개 인 정 보 보 호 위 원 회

심의·의결

의 안 번 호 제2021-015-172호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2021. 9. 8.

주 문

1. 피심인 에 대하여 다음과 같이 과태료를 부과한다.

   가. 금 액 : 4,800,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대해 다음과 같이 시정조치를 권고한다.

   가. 피심인은 위반행위와 관련하여 향후 재발방지대책을 수립하여야 한다.

   나. 가의 시정조치 권고를 이행하고, 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

이 유

Ⅰ. 기초 사실

피심인은「개인정보 보호법」(이하 ’ 보호법 ‘) 제2조제5호에 따른 개인정보처리자이고, 같은 법 제2조제6호에 따른 “공공기관”으로

에 따른 이다.

< 피심인의 일반현황 >

대표자	설립 일자	직원 수	자산('20년 기준)	주요서비스

Ⅱ. 조사 결과

개인정보보호위원회는 개인정보 관리실태 현장조사('21. 4. 7.~ 4. 9.)를 통해 피심인의 개인정보보호 법규 위반행위와 관련하여 다음과 같은 사실을 확인하였다.

1. 행위 사실

가. 개인정보에 대한 안전조치의무를 소홀히 한 행위

1) 피심인은 홈페이지와 홈페이지에서, 개인정보취급자가 안전한 비밀번호를 설정하여 이행할 수 있도록 자체수립한 내부관리계획의 비밀번호 작성규칙(문자·숫자 9자리)을 적용하여야 하나 작성규칙에 미달(문자·숫자 6자리)하여 적용한 사실이 있다.

2) 피심인은 홈페이지와 홈페이지

에서 비밀번호를 일정 횟수 이상 잘못 입력하는 경우에 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하지 않은 사실이 있다.

3) 피심인은 외부에서 홈페이지와 홈페이지의 관리자페이지에 접속하려는 경우, 아이디·비밀번호 외에 안전한 접속수단이나 안전한 인증수단을 적용하지 있지 않은 사실이 있다.

4) 피심인은 홈페이지와 홈페이지에서 불법적인 접근 및 침해사고 방지를 위해 일정시간 이상 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되는 조치되고 있지 않은 사실이 있다.

5) 피심인은 홈페이지, 홈페이지 및 홈페이지에서 개인정보의 다운로드 기록을 보관하지 않는 등 개인정보 처리시스템에 접속한 기록을 1년 이상 보관하지 않은 사실이 있다.

6) 피심인은 홈페이지와 홈페이지에 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하지 않은 사실이 있다.

2. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 7.19. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2021. 8. 13. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 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.

나. 보호법 시행령 제30조제1항은 ’개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보조치를 하여야 한다‘고 규정하고 있으며, 각호는 ①개인정보의 안전한 처리를 위한 내부 관리계획의 수립 · 시행(제1호), ②개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호), ③개인정보를 안전하게 저장 · 전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호), ④개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조 · 변조 방지를 위한 조치(제4호), ⑤개인정보 보안프로그램의 설치·갱신(제5호), ⑥개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치(제6호)를 해야 한다고 규정하고 있다.

다. 보호법 시행령 제30조제3항에 근거하여 제정된「개인정보의 안전성 확보조치 기준(고시)」(이하 ‘고시’라 함)에 정한 다음 사항을 지켜야 한다.

1) 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.(고시 제5조제5항)

2) 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못

입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.(고시 제5조제6항)

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

4) 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.(고시 제6조제5항)

5) 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.(고시 제8조제1항)

6) 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다. 1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지 2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시 3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치(고시 제9조)

2. 위법성 판단

가. 개인정보에 대한 안전조치의무(보호법 제29조)를 소홀히 한 행위

1) 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 하나, 피심인의 행위는 제29조 및 같은 법 시행령 제30조제1항제2호, 고시 제5조제5항을 위반한 것이다.

2) 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 하나, 피심인의 행위는 보호법 제29조, 같은 법 시행령 제30조제1항제2호 및 고시 제5조제6항을 위반한 것이다.

3) 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 하나, 피심인의 행위는 제29조 및 같은 법 시행령 제30조제1항제2호, 고시 제6조제2항을 위반한 것이다.

4) 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 하나, 피심인의 행위는 제29조 및 같은 법 시행령 제30조제1항제2호, 고시 제6조제5항을 위반한 것이다.

5) 개인정보처리자는 개인정보처리 시스템에 접속한 기록을 1년 이상 보관·관리하여야 하나, 피심인의 행위는 보호법 제29조 및 같은 법 시행령 제30조제1항제4호, 고시 제8조제1항을 위반한 것이다.

6) 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하나, 피심인의 행위는 보호법 제29조 및 같은 법 시행령 제30조제1항제5호, 고시 제9조를 위반한 것이다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반행위에 대한 과태료는 같은 법 제75조제2항제6호 및 같은 법 시행령 제63조〔별표2〕'과태료의 부과기준' 및「개인정보 보호법 위반에 대한 과태료 부과기준」(2021. 1. 27. 개인정보보호위원회 의결, 이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

보호법 제63조의 [별표2]와 과태료의 부과지침 제6조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 과태료인 600만원을 적용한다.

<「개인정보 보호법」 시행령 [별표2] 2. 개별기준 >

(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 및 감경

1) **(과태료의 가중)** 과태료 부과지침 제8조는 사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲위반의 정도 등)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다고 규정하고 있다.

피심인의 경우, 보호법 제29조(안전조치의무) 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상인 경우에 해당하므로 기준금액의 10%인 60만원을 가중한다.

2) **(과태료의 감경)** 과태료 부과기준 제7조는 사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1] 의 감경기준(▲위반정도, ▲조사협조 및 자진시정 등)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

피심인의 경우 정보주체에게 피해자 발생하지 않은 등 위반행위의 결과가 경미한 점, 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 시정완료한 점, 조사 기간 중 일관되게 행위 사실을 인정하면서 자료제출 등 조사에 적극 협력한 점을 고려하여 기준금액의 30%인 180만원을 감경한다.

다. 최종 과태료

피심인의 보호법 제29조를 위반한 행위에 대해 기준금액에 가중.감경을 거쳐 총 480만원의 과태료를 부과한다.

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

2. 시정조치 권고

가. 피심인은 위반행위와 관련하여 향후 재발방지대책을 수립하여야 한다.

나. 가에 대한 시정조치 권고를 이행하고, 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 같은 법 제75조(과태료)제2항제6호 및 제64조(시정조치 등)제4항에 따라 과태료, 시정조치 권고를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정권고 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날로부터 90일 이내에 행정심판청구 또는 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.

2021년 9월 8일

위 원 장　　윤 종 인　(서 명)

부위원장　　최 영 진　(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)