개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2023-016-203호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

(사업자등록번호 :)

피 심 인

대표자

의결연월일 2023. 10. 11.

주 문

1. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

   가. 과 징 금 : 57,500,000원

   나. 과 태 료 : 7,200,000원

   다. 납부기한 : 고지서에 명시된 납부기한 이내

   라. 납부장소 : 한국은행 국고수납 대리점

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

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법[1]」(이하 "舊보호법"이라 한다.) 제2조제6호에 따른 공공기관으로, 같은 법 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

피심인명	사업자등록번호	대표자 성명	주소	직원 수

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 유출 신고('22. 11. 7.)가 접수되어 개인정보 관리실태에 대한 조사('22. 11. 7. ~ '23. 6. 19.)를 실시하였으며, 피심인의 舊보호법규 위반행위와 관련된 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 학사 관리 등을 위해 '22. 12. 14. 기준 아래와 같이 개인정보를 수집·보관하고 있다.

1) 개정된 보호법 시행(2023.9.15.) 이전에 위반행위가 종료된 경우로서 舊개인정보 보호법[법률 제16930호]을 적용

개인정보파일 (시스템명)	수집·이용 항목	수집일	보유건수
학사 정보 (舊인증지원시스템 / 기관 홈페이지 통합구축시스템)	(필수) (선택)	'09.7월~ 현재	
연구행정 사용자관리 (통합연구행정 지원시스템)	(필수) (선택)	'11.3.20.~ 현재	
입학전형 지원자 (입학정보시스템 / 학년도 입학사정관 종합평가시스템)	(필수) (선택)	'14.1.1.~ 현재	

나. 개인정보 유출 관련 사실관계

1) 유출 규모 및 항목

'舊인증지원시스템' 등 5개 시스템에서 재학생·졸업생·교직원 700,054건의 개인정보가 유출되었고, 유출된 정보 중에 ' 학년도 입학사정관 종합평가 시스템'에 보관하던 주민등록번호 11,099건도 포함된 사실을 확인하였으며, 세부 유출 규모 및 항목은 다음과 같다.

개인정보파일 (시스템명)	유출 항목	유출 규모
학생생활부( ) (舊인증지원시스템)	성명, 소속학과, 학번, 성별, 출신고교·졸업연월, 입학 구분, 주소, 전화번호, 이메일, 증명사진, 군필여부, 보호자 주소, 보호자 연락처, 장학금 수여정보 등	143,234건
구 통합정보시스템 학생정보 (기관홈페이지 통합구축시스템)	성명, 생년월일, 비밀번호 등	258,208건
산학협력단 연구자정보 (통합연구행정 지원시스템)	성명, 로그인아이디, 휴대폰번호, 직장연락처, 이메일, 주소(집), 소속, 직급, KRI연구자번호	286,545건
학년도 수시모집 서류평가 대상자 (학년도 입학사정관 종합평가시스템)	주민등록번호, 수험번호, 졸업(예정)연월, 지원학과, 출신고교, 전형구분, 성적 등	11,099건
년도 수시 입학원서 (입학정보시스템)	성명, 생년월일, 수험번호, 휴대폰번호, 이메일, 주소(집), 추가 연락처, 출신고교·졸업연월, 사진 등	968건

2) 유출 인지 및 대응

일시		피심인의 유출 인지·대응 내용
2021.	8.19.	학생들이 파라미터 변조 방식으로 '舊인증지원시스템' 최초 무단 접속
2022.	11. 1.	정기점검 중 이상 접속행위 발견 / IP를 통해 접속한 재학생 2명 특정
	11. 4.	입학정보시스템 BIO 인증 차단
	11. 5.	해당 학생의 노트북에 보관하던 개인정보 파일 회수, **유출 사실 최초 인지**
	11. 7.	개인정보위·한국인터넷진흥원에 개인정보 **유출 신고**
		통합연구행정지원시스템 파라미터 변조 취약점 제거
	11. 8.	학년도 입학사정관 종합평가시스템 서버 중지, admin 및 test 계정 삭제
	11. 9.	교육부 1차 현장 점검(~11.10.) / 파라미터 변조 취약점 제거 및 접근 권한 보안 강화
	11.10.	대표 홈페이지 및 산학협력단 홈페이지에 유출 사실 게재
	11.14.	포털 및 시스템 사용자 비밀번호 강제 변경 조치
	11.17.	정보주체에게 **유출 통지**(문자, 이메일)
	11.22.	입학정보시스템 SSO 제조사 취약점 제거
	12. 7.	교육부 2차 현장 점검(~12.9.)
	12. 8.	교육부 현장 점검시 **추가 유출 사실 인지**(舊인증지원시스템)
	12. 9.	이메일 인증 절차 도입 등 비밀번호 변경 취약점 제거
	12.12.	개인정보위·한국인터넷진흥원에 개인정보 **추가 유출 신고**
		추가 유출 통지 / 대표 홈페이지에 추가 유출 사실 게재

3) 유출 경위

피심인 소속 학생 2명(보안 동아리 소속, 이하 '학생들')이 보안 취약점을 점검한다는 명분으로 '21. 8월부터 '22. 10월까지 자택·기숙사·동아리방 등에서 피심인의 업무시스템 및 웹사이트를 탐색하였고, ① 파라미터 변조, ② 웹셸 업로드, ③ 관리자페이지 취약점 이용 등 방법으로 개인정보처리시스템에 무단으로 접속하여 데이터를 다운로드함으로써 개인정보가 유출된 것으로, 세부 유출 경위는 아래 표와 같다.

시스템명	세부 유출 경위	접근 유형
舊 인증지원 시스템	• '21. 8. 19. 학생들이 파라미터를 변조하여 년~ 학년도 학번을 차례로 대입하여 접속함으로써 성적표, 장학금, 시간표 등 정보를 열람하고 이를 자신의 컴퓨터에 내려받아 저장 • '22. 3. 8. 학생들이 학내에서 시스템의 학생생활부 메뉴를 파라미터 변조 공격하여 학생생활부 정보와 사진 파일을 다운로드	파라미터 변조

시스템명	세부 유출 경위	접근 유형
기관홈페이지 통합구축 시스템	• '22. 2. 23. 학생들이 자택 등에서 특정 소스코드( )에서 파일 다운로드 취약점을 발견 • '22. 6. 8. ~ 6. 9. 학생들이 다운로드 취약점을 이용하여 웹사이트 관리 솔루션의 주요 소스코드를 다운로드, DB접속정보 및 파일 업로드 취약점 발견 • '22. 6. 9. ~ 8. 3. 학생들이 자택 등에서 파일 업로드 취약점을 이용하여 웹셸 업로드, 원격코드( )를 실행하여 시스템 DB의 모든 테이블 정보와 컬럼명을 획득하고, 학사계정으로 접속하여 학생 개인정보 탈취	웹셸 공격
통합연구행정 지원시스템	• '22. 3. 21. 학생들이 기숙사에서 시스템 ' ' 메뉴의 ' '를 파라미터 변조 공격하여 산학협력단의 연구자 정보를 탈취	파라미터 변조
학년도 입학사정관 종합평가 시스템	• '22. 10월 학년도 수시모집 서류평가 관리자페이지( ) 접속*, 다양한 패스워드 조합을 시도하여 비밀번호('1', 숫자 한 자리)를 알아낸 뒤 관리자 계정으로 로그인에 성공 * (대학원서 접수회사)가 개발한 시스템으로 년 이후 사용하지 않았으나, 학생들은 Censys 검색엔진을 통해 동 시스템이 외부에 열려있음을 발견했다고 소명 • '22. 10. 14. 학내 무선망 등을 통해 평가대상자 정보(주민등록번호 포함), 서류평가 결과(성적 포함) 등을 엑셀 형태로 다운로드	관리자페이지 비밀번호 취약점 이용
입학정보 시스템	• '22. 10. 18. 동아리방에서 시스템의 생체인증 세션 파라미터를 변조하여 담당자 계정으로 로그인 후, 메뉴에서 지원자 선택·조회하여 PDF 형태로 다운로드 * SSO 개발사( )가 자사 서버와 인증 플랫폼 서버(FIDO)를 연계하는 과정에서, 로그인 사용자의 인증 여부가 확인된 경우에만 접근을 허용해야 하나, 확인되지 않더라도 접근을 허용하도록 검증과정 누락	파라미터 변조

다. 개인정보의 취급·운영 관련 사실관계

1) 고유식별정보(주민등록번호)의 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 ' 학년도 입학사정관 종합평가시스템'에서 ①개인정보취급자 계정에 안전한 비밀번호를 설정하지 않았고('1' 숫자 한 자리), ②비밀번호를 일정 횟수 이상 잘못 입력할 경우 시스템 접근을 제한하는 등의 접근 권한과 관련된 조치를 하지 않았으며, ③외부에서 관리자페이지에 접속할 때 안전한 인증수단 없이 아이디와 비밀번호만으로도 접속할 수 있도록 접근 통제 조치를 소홀히 한 사실이 있다. 이로 인해 권한 없는 제3자가 관리자 계정에 비밀번호를 대입해보는 방식으로 해당 계정을 탈취할 수 있었고, 관리자처럼 시스템에 접속하여 암호화되어 있던 주민등록번호를 복호화하여 엑셀 형태로 다운로드함으로써 고유식별정보(주민등록번호)가 유출된 사실이 있다.

2) 개인정보의 안전성 확보 조치를 소홀히 한 행위

피심인은 '舊인증지원시스템, 기관홈페이지 통합구축시스템, 통합연구행정 지원시스템, 차세대입학정보시스템'에 아래 표와 같이 접근 통제 조치를 하지 않은 사실이 있으며, '구 인증지원시스템'에 개인정보취급자가 접속한 기록을 월 1회 이상 점검하지 않은 사실이 있다.

시스템명	접근 통제 미흡 관련 사실
舊인증지원 시스템	• 조회 메뉴에서 입력된 파라미터에 대한 검증을 누락하여, 학생들이 재학생의 개인정보 및 증명사진 등을 다운로드하도록 허용함
기관홈페이지 통합구축 시스템	• 특정 소스코드에서 입력된 파라미터에 대한 검증을 누락하여, 학생들이 웹사이트 관리 솔루션의 소스코드를 다운로드 후 DB 연결정보를 발견하도록 함 • 페이지와 페이지에서 파일 업로드시 관리자 권한 확인 및 파일 확장자 등에 대한 검증 구문을 누락, 학생들이 웹셸을 업로드하여 DB로부터 개인정보를 탈취하도록 허용함
통합연구행정 지원시스템	• ' ' 메뉴 열람시 'USER_ID'에 대한 사용자 인증 로직을 누락하여 HTTP 프록시툴 등을 통해 파라미터 변조를 가능하게 함
입학정보 시스템	• SSO 개발사가 모바일앱에서 QR스캔 후 생체인증시 'login ID'에 대한 사용자 인증 로직을 누락한 사실을 검증하지 못하여, HTTP 프록시툴 등을 통해 파라미터 변조를 가능하게 함

3) 개인정보 유출 사실을 지체없이 통지하지 않은 행위

피심인은 '22. 11. 5. 개인정보 유출 사실을 최초 인지하였음에도 이로부터 12일이 지난 '22. 11. 17. 정보주체에게 해당 내용을 통지한 사실이 있다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 6. 26. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 8. 28. 개인정보보호위원회에 "위반 사실을 시정하였으며 선처를 요청한다"라는 내용의 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 고유식별정보의 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련 법 규정

舊보호법 제24조제3항은 “개인정보처리자가 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.”라고 규정하고 있고, 같은 법 시행령 제30조제1항은 “개인정보처리자는 법 제29조에 따라 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)를 하여야 한다”라고 규정하고 있다.

또한 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호, 이하 ‘舊고시’) 제5조제5항은 “개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.”라고 규정하고 있고, 제5조제6항은 “개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.”라고 규정하고 있으며, 제6조제2항은 “개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.”라고 규정하고 있다.

나. 위법성 판단

1) 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 하나, 피심인이 내부관리계획에 따라 개인정보취급자의 비밀번호를 영문, 숫자, 특수문자를 조합하여 구성하도록 규정하고 있음에도 이를 적용하지 않고, 학년도 입학사정관 종합평가시스템의 개인정보취급자 비밀번호를 안전한 비밀번호로 설정하지 않은 행위는 舊보호법 제24조제3항, 같은 법 시행령 제30조제1항, 舊고시 제5조제5항 위반에 해당한다.

2) 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 하나, 피심인이 ‘ 학년도 입학사정관 종합평가시스템’에서 비밀번호를 일정 횟수 이상 틀리더라도 시스템 접근을 차단하지 않은 행위는 舊보호법 제24조제3항, 같은 법 시행령 제30조제1항, 舊고시 제5조제6항 위반에 해당한다.

3) 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 하나, 피심인이 외부에서 ‘ 학년도 입학사정관 종합평가시스템’ 관리자페이지 접속할 때 아이디와 비밀번호만으로도 접속할 수 있도록 한 행위는 舊보호법 제24조제3항, 같은 법 시행령 제30조제1항, 舊고시 제6조제2항 위반에 해당한다.

2. 개인정보의 안전성 확보 조치를 소홀히 한 행위

가. 관련 법 규정

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.

또한 舊고시 제6조제3항은 “개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.”라고 규정하고 있으며, 제8조제2항은 “개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다.”라고 규정하고 있다.

나. 위법성 판단

1) 개인정보처리자는 취급중인 개인정보가 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템 등에 접근 통제 등에 관한 조치를 하여야 하나, 피심인이 舊인증지원시스템, 기관홈페이지 통합구축 시스템, 통합연구행정지원시스템, 입학정보시스템에 대해 접근 통제 등 조치를 하지 않은 행위(Ⅱ. 2. 다. 2) 표 참조)는 舊보호법 제29조, 같은 법 시행령 제30조제1항, 舊고시 제6조제3항 위반에 해당한다.

2) 개인정보처리자는 개인정보의 유출 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 하나, 피심인이 '舊인증지원시스템'의 접속 기록을 월 1회 이상 점검하지 않은 행위는 舊보호법 제29조, 같은 법 시행령 제30조제1항, 舊고시 제8조제2항 위반에 해당한다.

3. 개인정보 유출 사실을 지체없이 통지하지 않은 행위

가. 관련 법 규정

舊보호법 제34조제1항은 "개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체없이 해당 정보주체에게 유출된 개인정보의 항목, 유출된 시점과 그 경위, 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, 개인정보처리자의 대응조치 및 구제절차, 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처 등을 알려야 한다."라고 규정하고 있다.

나. 위법성 판단

개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때 지체없이 해당 정보주체에게 관련 사실을 알려야 하나, 피심인이 유출 사실을 '22. 11. 5. 인지하고도 정보주체에게 관련 내용을 12일이 경과한 '22. 11. 17. 통지한 행위는 舊보호법 제34조제1항 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 舊보호법 제24조제3항 위반행위에 대해 같은 법 제34조의2 제1항, 같은 법 시행령 제40조의2 [별표 1의3], 「주민등록번호 유출 등에 대한 과징금 부과기준(고시 제2022-4호, 2022.10.20., 이하 '舊과징금 부과기준')」에 따라 다음과 같이 과징금을 부과한다.

가. 기준금액

舊보호법 시행령 제40조의2 [별표 1의3]은 고의·중과실·경과실 여부 및 유출 주민등록번호 규모에 따라 산정기준액을 규정하고 있고, 舊과징금 부과기준 제4조제2항은 "위반행위의 고의 또는 중과실 여부는 위반행위의 목적, 동기, 당해 행위에 이른 경위 등을 종합적으로 고려하여 판단한다'라고 규정하고 있다.

피심인의 경우, 소속 학생들이 약 1년 3개월에 걸쳐 다양한 해킹 방법을 활용하여 학내 여러 시스템에 무단 침입하는 동안 장기간 현저하게 안전조치 의무를 위반하였고, 불법적인 접근 시도(최소 11회 이상)들이 이어지는 과정에서 일반 수준의 주의를 기울였더라면 결과 발생을 충분히 예방할 수 있었음에도 적기에 대응하지 못하여 주변 기관·단체로 유사 피해가 확산한 사실이 확인되는 만큼, 당해 행위에 이른 경위를 종합할 때 중과실로 인하여 10만 건 미만의 주민등록번호가 유출된 경우로서, '중대한 위반행위'에 해당하는 금액인 2억3천만 원을 적용한다.

<舊보호법 시행령 제40조의2 [별표 1의3] >

위반 정도	산정 기준액	비고
매우 중대한 위반행위	3억 5천만 원	고의 또는 중과실로 인하여 10만 건 이상의 주민등록번호가 분실·도난·유출·변조 또는 훼손(이하 '분실 등'이라 한다)된 경우
중대한 위반행위	2억 3천만 원	고의 또는 중과실로 인하여 10만 건 미만의 주민등록번호가 분실 등이 된 경우 및 경과실로 인하여 10만 건 이상의 주민등록번호가 분실 등이 된 경우
일반 위반행위	1억 원	경과실로 인하여 10만 건 미만의 주민등록번호가 분실 등이 된 경우

나. 1차 조정

舊과징금 부과기준 제5조는 “1차 조정금액은 산정기준액에 따라 <1차 조정 기준표>에서 정한 1차 조정비율을 곱한 금액으로 정한다. 1차 조정 비율은 <세부평가 기준표>에 따라 산정한다”라고 규정하고 있다.

피심인의 舊보호법 제24조제3항 위반행위는 舊과징금 부과기준 제5조의 <세부평가 기준표>에 따른 산정 점수가 1.4점에 해당하므로, <1차 조정 기준표>에 따라 기준금액의 50%인 1억 1,500만 원을 감경한다.

< 舊세부평가 기준표 >

고려사항 \ 부과점수		비중	3점	2점	1점
안전성확보조치	개인정보에 대한 접근	0.2	주민등록번호에 대하여 다음 각 호의 조치를 모두 하지 아니하거나 현저히 부실하게 한 경우 1. **접근통제** 2. **접근권한의 관리**	주민등록번호에 대하여 다음 각 호의 조치 중 한 가지를 하지 아니하거나 현저히 부실하게 한 경우 1. 접근통제 2. 접근권한의 관리	3점 또는 2점에 해당되지 않는 경우
안전성확보조치	암호화	0.2	주민등록번호의 송신·전달·저장 시 이를 암호화하지 아니한 경우	주민등록번호를 안전한 암호화알고리즘으로 암호화하지 않은 경우	3점 또는 2점에 해당되지 않는 경우
안전성확보조치	보안 프로그램	0.2	악성프로그램 등을 방지·치료할 수 있는 보안프로그램을 설치·운영하지 않은 경우	보안프로그램에 대한 업데이트를 실시하지 아니하여 최신의 상태로 유지하지 않은 경우	3점 또는 2점에 해당되지 않는 경우
안전성확보조치	접속기록의 보관 등	0.2	개인정보처리시스템의 접속기록 보관 및 위조·변조 등 방지를 위한 조치를 하지 아니하고, 주민등록번호를 보관하는 물리적 보관장소를 별도로 두지 아니하거나 잠금장치를 하지 않은 경우	개인정보처리시스템의 접속기록 보관 및 위조·변조 등 방지를 위한 조치를 하지 아니하거나, 주민등록번호에 대한 물리적 보관장소를 별도로 두지 않는 등 물리적 안전조치가 없는 경우	3점 또는 2점에 해당되지 않는 경우*
피해 방지 후속 조치 등		0.2	개인정보가 유출되었음을 알게 된 때로부터 5일 이내에 다음 각 호의 조치를 모두 하지 아니한 경우 1. 정보주체에게 통지 2. 피해 최소화를 위한 대책 마련 및 조치 3. 조치결과를 신고	개인정보가 유출되었음을 알게 된 때로부터 5일 이내에 다음 각 호의 조치 사항 중 두 가지 이상을 하지 아니한 경우 1. 정보주체에게 통지 2. 피해 최소화를 위한 대책 마련 및 조치 3. 조치결과를 신고	3점 또는 2점에 해당되지 않는 경우

* 접속 기록 관련 위반이 확인되었으나 이는 ‘舊인증지원시스템’에서 확인된 위반 사항으로, 주민등록번호 유출의 원인이 된 ‘ 학년도 입학사정관 종합평가시스템’과는 무관하므로, 평가시 포함하여 판단하지 않음

< 舊1차 조정 기준표 >

세부평가 기준표에 따른 산정 점수	1차 조정 비율
2.5이상	+100분의 50
2.3이상 2.5미만	+100분의 35
2.1이상 2.3미만	+100분의 20
1.9이상 2.1미만	-
1.7이상 1.9미만	-100분의 20
1.5이상 1.7미만	-100분의 35
1.5미만	-100분의 50

다. 2차 조정

舊과징금 부과기준 제6조는 "2차 조정금액은 1차 조정된 금액에 <2차 조정 기준표>에서 정한 2차 조정비율을 곱한 금액으로 정한다. 2차 조정 비율은 <세부평가 기준표>에 따라 산정한다"라고 규정하고 있다.

피심인의 舊보호법 제24조제3항 위반행위는 舊과징금 부과기준 제6조의 <세부평가 기준표>에 따른 산정 점수가 1.2점에 해당하므로, <2차 조정 기준표>에 따라 1차 조정된 금액의 50%인 5,750만 원을 감경한다.

< 舊세부평가 기준표 >

고려사항 \ 부과점수 / 비중	비중	3점	2점	1점
위반기간	0.2	위반기간이 6개월을 초과하는 경우	위반기간이 3개월 초과 6개월 이내인 경우	3점 또는 2점에 해당되지 않는 경우
위반횟수	0.2	최근 3년 내 주민등록번호 유출로 과징금 부과 처분을 2회 이상 받은 경우	최근 3년 내 주민등록번호 유출로 과징금 부과 처분을 1회 이상 받은 경우	3점 또는 2점에 해당되지 않는 경우
조사협조	0.2	위반행위 조사 시 조사기간내 자료 미제출, 조사자료 은폐 등 조사방해의 부당성이 현저히 큰 경우	위반행위 조사 시 조사기간내 자료 미제출, 조사자료 은폐 등 조사방해의 부당성이 경미하지 않은 경우	3점 또는 2점에 해당되지 않는 경우
2차 피해	0.2	위반행위로 인해 보이스피싱 등 2차 피해가 발생한 경우	위반행위로 인해 보이스피싱 등 2차 피해 발생할 우려가 상당히 큰 경우	3점 또는 2점에 해당되지 않는 경우
개인정보 보호를 위한 노력	0.2	참작할 사유가 없는 경우	개인정보 보호 관련 직원교육을 하거나 표창을 받는 등 개인정보 보호를 위한 노력이 상당히 있는 경우*	다음 각 호의 어느 하나에 해당하는 경우 등 개인정보 보호를 위한 노력이 현저히 큰 경우

* '22.6.9.~'22.7.7. 개인정보책임자 및 취급자 440여명 상대 개인정보 보호 교육 4회 진행

< 舊2차 조정 기준표 >

세부평가 기준표에 따른 산정 점수	2차 조정 비율
2.5이상	+100분의 50
2.1이상 2.5미만	+100분의 25
1.7이상 2.1미만	-
1.3이상 1.7미만	-100분의 25
1.3미만	-100분의 50

라. 부과과징금의 결정

舊과징금 부과기준 제8조제1항은 "위반행위자의 현실적인 부담 능력, 위반행위로 발생한 정보주체의 피해 및 배상의 정도, 위반행위자가 속한 시장·산업 여건 등을 고려하여 2차 조정된 과징금이 과중하다고 인정되는 경우 해당 금액의 100분의 90 범위에서 감경할 수 있다"라고 규정하고 있으며, 제8조제2항은 "객관적으로 과징금을 낼 능력이 없다고 인정되는 경우(제1호), 정보주체에게 피해가 발생하지 않았거나 경미한 경우(제2호), 본인의 행위가 위법하지 않은 것으로 잘못 인식할 만한 정당한 사유가 있는 경우(제3호)에 2차 조정된 금액을 면제할 수 있다"라고 규정하고 있다.

피심인의 위반행위는 舊과징금 부과기준 제8조의 감경 또는 면제 기준에 해당하지 않아 2차 조정 금액을 유지한다.

마. 최종 과징금

피심인의 舊보호법 제24조제3항 위반행위에 대하여 기준금액에서 1차·2차 조정 및 부과과징금의 결정을 거쳐 총 5,750만 원의 과징금을 부과한다.

< 과징금 산출내역 >

기준금액	1차 조정	2차 조정	부과 과징금 결정	최종 과징금
2억3천만 원	1억1,500만 원	5,750만 원	5,750만 원	**5,750만 원**
중대한 위반행위 ※ 주민등록번호 10만건 미만 / 중과실	1차 산정점수 : 1.4점 ⇒ 50%(1억1,500만 원) 감경	2차 산정점수 : 1.2점 ⇒ 50%(5,750만 원) 감경	해당 없음 ⇒ 감경 없음	

2. 과태료 부과

舊보호법 제76조는 “제75조의 과태료에 관한 규정을 적용할 때 제34조의2에 따라 과징금을 부과한 행위에 대하여는 과태료를 부과할 수 없다”라고 규정하고 있다.

피심인의 舊보호법 제24조제3항 위반행위는 같은 법 제75조제2항제6호, 같은 법 시행령 제63조의 [별표2]에 따라 과태료 부과 사유에 해당하나, 舊보호법 제76조에 따라 과태료를 부과하지 아니한다.

피심인의 舊보호법 제29조 및 제34조제1항 위반행위에 대해 같은 법 제75조제2항제6호·제8호, 같은 법 시행령 제63조의 [별표2]에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

舊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 제29조 및 제34조제1항 위반행위에 대해 1회 위반에 해당하는 과태료인 1,200만 원(각 600만 원)을 적용한다.

< 舊보호법 시행령 제63조 [별표 2] - 과태료 부과기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
처. 법 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제8호	600	1,200	2,400

나. 과태료의 가중

「개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보위 2023. 3. 8. 이하 '舊과태료 부과지침') 제8조(과태료의 가중)는 "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 舊보호법 제29조 위반행위는 舊과태료 부과지침 제8조의 과태료 가중기준에서 각 목의 세부기준에서 정한 행위가 2개 이상인 경우(+10%)에 해당하며, 법 위반 상태의 기간이 3개월 이상인 경우(+10%)에 해당하므로 기준금액의 20%인 120만원을 가중한다.

< 舊과태료 부과지침 [별표 2] - 과태료 가중기준 >

기준	가중사유	가중비율
위반의 정도	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내
위반 기간	법 위반상태의 기간이 3개월 이상인 경우	기준금액의 50% 이내

피심인의 舊보호법 제34조제1항 위반행위는 舊과태료 부과지침 제8조의 과태료 가중기준에 해당하지 않아 기준금액을 유지한다.

다. 과태료의 감경

舊과태료 부과지침 제7조(과태료의 감경)는 "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.

피심인은 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 시정 완료하고, 조사 기간 중 일관되게 행위 사실을 인정하면서 자료 제출 등 조사에 적극 협력하였으므로, 舊과태료 부과지침 제7조 [별표1] 감경기준에 따라 기준금액의 50%인 600만 원(각 300만 원)을 감경한다.

< 舊과태료 부과지침 [별표 1] - 과태료 감경기준 >

기준	감경사유	감경비율
조사 협조·자진 시정 등	1. 과태료의 사전 통지 및 의견 제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 50% 이내
	2. 보호위원회의 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 경우	기준금액의 40% 이내

라. 최종 과태료

피심인의 舊보호법 제29조 및 제34조제1항 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 총 720만 원의 과태료를 부과한다.

< 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만 원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
제29조(안전조치 의무)	법 제75조제2항제6호	600	120	300	**420**
제34조제1항(통지 의무)	법 제75조제2항제8호	600		300	**300**
계		1,200	120	600	**720**

3. 처분 결과의 공표

舊보호법 제66조제1항에 따라 피심인이 과태료를 부과받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다.

> * **「舊개인정보 보호위원회 처분결과 공표기준」 제2조(공표요건)** 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우 처분 결과를 공표할 수 있다.
>
> 4. 법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우
> 5. 위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우
>
> * **「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」 제5조(공표기간)** 보호위원회가 인터넷 홈페이지 등에 공표하는 경우 기간은 1년으로 한다.

개인정보보호법 위반 행정처분 결과 공표

개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.

순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1		법 제29조	안전조치 의무 위반	2023. 10. 11.	과태료 420만 원
		법 제34조 제1항	개인정보 유출 통지 위반		과태료 300만 원

2023년 10월 11일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인의 舊보호법 제24조제3항, 제29조, 제34조제1항 위반행위에 대하여 같은 법 제34조의2제1항, 제75조제2항, 제66조제1항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 과징금 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(피심인 주소지의 지방법원 또는 그 지원)이 과태료 재판절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다

2023년 10월 11일

위 원 장　　고 학 수　(서 명)

부위원장　　최 장 혁　(서 명)

위　　원　　김 일 환　(서 명)

위　　원　　김 진 욱　(서 명)

위　　원　　김 진 환　(서 명)

위　　원　　박 상 희　(서 명)

위　　원　　윤 영 미　(서 명)

위　　원　　조 소 영　(서 명)