

I. 기초 사실

피심인은 교육 서비스업을 운영하는 사업자로 영리를 목적으로 정보통신망을 통해 웹사이트에서 강의 영상공유 등 서비스를 제공하고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조 제1항 제3호에 따른 정보통신서비스 제공자이며, 舊 「개인정보 보호법」¹⁾(이하 '舊 보호법'이라 한다)에 따른 개인정보처리자로서 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

II. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 2023년 7월 29일 개인정보 포털(privacy.go.kr)에 유출 신고한 피심인에 대하여 2023년 7월 31일부터 2024년 1월 22일까지 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 입시설명회 및 강의 영상공유 등 서비스 제공을 위해 홈페이지()를 운영하면서, 2023년 8월 16일 기준 이용자 명의 개인정보를 수집하여 보관하고 있다.

1) 舊 개인정보 보호법(법률 제16930호, 2020. 2. 4. 일부개정, 2020. 8. 5. 시행)

< 개인정보 수집현황 >

구 분	항 목	기 간	건 수(건)

* 피심인은 '23. 12. 23.에 사고 당시 보유 중이던 DB 데이터를 삭제함

※ 전체 단과 수강생의 개인정보는 '21.1.1.부터 별도 DB에 총 건 수집·보관 중

나. 개인정보 유출 관련 사실관계

피심인은 학원생²⁾ 및 설명회 신청자의 개인정보를 수집하여 사이트의 회원으로 성명과 휴대전화번호의 조합의 계정을 생성³⁾하여 회원정보DB를 구축하였고, 해당 DB에는 2020년 2월 24일부터 2023년 12월 22일 사이에 피심인의 웹사이트에 계정이 생성된 학원생의 개인정보가 포함되어 있었다.

이용자별 영상 접근권한을 부여하기 위하여 운영 중인 사이트의 특정 경로⁴⁾에 성명과 휴대전화번호 일부가 포함된 ID목록 파일(엑셀)을 업로드하였으나, 해커가 무단 접근하여 해당 파일을 다운로드하고 이용자 페이지에서 성명과 무작위 휴대전화번호를 대입하는 로그인 시도 및 인증번호 입력⁵⁾을 통해 이용자의 개인정보 15,143건을 유출(' 23.7.15~16.)하였다.

1) 유출 규모 및 항목

2023년 8월 16일 자료제출일 기준 피심인이 보유한 이용자 명 중 15,143명의 성명, 휴대전화번호 등 개인정보가 유출되었다.

유출 항목	정보주체 수
성명, 휴대전화번호 일부	15,143명
성명, 휴대전화번호 전부	719명
합계	15,143명

2) 를 이용하는 강사의 수강생

3) ID(성명+휴대전화번호 뒤4자리), PW(휴대전화번호 11자리, 초기비밀번호 변경 필수 아님)

4) 교육 영상별 시청 가능 학원생 등록을 위해 엑셀 파일 업로드(<https://>)

5) 피심인은 인증번호가 휴대전화번호만 아니라 브라우저의 응답 값으로도 전송하여 해커가 탈취 가능하였음

2) 유출 인지 및 대응

일 시	유출 인지 및 대응 내용	비고
7. 15 ~ 16.	해커가 시스템 내 취약점을 이용하여 성명 엑셀파일을 다운로드	
7. 17.	피심인 메일로 개인정보 유출 의심 신고 접수	
7. 17 ~ 21.	신고 메일 내 캡처된 5개 계정 정보 확인 및 시스템 로그 분석, 조치	인지 ^(1차)
7. 19 ~ 22.	유출 확인된 5명에 대하여 유선 통지	통지 ^(1차)
7. 25.	성명, 전화번호 모두 유출된 대상자 확인(719명)	인지 ^(2차)
7. 28.	성명만 유출된 대상자 확인(14,424명)	인지 ^(3차)
7. 29.	개인정보 유출신고, 사이버수사대 수사의뢰 및 신고, 홈페이지 고지 및 SMS통지	신고·통지

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 이용자에게 영상 시청권한을 부여하기 위하여 성명 및 휴대전화번호(일부)가 포함된 엑셀파일을 웹사이트 특정 경로에 업로드하면서, 해당 파일 및 경로에 대한 인증 및 접근통제 등의 보호조치를 하지 않아 누구나 접근이 가능한 상태로 공개되어 있었다.

이용자 페이지에서 전체 이용자의 약 87배 및 평소 분당 로그인 횟수의 약 39배에 달하는 대량의 로그인 시도 행위⁶⁾가 발생하였으나 불법적인 접근에 대응하여 비정상적인 시스템 접속 시도를 탐지·차단하는 등의 조치를 하지 아니하였다.

이로 인해 실제 해커는 개인정보가 포함된 엑셀 파일에 외부에서 접근하여 이를 다운로드한 후, 탈취한 개인정보를 바탕으로 대량의 로그인 시도를 하였으나, 피심인은 외부 신고자가 메일로 유출 의심 신고를 하기 전까지 이러한 사실을 알지 못하였다.

6) 전체 이용자(명)의 87배에 달하는 대량의 로그인 시도(건 이상) 및 실패(99.9%)가 발생

또한, 외부에서 관리자 페이지에 접속할 때에 안전한 인증 수단이 적용되지 않은 사실이 있다.

※ 엑셀파일 업로드 시 즉시삭제 로직 도입('23.7.28.), 해외 IP 및 공격 IP 차단('23.8.10.), 로그인 임계치 적용('23.7.31.), SMS 인증 오류 개선('23.7.31.), 관리자 SMS인증 도입('23.9.1.)

나. 개인정보 유출통지·신고를 소홀히 한 행위

피심인은 2023년 7월 17일 17시 10분에 유출 의심 신고 접수 메일 내 계정이 피심인 서비스 회원임을 확인^(1차)하였고, 2023년 7월 18일 9시 40분에는 의심 IP 차단 및 계정에 대한 접근 차단 등 보호조치를 하였으나, 2023년 7월 19일 13시에 해당 사실을 이용자에게 통지^(1차)하기 시작하였고,

2023년 7월 25일 18시에 추가 유출 대상자 확인^(2차)을 하였으나, 2023년 7월 29일 9시 58분에 개인정보 포털에 해당 사실을 신고하였으며 2023년 7월 29일 17시 50분에 이용자에게 통지하였다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2024년 1월 26일 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2024년 2월 14일 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 舊 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 시행령⁷⁾(이하 ‘舊 시행령’이라 한다) 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위해 ‘개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영^(나목)’, ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치^(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

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

舊 「개인정보의 기술적·관리적 보호조치 기준」⁸⁾(이하 ‘舊 기술적 보호조치 기준’이라 한다) 제4조제4항은 “정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.”라고 규정하고 있고, 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한^(제1호)’, ‘개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지^(제2호)’하는 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있으며, 제4조제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다”라고 규정하고 있다.

舊 기술적 보호조치 기준 해설서는 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 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등에 관한 보호조치를 하여야 한다.”라고 해설하고 있다.

7) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2022. 10. 20. 시행

8) 舊 「개인정보의 기술적·관리적 보호조치 기준」(2023. 9. 22. 개인정보보호위원회고시 제2023-7호로 폐지)

나. 舊 보호법 제39조의4제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출 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.

舊 시행령 제48조의4제2항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제39조의4제1항 각 호의 모든 사항을 서면등의 방법으로 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고해야 한다.”라고 규정하며, 제3항은 “정보통신서비스 제공자등은 제2항에 따른 통지·신고를 하려는 경우에는 법 제39조의4제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 안전조치 의무를 소홀히 한 사실

[舊 보호법 제29조(안전조치의무)]

피심인이 웹사이트를 통하여 강의 영상공유 등 서비스를 제공하면서 로그인을 성명과 휴대전화번호로 하도록 구성하였으나, 전체 이용자 수의 약 87배 및 평소 분당 로그인 횟수의 약 39배에 달하는 대량의 로그인 시도(건 이상) 및 실패(99.9%)가 발생했음에도 비정상적인 접속 시도를 탐지·차단하는 등의 조치를 하지 않은 행위는 舊 보호법 제29조, 舊 시행령 제30조 제1항, 舊 기술적 보호조치 기준 제4조 제5항을 위반한 것이다.

피심인이 이용자에게 영상 시청권한을 부여하기 위하여 외부에서 접근이 가능한 웹사이트 특정 경로에 개인정보가 포함된 파일을 업로드하면서 해당 경로에 어떠한 접근

통제 조치도 하지 않아 누구나 다운로드할 수 있도록 허용한 행위는 舊 보호법 제29조, 舊 시행령 제30조제1항, 舊 기술적 보호조치 기준 제4조제9항을 위반한 것이다.

피심인이 외부에서 관리자 페이지로 접속하여 교육 영상별 시청가능 이용자의 성명 및 휴대전화번호 일부가 포함된 엑셀 파일을 업로드하는 과정에 안전한 인증 수단을 적용하지 않은 행위는 舊 보호법 제29조, 舊 시행령 제30조제1항, 舊 기술적 보호조치 기준 제4조제4항을 위반한 것이다.

나. 개인정보 유출통지·신고를 소홀히 한 행위

[舊 보호법 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항)]

피심인은 2023년 7월 17일 16시 31분에 외부 신고자로부터 개인정보 유출 의심 내용이 포함된 메일을 수신하였고, 17시 10분에 유출된 개인정보가 서비스 내 등록된 회원의 정보임을 확인하였다.

따라서 피심인은 적어도 2023년 7월 17일 17시 10분에는 개인정보의 유출 사실을 확인한 것으로 판단되나, 24시간을 경과하여 2023년 7월 19일 13시부터 해당 사실을 이용자에게 통지하기 시작하였고, 2023년 7월 29일 09시 58분에 개인정보 포털에 해당 사실을 신고하였다.

따라서 피심인이 24시간을 경과하여 개인정보 유출 사실을 통지하고, 신고한 행위는 舊 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	舊 시행령	세부내용(고시 등)
안전조치의무	舊 보호법 §29	§48의2① 제2호	<ul style="list-style-type: none">개인정보취급자가 정보통신망을 통해 외부에서 개인정보 처리시스템에 접속이 필요한 경우 안전한 인증 수단 미적용(舊 기술적 보호조치 기준§4④)불법적인 접근 및 침해사고 방지를 위한 개인정보 처리시스템에 대한 침입 탐지·차단 시스템 미운영(舊 기술적 보호조치 기준§4⑤)처리중인 개인정보가 인터넷 홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터 등에 미조치(舊 기술적 보호조치 기준§4⑨)
개인정보유출 등의 통지·신고에 대한 특례	舊 보호법 §39의4①	§48조의4	<ul style="list-style-type: none">정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 유출 신고 및 통지한 행위

IV. 피심인의 주장에 대한 검토

1. 개인정보 유출 및 안전조치의무 위반에 대하여

가. 피심인 주장

피심인은 이 사건 개인정보 유출사고가 발생한 서비스를 통하여 개인정보를 수집하지 아니하였고, 오프라인 강의의 부수적·보조적 수단으로 운영하여 舊 보호법상 정보통신서비스 제공자에 해당하지 않아 제39조의4제1항에 따른 24시간 이내 유출 통지·신고의무와 제39조의15제1항제5호에 따른 과징금 부담의 책임을 지지 않는다고 주장한다.

나. 검토의견: 불수용

피심인은 교육 서비스를 제공하기 위해 현장 강의와 구분하여 웹사이트를 개설하고 강의 영상 등을 게시·공유하여 정보통신망을 통해 정보를 제공하였으며, 수강생의 개인정보를 이용하여 회원 계정을 생성하여 지급하고,

수강생은 영상을 시청하는 등 서비스를 이용하여 정보통신서비스 이용관계가 성립하므로 피심인은 舊 보호법상 정보통신서비스 제공자에 해당하여 제39조의4제1항에 따른 24시간 이내 유출 통지·신고의무와 제39조의15제1항제5호에 따른 과징금 부담의 책임을 진다.

2. 과징금·과태료 산정에 대하여

가. 피심인 주장

피심인은 를 통하여 매출이 발생하지 않아 본건 위반행위는 매출액이 없는 경우에 해당하여 정액과징금 대상이라고 주장하며, 최근 3년간 법 제39조의15제1항 각 호에 해당하는 행위로 과징금 처분을 받은 적이 없는 경우로 최초 위반행위인 점 및 조사 적극 협력 등 감경을 요청하고,

과태료 산정과 관련하여, 정보주체에게 피해가 발생하지 않았으며 조사협조 및 자진시정 등 감경을 요청하였다.

나. 검토의견: 일부수용

피심인의 위반행위가 발생한 정보통신서비스는 과금체계가 없는 등 매출이 있다고 보기 어려우므로, 정액과징금 대상이라는 주장은 수용한다.

다만, 피심인은 위원회 자료제출 요구에 대해 회신하였으나 일부 누락된 자료가 있어 수차례 자료제출 요구가 이루어지는 등 성실하고 충실한 답변 및 조사에 협조하였다고 보기 어려우므로, 조사에 적극 협력하였다는 피심인의 주장을 수용하지 않는다.

V. 시정조치

1. 과징금 부과

피심인의 舊 보호법 제29조(안전조치의무) 위반에 대한 과징금은 같은 법 제39조의 15제1항제5호, 舊 시행령 제48조의11제1항, 제2항, 및 제4항, [별표 1의5] ‘과징금의 산정 기준과 산정절차’ 및 舊 「개인정보보호 법규 위반에 대한 과징금 부과기준」⁹⁾(이하 ‘舊 과징금 부과기준’이라 한다)에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 舊 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제39조의15, 舊 시행령 제48조의11에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업 연도 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 4억원 이하의 과징금을 부과할 수 있다.

9) 개인정보보호위원회 고시 제2022-3호, 2022. 10. 20. 시행

나. 기준금액

1) 고의·중과실 여부

舊 과징금 부과기준 제5조제1항은, 舊 시행령 [별표 1의5] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 舊 시행령 제48조의 2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

이에 따라, 舊 보호법 제29조(안전조치의무), 舊 시행령 제48조의2(개인정보의 안전성 확보 조치에 관한 특례)를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

舊 과징금 부과기준 제5조제3항은, 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 ‘매우 중대한 위반행위’로 판단하도록 규정하고 있다. 다만, 舊 과징금 부과기준 제5조제3항 단서에서 위반행위의 결과가 ▲위반 정보통신서비스 제공자등이 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우^(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우^(제2호), ▲이용자의 개인정보가 공중에 노출되지 않은 경우^(제3호) 중 모두에 해당하는 경우 ‘보통 위반행위’로, 1개 이상 2개 이하에 해당하는 경우 ‘중대한 위반행위’로 감경하도록 규정하고 있다.

피심인의 경우, 안전조치 의무 위반으로 인해 ‘직접적으로 이득을 취하지 않은 경우^(제1호)’에 해당하나, 해킹으로 인해 유출피해 규모가 보유한 이용자 명 중 15,143명(%)으로 ‘피해규모가 100분의 5 이내인 경우^(제2호)’, ‘이용자의 개인정보가 공중에 노출되지 않은 경우^(제3호)’에 해당하지 아니하여 ‘중대한 위반행위’로 판단한다.

3) 기준금액 산출

피심인의 개인정보가 유출된 홈페이지는 매출이 별도로 발생하지 않아 舊 시행령

[별표 1의5] 2. 가. 2)에 따른 '중대한 위반행위'의 부과 기준금액을 적용하여 기준금액을 280,000천원으로 한다.

다. 필수적 가중 및 감경

舊 과징금 부과기준 제6조제1항에 따라 위반기간이 2년을 초과하는 경우에 대하여 기준금액의 100분의 50에 해당하는 140,000천원을 가중한다.

舊 과징금 부과기준 제6조제2항에 따라 최근 3년 이내 舊 보호법 제39조의15 제1항 각 호에 해당하는 행위로 과징금 처분을 받은 적이 없으므로 기준금액의 100분의 50에 해당하는 140,000천원을 감경한다.

라. 추가적 가중 및 감경

舊 과징금 부과기준 제8조는 사업자의 위반행위의 주도 여부, 조사 협력 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있으며, 피심인의 경우 해당사항이 없어 추가적 가중·감경을 적용하지 아니한다.

마. 과징금의 결정

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15제1항제5호, 舊 시행령 제48조의11, [별표 1의5] 2. 가. 1)(과징금의 산정 기준과 산정절차) 및 舊 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액인 280,000천원을 최종 과징금으로 결정한다.

<과징금 산출 내역>

①기준금액	②필수적 가중·감경	③추가적 가중·감경	④최종과징금
<ul style="list-style-type: none"> •직전 3개 사업연도 연평균 매출액(없음) •기준금액 2억 8천만원 적용 (중대한위반*) 	<ul style="list-style-type: none"> •장기위반으로 50% 가중 (140,000천 원) •최초위반으로 50% 감경 (140,000천 원) 	-	280,000천 원
⇒ 280,000천 원	⇒ 280,000천 원	⇒ 280,000천 원	

* 중대한위반 : ▲위반행위로 직접 이득을 취하지 않은 경우(해당), ▲유출피해 규모가 보유하고 있는 개인정보의 5% 이내인 경우(32.3%로 미해당), ▲개인정보가 공중에 노출되지 않은 경우(미해당)
→ 1개 이상 2개 이하에 해당

3. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항 위반행위에 대한 과태료는 같은 법 제75조제2항제6호·제12호의3, 舊 시행령 제63조, 舊 시행령 [별표2] ‘과태료의 부과기준’ 및 舊 개인정보 보호법 위반에 대한 과태료 부과기준¹⁰⁾(이하 ‘舊 과태료 부과기준’이라 한다)에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

舊 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 기준금액을 600만원으로 산정한다.

< 舊 시행령 [별표2] 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
도. 법 제39조의4제1항(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) 舊 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.

10) 개인정보보호위원회지침, 2023. 3. 8. 시행

피심인의 경우, 舊 과태료 부과기준 제8조 및 [별표2] 과태료의 가중기준에 따라 舊 보호법 제29조(안전조치의무) 위반행위는 '법 위반상태의 기간이 3개월 이상인 경우'에 해당하여 기준금액의 10%를 가중하고, 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항 위반행위는 '제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상에 해당하는 경우'에 해당하여 기준금액의 10%를 가중한다.

2) (과태료의 감경) 舊 과태료 부과지침 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경 기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력 정도, ▲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, 舊 과태료 부과기준 제7조 및 [별표1] 과태료의 감경기준에 따라 舊 보호법 제29조(안전조치의무) 위반행위는 '과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우'에 해당하여 기준 금액의 50%를 감경하고, 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항 위반행위는 감경하지 아니한다.

다. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 1,020만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제)	600만 원	60만 원	300만 원	360만 원
개인정보 유출등의 통지·신고에 대한 특례	600만 원	60만 원	-	660만 원
계				1,020만 원

4. 결과 공표

舊 보호법 제66조제1항 및 舊 「개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 ‘법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우^(제4호)’, ‘위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우^(제5호)’에 해당하므로 舊 보호법 제66조제1항에 따라 피심인이 과태료 부과를 받은 사실을 개인정보보호위원회 홈페이지에 공표한다.

다만, 개정된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」(2023. 10. 11. 시행)에 따라 공표 기간은 1년으로 한다.¹¹⁾

개인정보 보호법 위반 행정처분 결과 공표					
개인정보 보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위 반내용	처분일자	처분내용
1		舊 보호법* 제29조	안전 조치의무 (접근통제)	2024. 3. 27.	과태료 부과 360만 원
		舊 보호법 제39조의4 제1항	개 인 정보 유출등의 통지·신고에 대한 특례	2024. 3. 27.	과태료 부과 660만 원
* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호					
2024년 3월 27일					
개 인 정 보 보 호 위 원 회					

11) 피심인에게 유리하게 변경된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침(2023.10.11 시행)」에 따라 공표기간 1년을 소급 적용