92일)

◈ 개인정보 손해배상책임 보장제도에 대한 기존 안내서 개정 예정(~'24.3월)

5. 제재 규정

위반행위	제재 내용
이 법 위반행위에 대해 법 제64조제1항에 따라 시정조치 명령을 받은 후 시정조치 명령에 따르지 아니한 자	3천만원 이하 과태료 (법 제75조제2항제27호)

6. 질의 응답

□ 비영리단체 및 학교 등도 개인정보보호 손해배상책임보험 가입 또는 준비금 적립 의무대상인지?

⇨ 개인정보 보호법 제39조의7에 따라 손해배상책임 이행을 위해 보험 가입 등의 조치 의무가 있는 대상은 '개인정보처리자'이므로 전년도 매출액등이 10억원 이상이면서 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 정보주체 수가 일일평균 1만명 이상인 요건을 충족하는 개인정보처리자의 경우 적용 대상에 해당함(요건 미충족시 의무대상에서 제외)

⇨ 다만, 매출액등이 10억원 이상이고 정보주체 수 1만명 이상인 경우에도, 각급 학교*, 「공익법인의 설립·운영에 관한 법률」 제2조에 따른 공익법인이나 「비영리민간단체 지원법」 제4조에 따라 등록한 단체는 조치 의무가 면제됨

* 재학생 수(대학원생 포함)가 2만명 이상인 대학은 의무적용 대상임

□ 위탁사(A사)를 대신하여 개인정보를 처리하는 수탁사(B사)가 있는 경우, 개인정보는 수탁사의 DB에 저장되고 위탁사는 접근 권한만 부여받은 때에도 보험에 가입하거나 준비금을 적립해야 하는지?

⇨ 개인정보 보호법 제39조의7 규정은 정보주체의 개인정보를 수집·처리하는 개인정보처리자로 하여금 개인정보 유출 등에 따른 손해배상 책임의 이행을 위해 보험 가입 등을 의무화하는 것으로, 개인정보처리자로부터 개인정보 업무를 위탁받은 수탁자에 대해서는 손해배상책임 보험(공제) 가입 또는 준비금 적립 등의 의무가 적용되는 대상에 해당되지는 않으나 위탁한 개인정보처리자는 의무대상에 해당됨

⇨ 다만, 수탁자도 그 자신이 고유업무 수행 등 독립적인 개인정보처리자의 지위에서 개인정보를 저장·관리하는 경우에는 의무대상이 될 수 있음

□ 소상공인이고 홈페이지 운영 및 개인정보 관리를 전문회사에 위탁하고 있는데, 이 경우 보험 가입 등의 의무가 면제되는지?

⇨ 소상공인이 수탁사(예: 클라우드 사업자, 호스팅 사업자 등)에게 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인정보의 저장·관리 업무를 위탁하였고, 해당 수탁자가 위탁받은 업무에 대하여 법 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 한 경우에는 의무가 면제될 수 있음

□ 준비금을 적립(또는 보험가입)한 사실은 어떻게 증빙하는지? 신고 또는 증빙서류의 별도 제출이 필요한지?

⇨ 이행 여부에 대한 신고·보고 의무는 없음. 다만, 향후 이행점검 시에 보험증권, 회계장부, 주주총회 의사록 등이 자료제출 요구 대상이 될 수 있음

5 고유식별정보 관리실태 정기조사(영 제21조)

1. 개정 개요

□ 조사의 필요성이 낮은 경우*에도 매 2년마다 동일한 기관을 대상으로 조사를 반복적으로 실시하고, 다른 조사·점검과 점검항목이 중복되는 등 조사의 실효성이 저하되어 개선 필요성이 증가하였다.

* 각급학교(초중고), 소규모 기관 등 고유식별정보를 보유하지 않거나 보유 건수가 극히 적은 경우 등

○ 이에, 조사 대상기관·조사 주기 등을 합리적으로 조정하였으며, 유사한 점검을 통해 고유식별정보 안전성 확보 조치 이행 여부를 확인하였을 경우 정기조사에 갈음할 수 있는 근거를 신설하는 등 조사의 실효성을 확보하였다.

2. 개정 법령

법률	**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. 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. ⑤ 보호위원회는 대통령령으로 정하는 전문기관으로 하여금 제4항에 따른 조사를 수행하게 할 수 있다.
시행령	**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. ② 법 제24조제4항에서 "대통령령으로 정하는 기준에 해당하는 개인정보처리자"란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다. 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. ④ 다음 각 호의 어느 하나에 해당하는 경우로서 고유식별정보의 안전성 확보 조치에 대한 점검이 이루어진 경우에는 제3항에 따른 조사를 실시한 것으로 본다. 1. 법 제11조의2에 따라 개인정보 보호 수준 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

3. 개정내용 해설

□ 조사대상을 모든 공공기관에서 1만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 공공기관으로 조정하였다.

○ 1만명 미만의 정보주체에 관하여 고유식별정보를 처리하는 공공기관의 경우에도 법 위반 이력 및 내용·정도 등을 고려하여 조사가 필요하다고 인정하는 경우 조사 대상에 포함할 수 있도록 하였다.

□ 고유식별정보 관리실태 정기조사 주기를 기존 2년마다 1회 이상에서 3년마다 1회 이상으로 완화하였다.

□ 고유식별정보 관리실태 정기조사에 준하는 조사·점검 등이 이루어진 경우 정기조사를 실시한 것으로 볼 수 있는 근거를 신설하였다.

○ 법 제11조의2에 따른 개인정보 보호 수준 평가, 법 제32조의2에 따라 개인정보 보호 인증이 이에 해당하며,

○ 그 밖에 다른 법률에 따라 고유식별정보의 안전성 확보 조치 이행 여부에 대한 정기적인 점검이 이루어지는 경우로서 관계 중앙행정기관의 장의 요청에 의해 정기조사에 준하는 것으로 보호위원회가 인정한 경우에도 정기조사를 실시한 것으로 볼 수 있는 근거를 마련하였다.

4. 개인정보처리자 유의사항

□ 보호수준 평가, 개인정보 보호 인증 등을 실시하여 정기조사 예외에 해당하더라도 조사 대상기관에서 완전히 제외되는 것은 아니며, 점검 결과 고유식별정보에 대한 안전조치가 미흡한 경우 차년도 고유식별정보 안전조치 실태조사에 포함될 수 있다.

5. 질의 응답

□ 1만명 이상의 고유식별정보를 처리하는 공공기관만 정기조사의 대상인지?

⇨ 공공기관의 경우에는 1만명 미만의 정보주체에 관하여 고유식별정보를 처리하는 경우라고 하더라도, 보호위원회가 법 위반 이력 및 내용·정도, 고유식별정보 처리의 위험성 등을 고려해 법 제24조제4항에 따른 조사가 필요하다고 인정하는 경우에는 정기조사의 대상이 될 수 있음

⇨ 공공기관 외의 자라도 5만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 개인정보처리자의 경우에는 시행령 개정 전과 동일하게 정기조사의 대상임

□ 시행령 제21조제4항제3호에서 의미하는 다른 법률에 따라 정기적인 점검이 이루어지는 경우에는 어떤 것들이 있는지?

⇨ 다른 법률에 따라 고유식별정보의 안전성 확보 조치 이행 여부에 대한 정기적인 점검이 이루어지는 경우라 하더라도, 관계 중앙행정기관의 장이 「개인정보 보호법」 상의 고유식별정보 관리실태 정기조사에 준하는 것으로 인정해 줄 것을 요청하고, 이에 따라 보호위원회가 인정하는 경우에만 해당함

6 국외 수집·이전에 대한 개인정보 처리방침 공개(영 제31조)

1. 개정 개요

□ 모든 유형의 개인정보 국외 수집·이전에 대해 개인정보 처리 방침에 관련 정보를 기재하도록 정비하였다.

○ 시행령 개정 전에는 정보 주체가 개인정보의 국외 이전에 관한 정보*를 확인하는 방법이 국외 이전 유형별로 달라 정보주체의 혼란을 초래한다는 지적이 있었다.

* 국외 이전의 법적 근거, 이전되는 정보, 이전받는자, 이전 시기, 이전 목적 등

< 참고: 이전 유형별 개인정보 이전 정보 확인 방법(시행령 개정 전) >

국외 이전 유형	국외 이전 정보 확인 방법
국외 이전 동의 획득	국외 이전 동의 시점(서비스 가입시 등)에 확인 가능 이후에는 국외 이전에 대한 상세 내용을 다시 확인하기 어려움
조약 및 타 법령에 근거한 이전	x (확인 불가)
계약에 따른 처리 위탁·보관	개인정보 처리방침을 통해 확인 가능
개인정보 보호 인증 획득 처리자	x (확인 불가)
보호수준이 동등한 국가	x (확인 불가)

○ 또한, 국외에서의 직접 수집의 경우, 개인정보가 국외에서 처리됨에도 불구하고 개인정보가 처리되는 국가에 관한 정보를 정보주체에게 알릴 의무가 없었다.

○ 이에, 시행령 개정을 통해 모든 유형의 국외 수집·이전에 대해 국외 수집·이전 주요 내용을 개인정보 처리 방침에 공개하도록 하였다.

2. 개정 법령

법률	**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 법 제30조제1항제8호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다. 8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항
시행령	**제31조(개인정보 처리방침의 내용 및 공개방법 등)** ① 법 제30조제1항제8호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다. 1. (현행과 같음) 2. 법 제28조의8제1항 각 호에 따라 개인정보를 국외로 이전하는 경우 국외 이전의 근거와 같은 조 제2항 각 호의 사항 3. (현행과 같음) 4. 국외에서 국내 정보주체의 개인정보를 직접 수집하여 처리하는 경우 개인정보를 처리하는 국가명

3. 개정내용 해설

□ 시행령 개정에 따라 아래 항목을 개인정보 처리방침에 작성하여 공개하여야 한다.

구분 / 근거	국외에서 국내 정보주체의 개인정보를 직접 수집하여 처리하는 경우	개인정보를 국외로 이전하는 경우
영 제31조 제1항제2호	-	· 국외 이전 법적 근거 · 이전되는 개인정보 항목 · 개인정보가 이전되는 국가, 시기, 방법 · 개인정보를 이전받는 자의 성명 · 개인정보를 이전받는 자의 개인정보 이용 목적 및 보유·이용기간 · 개인정보의 이전을 거부하는 방법, 절차 및 거부의 효과
영 제31조 제1항제4호	· 개인정보를 처리하는 국가명	-

○ 개인정보의 국외 이전 시 이전 유형(제공, 처리위탁, 보관)에 무관하게 국외 이전의 법적 근거와 함께 법 제28조의8제2항 각호의 사항(국외 이전 동의를 받을 때 알려야 할 사항)을 개인정보 처리 방침에 공개하여야 한다.

사례 **국내 정보주체의 개인정보를 국외로 이전하는 경우**

· (제공) 다국적기업의 한국 법인이 수집한 고객정보를 해외 본사로 이전하는 경우, 또는 다국적기업의 한국 법인 고객DB를 해외 본사에서 조회하는 경우

· (처리위탁) 해외에 자회사인 콜센터를 설립하고 국내 고객DB를 이용해 고객대응 업무를 대행시키는 경우

· (보관) 국내에 저장된 고객 DB를 해외 서버 등에 분산 저장(백업 등)하는 경우

○ 국외에서 국내 정보주체의 개인정보를 직접 수집하여 처리하는 경우는, 한국 정보주체를 대상으로 서비스하는 국외 사업자 등이 자사 개인정보 처리시스템에서 국내 정보주체로부터 개인정보를 직접 수집하는 경우를 의미한다. 이 경우 개인정보를 수집·처리하는 국가에 대한 정보를 개인정보 처리 방침에 공개하여야 한다.

사례 **국외에서 국내 정보주체의 개인정보를 직접 수집하여 처리하는 경우**

· 한국 정보주체를 대상으로 상품을 판매하는 해외 사업자가 회원가입·서비스 이용시 국내 정보주체의 개인정보를 국외에 위치한 자사 시스템에서 직접 수집·처리하는 경우

· 한국 정보주체를 대상으로 게임, 영상 등 서비스를 제공하는 콘텐츠 사업자가 국외에 위치한 자사 시스템에서 직접 개인정보를 수집·처리하는 경우

4. 개인정보처리자 유의사항

□ 모든 종류의 국외 이전은 개인정보 처리방침에 국외 이전 법적 근거 및 국외 이전 관련 주요 내용을 공개해야 한다. 현재 서비스의 국외 이전 유형에 따라 근거 법령 및 개인정보 처리방침 보완 필요 여부를 확인할 필요가 있다.

□ 국내 정보주체의 개인정보를 국외에서 직접 수집하여 처리하는 경우, 개인정보를 처리하는 국가에 대한 정보를 개인정보 처리방침에 기재해야 하는 의무가 신설되었으므로 개인정보 처리방침에 관련 내용을 보완하여야 한다.

□ 개인정보 처리방침 작성에 관한 구체적인 방법은 개인정보 처리방침 작성지침('24.3~4월 예정)을 통해 안내할 계획이다.

5. 제재 규정

위반행위	제재 내용
법 제30조제1항 또는 제2항(제26조8항에 따라 준용되는 경우를 포함한다)를 위반하여 개인정보 처리방침을 정하지 아니하거나 이를 공개하지 아니한 자	1천만원 이하 과태료 (법 제75조제4항제8호)
이 법 위반행위에 대해 법 제64조제1항에 따라 시정조치 명령을 받은 후 시정조치 명령에 따르지 아니한 자	3천만원 이하 과태료 (법 제75조제2항제27호)

6. 질의 응답

□ 개인정보처리자가 법 제28조의8제1항제1호에 따라 개인정보를 국외로 이전한 경우에도 시행령 제31조제1항제2호에 따라 개인정보 처리방침에 작성하고 공개하여야 하는지?

⇨ 개인정보의 국외 이전 관련해서는 언제든 정보주체가 해당 내용을 확인할 수 있도록 개인정보 처리방침에 공개해야 함

□ 국외에서 국내 정보주체의 개인정보를 직접 수집하는 개인정보처리자는 시행령 개정에 따라 어떤 조치를 하여야 하는지?

⇨ 국외에서 국내 정보주체의 개인정보를 직접 수집하는 경우, 이번에 개정되는 시행령 제31조제1항제4호에 따라 개인정보를 처리하는 국가명을 개인정보 처리방침을 통해 공개해야 함

□ 국외에서 국내 정보주체의 개인정보를 직접 수집하는 개인정보처리자는 개인정보 국외 이전에 관한 동의도 받아야 하는지?

⇨ 국외에서 국내 정보주체의 개인정보를 직접 수집하는 것은 개인정보 국외 이전에 해당하지 않으므로, 국외 이전에 관한 정보주체의 동의 획득 의무가 발생하지 않음. 다만, 개인정보 처리방침에 개인정보를 처리하는 국가명을 공개해야 함