

개 인 정 보 보 호 위 원 회

심의 · 의결

안 건 번 호 제2022 - 002 - 007호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2022. 1. 26.

주 문

1. 피심인 에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 10,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

I. 기초 사실

피심인은 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)	주소	종업원 수 (명)

II. 사실조사 결과

1. 조사 배경

개인정보보호위원회¹⁾는 개인정보종합포털(privacy.go.kr)에 유출 신고('20. 3. 9.)한 피심인에 대하여 개인정보 취급·운영 실태 및 정보통신망법 위반 여부를 조사('20. 12. 7. ~ '21. 3. 5.)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 '20. 4. 7. 기준으로 이용자 15,102명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	(필수) 이름, 아이디(이메일), 핸드폰, 주소, 비밀번호(암호화) (선택) 개인통관번호(암호화)	'15. 2. 25. ~ '20. 4. 7.	15,102건

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지·대응 내용
'20. 2. 26.	15:00	신원 미상의 자로부터의 해킹 공격 및 금품요구 연락 수신
	15:53	사이버경찰청에 신고 및 호스팅사()에 해킹 대응 요청, 공격자 IP(223.152.213.249) 차단
	22:28	서비스 장애 안내 홈페이지 공지
	-	한국인터넷진흥원 보호나라를 통해 해킹신고
	-	기존 개발자를 통한 취약점 보완 조치 및 DB 복구
'20. 2. 28.	09:18	한국인터넷진흥원 118 상담센터 신고접수 (보호나라 침해사고 재발방지 기술지원 진행)
'20. 3. 6.	14:11	보호나라 분석결과 수신 및 유출 인지
'20. 3. 9.	14:50	개인정보보호 포털을 통한 유출신고
'20. 3. 11.	00:33	이용자 대상 개인정보 유출 통지

2) 유출규모 및 경위

(유출항목 및 규모) 해킹으로 인한 개인정보 유출 당시 DB 내 저장된 전체 회원정보 테이블 약 55MB*로 추정

- '20. 2. 26. 기준 보유한 회원정보 데이터 크기가 55MB임을 확인하였으며, 이는 로그 기록 내 유출된 회원 테이블 용량*과 거의 일치

* 223.152.213.249(중국), 24/Feb/2020:13:15:16, POST/include/adminer.php?username='&db= &dump=t_member, 54,502,944 Byte

(유출 경위) 신원 미상의 자가 웹사이트 내 기프트카드 페이지의 파일 업로더 취약점을 이용하여 웹shell을 업로드하고, DB 관리 툴을 이용하여 개인정보를 외부로 유출

3. 개인정보의 취급·운영 관련 사실관계

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

피심인은 운영 중인 개인정보처리시스템 관리자페이지에 외부에서 접속 시 ID/PW만을 이용하며 안전한 인증수단을 적용하지 않고, 파일 업로드 및 실행 제한, 취약점 점검 및 개선 등을 실시하지 않아, 55MB 크기의 회원정보 테이블이 유출 되도록 한 사실이 있다.

나. 개인정보 유출신고 및 이용자 대상 유출통지를 지연한 행위

피심인은 '20. 3. 6. 해킹 관련 보호나라 분석결과를 수신하고 개인정보 유출사실을 인지하였으나 약 3일을 경과하여 개인정보보호 포털에 유출신고('20. 3. 9.)하였으며, 약 5일을 경과하여 이용자 대상 유출 통지를 실시('20. 3. 11.)한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '21. 5. 18. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 5. 24. 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 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)’, ‘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’) 제4조제4항은 “정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.”고 규정하고 있으며

‘고시 해설서’는 고시 제4조제4항에 대해 “인터넷 구간 등 외부로부터 개인정보 처리시스템에 접속은 원칙적으로 차단하여야 하나, 정보통신서비스 제공자등의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용 컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요할 때에는 안전한 인증수단을 적용하여야 한다.”라고 해설하고 있다.

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 있으며

‘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 접근 통제 등에 관한 보호조치를 하여야 한다.”고 해설하고 있다.

나. 정보통신망법 제27조의3제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 ‘유출등’이라 한다) 사실을 안 때에는 지체없이 다음 각호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니된다.”고 규정하고 있다.

같은 법 시행령 제14조의2제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제27조의3제1항 각 호의 모든 사항을 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.”고 규정하고 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, 개인정보처리시스템 관리자 페이지에 외부에서 접속 시 ID/PW만을 이용하고, 업로드 취약점 점검 등을 수행하지 않아 권한 없는 자에게 이용자의 개인정보가 공개되도록 한 행위는 정보통신망법 제28조제1항, 같은 법 시행령 제15조제2항, 고시 제4조제4항 및 제9항을 위반한 것이다.

나. 개인정보 유출신고 및 이용자 대상 유출통지를 지연한 행위{정보통신망법 제27조의3(개인정보 유출등의 통지·신고)제1항}

피심인은 개인정보의 유출 사실을 안 때에는 24시간 내 유출신고 및 이용자 대상 유출통지를 하여야 하나, 이를 경과하여 신고 및 통지한 행위는 정보통신망법 제27조의3제1항, 같은 법 시행령 제14조의2제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
보호조치 위반 (접근통제)	§28①	§15②	- 외부에서 개인정보처리시스템에 접속 시 안전한 인증 수단을 적용하지 않은 행위(고시§4④) - 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§4⑨)
개인정보 유출등의 통지·신고 위반	§27조의3①	§14조의2①	- 개인정보의 유출 사실을 안 때로부터 24시간 내에 유출 신고 및 이용자 대상 유출 통지를 하지 않은 행위

IV. 처분 및 결정

1. 과태료 부과

피심인의 정보통신망법 제27조의3(개인정보 유출등의 통지·신고) 제1항 및 제28조(개인정보의 보호조치)제1항 위반행위에 대한 과태료는 같은 법 제76조(과태료)제1항 제2호의3 및 제3호, 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 각 적용한다.

< 정보통신망법 시행령 [별표2] 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 제1항 제2호의3	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 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 1인 창조기업으로서 재정적 부담이 어려운 경우, 위반행위 시정 완료 및 조사에 적극 협력한 점 등을 고려하여 기준금액의 50%인 500만원을 각 감경한다.

다. 최종 과태료

피심인의 정보통신망법 제27조의3(개인정보 유출등의 통지·신고) 제1항 및 제28조(개인정보의 보호조치)제1항 위반행위에 대해 기준금액에 가중·감경을 거쳐 총 1,000만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보 보호조치 의무 위반 (접근통제)	1,000만원	-	500만원	500만원
개인정보 유출등의 통지·신고 위반	1,000만원	-	500만원	500만원

V. 결론

피심인의 정보통신망법 제27조의3(개인정보 유출등의 통지·신고) 제1항 및 제28조(개인정보의 보호조치)제1항 위반행위에 대하여 정보통신망법 제76조(과태료)제1항제2호의3 및 제3호에 따라 과태료 부과를 주문과 같이 의결한다.

이의제기 방법 및 기간

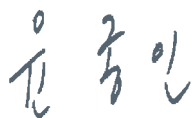
피심인은 이 시정명령 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

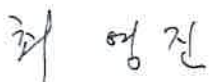
피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.


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.

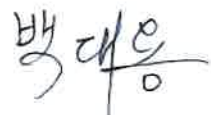
이상과 같은 이유로 주문과 같이 의결한다.

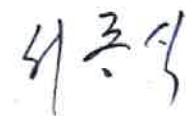
2022년 01월 26일

위원장 윤종인 


부위원장 최영진 

위원 고성학 

위원 백대용 

위원 서종식 

위원 염홍열 

위원 지성우 



심의 · 의결

피 심 인 (사업자등록번호 :)

의결연월일 2022. 1. 26.

다. 납부장소 : 한국은행 국고수납 대리점

이 유

I. 기초 사실

피심인은 온라인 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 일반 현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	주소	종업원 수 (명)

II. 사실조사 결과

1. 조사 배경

개인정보보호위원회¹⁾는 개인정보종합포털(privacy.go.kr)에 유출 신고(‘20. 5. 13.)한 피심인에 대하여 개인정보 취급·운영 실태 및 정보통신망법 위반 여부를 조사(‘21. 1. 28. ~ ’21. 8. 20.)하였으며, 다음과 같은 사실을 확인하였다.

1) 2020. 8. 5. 시행된 개정 「개인정보 보호법」(법률 제16930호, 2020. 2. 4. 일부개정) 부칙 제3조에 따라, 개인정보보호 위원회가 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 '21. 3. 18. 기준, 이용자 6,200명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	(필수) 아이디, 비밀번호, 이름, 닉네임, 성별, 생년월일, 이메일, 주소, 휴대전화번호, 전화번호 (선택) 추천인 아이디	'12. 10. 31. ~ '21. 3. 18.	6,200건

* 해킹사고 발생('20.5.2.) 이후, 분리보관 중이었던 회원정보 모두 파기 조치하였다고 소명

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시	피심인의 유출인지·대응 내용
'20. 5. 11.	- 호스팅사()로부터 신원 미상의 자의 알 수 없는 방법으로 DB 회원정보가 엑셀파일로 다운로드되어 유출되었다는 유선연락 수신
15:38	자세한 해킹 정황 파악을 위해 호스팅사 홈페이지에 문의글 작성
15:46	호스팅사 답변 글을 통해 개인정보 유출 인지
'20. 5. 12.	- 이용자 대상 개인정보 유출통지
'20. 5. 13.	15:16 개인정보보호 포털을 통한 개인정보 유출신고

2) 유출규모 및 경위

(유출항목 및 규모) 해킹('20.5.2.) 당시 보유하고 있던 개인정보 71,188건(추정)

(유출 경위) 피심인은 로그기록 등을 별도로 백업하여 보관하고 있지 않았으며 해킹 정황을 안내한 호스팅사 또한 별도로 보관하고 있지 않아 유출 경위를 파악하는데 한계

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 운영 중인 개인정보처리시스템 관리자페이지에 외부에서 접속 시 ID/PW만을 이용하고 안전한 인증수단을 적용하지 않았으며, 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ① 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하거나 ② IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영하지 않은 사실이 있다.

나. 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위

또한 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 하나 관련 자료를 제출하지 못한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '21. 9. 1. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '22. 1. 7. 개인정보보호위원회에 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 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)’, ‘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’) 제4조제4항은 “정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.”고 규정하고 있으며

‘고시 해설서’는 고시 제4조제4항에 대해 “인터넷 구간 등 외부로부터 개인정보처리시스템에 접속은 원칙적으로 차단하여야 하나, 정보통신서비스 제공자등의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용 컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요할 때에는 안전한 인증수단을 적용하여야 한다.”라고 해설하고 있다.

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 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 한다."고 규정하고 있다.

같은 법 시행령 제15조제3항은 "정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 '개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(제1호)', '개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관(제2호)'하여야 한다."라고 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') 제5조제1항은 "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 하며, 식별자, 접속일시, 접속지, 수행업무 등의 접속기록을 최소 1년 이상 보존·관리하여야 한다."라고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 개인정보 안전성 확보 등을 위하여 기술적·관리적 조치를 하여야 하나, 개인정보처리시스템 관리자페이지에 외부에서 접속 시 ID/PW만을 이용하고, 침입탐지·차단시스템 등을 설치·운영하지 않은 행위는 정보통신망법 제28조제1항, 같은 법 시행령 제15조제2항, 고시 제4조제4항 및 제5항을 위반한 것이다.

나. 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위

피심인은 개인정보 안전성 확보 등을 위하여 기술적·관리적 조치를 하여야 하나, 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 않았고 시스템 이상 유무 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하지 아니한 행위는 정보통신망법 제28조제1항, 같은 법 시행령 제15조제3항, 고시 제5조제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
보호조치 위반 (접근통제) (접속기록 위·변조 방지)	§28①	§15②③	<ul style="list-style-type: none"> - 외부에서 개인정보처리시스템에 접속 시 안전한 인증수단을 적용하지 않은 행위(고시§4④) - 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 침입탐지·차단시스템을 설치·운영하지 않은 행위(고시§4⑤) - 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 1년 이상 보존·관리하지 않은 행위(고시§5①)

IV. 처분 및 결정

1. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 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 따라 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우(제3호)에 해당하여 기준 금액의 10%인 100만원을 가중한다.

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 위반행위에 대해 시정완료한 경우 등에 해당하여 기준금액의 50%인 500만원을 감경한다.

다. 최종 과태료

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 위반행위에 대해 기준 금액에 가중·감경을 거쳐 총 600만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보 보호조치 의무 위반 (접근통제) (접속기록 위·변조 방지)	1,000만원	100만원	500만원	600만원

V. 결론

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 위반행위에 대하여 정보통신망법 제76조(과태료)제1항제3호에 따라 과태료 부과를 주문과 같이 의결한다.

이의제기 방법 및 기간

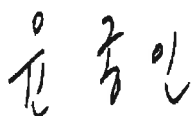
피심인은 이 시정명령 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

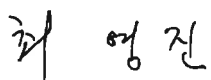
피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.

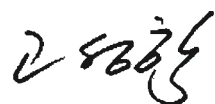
과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 규정에 따라 그 효력을 상실하고 관할법원(당사자 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료 납입 의무를 부담한다.

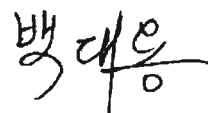
이상과 같은 이유로 주문과 같이 의결한다.

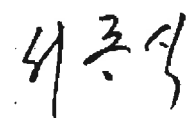
2022년 01월 26일

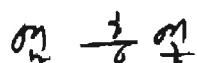
위원장 윤종인 


부위원장 최영진 

위원 고성학 

위원 백대용 

위원 서종식 

위원 염홍열 

위원 지성우 



개 인 정 보 보 호 위 원 회

심의 · 의결

안 건 번 호 제2022 - 002 - 009호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자 :

의결연월일 2022. 1. 26.

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

4) 이용자의 비밀번호, 주민등록번호는 복호화되지 아니하도록 안전한 암호 알고리즘으로 일방향 암호화하여 저장하여야 한다.

다. 1년 이상 서비스를 이용하지 아니하는 이용자의 개인정보를 보호하기 위해 파기 또는 분리보관 등의 조치를 취하여야 한다.

라. 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 : 10,800,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

I. 기초 사실

피심인은 홈페이지를 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	대표자 성명	주소	종업원 수 (명)

II. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보종합포털(privacy.go.kr)에 유출 신고('21. 7. 31.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('21. 12. 24. ~ '21. 1. 7.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 홈페이지를 운영하면서 '21. 10. 14. 기준으로 이용자 5,690명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원 정보	(필수) 아이디, 비밀번호, 이름, 주소, 이메일 핸드폰번호 (선택) 성별, 생년월일, 전화번호	'12. 2. 14. ~ '21. 10. 14.	5,609건

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지·대응 내용
'21. 7. 23.	-	KISA 118민원센터에서 개인정보가 검색된다는 민원 접수
'21. 7. 30.	-	KISA 개인정보탐지조사팀에서 확인 후 개인정보 노출 삭제 요청
	-	개인정보 유출 페이지에 대한 URL 접속 차단
'21. 7. 31.	04:07	이용자 대상 개인정보 유출 통지
	05:10	개인정보보호 포털을 통한 개인정보 유출신고

2) 유출규모 및 경위

(유출항목 및 규모) 이름·주소·연락처·이메일 등 관리자페이지의 주문정보 페이지에 포함된 이용자 2,478명의 개인정보

(유출 경위) 피심인은 제작 홈페이지를 운영하면서 관리자페이지에 대한 접근통제 조치를 하지 않아 URL 주소* 입력 시 별도의 로그인 절차 없이 접속되도록 운영

- 이후 구글, Bing, 야후 등 검색엔진이 해당 URL 주소를 수집·표출하여 누구나 검색엔진을 통해 관리자페이지에 접속 가능하게 됨

3. 개인정보의 취급·운영 관련 사실관계

가. 법령상 근거 없이 이용자의 주민등록번호를 수집·이용한 행위

피심인은 '21. 10. 14. 기준, '11. 5. 3. ~ '13. 7. 17 기간 동안 법적근거 없이 수집한 823건의 주민등록번호를 보관한 사실이 있다.

나. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하거나, 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 시스템을 설치·운영한 사실이 없으며, 관리자페이지에 로그인 등 인증절차를 적용하지 않아 처리 중인 개인정보가 열람 권한이 없는 자에게 공개되도록 한 사실이 있다.

다. 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위

피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 1년 이상 보존·관리하지 않은 사실이 있다.

라. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

피심인은 수집한 이용자의 비밀번호 및 주민등록번호를 암호화하지 않고 평문으로 저장하여 관리한 사실이 있다.

마. 1년 이상 장기 미이용자의 개인정보를 파기하지 않은 행위

피심인은 주문정보 확인을 위한 관리자페이지에서 '21. 7. 30. 기준, 배송이 완료된 후 5년이 경과된 2,631건의 주문정보를 파기하지 않고 보관한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '21. 12. 24. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '22. 1. 6. 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 제48조의2제1항제2호는 “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 있다.

제48조의2제1항제3호는 “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 있다.

제48조의2제1항제4호는 “개인정보가 안전하게 저장·전송될 수 있도록 비밀번호, 주민등록번호 등 보호위원회가 정하여 고시하는 정보의 암호화 저장(나목)”을 하여야 한다.”라고 규정하고 있다.

제48조의2제3항은 “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 있으며 제4조제9항은 “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.”라고 규정하고 있다.

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 제6조제1항은 “정보통신서비스 제공자등은 비밀번호는 복호화되지 아니

하도록 일방향 암호화하여 저장한다.”고 규정하고 있으며, 제6조제2항은 “정보통신 서비스 제공자들은 주민등록번호 등 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다.”라고 규정하고 있다.

다. 보호법 제39조의6제1항은 정보통신서비스 제공자들은 정보통신서비스를 1년의 기간동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다고 규정하고 있다.

보호법 시행령 제48조의5는 정보통신서비스 제공자들은 이용자가 정보통신서비스를 법 제39조의6제1항의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나, 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다고 규정하고 있다.

2. 위법성 판단

가. 법령상 근거 없이 이용자의 주민등록번호를 수집·보관한 행위{보호법 제24조의2(주민등록번호 처리의 제한)}

피심인이 법적 근거없이 이용자의 주민등록번호를 수집·보관한 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 관리자페이지에 로그인 인증절차를 적용하지 않는 등 접근통제 조치를 취하지 않아 개인정보가 열람 권한이 없는 자에게 공개되도록 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제9항을 위반한 것이다.

다. 개인정보처리시스템의 접속기록 보관 및 점검을 소홀히 한 행위{보호법 제29조(안전조치의무) 중 접속기록의 위·변조 방지}

피심인은 개인정보취급자가 개인정보처리시스템(웹서버 및 DB 서버)에 접속한 기록을 월 1회 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.

라. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위{보호법 제29조(안전조치의무) 중 암호화}

피심인이 이용자의 비밀번호 및 수집한 주민등록번호를 저장하면서 안전한 암호알고리즘으로 암호화하지 않고 저장한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제4호, 고시 제6조제1항 및 제2항을 위반한 것이다.

마. 1년 이상 장기 미이용자의 개인정보를 별도로 저장·관리하지 않은 행위 {보호법 제39조의6(개인정보의 파기에 대한 특례)제1항}

피심인이 배송이 완료된 후 5년이 경과된 2,631건의 주문정보를 파기하지 않고, 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 행위는 보호법 제39조의6제1항 및 같은 법 시행령 제48조의5를 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
주민등록번호 처리의 제한	보호법 §24의2④	-	• 법령상 근거 없이 이용자의 주민등록번호 처리한 행위
안전조치의무 위반 (접근통제, 접속기록, 암호화)	보호법 §29	§48의2① 제2호·제3호·제4호	<ul style="list-style-type: none"> • 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) • 이용자의 비밀번호가 복호화 되지 아니하도록 일방향 암호화하여 저장하지 아니한 행위(§6①) • 주민등록번호, 계좌번호 등을 안전한 암호알고리즘으로 암호화하여 저장하지 아니한 행위(§6②)
개인정보 파기 위반 (유효기간제)	보호법 §39의6	§48의5	• 1년 이상 미이용자의 개인정보를 파기하거나, 다른 이용자의 개인정보와 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) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.

4) 이용자의 비밀번호, 주민등록번호는 복호화되지 아니하도록 안전한 암호 알고리즘으로 일방향 암호화하여 저장하여야 한다.

다. 1년 이상 서비스를 이용하지 아니하는 이용자의 개인정보를 보호하기 위해 파기 또는 분리보관 등의 조치를 취하여야 한다.

라. 가.부터 나.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출 하여야 한다.

2. 과태료 부과

피심인의 보호법 제24조의2, 제29조, 제39조의6 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제4호·제4호의2·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 각각 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
차. 법 제24조의2제1항을 위반하여 주민등록번호를 처리한 경우	법 제75조 제2항제4호의2	600	1,200	2,400
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

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, 안전성 확보에 필요한 조치를 하지 않은 행위에 대하여 ▲제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상인 경우로 기준금액의 10%를 가중하며, 법령에 근거 없이 주민등록번호를 처리한 행위, 개인정보 파기 등 필요한 조치를 하지 않은 행위에 대하여 ▲위반 기간이 3개월 이상인 경우로 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 과태료의 사전통지 및 의견제출 기간 내에 법규 위반행위에 대하여 시정 완료한 점, 일관되게 행위 사실을 인정하면서 위법성 판단에 도움되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점을 고려하여 기준금액의 50%를 각각 감경한다.

다. 최종 과태료

피심인의 보호법 제24조의2, 제29조, 제39조의6을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,080만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
주민등록번호 처리의 제한 (법령상 근거 없이 이용자의 주민등록번호 처리)	600만원	60만원	300만원	360만원
안전조치의무 위반 (접근통제, 접속기록, 암호화)	600만원	60만원	300만원	360만원
개인정보의 파기에 대한 특례	600만원	60만원	300만원	360만원
계	1,800만원	180만원	900만원	1,080만원

V. 결론

피심인의 보호법 제24조의2, 제29조, 제39조의6 위반행위에 대하여 같은 법 제75조 (과태료)제2항 제4호·제4호의2·제6호, 제64조(시정조치 등)제1항에 따라 과태료, 시정조치 명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

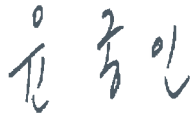
피심인은 이 시정명령 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

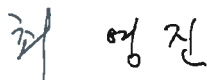
피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.


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.

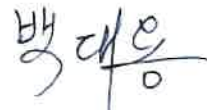
이상과 같은 이유로 주문과 같이 의결한다.

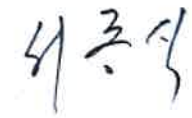
2022년 01월 26일

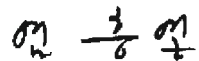
위원장 윤종인 

부위원장 최영진 

위원 고성학 

위원 백대용 

위원 서종식 

위원 염홍열 

위원 지성우 