개 인 정 보 보 호 위 원 회

심의·의결

안건번호 제2021-020-288호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 ㈜슈빅
서울시 성동구

의결연월일 2021. 12. 8.

주 문

1. 피심인 ㈜슈빅에 대하여 다음과 같이 시정조치를 명한다

가. 처리목적 달성 등으로 불필요하게 된 개인정보를 즉시 파기할 것

나. 개인정보보호법 제29조에 따른 안전조치 의무를 준수할 것

다. 개인정보 처리 업무를 위탁받아 수행하는 경우 「개인정보보호법」 제26조 제7항에 따른 수탁자로서의 의무를 준수할 것

라. 처분통지를 받은 날로부터 30일 이내에 위의 가부터 다까지 사항의 이행결과 및 재발 방지 대책을 제출할 것

2. 피심인 ㈜슈빅에 대하여 다음과 같이 과태료를 부과한다.

가. 금 액 : 6,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

3. 피심인의 법 위반 내용 및 처분 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 피심인의 일반 현황

피심인 ㈜슈빅은 동창회·단체 등의 홈페이지 개발·유지보수 업무 등을 위탁받아 수행하는 사업자로서 개인정보보호법[1](이하 '보호법') 상 개인정보처리 업무 수탁자임과 동시에,

이들 위탁단체 등의 회원을 대상으로 온라인 쇼핑몰을 운영하는 자로서 舊정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '舊정보통신망법') 제2조제1항제3호에 따른 정보통신서비스 제공자이다.

< 피심인의 일반현황 >

대 표	설립일	주요서비스

〈 피심인의 최근 3년간 매출액 현황 (단위 : 천원) 〉

구 분	2017년	2018년	2019년	3년 평균
전체 매출액				
OK 동창 솔루션				
OK 회원제 건강전문몰				

※ 자료 출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성

Ⅱ. 사실조사 결과

개인정보보호위원회[2]는 '20.7.2.일, 7.20일 피심인이 개인정보 유출 사실을 신고한 건과 관련하여 현장조사('20.7.27.~'20.7.30.) 및 관련 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

---

1) 개인정보유출은 現 개인정보 보호법[법률 제16930호] 개정 시행(2020.8.5.) 이전에 발생한 행위로 舊 개인정보 보호법[법률 제14839호, 시행, 2017.10.19.] 및 舊정보통신망 이용촉진 및 정보보호 등에 관한 법률[법률 제16825호, 시행, 2020.06.11.] 적용

2) 現 개인정보 보호법 부칙.
제3조(기능조정에 따른 소관 사무 등에 관한 경과조치) ② 이 법 시행 당시 행정안전부장관의 소관 사무 중 제7조의8의 개정규정에 따른 사무는 보호위원회가 승계한다.
③ 이 법 시행 전에 행정안전부장관이 행한 고시 · 행정처분, 그 밖에 행정안전부장관의 행위와 행정안전부장관에 대한 신청 · 신고, 그 밖의 행위 중 그 소관이 행정안전부장관으로부터 보호위원회로 이관되는 사항에 관한 행위는 보호위원회의 행위 또는 보호위원회에 대한 행위로 본다.

1. 개인정보 수집 현황

피심인은 개 단체로부터 총 개의 홈페이지 개발·유지보수 등을 위탁받아, '20. 7월 기준 명의 개인정보를 저장하고 있으며,

위탁사의 회원들을 대상으로 건강 전문 온라인 쇼핑몰을 운영하면서 별도의 수집 동의 절차를 거친 명의 개인정보를 수집·보관하고 있다.

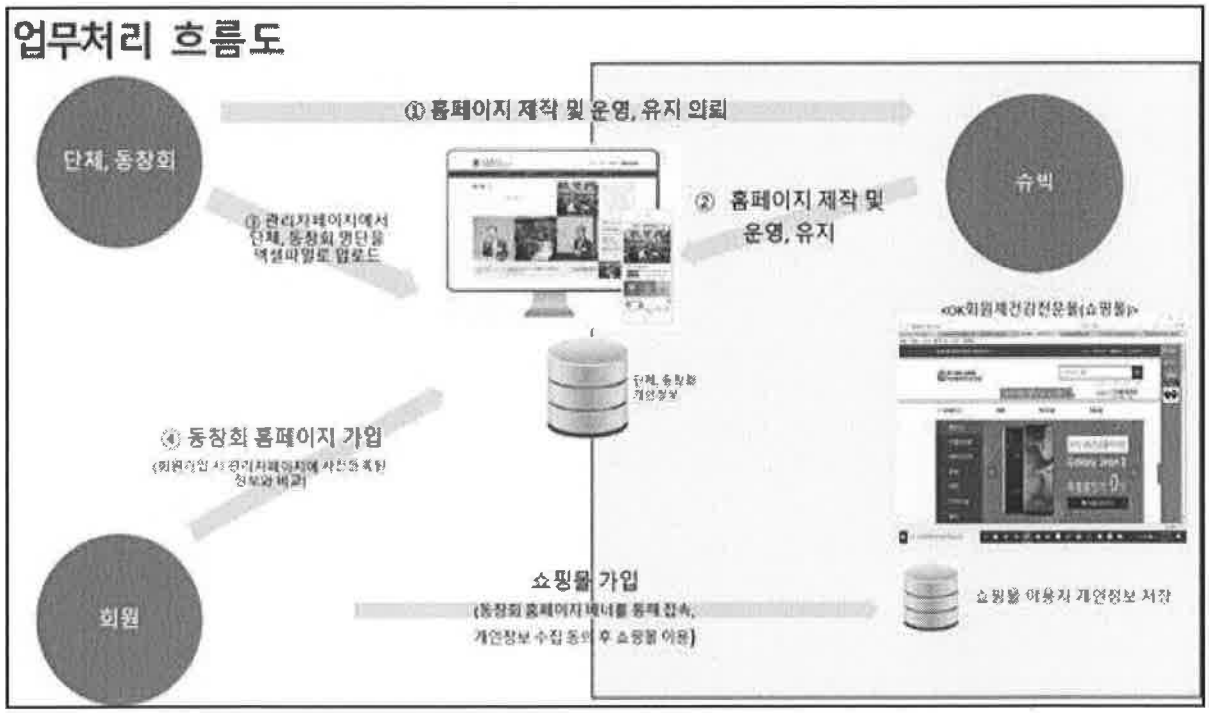
< 개인정보 수집 현황 ('20. 7월 기준)>

구분	항목	수집일	건수
OK동창솔루션 고객정보	이름, 전화번호, 휴대폰번호, 생년월일, 입학·졸업년도, 이메일, 성별, 주소, 직장정보 등*	'11.5.16 ~	
OK회원제건강 전문몰회원정보	이름, 전화번호, 휴대폰 번호, 이메일 등**	'15.3.23 ~	

* 홈페이지별로 개인정보 수집 항목에 차이가 있음

** OK 회원제 건강 전문몰 회원 정보는 OK 동창 솔루션 고객정보와 중복됨

< ※ 참고 : 업무 처리 흐름도 >



2. 개인정보 유출 경과 및 대응

가. 유출 경과 및 대응

<쇼핑몰 개인정보 유출 관련>

- ○ '20. 7. 1. 해커의 협박 메일로 OK회원제 건강 전문몰 개인정보 유출 확인
- ○ '20. 7. 2. 유출 신고 및 사이버 범죄 신고(경찰청)
- ○ '20. 7. 3. 유출사실 통지 및 홈페이지(okdcm.com)에 유출 사실 공지
- ○ '20. 7. 13. OK회원제 건강 전문몰 폐쇄

<동창회 등 위탁사 홈페이지 개인정보 유출 관련>

- ○ '20. 7. 20. 해커의 2차 협박메일로 OK 동창 솔루션 서버에 저장된 회원정보 유출 추가 확인, 위탁사 관리자 게시판에 유출 사실 게시
- ○ '20. 7. 21. 유출 추가 신고 및 새로운 솔루션으로 고객사 홈페이지 이전
- ○ '20. 7. 22. 동창회 등 위탁사 관리자에게 유출 신고 및 통보 등 업무 위임에 관한 사항 안내
- ○ '20. 7. 23. 동창회 등 위탁사 홈페이지에 유출 사실 게시 및 유출 여부 조회 기능 연동 작업 완료
- ○ '20. 7. 24. 위탁사 회원들에게 개인정보 유출 통지

나. 유출 규모 및 경로

신원미상의 해커가 OK동창솔루션의 취약점( )을 이용한 해킹 공격(웹셸[3]로 추정)을 통해 슈빅 서버에 접근하여

온라인 쇼핑몰 고객정보 1,424명, OK동창회 솔루션을 사용하는 239개 단체가 운영 중인 359개 홈페이지의 1,570,986명 개인정보 유출하였다.

---

3) 웹쉘(web shell)은 업로드 취약점을 통해 시스템에 명령을 내릴 수 있는 코드로서, 간단한 서버 스크립트(jsp,php,asp ..)로 만드는 방법이 널리 사용되며, 이 스크립트들은 웹서버 취약점을 통해 업로드되고, 웹쉘 설치 시 해커들은 보안 시스템을 피해 별도 인증 없이 시스템에 접속 가능

< 피심인의 개인정보 유출 현황 >

구분	유출항목	유출 건수
OK 동창 솔루션 고객정보	이름, 전화번호, 휴대폰 번호, 생년월일, 입학·졸업 년도, 이메일, 성별, 주소, 직장정보 등*	1,570,986명
OK 회원제 건강전문몰 회원정보	이름, 전화번호, 휴대폰 번호, 이메일 등	1,424명

* 359개 홈페이지에 따라 유출항목 상이

** OK 회원제 건강 전문몰은 OK 동창 솔루션 고객 대상 쇼핑몰로 유출된 OK 동창 솔루션 고객정보와 중복

3. 행위 사실

가. (OK 동창 솔루션) 수탁자에게 부여된 의무 불이행

1) 계약기간이 종료된 개인정보 미파기

피심인은 계약기간이 종료된 단체 등으로부터 위탁받은 개인정보(8개 단체, 88,090건)를 파기하지 않았다.

2) 안전성 확보에 필요한 조치 미이행

피심인은 취급 중인 개인정보가 인터넷 홈페이지 등을 통해 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 하지 않았다.

* 해커가 피심인이 보유 중인 개인정보 일부를 다크웹에 업로드

나. (OK 회원제 건강 전문몰) 정보통신서비스 제공자로서의 의무 불이행

1) 개인정보의 기술적 · 관리적 보호에 필요한 조치 미이행

피심인은 개인정보처리 시스템에 대한 접속기록을 월 1회 이상 정기 점검하지 않았고, 개인정보취급자 계정 및 접속지 정보를 누락하였으며,

부관리자 계정의 비밀번호를 복호화되지 아니하도록 일방향 암호화하여 저장하지 않고, 평문으로 저장한 사실이 있다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '20.12.15. '개인정보 보호법 위반 행정처분 사전통지' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 'OK회원제 건강쇼핑몰'은 폐쇄하였고, 계약기간이 종료된 단체의 데이터는 모두 삭제하고, 정보 유출 방지 솔루션 도입, 방화벽, IPS 도입, 위탁 홈페이지 무상업그레이드 등 시스템 보완에 가용 가능한 자원을 동원하여 추가 피해가 없도록 노력하고 있다'는 의견을 제출하였다.

Ⅲ. 위법성 판단[4)]

1. (OK 동창 솔루션) 수탁자에게 부여된 의무 불이행 관련

가. 관련 법령의 규정

보호법 제26조제7항은 '수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.'라고 규정하여 수탁자의 법규 준수 의무를 명확히 하고 있다.

과태료 관련 규정에 수탁자를 별도의 처분대상으로 규정하고 있지 않아 과태료 처분은 어려우나, 보호법 제64조제1항은 이 법을 위반한 자에게 시정조치를 명할 수 있도록 하고 있다.

수탁자에게 준용되는 보호법 제21조제1항은 '개인정보처리자는 보유기간이 경과, 개인정보의 처리 목적달성 등 그 개인정보가 불필요하게 된 때에는 지체없이 파기하여야 한다'고 규정하고 있다.

또한, 또 다른 준용 규정인 보호법 제29조는 '개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속

4) 피심인이 수탁자로서 행한 홈페이지 관련 사항은 보호법을, 정보통신서비스 제공자로서 행한 온라인 쇼핑몰 관련 사항은 정보통신망법을 적용함

기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적·물리적 조치를 하여야 한다.'라고 규정하고 있으며,

표준개인정보지침('17.7.26. 시행, 행안부 고시 2017-1) 제17조는 '수탁자는 위탁받은 개인정보 보호를 위해 「개인정보의 안전성 확보조치 기준 고시」에 따른 관리적·기술적·물리적 조치를 하여야 한다.'고 규정하고 있다.

같은 법 시행령 제30조제1항은 법 제29조에 따른 안전성 확보 조치로서, 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행(제1호), 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호), 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호), 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호), 개인정보에 대한 보안프로그램의 설치 및 갱신(제5호), 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치(제6호)를 하도록 규정하고 있고,

시행령 제30조에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준(위원회 고시)」에서 개인정보처리자의 안전성확보 조치 내용을 다음과 같이 구체적으로 정하고 있다.

- (제6조제3항) 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근통제 등에 관한 조치를 하여야 한다.

나. 위법성 판단

피심인은 개인정보처리 업무를 위탁한 8개 단체와의 계약기간이 종료되어 처리기간의 경과, 처리목적 달성 등으로 해당 단체의 개인정보(88,090건)가 불필요하게 되었음에도 이를 지체없이 파기하지 않아 보호법 제21조제1항을 위반하였으며,

또한, 취급 중인 개인정보가 인터넷 홈페이지 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 조치하지 않아 보호법 제29조를 위반하였다.

2. (OK 회원제 건강 전문몰) 정보통신서비스 제공자로서의 의무 불이행 관련

가. 관련 법령의 규정

舊정보통신망법 제28조제1항은 '접속기록의 위조·변조 방지를 위한 조치(3호), 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(4호)를 하도록 규정하고 있으며,

같은 법 시행령 제15조제3항 및 고시 제5조제1항은 접속기록의 위·변조 방지 등을 위해 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하도록 규정하고 있다.

또한, 같은 법 시행령 제15조제4항 및 고시 제6조제1항은 '정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 비밀번호를 일방향 암호화 하여야 한다'라고 구체적으로 규정하고 있다.

나. 위법성 판단

개인정보취급자의 개인정보처리시스템에 대한 접속기록을 월 1회 이상 정기 점검하지 않고, 개인정보취급자 계정 및 접속지 정보를 누락하였으며, 이용자의 비밀번호를 안전한 해쉬함수 등으로 암호화하지 않고 평문으로 저장하는 등 개인정보 보호 조치 의무를 다하지 않은 피심인의 행위는 舊정보통신망법 제28조제1항을 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 시정조치 명령

피심인의 개인정보 미파기, 안전성 확보조치 소홀 등 舊보호법 위반행위에 대해 같은 법 제64조제1항에 따라 아래와 같이 시정조치를 명한다.

① 처리목적 달성 등으로 불필요하게 된 개인정보를 즉시 파기할 것

② 개인정보보호법 제29조에 따른 안전조치 의무를 준수할 것

③ 개인정보 처리 업무를 위탁받아 수행하는 경우 「개인정보 보호법」 제26조 제7항에 따른 수탁자로서의 의무를 준수할 것

④ 처분통지를 받은 날로부터 30일 이내에 ①부터 ③까지 사항의 이행결과 및 재발 방지 대책을 제출할 것

2. 과태료 부과

피심인의 舊정보통신망법 제28조(개인정보의 보호조치) 제1항 위반에 대해 같은 법 제76조(과태료) 제1항제3호 및 같은 법 시행령 제74조(과태료의 부과기준)의 〔별표9〕 「과태료의 부과기준」 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(2018. 7. 4. 방송통신위원회 의결, 이하 '과태료 부과지침') 에 따라 다음과 같이 600만원의 과태료를 부과한다.

가. 기준금액 산정

피심인은 최근 3년간 개인정보의 보호조치 위반으로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 과태료 기준금액 1,000만원을 적용한다.

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
너. **법 제28조제1항**(법 제67조에 따라 준용되는 경우를 포함한다)에 따른 **기술적·관리적 조치를 하지 않은 경우**	법 제76조 제1항제3호	1,000	2,000	3,000

나. 과태료의 가중 및 감경

1) (과태료의 가중) 과태료 부과지침 제8조는 ▲조사방해, ▲위반의 정도 ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우에는, 기준 금액의 2분의 1까지 가중할 수 있다고 규정하고 있다.

이에 따라 피심인의 舊정보통신망법 제28조제1항 위반행위는 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상인 경우에 해당하므로 기준금액의 10%인 100만원을 가중한다.

2) (과태료의 감경) 과태료 부과지침 제7조는 ▲당사자 환경, 사업규모와 자금사정, ▲개인(위치)정보 보호 노력정도 ▲조사 협조·자진시정, ▲기타 위반행위의 정보와 동기, 사업 규모, 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 감경할 수 있다고 규정하고 있다.

이에 따라 피심인의 경우 사전통지 및 의견제출 기간 내에 법규 위반행위를 중지하고, 자료 제출 등 조사에 적극 협력한 점을 고려하여 기준금액의 50%인 500만원을 감경한다.

다. 최종 과태료

피심인의 舊정보통신망법 제28조제1항 위반행위에 대해 기준금액 1,000만원에 10% 가중과 50% 감경을 적용한 **600만원의 과태료를 부과**한다.

< 최종 과태료 산출내역 >

근거법령		과태료 금액 (단위 : 만원)			
위반 조항	위반내용	기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) =(A+B+C)
법 §28①	**개인정보 보호조치 위반** (접속기록, 암호화)	1,000	100	△500	600
계					600

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

3. 처분결과의 공표

피심인의 위반행위가 보호법 제66조제1항, 같은 법 시행령 제61조에 해당함에 따라 피심인의 처분결과를 다음과 같이 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 및 (구)정보통신망법 위반 행정처분 결과 공표					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1	㈜슈빅	개인정보 보호법 제21조제1항	개인정보 미파기	2021.12.08	시정조치 명령
		개인정보 보호법 제29조	안전조치 미이행	2021.12.08	시정조치 명령
		정보 통신망법 제28조제1항	개인정보보호 조치 미이행 (접속기록, 암호화)	2021.12.08	과태료 600만원
2021년 0월 00일 개 인 정 보 보 호 위 원 회					

V. 결론

피심인이 보호법 제21조제1항, 제29조를 위반한 행위에 대하여 같은 법 제64조제1항 의한 시정명령, 舊정보통신망법 제28조제1항을 위반한 행위에 대하여 같은 법 제76조제1항에 의한 과태료, 10만명 이상의 개인정보가 유출된 것에 대해 보호법 제66조에 의한 처분결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 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 12월 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)

개 인 정 보 보 호 위 원 회

심의·의결

안건번호 제2021-020-289호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 청주시자원봉사센터
충청북도 청주시

의결연월일 2021. 12. 8.

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 위반의 내용 및 처분 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 피심인의 일반 현황

피심인은 청주지역 자원봉사활동 지원 업무 수행을 위해 청주시가 설치·운영하는 비영리 단체로서 「개인정보보호법[1]」(이하 "보호법"이라 함) 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

대표자 (센터장)	설립일자	2020년 예산 (단위: 천원)	주요 활동	직원수
김우혁	2014.7.1.		청주지역 자원봉사자 관리·지원	10명

Ⅱ. 사실조사 결과

개인정보보호위원회[2]는 2020. 8월에 개인정보보호 포털에 유출신고가 접수된 건과 관련하여 사실조사(2020.12.9. ~ 12.11.) 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 수집·이용 현황

피심인은 행정안전부가 개발·제공하는 자원봉사포털(www.1365.go.kr) (이하 "자원봉사포털"이라 함)에 가입된 청주시 자원봉사자 178,725명의 개인정보를 보유하고 있다('20.11.말 기준)

---

1) 개인정보유출은 現 개인정보 보호법[법률 제16930호] 개정 시행(2020.8.5.) 이전에 발생한 행위로 舊 개인정보 보호법[법률 제14839호, 시행, 2017.10.19.] 적용되고, 통지지연은 現 개인정보 보호법 개정 시행 이후에 발생한 행위로 현행법 적용

2) 現 개인정보 보호법 부칙.
제3조(기능조정에 따른 소관 사무 등에 관한 경과조치) ② 이 법 시행 당시 행정안전부장관의 소관 사무 중 제7조의8의 개정규정에 따른 사무는 보호위원회가 승계한다.
③ 이 법 시행 전에 행정안전부장관이 행한 고시·행정처분, 그 밖에 행정안전부장관의 행위와 행정안전부장관에 대한 신청·신고, 그 밖의 행위 중 그 소관이 행정안전부장관으로부터 보호위원회로 이관되는 사항에 관한 행위는 보호위원회의 행위 또는 보호위원회에 대한 행위로 본다.

< 개인정보 보유 현황 >

구 분	항 목	건수
자원봉사포털 회원 중 청주시 자원봉사자 정보	이름, 성별, 생년월일, 아이디, 비밀번호, 주소, 휴대폰번호, 유선전화번호, 이메일주소	

2. 개인정보 유출 경위

가. 유출 경과 및 대응

- '20.6.26. 청주지방검찰청에서 별건 수사 중 확인된 청주시 자원봉사자 리스트 관련하여 피심인 PC를 압수수색하여 피심인이 유출 사고 처음 인지
- '20.7.27. 언론보도를 통해 자원봉사자 개인정보 3만여건 유출 사실 인지
- '20.7.31. 피심인 홈페이지에 개인정보 유출 사과문 팝업 공지
- '20.8.4. 한국인터넷진흥원에 유출 신고
- '20.10.16. 청주지방검찰청으로부터 유출된 개인정보 명단 입수(31,314명)
- '20.11.19. 개인정보 유출 통지(문자/휴대폰번호 확인자 24,987명)
- '20.12.2. 피심인 홈페이지에 개인정보 유출 팝업 공지
- '20.12.4. 개인정보 유출 추가 통지(우편/주소 확인자 5,813명)

나. 유출 경위 및 규모

피심인의 직원이 자원봉사포털에서 청주지역 자원봉사자 리스트를 엑셀파일로 다운로드('20.2.26., 171,294명)하여 국회의원 정○○ 선거캠프에 제공(31,314명)하였고, 이로 인해 청주시 자원봉사자 31,314명의 이름, 성별, 생년월일, 집전화번호, 휴대전화번호, 주소 등의 개인정보가 유출되었다.

3. 개인정보보호 법규 위반 행위 사실

가. 안전성 확보에 필요한 조치 미이행

피심인은 내부관리계획을 수립하지 아니하고 있다가 유출 사고 발생 이후인 2020.8.6.에 내부관리계획을 제정하였고,

자원봉사포털의 개인정보처리시스템에 대한 접속기록을 점검하지 아니하고, 다운로드 사유를 확인하지 아니하였으며,

개인정보처리시스템에 대한 접근 권한을 차등 부여하지 아니하였다.

나. 개인정보 유출 사실 통지 지연

피심인은 2020.10.16. 청주지방검찰청으로부터 유출된 개인정보 명단을 입수한 후 30여일이 경과한 2020.11.19.부터 해당 정보주체에게 유출 사실을 통지하였다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021.6.9. '개인정보 보호법 위반 행정처분 사전통지' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 '국가·지자체 보조금으로 운영되는 비영리기관으로 과태료 예산확보가 어렵고, 전문지식·경험 부족으로 대응이 미흡했으나, 미비점을 모두 보완, 적극적인 재발 방지 노력을 하고 있는 점을 감안, 선처를 요망한다'는 의견을 2021.6.23.에 제출하였고, 2021.12.7.에 개선 현황을 포함한 추가의견서를 제출하였다.

Ⅲ. 위법성 판단

1. 안전성 확보 조치 미이행

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·물리적 조치를 하여야 한다."라고 규정하고 있다.

같은 법 시행령 제30조제1항에서는 '개인정보의 안전한 처리를 위한 내부관리계획의 수립·시행'(1호), '개인정보에 대한 접근 통제 및 접근 권한의 제한'(2호) 등의 안전성 확보조치를 규정하고 있다.

보호법 제29조 및 같은 법 시행령 제30조제3항에 따라 안전성 확보 조치에 필요한 기술적·관리적 및 물리적 안전조치에 대한 최소한의 기준을 정하는「개인정보의 안전성 확보조치 기준」(행정안전부고시 제2019-47호)의 제4조제1항, 제5조제1항, 제8조제2항에서 관련 내용을 규정하고 있다.

나. 위법성 판단

피심인이 ①내부관리계획을 수립하지 아니하고, ②개인정보에 대한 접근 권한 제한조치를 취하지 아니하고, ③개인정보처리시스템의 접속기록을 월 1회 이상 점검하지 아니하고, 다운로드 사유를 확인하지 않은 것은 보호법 제29조 및 같은 법 시행령 제30조제1항 위반에 해당한다.

2. 개인정보 유출 통지 지연

가. 관련 법령의 규정

보호법 제34조제1항에서는 개인정보처리자는 개인정보가 유출된 사실을 알게 된 때에는 지체없이 해당 정보주체에게 관련 사실을 알리도록 규정하고 있고,

「표준 개인정보 보호지침」제26조제1항은 개인정보처리자는 개인정보가 유출되었음을 알게 된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 알리도록 규정하고 있다.

나. 위법성 판단

유출된 개인정보 명단을 확보('20.10.16.)한 후 지체없이 통지하지 아니하고 30여 일이 경과한 '20.11.19.부터 순차적으로 통지한 피심인의 행위는 보호법 제34조제1항 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 및 제34조제1항 위반에 대해서 같은 법 제75조제2항 제6호 및 제8호, 같은 법 시행령 제63조의 [별표2]「과태료의 부과기준」에 따라 다음과 같이 총 600만원의 과태료를 부과한다.

가. 기준금액

피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 위반행위별 1회 위반에 해당하는 600만원(총 1,200만원)을 적용한다.

< (舊)과태료 부과기준 2. 개별기준 >

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
타. 법 제29조를 위반하여 안전성확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400

< 과태료 부과기준 2. 개별기준 >

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
처. 법 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제8호	600	1,200	2,400

나. 과태료의 가중

피심인의 위반행위는 과태료의 부과기준 1. 다.[3]에 따른 가중할 수 있는 사유에 해당하지 않으므로 가중을 하지 않고 기준금액을 유지한다.

3) 개정전 시행령 기준이며 현행 시행령(2020.8.4.개정) 기준으로는 <과태료 부과기준 1.라.>에 해당하고, 일부 표현상의 차이를 제외하고 내용은 동일함

< 과태료의 부과기준 1. 다. >

1. 일반기준

다. 행정안전부장관 또는 관계 중앙행정기관의 장은 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 부과금액의 2분의 1의 범위에서 그 금액을 가중할 수 있다. 다만, 가중할 사유가 여러 개인 경우라도 법 제75조제1항부터 제3항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.

1) 위반의 내용 및 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 가중할 필요가 있다고 인정되는 경우

다. 과태료의 감경

피심인의 위반행위가 피심인의 사소한 부주의로 발생하였고 추가 피해가 없으며, 현장조사 이전에 위반 사항을 모두 시정한 점을 고려하여, 과태료 부과기준에 따라 위반행위별 기준금액의 50%인 300만원(총 600만원)을 감경한다.

< 과태료의 부과기준 1. 나.[4] >

1. 일반기준

나. 행정안전부장관 또는 관계 중앙행정기관의 장은 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 부과금액의 2분의 1의 범위에서 그 금액을 감경할 수 있다. 다만, 과태료를 체납하고 있는 위반행위자의 경우에는 그러하지 아니하다.

1) 위반행위자가 「질서위반행위규제법 시행령」 제2조의2제1항 각 호의 어느 하나에 해당하는 경우
2) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우
3) 위반행위자가 위법행위로 인한 결과를 시정하였거나 해소한 경우
4) 위반행위자가 「중소기업기본법」 제2조에 따른 중소기업자인 경우
5) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우

4) 개정전 시행령 기준이며 현행 시행령상 대응 조항인 < 과태료의 부과기준 1.다. >의 내용은 다음과 같음

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 및 제34조제1항 위반 행위에 대해 위반행위별 기준금액 600만원에서 50%를 감경한 300만원(총 600만원)을 부과한다.

< 최종 과태료 산출내역 >

과태료 처분의 근거		과태료 금액 (단위 : 만원)			
위반조항	위반내용	기준 금액(A)	가중액 (B)	감경액 (C)	최종액 (D=A+B+C)
법 §29	안전성 확보에 필요한 조치를 하지 않은 경우	600	-	△300	300
법 §34①	(유출 시) 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	600	-	△300	300
계		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. 공표

피심인의 위반행위가 보호법 제66조 및 같은 법 시행령 제61조에 해당함에 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	청주시자원봉사센터	법 제29조	안전성 확보조치 미흡	2021.12.8.	과태료 부과 300만원
		법 제34조제1항	유출통지 지연	2021.12.8.	과태료 부과 300만원
2021년 12월 8일 개 인 정 보 보 호 위 원 회					

V. 결론

피심인의 보호법 제29조 및 제34조제1항 위반에 대하여 같은 법 제75조제2항 제6호 및 제8호, 제66조 및 법 시행령 제63조 및 제61조에 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(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 12월 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)

개 인 정 보 보 호 위 원 회

심의 · 의결

안건번호 제2021-020-290호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 사단법인 한국정보산업연합회
서울시 강남구

의결연월일 2021. 12. 8.

주 문

1. 피심인 사단법인 한국정보산업연합회에 대하여 다음과 같이 과태료를 부과한다.

   가. 금 액 : 6,600,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인의 법 위반 내용 및 처분 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 피심인의 일반 현황

피심인은 SW 산업과 지식정보 산업의 발전 및 활용 확산추진, 인력육성, 관련 업계 및 단체 의견수렴을 위해 설립된 과기정통부 소관 비영리법인으로 일반현황은 다음과 같다.

< 피심인의 일반현황 >

대 표	설립일자	주요서비스

Ⅱ. 사실조사 결과

개인정보보호위원회는 '21.3.8. 피심인이 개인정보 유출 사실을 신고한 건과 관련하여 현장조사('21.4.14.~'21.5.10.) 및 관련 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 수집 현황

피심인은 임베디드 SW·System산업협회* 홈페이지(kessia.kr)를 운영하면서 건의 개인정보를 처리하고 있다.

* 한국정보산업연합회 산하기구

< 개인정보 수집 현황 >

구분	항목	수집보유기간	건수
홈페이지 회원정보	(필수) 이름, 이메일 주소, 휴대폰번호, 아이디 (선택) 회사명, 부서, 직위, 전화번호, 주소, 생년월일, 성별, 홈페이지 주소	'17.10.10~ '21.2.23	
행사 참석자 정보	(필수) 이름, 이메일 주소, 휴대폰 번호 (선택) 회사명, 부서, 직위, 전화번호, 팩스 번호	연도 확인 불가 (13년~15년 추정)	
계			

* 탈퇴회원의 개인정보는 삭제하고 ID, 탈퇴 여부만 DB에 기록

2. 개인정보 유출 경과 및 대응

가. 유출 경과 및 대응

○ '21. 3. 8. 다크웹에 내부정보가 공개된 사실을 한국인터넷진흥원으로부터 통보받고 유출 사실 확인* 후 신고

* 다크웹에 공개된 정보(이메일, 휴대폰번호)와 홈페이지 DB 비교・분석

○ '21. 3. 9. 홈페이지 공지 및 유출된 회원들에게 유출 사실 통지(이메일, 문자)

○ '21. 5. 7. 조사 과정에서 행사 참석자의 개인정보 유출 사실 추가 확인

○ '21. 5. 12. 유출된 행사 참석자에게 유출 사실 통지(이메일, 문자)

나. 유출 규모 및 경로

신원 미상자(러시아, 45.145.164.176)가 게시판 취약점을 이용한 해킹 공격(SQL Injection[1])을 하여 홈페이지(kessia.kr) DB를 조회하고 유출하였다.

'20. 11월부터 다크웹에 동 기관의 회원정보(이름, 아이디, 이메일, 전화번호, 휴대폰번호, 회사명, 직위 등) 3,587건, 행사 참석자 정보(이름, 이메일, 회사명, 부서, 직위) 19,841건이 유출되어 있었고, '21.3월 공개된 91개의 DB 중 홈페이지 회원정보 테이블에서(V_member) 3,584건(탈퇴회원 포함 이메일, 비밀번호), 행사 참석자 테이블(cevent_app)에서 19,784건(이메일주소)의 개인정보 유출을 확인하였다.

3. 행위 사실

가. 보유기간이 지난 개인정보 미파기

피심인은 2013년~2015년에 수집한 것으로 추정되는 행사 참석자의 개인정보(이름, 이메일, 휴대폰번호, 전화번호, 회사명, 직급 등) 19,841건을 보유기간(개인정보처리방침 상 등록시점 부터 12개월)이 지났음에도 삭제하지 않고 cevent_app 테이블에 보관하였다.

---

1) SQL Injection(structured query language injection) 웹사이트 보안상 허점을 이용해 특정 SQL쿼리문을 전송하여 공격자가 원하는 DB의 정보를 가져오는 해킹 기법

나. 홈페이지 시스템의 안전성 확보조치 소홀

피심인은 취급 중인 개인정보가 홈페이지 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템 등에 접근 통제 등에 관한 조치를 하여야 하나, 이를 소홀히 하여 회원정보와 행사참석자 정보 등이 다크웹에 유출되었으며,

비밀번호를 안전하지 않은 암호화 알고리즘인 SHA-1[2]을 사용하여 저장하여 비밀번호가 복호화되어 다크웹에 공개되었다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '21. 7. 9. '개인정보 보호법 위반 행정처분 사전통지' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 '확인된 위반사항에 대해서 보유기간 지난 개인정보파일 삭제, 안전한 암호화 알고리즘 도입 등 위반사항에 대한 개선완료 및 홈페이지 시스템 재정비 및 개인정보 관리시스템(클라우드) 도입을 추진 중에 있으며, 개인정보 관련 내부통제 강화와 정기적인 교육 실시 등 재발방지를 위한 노력을 기울이겠다'는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련 법령의 규정

보호법 제21조제1항에서는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체없이 그 개인정보를 파기하도록 규정하고 있다.

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·물리적 조치를 하도록 규정하고 있다.

2) SHA-1(Secure Hash Algorithm-1) 미국의 국가안보국 NSA가 메시지 다이제스트(MD) 방식으로 고안한 암호 해시 암고리즘, 1995년 미국 표준(FIPS PUB 180-1)으로 채택하였으나 2005년 취약점이 제기됨 (IT용어사전, 한국정보통신기술협회)

같은 법 시행령 제30조제1항은 법 제29조에 따른 안전성 확보 조치로서, 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행(제1호), 개인정보에 대한 접근통제 및 접근 권한의 제한 조치(제2호), 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호), 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)를 하도록 규정하고 있고,

시행령 제30조에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준(위원회 고시)」에서 개인정보처리자의 안전성 확보조치 내용을 다음과 같이 구체적으로 정하고 있다.

- (제6조제3항) 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근통제 등에 관한 조치를 하여야 한다.
- (제7조제5항) 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

2. 위법성 판단

2013년~2015년에 수집한 것으로 추정되는 행사참석자 개인정보 19,841건을 보유기간(등록 시점부터 12개월)이 지났음에도 파기하지 않은 피심인의 행위는 보호법 제21조제1항 위반에 해당한다.

취급 중인 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템에 접근통제 등에 관한 조치를 하지 않았고, 개인정보취급자의 비밀번호를 안전하지 않은 암호화 알고리즘을 사용하여 저장하는 등 홈페이지 시스템의 안전성 확보에 필요한 조치를 다하지 않은 피심인의 행위는 보호법 제29조 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제21조제1항, 제29조 위반에 대해 같은 법 제75조제2항제4호, 제6호, 같은 법 시행령 제63조 및 [별표2] 과태료 부과기준에 따라 다음과 같이 660만원의 과태료를 부과한다.

가. 기준 금액

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

< [별표2] 과태료 부과기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만원)		
		1회 위반	2회 위반	3회 이상 위반
마. 법 제21조제1항·제36조의6(제39의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제4호	600	1,200	2,400
자. 법 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중

피심인의 위반행위는 제29조에 따른 안전성 확보에 필요한 조치를 2개 위반*하여 과태료의 부과기준에 따라 기준금액의 10%인 60만원을 가중한다.

* ①접근통제 및 접근권한 제한 미조치, ②암호화 미적용

<과태료의 부과기준 1. 라.>

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) 위반기간이 3개월 이상인 경우

3) 그 밖에 위반행위 정도, 동기와 그 결과 등 고려하여 과태료를 늘릴 필요가 있다고 인정되는 경우

다. 과태료의 감경

피심인은 사전통지·의견제출 기간 내 위법행위를 중지·시정완료하거나 시정 중에 있으며, 조사기간 중 행위사실을 인정하면서 자료제출·진술 등 조사에 협력하였고 그 위반행위에 고의가 없는 점 등을 고려하여 과태료 부과기준에 따라 위반행위 별 기준금액의 50%씩 총 600만원을 감경한다.

< 과태료의 부과기준 1. 다. >

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

피심인이 보호법 제21조 제1항 및 제29조를 위반한 행위에 대해 660만원을 부과한다.

< 최종 과태료 산출내역 >

근거법령		과태료 금액 (단위 : 만원)			
위반 조항	위반내용	기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) =(A+B+C)
법 §21①	개인정보 미파기	600	-	△300	300
법 §29	안전조치 의무 위반	600	60	△300	360
계		1,200	60	△600	660

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

2. 처분 결과의 공표

피심인의 위반행위가 보호법 제66조제1항, 같은 법 시행령 제61조에 해당함에 따라 피심인의 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	사단법인 정보산업연합회	법 제21조제1항	개인정보의 파기 위반	2021.12.08	과태료 부과 300만원
		법 제29조	안전성 확보조치 미흡	2021.12.08	과태료 부과 360만원
2021년 00월 00일 개 인 정 보 보 호 위 원 회					

V. 결론

피심인의 보호법 제21조제1항 및 제29조 위반에 대하여 같은 법 제75조제2항제4호, 제6호 및 법 시행령 제63조에 따른 과태료, 보호법 제66조에 의한 공표를 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(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 12월 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)

개 인 정 보 보 호 위 원 회

심의·의결

안건번호 제2021-020-291호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 협회

서울시

대표

의결연월일 2021. 12. 8.

주 문

피심인 에 대하여 다음과 같이 과태료를 부과한다.

가. 금 액 : 3,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 등을 하는 비영리법인으로 일반 현황은 다음과 같다.

< 피심인 일반현황 >

대 표	설립일자	자본('20년)	매출액('20년)	주요서비스	종업원 수

Ⅱ. 사실조사 결과

개인정보보호위원회는 2021.4.21. 피심인이 개인정보 유출 사실을 신고한 건과 관련하여 현장조사(2021.5.11.~2021.5.13.) 및 관련 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 수집 현황

피심인은 홈페이지를 운영하면서 총 명의 개인정보를 수집·보관하고 있다.('21.5월 기준)

< 개인정보 보유 현황 >

구 분	내용	항 목	수집기간	수집건수
대표 홈페이지	개인 회원	(필수) 아이디, 이름, 휴대폰번호, 생년월일, 이메일	'08.1월 ~ 현재	
	기관 회원	(필수) 아이디, 이름, 휴대폰번호, 이메일주소 (선택) 직장명		
총 계				

2. 개인정보 유출 경과 및 대응

가. 유출 경과 및 대응

○ '21. 4. 21. 한국인터넷진흥원의 통지(민원인 신고)를 통해 관련 내용 인지

○ '21. 4. 21. 해당 웹페이지 접근 차단 조치

○ '21. 4. 21. 유출 신고

○ '21. 4. 23. 통지(홈페이지 공지, 이메일 통지)

○ '21. 5. 3. 통지(이메일 전송 실패자 및 휴대전화만 등록된 자에 대해 문자 발송)

나. 유출 규모 및 경로

홈페이지 회원정보를 조회할 수 있는 웹페이지*가 접근통제 조치 없이 운영되어 인터넷 검색엔진(bing.com)에서 해당 웹페이지가 노출되었고, 웹서버 로그 분석('18.3.30. ~ '21.5.1.) 결과, 최소 12개 외부 IP에서 해당 웹페이지에 접근, 개인정보를 조회한 것으로 나타났다.

---

3. 행위 사실

가. 홈페이지 시스템의 안전성 확보에 필요한 조치 의무 위반

피심인은 내부 관리계획을 수립·시행함에 있어 법에 정한 사항인 위험도 분석 및 대응방안 마련에 관한 사항, 재해 및 재난대비 개인정보처리시스템의 물리적 안전조치에 관한 사항을 누락하고, 홈페이지의 관리자페이지 접근 시 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근을 제한하는 조치를 하지 않았다.

또한 개인정보취급자가 정보통신망을 통해 외부에서 홈페이지 관리자페이지에 접속하려는 경우 가상사설망(VPN) 또는 전용선 등 안전한 접속수단 또는 인증수단을 적용하지 않고, 홈페이지에서 주민등록번호를 처리하면서 취약점 점검을 실시하지 않았으며, 주민등록번호, 비밀번호를 정보통신망을 통하여 송신하는 경우 이를 암호화하지 않았다.

피심인은 홈페이지 관리자페이지에 접속한 기록을 보관하지 않고 개인정보(홈페이지 회원정보)를 조회할 수 있는 웹페이지*에 대해 접근 통제 조치를 하지 않아 외부에 노출된 사실이 있다.

---

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021.6.11. '개인정보 보호법 위반 행정처분 사전통지' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 '확인된 위반 사항에 대해서는 대부분 중지, 개선완료하였고 일부는 현재 개발 중인 차세대 통합정보 관리시스템(홈페이지 포함)에 반영하여 개선 진행 중임. 아울러 사이버안전센터를 통해 시스템, 웹취약점 분석을 진행하여 조치하였으며, 재해·재난 및 보안 관련 예산을 추가로 확보하는 등 향후 개인정보 보호 조치를 지속적으로 철저히 이행하겠다'는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련 법령의 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·물리적 조치를 하도록 규정하고 있다.

같은 법 시행령 제30조제1항은 법 제29조에 따른 안전성 확보 조치로서, 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행(제1호), 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호), 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호), 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)를 하도록 규정하고 있고,

시행령 제30조에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준(위원회 고시)」에서 개인정보처리자의 안전성 확보 조치 내용을 다음과 같이 구체적으로 정하고 있다.

△ (제4조제1항) 개인정보처리자는 위험도 분석 및 대응방안 마련에 관한 사항(제12호), 재해 및 재난대비 개인정보처리시스템의 물리적 안전조치에 관한 사항(제13호)를 포함하여 내부 관리계획을 수립·시행하여야 함

▵ (제5조제6항) 개인정보처리자는 개인정보취급자가 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 함

▵ (제6조제2항) 개인정보처리자는 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 함

▵ (제6조제3항) 개인정보처리자는 취급중인 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 함

▵ (제6조제4항) 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 함

▵ (제7조제1항) 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 함

▵ (제8조제1항) 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 함

2. 위법성 판단

내부 관리계획에 법에 정한 사항(위험도 분석 및 대응방안, 재해 및 재난대비 개인정보처리시스템의 물리적 안전조치)을 누락하고 홈페이지 관리자페이지 접근하려는 경우 가상사설망(VPN) 또는 전용선 등 안전한 접속 및 수단을 적용하지 않는 등* 안전성 확보 조치 의무를 다하지 않은 피심인의 행위는 보호법 제29조 위반에 해당한다.

* ①내부 관리계획 일부 법정 항목 누락, ②홈페이지 관리자페이지 접근 시 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근 제한 미조치, ③안전한 접속 및 수단 미적용, ④개인정보 조회 웹페이지 접근 통제 미조치, ⑤홈페이지 취약점 점검 미조치, ⑥주민등록번호·비밀번호 송신 암호화 미조치, ⑦접속기록 미보관

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반에 대해 같은 법 제75조제2항제6호, 같은 법 시행령 제63조 및 [별표2] 과태료 부과기준에 따라 다음과 같이 360만원의 과태료를 부과한다.

가. 기준 금액

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

< [별표2] 과태료 부과기준 >

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

나. 과태료의 가중

피심인의 위반행위는 제29조에 따른 안전성 확보에 필요한 조치를 4개 위반* 하여 중과실에 해당하여 과태료의 부과기준에 따라 기준금액의 10%인 60만원을 가중한다.

* ①내부 관리계획 미흡, ②접근통제 및 접근권한 제한 미조치, ③암호화 미적용, ④접속기록 미보관

< 과태료의 부과기준 1. 라. >

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) 위반기간이 3개월 이상인 경우
3) 그 밖에 위반행위 정도, 동기와 그 결과 등 고려하여 과태료를 늘릴 필요가 있다고 인정되는 경우

다. 과태료의 감경

피심인은 사전통지·의견제출 기간 내 위법행위를 중지·시정완료하거나 시정 중에 있으며, 조사기간 중 행위사실을 인정하면서 자료제출·진술 등 조사에 협력하였고 그 위반행위에 고의가 없는 점 등을 고려하여 과태료 부과기준에 따라 기준금액의 50%인 300만원을 감경한다.

< 과태료의 부과기준 1. 다. >

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

피심인이 보호법 제29조를 위반한 행위에 대해 360만원을 부과한다.

< 최종 과태료 산출내역(안) >

과태료 처분의 근거		과태료 금액 (단위:만원)			
위반조항	위반내용	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B+C)
법 §29	안전조치의무 위반	600	60	△300	360

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

V. 결론

피심인의 보호법 제29조위반에 대하여 같은 법 제75조 제2항제6호 및 법 시행령 제63조에 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(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 12월 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)

개 인 정 보 보 호 위 원 회

심의·의결

안건번호 제2021-020-292호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 [redacted] (대표자 [redacted])

[redacted]

의결연월일 2021. 12. 8.

주 문

피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

1. 피심인 현황

[redacted](이하 '피심인')은 「개인정보 보호법」(이하 '보호법'이라 함)에 따른 개인정보처리자로서 피심인의 일반 현황은 다음과 같다.

대표자	설립일자	업종 및 주요서비스	종업원 수	자본금
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

2. 조사 결과

가. 개인정보 수집·보유 현황

'21.7.14. 09:00~09:20 피심인은 한정판 신발 구입 응모 이벤트 행사를 위해 4,594명[1]의 개인정보(이메일, 성명, 연락처, 생년월일, 아이디)를 수집했다.

나. 사고 경위

'21.7.14. 09:00 피심인은 한정판 신발 구입 응모 이벤트 행사 진행 과정에서 담당자의 실수로 '구글 설문지'의 옵션을 공개로 잘못 설정('이전 응답 참조' 기능 활성화)하여 관리자가 아닌 다른 이벤트 참여자에게 먼저 응답한 응답자의 개인정보(응답 항목[2] 별 100개[3])가 공개되었다.

< 설문 응답 항목 예시 >[4]

OOO(매장명) 응모 정보를 적어주세요				
응모자 성함을 기재해 주세요	이메일을 기재해 주세요	연락처를 기재해 주세요	생년월일을 기재해 주세요	아이디를 기재해주세요
홍길동	adb@naver.com	010-XXXX-XXX	XX.XX.XX.	abc
...(100개)	...(100개)	...(100개)	...(100개)	...(100개)

나. 사고 인지 및 대응

'21.7.14. 09:13 피심인은 네이버 카페 ' '에서 해당 구글 설문지에 문제가 있다는 글이 작성된 것을 확인하여 인지했고, 아래와 같이 대응했다.

'21.7.14. 09:15 관리자만 '이전 응답 참조'에 접속할 수 있도록 권한 변경

'21.7.14. 09:20 응답 제출 내역 다운로드 및 구글 설문지 응모 중단

'21.7.14. 10:07 웹 상에서 구글 설문지의 모든 응답 결과 삭제

'21.7.14. 14:45 개인정보보호 포털에 개인정보 유출 신고

'21.7.14.~7.16. 개인정보 유출 통지 문자 및 이메일 발송

'21.7.14.~7.21. 피심인의 홈페이지에 개인정보 유출 안내 팝업 공지

1) 응답 건수 13,579건 중 연락처(연락처가 없는 경우 이메일) 중복 제거 시 4,594건
2) ①이메일, ②성명, ③연락처, ④생년월일, ⑤
3) '구글 설문지' 기능상 응답 항목 별 100개의 응답 내용 확인 가능
4) 응답 항목별 개인정보가 동일 응답자의 것을 의미하는 것은 아님

3. 위법성 판단

가. 관련 법령

1) 보호법 제29조는 개인정보의 안전성 확보에 필요한 기술적·관리적·물리적 조치를 해야 한다고 규정하고 있다.

2) 개인정보의 안전성 확보조치 기준(이하 '고시') 제6조제3항은 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 해야 한다고 규정하고 있다.

나. 행위 사실

'21.7.14. 09:00 피심인은 한정판 신발 구입 응모 이벤트 행사 진행 과정에서 담당자의 실수로 '구글 설문지'의 옵션을 공개로 잘못 설정하여 관리자가 아닌 다른 이벤트 참여자에게 먼저 응답한 응답자의 개인정보(응답 항목[5] 별 100개)가 공개되었다.

다. 위법성 판단

피심인은 '구글 설문지'를 활용하는 과정에서 열람 범위를 잘못 설정하여 권한이 없는 자에게 이용자의 개인정보가 공개되도록 하여 보호법 제29조, 같은 법 시행령 제30조제1항제2호, 고시 제6조제3항을 위반했다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '21.11.3. '개인정보보호 법규 위반 행정처분 사전통지' 공문을 통해 이 사건에 대한 피심인의 의견을 요청했으며, 피심인은 과태료 대상 위반행위에 대해 조사 협조·자진 시정 완료했음 등을 고려하여 과태료 금액을 최소화해달라는 요청을 의견으로 제출했다.

5) ①이메일, ②성명, ③연락처, ④생년월일, ⑤

5. 처분 및 결정 : 과태료 부과

피심인의 보호법 제29조 위반행위에 대해 같은 법 제75조제2항제6호, 같은 법 시행령 제63조 [별표 2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」(이하 '과태료 부과기준')에 따라 300만원의 과태료를 부과한다.

1) 기준금액

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

(단위 : 만원)

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회이상 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

2) 과태료의 가중

과태료 가중 사유가 없으므로 기준금액을 유지한다.

3) 과태료의 감경

가중·감경 금액은 사유가 2개 이상 해당되는 경우 합산하여 기준금액의 50%의 범위에서 가중·감경하여 결정하며, 위반 정도가 경미하고, 조사협조 및 자진 시정, 중소기업인 점 등을 고려하여 기준금액의 50%인 300만원을 감경한다.

< 과태료 감경기준 및 적용 >

기준	감경사유	감경비율
위반 정도	정보주체에게 피해가 발생하지 않은 등 위반행위의 결과가 경미하거나, 사소한 부주의 또는 시스템의 오류로 인한 것으로 인정되며 피해발생이 없는 경우	50%이내
조사 협조·자진 시정 등	1. 과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우	50%이내
	2. 보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	40%이내
사업 규모	「중소기업기본법」 제2조에 따른 중소기업인 경우	20%이내

4) 최종 과태료

기준금액 600만원에서 300만원을 감경한 300만원을 부과한다.

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

6. 결론

피심인의 보호법 제29조 위반행위에 대해 제75조제2항제6호에 따른 과태료 부과를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 과태료 부과 처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조제1항에 따라 처분을 받은 날부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과 처분에 대한 피심인의 이의 제기가 있는 경우, 개인정보보호위원회의 과태료 부과 처분은 「질서위반행위규제법」 제20조제2항에 따라 그 효력을 상실하고 관할 법원(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 12월 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)

개 인 정 보 보 호 위 원 회
심의·의결

안건번호 제2021-020-293호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 [redacted] 주식회사

서울시 [redacted]

대표자 [redacted]

의결연월일 2021. 12. 8.

주 문

1. 피심인에 대하여 다음과 같이 개선할 것을 권고한다.

가. 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보취급자(개인정보 처리자의 지휘·감독을 받아 개인정보를 처리하는 자)에 대하여 적절한 관리·감독을 실시할 것.

나. 개인정보의 적정한 취급을 보장하기 위해 개인정보취급자를 대상으로 정기적인 개인정보보호 관련 교육을 실시할 것.

다. 처분통지를 받은 날로부터 60일 이내에 위의 가, 나의 개선권고 이행결과를 제출할 것.

이 유

Ⅰ. 피심인의 일반 현황

피심인 [redacted] 주식회사*는 음료식품 제조업 법인으로서 일반현황은 다음과 같다.

* [redacted]

< 피심인의 일반현황 >

대표자	개업일자	주요서비스	종업원 수	자산('19년도)
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Ⅱ. 사실조사 결과

개인정보보호위원회는 2020. 12월에 개인정보보호 포털에 유출신고가 접수된 건과 관련하여 사실조사(2021.2.3.~2021.2.5.) 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 수집·이용 현황

피심인은 내부망에서 인사시스템을 운영하면서 임직원의 개인정보 [redacted]건을 수집·보관하고 있다.('21.02.03. 기준)

< 인사시스템 개인정보 수집 현황 >

구 분	항 목	수집일수	건수
임직원 정보	사원번호, 사원명, 성별, 주민등록번호, 직책, 직급, 직군, 직종, 직무, 사원구분, 직급연차, 입사일자, 입사구분, 공채기수, 그룹입사일, 재직구분, 휴직일자, 간부구분, 사내이메일, 장애여부, 장애유형, 장애등급, 중증여부, 보훈여부, 보훈유형, 보훈등급, 여권번호, 주소, 생년월일, 결혼기념일, 병역여부, 미필사유, 군별, 병과, 계급, 자택전화, 휴대폰, 최종학력, 출신학교명, 전공, 본/분교여부, 나이, 근속년수, 부서명(본부, 부문, 팀, 부서), 급여체계	'58. 01. 10. ~ '21. 02. 03.	[redacted]건

2. 개인정보 유출 경위

가. 유출 경과 및 대응

- '20. 12. 10. 업무 담당자가 지점 담당자(119명)에게 크리스마스 트리 배송 관련 하여 내부 메일 발송
- '20. 12. 11. 수신인 제보(1명)로 해당 사실 인지
- '20. 12. 11. 메일 수신자(119명)에게 이메일로 해당 메일 삭제 요청
- '20. 12. 11. 임직원(2,027명)에게 이메일로 개인정보 유출 통지
- '20. 12. 11. 메일 수신자(119명)에게 유선으로 메일 삭제 협조 요청
- '20. 12. 12. 메일 서버 내 해당 메일(원본) 삭제 조치

* 해당 파일 다운로드 기록 확인(12명), 오발송 이후 29시간 내에 메일서버에서 삭제 조치(수신자 포함)

- '20. 12. 14. 개인정보보호 포털(www.privacy.go.kr)에 개인정보 유출 신고
- '20. 12. 16. 홈페이지에 개인정보 유출 안내문 게시
- '20. 12. 17. 인사시스템 변경 조치(접근 인원 최소화 등)

나. 유출 규모 및 경위

피심인의 인사 담당자가 내부 인트라넷(업무망)에서 각 지점 담당자에게 크리스마스 트리 배송 안내* 메일을 발송하면서 첨부자료를 오인하여 배송 주소 파일 대신 임직원의 인사정보 2,027건이 포함된 엑셀파일(이하 '유출파일')**을 실수로 첨부(유출) 하였다.

* 연말연시 마무리 및 조직 내 분위기 고취를 위한 목적으로 발송

** 엑셀파일 '[redacted] 트리 발송 주소(201208)_부서 발송용.xlsx(876 KB)'

< 피심인의 개인정보 유출 현황 >

구 분	유 출 항 목	유출건수
유출파일 (임직원 정보, 엑셀)	사원번호, 사원명, 성별, 주민등록번호, 직책, 직급, 직군, 직종, 직무, 사원구분, 직급연차, 입사일자, 입사구분, 공채기수, 그룹입사일, 재직구분, 휴직일자, 간부구분, 사내이메일, 장애여부, 장애유형, 장애등급, 중증여부, 보훈여부, 보훈유형, 보훈등급, 여권번호, 주소, 생년월일, 결혼기념일, 병역여부, 미필사유, 군별, 병과, 계급, 자택전화, 휴대폰, 최종학력, 출신학교명, 전공, 본/분교여부, 나이, 근속년수, 부서명(본부, 부문, 팀, 부서), 급여체계	[redacted] 건

3. 행위 사실

가. 개인정보취급자에 대한 감독을 소홀히 한 행위

개인정보취급자인 인사과 직원 부주의로 내부 메일 발송 과정에서 임직원의 인사정보 파일이 첨부된 사실이 있다.

※ 내부 관리계획 수립, 접속기록 보관 등 안전성 확보에 필요한 조치를 하고 있음

Ⅲ. 위법성 판단

1. 관련 법령

가. 개인정보 보호법[1](이하 '보호법'이라 함) 제29조에서는 "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 한다." 라고 규정하고 있다.

나. 보호법 제28조제1항에서는 개인정보처리자는 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보취급자에 대해 적절한 관리 · 감독을 하도록 하고 있다.

2. 위법성 판단

가. 개인정보취급자에 대한 감독을 소홀히 한 행위

개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 개인정보취급자에 대한 관리·감독을 소홀히 한 피심인의 행위는 보호법 제28조제1항 위반에 해당한다.

개인정보가 포함된 파일을 처리하면서 해당 파일을 암호화 처리 등 필요한 조치를 하고 있는 등 안전성 확보조치 의무 위반은 확인되지 않으나, 개인정보취급자의 부주의로 내부망에서 임직원의 개인정보가 포함된 메일이 발송되었다.

1) 현행 개인정보 보호법[법률 제16930호] 적용

※ 피심인은 고유식별번호가 포함된 파일을 처리하면서 해당 파일을 암호화 처리(문서보안 DRM 및 매체 제어솔루션 통제 적용) 등을 하며, 내부 관리계획 수립, 접속기록 보관 등 안전한 처리를 위한 필요한 조치를 한 것으로 확인됨

Ⅳ. 처분 및 결정

1. 개선 권고

피심인은 보호법 제28조제1항을 위반하여 개인정보취급자에 대해 적절한 관리·감독을 하지 않은 것에 대해 같은 법 제61조제2항에 따라 아래와 같이 개선할 것을 권고한다.

① 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보취급자(개인정보 처리자의 지휘·감독을 받아 개인정보를 처리하는 자)에 대하여 적절한 관리·감독을 이행할 것
② 개인정보의 적정한 취급을 보장하기 위해 개인정보취급자를 대상으로 정기적인 개인정보보호 관련 교육을 실시할 것
③ 처분통지를 받은 날로부터 60일 이내에 위 ①과 ②의 개선권고 이행결과를 제출할 것

Ⅴ. 결론

피심인은 보호법 제28조제1항을 위반한 행위에 대하여 같은 법 제61조제2항에 의한 개선권고를 주문과 같이 의결한다.

2021년 12월 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)

개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2021-020-294호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치 등에 관한 건

피 심 인 [redacted]

의결연월일 2021. 12. 8.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 5,000,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 [redacted] 서비스를 제공하는 정보통신서비스 제공자로서 일반현황은 다음과 같다.

* [redacted]

1) [redacted]

< 피심인의 일반현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수

※

피심인의 2018년 5월 기준 대한민국 이용자는 명 정도로 추산된다.

< 개인정보 수집 현황 >

구 분	항 목	수집일수	수집건수
회원정보	이메일주소, 성명, 휴대폰번호	'12. 4. 이후	건

Ⅱ. 사실조사 결과

개인정보보호위원회[2](이하 '위원회'라 한다)는 이용자의 비밀번호가 평문으로 보관되고 있다는 언론보도와 관련하여 사실조사 및 관련 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 행위 사실

를 통해 2019년 1월 정기 보안검토 과정에서 서비스 일부 이용자의 비밀번호가 평문으로 보관된 사실을 확인하였다고 2019년 3월 21일 밝혔다

2) 개인정보 보호법 [법률 제16930호, 시행 2020. 8. 5.] 부칙.
제3조(기능조정에 따른 소관 사무 등에 관한 경과조치) ① 이 법 시행 당시 「방송통신위원회의 설치 및 운영에 관한 법률」 제11조제1항의 방송통신위원회의 소관사무 중 개인정보 보호에 해당하는 사무는 보호위원회가 승계한다.
② 이 법 시행 당시 행정안전부장관의 소관 사무 중 제7조의8의 개정규정에 따른 사무는 보호위원회가 승계한다.
③ 이 법 시행 전에 행정안전부장관이 행한 고시·행정처분, 그 밖에 행정안전부장관의 행위와 행정안전부장관에 대한 신청·신고, 그 밖의 행위 중 그 소관이 행정안전부장관으로부터 보호위원회로 이관되는 사항에 관한 행위는 보호위원회의 행위 또는 보호위원회에 대한 행위로 본다.
④ 이 법 시행 전에 방송통신위원회가 행한 고시·행정처분, 그 밖의 행위와 신고 등 방송통신위원회에 대한 행위 중 그 소관이 방송통신위원회에서 보호위원회로 이관되는 사항에 관한 행위는 이 법에 따른 보호위원회의 행위 또는 보호위원회에 대한 행위로 본다.
제7조(벌칙 및 과태료에 관한 경과조치) 이 법 시행 전의 행위에 대한 벌칙 및 과태료의 적용은 종전의 규정에 따른다.

위원회가 대한민국 이용자의 비밀번호가 평문으로 저장되어 유출되는 등 침해되었을 가능성과 관련하여 사실관계를 확인한 결과, 내부 데이터 저장 시스템에 비밀번호가 평문으로 보관된 전 세계 이용자와 대한민국 이용자는 아래와 같다.

< 비밀번호 평문저장 이용자 현황 >

구 분	
전 세계 이용자	
대한민국 이용자	

이용자의 비밀번호가 평문으로 보관된 원인은 ①"새니티제이션 프레임워크"[3]가 갖춰지지 않은 일부 시스템에 비밀번호가 기록됨으로써 비밀번호가 평문으로 보관되었으며,

새니티제이션 프레임워크를 갖춘 일부 시스템에 ②평문 비밀번호가 기록되었으나 프레임워크가 이를 탐지하지 못하였고,

③클라이언트 어플리케이션에 대한 세션 쿠키(session cookie)[4]의 일부로 평문 비밀번호를 수집하였으나, 의도한 사용이 완료된 후 해당 데이터가 자동으로 삭제되지 않아 비밀번호가 평문으로 보관된 것으로 확인하였다.

내부 데이터 저장 시스템에 평문으로 기록된 이용자의 비밀번호 중 대한민국 이용자의 평문 비밀번호가 기록된 기간은 2016년부터 2019년 3월까지로 확인하였으며,

2019년 3월 말까지 조사를 진행하면서 확인된 평문 비밀번호에 대한 삭제를 완료하였다고 소명하였다.

2. 처분의 사전통지 및 의견 수렴

위원회는 2021년 1월 27일 '개인정보보호 법규 위반에 대한 행정처분 사전통지' 공문을 통하여 처분에 대한 피심인의 의견을 요청하였고, 피심인은 2021년 2월 26일 다음과 같이 의견을 제출하였다.

3) 비밀번호와 같이 민감한 데이터를 데이터가 기록되기 전에 확인하여 식별될 수 없는 값으로 대체하는 일련의 코드
4) 이용자 웹 브라우저의 임시 메모리 위치에 저장된 후 세션이 완료되거나 웹 브라우저가 종료되면 삭제되는 작은 데이터 조각

①이용자의 신고가 아니라 자체적으로 행하는 정기 보안 검토과정에서 발견하여 자발적으로 뉴스룸을 통해 공개하였으며, ②적극적으로 개선 조치를 취했을 뿐만 아니라 ③이용자의 피해가 발생하지 않은 점을 고려하여, 제재받을 사안이 아니라고 위원회가 판단해줄 것을 요청하였다.

Ⅲ. 위법성 판단

1. 관련 법령의 규정

舊정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법' 이라 함) 제28조제1항은 "정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 '개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)' 등의 기술적·관리적 조치를 하여야 한다."라고 규정하고 있다.

가. 시행령 제15조제4항은 "법 제28조제1항제4호에 따라 정보통신서비스 제공자 등은 개인정보가 안전하게 저장·전송될 수 있도록 '비밀번호의 일방향 암호화 저장(제1호)' 등의 보안조치를 하여야 한다."라고 규정하고 있다.

나. 시행령 제15조제6항에 따른 개인정보의 안전성 확보 조치의 구체적인 기준을 「개인정보의 기술적 관리적 보호조치 기준」(방통위 고시 제2019-13호, 이하 '고시'라 함)에서 정하고 있다.

① 기준 제2조제6호는 "비밀번호라 함은 이용자 및 개인정보취급자 등이 시스템 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로 타인에게 공개되지 않는 정보를 말한다."라고 규정하고 있다.

② 「개인정보의 기술적·관리적 보호조치 기준 해설서(2017.12.)」(이하 '기준 해설서')는 ▲"식별자는 정보주체 식별을 위한 목적으로 사용되는 ID, 사용자 이름, 사용자 계정명 등을 말한다."라고 설명하고 있다.

③ 기준 해설서는 ▲ "정보통신서비스 제공자등은 이용자 및 개인정보취급자 등의 비밀번호가 노출 또는 위·변조되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 보조저장매체 등에 일방향 암호화(해쉬함수 적용)하여 저장하여야 한다.

일방향 암호화는 개인정보취급자 및 이용자 등이 입력한 비밀번호를 평문 형태가 아닌 해쉬함수를 통해 얻은 결과 값으로 시스템에 저장하는 것을 말한다. 입력한 비밀번호와 시스템에 저장된 비밀번호를 비교하여 인증된 사용자임을 확인한다."라고 설명하고 있다.

다. 즉, 이용자의 비밀번호는 외부자는 물론 개인정보처리시스템을 관리하는 내부자 또한 어떠한 경우에도 알 수 없도록 해쉬함수를 적용하여 복호화 되지 않도록 암호화하여야 한다.

2. 위법성 판단

피심인이 대한민국 이용자 약 8,200명의 비밀번호를 암호화하지 않고 평문으로 보관한 행위는 정보통신망법 제28조제1항제4호 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료의 부과

피심인의 정보통신망법 제28조제1항제4호 위반에 대해 같은 법 제76조제1항제3호 및 같은 법 시행령 제74호 [별표 9] 과태료 부과기준(이하 '과태료 부과기준')에 따라 다음과 같이 500만원의 과태료를 부과한다.

가. 기준금액

피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 1,000만원을 적용한다.

< 과태료 부과기준 2.개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
너. 법 제28조의제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 아니한 자	법 제76조 제1항제3호	1,000	2,000	3,000

나. 가중·감경

가중할 사유는 없으며, 사전통지 기간('21.1.27.~2.19.) 이전인 2019년 3월 말까지 암호화 조치 위반행위가 시정된 점을 고려하여 과태료 부과기준에 따라 기준금액의 50%인 500만원을 감경한다.

< 과태료 부과지침 [별표 1] 과태료의 감경기준 >

기준	감 경 사 유	감경비율
자진시정	1. 과태료의 사전 통지 및 의견 제출 기간 내에 법규 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 50% 이내

다. 최종 과태료

피심인의 정보통신망법 제28조제1항제4호 위반행위에 대해 다음과 같이 500만원의 과태료를 부과한다.

< 최종 과태료 산출내역(안) >

과태료 처분의 근거		과태료 금액 (단위:만원)			
위반 조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액 D=(A+B+C)
제28조(개인정보의 보호조치)	제76조제1항제3호	1,000	-	△500	500

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

Ⅴ. 결론

피심인의 정보통신망법 제28조제1항제4호 위반행위에 대하여 같은 법 제76조에 의한 과태료 부과를 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(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 12월 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)

개 인 정 보 보 호 위 원 회

심의·의결

안건번호 제2021-020-295호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (주)
서울시
대표

의결연월일 2021. 12. 8.

주 문

피심인 (주) 에 대하여 다음과 같이 과태료를 부과한다.

가. 금 액 : 3,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 과학, 수학 교육 영재교육원 등을 운영하는 사업자로 일반현황은 다음과 같다.

< 피심인 일반현황 >

대 표	설립일자	자산('20년)	매출액('20년)	주요서비스	종업원 수

Ⅱ. 사실조사 결과

개인정보보호위원회[1]는 개인정보 침해신고와 관련하여 점검을 실시(2020.2.24.~2.26.) 및 관련 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 수집 현황

피심인은 학원업무관리시스템을 운영하면서 총 명의 개인정보를 수집·보관하고 있다.('21.2월 기준)

< 개인정보 보유 현황 >

구 분	내용	항 목	보유근거	수집건수
학원업무 관리시스템	회원정보	(필수) 이름, 생년월일, 학교명, 학년, 연락처, 주소, 학부모정보(성명, 관계, 직업, 휴대폰, 이메일) (선택) 수상실적, 진학실적	정보주체의 동의	명
	교직원 정보	(필수) 이름, 생년월일, 성별, 결혼여부, 연락처(전화, 휴대폰), 주소, 이메일 (선택) 이름(한문), 학력	정보주체의 동의	명
총 계				명

2. 행위 사실

피심인은 학원업무관리시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응을 하여야 하나 조치하지 않았으며, 외부에서 학원업무관리시스템에 접속할 경우 가상사설망(VPN) 또는 전용선 등 안전한 접속 또는 인증수단을 적용하지 않았다.

---

1) 개인정보 보호법 [법률 제16930호, 시행 2020. 8. 5.] 부칙.
제3조(기능조정에 따른 소관 사무 등에 관한 경과조치) ② 이 법 시행 당시 행정안전부장관의 소관 사무 중 제7조의8의 개정규정에 따른 사무는 보호위원회가 승계한다.
③ 이 법 시행 전에 행정안전부장관이 행한 고시·행정처분, 그 밖에 행정안전부장관의 행위와 행정안전부장관에 대한 신청·신고, 그 밖의 행위 중 그 소관이 행정안전부장관으로부터 보호위원회로 이관되는 사항에 관한 행위는 보호위원회의 행위 또는 보호위원회에 대한 행위로 본다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021.5.27. '개인정보 보호법 위반 행정처분 사전통지' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 '2020년 7월 시정하는 등을 고려하여 선처를 요청한다'는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련 법령의 규정

개인정보 보호법[2](이하 '보호법' 이라 함) 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·물리적 조치를 하도록 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 있고,

시행령 제30조에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준(행정안전부 고시)」 제6조제1항에서는 개인정보취급자는 정보통신망을 통한 불법적인 접근 및 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응의 기능을 포함한 조치를 하도록 하며, 제6조제2항은 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하도록 규정하고 있다.

2. 위법성 판단

학원업무관리시스템에 접속한 IP를 분석하여 불법적인 개인정보 유출 시도 탐

2) 現 개인정보 보호법[법률 제16930호] 개정 시행(2020.8.5.) 이전에 발생한 행위로 舊 개인정보 보호법[법률 제14839호, 시행, 2017.10.19.] 적용

지 및 대응하지 않고, 학원업무관리시스템 접속 시 안전한 접속 및 인증수단을 적용하지 않은 피심인의 행위는 보호법 제29조 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반에 대해 같은 법 제75조제2항제6호, 같은 법 시행령 제63조 및 [별표2] 과태료 부과기준에 따라 다음과 같이 300만원의 과태료를 부과한다.

가. 기준 금액

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

< [별표2] 과태료의 부과기준 >

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

나. 과태료의 가중

피심인의 위반행위는 과태료의 부과기준 1. 다.에 따른 가중할 수 있는 사유에 해당하지 않으므로 가중을 하지 않고 기준금액을 유지한다.

< 과태료의 부과기준 1. 다. >

1. 일반기준

다. 행정안전부장관 또는 관계 중앙행정기관의 장은 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 부과금액의 2분의 1의 범위에서 그 금액을 가중할 수 있다. 다만, 가중할 사유가 여러 개인 경우라도 법 제75조제1항부터 제3항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.

1) 위반의 내용 및 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 가중할 필요가 있다고 인정되는 경우

다. 과태료의 감경

피심인의 위반행위가 부주의에 의한 것으로 추가 피해가 없고 의견제출 기간 전 시정 완료하였으며 「중소기업기본법」 제2조에 따른 중기업에 해당하여 과태료 부과기준에 따라 기준금액의 50%인 300만원을 감경한다.

< 과태료의 부과기준 1. 나. >

1. 일반기준

나. 행정안전부장관 또는 관계 중앙행정기관의 장은 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 부과금액의 2분의 1의 범위에서 그 금액을 감경할 수 있다. 다만, 과태료를 체납하고 있는 위반행위자의 경우에는 그러하지 아니하다.

1) 위반행위자가 「질서위반행위규제법 시행령」 제2조의2제1항 각 호의 어느 하나에 해당하는 경우
2) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우
3) 위반행위자가 위법행위로 인한 결과를 시정하였거나 해소한 경우
4) 위반행위자가 「중소기업기본법」 제2조에 따른 중소기업자인 경우
5) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우

라. 최종 과태료

피심인이 보호법 제29조를 위반한 행위에 대해 300만원을 부과한다.

< 최종 과태료 산출내역(안) >

과태료 처분의 근거		과태료 금액 (단위:만원)			
위반조항	위반내용	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B+C)
법 §29	안전조치의무 위반	600	-	△300	300

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

V. 결론

피심인의 보호법 제29조위반에 대하여 같은 법 제75조제2항제6호 및 법 시행령 제63조에 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(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 12월 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)