개 인 정 보 보 호 위 원 회

심의・의결

안건번호 제2022-016-128호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (주)엘지유플러스 (사업자등록번호 :)
서울시 용산구
대표자

의결연월일 2022. 9. 28.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 6,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인의 법 위반행위에 따른 행정처분의 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 피심인의 일반 현황

피심인은 홈페이지( )를 운영하면서 임직원, 대리점 직원 등의 개인정보를 처리하는「개인정보 보호법」(법률 제16930호, 이하 "보호법"이라 함) 제2조제5호에 따른 '개인정보처리자'로 일반현황은 다음과 같다.

< 피심인의 일반현황 >

대 표	사업자등록번호	설립일자	종업원 수	매출액('20년)

Ⅱ. 사실조사 결과

개인정보보호위원회는 개인정보보호 포털에 유출 신고가 접수된 건과 관련하여 현장조사 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 유출 사실

가. 유출 경위 및 규모

신원 미상자( )가 내 하위페이지(.php*)의 취약점을 활용하여 SQL injection 공격을 하여 엘지유플러스의 임직원.대리점직원 등 개인정보(이메일주소, 비밀번호(dummy**, 암호화))가 유출되었다.

*

**

나. 경과 및 대응

일 시	유출 인지·대응 내용
‘21. 12. 9.(목) 19:00	다크웹에 신원 미상자(ID : mont4na)가 LGU+의 정보 3만여 건을 판매한다는 게시물을 게시 * https://raidforums.com/Thread-SELLING-LG-U-KR—162623
20:50	위 내용에 대한 언론보도(디지털데일리)
22:58	다크웹 게시물 샘플 데이터(이메일주소, 비밀번호) 34건을 확보하여 홈페이지의 정보와 일치함을 확인
‘21. 12. 10.(금) 10:46	SQL Injection 공격 스크립트 및 웹로그* 등 분석·확인
11:11	해당 페이지 SQL Injection 취약점 개선 조치 *
12:00	개인정보 유출 신고 및 통지
‘21. 12. 12.(월) ~	전체 홈페이지 취약점 점검 등 재발방지 조치

2. 개인정보보호 법규 위반 행위 사실

가. 개인정보처리시스템의 안전성 확보 조치를 소홀히 한 행위

피심인은 홈페이지 내 하위 페이지(.php)를 로그인 없이 접근 가능하도록 운영하였고 해당 페이지에 SQL Injection 공격을 유발할 수 있는 특수 문자를 차단하지 않는 등 접근 통제에 관한 안전조치를 소홀히 하였다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 개인정보처리시스템의 안전성 확보 조치를 소홀히 한 행위

가. 관련 법령의 규정

보호법 제29조는 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령이 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다고 규정하고 있다.

같은 법 시행령 제30조제1항은 개인정보처리자는 법 제29조에 따라 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)의 안전성 확보 조치를 하도록 규정하고 있고, 시행령 제30조제3항에 따른 안전성 확보 조치의 세부기준인「개인정보의 안전성 확보조치 기준」(고시 제2020-2호) 제6조제3항은 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하도록 규정하고 있다.

나. 위법성 판단

피심인의 홈페이지 하위 페이지가 별도의 통제 없이 접근이 가능하였고 SQL Injection 공격을 유발할 수 있는 특수문자를 차단하지 않은 등 홈페이지에 접근 통제에 관한 조치를 소홀히 한 행위는 보호법 제29조 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반에 대해 같은 법 제75조제2항제6호 및 같은 법 시행령 제63조 [별표2]「과태료의 부과기준」에 따라 600만원의 과태료를 부과한다.

가. 기준금액

피심인은 최근 3년간에 같은 위반행위로 과태료 처분*을 받은 사실이 있어 기준금액은 2회 위반에 해당하는 1,200만원을 적용한다.

* '20.12.9. 舊망법 제28조(개인정보의 보호조치)제1항 위반으로 과태료(1,000만원) 처분

< [별표2] 과태료 부과기준 >

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

나. 과태료의 가중

피심인의 위반행위는 보호법 시행령 [별표2] 과태료 부과기준 1. 일반기준 라.에 규정된 가중할 수 있는 사유에 해당하는 사항이 없으므로 가중 없이 기준금액을 유지한다.

< 과태료의 부과기준 >

1. 일반기준

라. 부과권자는 다음의 어느 하나에 해당하는 경우에는 제2호의 개별기준에 따른 과태료의 2분의 1 범위에서 그 금액을 늘려 부과할 수 있다. 다만, 늘려 부과하는 경우에도 법 제75조제1항부터 제4항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.

1) 위반의 내용·정도가 중대하여 소비자 등에게 미치는 피해가 크다고 인정되는 경우

2) 법 위반상태의 기간이 3개월 이상인 경우

3) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 늘릴 필요가 있다고 인정되는 경우

다. 과태료의 감경

피심인은 과태료 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하여 시정 완료하였고 조사기간 중 일관되게 행위사실을 인정하면서 조사에 적극 협력하였다. 또한 개인정보보호 인증(ISMS-P) 및 정보보호 관리체계 인증(ISMS), 개인정보보호와 관련된 국제 인증(ISO27001)을 받았고 자율규제단체(개인정보보호협회)에 소속된 자로, 개인정보보호 활동을 성실히 수행하고 있으므로 과태료 부과기준에 따라 기준금액의 50%인 600만원을 감경한다.

< 과태료의 부과기준 >

다. 부과권자는 다음의 어느 하나에 해당하는 경우에는 제2호의 개별기준에 따른 과태료의 2분의 1 범위에서 그 금액을 줄일 수 있다. 다만, 과태료를 체납하고 있는 위반행위자에 대해서는 그렇지 않다.

1) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우
2) 위반의 내용·정도가 경미하다고 인정되는 경우
3) 위반행위자가 법 위반상태를 시정하거나 해소하기 위하여 노력한 것이 인정되는 경우
4) 위반행위자가 「중소기업기본법」 제2조에 따른 중소기업자인 경우
5) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 줄일 필요가 있다고 인정되는 경우

라. 최종 과태료

피심인의 보호법 제29조 위반행위에 대해 600만원의 과태료를 부과한다.

< 최종 과태료 산출내역 >

과태료 처분의 근거		과태료 금액 (단위:만원)			
위반 조항	처분 조항	기준금액 (A)	가중액 (B)	감경액 (C)	최종액 D=(A+B-C)
제29조(안전조치의무)	제75조제2항제6호	1,200	-	600	600

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

2. 처분결과의 공표

피심인의 위반행위에 대해 보호법 제66조 및 같은 법 시행령 제61조에 따라 처분결과를 다음과 같이 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1	㈜엘지유플러스	법 제29조	안전성 확보 조치 위반	2022.9.28.	과태료 부과 600만원
2022년 10월 00일 개 인 정 보 보 호 위 원 회					

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반에 대해서 같은 법 제75조(과태료) 제2항제6호와 제66조(결과의 공표)에 따라 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 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

2022년 9월 28일

위 원 장　　윤 종 인　(서 명)

부위원장　　최 장 혁　(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)