

개 인 정 보 보 호 위 원 회

심의 · 의결

의 안 번 호 제2023-008-075호 (사건번호 : 2022조총0031)

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의 결 연 월 일 2023. 5. 10.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 개선을 권고한다.

가. 피심인은 보유 시스템 전반에 대하여 「공공기관 개인정보 유출방지 대책」(‘22.7월)에 따라 개인정보 처리 전반에 대한 점검을 실시하고, 재발방지 대책을 수립하여 이행한다.

나. 피심인은 개인정보책임자와 개인정보취급자를 대상으로 정기적인 개인정보 보호교육을 실시한다.

다. 피심인은 가.부터 나.까지의 권고 조치를 이행하고, 개선권고 통지를 받은 날로부터 60일 이내에 개인정보보호위원회에 이행 결과를 제출한다.

이 유

I. 기초 사실

피심인은 「개인정보 보호법」(이하 “보호법”이라 한다.) 제2조제6호에 따른 공공기관으로, 같은 법 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	종업원 수 (명)

II. 사실조사 결과

개인정보보호위원회는 피심인의 직원이 그룹웨어를 통해 피해자 개인 정보를 조회하여 범행을 저지르는 사건()과 관련 조사를 진행하여, 피심인의 개인정보보호 법규 위반행위와 관련된 다음과 같은 사실을 확인하였다.

1. 행위 사실

가. 개인정보 수집 현황

피심인은 SAP(전사적자원관리 프로그램)를 통해 '22. 9. 27. 기준 아래와 같이 개인정보를 수집·보관하고 있다.

개인정보파일	수집·이용 항목	수집기간	보유건수(명)
재직자 인사정보	(필수) 성명, 사진, 연락처, 주민등록번호 (선택) 주소(주민등록지, 거주지), 학력, 병역사항, 입사전 경력, 자격·면허, 보훈·장애, 직종·직급·직위, 근무기간, 부서, 연말정산내역, 계좌번호, 급여·상여내역, 포상내역 등	'81.10월 ~ 현재	16,631
세금계산서 발급자정보	(필수) 성명, 휴대전화번호, 주소, 이메일주소, 주민등록번호 (선택) 없음	'20. 8월 ~ 현재	3,999

나. 관련 사실관계

1) 주요 경과 및 대응

일시		사고 경과 및 피심인의 대응
2021.	10. 7.	경찰서, 피심인에 전○○ 대상 수사개시 통보* * 『성폭력범죄의처벌등에관한특례법』위반(카메라 등 이용 촬영)
	10. 13.	피심인, 내부 인사규정에 따라 전○○에 대해 직위해제 인사발령
2022.	9. 14.	사고 발생
	9. 19.	피심인, ERP 검색기능에서 주소지 정보가 포함된 '공급업체 정보' 조회 차단
	9. 20.	피심인, 직위해제자에 대한 내부 전산망 접속 차단

Ⅲ. 위법성 판단

1. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련 법 규정

보호법 제29조는 “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.”고 규정하고 있으며, 보호법 시행령 제30조제1항은 “개인정보처리자는 법 제29조에 따라 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호) 및 개인정보 침해사고 발생에 대응하기 위한 접속 기록의 보관 및 위조·변조 방지를 위한 조치(제4호)를 하여야 한다”고 규정하고 있다.

또한 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호, 이하 ‘고시’) 제5조제1항은 “개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여 하여야 한다.”고 규정하고 있고, 제5조제2항은 “개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.”고 규정하고 있으며, 제8조제1항은 “개인정보처리자는 개인정보취급자가 개인정보처리 시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다.”고 규정하고 있다.

나. 위법성 판단

1) 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무담당자에게 차등 부여하여야 하나, 피심인이 ERP에서 전 직원 누구나 타 직원의 주소지(입사시 제출한 주소)를 검색할 수 있도록 한 행위는 보호법 제29조, 시행령 제30조제1항, 고시 제5조제1항 위반에 해당한다.

2) 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보 취급자가 변경되었을 경우, 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하나, 피심인이 직위해제 인사명령 후 해당 직원이 ERP에서 부여받은 접근권한을 지체 없이 말소하지 않은 행위는 보호법 제29조, 시행령 제30조제1항, 고시 제5조제2항 위반에 해당한다.

3) 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 계정, 접속일시, 접속지 정보, 처리한 정보 주체 정보, 수행업무 등을 기록하여야 하나, 피심인이 ERP(웹화면, FIORI)에서 개인정보처리시스템의 접속기록 수행업무 중 수정기록을 보관·관리하지 않은 행위는 보호법 제29조, 시행령 제30조제1항, 고시 제8조제1항 위반에 해당한다.

IV. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반행위에 대해 같은 법 제75조제2항제6호 및 같은 법 시행령 제63조의 [별표2]「과태료 부과기준」에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

보호법 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 제29조 위반에 대해서 1회 위반에 해당하는 과태료인 600만 원을 적용한다.

< 과태료 부과기준, 보호법 시행령 제63조 [별표 2] >

위반행위	근거 법조문	과태료 금액(단위 : 만원)		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중

「개인정보보호법 위반에 대한 과태료 부과기준」(개인정보위 2023. 3. 8. 이하 ‘과태료 부과지침’) 제8조(과태료의 가중)는 “사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다”라고 규정하고 있다.

피심인의 보호법 제29조 위반행위는 과태료 부과지침 제8조 [별표2]의 가중기준에 따라 ‘위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우’로서 기준금액의 10%인 60만 원을 가중한다.

< 과태료 가중기준(제8조 관련) >

기준	가중사유	가중비율
위반의 정도	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내

다. 과태료의 감경

과태료 부과지침 제7조(과태료의 감경)는 “사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.”라고 규정하고 있다.

피심인은 의견제출 기간내 법규 위반행위를 시정 완료하고, 자료제출 등 조사에 적극 협력하였으므로, 과태료 부과지침 제7조 [별표1] 감경기준에 따라 기준금액의 50%인 300만 원을 감경한다.

< 과태료의 감경기준(제7조 관련) >

기준	감경사유	감경비율
조사 협조· 자진 시정 등	1. 과태료의 사전 통지 및 의견 제출 기간 내에 법규 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 50% 이내
	2. 보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액의 40% 이내

라. 최종 과태료

피심인의 보호법 제29조 위반 행위에 대하여 기준금액에서 가중·감경을 거쳐 총 360만 원의 과태료를 부과한다.

< 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
제29조(안전조치의무)	제75조제2항제6호	600	60	300	360

2. 개선 권고

피심인의 보호법 제29조 위반행위에 대해 법 제61조제2항에 따라 다음과 같이 개선을 권고한다.

가. 피심인은 보유 시스템 전반에 대하여 「공공기관 개인정보 유출방지 대책」(21.7월)에 따라 개인정보 처리 전반에 대한 점검을 실시하고, 재발방지 대책을 수립하여 이행한다.

나. 피심인은 개인정보책임자와 개인정보취급자를 대상으로 정기적인 개인정보 보호교육을 실시한다.

다. 피심인은 가.부터 나.까지의 권고 조치를 이행하고, 개선권고 통지를 받은 날로부터 60일 이내에 개인정보보호위원회에 이행 결과를 제출한다.

V. 결론

피심인의 보호법 제29조 위반행위에 대하여 같은 법 제75조제2항제6호에 따른 과태료 부과, 제61조제2항에 따른 개선 권고를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 규정에 따라 그 효력을 상실하고 관할법원(피심인 주소지의 지방법원 또는 그 지원)이 과태료 재판절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

2023년 5월 10일

부위원장 최 장 혁 (서 명)

위 원 강 정 화 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 홍 열 (서 명)

위 원 이 희 정 (서 명)

위 원 지 성 우 (서 명)