개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2023-001-001호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2023. 1. 11.

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

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

이 유

Ⅰ. 기초 사실

커피 및 관련 용품, 커피숍 서비스 등을 제공하는 피심인은 「(舊)정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2020. 8. 5. 법률 제16955호로 개정·시행되기 이전, 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

개인정보보호위원회는 언론보도('22. 8. 9., 디지털타임스 등)와 국민신문고 민원 신고에 따라 피심인에 대하여 개인정보 취급·운영 실태 및 정보통신망법·「개인정보보호법」(2020. 8. 5. 시행, 법률 제16930호, 이하 '보호법'이라 한다) 위반 여부를 조사('22. 8. 23. ~ 11. 28.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 서비스 관련 온라인 홈페이지(　　)를 운영하면서 '22. 8. 29. 기준으로 이용자　　명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
회원 정보	(필수) 이름, 생년월일, 성별, 아이디, 비밀번호, 휴대전화 번호, 이메일, DI, ****** 카드번호, ****** 카드 핀번호 (선택) 자동차 등록번호, 배송지 정보(배송지 주소, 연락처, 이름), 은행 계좌번호		
합 계			

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출 인지·대응 내용
’15. 8. 경	-	정보통신망법 시행령 개정에 따른 휴면 계정 처리 관련, 유효회원과 휴면회원 분리보관을 위한 시스템 변경·시행
‘16. 10. 14.	-	이용자 A가 본인의 아이디( )가 아닌 이용자 B의 아이디( )로 ******** 홈페이지에 로그인을 시도하였고, 휴면 계정 해제 및 계정정보(이름, 휴대전화 번호, 이메일주소) 수정 진행
‘17. 10. 6.	-	이용자 C가 본인의 아이디( )가 아닌 이용자 D의 아이디( )로 ******** 홈페이지에 로그인을 시도하였고, 휴면 계정 해제 및 계정정보(이름, 휴대전화 번호, 이메일) 수정을 진행
‘17. 11. 22.	-	이용자 B가 홈페이지에 로그인 시도했으나 실패하자 본인 인증*을 통해 비밀번호 변경 후 로그인하였고, 이후 계정정보에 타인의 정보(이용자 A)가 입력되어 있는 것을 보고 ********** 고객센터에 신고함 * 본인 인증은 최초 회원가입 시 수집한 이용자 B의 DI값 확인으로 수행
‘17. 12. 18.	-	이용자 D가 홈페이지에 로그인 시도했으나 실패하자 본인 인증*을 통해 비밀번호 변경 후 로그인하였고, 이후 계정정보에 타인의 정보(이용자 C)가 입력되어 있는 것을 보고 ********** 고객센터에 신고함 * 본인 인증은 최초 회원가입 시 수집한 이용자 D의 DI값 확인으로 수행
’18. 1. 30.	-	시스템 오류 사항 파악 후, 휴면 해제 시 아이디와 비밀번호를 확인하는 로직 추가 ※ 피심인은 상기 로직 외, 휴면 해제 시 아이디와 DI값을 비교하는 로직과 회원정보 수정 시 아이디와 DI값을 비교하는 로직 등을 추가함

2) 유출규모 및 경위

(유출항목 및 규모) 홈페이지 이용자 4명의 이름, 휴대전화 번호, 이메일주소

(유출 경위) 피심인은 ’15. 8월경 시스템을 고도화(정보통신망법 시행령 개정에 따른 조치)하는 과정에서, 휴면 계정 해제 시 비밀번호 확인 없이 아이디 입력만으로도 휴면 계정이 해제될 수 있도록 운영하여 이용자의 개인정보가 유출되었다.

- 언론보도 내용인 DI값 중복 설정 오류가 아닌, 휴면 계정 해제 시 아이디와 해당 아이디에 대한 비밀번호를 확인하는 로직이 누락되어, 이용자가 타인의 아이디만을 입력하고 접속을 시도해도 휴면 계정이 해제되는 오류가 발생하였다.

  ※ 해당 계정이 휴면 계정일 경우에만 발생하는 현상으로, 휴면 계정이 아닐 경우에는 비밀번호 불일치 시 로그인되지 않음

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 '15. 8. 경부터 '18. 1. 30.까지 홈페이지 휴면 계정 해제 시, 아이디와 해당 아이디에 대한 비밀번호를 확인하는 로직을 누락하여 이용자 4명의 개인정보가 유출된 사실이 있다.

나. 개인정보 유출신고를 소홀히 한 행위

피심인은 정당한 사유 없이 유출 사실을 신고하지 않은 사실이 있다.

다. 기타 언론보도 및 민원신고 내용에 대한 행위

상기 사항 외, 언론보도 등에 따른 내용인 ①'22년에 발생한 클라우드서비스 보안취약점에 관한 건 ②개인정보 보호책임자에 대한 불이익한 인사조치 건에 대해서는 보호법 위반 사실을 확인하지 못하였다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '22. 11. 29. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '22. 12. 14. 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 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 ‘개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영(제2호)’ 등 기술적·관리적 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제15조제2항은 “정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)’ 등을 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제15조제6항에 따라 위 기준 수립 · 시행의 내용을 구체적으로 정하고 있는 「(舊)개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-03호, 이하 ‘고시’라 한다) 제4조제9항은 “취급 중인 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.

나. 정보통신망법 제27조의3제1항은 “정보통신서비스 제공자등은 개인정보의 유출등 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 아니 된다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위[정보통신망법 제28조(개인정보의 보호조치)제1항]

피심인이 인터넷 홈페이지를 통한 휴면 계정 해제 시, 아이디와 해당 아이디에 대한 비밀번호를 확인하는 로직을 누락하여 이용자의 개인정보가 유출되도록

운영한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.

나. 유출 신고를 소홀히 한 행위[정보통신망법 제27조의3(개인정보 유출등의 통지·신고)제1항]

피심인이 정당한 사유 없이 유출 사실을 신고하지 않은 행위는 정보통신망법 제27조의3제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보의 보호조치 위반	정보통신망법 §28①	§15②제5호	・열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위(고시§4⑨)
개인정보 유출등의 통지·신고 위반	정보통신망법 §27의3①	-	・정당한 사유 없이 유출 사실을 신고하지 않은 행위

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 및 제27조의3(개인정보 유출등의 통지·신고)제1항을 위반한 행위에 대하여 같은 법 제76조(과태료)제1항제3호·제2호의3, 같은 법 시행령 제74조, 같은 법 시행령 [별표9] '과태료의 부과기준' 및 '(舊)개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침'(2018. 7. 4. 방송통신위원회 의결, 이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

정보통신망법 시행령 제74조의 [별표9]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 각 위반행위별 기준금액을 1,000만원으로 산정한다.

< 정보통신망법 시행령 [별표9] 2. 개별기준 >

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
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

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 있다'라고 규정하고 있다.

피심인의 경우 해당사항이 없어 기준금액을 유지한다.

2) 과태료의 감경

과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲사업규모·자금사정, ▲개인(위치)정보보호 노력정도, ▲조사협조·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 있다.'라고 규정하고 있다.

피심인의 경우, 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위는 '정보보호 관리체계 인증(ISMS)을 받은 경우', '위반행위에 대해 시정을 완료한 경우', '조사에 적극 협력한 경우'에 해당하여 기준금액의 50%를 감경하고, 유출 신고를 소홀히 한 행위는 '정보보호 관리체계 인증(ISMS)을 받은 경우', '조사에 적극 협력한 경우'에 해당하여 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 정보통신망법 제28조제1항 및 같은 법 제27조의3제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,000만 원의 과태료를 부과한다.

< 과태료 산출내역 >

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

3. 결과 공표

보호법 제66조제1항 및 '개인정보 보호위원회 처분결과 공표기준'(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따르면 피심인의 위반행위는 보호법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우(제4호), 위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)에 해당하므로 피심인에 대한 과태료 부과 사실에 대해 개인정보보호위원회 홈페이지에 공표한다.

(舊)정보통신망 이용촉진 및 정보보호에 관한 법률 위반 행정처분 결과 공표				
위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	위반조항	위반내용	처분일자	처분내용
	법 제28조제1항	개인정보의 보호조치 위반	2023.1.11.	과태료 부과 500만원
	법 제27조의3 제1항	개인정보 유출등의 통지·신고 위반	2023.1.11.	과태료 부과 500만원

Ⅴ. 결론

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 및 같은 법 제27조의3(개인정보 유출등의 통지·신고)제1항을 위반한 행위에 대하여 같은 법 제76조(과태료)제1항제3호·제2호의3, 보호법 제66조(결과의 공표)제1항에 따라 과태료, 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

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

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

2023년 1월 11일

위 원 장　　고 학 수　(서 명)

부위원장　　최 장 혁　(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　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)