개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2022-004-013호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인

의결연월일 2022. 2. 23.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.

나. 피심인은 법령에서 민감정보의 처리를 요구하거나 허용하는 경우 또는 이용자에게 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우가 아니면 민감정보를 처리하지 아니하여야 한다.

다. 피심인은 법령 등에서 주민등록번호의 처리를 요구하거나 허용한 경우 등을 제외하고는 이용자의 주민등록번호를 처리하지 아니하여야 한다.

라. 피심인은 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.

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

3) 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.

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

5) 주민등록번호에 대해서는 안전한 암호알고리듬으로 암호화하여 저장하여야 한다.

마. 피심인은 개인정보의 유출 사실을 안 때에는 지체 없이 유출된 개인정보 항목, 유출이 발생한 시점, 이용자가 취할 수 있는 조치, 정보통신서비스 제공자등의 대응 조치, 이용자가 상담 등을 접수할 수 있는 부서 및 연락처 등을 해당 이용자에게 알려야 한다.

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

사. 피심인은 가.부터 바.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 : 129,790,000원

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.

4. 피심인을 수사기관에 고발한다.

이 유

Ⅰ. 기초 사실

피심인은 소개팅앱 ‘ ’을 운영하는 「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16930호, 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. 9. 28.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사(’21. 10. 15. ~ ’21. 12. 21.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 소개팅앱인 ‘ ’을 운영하면서 ’21.9.23. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
회원 정보	(필수) 이름, 나이, 휴대전화번호, 이메일, 직업, 종교, 사진 등 (선택) 회사·학교 정보, 인증서류(신분증, 가족관계증명서 등)	‘18. 11. 12. ~ ’21. 9. 23.	

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출 인지·대응 내용
2021. 9. 26.	01:33	해커로부터 협박 메일 수신
	08:30	협박 메일 확인
2021. 9. 27.	14:00	서울경찰청 사이버수사과에 신고
	18:00	외부 보안업체 분석 의뢰
	19:00	경찰 조사 직후 TF팀을 구성하여 해커가 송부한 파일이 회원의 개인정보가 맞는지 여부 확인 등 유출 인지
	21:47	보호나라에 해킹 신고
2021. 9. 28.	18:00	개인정보보호포털에 개인정보 유출 신고

2) 유출규모 및 경위

(1) 유출규모

소개팅앱 ‘ ’ 서비스 이용자 143,435명의 개인정보*가 유출되었다.

* 이름, 나이, 휴대전화번호, 이메일, 직업, 종교, 사진, 회사·학교 정보, 인증서류(신분증, 가족관계증명서 등), 게시판 글 등

(2) 유출경위

해커는 ’21. 9. 23. 노출된 아마존웹서비스(이하, AWS) 루트 Access Key를 이용하여 AWS에 접속한 후 DB의 백업 파일을 생성하여 외부로 전송하였으며, ’21. 9. 24. AWS S3에 추가 접속하여 이용자가 제출한 증빙서류 및 프로필 이미지를 다운로도 하였다.

3. 개인정보의 취급.운영 관련 사실관계

가. 불필요하게 된 개인정보를 파기하지 않은 행위

피심인은 ’19. 5. 22.부터 ’21. 9. 13.까지 가입한 이용자 중 서비스를 탈퇴한 이용자의 개인정보를 파기하지 않고 보관한 사실이 있다.

나. 민감정보 처리에 대한 별도 동의를 받지 않은 행위

피심인은 ’18. 11. 12.부터 법령에서 민감정보의 처리를 요구하거나 허용하는 경우가 아님에도 불구하고 이용자에게 별도 동의를 받지 않고 민감정보를 처리한 사실이 있다.

다. 법령 등의 근거 없이 주민등록번호를 처리한 행위

피심인은 ’18. 11. 12.부터 법령 등에서 주민등록번호의 처리를 요구하거나 허용한 경우 등이 아님에도 불구하고 이용자 주민등록번호가 포함된 인증서류를 수집·저장한 사실이 있다.

라. 안전성 확보에 필요한 조치를 하지 않은 행위

1) 피심인은 ’18. 11. 12.부터 AWS를 이용하면서 추가 인증수단을 적용하지 않고 운영하였으며, 개인정보처리시스템에 대한 접속권한을 아이피주소 등으로 제한하지 않고, AWS S3에 저장된 일부 파일의 접근통제를 공개로 설정하여 운영하는 등 개인정보가 열람권한 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하지 않은 사실이 있다.

2) 피심인은 ’18. 11. 12.부터 앱 이용자 개인정보를 저장하면서 접속기록을 1년 이상 보존하지 않은 사실이 있다.

3) 피심인은 ’18. 11. 12.부터 주민등록번호가 포함된 인증서류를 수집한 후 주민등록번호를 암호화하지 않고 저장한 사실이 있다.

마. 유출 통지를 하지 않은 행위

피심인은 유출된 개인정보 항목, 유출이 발생한 시점, 이용자가 취할 수 있는 조치 등을 이용자에게 알리지 않은 사실이 있다.

바. 1년 이상 미이용자의 개인정보를 파기 등을 하지 않은 행위

피심인은 앱에 가입한 이용자 중 1년 이상 접속하지 않은 이용자의 개인정보를 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’22. 1. 10. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’22. 1. 26. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 보호법 제21조제1항은 “개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.”라고 규정하고 있다.

나. 보호법 제23조제1항은 “개인정보처리자는 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다. 다만, ‘정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우(제1호)’, ‘법령에서 민감정보의 처리를 요구하거나 허용하는 경우(제2호)’의 어느 하나에 해당하는 경우에는 그러하지 아니하다.”라고 규정하고 있다.

다. 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)’의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.”라고 규정하고 있다.

라. 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.

같은 법 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.

같은 법 시행령 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.

같은 법 시행령 제48조의2제1항제4호는 “개인정보가 안전하게 저장ㆍ전송될 수 있도록 주민등록번호 등 보호위원회가 정하여 고시하는 정보의 암호화 저장(나목)”을 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제48조의2제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

같은 법 시행령 제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시

제2021-3호, 이하 '고시') 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다."라고 규정하고 있으며, 제4조제5항제1호는 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다."라고 규정하고 있고, 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 제6조제2항은 "정보통신서비스 제공자등은 주민등록번호 등의 정보에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다."라고 규정하고 있다.

마. 보호법 제39조의4제1항은 "정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 유출등이 된 개인정보 항목(제1호), 유출등이 발생한 시점(제2호), 이용자가 취할 수 있는 조치(제3호), 정보통신서비스 제공자등의 대응 조치(제4호), 이용자가 상담 등을 접수할 수 있는 부서 및 연락처(제5호)를 해당 이용자에게 알리고 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다."라고 규정하고 있다.

바. 보호법 제39조의6제1항은 정보통신서비스 제공자등은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다고 규정하고 있다.

같은 법 시행령 제48조의5제1항은 “정보통신서비스 제공자등은 이용자가 정보통신서비스를 법 제39조의6제1항의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나, 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

가. 불필요하게 된 개인정보를 파기하지 않은 행위{보호법 제21조(개인정보의 파기)제1항}

피심인이 서비스를 탈퇴한 이용자의 개인정보를 파기하지 않은 행위는 보호법 제21조제1항을 위반한 것이다.

나. 민감정보 처리에 대한 별도 동의를 받지 않은 행위{보호법 제23조(민감정보의 처리 제한)제1항}

피심인이 법령에서 민감정보의 처리를 요구하거나 허용하는 경우가 아님에도 불구하고 민감정보인 종교 정보를 별도 동의를 받지 않고 처리한 행위는 보호법 제23조제1항을 위반한 것이다.

다. 법령 등의 근거 없이 주민등록번호를 처리한 행위{보호법 제24조의2(주민등록번호 처리의 제한)제1항}

피심인이 법령 등에서 주민등록번호의 처리를 요구하거나 허용한 경우 등이 아님에도 불구하고 주민등록번호가 포함된 인증서류를 수집·저장한 행위는 보호법 제24조의2제1항을 위반한 것이다.

라. 안전성 확보에 필요한 조치를 하지 않은 행위{보호법 제29조(안전조치의무)}

피심인이 AWS를 이용하면서 추가 인증수단을 적용하지 않고, 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하지 않고, 일부 AWS S3에 대한 접근통제를 공개로 설정하여 운영한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항 제2호, 고시 제4조제4항·제5항·제9항을 위반한 것이다.

피심인이 접속기록을 1년 이상 보존·관리하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제3호, 고시 제5조제1항을 위반한 것이다.

피심인이 주민등록번호가 포함된 인증서류를 수집한 후 주민등록번호를 암호화하지 않고 저장한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제4호, 고시 제6조제2항을 위반한 것이다.

마. 유출 통지를 하지 않은 행위{보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항}

피심인이 유출된 개인정보 항목, 유출이 발생한 시점, 이용자가 취할 수 있는 조치 등을 이용자에게 알리지 않은 행위는 보호법 제39조의4제1항을 위반한 것이다.

바. 1년 이상 미이용자의 개인정보를 파기 등을 하지 않은 행위{보호법 제39조의6(개인정보의 파기에 대한 특례)제1항}

피심인이 1년 이상 정보통신서비스를 이용하지 않은 이용자의 개인정보를 파기하거나, 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 행위는 보호법 제39조의6제1항, 같은 법 시행령 제48조의5제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보의 파기 위반	보호법 §21①	-	・불필요하게 된 개인정보를 파기하지 않은 행위
민감정보의 처리 제한 위반	보호법 §23①	-	・민감정보 처리에 대한 별도 동의를 받지 않은 행위
주민등록번호 처리의 제한 위반	보호법 §24의2①	-	・법령 등의 근거 없이 주민등록번호 처리한 행위

안전조치의무 위반	보호법 §29	§48의2① 제2호·제3호·제4호	• 외부에서 개인정보처리시스템에 접속 시 안전한 인증수단을 적용하지 않은 행위(고시§4④) • 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하지 않은 행위(고시§4⑤) • 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위(고시§4⑨) • 개인정보취급자의 개인정보처리시스템의 접속기록을 보관 및 점검을 하지 않은 행위(고시§5①) • 주민등록번호를 안전한 암호알고리듬으로 암호화하여 저장하지 아니한 행위(§6②)
개인정보 유출등의 통지·신고에 대한 특례 위반	보호법 §39의4	-	• 유출 통지를 하지 않은 행위
개인정보의 파기에 대한 특례 위반	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 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.

나. 피심인은 법령에서 민감정보의 처리를 요구하거나 허용하는 경우 또는 이용자에게 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우가 아니면 민감정보를 처리하지 아니하여야 한다.

다. 피심인은 법령 등에서 주민등록번호의 처리를 요구하거나 허용한 경우 등을 제외하고는 이용자의 주민등록번호를 처리하지 아니하여야 한다.

라. 피심인은 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

1) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.

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

3) 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.

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

5) 주민등록번호에 대해서는 안전한 암호알고리듬으로 암호화하여 저장하여야 한다.

마. 피심인은 개인정보의 유출 사실을 안 때에는 지체 없이 유출된 개인정보 항목, 유출이 발생한 시점, 이용자가 취할 수 있는 조치, 정보통신서비스 제공자 등의 대응 조치, 이용자가 상담 등을 접수할 수 있는 부서 및 연락처 등을 해당 이용자에게 알려야 한다.

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

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

2. 과징금 부과

피심인의 보호법 제23조(민감정보의 처리 제한)제1항 및 제29조(안전조치의무) 위반행위에 대해 같은 법 제39조의15제1항제3호·제5호, 같은 법 시행령 제48조의11 제1항·제3항, [별표 1의5] '과징금의 산정기준과 산정절차' 및 '개인정보보호 법규 위반에 대한 과징금 부과기준'(개인정보보호위원회 고시 제2020-6호, 이하 '과징금 부과기준')에 따라 다음과 같이 과징금을 부과한다.

가. 과징금 상한액

피심인의 위반행위에 대한 과징금 상한액은 보호법 제39조의15제1항, 같은 법 시행령 제48조의11제1항에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도의 연평균 매출액(다만, 해당 사업연도 첫날 현재 사업을 개시한지 3년이 되지 않은 경우에는 그 사업개시일부터 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액)의 100분의 3이하에 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.

피심인은 영리를 목적으로 정보통신망을 통해 정보통신서비스를 제공하는 자이며 보호법 시행령 제48조의2에 따른 안전성 확보조치를 이행하지 않은 사실이 있으므로 피심인에게 고의 또는 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 제공자 등이 위반행위로 인해 직접적으로 이득을 취하지 않은 경우(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자 등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ▲이용자의 개인정보가 공중에 노출되지 않은 경우(제3호)' 중 모두에 해당하는 경우에는 보통 위반행위로, 1개 이상 2개 이하에 해당하는 경우에는 중대한 위반행위로 감경한다."라고 규정하고 있다.

피심인에게 고의 또는 중과실이 있으며, 과징금 부과기준 제5조제3항 단서 각 호에 해당하는 사유가 없으므로 위반행위의 중대성을 매우 중대한 위반행위로 판단한다.

3) 기준금액의 산출

서비스의 사업개시일로부터 직전 사업연도 말일까지의 연평균 매출액 천원에 부과기준율 1천분의 27을 곱하여 기준금액을 천원으로 한다.

< 피심인의 위반행위 관련 매출액 > (단위 : 천원)

구 분	2018년	2019년	2020년	평 균
매출액				

<보호법 시행령 [별표 1] 2. 가. 1)에 따른 과징금 부과기준율>

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

다. 필수적 가중 및 감경

피심인이 '민감정보 처리에 대한 별도 동의를 받지 않은 행위('18. 11. 12. ~ '22. 2. 3.)'와 '이용자의 개인정보를 유출한 경우로서 안전성 확보에 필요한 조치를 하지 않은 행위('18. 11. 12. ~ '21. 12. 6.)'의 위반기간이 2년을 초과하므로 과징금 부과기준 제6조 및 제7조에 따라 기준금액의 100분의 50인을 천원을 가산하고, 최근 3년간 보호법에 의한 과징금 처분을 받은 적이 없으므로 기준금액의 100분의 50인 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.

가중 사유는 없으며, 개인정보 유출 사실을 자진 신고한 점, 조사에 적극 협력한 점을 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 천원을 감경한다.

마. 과징금의 결정

피심인의 보호법 제23조(민감정보의 처리 제한)제1항 및 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15제1항제3호·제5호, 같은 법 시행령 제48조의11제1항·제4항, [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 1) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 천원을 최종 과징금으로 결정한다.

< 위반행위별 과징금 산출내역 > (단위 : 천원)

위반행위	기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금
민감정보 처리에 대한 별도 동의를 받지 않은 행위				
이용자의 개인정보를 유출한 경우로서 안전성 확보에 필요한 조치를 하지 않은 행위				

3. 과태료 부과

피심인의 보호법 제21조(개인정보의 파기)제1항, 제24조의2(주민등록번호 처리의 제한)제1항, 제29조(안전조치의무), 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항 및 제39조의6(개인정보의 파기에 대한 특례)제1항을 위반한 행위에 대하여 같은 법 제75조(과태료) 제75조제2항제4호·제4호의2·제6호·제12호의3 및 같은 법 시행령 제63조 및 [별표2] '과태료의 부과기준' 및 '개인정보 보호법 위반에 대한 과태료 부과기준'(2021. 1. 27. 개인정보보호위원회 의결, 이하 '과태료 부과지침')에 따라 다음과 같이 과태료를 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 각 위반행위별 기준 금액을 600만원으로 산정한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

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
차. 법 제24조의2제1항을 위반하여 주민등록번호를 처리한 경우	법 제75조 제2항제4호의2	600	1,200	2,400
도. 법 제39조의4제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·보호위원회 및 전문기관에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 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, ① 탈퇴한 이용자의 개인정보를 파기 하지 아니한 행위, ② 법령 등의 근거 없이 주민등록번호를 처리한 행위, ③ 안전성 확보에 필요한 조치를 하지 않은 행위, ④ 유출 통지를 하지 않은 행위, ⑤ 1년 이상 서비스 미사용자 개인정보의 파기 등을 하지 않은 행위의 각 위반기간이 3개월 이상이므로 10%를 각 가중하며, 각 위반행위 중 '안전성 확보에 필요한 조치를 하지 않은 행위'는 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 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 과태료의 사전통지 및 의견제출 기간 내에 법규 위반행위에 대하여 시정을 완료하거나 시정 중에 있는 것으로 인정되는 점, 일관되게 행위 사실을 인정하면서 위법성 판단에 도움되는 자료 제출 또는 진술 등 조사에 적극적으로 협력한 점, 「중소기업기본법」 제2조에 따른 소기업인 점을 고려하여 과태료 부과지침 제7조에 따라 기준금액의 50%를 각각 감경한다.

다. 최종 과태료

피심인의 보호법 제21조제1항, 제24조의2제1항, 제29조, 제39조의4제1항, 제39조의6제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,860만원의 과태료를 부과한다.

< 위반행위별 과태료 산출내역 > (단위 : 만원)

위반 조항	위반내용	기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) =(A+B+C)
법 §21①	탈퇴한 이용자의 개인정보 미파기	600	60	△300	**360**
법 §24의2①	법령 등의 근거 없이 주민등록번호를 처리한 행위	600	60	△300	**360**
법 §29	안전성 확보에 필요한 조치를 하지 않은 행위	600	120	△300	**420**
법 §39의4①	유출 통지를 하지 않은 행위	600	60	△300	**360**
법 §39의6①	1년 이상 서비스 미사용자 개인정보의 파기등을 하지 않은 행위	600	60	△300	**360**
계					**1,860**

4. 고발

피심인이 보호법 제21조제1항을 위반하여 탈퇴한 이용자의 개인정보를 파기하지 않은 행위, 제23조제1항을 위반하여 민감정보 처리에 대한 별도 동의를 받지 않은 행위 및 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 유출당한 행위는 보호법 제71조 또는 제73조의 벌칙에 해당되며, 고발기준 제3조제2항제3호에 해당하므로 보호법 제65조제1항에 따라 피심인을 수사기관에 고발한다.

5. 결과 공표

보호법 제66조제1항 및 '개인정보보호위원회 처분결과 공표기준'(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따르면 피심인의 위반행위는 보호법 제75조제2항 각 호에 해당하는 위반행위 2개 이상 한 경우(제4호), 위반행위 기간이 6개월 이상 지속된 경우(제5호) 및 개인정보 침해사고 피해자 수 10만 명 이상인 경우(제7호)에 해당하므로 보호법 제66조제1항에 따라 피심인이 시정조치 명령을 받은 사실과 고발, 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표				
위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	위반조항	위반내용	처분일자	처분내용
	법 제21조제1항	개인정보 미파기	2022.2.23	시정조치 명령 과태료 부과 360만원 고발
	법 제23조제1항	민감정보 처리 위반	2022.2.23	시정조치 명령 고발
	법 제24조의2제1항	주민등록번호 처리 위반	2022.2.23	시정조치 명령 과태료 부과 360만원
	법 제29조	안전조치의무 위반	2022.2.23	시정조치 명령 과태료 부과 420만원 고발
	법 제39조의4제1항	유출 통지 미이행	2022.2.23	시정조치 명령 과태료 부과 360만원
	법 제39조의6제1항	유효기간제 위반	2022.2.23	시정조치 명령 과태료 부과 360만원

Ⅴ. 결론

피심인의 보호법 제21조(개인정보의 파기)제1항, 제23조(민감정보의 처리 제한) 제1항, 제24조의2(주민등록번호 처리의 제한)제1항, 제29조(안전조치의무), 제39조의4 (개인정보 유출등의 통지·신고에 대한 특례)제1항 및 제39조의6(개인정보의 파기에 대한 특례)제1항을 위반한 행위에 대하여 같은 법 제39조의15(과징금 부과 등)제1항 제3호·제5호, 제75조(과태료)제2항제4호·제4호의2·제6호·제12호의3, 제65조(고발 및 징계권고)제1항, 제64조(시정조치 등)제1항 및 제66조(결과의 공표)제1항에 따라 과징금·과태료, 고발, 시정조치 명령 및 결과 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.

이상과 같은 이유로 주문과 같이 의결한다.

2022년 02월 23일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 홍 열 (서 명)

위 원 이 희 정 (서 명)

위 원 지 성 우 (서 명)