개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2022-014-120호 (사건번호 :)

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2022. 9. 14.

주 문

1. 피심인 에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 시정조치를 권고한다.

가. 대표자를 비롯하여 개인정보 보호책임자 및 개인정보 취급자를 대상으로 개인정보 보호 의식 및 역량 제고를 위한 정기적인 교육계획을 세워 제출하고 이에 따라 정기적인 교육을 수행하여야 한다.

나. 금번 안전조치의무 위반행위 관련 재발방지대책을 수립하여 처분통지를 받은 날로부터 40일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은「개인정보 보호법」(이하 '보호법') 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 "공공기관"으로 지방행정, 지방세 등 관련 사무를 처리하고 있는 지방자치단체이다.

< 피심인의 일반현황 >

사업자 등록번호	대표자 성명	주소	직원 수

Ⅱ. 조사 결과

개인정보보호위원회는 개인정보 보호실태 현장조사( )를 통해 피심인의 개인정보보호 법규 위반행위와 관련하여 다음과 같은 사실을 확인하였다.

1. 행위 사실

가. 개인정보의 안전성 확보를 소홀히 한 행위

1) 피심인은 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하지 않고 부서 단위로 부여한 사실이 있다.

2) 피심인은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 접근권한을 변경 또는 말소하여야 하나 이용목적이 종료된 계정(cmctest, test 등)이나 현재 운영하지 않는 계정(localhost, e-biz, remote 등) 등을 점검 및 삭제하지 않은 사실이 있다.

3) 피심인은 개인정보처리시스템에서 권한 부여, 변경, 말소 내역을 기록·보관하지 않은 사실이 있다.

4) 피심인은 개인정보취급자들이 시스템에 접속 시 사용자 별로 계정을 발급하지 않고 업무별 관리자 계정(lifelong, sahahome)을 공유하여 처리하게 한 사실이 있다.

5) 피심인은 개인정보취급자가 외부에서 접근 시 본인확인, 문자 확인 등의 2차 인증수단 등을 시스템에 적용하지 않고 ID·비밀번호로만 접근 가능하게 하는 등 안전한 접속 수단을 적용하거나 안전한 인증수단을 적용하지 않은 사실이 있다.

2. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련법 규정

보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

같은 법 시행령 제30조제1항은 법 제29조에 따른 안전성 확보 조치로서, 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)를 하도록 규정하고 있으며,

시행령 제30조제1항에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시 제2021-2호)」에서 개인정보처리자의 안전성 확보조치 내용을 다음과 같이 구체적으로 정하고 있다.

① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다. (제5조제1항)

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다. (제5조제2항)

③ 개인정보처리자는 접근권한 부여, 변경 또는 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다. (제5조제3항)

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. (제5조제4항)

⑤ 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. (제6조제2항)

나. 위법성 판단

피심인이 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하지 않고 부서 단위로 부여한 점, 이용목적이 종료된 계정이나 운영하지 않는 계정을 점검 및 삭제하지 않은 점,

개인정보처리시스템에서 권한 부여, 변경, 말소 내역을 기록·보관하지 않은 점, 개인정보취급자들이 업무별 관리자 계정을 공유하여 처리하게 한 점, 개인정보취급자가 외부에서 접근 시 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하지 않은 것은「개인정보 보호법」제29조를 위반한 것이다.

Ⅳ. 처분 및 결정

1. 과태료의 부과

피심인의 보호법 제29조 위반에 대해서 같은 법 제75조제2항제6호, 같은 법 시행령 제63조의〔별표2〕「과태료의 부과기준」에 따라 다음과 같이 300만원의 과태료를 부과한다.

가. 기준금액 산정

최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 금액 600만원을 적용한다.

< [별표 2] 과태료 부과기준 > **(단위 : 만원)**

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중

「개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보보호위원회 지침 2021. 1.27. 제정, 이하 '과태료 부과지침') 제8조(과태료의 가중)에 해당하지 않아 기준금액을 유지한다.

다. 과태료의 감경

과태료 부과지침 제7조 [별표1] 감경기준에 따라 의견제출 기간 내 법규 위반 행위를 시정 완료하고, 자료제출 등 조사에 적극 협력한 점을 고려하여 기준 금액의 50%인 300만원을 감경한다.

< 과태료의 감경기준(제7조 관련) >

기준	감경사유	감경비율
위반 정도	정보주체에게 피해가 발생하지 않은 등 위반행위의 결과가 경미하거나, 사소한 부주의 또는 시스템의 오류로 인한 것으로 인정되며 피해발생이 없는 경우	기준금액의 50%이내
조사 협조 · 자진 시정 등	1. 과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 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
	3. 사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 완료하지는 못하였으나 시정 중에 있는 것으로 인정되는 경우	기준금액의 30%이내

* 「과태료 감경률 적용 보고」('21.11.24. 위원회 보고)에 따라 감경률 상한 범위인 50%를 적용

※ 과태료 부과지침 제7조에 따라 과태료의 감경은 기준금액의 50%를 초과할 수 없음

라. 최종 과태료

기준금액 600만원에 가중 및 감경사유를 적용한 **300만원을** 부과한다.

< 최종 과태료 산출내역(안) > **(단위 : 만원)**

개인정보보호법		과태료 금액 (단위:만원)			
위반조항	처분 조항	기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
제29조(안전조치의무)	제75조제2항제6호	600	0	300	**300**

☞ 피심인이 과태료 고지서를 송달받은 날부터 14일 이내에 과태료를 자진납부하는 경우, 100분의 20을 감경함(질서위반행위규제법 제18조 및 같은 법 시행령 제5조 준용)

2. 시정조치 권고

보호법 제64조제4항에 따라 피심인의 보호법 위반행위에 대하여 다음과 같이 시정조치를 권고한다.

가. 대표자를 비롯하여 개인정보 보호책임자 및 개인정보 취급자를 대상으로 개인정보 보호 의식 및 역량 제고를 위한 정기적인 교육계획을 세워 제출하고 이에 따라 정기적인 교육을 수행하여야 한다.

나. 금번 안전조치의무 위반행위 관련 재발방지대책을 수립하여 처분 통지를 받은 날로부터 40일 이내에 개인정보보호위원회에 그 결과를 제출하여야 한다.

Ⅴ. 결론

피심인의 제29조(안전조치의무) 위반행위에 대해 같은 법 제75조(과태료) 제2항 제6호에 따른 과태료 부과 및 제64조(시정조치 등) 제4항에 따른 시정조치 권고를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정 심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

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(당사자 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료 납입 의무를 부담한다.

2022년 9월 14일

위 원 장　　윤 종 인　(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 흥 열　(서 명)

위　　원　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)