개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2021 - 017 - 264호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2021. 10. 27.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.

2) 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

3) 개인정보취급자를 대상으로 비밀번호 작성규칙을 적용·운용하여야 한다.

4) 처리중인 개인정보가 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다.

나. 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

다. 이용자의 개인정보를 국외에 보관하려면 이에 대하여 이용자에게 동의를 받거나 알려야 한다.

라. 피심인은 가.부터 다.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 126,166,000원

나. 과 태 료 : 18,600,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 제휴사 온라인쇼핑몰을 통해 화장품을 판매하고, 쇼핑몰(----------) 및 앱을 운영하는「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16955호, 이하 '보호법'이라 한다.)에 따른 개인정보처리자 및 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 가 앱 이용자의 개인정보가 타인에게 공개되었다고 유출 신고(2020. 11. 10.)하였고, 이용자의 개인정보가 신원미상의 자(이하, '해커'라 한다.)에게 유출되었다고 신고(2021. 8. 7.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사(2021. 8. 11. ~ 2021. 9. 6.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 화장품 및 잡화류를 판매하면서 국내 이용자의 개인정보를 수집(온라인·오프라인)하였으며, ’21. 8. 12. 기준 건의 이용자 정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원정보 (유효회원)	(필수) 이름, 생년월일, 휴대전화번호, 구매이력, 고객등록일	’17. 12. 15. ~ ’21. 8. 12.	
(분리보관)	(선택) 이메일, 성별, 주소, 거주지, 국적, 기념일, 자택전화번호, 직업 등		
계			

나. 개인정보 유출 경위

< 전달서버 개인정보 유출 사건(‘21.8월) >

1) 유출 경과 및 대응

일 시		피심인의 유출인지 및 대응 내용
’21. 8. 6.	09:20	국내 서버 관리자가 시스템 점검 중 DB 삭제 및 DB 내 협박 메시지 확인
	10:30	보안담당 부서( )로 사고사실 전달 및 분석
	22:40	보안담당 부서( )에서 사고조사 결과 이메일로 유출 사실인지
’21. 8. 7.	22:25	개인정보 유출 관련 홈페이지 공지
	22:45	한국인터넷진흥원에 개인정보 유출 신고
	22:54	유출 대상자 81,654명에 이메일·문자로 유출 사실 통지

2) 유출규모 및 경위

(유출항목 및 규모) 9개* 제휴사의 온라인쇼핑몰을 통한 구매 이력이 있는 이용자의 개인정보(이름, 생년월일, 휴대전화번호, 구매이력, 고객등록일, 이메일, 성별, 주소, 거주지, 국적) 81,654건**

*

9개 사이트

** 9개 제휴사의 온라인쇼핑몰을 통한 구매이력이 있는 한국 국적의 이용자(서버의 DB가 삭제되어, CRM시스템에서 산출)

(유출경위) 해커( )는 피심인이 운영하는 미국 AWS의 멤버십 전달 서버에 DB관리도구(phpMyAdmin)를 이용하여 관리자계정('root')으로 접속한 후, 개인정보가 포함된 DB를 유출

서버명	
도메인	
기능	9개 제휴사의 온라인쇼핑몰로부터 수집된 회원정보 및 구매정보를 에 있는 고객관리(CRM)시스템으로 전송하기 위한 전달서버임

- '21. 7. 23. 00:28 해커는 DB관리도구(phpMyadmin)에 일반적으로 사용되는 관리자페이지 URL로 7초 동안 57회 접속을 시도하여 성공함(' ')

- '21. 8. 4. 05:34 해커는 일반적으로 사용되는 DB관리자 계정으로 12초 동안 43회 로그인을 시도하여 성공함('root')

- '21. 8. 5. 18:33 해커는 개인정보가 포함된 2개의 DB*를 유출함

* db_ _dev(3.5MB), _dev(228MB)를 웹서버 및 방화벽을 통해 전송함

< 앱 개인정보 노출 사건('20.11월) >

1) 유출 경과 및 대응

일 시		피심인의 개인정보 유출인지 및 대응 내용
'20.11. 9.	11:37	이용자 제보(이메일)로 유출 사실 인지
'20.11.10.	11:38	에서 문제가 된 캐시 삭제
	11:38	한국인터넷진흥원에 개인정보 유출 신고
	11:54	유출 대상자 4명에 전화로 유출사실 통지
'20.11.13.	-	SSO정보(자동 로그인 정보)는 캐시되지 않도록 캐시정책 변경

2) 유출규모 및 경위

(유출항목 및 규모) 타인에게 노출된 이용자의 개인정보 총 4건*

* 1명(이름, 주소, 이메일, 휴대폰번호, 생년월일, 유선전화번호), 3명(이름, 주소)

(유출경위) 앱의 제품 홍보 배너와 연결되는 쇼핑몰 페이지(URL)를 잘못 설정하여 타인의 계정으로 자동 로그인되었고, 회원 4명의 개인정보가 타인에게 공개

- '20. 11. 2. 제품 홍보 배너 게재 시 직원 실수로 접속되지 않는 URL로 연결 설정하여, 상위페이지로 자동으로 연결되면서 SSO정보(자동 로그인 정보)가 CDN에 캐시됨

3. 개인정보의 취급·운영 관련 사실관계

< 전달서버 개인정보 유출 사건('21.8월) >

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 개인정보처리시스템의 관리자페이지에 외부 인터넷망에서 접속 시 안전한 인증수단을 적용하지 않고 계정·비밀번호만으로 접속되도록 운영한 사실이 있다.

또한 피심인은 불법적인 접근을 차단하기 위해 AWS에서 제공하는 방화벽을 설치하였으나 개인정보처리시스템에 대한 접근권한을 개인정보취급자에게 허용된 IP로 제한하지 않고, 외부 인터넷 어디서나 접속할 수 있도록 운영한 사실이 있다.

아울러, 피심인은 개인정보처리시스템에 접속 가능한 개인정보취급자의 계정('root') 비밀번호를 계정명과 동일한 'root'로 설정하여 운용한 사실이 있다.

나. 장기 미이용자의 개인정보 파기 등 필요한 조치를 하지 않은 행위

피심인이 제출한 백업DB*(백업일 : '21. 7. 30.) 확인 결과, 피심인은 정보통신서비스를 1년 이상 이용하지 않은 명의 개인정보를 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 사실이 있다.

* 9개 제휴사의 온라인쇼핑몰로부터 수집된 회원정보 및 구매정보를 백업한 것으로, 총 명(회원정보의 휴대폰번호로 중복제거) 중 1년 이상 구매이력이 없는 회원수는 명임

다. 이용자의 개인정보를 국외 이전하면서 법령상 고지사항을 이용자에게 알리지 않은 행위

피심인은 이용자의 개인정보를 국외(AWS, 미국 오하이오 在)로 이전하여 운영 중이나, 이용자에게 동의받거나 개인정보처리방침에 공개 또는 전자우편 등으로 알리지 아니한 사실이 있다.

< 앱 개인정보 노출 사건('20.11월) >

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 앱의 제품 홍보 배너와 연결되는 쇼핑몰 페이지(URL)를 잘못 설정하여 타인의 계정으로 자동 로그인되었고, 권한 없는 자에게 이용자의 개인정보가 공개된 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 9. 3. 및 2021. 9. 10. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 9. 17. 및 9. 24. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 및 물리적 조치를 하여야 한다."라고 규정하고 있다.

보호법 시행령 제48조의2제1항 제2호는 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '침입차단시스템 및 침입탐지시스템의 설치·운영(나목)', '비밀번호의 생성 방법 및 변경 주기 등의 기준 설정 및 운영(라목)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)' 등의 조치를 하여야 한다."라고 규정하고 있고, 제3항은 "제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다."라고 규정하고 있다.

제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시 제2020-5호, 이하 '고시') 제4조제4항은 "개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다"고 규정하고 있고, 고시 제4조제5항은 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)', '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)' 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있으며, 고시 제4조제8항은 "정보통신서비스 제공자등은 개인정보취급자를 대상으로 '영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성(제1호)', '연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고(제2호)', '비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경(제3호)' 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다."라고 규정하고 있고, 고시 제4조제9항은 "정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다."라고 규정하고 있다.

'고시 해설서'는 고시 제4조제4항에 대해 외부에서 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만을 이용할 경우 유출 위험이 커지기 때문에 계정(ID)과 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 인증서, 보안토큰, 휴대전화 인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단의 적용이 필요하다고 해설하고 있고, 고시 제4조제5항에 대해 정보통신서비스 제공자등은 불법적인 접근(인가되지 않은 자가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말함) 및 침해사고(해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태) 방지를

위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있으며, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 하며 신규 위협 대응 등을 위하여 지속적인 업데이트 적용 및 운영·관리하여야 한다고 해설하고 있으며, 고시 제4조제8항에 대해 비밀번호는 정당한 접속 권한을 가지지 않은 자가 추측하거나 접속을 시도하기 어렵도록 문·숫자 등으로 조합·구성하여야 하고, 개인정보처리시스템에 권한 없는 자의 접근을 방지하기 위하여 비밀번호 등으로 일정 횟수 이상 잘못 입력할 때에는 개인정보처리시스템에 접근을 제한하는 등의 보호조치를 추가적으로 적용할 수 있다고 해설하고 있고, 고시 제4조제9항에 대해 인터넷 홈페이지를 통한 개인정보 유·노출 방지를 위해 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방지 조치를 하여야 하며, 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등에 관한 보호조치를 하여야 한다고 해설하고 있다.

나. 보호법 제39조의6제1항은 “정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다.”라고 규정하고 있다.

보호법 시행령 제48조의5제1항 “이용자가 정보통신서비스를 법 제39조의6제1항의 기간 동안 이용하지 않는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.” 라고 규정하고 있다.

다. 보호법 제39조의12제2항은 “정보통신서비스 제공자등은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이전)하려면 이용자의 동의를 받아야 한다. 다만 제3항 각호의 사항 모두를 제30조제2항에 따라 공개

하거나 전자우편 등 대통령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁·보관에 따른 동의 절차를 거치지 아니할 수 있다.”라고 규정하고 있다.

2. 위법성 판단

< 전달서버 개인정보 유출 사건(‘21.8월) >

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 불법적인 접근 차단}

피심인은 국내 대표적인 화장품 및 잡화류 판매 사업자로 2020년 매출액이 억 원이고, 2021년 8월 기준 개인정보를 보관하고 있는 건수가 만 명 이상으로 일정규모 이상의 사업자에 해당하며, 피심인이 수집한 이름, 생년월일, 휴대전화번호, 이메일 등의 개인정보는 이용자를 특정할 수 있는 기본적인 개인정보로서 제3자가 이용할 경우 이용자에게 적지 않은 피해가 발생할 수 있어 보안을 철저히 할 필요가 있다.

또한 IP 제한, 비밀번호 작성규칙 등을 적용하는 조치를 통해 해킹을 방지하는 것은 누구나 생각할 수 있는 보편적으로 알려진 정보보안 기술 수준이고, 이를 조치하는데 비용이 발생하지도 않으며, 적용 시 피해발생이 줄어들 수 있는 등 사회통념상 합리적으로 기대 가능한 정도의 보호조치에 해당한다.

아울러 OWASP(Open Web Application security Project, 국제 웹 보안 표준기구)에서는 매년 대표적인 웹 취약점을 발표하는데, 이는 보안전문가와 업계에서 가장 많이 인용되는 권위적인 보안문서이며, 2021년에 OWASP 발표한 취약점 Top 10 중 2위에 Broken Authentication(취약한 인증)이 포함되어 있다. 무작위 대입공격은 취약한 인증과 관련된 해킹수법으로 많이 알려진 대표적인 웹 공격이다.

피심인은 개인정보 내부관리계획에는 “회사는 ‘영문대문자, 영문소문자, 숫자, 특수문자 중 3종류 이상을 조합하여 최소 8자리 이상, 2종류 이상을 조합하여 최소 10자리 이상’(1호), ‘연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고’(2호), ‘비밀번호에 유효기간을 설정하여 분기별 1회 이상 변경’(3호)을 포함하는 비밀번호 작성규칙을 수립하고 이를 적용·운용하여야 한다.”라고 규정하고 있다. 피심인이 내부관리계획을 준수하였다면 개인정보 유출을 방지할 수 있음에도 이를 준수하지 않은 것이다.

1) (안전한 인증수단) 피심인의 개인정보처리시스템 관리자페이지에 정보통신망을 통해 외부에서 접속 시 안전한 인증수단을 적용하지 않고 계정·비밀번호만으로 접속하도록 운영한 행위는 보호법 제29조, 같은 법 시행령 제48조의2, 고시 제4조제4항 위반한 것이다.

2) (침입차단 및 탐지시스템의 운영) 피심인이 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하지 않고, 외부 인터넷 어디서나 접속할 수 있도록 운영한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제5항을 위반한 것이다.

3) (비밀번호 작성규칙) 피심인이 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경 사항을 포함하는 비밀번호 작성규칙을 수립하여 이를 적용·운영하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제8항을 위반한 것이다.

나. 장기 미이용자의 개인정보 파기 등 필요한 조치를 하지 않은 행위

{보호법 제39조의6(개인정보의 파기에 대한 특례)}

피심인이 제공자등은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는

이용자의 개인정보를 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 하나, 1년 이상 정보통신서비스를 이용하지 않은 회원 의 개인정보를 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 행위는 보호법 제39조의6, 같은 법 시행령 제48조의5를 위반한 것이다.

다. 이용자의 개인정보를 국외로 이전하면서 법령상 고지사항을 이용자에게 알리지 않은 행위 {보호법 제39조의12(국외 이전 개인정보의 보호)}

피심인이 이용자의 개인정보를 국외에 보관하면 이를 이용자에게 동의받거나 알려야 하나, 이용자의 개인정보를 국외에 보관하면서 이용자에게 동의받거나 개인정보처리방침에 공개 또는 전자우편 등으로 알리지 아니한 행위는 보호법 제39조의12를 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제)	보호법 §29	§48의2① 제2호	• 정보통신망을 통해 외부에서 개인정보처리시스템에 접속시 안전한 인증수단을 적용하지 않고 계정·비밀번호만으로 접속하도록 운영한 행위(고시§4④) • 개인정보처리시스템에 대한 접근권한을 개인정보취급자에게 허용된 아이피로 제한하지 않고, 외부 인터넷 어디서나 접속할 수 있도록 운영한 행위(고시§4⑤) • 개인정보취급자의 비밀번호를 작성규칙을 따르지 않고 사용한 행위(고시§4⑧)
유효기간제	보호법 §39의6	§48의5	• 1년 이상 정보통신서비스를 이용하지 않은 회원의 개인정보를 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 행위
국외 이전	보호법 §39의12①	-	• 이용자의 개인정보를 국외에 보관하고 있다는 사실을 이용자에게 고지하지 않은 행위

< 앱 개인정보 노출 사건('20.11월) >

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 불법적인 접근 차단}

1) (개인정보 유·노출 방지) 피심인이 처리중인 개인정보가 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 접근통제 등에 관한 보호조치를 취하지 않아 앱의 제품 홍보 배너와 연결되는 쇼핑몰 페이지(URL)를 통해 로그인 시 타인의 계정으로 자동 로그인되었고, 권한 없는 자에게 이용자의 개인정보가 공개되도록 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2, 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제)	보호법 §29	§48의2① 제2호	・열람 권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.

2) 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

3) 개인정보취급자를 대상으로 비밀번호 작성규칙을 적용·운용하여야 한다.

4) 처리중인 개인정보가 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다.

나. 피심인은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

다. 피심인은 이용자의 개인정보를 국외에 보관하려면 이에 대하여 이용자에게 동의를 받거나 알려야 한다.

라. 피심인은 가.부터 다.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 과징금 부과

< 전달서버 개인정보 유출 사건('21.8월) >

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15 제1항제5호, 같은 법 시행령 제48조의11제1항과 제4항, [별표 1의5] '과징금의 산정기준과 산정절차' 및 「개인정보보호 법규 위반에 대한 과징금 부과기준」(2020. 8. 5. 개인정보보호위원회 고시 제2020-6호, 이하 '과징금 부과기준'이라 한다)에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제39조의15, 같은 법 시행령 제48조의11에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의 · 중과실 여부

과징금 부과기준 제5조제1항은 '보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 시행령 제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단한다.'라고 규정하고 있다.

이에 따라, 보호법 제29조(안전조치의무)를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

과징금 부과기준 제5조제3항은 '위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 매우 중대한 위반행위로 판단한다'라고 규정하고 있다.

다만, 과징금 부과기준 제5조제3항 단서에서 '위반행위의 결과가 ▲위반 정보통신서비스 제공자등이 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ▲이용자의 개인정보가 공중에 노출되지 않은 경우(제3호) 중 모두에 해당할 때에는 보통 위반행위로,

1개 이상 2개 이하에 해당하는 경우에는 중대한 위반행위로 감경한다.'라고 규정하고 있다.

이에 따라, 피심인이 위반행위로 인해 직접적인 이득을 취하지 않은 점, 개인정보의 피해 규모가 보유하고 있는 개인정보의 100분의 5 이내인 점, 이용자의 개인정보가 공중에 노출되지 않은 점을 고려하여 '보통 위반행위'로 판단한다.

3) 기준금액 산출

피심인의 관련 매출액은 9개 제휴사의 온라인쇼핑몰을 통해 발생한 매출액으로 하고, 직전 3개 사업년도의 연평균 매출액 천원에 보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 '보통 위반행위'의 부과기준율 1천분의 15을 적용하여 기준금액을 천원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2018년	2019년	2020년	평 균
관련 매출액*				

* 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

<보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
보통 위반행위	1천분의 15

다. 필수적 가중 및 감경

과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 2년을 초과

('18. 9. ~ '21. 8. 6.)하는 '장기 위반행위'에 해당하므로 기준금액의 100분의 50에 해당하는 금액인 천원을 가산하고,

최근 3년 이내 보호법 제39조의15제1항 각호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 천원을 감경한다.

라. 추가적 가중 및 감경

과징금 부과기준 제8조는 사업자의 위반행위 주도 여부, 조사 협력 여부 등을 고려하여 필수적 가중 · 감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

이에 따라, 피심인이 ▲조사에 적극 협력한 점, ▲개인정보 유출사실을 자진 신고한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 에 해당하는 천원을 감경한다.

마. 과징금의 결정

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15 제1항제5호, 같은 법 시행령 제48조의11, [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 1) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 126,166천원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중・감경	추가적 가중・감경	**최종 과징금**
천원	필수적 가중 (50% : 천원) 필수적 감경 (50% : 천원)	추가적 가중 없음 추가적 감경 (%, 천원)	**126,166천원**
	→ 천원	→ 천원	

3. 과태료 부과

피심인의 보호법 제29조, 제39조의6, 제39조의12 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항 제4호·제6호 및 제3항제3호 및 같은 법 시행령 제63조의 ［별표2］‘과태료 부과기준’ 및「개인정보 보호법 위반에 대한 과태료 부과기준」(2021. 1. 27. 개인정보보호위원회 의결, 이하 ‘과태료 부과지침’이라 한다)에 따라 다음과 같이 부과한다.

< 전달서버 개인정보 유출 사건(‘21.8월) >

가. 기준금액

보호법 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 제29조(안전조치의무) 및 제39조의6(개인정보의 파기에 대한 특례)에 대해서는 1회 위반에 해당하는 과태료인 600만원을, 제39조의12(국외 이전 개인정보의 보호)에 대해서는 400만원을 각각 적용한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위:만원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
마. 법 제21조제1항·**제39조의6(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우**	법 제75조 제2항제4호	600	1,200	2,400
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 **제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우**	법 제75조 제2항제6호	600	1,200	2,400
초. 법 **제39조의12제2항 단서를 위반하여 같은 조 제3항 각 호의 사항 모두를 공개하지 않거나 이용자에게 알리지 않고 이용자의 개인정보를 국외에 처리위탁·보관**한 경우	법 제75조 제3항제3호	400	800	1,600

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(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중기준)에 따라 ▲위반 기간이 3개월 이상인 경우로 위반행위별 기준금액의 10%를 각각 가중한다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.'라고 규정하고 있다.

피심인의 경우 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점, 사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 완료하지는 못하였으나 시정중에 있는 것으로 인정되는 경우에 해당하는 점을 고려하여 과태료 부과지침 제7조에 따라 기준금액의 20%를 각각 감경한다.

다. 최종 과태료

피심인의 보호법 제29조, 제39조의6, 제39조의12제2항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,440만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만원	60만원	120만원	**540만원**
개인정보 유효기간제	600만원	60만원	120만원	**540만원**
개인정보 국외이전	400만원	40만원	80만원	**360만원**
계				**1,440만원**

< 앱 개인정보 노출 사건('20.11월) >

가. 기준금액

보호법 시행령 제63조의 [별표2]는 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.

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위:만원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 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(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중기준)에 해당하지 않아, 기준금액을 유지한다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다'라고 규정하고 있다.

피심인의 경우 정보주체에게 피해가 발생하지 않은 등 위반행위의 결과가 경미하거나, 사소한 부주의 또는 시스템의 오류로 인한 것으로 인정되며 피해 발생이 없는 점, 사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 완료한 점, 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점을 고려하여 과태료 부과지침 제7조에 따라 기준금액의 30%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 420만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만원	-	180만원	**420만원**
계				**420만원**

4. 결과 공표

「개인정보 보호법」 제66조제1항 및 「개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위('21.8월 사건)는 6개월 이상 지속된 경우(제5호)에 해당하므로, 피심인이 시정조치 명령을 받은 사실과 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표

개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.

순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1		법 제29조	안전조치의무 위반 (접근통제)	2021.10.27.	시정조치 명령 과태료 부과 540만원
		법 제39의6	개인정보 유효기간제	2021.10.27.	시정조치 명령 과태료 부과 540만원
		법 제39의12	개인정보 국외이전	2021.10.27.	시정조치 명령 과태료 부과 360만원

Ⅴ. 결론

피심인의 보호법 제29조, 제39조의6, 제39조의12 위반행위에 대하여 같은 법 제39조의15(과징금의 부과 등에 대한 특례)제1항제5호, 제75조(과태료)제2항 제4호·제6호 및 제3항제3호, 제64조(시정조치 등)제1항, 제66조(결과의 공표)제1항에 따라 과징금, 과태료, 시정조치, 결과 공표 명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 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 10월 27일

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　　지 성 우　(서 명)

개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2021 - 017 - 265호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2021. 10. 27.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리 시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

2) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.

나. 피심인은 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체없이 ‘유출등이 된 개인정보 항목’, ‘유출등이 발생한 시점’, ‘이용자가 취할 수 있는 조치’, ‘정보통신서비스 제공자등의 대응조치’, ‘이용자 상담 등을 접수할 수 있는 부서 및 연락처’ 등 모든 사항을 해당 이용자에게 알려야 하며, 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 ‘이용자가 취할 수 있는 조치’, ‘정보통신서비스 제공자등의 대응조치’, ‘이용자 상담 등을 접수할 수 있는 부서 및 연락처’의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.

다. 피심인은 가.부터 나.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 903,353,000원

나. 과 태 료 : 17,400,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 초등온라인학습 ( ) 서비스를 운영하는 「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16955호, 이하 '보호법'이라 한다.)에 따른 개인정보처리자 및 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 가 초등 이용자의 개인정보 유출 흔적이 감지되었다'고 유출 신고(2021. 4. 8.)함에 따라 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사(2021. 4. 9. ~ 2021. 9. 1.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 초등온라인학습 ( ) 서비스를 운영하면서 '21. 4. 7. 기준 건의 이용자 정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원정보 (유효회원)	(필수) 이름, 아이디, 비밀번호, 생년월일, 학년, 휴대전화번호, 학부모 이름, 학부모 휴대전화번호, 학부모 생년월일 (선택) 전화번호, 이메일주소, 주소, 학교, 성별	'15. 1. 4. ~ '21. 4. 7.	
(분리보관)			
계			

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일 시		피심인의 유출인지 및 대응 내용
'21. 4. 7.	17:30	DB 관리자가 모니터링 중 비정상 쿼리 발견하여 유출 사실인지
	23:00	백과 웹서버에 웹셸 및 터널링 프로그램 존재 확인
'21. 4. 8.	13:50	한국인터넷진흥원에 개인정보 유출 신고
	17:20	유출 대상자 명*에 이메일, 문자로 유출 가능성 통지 홈페이지에 개인정보 유출 가능성에 대한 공지사항 게시 * 유출 신고 및 통지 시 초등 회원 전체(명)를 대상으로 산정
'21. 5. 7.	-	위원회는 신원미상의 자가 DB에서 회원정보 만건 조회·유출한 사실을 확인하고 이용자에게 추가 통지할 것을 안내

2) 유출규모 및 경위

(유출항목 및 규모) 신원미상의 자(이하, '해커'라 한다)가 DB에서 유출한 이용자(법정대리인 정보 포함) 개인정보(이름, 아이디, 생년월일, 학년, 학교명(코드), 이메일, 주소, 전화번호, 휴대전화번호, 학부모 이름, 학부모 휴대전화번호, 학부모 생년월일) 23,624건

※ 해커가 조회한 TOP 만건에 포함된 유효한 이용자 수는 23,624명임(탈퇴, 분리보관 등으로 USERID를 제외하고 삭제된 정보는 유효하지 않아 제외)

(유출경위) 해커가 (백과)의 웹서버에 업로드한 웹셸과 터널링 프로그램을 통해 피심인 DB의 회원정보 만건을 ( ) 웹서버를 거쳐 피심인과 이 공동 운영하는 방화벽을 통해 외부로 전송함

- ’19. 4. 2. 10:19 해커(, 미국)가 (백과) 웹서버에 웹셸( )을 업로드함

- ’20. 4. 10. 02:19 해커(, 미국)가 旣업로드된 웹셸을 통해 터널링프로그램( )을 업로드함

- ’21. 4. 7. 09:45~15:14 해커(, 미국)가 (백과)에 旣업로드된 터널링프로그램을 통해 ( ) DB에 접속하여 member 테이블의 회원정보 만건을 유출*함

* 피심인의 DB에서 개인정보를 조회하여 의 웹서버, 외부방화벽을 통해 전송된 로그가 확인(총3회)되었으며, 전달정보를 포함하여 전송되므로 파일크기는 증가함

구분	DB	웹서버	외부방화벽
전송량(Byte)	38,857,955	38,889,046	40,343,203

※ 유출에 사용된 DB 계정정보는 암호화되어 확인 불가

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 DB 접근제어 솔루션( )을 설치·운영하였으나, DB 접근제어 솔루션( )을 통한 DB 접속만 가능하도록 취급자 IP 대역( )에서 DB 직접 접속을 차단하는 정책을 수집하였으나, 화이트 리스트 방식(모든 접속을 차단하고 필요한 서비스만 허용)의 기본정책인 Any→Any Deny 정책을 기본정책으로 반영하지 않아, 취급자

IP 대역( )을 제외한 다른 IP에서 DB에 직접 접속을 하더라도 방화벽에서 차단되지 않도록 방화벽 정책을 운영한 사실이 있다.

따라서, 해커(, 미국)가 (백과) 웹서버를 경유하고, 웹서버에 설치된 터널링 프로그램을 이용하여 DB서버에 직접 접속을 시도하였으나, 피심인의 방화벽은 비정상적인 접속을 차단하지 못한 사실이 있다.

나. 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위

피심인은 개인정보취급자가 개인정보처리시스템(MSSQL)에 접속한 정보를 DB 접근제어 솔루션( )에서 스니핑 방식으로 수집하여 저장하고 있으나, DB 접근제어 솔루션 연동시 암호화된 MSSQL 인증정보를 복호화하지 않고 저장하여 DB서버에 접속한 개인정보취급자의 접속기록(식별자, 접속일시, 접속지, 수행업무 등) 중 식별자를 식별할 수 없는 형태로 저장한 사실이 있다.

다. 개인정보 유출 추가 신고·통지를 소홀히 한 행위

피심인이 최초 유출을 인지한 시점으로부터 24시간 내 '유출 흔적이 감지되었다'고 우선 신고 및 통지를 완료하였으나, 위원회 조사과정에서 해커가 피심인의 DB의 회원정보를 외부에서 조회·유출한 사실을 확인하여, 관련 내용 전달하고 추가 확인된 내용으로 신고·통지할 것을 안내('21.5.7.)하였으나, 마지막 현장조사 당일까지('21.6.30.)도 추가 신고·통지하지 않은 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 9. 10. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 9. 24., 9. 30. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

보호법 시행령 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(나목)’ 등의 조치를 하여야 한다.”라고 규정하고 있고, 제3호는 “접속기록의 위조·변조 방지를 위하여 ‘개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등을 저장 및 이의 확인·감독(가목)’ 등의 조치를 하여야 한다.”라고 규정하고 있으며, 제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시 제2020-5호, 이하 ‘고시’) 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)’, ‘개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)’ 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있고, 고시 제5조제1항은 “정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.”라고 규정하고 있다.

‘고시 해설서’는 고시 제4조제5항에 대해 정보통신서비스 제공자등은 불법적인 접근(인가되지 않은 자가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말함) 및 침해사고(해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태) 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있으며, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 하며 신규 위협 대응 등을 위하여 지속적인 업데이트 적용 및 운영·관리하여야 한다고 해설하고 있고, 고시 제5조제1항에 대해 식별자, 접속일시, 접속지, 수행업무 등을 포함하는 접속기록을 최소 1년 이상 보존·관리하여야 한다고 해설하고 있다.

나. 보호법 제39조의4제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 ‘유출등’이라 한다) 사실을 안 때에는 지체없이 ‘유출등이 된 개인정보 항목(제1호)’, ‘유출등이 발생한 시점(제2호)’, ‘이용자가 취할 수 있는 조치(제3호)’, ‘정보통신서비스 제공자등의 대응조치(제4호)’, ‘이용자 상담 등을 접수할 수 있는 부서 및 연락처(제5호)’의 사항을 해당 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니된다. ”라고 규정하고 있다.

보호법 시행령 제48조의4제3항은 “정보통신서비스 제공자등은 제2항에 따른 통지·신고를 하려는 경우에는 법 제39조의4제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 같은 항 제3호로부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고해야 한다.”라고 규정하고 있다.

「개인정보 보호법 해설서」는 법 제39조의4, 영 제48조의4제3항에 대해 “24시간 이내에 진행된 통지 및 신고 내용 중 유출등이 된 개인정보 항목 및 유출등이

발생한 시점에 관한 내용이 미흡하다는 사실만으로는 해당 통지 및 신고가 위법하다 할 수 없으나 이에 대하여는 추후에 해당 내용을 보충하여 빠른 시일 내에 통지가 이루어져야 한다.”라고 해설하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 불법적인 접근 차단}

개인정보 유출은 사회적·기술적 통념상 개인정보가 저장된 DB 등 개인정보처리시스템에 권한 없는 자가 접근한 경우를 포함한다. 또한, 표준 개인정보보호 지침 제25조에도 “개인정보의 유출은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것으로서 다음 각 호의 어느 하나에 해당하는 경우를 말한다”고 규정하며, 제2호에서 “개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우”를 규정하고 있다.

따라서 권한 없는 자가 피심인의 데이터베이스에 접근하여 개인정보를 조회한 사실이 데이터베이스 로그에서 확인되고, 데이터베이스에서 개인정보를 조회하여 웹서버, 방화벽을 통해 외부로 전송된 사실에 대해 로그, 전송용량 및 시간적 선후관계가 확인되는 등 개인정보가 유출된 것이 명확히 입증된다.

* 해커( )는 2021.4.7. DB에서 개인정보를 조회[1]하여 웹서버, 외부방화벽을 통해 전송된 로그가 확인(총3회)되었으며, 전달정보를 포함하여 전송되므로 파일크기는 증가함

1) DB조회문( )을 이용하여 만건 조회

구분	DB	웹서버	외부방화벽
총 전송량(Byte)	38,857,955	38,889,046	40,343,203
1차 조회	오전 9:45:43	오전 9:45:43	오전 9:45:43
2차 조회	오후 3:08:03	오후 3:08:03	오후 3:08:25
3차 조회	오후 3:14:13	오후 3:14:45	오후 3:14:51

※ DB, 웹서버, 외부방화벽 각각의 로그에서 데이터가 전송된 시간을 일정하게 재계산하였을 때, 2차 조회 및 3차 조회 건의 구간별 시간 지연은 공격자가 테이블 정보를 대량으로 조회하는 쿼리를 다수의 질의를 웹서버를 통해 DB로 전송하면서 DB부하, 네트워크 부하가 발생하여 응답시간이 지연된 것으로 판단됨

대법원 판례에서는, “특정 정보통신서비스제공자가 개인정보의 안전성 확보에 필요한 조치를 취하여야할 법률상 의무를 위반하였는지 여부를 판단함에 있어서는 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술수준, 정보통신서비스 제공자의 업종·영업규모와 정보통신서비스제공자가 취하고 있던 전체적인 보안 조치의 내용, 정보보안에 필요한 경제적 비용 및 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해발생의 회피가능성 등을 종합적으로 고려하여 정보통신서비스 제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부가 기준이 된다.”고 판시하였다.

피심인은 국내 대표적인 초등학생 등 아동을 대상으로 한 온라인 학습 서비스로 2020년 매출액이 억 원이고, 2021년 4월 기준 개인정보를 보관하고 있는 건수가 만 명 이상으로 일정규모 이상의 사업자에 해당하며, 피심인이 수집한 성명, 이메일, 생년월일, 휴대전화번호 등의 개인정보는 이용자를 특정할 수 있는 기본적인 개인정보로서 제3자가 이용할 경우 이용자에게 적지 않은 피해가 발생할 수 있어 보안을 철저히 할 필요가 있다. 특히, 아동은 개인정보의 중요성이나 위험성에 대한 인식이 부족하고 수집 목적의 진위를 평가하는 능력이 부족하기 때문에 아동의 개인정보를 제3자가 이용할 경우 이용자에게 더 큰 피해가 발생할 수 있으므로 더욱 보안을 철저히 할 필요가 있다.

‘모든’ 해커의 공격에 따른 개인정보 유출이 발생하지 않도록 조치를 하는 것은 현실적으로 불가능하나, 피심인은 적어도 월경 웹셸 공격을 통한 개인정보 유출 사고를 겪은바, 외부 공격자가 공개된 웹서버를 경유하여 데이터베이스에 저장된 개인정보를 유출하는 수법을 인지하였으므로, 데이터베이스에 대한 IP 제한 등의 조치를 통해 추가로 발생할 수 있는 이용자의 피해를 최소화하고, 타 사업자의 서비스와 네트워크 대역을 분리하고, 서비스에 필요한 접속만 허용하는 등의 조치를 통해 또다시 발생할 수 있는 웹셸을 통한 해킹 공격을 차단할 수 있도록 하였어야 한다.

통상적으로 개인정보가 포함된 DB는 서비스에 필요한 IP 외에는 차단하는 것이 상식이며, 고시 해설서에도 “개인정보처리시스템의 데이터베이스(DB)에의 직접 접속은 데이터베이스 운영·관리자에 한정하는 등 보호조치를 적용할 필요성이 있다.”고 해설하고 있다. IP 제한 등을 적용하는 조치를 통해 해킹을 방지하는 것은 누구나 생각할 수 있는 보편적으로 알려진 정보보안 기술 수준이고 IP 제한 조치는 장비에 정책만 설정하면 되므로 비용이 발생하지도 않으며, 적용 시 피해 발생이 줄어들 수 있는 등 사회통념상 합리적으로 기대 가능한 정도의 보호조치에 해당한다. 피심인의 백과 웹서버 IP가 서비스 DB와 직접 통신하지 않았던 점, 피심인이 후속 조치로서 내부망에서 접근할 수 없도록 즉시 정책을 수립했던 점을 고려할 때 DB의 서비스에 직접 접속이 필요한 IP는 아니었다고 판단된다.

피심인은 자사가 운영 중인 초등학생용 온라인 학습지원을 위한 ‘ ’ 서비스와 타 사업자인 의 백과 컨텐츠만 제한적으로 검색할 수 있도록 서비스를 연동하였다. 기존 백과의 사용자 계정과는 연동하지 않아 백과 서비스는 DB와는 직접 통신하지 않는 구조로 운영한 사실이 있다.

따라서, 피심인은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 서비스 운영에 반드시 필요한 IP주소 등으로 제한하여 ‘ ’ 데이터베이스에 대한 인가받지 않은 접근을 제한하였다면 유출을 방지할 수 있었으며, 타 사업자의 시스템이 동일한 IDC 내부에 존재하였음에도 사업자의 네트워크 대역을 통지하지 않고 오고 가는 패킷을 모두 허용하도록 정책을 운영하여 초등 이용자의 개인정보가 외부로 유출되게 함으로써 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제5항을 위반한 것이다.

나. 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 접속기록의 위조·변조 방지를 위한 조치}

피심인이 개인정보처리시스템에 대한 접속기록을 최소 1년 이상 보존·관리하여야 하나, 개인정보가 저장되는 DB서버에 접속하는 개인정보취급자의 접속기록 중 식별자를 식별할 수 없는 형태로 저장하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제3호, 고시 제5조제1항을 위반한 것이다.

다. 개인정보의 유출 사실을 추가 통지하지 않은 행위

{보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)}

피심인은 피심인 소속의 DB 관리자가 모니터링 중 비정상 쿼리를 발견하여 유출 가능성이 확인되어 신고하고, 전체 회원을 대상으로 공지 및 관련 내용을 통지한 사실은 있으나, 조사과정에서 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실이 추가로 확인되었음에도 마지막 현장조사 당일까지 관련 내용을 홈페이지에 공지하거나, 개인정보 유출이 확인된 이용자에게 변경된 내용을 추가 통지를 하지 않은 행위는 보호법 제39조의4, 같은 법 시행령 제48조의4를 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제, 접속기록)	보호법 §29	§48의2① 제2호·제3호	• 개인정보처리시스템에 대한 접근권한을 IP주소 등으로 제한하지 않고 개인정보처리시스템의 접근권한 정책을 일부 아이피(IP)에 대해 차단하고 나머지는 모두 허용하도록 수집하여 운영한 행위(고시§4⑤) • 개인정보취급자의 개인정보처리시스템의 접속기록을 보관 및 점검을 소홀히 한 행위(고시§5①)
개인정보 유출통지 위반	보호법 §39의4①	§48의4③④	• 추가로 확인된 개인정보 유출 사실에 대해 이용자 또는 홈페이지에 공지하지 않음

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

2) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.

나. 피심인은 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체없이 ‘유출등이 된 개인정보 항목’, ‘유출등이 발생한 시점’, ‘이용자가 취할 수 있는 조치’, ‘정보통신서비스 제공자등의 대응조치’, ‘이용자 상담 등을 접수할 수 있는 부서 및 연락처’ 등 모든 사항을 해당 이용자에게 알려야 하며, 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 ‘이용자가 취할 수 있는 조치’, ‘정보통신서비스 제공자등의 대응조치’, ‘이용자 상담 등을 접수할 수 있는 부서 및 연락처’의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.

다. 피심인은 가.부터 나.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 과징금 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15 제1항제5호, 같은 법 시행령 제48조의11제1항과 제4항, [별표 1의5] '과징금의 산정기준과 산정절차' 및 「개인정보보호 법규 위반에 대한 과징금 부과기준」(2020. 8. 5. 개인정보보호위원회 고시 제2020-6호, 이하 '과징금 부과기준'이라 한다)에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제39조의15, 같은 법 시행령 제48조의11에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의 · 중과실 여부

과징금 부과기준 제5조제1항은 '보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 시행령 제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단한다'라고 규정하고 있다.

이에 따라, 보호법 제29조(안전조치의무)를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

과징금 부과기준 제5조제3항은 '위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 매우 중대한 위반행위로 판단한다'라고 규정하고 있다.

다만, 과징금 부과기준 제5조제3항 단서에서 '위반행위의 결과가 ▲위반 정보통신서비스 제공자등이 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ▲이용자의 개인정보가 공중에 노출되지 않은 경우(제3호) 중 모두에 해당할 때에는 보통 위반행위로, 1개 이상 2개 이하에 해당하는 경우에는 중대한 위반행위로 감경한다.'라고 규정하고 있다.

이에 따라, 피심인이 개인정보 유출로 직접적인 이득을 취하지 않은 점, 이용자의 개인정보가 공중에 노출되지 않은 점을 고려하여 '중대한 위반행위'로 판단한다.

3) 기준금액 산출

피심인의 초등온라인학습 서비스에서 발생한 매출을 위반행위 관련 매출로 하고, 직전 3개 사업년도의 연평균 매출액 천원에 보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 21을 적용하여 기준금액을 천원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2018년	2019년	2020년	평 균
관련 매출액*				

* 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

<보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
보통 위반행위	1천분의 15

다. 필수적 가중 및 감경

과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 2년을 초과하는 '장기 위반행위'에 해당하므로 기준금액의 100분의 50에 해당하는 금액인 천원을 가산하고,

최근 3년 이내 보호법 제39조의15제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 천원을 감경한다.

라. 추가적 가중 및 감경

과징금 부과기준 제8조는 사업자의 위반행위 주도 여부, 조사 협력 여부 등을 고려하여 필수적 가중 · 감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

이에 따라, 피심인이 ▲조사에 적극 협력한 점, ▲개인정보 유출사실을 자진 신고한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 천원을 감경한다.

마. 과징금의 결정

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15 제1항제5호, 같은 법 시행령 제48조의11, [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 1) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 903,353천원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중·감경	추가적 가중·감경	**최종 과징금**
천원	필수적 가중 (50% : 천원) 필수적 감경 (50% : 천원)	추가적 가중 없음 추가적 감경 (20%, 천원)	**천원**
	→ 천원	→ 천원	

3. 과태료 부과

피심인의 보호법 제29조, 제39조의4제1항 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항 제6호·제12의3호 및 같은 법 시행령 제63조의 〔별표2〕 '과태료 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 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 제29조(안전조치의무) 위반행위에 관해서는 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 있으므로 2회 위반에 해당하는 과태료 1,200만원을, 제39조의4(개인정보 유출등의 통지·신고에 대한 특례) 위반행위에 대해서는 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 과태료 600만원을 적용한다.

< 「보호법」 시행령 [별표2] 2. 개별기준 >

(단위:만원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 **제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우**	법 제75조 제2항제6호	600	1,200	2,400
도. 법 **제39조의4제1항**(법 제39조의14에 따라 준용되는 경우를 포함한다)을 **위반하여 이용자**·보호위원회 및 전문기관에 **통지** 또는 신고**하지 않거나 정당한 사유 없이 24시간을 경과하여 통지** 또는 신고**한 경우**	법 제75조 제2항제12호의3	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(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중기준)에 따라 제29조(안전조치 의무) 위반행위에 대해 ▲제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상이며, ▲위반 기간이 3개월 이상인 경우로 기준금액의 20%를 가중하고, 제39조의4(개인정보 유출등의 통지·신고에 대한 특례) 위반행위에 대해서는 해당하지 않아 가중없이 기준금액을 유지한다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.'라고 규정하고 있다.

피심인의 경우 제29조(안전조치의무) 위반행위에 대해 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점, 사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 완료하지는 못하였으나 시정 중에 있는 것으로 인정되는 경우에 해당하는 점을 고려하여 과태료 부과지침 제7조에 따라 기준금액의 20%, 제39조의4(개인정보 유출등의 통지·신고에 대한 특례) 위반행위에 대해 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점을 고려하여 과태료 부과지침 제7조에 따라 기준금액의 10%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조, 제39조의4를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,740만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제, 접속기록)	1,200만원	240만원	240만원	**1,200만원**
개인정보 유출 통지 위반 (개인정보 유출 추가 통지 위반)	600만원	-	60만원	**540만원**
계				**1,740만원**

4. 결과 공표

「개인정보 보호법」 제66조제1항 및 「개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 법 제75조제2항 각호에 해당하는 위반행위를 2개 이상 한 경우(제4호), 6개월 이상 지속된 경우(제5호)에 해당하므로, 피심인이 시정조치 명령을 받은 사실과 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표 개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1		법 제29조	안전조치의무 위반 (접근통제, 접속기록)	2021.10.27.	시정조치 명령 과태료 부과 1,200만원
		법 제39의4	개인정보 유출 통지 위반	2021.10.27.	시정조치 명령 과태료 부과 540만원

Ⅴ. 결론

피심인의 보호법 제29조, 제39조의4 위반행위에 대하여 같은 법 제39조의15(과징금의 부과 등에 대한 특례)제1항제5호, 제75조(과태료)제2항 제6호·제12의3호, 제64조(시정조치 등)제1항, 제66조(결과의 공표)제1항에 따라 과징금, 과태료, 시정조치 명령, 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 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 10월 27일

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　　지 성 우　(서 명)

개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2021 - 017 - 266호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2021. 10. 27.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다. 또한, 처리중인 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다.

2) 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하기 위한 백신소프트웨어 설치 및 주기적 갱신·점검 조치하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 5,400,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 ( ) 서비스를 운영하는 「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16955호, 이하 '보호법'이라 한다.)에 따른 개인정보처리자 및 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 가 ‘ 이용자의 개인정보 유출 흔적이 감지되었다‘고 유출 신고(2021. 4. 8.)함에 따라 조사과정에서 피심인이 유출경로로 이용된 것으로 확인되어 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사(2021. 4. 9. ~ 2021. 9. 1.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 ( ) 서비스를 운영하면서 ’21. 3. 16. 기준 건의 이용자 정보를 수집하여 보관하고 있으며, ‘21. 3. 17.에 서비스 종료하여 수집·보관한 개인정보를 파기하였다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원정보	(필수) 이름, 로그인ID, 비밀번호, 이메일, 휴대폰번호, IP주소, 쿠키, 방문일시, 서비스 이용 기록 (선택) SMS, 이메일 수신 동의, 학교 종류, 학교명, 주소	’16. 8. 2. ~ ’21. 3. 16.	

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일 시		피심인의 유출인지 및 대응 내용
'21. 4. 7.	17:30	DB 관리자가 모니터링 중 비정상 쿼리 발견하여 유출 사실인지
	23:00	백과 웹서버에 웹셸 및 터널링 프로그램 존재 확인
'21. 4. 8.	13:50	한국인터넷진흥원에 개인정보 유출 신고
	17:20	유출 대상자 명*에 이메일, 문자로 유출 가능성 통지 홈페이지에 개인정보 유출 가능성에 대한 공지사항 게시 * 유출 신고 및 통지 시 회원 전체(명)를 대상으로 산정
'21. 5. 7.	-	위원회는 신원미상의 자가 DB에서 회원정보 만건 조회·유출한 사실을 확인하고 이용자에게 추가 통지할 것을 안내

2) 유출규모 및 경위

(유출항목 및 규모) 없음

※ 피심인은 의 유출경로로 이용되었고, 유출된 DB의 직접 당사자가 아님

(유출경위) 신원미상의 자(이하, '해커'라 한다)가 ( )의 웹서버에 업로드한 웹셸과 터널링 프로그램을 통해 피심인 DB의 회원정보 만건을 (백과) 웹서버와 방화벽을 통해 외부로 전송함

- '19. 4. 2. 10:19 해커(, 미국)가 ( ) 웹서버에 웹셸( )을 업로드함

※ 웹서버에 웹셸을 업로드하면, 파일명은 시간정보(타임스탬프 값)으로 저장됨

- '20. 4. 10. 02:19 해커(, 미국)가 旣업로드된 웹셸을 통해 터널링 프로그램*( )을 업로드함

* 서로 다른 네트워크를 통신을 할 수 있도록 경유지 서버에 설치되는 프로그램이며, 旣업로드된 웹셸을 이용하여 업로드 한 것으로 원본 파일명은 유지됨

- ’21. 4. 7. 09:45~15:14 해커(, 미국)가 ( )에 既업로드된 터널링프로그램을 통해 DB에 접속하여 member 테이블의 회원정보 만건을 유출*함

* 의 DB에서 개인정보를 조회하여 피심인의 웹서버, 외부방화벽을 통해 전송된 로그가 확인(총3회)되었으며, 전달정보를 포함하여 전송되므로 파일크기는 증가함

구분	DB	웹서버	외부방화벽
전송량(Byte)	38,857,955	38,889,046	40,343,203

※ 유출에 사용된 DB 계정정보는 암호화되어 확인 불가

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 방화벽·웹방화벽·침입탐지시스템을 설치·운영하고 있으나, 개인정보취급자에게 허용한 IP로 제한하지 않아 해커(, 미국)가 피심인의 웹서버를 통해 동일 IDC 내 ( ) DB서버로 접속이 가능하도록 운영한 사실이 있다. 또한, 웹방화벽에서 스크립트 파일(jsp) 업로드 탐지 정책을 적용하지 않아 웹셸(, ’19. 4. 2. 10:19) 및 터널링 프로그램(, ’20. 2. 19.)을 탐지하지 못한 사실이 있다.

나. 악성프로그램 방지를 위한 보안프로그램 설치·운영을 소홀히 한 행위

피심인은 웹셸탐지솔루션을 웹서버에 설치하였으나, 서버 부하 발생으로 상시로 운영하지 않았으며, 웹셸(, ’19.4.2. 10:19) 및 터널링프로그램(, ’20.2.19)을 탐지할 수 있는 정책이 적용되지 않아 웹셸 및 터널링 프로그램을 탐지하지 못한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 9. 10. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 10. 1. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

보호법 시행령 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(나목)’, ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있고, 제5호는 “개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료 할 수 있도록 하기 위한 백신소프트웨어 설치 및 주기적 갱신·점검 조치하여야 한다.”라고 규정하고 있으며, 제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시 제2020-5호, 이하 ‘고시’) 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP주소

등으로 제한하여 인가받지 않은 접근을 제한(제1호)', '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)' 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있고, 제9항은 "정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다."라고 규정하고 있으며, 제7조는 "정보통신서비스 제공자등은 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, '보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일1회 이상 업데이트를 실시하여 최신의 상태로 유지(제1호)', '악성프로그램관련 경보가 발령된 경우 또는 사용중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시(제2호)'사항을 준수하여야 한다."라고 규정하고 있다.

'고시 해설서'는 고시 제4조제5항에 대해 정보통신서비스 제공자등은 불법적인 접근(인가되지 않은 자가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말함) 및 침해사고(해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태) 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제 시스템 등을 활용할 수 있으며, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 하며 신규 위협 대응 등을 위하여 지속적인 업데이트 적용 및 운영·관리하여야 한다고 해설하고 있고, 제9항에 대해 인터넷 홈페이지를 통한 개인정보 유·노출 방지를 위해 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방지조치를 하여야 하며, 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 보호조치를 하여야

한다고 해설하고 있으며, 고시 제7조에 대해 정보통신서비스 제공자 등은 보안 프로그램 설치 후, 최신 상태의 보안 업데이트 적용, 보안프로그램의 정책·환경 설정 등을 통해 사내의 보안정책을 적용, 보안프로그램을 통해 발견되는 악성프로그램 등 확산 방지 조치(삭제·치료, 물리적 차단·분리 등)하는 등 설치한 보안프로그램을 적절하게 운영하여야 하며, 백신 소프트웨어 등의 보안프로그램은 실시간 감시 등을 위해 항상 실행된 상태를 유지해야 한다고 해설하고 있다.

2. 위법성 판단

대법원 판례에서는, “특정 정보통신서비스제공자가 개인정보의 안전성 확보에 필요한 조치를 취하여야 할 법률상 의무를 위반하였는지 여부를 판단함에 있어, 침해사고 당시 보편적으로 알려진 정보보안의 기술수준, 정보통신서비스 제공자의 업종·영업규모와 정보통신서비스제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해발생의 회피가능성 등을 종합적으로 고려하여 정보통신서비스 제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부가 기준이 된다.”고 판시하였다.

피심인은 국내 대표적인 교과서, 학습 관련 서비스를 제공하고 있으며, 피심인의 2020년 전체 매출액은 억으로 일정 규모의 이상의 사업자에 해당한다.

‘모든’ 해커의 공격에 따른 개인정보 유출이 발생하지 않도록 조치를 하는 것은 현실적으로 불가능하나, 적어도 피심인은 년 월 발생한 것으로 추정되는 해킹 사고를 통해 해킹을 통한 개인정보 유출 수법을 인지하였을 것이고 웹셸 공격은 잘 알려진 대표적인 해킹기법이며, 피심인이 웹서비스에서 이미지를 업로드하는 기능을 운영하면서 업로드되는 파일을 제한해야 하는 것은 보편적으로 알려진 보안기술로 피심인은 이를 적용하였어야 한다.

피심인이 웹서비스 업로드 폴더에 대한 악성코드 점검을 주기적으로 실시하였다면 추가적인 개인정보 유출을 방지할 수 있었을 것이며, 또한 업로드 디렉토리의 파일을 grep 등으로 읽어와 셸 스크립트를 탐지할 수 있고, 기존에 사용하고 있는 장비의 정책을 제대로 수립하여 운영하였다면 추가적인 비용 발생 없이도 개인정보 유출을 방지할 수 있었다. 그리고 2년 전에 업로드된 웹셸을 탐지하여 삭제하였다면 IDC 내부에 네트워크로 피해 확산 방지 및 예방되었을 것이다.

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 불법적인 접근 차단}

1) (침입차단 및 탐지시스템의 운영) 피심인은 컨텐츠를 초등학생용 온라인 학습지원을 위한 ‘ ’ 서비스에서 검색할 수 있도록 서비스를 제공하였으며, 서비스는 DB와는 직접 통신하지 않는 서비스로 운영한 사실이 있다. 따라서, 피심인이 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하지 않고 운영한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제5항을 위반한 것이다.

2) (개인정보 유·노출 방지) 피심인이 처리중인 개인정보가 인터넷 홈페이지를 통해 권한이 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 웹방화벽에서 스크립트 파일(jsp) 업로드를 탐지 정책에 적용하지 않는 등 개인정보처리시스템에 대한 보호조치를 취하지 않아 접근통제를 소홀히 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제9항을 위반한 것이다.

나. 악성프로그램 방지를 위한 보안프로그램 설치·운영을 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 악성프로그램 방지}

피심인이 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안프로그램을 설치하고 주기적으로 갱신·점검조치를 하여야 하나, 웹셸탐지솔루션 점검

등 운영을 소홀히 하여 웹셸을 탐지하지 못한 행위는 보호법 제29조, 같은 법 시행령 제48조의2, 고시 제7조를 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제, 악성프로그램 방지)	보호법 §29	§48의2① 제2호·제5호	• 개인정보처리시스템에 대한 접근권한을 IP주소 등으로 제한하지 않고 운영한 행위(고시§4⑤) • 열람권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨) • 악성프로그램 방지를 위한 보안프로그램 설치·운영을 소홀히 한 행위(고시§7)

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

2) 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

3) 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하기 위한 백신소프트웨어 설치 및 주기적 갱신·점검 조치하여야 한다.

나. 피심인은 가의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 과태료 부과

피심인의 보호법 제29조 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제6호 및 같은 법 시행령 제63조의 [별표2] '과태료 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 시행령 제63조의 [별표2]는 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 과태료 600만원을 적용한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위:만원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
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(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.'라고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중기준)에 따라 ▲제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상이며, ▲위반 기간이 3개월 이상인 경우로 기준금액의 20%를 가중한다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.'라고 규정하고 있다.

피심인의 경우 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점, 사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 완료하지는 못하였으나 시정 중에 있는 것으로 인정되는 경우에 해당하는 점, 정보보호 관리체계 인증(ISMS)을 획득한 점 등을 고려하여 과태료 부과지침 제7조에 따라 기준금액의 30%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 540만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제, 악성프로그램 방지)	600만원	120만원	180만원	**540만원**
계				**540만원**

4. 결과 공표

「개인정보 보호법」 제66조제1항 및 「개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 6개월 이상 지속된 경우(제5호)에 해당하므로, 피심인이 시정조치 명령을 받은 사실과 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표

개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.

순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1		법 제29조	안전조치의무 위반 (접근통제, 악성프로그램 방지)	2021.10.27.	시정조치 명령 과태료 부과 540만원

Ⅴ. 결론

피심인의 보호법 제29조 위반행위에 대하여 같은 법 제75조(과태료)제2항 제6호, 제64조(시정조치 등)제1항, 제66조(결과의 공표)제1항에 따라 과태료, 시정조치 명령, 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 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 10월 27일

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 흥 열　(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 - 017 - 267호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2021. 10. 27.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체없이 '유출등이 된 개인정보 항목', '유출등이 발생한 시점', '이용자가 취할 수 있는 조치', '정보통신서비스 제공자등의 대응조치', '이용자 상담 등을 접수할 수 있는 부서 및 연락처' 등 모든 사항을 해당 이용자에게 알려야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지해서는 아니 된다.

나. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 시스템을 설치·운영하여야 한다. 또한, 처리중인 개인정보가 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다.

2) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.

3) 정보통신서비스 제공자 등은 비밀번호는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

4) 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하기 위한 백신소프트웨어 설치 및 주기적 갱신·점검 조치하여야 한다.

다. 피심인은 가.부터 나.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 17,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 ( ) 서비스를 운영하는 「舊정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2020. 8. 5. 법률 제16955호로 개정·시행되기 이전의 것, 이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회[1]는 이 신원미상의 자(이하 '해커')로부터 이용자의 개인정보를 일부 제시하면서 금전을 요구하는 협박을 받아 유출 신고(2020. 7. 22.)함에 따라 개인정보 취급·운영 실태 및 정보통신망법 위반 여부를 조사(2021. 1. 11. ~ 2021. 6. 18.)하였으며, 다음과 같은 사실을 확인하였다.

1) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라, 개인정보보호위원회가 방송통신위원회의 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제1항), 법 시행 전 방송통신위원회가 행한 고시·행정처분 중 그 소관이 방송통신위원회에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제4항)

2. 행위 사실

가. 개인정보 수집현황

피심인은 ( ) 서비스를 운영하면서 ’21. 1. 14. 기준 건의 이용자 정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
유효회원	(필수) 아이디, 비밀번호, 성명, 생년월일, 성별, 휴대전화번호, 거주지역 (선택) 이메일	’00. 6. 2. ~ ’21. 1. 14.	
분리보관			
계			

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일 시		피심인의 유출인지 및 대응 내용
’20. 7. 21.	15:36	해커가 카카오톡을 통해 유출정보 샘플(개)를 전달
	15:36	샘플(개) 비교 결과, 피심인의 DB와 일치하여 유출 사실 인지
’20. 7. 22.	14:21	한국인터넷진흥원에 개인정보 유출 신고
	14:49	홈페이지에 해킹 정황 사실 안내
’21. 5. 24.	-	유출 대상자 명에게 유출 사실 통지

2) 유출규모 및 경위

(유출항목 및 규모) ’20. 7. 21.에 해커가 전달한 회원의 개인정보(아이디, 이름, 휴대전화번호, 이메일) 총 건

(유출경위) 해커가 이미지 서버의 취약점을 이용하여 웹셸을 올리고, DB에 보관 중인 개인정보를 유출한 것으로 추정*

* 조사 결과, 웹서버·이미지 서버에서 중국 IP(/)에 약 92M의 정보를 전송하였으나, 전송한 정보 내 개인정보 포함 여부는 웹서버·이미지서버·DB서버의 로그가 없어 확인이 불가함

3. 개인정보의 취급・운영 관련 사실관계

가. 개인정보 유출 통지를 소홀히 한 행위

피심인은 '20. 7. 21.에 해커가 제공한 개인정보 DB 건이 피심인의 DB와 일치함을 확인하여 유출 사실을 인지하고 '20. 7. 22.에 개인정보보호 포털에 신고하였으나, 개인정보가 유출된 이용자 명에게는 정당한 사유 없이 24시간을 경과하여 약 10개월 뒤인 2021. 5. 24.에 유출을 통지한 사실이 있음

나. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 웹방화벽, 침입탐지시스템, 웹셸 탐지 솔루션 등 보안장비를 설치하고 차단 및 탐지 정책을 운영하고 있으나, 웹방화벽에서 jpg 등 일부 확장자를 차단 정책에서 예외*처리하여 운영한 사실이 있다. 또한, 이미지 서버의 게시판 프로그램에 대한 취약점**을 개선하지 않아 웹셸이 업로드되어 실행된 사실이 있다.

* 업로드 검사 예외처리 파일 : bmp, doc, docx, gif, hwp, jpg, jpge, pdf, ppt, pptx, xls, xlsx, zip

** 2.0 Basic 버전 취약점('13. 7. 발표) : 파일에서 업로드된 파일의 이름 및 확장자를 필터링 로직 우회 가능

※ 이미지 서버의 업로드 디렉토리( )에 종의 웹셸이 업로드됨('16.1.7.~'20.7.22.)

다. 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위

피심인은 개인정보가 저장되는 DB서버에 개인정보취급자가 접속한 접속기록

(식별자, 접속일시, 접속지, 수행업무 등)을 보존·관리하지 않은 사실이 있다.

라. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

피심인은 이미지 서버의 ‘ ’ 파일에 DB계정 및 비밀번호를 저장하면서 비밀번호를 암호화하지 않고 평문으로 저장한 사실이 있다.

마. 악성프로그램 방지를 위한 보안프로그램 설치·운영을 소홀히 한 행위

피심인은 웹셸탐지솔루션을 설치하였으나, 모니터링 대상에 이미지 서버의 업로드 디렉토리( )를 포함하지 않아 웹셸이 업로드되어 실행된 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 6. 25. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 7. 9. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제27조의3제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 ‘유출등’이라 한다) 사실을 안 때에는 지체없이 ‘유출등이 된 개인정보 항목(제1호)’, ‘유출등이 발생한 시점(제2호)’, ‘이용자가 취할 수 있는 조치(제3호)’, ‘정보통신서비스 제공자등의 대응조치(제4호)’, ‘이용자 상담 등을 접수할 수 있는 부서 및 연락처(제5호)’의 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니된다.”라고 규정하고 있다.

정보통신망법 시행령 제14조의2제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제27조의3제1항 각 호의 모든 사항을 서면등의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.”고 규정하고 있으며, 제2항은 “정보통신서비스 제공자등은 법 제27조의3제1항 제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.”라고 규정하고 있으며, 제3항은 “정보통신서비스 제공자등은 법 제27조의3제1항 각 호외의 부분 단서에 따른 정당한 사유가 있는 경우에는 법 제27조의3제1항 각 호의 사항을 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항의 통지를 갈음할 수 있다.”라고 규정하고 있다.

「정보통신망법 해설서」는 정보통신망법 제27조의3제1항의 ‘지체 없이’에 대해서 정보통신망법에 별도로 규정된 정의는 없으나, 관련 판례에서는 ‘합리적인 이유 및 근거가 없는 한 즉시’로 해석하고 있다.

나. 정보통신망법 제28조제1항은 정보통신서비스 제공자등은 개인정보를 처리할 때 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손을 방지하고 개인정보의 안정성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영 등 기술적·관리적 조치를 하여야 한다고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 ’개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)‘, ’그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)’ 등을 하여야 한다고 규정하고 있고, 제3항은 정보통신서비스 제공자등은 접속기록의 위조 · 변조 방지를 위하여 ‘개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인 · 감독(제1호)’ 등의 조치를 하여야 한다고 규정하고 있으며,

제4항은 정보통신서비스 제공자등은 개인정보가 안전하게 저장 · 전송될 수 있도록 '비밀번호의 일방향 암호화 저장(제1호)' 등의 보안조치를 하여야 한다고 규정하고 있고, 제5항은 정보통신서비스 제공자등은 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검 · 치료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로 갱신 · 점검하여야 한다고 규정하고 있다.

정보통신망법 시행령 제15조제6항에 따라 위 기준 수립 · 시행의 내용을 구체적으로 정하고 있는 「舊개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2019-13호, 이하 '고시') 제4조제5항은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)', '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)' 기능을 포함한 시스템을 설치·운영하여야 한다고 규정하고 있고, 제4조제9항은 처리 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다고 규정하고 있고, 제5조제1항에서는 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다고 규정하고 있으며, 제6조제1항에서는 정보통신서비스 제공자등은 비밀번호는 복호화되지 아니하도록 일방향 암호화하여 저장한다고 규정하고 있고, 제7조에서는 정보통신서비스 제공자등은 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안프로그램을 설치·운영하여야 하며, '보안프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지(제1호)'를 준수해야 한다고 규정하고 있다.

'고시 해설서'는 고시 제4조제5항에 대해 정보통신서비스 제공자등은 불법적인 접근(인가되지 않은 자가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말함) 및 침해사고(해킹, 컴퓨터바이러스, 논리폭탄,

메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태) 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있으며, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 하며 신규 위협 대응 등을 위하여 지속적인 업데이트 적용 및 운영·관리하여야 한다고 해설하고 있고, 고시 제4조제9항에 대해 인터넷 홈페이지를 통한 개인정보 유·노출 방지를 위해 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방지조치를 하여야 하며, 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등에 관한 보호조치를 하여야 한다고 해설하고 있으며, 고시 제5조제1항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무의 확인 등을 위해 식별자, 접속일시, 접속지, 수행업무 등을 포함하는 접속기록을 최소 1년 이상 보존·관리하여야 한다고 해설하고 있고, 고시 제7조에 대해 보안프로그램은 그 목적과 기능에 따라 다양한 종류의 제품이 있으므로, 정보통신서비스 제공자등은 스스로의 환경에 맞는 보안프로그램을 설치하고, 보안프로그램의 정책·환경 설정 등을 통해 사내의 보안정책을 적용하는 등 설치한 보안프로그램을 적절하게 운영하여야 한다고 해설하고 있다. 특히 대규모의 개인정보를 처리하거나 주민등록번호, 금융정보 등 중요도가 높은 개인정보를 처리할 때는 키보드, 화면, 메모리해킹, 랜섬웨어 등 신종 악성 프로그램에 대해 대응할 수 있도록 보안프로그램을 운영할 필요가 있으며, 항상 최신의 상태로 유지하여야 한다고 해설하고 있다.

2. 위법성 판단

가. 개인정보 유출통지를 소홀히 한 행위

{정보통신망법 제27조의3(개인정보 유출등의 통지·신고)제1항}

피심인이 해커가 카카오톡을 통해 전달받은 유출정보 샘플(건) 비교 결과, 피심인의 DB와 일치하여 개인정보의 유출 사실을 안 때('21.7.21. 15:36)로부터 정당한 사유 없이 약 10개월이 지난 후에 개인정보 유출 사실을 통지한 행위는 舊정보통신망법 제27조의3제1항, 같은 법 시행령 제14조의2 위반한 것이다.

나. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{정보통신망법 제28조(개인정보 보호조치)제1항 중 접근통제}

1) (침입차단 및 탐지시스템의 운영) 피심인이 침입차단시스템 등 접근 통제 장치의 운영을 소홀히 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항, 고시 제4조제5항을 위반한 것이다.

2) (개인정보 유·노출 방지) 피심인이 처리중인 개인정보가 인터넷 홈페이지를 통해 권한이 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 피심인이 취약점을 개선하지 아니한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항, 고시 제4조제9항을 위반한 것이다.

다. 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위

{정보통신망법 제28조(개인정보 보호조치)제1항 중 접속기록의 위조 · 변조 방지}

피심인이 개인정보가 저장되는 DB서버에 개인정보 취급자의 접속기록을 보존·관리하지 않은 행위는 정보통신망법 제28조제1항제3호, 같은 법 시행령 제15조제3항, 고시 제5조제1항을 위반한 것이다.

라. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

{정보통신망법 제28조(개인정보 보호조치)제1항 중 개인정보의 암호화}

피심인이 이미지 서버의 ‘ ’ 파일에 DB를 접속하는 비밀번호를 암호화하지 않고 평문으로 저장한 행위는 정보통신망법 제28조제1항제4호, 같은 법 시행령

제15조제3항, 고시 제6조제1항을 위반한 것이다.

마. 악성프로그램 방지를 위한 보안프로그램 설치·운영을 소홀히 한 행위

{정보통신망법 제28조(개인정보 보호조치)제1항 중 악성프로그램 방지}

피심인이 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치하고 주기적으로 갱신·점검조치를 하여야 하나, 웹셸탐지솔루션 점검 등 운영을 소홀히 하여 웹셸을 탐지하지 못한 행위는 정보통신망법 제28조 제1항제5호, 같은 법 시행령 제16조제5항, 고시 제7조를 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보 유출통지 위반	정보통신망법 §27조의3①	§14조의2	• 개인정보 유출통지 지연
안전조치의무 위반 (접근통제, 접속기록, 암호화, 악성프로그램 방지)	정보통신망법 §28조①	§15조	• 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위(고시§4) • 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위(고시§5) • 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위(고시§6) • 악성프로그램 방지를 위한 보안프로그램 설치·운영을 소홀히 한 행위(고시§7)

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체없이 ‘유출등이 된 개인정보 항목’, ‘유출등이 발생한 시점’, ‘이용자가 취할 수 있는 조치’, ‘정보통신서비스 제공자등의 대응조치’, ‘이용자 상담 등을 접수할 수 있는 부서 및 연락처’ 등 모든 사항을 해당 이용자에게 알려야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지해서는 아니 된다.

나. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 시스템을 설치·운영하여야 한다. 또한, 처리중인 개인정보가 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다.

2) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.

3) 정보통신서비스 제공자 등은 비밀번호는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

4) 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하기 위한 백신소프트웨어 설치 및 주기적 갱신·점검 조치하여야 한다.

다. 피심인은 가.부터 나.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 과징금 미부과

피심인의 정보통신망법 제28조제1항 위반행위는 「舊개인정보보호 법규 위반에 대한 과징금 부과기준」(방통위 고시, 제2019-12호) 제9조의 위반행위가 경미하여 시정조치로 갈음할 수 있는 경우*에 해당하여 과징금을 미부과하나, 추후 100건 이상의 개인정보 유출이 확인되면 과징금을 부과한다.

* (ii) 개인정보 유출규모가 100건 미만으로 피해가 발생하지 않거나, 미미한 경우에 해당

3. 과태료 부과

피심인의 정보통신망법 제27조의3제1항, 제28조제1항 위반행위에 대한 과태료는 같은 법 제76조(과태료)제1항제2의3호·제3호, 같은 법 시행령 제74조의 〔별표9〕 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(2018. 7. 4. 방송통신위원회 의결, 이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 부과지침 제6조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 위반행위별 1회 위반에 해당하는 1,000만원을 각각 적용한다.

< 「정보통신망법」 시행령 [별표9] 2. 개별기준 >

(단위:만원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
하. **법 제27조의3제1항**(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·방송통신위원회 및 한국인터넷진흥원에 통지 또는 신고하지 않거나 정당한 사유없이 **24시간을 경과하여 통지** 또는 신고한 경우	법 제76조 제1항제2호의3	1,000	2,000	3,000
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 사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲조사방해, ▲위반의 정도, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중기준)에 따라 보호조치 위반 행위는 ▲위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상인 경우(제3호)로 기준금액의 10%를 가중하고, 개인정보 유출통지 위반행위에 대해서는 과태료 부과지침 제8조(과태료 가중기준)에 해당하지 않아 가중없이 기준금액을 유지한다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲사업규모·자금사정, ▲개인(위치)정보보호 노력정도, ▲조사협조 및 자진시정 등, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

피심인의 경우 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점, 사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 완료하지는 못하였으나 시정 중에 있는 것으로 인정되는 경우에 해당하는 점등을 고려하여 과태료 부과지침 제7조에 따라 기준금액의 20%를 각각 감경한다.

다. 최종 과태료

피심인의 정보통신망법 제27조의3제1항, 제28조제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,700만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보 유출통지 위반	1,000만원	0만원	200만원	**800만원**
개인정보 보호조치 위반 (접근통제, 접속기록, 암호화, 악성프로그램 방지)	1,000만원	100만원	200만원	**900만원**
계				**1,700만원**

4. 결과 공표

「개인정보 보호법」 제66조제1항 및 「개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 제75조제2항 각호에 해당하는 위반행위를 2개 이상 한 경우(제4호), 위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)에 해당하므로, 피심인이 시정조치 명령을 받은 사실과 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다.

「정보통신망 이용촉진 및 정보보호에 관한 법률」위반 행정처분 결과 공표

정보통신망법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.

순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1		정보통신망법 제27조의3①	개인정보 유출통지 위반	2021.10.27.	시정조치 명령 과태료 부과 800만원
		정보통신망법 제28조①	보호조치 위반 (접근통제, 접속기록, 암호화, 악성프로그램 방지)	2021.10.27.	시정조치 명령 과태료 부과 900만원

Ⅴ. 결론

피심인의 정보통신망법 제27조의3제1항, 제28조제1항 위반행위에 대하여 같은 법 제76조(과태료)제1항제2의3호·제3호, 제64조(시정조치 등)제1항, 보호법 제66조(결과의 공표)제1항에 따라 과태료, 시정조치 명령, 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 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 10월 27일

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　　지 성 우　(서 명)

개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2021 - 017 - 268호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2021. 10. 27.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보취급자가 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하고, 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제 장치를 운영하여야 하며, 처리중인 개인정보가 열람 권한이 없는 자에게 공개되지 않도록 조치를 하여야 한다.

2) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 5,400,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

피심인은 ( ) 서비스를 운영하는 「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16955호, 이하 '보호법'이라 한다.)에 따른 개인정보처리자 및 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 가 자사 고객들에게 신원미상의 자(이하 '해커')에 의해 광고성 문자가 발송되어 유출 신고('20. 12. 5.)함에 따라 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사(2021. 2. 23. ~ 2021. 5. 13.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 서비스를 운영하면서 '21. 5. 10. 기준 건의 이용자 정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원정보	(필수) 핸드폰번호, 닉네임 (선택) 이름, 이메일주소	'20. 9. 15. ~ '21. 5. 10.	

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일 시		피심인의 유출인지 및 대응 내용
'20.12.4.	16:13	대표에게 를 사칭한 광고 문자가 발송
	16:35	유출 대상자에 문자로 유출 사실 통지
'20.12.5.	13:36	한국인터넷진흥원에 개인정보 유출 신고
'20.12.11.	17:18	개인정보 유출사고 관련 홈페이지 팝업 게시

2) 유출규모 및 경위

(유출항목 및 규모) 확인 불가*

* 유출 신고 시 명('20.12.4.기준 이용자)을 유출 대상으로 신고하였으나, 조사 결과 개인정보 유출 사실 및 관리자페이지를 통한 문자발송 내역이 확인되지 않음

(유출경위) 웹셸 업로드를 통해 개인정보가 유출된 것으로 추정

- '20. 12. 4. 13:50, 14:27 해커가 의 관리자페이지의 업로드 페이지를 통해 웹셸 업로드

- '20. 12. 4. 16:13 를 사칭한 문자가 발송됨

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 개인정보취급자가 개인정보처리시스템에 외부에서 접속 시 안전한 인증수단을 적용하지 않고 계정·비밀번호만으로 접속한 사실이 있으며, 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하거나, 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 시스템을 설치·운영하지 않은 사실이 있다. 또한, 처리중인 개인정보가 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 하나, 파일 업로드 페이지에 확장자 제한 등 취약점 점검 및 개선조치를 하지 않은 사실이 있다.

나. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위

피심인은 개인정보처리시스템에 접속한 개인정보취급자의 접속기록(식별자, 접속일시, 접속지, 수행업무 등)을 보존·관리하지 않은 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 6. 10. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 6. 24. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

보호법 시행령 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(나목)’, ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있고, 제3호는 “접속기록의 위조·변조 방지를 위하여 ‘개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등을 저장 및 이의 확인·감독(가목)’ 등의 조치를 하여야 한다.”라고 규정하고 있고, 제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시 제2020-5호, 이하 ‘고시’) 제4조제4항은 “개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.”라고 규정하고 있고, 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인

접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)’, ‘개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)’ 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있으며, 제4조제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.” 라고 규정하고 있다. 또한, 제5조제1항은 “정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.”라고 규정하고 있다.

‘고시 해설서’는 고시 제4조제4항에 대해 외부에서 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만을 이용할 경우 유출 위험이 커지기 때문에 계정(ID)과 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 인증서, 보안토큰, 휴대전화 인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단의 적용이 필요하다고 해설하고 있고, 제5항에 대해 정보통신서비스 제공자등은 불법적인 접근(인가되지 않은 자가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말함) 및 침해사고(해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태) 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제 시스템 등을 활용할 수 있으며, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 하며 신규 위협 대응 등을 위하여 지속적인 업데이트 적용 및 운영·관리하여야 한다고 해설하고 있으며, 제9항에 대해 인터넷 홈페이지를 통한 개인정보 유·노출 방지를 위해 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방지 조치를 하여야 하며, 권한 설정 등의

조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등에 관한 보호조치를 하여야 한다고 해설하고 있다. 또한, 고시 제5조제1항에 대해 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여 개인정보 처리를 위한 업무수행과 관련이 없거나 과도한 개인정보의 조회, 정정, 다운로드, 삭제 등 비정상적인 행위를 탐지하고 적절한 대응조치를 하여야 한다고 해설하고 있으며, 개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무의 확인을 위해 ⅰ)식별자(개인정보처리시스템에서 개인정보취급자를 식별할 수 있도록 부여된 ID 등), ⅱ)접속일시(개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시점) 〈년-월-일, 시:분:초〉, ⅲ)접속지(개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등), ⅳ)수행업무(개인정보처리시스템에서 개인정보취급자가 처리한 내용을 알 수 있는 정보) 〈개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위〉 등을 포함하는 접속기록을 최소 6개월 이상 보존·관리하여야 한다고 해설하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 불법적인 접근 차단}

1) (안전한 인증수단) 피심인이 개인정보처리시스템에 정보통신망을 통해 외부에서 접속 시 안전한 인증수단을 적용하지 않고 아이디·비밀번호만으로 접속하도록 운영한 행위는 보호법 제29조, 같은 법 시행령 제48조의2, 고시 제4조제4항을 위반한 것이다.

2) (침입차단 및 탐지시스템의 운영) 피심인이 침입차단·탐지시스템을 설치·운영하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제5항을 위반한 것이다.

3) (개인정보 유·노출 방지) 피심인이 처리중인 개인정보가 인터넷 홈페이지를 통해 권한이 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 파일 업로드 페이지 확장자 제한 등 취약점 점검 및 개선조치를 취하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제9항을 위반한 것이다.

나. 개인정보처리시스템에 접속한 기록의 보관 및 점검을 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 접속기록의 위·변조 방지}

피심인은 개인정보취급자가 개인정보처리시스템(웹서버 및 DB 서버)에 접속한 기록을 월1회 이상 정기적으로 확인·감독하지 않았고 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하지 아니한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제3호, 고시 제5조제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제, 접속기록)	보호법 §29	§48의2① 제2호·제3호	• 개인정보취급자가 외부에서 개인정보처리시스템에 접속 시 안전한 인증수단을 적용하지 않은 행위 (고시§4④) • 개인정보처리시스템에 침입차단·탐지시스템을 설치·운영하지 않은 행위 (고시§4⑤) • 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨) • 개인정보취급자의 개인정보처리시스템의 접속기록을 보관 및 점검을 소홀히 한 행위(고시§5①)

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·

관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보취급자가 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하고, 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제 장치를 운영하여야 하며, 처리중인 개인정보가 열람 권한이 없는 자에게 공개되지 않도록 조치를 하여야 한다.

2) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 과태료 부과

피심인의 보호법 제29조 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제6호 및 같은 법 시행령 제63조의 〔별표2〕 '과태료 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 시행령 제63조의 [별표2]는 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 과태료 600만원을 적용한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위:만원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
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(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.'라고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중기준)에 따라 ▲제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상인 경우로 기준금액의 10%를 가중한다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다'라고 규정하고 있다.

피심인의 경우 사전통지 및 의견제출 기간이 종료되기 전에 위반행위를 중지하는 등 시정을 완료한 점, 소기업인 점등을 고려하여 과태료 부과지침 제7조에 따라 기준금액의 20%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 540만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제, 접속기록)	600만원	60만원	120만원	**540만원**
계				**540만원**

Ⅴ. 결론

피심인의 보호법 제29조 위반행위에 대하여 같은 법 제75조(과태료)제2항 제6호, 제64조(시정조치 등)제1항에 따라 과태료, 시정조치 명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 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 10월 27일

위 원 장　　윤 종 인　(서 명)

부위원장　　최 영 진　(서 명)

위　　원　　고 성 학　(서 명)

위　　원　　강 정 화　(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　　지 성 우　(서 명)

개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2021 - 017 - 269호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2021. 10. 27.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.

2) 처리중인 개인정보가 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 9,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

피심인은 쇼핑몰( )을 운영하는 「(구)정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2020. 8. 5. 법률 제16955호로 개정·시행되기 전의 것, 이하 '정보통신망법'이라 한다)에 따른 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회[2]는 개인정보보호포털(privacy.go.kr)에 유출 신고('20. 4. 3.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('20. 11. 7. ~ '21. 8. 11.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 쇼핑몰을 운영하면서 '20. 12. 7. 기준 건의 이용자 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
회원정보	이름, 아이디, 생년월일, 전화번호, 휴대전화번호, 이메일주소	'16. 11. 18. ~ '20. 12. 7.	

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일 시		피심인의 유출인지 및 대응 내용
'20. 4. 3.	00:20	관리자 페이지에 로그인 과정에서 패스워드 미일치로 접속불가 사실 확인
	01:00	개발사 문의 결과 관리자 비밀번호 변경 및 무단 접속 확인
	16:30	악성 스크립트 관련 취약점 패치 완료

2) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라, 개인정보보호위원회가 방송통신위원회의 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제1항), 법 시행 전 방송통신위원회가 행한 고시·행정처분 중 그 소관이 방송통신위원회에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제4항)

	18:00	개발사 추가분석 후 개인정보 포함 엑셀파일 다운로드 사실 인지
	20:02	개인정보보호 포털을 통한 유출 신고
	20:08	이용자 대상 개인정보 유출 사실 통지

2) 유출규모 및 경위

(유출항목 및 규모) 이름, 전화번호, 휴대전화번호, 배송지 주소 등 이용자의 개인정보 총 건(주문내역 화면 페이지 내 포함된 일간의 주문내역)

(유출 경위) 신원 미상의 자가 1:1 문의 게시판에 웹셸 공격으로 탈취한 쿠키·세션 등을 이용하여 관리자 계정으로 로그인 후, 이용자 주문내역을 다운로드

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보가 열람권한이 없는 자에게 공개되지 않도록 하는 접근 통제를 소홀히 한 행위

피심인은 개인정보처리시스템의 관리자페이지에 외부에서 접속 시 안전한 인증수단을 적용하지 않고 아이디·비밀번호만으로 접속할 수 있도록 운영하였으며, 웹셸 공격을 예방하기 위한 취약점 조치 등을 실시하지 않아 건의 이용자 개인정보가 공개되도록 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’21. 8. 20. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 9. 8. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제28조제1항은 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령이 정하는 기준에 따라 '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영(제2호)' 및 '그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치(제6호)'를 하여야 한다고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영' 및 '그 밖에 개인정보에 대한 접근 통제를 위하여 필요한 조치'를 하여야 한다고 규정하고 있다.

개인정보의 기술적·관리적 보호조치 기준(방송통신위원회고시, 2020.1.2., 이하 '고시'라 한다) 제4조는 '정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.(제4항)', '정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.(제9항)'고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{정보통신망법 제28조(개인정보의 보호조치)}

피심인이 이용자의 개인정보가 열람 권한이 없는 자에게 공개되도록 한 행위는 정보통신망법 제28조제1항, 같은 법 시행령 제15조제2항, 고시 제4조제4항 및 제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보 보호조치 위반(접근통제)	§28①	§15②	- 외부에서 개인정보처리시스템에 접속 시 안전한 인증 수단을 적용하지 않은 행위(고시§4④) - 처리중인 개인정보가 열람권한이 없는 자에게 공개되지 않도록 조치를 취하지 않은 행위(고시§4⑨)

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.

2) 처리중인 개인정보가 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 과태료 부과

피심인의 정보통신망법 제28조제1항 위반행위에 대한 과태료는 같은 법 제76조(과태료)제1항제3호, 같은 법 시행령 제74조의 〔별표9〕 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(2018. 7. 4. 방송통신위원회 의결, 이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 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 1,000만원을 적용한다.

< 정보통신망법 시행령 [별표9] 2. 개별기준 >

(단위:만원)

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 사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲조사방해, ▲위반의 정도, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중기준)에 해당하지 않아 가중 없이 기준금액을 유지한다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

피심인의 경우 시정조치(안) 사전통지 및 의견제출 기간 내에 법규 위반행위에 대하여 시정 완료한 점 등을 고려하여 기준금액의 10%인 100만원을 감경한다.

다. 최종 과태료

피심인의 정보통신망법 제28조제1항을 위반한 행위에 대해 기준금액에 가중·감경을 거쳐 총 900만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보 보호조치 위반 (접근통제)	1,000만원	0	100만원	**900만원**

Ⅴ. 결론

피심인의 정보통신망법 제28조(개인정보의 보호조치) 위반행위에 대하여 같은 법 제76조(과태료)제1항제3호,「개인정보 보호법」제64조(시정조치 등)제1항에 따라 과태료, 시정조치 명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 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 10월 27일

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 흥 열　(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 - 017 - 270호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2021. 10. 27.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 법령에서 허용하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용하지 아니하여야 한다.

나. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인

개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영하여야 한다.

2) 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

3) 처리중인 비밀번호는 복호화되지 아니하도록 일방향 암호화하여 저장하고, 처리중인 주민등록번호는 안전한 암호알고리즘을 이용하여 암호화하여 저장하여야 한다.

다. 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

라. 피심인은 가.부터 다.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 4,567,000원

나. 과 태 료 : 15,000,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 서비스를 운영하는 개인정보 보호법」(2020. 8. 5. 시행, 법률 제16955호, 이하 '보호법'이라 한다.)에 따른 개인정보처리자 및 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 국내 어학원 개인정보 7만여 건이 다크웹에 공개되었다는 언론보도*를 인지함에 따라 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사(2021. 1. 11. ~ 2021. 6. 4.)하였으며, 다음과 같은 사실을 확인하였다.

* 딥웹에 국내 어학원 회원정보 추정 7만여건 유출... 주민번호 포함(보안뉴스, '20.12.28.)

2. 행위 사실

가. 개인정보 수집현황

피심인은 서비스를 운영하면서 ’21. 1. 25. 기준 건의 이용자 정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원정보 (유효회원)	(필수) 이름, 아이디, 비밀번호(평문), 핸드폰번호, 이메일, 주소, 직업, 주민등록번호(평문) (선택) 학년, 주소, 전화번호, 생년월일, 성별	’10. 4. 24. ~ ’21. 1. 25.	

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일 시		피심인의 유출인지 및 대응 내용
’20.11.28.	13:00	언론사를 통해 개인정보 유출정보 샘플(개) 획득
	18:00	샘플(개) 비교 결과, 피심인의 DB와 일치하여 유출 사실 인지
’20.11.29.	15:00	한국인터넷진흥원에 개인정보 유출 신고 개인정보 유출사고 관련 공지사항 게시
	18:00	유출 대상자 명에게 이메일로 유출 사실 통지

2) 유출규모 및 경위

(유출항목 및 규모) ’20. 11. 25.에 해킹포럼사이트( )에 공개된 회원의 개인정보(이름, 아이디, 비밀번호(평문), 핸드폰번호, 이메일, 주소, 직업, 주민등록번호(평문) 등) 총 건

(유출경위) 해커의 SQL삽입공격으로 DB에 보관 중인 개인정보가 유출되었으며, 해킹포럼사이트(RAID Forums)에 개인정보가 공개됨

- ’20. 11. 24. 해커(, 네덜란드)가 피심인의 게시판( )을 대상으로 다양한 SQL Injection 공격이 시도되었으며, 회원 테이블에 보관중인 개인정보가 유출됨

3. 개인정보의 취급・운영 관련 사실관계

가. 법령상 근거 없이 이용자의 주민등록번호를 수집·이용한 행위

피심인은 ’10. 4. 24. ~ ’14. 3. 29. 동안 회원가입 시 본인확인을 목적으로 주민등록번호를 수집하였으며, ’20. 11. 28.까지 주민등록번호를 보유한 사실이 있다.

나. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하거나 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영하지 않고, SQL삽입공격을 예방하기 위한 시큐어 코딩 및 취약점 점검을 실시하지 않아 개인정보가 유출된 사실이 있다.

다. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

피심인은 이용자 계정 건의 비밀번호와 보유한 주민등록번호 건을 암호화하지 않고 평문으로 저장한 사실이 있다.

라. 장기 미이용자의 개인정보 파기 등 필요한 조치를 하지 않은 행위

피심인은 ’20. 11. 24. 기준 1년 이상 접속하지 않은 회원 건의 개인정보를 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 6. 23. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 7. 13. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 보호법 제24조의2제1항은 “개인정보처리자는 ‘법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우(제1호)’, ‘정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우(제2호)’, ‘제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우(제3호)’를 제외하고는 주민등록번호를 처리할 수 없다.”라고 규정하고 있다.

나. 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 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

보호법 시행령 제48조의2제1항 제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘침입차단시스템 및 침입탐지시스템의 설치·운영(나목)’, ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있고, 제4호는 “개인정보가 안전하게 저장·전송될 수 있도록 ‘비밀번호의 일방향 암호화 저장(가목)’, ‘주민등록번호, 계좌번호 등 보호위원회가 정하여 고시하는 정보의 암호화 저장(나목)’를 하여야 한다.”라고 규정하고 있으며, 제3항은

“제1항에 따른 안전성 확보조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시 제2020-5호, 이하 ‘고시’) 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)’, ‘개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)’ 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있고, 제4조제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있으며, 제6조제1항은 “정보통신서비스 제공자등은 비밀번호는 복호화되지 아니하도록 일방향 암호화하여 저장한다.”라고 규정하고 있으며, 제6조제2항은 “주민등록번호, 신용카드번호, 계좌번호 등 정보에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.”라고 규정하고 있다.

다. 보호법 제39조의6제1항은 “정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다.”라고 규정하고 있다.

보호법 시행령 제48조의5제1항 “이용자가 정보통신서비스를 법 제39조의6제1항의 기간 동안 이용하지 않는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

가. 법령상 근거 없이 이용자의 주민등록번호를 수집·이용한 행위

{보호법 제24조의2(주민등록번호 처리의 제한)}

피심인은 '법령에서 구체적으로 주민등록번호의 수집·이용을 허용하는 경우'에 해당하지 않고, '정보주체등을 위하여 명백히 필요하다고 인정되는 경우'에도 해당하지 않으며, '주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우'라고 볼 수 없음에도 불구하고, 이용자의 주민등록번호를 처리한 행위는 보호법 제24조의2제1항을 위반한 것이다.

나. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 불법적인 접근 차단}

1) (침입차단 및 탐지시스템의 설치·운영) 피심인이 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하지 않고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제5항을 위반한 것이다.

2) (개인정보 유·노출 방지) 피심인이 처리중인 개인정보가 인터넷 홈페이지를 통해 권한이 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 SQL 삽입 공격을 예방하기 위한 시큐어 코딩 및 취약점 점검을 실시하는 등 보호조치를 취하지 않아 권한 없는 자에게 이용자의 개인정보가 공개되도록 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제9항을 위반한 것이다.

다. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

{보호법 제29조(안전조치의무) 중 암호화}

1) (비밀번호 암호화) 이용자 계정 건의 비밀번호를 암호화하지 않고 평문으로 저장한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제4호, 고시 제6조제1항을 위반한 것이다.

2) (주민등록번호암호화) 피심인이 주민등록번호를 건을 저장하면서 안전한 암호알고리즘으로 암호화하지 않고 저장한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제4호, 고시 제6조제2항을 위반한 것이다.

라. 장기 미이용자의 개인정보 파기 등 필요한 조치를 하지 않은 행위

{보호법 제39조의6(개인정보의 파기에 대한 특례)}

피심인이 1년 이상 접속하지 않은 장기 미이용자 건의 개인정보를 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 행위는 보호법 제39조의6, 같은 법 시행령 제48조의5를 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
주민등록번호 처리의 제한	보호법 §24의2①	-	• 법령상 근거 없이 이용자의 주민등록번호 처리한 행위
안전조치의무 위반 (접근통제, 암호화)	보호법 §29	§48의2① 제2호·제4호	• 개인정보처리시스템에 침입차단·탐지시스템을 설치·운영하지 않은 행위 (고시§4⑤) • 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨) • 비밀번호를 일방향 암호화하여 저장하지 아니한 행위 (고시§6①) • 주민등록번호 등을 안전한 암호알고리즘으로 암호화하여 저장하지 아니한 행위(§6②)
유효기간제	보호법 §39의6	§48의5	• 1년 이상 정보통신서비스를 이용하지 않은 회원의 개인정보를 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 행위

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 법령에서 허용하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용하지 아니하여야 한다.

나. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영하여야 한다.

2) 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

3) 처리중인 비밀번호는 복호화되지 아니하도록 일방향 암호화하여 저장하고, 처리중인 주민등록번호는 안전한 암호알고리즘을 이용하여 암호화하여 저장하여야 한다.

다. 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

라. 피심인은 가.부터 다.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 과징금 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15 제1항제5호, 같은 법 시행령 제48조의11제1항과 제4항, [별표 1의5] '과징금의 산정기준과 산정절차' 및 「개인정보보호 법규 위반에 대한 과징금 부과기준」(2020. 8. 5. 개인정보보호위원회 고시 제2020-6호, 이하 '과징금 부과기준'이라 한다)에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제39조의15, 같은 법 시행령 제48조의11에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의 · 중과실 여부

과징금 부과기준 제5조제1항은 '보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 시행령 제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단한다'라고 규정하고 있다.

이에 따라, 보호법 제29조(안전조치의무)를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

과징금 부과기준 제5조제3항은 '위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 매우 중대한 위반행위로 판단한다'라고 규정하고 있다.

다만, 과징금 부과기준 제5조제3항 단서에서 '위반행위의 결과가 ▲위반 정보통신서비스 제공자등이 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ▲이용자의 개인정보가 공중에 노출되지 않은 경우(제3호) 중 모두에 해당할 때에는 보통 위반행위로, 1개 이상 2개 이하에 해당하는 경우에는 중대한 위반행위로 감경한다.'라고 규정하고 있다.

이에 따라, 피심인이 위반행위로 인해 직접적인 이득을 취하지 않은 점을 고려하여 '중대한 위반행위'로 판단한다.

3) 기준금액 산출

피심인의 직전 3개 사업년도의 연평균 매출액 천원에 보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 21을 적용하여 기준금액을 천원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2018년	2019년	2020년	평 균
관련 매출액*				

* 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

<보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
보통 위반행위	1천분의 15

다. 필수적 가중 및 감경

과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 2년을 초과('10. 4. 24. ~ '20. 11. 24.)하는 '장기 위반행위'에 해당하므로 기준금액의 100분의 50에 해당하는 금액인 천원을 가산하고,

최근 3년 이내 보호법 제39조의15제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 천원을 감경한다.

라. 추가적 가중 및 감경

과징금 부과기준 제8조는 사업자의 위반행위의 주도 여부, 조사 협력 여부 등을 고려하여 필수적 가중 · 감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

이에 따라, 피심인이 ▲조사에 적극 협력한 점, ▲개인정보 유출사실을 자진 신고한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 천원을 감경한다.

마. 과징금의 결정

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15 제1항제5호, 같은 법 시행령 제48조의11, [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 1) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 천원을 최종 과징금으로 결정한다.

<과징금 산출내역>

기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금*
천원	필수적 가중 (50% : 천원) 필수적 감경 (50% : 천원)	추가적 가중 없음 추가적 감경 (20%, 천원)	**4,567천원**
	→ 천원	→ 천원	

3. 과태료 부과

피심인의 보호법 제24조의2, 제29조, 제39조의6 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항 제4호·제4호의2·제6호 및 같은 법 시행령 제63조의 〔별표2〕 '과태료 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 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 위반행위별 1회 위반에 해당하는 과태료 600만원을 각각 적용한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위:만원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
마. **법** 제21조제1항·**제39조의6**(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 **개인정보의 파기 등 필요한 조치를 하지 않은 경우**	법 제75조 제2항제4호	600	1,200	2,400
자. **법** 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 또는 **제29조**를 위반하여 **안전성 확보에 필요한 조치를 하지 않은 경우**	법 제75조 제2항제6호	600	1,200	2,400
차. **법 제24조의2제1항**을 위반하여 **주민등록번호를 처리한 경우**	법 제75조 제2항제4호의2	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(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중기준)에 따라 제29조(안전조치 의무) 위반행위에 대해 ▲제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상이며, ▲위반 기간이 3개월 이상인 경우로 기준금액의 20%를 가중하고, 제39조의6(개인정보의 파기에 대한 특례) 및 제24조의2(주민등록번호 처리의 제한) 위반행위에 대해서는 ▲위반 기간이 3개월 이상인 경우로 위반행위별 기준금액의 10%를 각각 가중한다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다'라고 규정하고 있다.

피심인의 경우 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점, 사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 완료하지는 못하였으나 시정 중에 있는 것으로 인정되는 점, 중기업에 해당하는 점 등을 고려하여 과태료 부과지침 제7조에 따라 기준금액의 30%를 각각 감경한다.

다. 최종 과태료

피심인의 보호법 제24조의2, 제29조, 제39조의6를 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,500만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
주민등록번호 보유 (이용자의 주민등록번호 보유)	600만원	60만원	180만원	**480만원**
안전조치의무 (접근통제, 암호화)	600만원	120만원	180만원	**540만원**
개인정보 파기 위반 (유효기간제 위반)	600만원	60만원	180만원	**480만원**
계				**1,500만원**

4. 결과 공표

「개인정보 보호법」 제66조제1항 및 「개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 1천명 이상의 정보주체의 주민등록번호를 유출한 행위로 시정조치 명령 처분을 받은 경우(제2호), 법 제75조제2항 각호에 해당하는 위반행위를 2개 이상 한 경우(제4호), 6개월 이상 지속된 경우(제5호)에 해당하므로, 피심인이 시정조치 명령을 받은 사실과 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표					
개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1		법 제24의2	주민등록번호 보유	2021.10.27.	시정조치 명령 과태료 부과 480만원
		법 제29조	안전조치의무 위반 (접근통제, 암호화)	2021.10.27.	시정조치 명령 과태료 부과 540만원
		법 제39의6	개인정보 파기 위반	2021.10.27.	시정조치 명령 과태료 부과 480만원

Ⅴ. 결론

피심인의 보호법 제24조의2, 제29조, 제39조의6 위반행위에 대하여 같은 법 제39조의15(과징금의 부과 등에 대한 특례)제1항제5호, 제75조(과태료)제2항 제4호·제4의2호·제6호, 제64조(시정조치 등)제1항, 제66조(결과의 공표)제1항에 따라 과징금, 과태료, 시정조치 명령, 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 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 10월 27일

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 흥 열　(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 - 017 - 271호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2021. 10. 27.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.

2) 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 9,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

피심인은 판매사이트( )를 운영하는 「(구)정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2020. 8. 5. 법률 제16955호로 개정·시행되기 전의 것, 이하 '정보통신망법'이라 한다)에 따른 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회[3]는 개인정보보호포털(privacy.go.kr)에 유출 신고('20. 5. 14.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('21. 1. 28. ~ '21. 8. 11.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 품 판매사이트를 운영하면서 '21. 3. 4. 기준 건의 이용자 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
회원정보	(필수) 이름, 전화번호, 이메일(ID), 비밀번호 (선택) 생년월일, 배송지 주소	'18. 1. 3. ~ '21. 3. 4.	

나. 개인정보 훼손 경위

1) 훼손 경과 및 대응

일 시		피심인의 유출인지 및 대응 내용
'20. 5. 14.	09:27	서비스 모니터링 중 어플 접속불가 사실 확인
	09:33	DB 회원테이블 삭제 및 신원 미상자의 금품요구 메시지 확인
	-	백업 DB를 통해 회원 테이블 복구

3) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라, 개인정보보호위원회가 방송통신위원회의 소관사무 중 개인정보 보호에 해당하는 사무를 승계(제1항), 법 시행 전 방송통신위원회가 행한 고시·행정처분 중 그 소관이 방송통신위원회에서 개인정보보호위원회에게로 이관되는 사항에 관한 행위는 개인정보보호위원회가 행한 것으로 간주(제4항)

	13:36	개인정보보호 포털을 통한 개인정보 유출신고
	15:37	트위터 및 페이스북 게시를 통한 유출통지

2) 훼손규모 및 경위

(훼손항목 및 규모) 이름, 전화번호, 이메일, 비밀번호, 생년월일, 주소 등 이용자의 개인정보 총 건

(훼손 경위) 신원 미상의 자가 알 수 없는 방법으로 DB에 접속하여 회원정보 테이블을 삭제하고 금품요구 메시지를 남김

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보가 열람권한이 없는 자에게 공개되지 않도록 하는 접근 통제를 소홀히 한 행위

피심인은 개인정보처리시스템의 관리자페이지에 외부에서 접속 시 안전한 인증수단을 적용하지 않고 아이디·비밀번호만으로 접속할 수 있도록 운영하였으며, 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하거나 침입탐지·차단 시스템 등의 보안장비를 운영하지 않아 건의 이용자 개인정보가 훼손되도록 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’21. 8. 20. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 9. 6. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제28조제1항은 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령이 정하는 기준에 따라 '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영(제2호)' 및 '그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치(제6호)'를 하여야 한다고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영' 및 '그 밖에 개인정보에 대한 접근 통제를 위하여 필요한 조치'를 하여야 한다고 규정하고 있다.

개인정보의 기술적·관리적 보호조치 기준(방송통신위원회고시, 2020.1.2., 이하 '고시'라 한다) 제4조는 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.(제4항)", "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제5항제1호)', '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제5항제2호)' 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{정보통신망법 제28조(개인정보의 보호조치)}

피심인이 이용자의 개인정보가 열람 권한이 없는 자에게 공개되도록 한 행위는 정보통신망법 제28조제1항, 같은 법 시행령 제15조제2항, 고시 제4조제4항 및 제5항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보 보호조치 위반(접근통제)	§28①	§15②	- 외부에서 개인정보처리시스템에 접속 시 안전한 인증 수단을 적용하지 않은 행위(고시§4④) - 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하지 않은 행위(고시§4⑤)

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.

2) 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 과태료 부과

피심인의 정보통신망법 제28조제1항 위반행위에 대한 과태료는 같은 법 제76조(과태료)제1항제3호, 같은 법 시행령 제74조의 〔별표9〕 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(2018. 7. 4. 방송통신위원회 의결, 이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 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 1,000만원을 적용한다.

< 「정보통신망법」 시행령 [별표9] 2. 개별기준 >

(단위:만원)

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 사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲조사방해, ▲위반의 정도, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을

고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중기준)에 해당하지 않아 가중없이 기준금액을 유지한다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

피심인의 경우 시정조치(안) 사전통지 및 의견제출 기간 내에 법규 위반행위에 대하여 시정 완료한 점 등을 고려하여 기준금액의 10%인 100만원을 감경한다.

다. 최종 과태료

피심인의 정보통신망법 제28조제1항을 위반한 행위에 대해 기준금액에 가중·감경을 거쳐 총 900만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보 보호조치 위반 (접근통제)	1,000만원	0	100만원	**900만원**

Ⅴ. 결론

피심인의 정보통신망법 제28조(개인정보의 보호조치) 위반행위에 대하여 같은 법 제76조(과태료)제1항제3호,「개인정보 보호법」제64조(시정조치 등)제1항에 따라 과태료, 시정조치 명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 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 10월 27일

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 흥 열　(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 - 017 - 272호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2021. 10. 27.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 5,400,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

피심인은 서비스를 제공하는 「개인정보 보호법」(이하 '보호법'이라 한다.)에 따른 개인정보처리자 및 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보보호포털(privacy.go.kr)에 유출 신고('20. 11. 13.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('20. 12. 7. ~ '21. 8. 11.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 서비스를 제공하면서 이용자 약 만건의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
가입 정보	이메일, 비밀번호, 이름, 생년월일, 성별	'13. 6월 ~ '20. 12. 19.	약 만건
경품 수령	이메일(아이디), 이름, 추가 이메일, 연락처 및 주소 (실물 경품 배송 시에만)	'19. 8월 ~ '20. 12. 19.	
유료 재화 환전 신청 시	은행명, 예금주, 계좌번호, 신분증 사본 (14세 미만의 경우 법정대리인 신분증 사본)	'19. 8월 ~ '20. 12. 19.	
이벤트 /오디션 응모	이메일(아이디), 휴대전화번호, 주소(이름, 연락처)	'13. 6월 ~ '20. 12. 19.	

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지·대응 내용
'20. 11. 12.	18:00	내부 모니터링시스템에 남겨진 금품요구 메시지를 통해 유출 사실 인지
		내부 모니터링시스템 서버에 대한 외부 접근을 차단
'20. 11. 13.	12:07	개인정보보호 포털을 통한 개인정보 유출신고
	16:30	이메일을 통한 이용자 유출통지, 홈페이지 팝업 및 공지사항 게시

2) 유출규모 및 경위

(유출항목 및 규모) 이름, 이메일, 생년월일 등 '20. 11. 5. 12:00 ~ '20. 11. 10. 11:53 동안 어플에 접속한 이용자의 개인정보 총 건

(유출 경위) 앱 트래픽 관리 및 효율적인 고객응대 등을 위해 내부 모니터링 시스템을 구축하였으나, 방화벽 설정 등 시스템 접속 관련 접근통제를 실시하지 않아 신원 미상의 자가 접속하여 이용자의 개인정보를 유출

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보가 열람권한이 없는 자에게 공개되지 않도록 하는 접근통제를 소홀히 한 행위

피심인은 개인정보가 처리되는 내부 모니터링시스템에 대한 접근권한을 개인정보취급자에게 허용된 IP로 제한하지 않고, 외부 인터넷 어디에서나 접속 가능하도록 운영하여 건의 개인정보가 공개되도록 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '21. 8. 20. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 9. 2. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 및 물리적 조치를 하여야 한다"라고 규정하고 있다.

보호법 시행령 제48조의2제1항은 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영’ 및 ‘그 밖에 개인정보에 대한 접근 통제를 위하여 필요한 조치’를 하여야 한다.”라고 규정하고 있다.

개인정보의 기술적·관리적 보호조치 기준(개인정보보호위원회고시, 2020. 8. 11., 이하 ‘고시’라 한다.) 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)’, ‘개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)’ 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

{보호법 제29조(안전조치의무)}

피심인이 회원가입 신청자의 개인정보가 열람 권한이 없는 자에게 공개되도록 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2, 고시 제4조제5항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 (접근통제)	§29	§48조의2	- 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하지 않은 행위 (고시§4⑤)

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보를 처리할 때는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 과태료 부과

피심인의 보호법 제29조 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항 제6호, 같은 법 시행령 제63조의 〔별표2〕 '과태료 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 시행령 제63조의 [별표2]는 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.

< 「보호법」 시행령 [별표2] 2. 개별기준 >

(단위:만원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 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(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정하고 있다.

피심인의 경우 과태료 부과지침 제8조(과태료 가중기준)에 해당하지 않아 가중없이 기준금액을 유지한다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.'라고 규정하고 있다.

피심인의 경우 과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 점등을 고려하여 기준금액의 10%인 60만원을 감경한다.

다. 최종 과태료

피심인의 보호법 제29조를 위반한 행위에 대해 기준금액에 가중·감경을 거쳐 총 540만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만원	-	60만원	**540만원**

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반행위에 대하여 같은 법 제75조(과태료) 제2항제6호, 보호법 제64조(시정조치 등)제1항에 따라 과태료, 시정조치 명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 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 10월 27일

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 흥 열　(서 명)

위　　원　　지 성 우　(서 명)