개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2022-014-109호 (사건번호 :)

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 의 인 (사업자등록번호 :)

대표자

의결연월일 2022. 9. 14.

주 문

1. 피심인 에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고 수납 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 수행한다.

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 '대표홈페이지' 에서 안전하지 않은 암호알고리즘(MD5)*으로 비밀번호를 저장한 사실이 있다.

* MD5 암호화 알고리즘은 설계상 결함이 발견되어 해당 결함을 통하여 데이터를 변조할 수 있다는 사실이 발표되면서 보안 관련 용도로는 사용하지 않도록 하고 있음

2) 피심인은 '대표홈페이지'에서 '식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무'를 기록하고 있으나, 처리한 정보주체 정보를 남기지 않은

사실이 있다.

3) 피심인은 ‘대표홈페이지’에서 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 사실이 있다.

2. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 피심인에게 예정된 처분에 대한 사전통지서를 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 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용조치(제3호)를 하도록 규정하고 있으며, 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)를 하여야 한다고 규정하고 있다.

시행령 제30조제3항에 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 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다. (제7조제2항)

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위해 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. (제8조제2항)

나. 위법성 판단

1) 개인정보처리자는 비밀번호를 저장하는 경우 복호화되지 아니하도록 안전한 암호알고리즘으로 암호화하여 저장하여야 하나,

- 피심인이 대표 홈페이지에서 정보주체의 비밀번호를 안전하지 않은 MD5 알고리즘으로 저장한 것은 보호법 제29조, 같은 법 시행령 제30조제1항제3호, 개인정보의 안전성 확보조치 기준 제7조제2항을 위반한 것이다.

2) 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위해 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 하나,

- 피심인이 개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 않은 것은 보호법 제29조, 같은 법 시행령 제30조제1항제4호, 고시 제8조제2항을 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 360만원의 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) [별표2] 가중기준에 따라 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상에 해당하는 점을 고려하여 기준금액의 10%인 60만원을 가중한다.

< 과태료의 가중기준(제8조 관련) >

기준	가중사유	가중비율
위반의 정도	1. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개에 해당하는 경우	기준금액의 50% 이내
	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내

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

라. 최종 과태료

기준금액 600만원에 가중 및 감경사유를 적용한 **360만원을** 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	60	300	**360**

☞ 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 수행한다.

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

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 시정조치 권고에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 개인정보보호위원회에 행정심판청구 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)