개인정보 영향평가에 관한 고시

[시행 2024. 4. 3.] [개인정보보호위원회고시 제2024-7호, 2024. 4. 3., 일부개정]

개인정보보호위원회(자율보호정책과), 02-2100-3080

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 다음과 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 개선사항 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 제36조제1항 제1호에 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 평가기관 지정심사위원회(이하 "지정심사위원회"라 한다)를 구성・운영한다.

⑤ 보호위원회는 지정심사위원회의 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.

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 수행능력심사의 세부평가 및 지정기준) ① 평가기관의 영향평가 수행능력심사의 세부평가기준은 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 이행하고 그 결과를 보호위원회에 제출하여야 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 IT기술을 적용하는 경우에는 해당 기술이 개인정보 보호에 미치는 영향에 대한 평가항목을 개발하여 영향평가 시 반영하여야 한다.

제12조(영향평가서의 제출) 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.

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(영향평가 개선사항 이행) 영 제38조제2항에 따라 영향평가서를 제출받은 공공기관의 장은 개선사항으로 지적된 부분에 대한 이행계획 등을 별지 제13호서식에 따라 영향평가서를 제출받은 날로부터 1년 이내에 보호위원회에 제출하여야 한다.

제15조(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,2024.4.3.>

이 고시는 고시한 날부터 시행한다.