

개인정보 처리방침 평가에 관한 고시

[시행 2024. 2. 20.] [개인정보보호위원회고시 제2024-3호, 2024. 2. 20., 제정]

개인정보보호위원회(자율보호정책과), 02-2100-3050

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」 제2조 제2호에 따른 정보통신서비스를 운영할 것

② 보호위원회는 필요한 경우 평가 대상을 선정하기 전에 개인정보처리자에게 제1항 각 호의 평가 대상에 해당 하는지 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 검토 하여 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 이 에 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 평가 결과를 통보받은 날로부터 20일 이내에 별지 서식을 작성하여 보호위원회에 제출하여야 한다.

② 보호위원회는 제1항에 따른 이의신청을 받은 날로부터 30일 이내에 이의신청 내용을 검토하여 타당성이 인정 되는 경우 평가 결과에 반영하여야 하며, 그 결과를 이의신청을 한 자에게 통지하여야 한다. 다만 부득이한 사정 이 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 자 에게 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 이 행 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,2024.2.20.>

이 고시는 발령한 날부터 시행한다. 다만, 제4조제1항제4호의 개정규정은 2024년 3월 15일부터 시행한다.