

개 인 정 보 보 호 위 원 회

심의 · 의결

안 건 번 호 제2021 - 018 - 274호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :

대표자

의결연월일 2021. 11. 10.

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) 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.

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 : 8,400,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

I. 기초 사실

피심인은

하는 「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 로그인 과정에서 일부 회원의 개인정보가 타 이용자의 계정에 노출되어 유출 신고('20.12.18. / '21.1.4.)에 따라 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사(2021. 2. 23. ~ 2021. 6. 15.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 서비스를 제공하면서 2021. 4. 27. 기준으로 이용자 8,475,672명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	(필수) 이메일주소, 아이디, 비밀번호, 이름, 생년월일, 성별, 휴대전화번호, CI/DI (선택) 주소, 계좌, 사이즈	'04. 12. 28. ~ '21. 4. 27.	8,475,672

피심인은 서비스를 제공하면서 2021. 4. 27. 기준으로 이용자 358,190명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	(필수) 이메일주소, 이름, 생년월일, 성별, 휴대전화번호, CI/DI (선택) 주소, 계좌, 카드정보, 신발사이즈 및 결제 비밀번호	'20. 5. 20. ~ '21. 4. 27.	358,190

나. 개인정보 유출 경위

< 개인정보 유출 사건('20.12월) >

1) 유출 경과 및 대응

일시	피심인의 유출인지·대응 내용
2020. 12. 18.	13:30 타인의 개인정보가 조회된다는 이용자 문의 접수
	15:30 개인정보담당자의 개인정보 유출 사실 인지
	16:00 오류 조치 완료 및 DB 수정, 중복계정 정리, 마이페이지 마스킹 적용
	19:02 유출 대상자 23명에게 전화, 문자로 유출 사실 통지
	19:57 개인정보보호 포털을 통한 개인정보 유출 신고

2) 유출규모 및 경위

(유출항목 및 규모) 서비스에 통합계정 연동*기능을 제공하면서, 오류로 타인에게 유출된 이용자의 개인정보(이름, 이메일주소, 전화번호) 23건

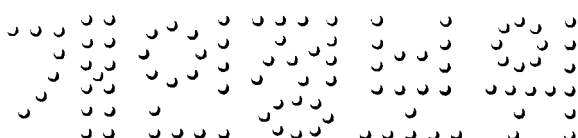
* 서비스에 등록된 계정으로 앱을 이용할 수 있는 방식

(유출 경위) 서비스에 계정으로 연동하여 접속할 경우, 각 이용자에게 부여되는 연동값에 대한 중복방지 기능이 누락*되어 23명의 회원 정보가 다른 23명에게 각각 저장됨

- '20. 9. 14. 서비스에 통합계정 연동 기능 도입

- '20. 12. 14. ~ 12. 15 홍보 이벤트 실시로 서비스에 접속자가 평소 대비 최대 30배 이상 폭증

* 정상적으로 계정 연동된 이용자A와 같은 시점에 이용자B가 계정 연동을 시도하는 경우
- 이용자B는 동일한 난수 사용으로 계정연동이 거절되나, 이용자A의 계정정보에 이용자B의 계정정보가 업데이트되어 조회됨



< 개인정보 유출 사건('21.1월) >

1) 유출 경과 및 대응

일시		피심인의 유출인지·대응 내용
2021. 1. 4.	17:23	이용자 제보 접수
	18:38	개인정보담당자의 개인정보 유출 사실 인지
	19:48	오류 조치 완료
	20:48	이용자 1명에게 문자, 전화로 개인정보 유출 통지
	22:06	개인정보보호 포털을 통한 개인정보 유출 신고

2) 유출규모 및 경위

(유출항목 및 규모) 서비스에 ‘로그인’ 기능을 이용한 1명의
개인정보(이름, 이메일주소, 전화번호, 주소)가 9명에게 노출됨

(유출 경위) 서비스에 ‘로그인’하는 기능을 적용하면서 연동값*에 오류가 있는 경우에 대한 예외 처리가 프로그램에 적용되지 않아, 타인의 개인정보가 노출됨

* 연동값이 잘못되었거나, 만료되어 유효하지 않은 경우, '401에러'가 발생하며, 연동 결과 값에 Empty가 저장됨

3. 개인정보의 취급·운영 관련 사실관계

< 개인정보 유출 사건('20.12월) >

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

피심인은 서비스에 계정으로 연동하여 접속할 경우, 각 이용자에게 부여되는 연동값에 대한 중복방지 기능이 누락되어 기존 이용자의 회원정보가 타 이용자의 개인정보로 업데이트되어 이용자의 개인정보가 공개되도록 한 사실이 있다.

< 개인정보 유출 사건('21.1월) >

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

피심인은 서비스에 ‘ 로그인’하는 기능을 적용하면서 연동값에 오류가 있는 경우 대한 예외 처리가 적용되지 않아, 이용자의 개인정보가 공개되도록 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 8. 18. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 9. 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 제48조의2제1항 제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘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’) 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 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.

2. 위법성 판단

< 개인정보 유출 사건(“20.12월) >

가. 개인정보가 열람권한이 없는 자에게 공개되지 않도록 하는 접근통제를 소홀히 한 행위 {보호법 제29조(안전조치의무)}

피심인은 개인정보 안전성 확보 등을 위하여 처리 중인 개인정보가 열람 권한이 없는 자에게 공개되지 않도록 조치를 하여야 하나, 계정 연동

1) 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.

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 부과 지침'이라 한다)에 따라 다음과 같이 부과한다.

< 개인정보 유출 사건('20.12월) >

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 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 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 사소한 부주의나 시스템의 오류로 인한 것으로 인정되는 점, 과태료의 사전통지 및 의견제출 기간 내에 법규 위반행위에 대하여 시정 완료한 점, 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점을 고려하여 기준금액의 30%인 180만원을 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

< 개인정보 유출 사건('21.1월) >

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 사소한 부주의나 시스템의 오류로 인한 것으로 인정되는 점, 과태료의 사전통지 및 의견제출 기간 내에 법규 위반행위에 대하여 시정 완료한 점, 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점을 고려하여 기준금액의 30%인 180만원을 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

V. 결론

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

이의제기 방법 및 기간

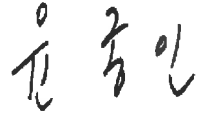
피심인은 이 시정명령 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

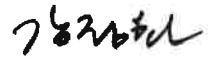
피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.

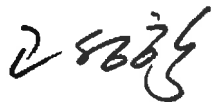
과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 규정에 따라 그 효력을 상실하고 관할법원(당사자 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료 납입 의무를 부담한다.

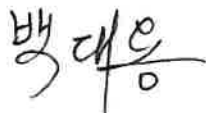
이상과 같은 이유로 주문과 같이 의결한다.

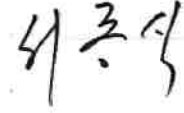
2021년 11월 10일

위원장 윤종인 


위원 강정화 

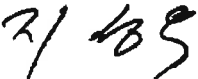
위원 고성학 

위원 백대용 

위원 서종식 

위원 염홍열 

위원 이희정 

위원 지성우 



개 인 정 보 보 호 위 원 회

심의 · 의결

안 건 번 호 제2021 - 018 - 275호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2021. 11. 10.

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) 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.

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

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 7,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

I. 기초 사실

피심인은 서비스 웹사이트를 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

개인정보보호위원회¹⁾는 개인정보종합포털(privacy.go.kr)에 유출 신고('20. 1. 30.)한 피심인에 대하여 개인정보 취급·운영 실태 및 정보통신망법 위반 여부를 조사('20. 2. 21. ~ '21. 2. 1.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 2020. 2. 19. 기준으로 이용자 3,724,689명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	(필수) 이메일(ID), 패스워드, 닉네임, 이름 (선택) 휴대전화번호, 성별	'19. 6. 11. ~ '20. 2. 19.	3,724,689건

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지·대응 내용
'20. 1. 28.	17:36	서버 성능 개선 시 소스코드에 회원구분 Key값을 잘못 입력
	21:15	서버 성능 개선 작업 후, 모니터링 과정 중 서버 저장 오류 발생 확인
	21:47	서버 저장 오류 개선을 위한 수정 소스코드 배포

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)

'20. 1. 29.	13:00	장애 원인 분석 과정에 개인정보 유출 가능성 인지
'20. 1. 30.	12:40	개인정보보호 포털을 통한 개인정보 유출신고
	13:00	이용자 대상 유출사실 통지

2) 유출규모 및 경위

(유출항목 및 규모) 성별, 이름, 회원번호 등 개인정보 137건

(유출 경위) 피심인은 운영 중인 어플의 서버 성능 개선과정에서 이용자를 구분할 때 사용하는 key값을 잘못 입력

3. 개인정보의 취급·운영 관련 사실관계

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

피심인은 운영 중인 어플의 서버 성능 개선과정에서 소스코드에 이용자 구분 key값을 잘못 입력하여, 이용자 로그인 시 타인 계정으로 로그인되어 이용자의 개인정보가 공개되도록 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 3. 3. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 4. 7. 개인정보보호 위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 한다.”고 규정하고 있다.

같은 법 시행령 제15조제2항은 “정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보처리시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)’, ‘개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)’, ‘개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단(제3호)’, ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)’ 등을 하여야 한다.”고 규정하고 있다.

정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2019-13호, 이하 ‘고시’) 제4조제9항은 “처리 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”고 규정하고 있다.

‘고시 해설서’는 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, (i) 인터넷 홈페이지 설계시

에는 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 필요한 보안 대책을 마련하고, (ii) 인터넷 홈페이지 개발시에는 개인정보 유·노출 방지를 위한 보안기술을 적용하고, (iii) 인터넷 홈페이지 운영·관리시에는 개인정보 유·노출 방지를 위한 보안대책 및 기술적용에 따른 적정성을 검증하고 개선조치를 하여야 한다고 해설하고 있으며, 또한 P2P 및 공유설정 등을 통한 개인정보 유·노출을 방지하기 위해 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 보호조치를 하여야 한다.”고 해설하고 있다.

2. 위법성 판단

가. 개인정보가 열람권한이 없는 자에게 공개되지 않도록 하는 접근통제를 소홀히 한 행위{정보통신망법 제28조(개인정보의 보호조치)제1항}

피심인은 개인정보 안전성 확보 등을 위하여 처리 중인 개인정보가 열람 권한이 없는 자에게 공개되지 않도록 조치를 하여야 하나, 프로그래밍 과정에서 이용자 key값을 잘못 입력하여 권한 없는 자에게 이용자의 개인정보가 공개되도록 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항, 고시 제4조 제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
보호조치 위반 (접근통제)	§28①	§15②	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) 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.

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 제74조(과태료의 부과기준)의 [별표9] ‘과태료 부과기준’ 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(2018. 7. 5. 방송통신위원회 의결, 이하 ‘과태료 부과지침’이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 제74조의 [별표9] 과태료 부과기준은 최근 3년간 같은 위반행위로 과태료 부과처분을 받은 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 과태료인 1,000만원을 적용한다.

< 정보통신망법 시행령 [별표2] 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 동 지침 [별표2]의 가중기준에 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 동 지침 [별표1]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

피심인의 경우 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점, 일관되게 행위 사실을 인정하면서 조사에 적극 협력한 점, 이용자에게 피해가 발생하지 않은 등 위반행위의 결과가 경미하고 개인정보처리자의 사소한 부주의로 인한 것으로 인정되는 점을 고려하여 기준금액의 30%인 300만원을 감경한다.

다. 최종 과태료

피심인의 정보통신망법 제28조제1항을 위반한 행위에 대해 기준금액에 가중·감경을 거쳐 총 700만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보 보호조치 의무 위반 (접근통제)	1,000만원	-	300만원	700만원

V. 결론

피심인의 정보통신망법 제28조제1항 위반행위에 대하여 정보통신망법 제76조(과태료)제1항제3호, 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.

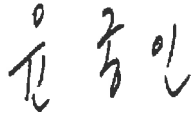
피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.


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.

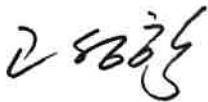



이상과 같은 이유로 주문과 같이 의결한다.

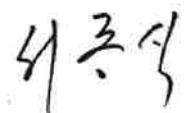
2021년 11월 10일

위원장 윤종인 


위원 강정화 

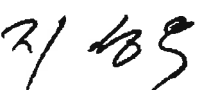
위원 고성학 

위원 백대용 

위원 서종식 

위원 염홍열 

위원 이희정 

위원 지성우 



개 인 정 보 보 호 위 원 회

심의회 의결

안 건 번 호 제2021 - 018 - 276호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2021. 11. 10.

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) 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.

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 : 7,000,000원
- 나. 납부기한 : 고지서에 명시된 납부기한 이내
- 다. 납부장소 : 한국은행 국고수납 대리점

이 유

I. 기초 사실

피심인은 쇼핑몰을 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)	주소	종업원 수 (명)



II. 사실조사 결과

1. 조사 배경

개인정보보호위원회¹⁾는 개인정보종합포털(privacy.go.kr)에 유출 신고('20. 7. 7.)한 피심인에 대하여 개인정보 취급·운영 실태 및 정보통신망법 위반 여부를 조사('21. 1. 28. ~ '21. 3. 24.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 2021. 3. 24. 기준으로 이용자 142,065명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	(필수) 아이디, 이름, 생년월일, 핸드폰번호, 우편번호, 주소, 이메일 (선택) 전화번호, 메일/SMS 수신여부	'18. 1. 1. ~ '21. 3. 24.	142,065건

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지·대응 내용
'20. 5. 22.	-	쇼핑몰 상품 주문페이지 내 '기존 배송지 선택' 기능 적용
'20. 7. 7.	11:00	언론사의 홍보실 문의로 일부 비회원 주문고객의 개인정보가 유출되었음을 인지 후 즉시 소스코드 수정
	17:45	개인정보보호 포털을 통한 개인정보 유출신고
'20. 7. 8.	-	이용자 대상 유출사실 문자 통지 및 유선전화 완료

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) 유출규모 및 경위

(유출항목 및 규모) 이름, 주소, 휴대전화번호 등 '20. 6. 23. ~ '20. 7. 4. 기간 비회원으로 상품 주문한 10명의 개인정보

(유출 경위) 피심인은 회원 상품 주문페이지에 '기존 배송지 선택' 기능을 개발·적용하는 과정에서, 비회원의 상품 주문페이지에도 해당 버튼이 표시 되도록 적용

- 비회원으로 주문 시 '기존 배송지 선택' 버튼을 선택하면 최근 비회원으로 구매한 다른 주문자의 개인정보가 유출됨

3. 개인정보의 취급·운영 관련 사실관계

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

피심인은 회원 상품 주문페이지에 '기존 배송지 선택' 기능을 개발·적용하는 과정에서 테스트 절차를 거쳤음에도 비회원에게도 해당 기능이 적용되도록 하여, 최근 비회원으로 주문한 10명의 개인정보가 공개되도록 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 5. 18. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 6. 3. 개인정보보호 위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 한다.”고 규정하고 있다.

같은 법 시행령 제15조제2항은 “정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보처리시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)’, ‘개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)’, ‘개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단(제3호)’, ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)’ 등을 하여야 한다.”고 규정하고 있다.

정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2019-13호, 이하 ‘고시’) 제4조제9항은 “처리 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”고 규정하고 있다.

‘고시 해설서’는 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, (i) 인터넷 홈페이지 설계시

에는 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 필요한 보안 대책을 마련하고, (ii) 인터넷 홈페이지 개발시에는 개인정보 유·노출 방지를 위한 보안기술을 적용하고, (iii) 인터넷 홈페이지 운영·관리시에는 개인정보 유·노출 방지를 위한 보안대책 및 기술적용에 따른 적정성을 검증하고 개선조치를 하여야 한다고 해설하고 있으며, 또한 P2P 및 공유설정 등을 통한 개인정보 유·노출을 방지하기 위해 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 보호조치를 하여야 한다.”고 해설하고 있다.

2. 위법성 판단

가. 개인정보가 열람권한이 없는 자에게 공개되지 않도록 하는 접근통제를 소홀히 한 행위[정보통신망법 제28조(개인정보의 보호조치)제1항]

피심인은 개인정보 안전성 확보 등을 위하여 처리 중인 개인정보가 열람 권한이 없는 자에게 공개되지 않도록 조치를 하여야 하나, 홈페이지 개발 과정에서 적용 범위를 잘못 설정하여 권한 없는 자에게 이용자의 개인정보가 공개되도록 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항, 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
보호조치 위반 (접근통제)	§28①	§15②	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) 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.

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 제74조(과태료의 부과기준)의 [별표9] '과태료 부과기준' 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(2018. 7. 5. 방송통신위원회 의결, 이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 제74조의 [별표9] 과태료 부과기준은 최근 3년간 같은 위반행위로 과태료 부과처분을 받은 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 과태료인 1,000만원을 적용한다.

< 정보통신망법 시행령 [별표2] 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 동 지침 [별표2]의 가중기준에 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 동 지침 [별표1]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

피심인의 경우 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점, 일관되게 행위 사실을 인정하면서 조사에 적극 협력한 점, 이용자에게 피해가 발생하지 않은 등 위반행위의 결과가 경미하고 개인정보처리자의 사소한 부주의로 인한 것으로 인정되는 점을 고려하여 기준금액의 30%인 300만원을 감경한다.

다. 최종 과태료

피심인의 정보통신망법 제28조제1항을 위반한 행위에 대해 기준금액에 가중·감경을 거쳐 총 700만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보 보호조치 의무 위반 (접근통제)	1,000만원	-	300만원	700만원

V. 결론

피심인의 정보통신망법 제28조제1항 위반행위에 대하여 정보통신망법 제76조(과태료)제1항제3호, 보호법 제64조(시정조치 등)제1항에 따라 과태료, 시정조치 명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

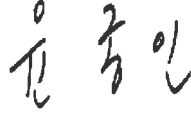
피심인은 이 시정명령 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.


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.


이상과 같은 이유로 주문과 같이 의결한다.

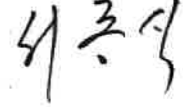
2021년 11월 10일

위원장 윤종인 


위원 강정화 


위원 고성학 

위원 백대용 

위원 서종식 

위원 염홍열 

위원 이희정 

위원 지성우 



개 인 정 보 보 호 위 원 회

심의 · 의결

안 건 번 호 제2021 - 018 - 277호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2021. 11. 10.

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) 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.

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

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

- 가. 과 태 료 : 3,600,000원
- 나. 납부기한 : 고지서에 명시된 납부기한 이내
- 다. 납부장소 : 한국은행 국고수납 대리점

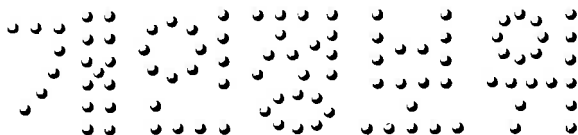
이 유

I. 기초 사실

(이하 ‘피심인’이라 한다)는 를 개발 하여 웹 과 앱에서 제공하는 「개인정보 보호법」(이하 ‘보호법’이라 한다)에 따른 개인정보처리자이자 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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



II. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인의 2021. 1. 17. 개인정보 유출 신고와 관련하여 개인정보 취급·운영 실태 및 개인정보보호 법규 위반 여부를 조사하였으며, 다음과 같은 사실을 확인하였다.

2. 개인정보의 취급·운영 관련 사실관계

가. 개인정보 수집 현황

피심인은 프로그램을 를 운영하면서 2021. 7. 22. 기준 1,341,326건의 이용자 정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	(필수) 이름, 생년월일, 성별, 휴대전화번호, 비밀번호, 사업자등록번호	'17. 1. 4. ~ '21. 7. 13.	1,341,326건

나. 개인정보 유출 규모 및 경로

1) 개인정보 유출규모

피심인은 주요 고객인 소상공인을 위한 일시적 부가서비스로 2021. 1. 16.부터 2021. 4. 21.까지 사업자등록증명, 부가세과세표준증명 서류를 이용자의 이메일로 발송해주는 서비스를 제공하였다. 이

과정에서 서비스를 신청한 이용자 86명의 이름, 생년월일 등이 포함된 사업자등록증명원과 부가세과세증명원이 다른 이용자 94명의 이메일 주소로 아래와 같이 발송되었다.

< 개인정보 수집 현황 >

유출 자료	정보주체 수	오발송 메일 수신자 수
사업자등록증명원	51명	58명
부가세과세증명원	30명	30명
사업자등록증명원 및 부가세과세증명원	5명	6명
합계	86명	94명

2) 개인정보 유출경로

피심인은 2021. 1. 16. 18시경 서비스'의 이용자 수 증가에 대비하여 프로세스 수를 10개로 확장하는 과정에서 시스템 설계 오류로 86명의 개인정보가 포함된 사업자등록증명원과 부가세과세증명원 PDF 문서를 다른 이용자의 이메일 주소로 발송되도록 하여 개인정보를 유출하였다.

3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

가. 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 조치를 취하지 않은 행위

피심인은 이용자가 이메일 주소를 입력하고 사업자등록증명원과 부가세과세증명원 발급을 신청하는 경우, 발급 신청인의 인증정보를 이용하여 홈택스 사이트에 접속, 사업자등록증명원과 부가세과세증명원을 조회한 후 이를 PDF 문서로 저장하여 신청인의 이메일 주소로 전송하도록 시스템을 설계하고, 2021. 1. 16. 14시경 서비스'를 개시하였다.



피심인은 서비스' 개시 4시간여가 지난 18시 15분경, 해당 서비스의 이용자 증가에 대비하여 서류 발급 프로그램의 PDF 문서 조회·저장(스크래핑) 프로세스 수를 1개에서 최대 10개로 변경하여 동시에 10개 신청을 병렬 처리할 수 있도록 서비스를 확장하였다.

피심인의 시스템 변경 조치 후, 병렬처리 프로세스 간 발급 신청인이 구분되지 않고 PDF 문서 조회·저장(스크래핑) 작업 종료 순서에 따라 파일이 저장되면서 특정 발급 신청인의 디렉토리에 다른 발급 신청인 명의의 PDF 문서 파일이 저장되어 이메일로 발송되는 현상이 발생하였다.

피심인은 위 시스템 변경 도입 과정에서 테스트를 실시하거나 발급 신청인과 저장된 PDF 문서의 명의자 일치 여부를 확인하는 설계를 구현하지 않았으며, 시스템 변경 1시간 후인 2021. 1. 16. 19시 11분경 내부 직원을 통해 이메일 오 발송 사실을 인지하고 서비스를 일시 중지하였다.

피심인은 1. 18. 1시 40분경 최초 서비스 개시 시점과 같이 병렬처리 프로세스를 단일 처리 프로세스로 변경하고, 메일을 발송할 때 수신자의 사업자번호와 PDF 문서 명의자 사업자번호의 동일성을 확인하는 검증 절차를 추가하였다.

나. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 9. 17. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 10. 5. 개인정보보호 위원회에 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 차단 하기 위하여 ‘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’) 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 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.



2. 위법성 판단

가. 개인정보 해당성

사업자의 성명과 생년월일은 살아 있는 개인에 관한 정보로서 사업자등록증명원과 부가세과세증명원 서류에 포함된 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보로서 개인정보에 해당한다.

나. 개인정보가 유·노출 방지 의무 위반

보호법 제29조 및 같은 법 시행령 48조의2, 고시 제4조제9항에 따라 정보통신 서비스 제공자등은 처리 중인 개인정보가 홈페이지, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부 유출되지 않도록 개인정보처리시스템에 조치를 취하는 등 사회통념상 합리적으로 기대 가능한 수준의 기술적 보호조치를 하여야 한다.

피심인은 소프트웨어 개발·공급을 업으로 하는 자이면서도, 시스템 설계 변경 시 적정성 검증을 위한 테스트를 실시하지 않고, PDF 문서 저장 및 발송 과정에서 발급 신청인과 PDF 문서 명의자의 일치 여부를 확인하는 설계를 구현하지 않은 채 변경된 시스템을 곧바로 실제 서비스에 적용함으로써 86명의 이용자 이름과 생년월일이 포함된 PDF 문서가 이용자에게 발송되어 유출되도록 하였는바, 이는 사회통념상 합리적으로 기대 가능한 수준의 조치를 다하지 않은 것으로서 보호법 제29조 및 같은 법 시행령 48조의2, 고시 제4조 제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제)	§29	§48조의2	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) 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.

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(안전조치의무) 위반에 대한 과태료는 같은 법 제75조(과태료) 제2항제6호, 같은 법 시행령 제63조(과태료의 부과기준)의 [별표2] '과태료의 부과 기준' 및 '개인정보 보호법 위반에 대한 과태료 부과기준'(2021. 1. 27. 개인정보보호 위원회 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, 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 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 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 위반정도가 경미한 점, 조사에 적극적으로 협력한 점, 위반행위를 자진 시정한 점, 「중소기업기본법」 제2조에 따른 소기업인 점을 고려하여, 기준 금액의 40%인 240만원을 감경한다.



다. 최종 과태료

피심인의 보호법 제29를 위반한 행위에 대해 기준금액 600만원에서 40% 감경을 거쳐 360만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만원	-	240만원	360만원
계				360만원

V. 결론

피심인의 보호법 제29조 위반행위에 대하여 같은 법 제75조(과태료)제2항제6호, 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.

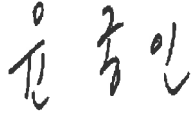
피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.


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.




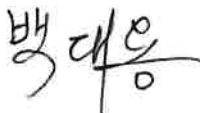
이상과 같은 이유로 주문과 같이 의결한다.

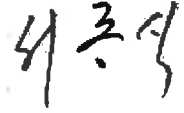
2021년 11월 10일


위원장 윤종인 


위원 강정화 

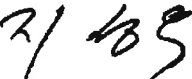
위원 고성학 

위원 백대용 

위원 서종식 

위원 염홍열 

위원 이희정 

위원 지성우 



심의 · 의결

피 심 인 (사업자등록번호 :)

다. 납부장소 : 한국은행 국고수납 대리점

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

II. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 이용자의 개인정보가 타인에게 유출되어 유출 신고 ('21.6.15.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사 (2021. 7. 6. ~ 2021. 8. 27.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 운영하면서 2021. 7. 7. 기준으로 이용자 348,269명의 개인정보를 수집하여 보관하고 있다.

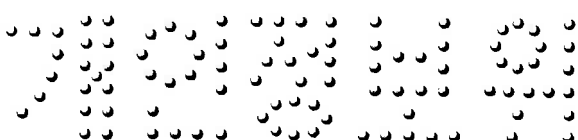
< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	(필수) 로그인ID, 비밀번호, 이름, 성별, 생년월일, 휴대전화 번호, 이메일, 주소 (선택) 관심주택형, 설문내용	'00. 3. 29. ~ '21. 7. 7.	348,269

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시	피심인의 유출원인·대응 내용
'21. 6. 15.	18:43 이용자 제보(전화)로 유출 사실 인지
	18:58 원인 파악 및 수정(기존 설정으로 복원) 완료
'21. 6. 16.	10:35 개인정보보호 포털을 통한 개인정보 유출 신고
	18:23 유출 대상자 19명에게 이메일, 전화, SMS로 유출 사실 통지



2) 유출규모 및 경위

(유출항목 및 규모) 캐시서버 설정을 잘못하여 자동 로그인된 이용자의 개인 정보(이름·생년월일·주소) 19건*

* 이름+생년월일+주소(3명), 이름+주소(2명), 이름+생년월일(14명)

(유출 경위) 홈페이지 응답속도 개선을 위해 캐시서버를 도입하며 이용자의 계정정보도 캐시서버에 저장하도록 설정하여, 타 이용자의 계정으로 자동 로그인됨

- '21. 6. 15. 18:30 홈페이지 응답속도 개선을 위해 캐시 설정 적용

3. 개인정보의 취급·운영 관련 사실관계

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

피심인은 캐시서버 도입 과정에서 캐시서버의 설정을 잘못하여 이용자가 로그인 시 타인 계정으로 로그인되어 이용자의 개인정보가 공개되도록 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 9. 8. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 9. 23. 개인정보보호 위원회에 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)’, ‘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’) 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 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.

2. 위법성 판단

가. 개인정보가 열람권한이 없는 자에게 공개되지 않도록 하는 접근통제를 소홀히 한 행위 {보호법 제29조(안전조치의무)}

피심인은 개인정보 안전성 확보 등을 위하여 처리 중인 개인정보가 열람 권한이 없는 자에게 공개되지 않도록 조치를 하여야 하나, 캐시서버의 설정을 잘못하여 타 이용자 계정으로 로그인되어 열람권한 없는 자에게 이용자의 개인정보가 공개 되도록 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2, 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제)	§29	§48조의2	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) 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 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 부과 지침'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 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 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 사소한 부주의나 시스템의 오류로 인한 것으로 인정되는 점, 과태료의 사전통지 및 의견제출 기간 내에 법규 위반행위에 대하여 시정 완료한 점, 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점을 고려하여 기준금액의 30%인 180만원을 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



V. 결론

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

이의제기 방법 및 기간

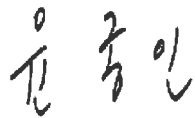
피심인은 이 시정명령 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.


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.

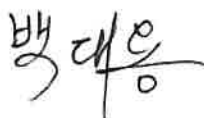
이상과 같은 이유로 주문과 같이 의결한다.

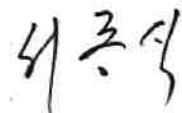
2021년 11월 10일

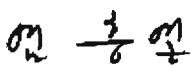
위원장 윤종인 


위원 강정화 

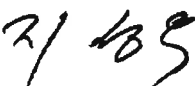
위원 고성학 

위원 백대용 

위원 서종식 

위원 염홍열 

위원 이희정 

위원 지성우 



II. 사실조사 결과

1. 조사 배경

개인정보보호위원회¹⁾는 캐시서버 설정 오류로 타 이용자 계정으로 로그인되어 유출 신고('20. 6. 5.) 및 이벤트 당첨자 공지 시 개인정보를 마스킹 처리하지 않고 공개하여 유출 신고('21. 7. 7.)에 따라 피심인에 대하여 개인정보 취급·운영 실태 및 정보통신망법·보호법 위반 여부를 조사(2021. 1. 11. ~ 2021. 9. 8.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 2021. 5. 3. 기준으로 이용자 16,625,469명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	(필수) 이름, 성별, 생년월일, 휴대전화번호, 이메일, ID, 비밀번호 (선택) 전화번호, 자택/직장주소, CI	08. 3. 27. ~ '21. 5. 3.	16,625,469

나. 개인정보 유출 경위

< 개인정보 유출 사건('20.6월) >

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)

1) 유출 경과 및 대응

일시		피해인의 유출입자 대응 내용
'20. 6. 4.	20:49	이용자 제보로 유출 사실 인지
	21:25	개발 담당자가 원인 파악
	21:35	개인정보 노출 URL 삭제 조치
'20. 6. 5.	16:09	한국인터넷진흥원에 개인정보 유출 신고
	19:02	유출 대상자 9명에게 이메일, 전화로 유출 사실 통지

2) 유출규모 및 경위

(유출항목 및 규모) 자동 로그인된 이용자의 개인정보(이름, 주소, 전화번호, 핸드폰번호, 이메일) 9건

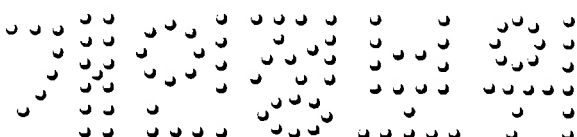
(유출 경위) 라이브커머스 행사 중 접속 페이지를 게시하면서 이용자의 로그인 정보도 같이 캐시 되도록 설정하여 타 이용자의 계정으로 로그인됨

- '21. 6. 4. 20:30 행사 도중 접속 페이지(URL) 게시

< 개인정보 유출 사건('21.7월) >

1) 유출 경과 및 대응

일시		피해인의 유출입자 대응 내용
'21. 7. 6.	22:00	이용자 제보(인스타그램 DM)로 유출 사실 인지
	22:10	이벤트 당첨자 게시물 삭제
'21. 7. 7.	16:39	유출 대상자 2,000명에게 문자로 유출 사실 통지
	17:01	한국인터넷진흥원에 개인정보 유출 신고



(유출항목 및 규모) 에 마스킹하지 않고 공지된 이벤트*

당첨자의 개인정보(이름, 휴대전화번호) 2,000건

- '21. 6. 28. ~ 7. 4. 이벤트를 진행하면서 통해 개인정보 2,733건
(성명, 휴대전화번호, 예방접종 완료 이미지) 수집

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

피심인은 이벤트 당첨자를 공지하면서 개인정보를 마스킹 처리하지 않고 게시하여, 권한 없는 자에게 이용자의 개인정보가 공개되도록 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 7. 7., 9. 10. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 7. 23., 9. 23. 개인정보보호위원회에 의견을 제출하였다.

III. 위법성 판단

1. 관련법 규정

< 개인정보 유출 사건('20.6월) - 정보통신망법 >

1. 관련법 규정

가. 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 한다.”고 규정하고 있다.

같은 법 시행령 제15조제2항은 “정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보처리시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)’, ‘개인정보처리시스템에 대한 침입

차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단(제3호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 등을 하여야 한다."고 규정하고 있다.

정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2019-13호, 이하 '고시') 제4조제9항은 "처리 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다."고 규정하고 있다.

'고시 해설서'는 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, (i) 인터넷 홈페이지 설계시에는 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 필요한 보안대책을 마련하고, (ii) 인터넷 홈페이지 개발시에는 개인정보 유·노출 방지를 위한 보안기술을 적용하고, (iii) 인터넷 홈페이지 운영·관리시에는 개인정보 유·노출 방지를 위한 보안대책 및 기술적용에 따른 적정성을 검증하고 개선조치를 하여야 한다고 해설하고 있으며, 또한 P2P 및 공유설정 등을 통한 개인정보 유·노출을 방지하기 위해 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등에 관한 보호조치를 하여야 한다."고 해설하고 있다.

< 개인정보 유출 사건('21.7월) >

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)’, ‘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’) 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 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.

2. 위법성 판단

< 개인정보 유출 사건('20.6월) >



가. 개인정보가 열람권한이 없는 자에게 공개되지 않도록 하는 접근통제를 소홀히 한 행위 {정보통신망법 제28조(개인정보의 보호조치)제1항}

피심인은 개인정보 안전성 확보 등을 위하여 처리 중인 개인정보가 열람 권한이 없는 자에게 공개되지 않도록 조치를 하여야 하나, 캐시서버 설정을 잘못하여, 권한 없는 자에게 이용자의 개인정보가 공개되도록 한 행위는 정보통신망법 제28조 제1항제2호, 같은 법 시행령 제15조제2항, 고시 제4조제9항 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
보호조치 위반 (접근통제)	§28①	§15②	열람 권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)

< 개인정보 유출 사건('21.7월) >

가. 개인정보가 열람권한이 없는 자에게 공개되지 않도록 하는 접근통제를 소홀히 한 행위 {보호법 제29조(안전조치의무)}

피심인은 개인정보 안전성 확보 등을 위하여 처리 중인 개인정보가 열람 권한이 없는 자에게 공개되지 않도록 조치를 하여야 하나, 이벤트 당첨자를 공지하면서 개인정보를 마스킹하지 않아 당첨자의 개인정보가 열람 권한이 없는 자에게 공개되도록 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2, 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제)	§29	§48조의2	열람 권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)

1. 시정조치 명령

1) 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.

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

< 개인정보 유출 사건('20.6월) >

가. 기준금액

정보통신망법 시행령 제74조의 [별표9] 과태료 부과기준은 최근 3년간 같은

위반행위로 과태료 부과처분을 받은 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 과태료인 1,000만원을 적용한다.

< 정보통신망법 시행령 [별표2] 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 동 지침 [별표2]의 가중기준에 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 동 지침 [별표1]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

피심인의 경우 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점, 일관되게 행위 사실을 인정하면서 조사에 적극 협력한 점, 이용자에게 피해가 발생하지 않은 등 위반행위의 결과가 경미하고 개인정보처리자의 사소한 부주의로 인한 것으로 인정되는 점을 고려하여 기준금액의 30%인 300만원을 감경한다.

다. 최종 과태료

피심인의 정보통신망법 제28조제1항을 위반한 행위에 대해 기준금액에 가중·감경을 거쳐 총 700만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보 보호조치 의무 위반 (접근통제)	1,000만원	-	300만원	700만원

< 개인정보 유출 사건('21.7월) >

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 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 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 사소한 부주의나 시스템의 오류로 인한 것으로 인정되는 점, 과태료의 사전통지 및 의견제출 기간 내에 법규 위반행위에 대하여 시정 완료한 점, 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점을 고려하여 기준금액의 30%인 180만원을 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

V. 결론

피심인의 정보통신망법 제28조제1항, 보호법 제29조 위반행위에 대하여 정보통신망법 제76조(과태료)제1항제3호, 보호법 제75조(과태료)제2항제6호, 제64조(시정조치 등)제1항에 따라 과태료, 시정조치 명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

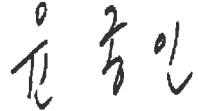
피심인은 이 시정명령 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.


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.

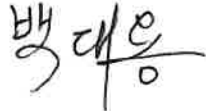
이상과 같은 이유로 주문과 같이 의결한다.

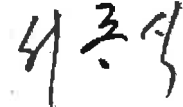
2021년 11월 10일

위원장 윤종인 


위원 강정화 


위원 고성학 

위원 백대용 

위원 서종식 

위원 염홍열 

위원 이희정 

위원 지성우 

심의회 의결

피 심 인 (사업자등록번호 :)

의결연월일 2021. 11. 10.

주 문

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 : 4,200,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

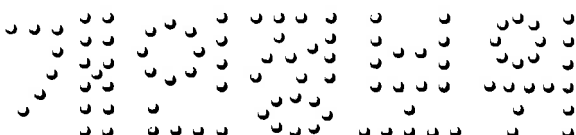
이 유

I. 기초 사실

피심인은 쇼핑 웹사이트를 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 >

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



II. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보종합포털(privacy.go.kr)에 유출 신고('20. 9. 18.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('20. 11. 23. ~ '21. 1. 8.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 쇼핑 웹사이트를 운영하면서 2020. 11. 27. 기준으로 이용자 16,142,764명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	(필수) 이름, 생년월일, 성별, 휴대폰번호, 이메일주소, 아이디(이메일), 비밀번호, 로그인번호, 기기정보, 셋탑박스아이디, TV비밀번호 (선택) 유선전화번호, SNS계정2차비밀번호, 주소, 닉네임, 결혼여부, 결혼기념일, 관심분야	'13. 7. 1. ~ '20. 11. 27.	16,142,764건

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지·대응 내용
'20. 9. 16.	18:54	홈페이지 공지사항에 이벤트 당첨자 명단 엑셀파일 게시
'20. 9. 17.	14:17	유출 관련 민원접수로 개인정보 유출인지
	14:19	해당 파일을 개인정보를 삭제한 엑셀파일로 교체
'20. 9. 18.	13:30	개인정보보호 포털을 통한 개인정보 유출신고
	14:40	유출된 이용자 대상 유출통지 이메일 발송

2) 유출규모 및 경위

(유출항목 및 규모) 이름, 휴대전화번호 등 업로드된 엑셀 파일에 포함된 개인정보 총 2,746건

(유출 경위) 피심인은 신규가입 고객을 대상으로 적립금 1억원 증정 이벤트를 진행하였으며 홈페이지에 당첨자 발표 시, 개인정보를 마스킹 처리하지 않고 단순 '숨기기' 처리한 엑셀 파일을 게시하여 개인정보가 공개됨

3. 개인정보의 취급·운영 관련 사실관계

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

피심인은 이벤트 당첨자 발표 과정에서 당첨자의 개인정보를 마스킹 처리하지 않아 이용자의 개인정보가 공개되도록 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021. 2. 22. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 3. 8. 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 차단 하기 위하여 ‘침입차단시스템 및 침입탐지시스템의 설치·운영(나목)’, ‘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’) 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 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.

2. 위법성 판단

가. 개인정보가 열람 권한이 없는 자에게 공개되지 않도록 하는 접근통제를 소홀히 한 행위{보호법 제29조(안전조치의무)}

피심인은 개인정보 안전성 확보 등을 위하여 처리 중인 개인정보가 열람 권한이 없는 자에게 공개되지 않도록 조치를 하여야 하나, 당첨자의 개인정보를 마스킹 처리하지 않고 발표하여 열람권한 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)	§29	§48조의2	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) 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 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 부과 지침'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 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 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 사소한 부주의나 시스템의 오류로 인한 것으로 인정되는 점, 과태료의 사전통지 및 의견제출 기간 내에 법규 위반행위에 대하여 시정 완료한 점, 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점을 고려하여 기준금액의 30%인 180만원을 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

V. 결론

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

이의제기 방법 및 기간

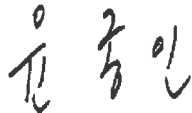
피심인은 이 시정명령 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.


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.

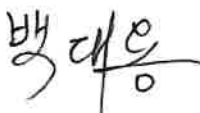
이상과 같은 이유로 주문과 같이 의결한다.

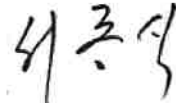
2021년 11월 10일

위원장 윤종인 


위원 강정화 

위원 고성학 

위원 백대용 

위원 서종식 

위원 염홍열 

위원 이희정 

위원 지성우 