개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호	제2023-008-072호 (사건번호: 2021조총0037)
안 건 명	공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인	

의결연월일 2023. 5. 10.

주 문

1. 피심인에 대하여 다음과 같이 과징금 및 과태료를 부과한다.

   가. 과 징 금 : 74,750,000원

   나. 과 태 료 : 6,600,000원

   다. 납부기한 : 고지서에 명시된 납부기한 이내

   라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인의 법 위반 행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 피심인의 일반 현황

피심인은 「개인정보 보호법」(이하 '보호법'이라 한다.) 제2조제6호나목에 따른 공공기관으로 보호법 제2조제5호에 따른 개인정보처리자이며, 일반현황은 다음과 같다.

< 피심인의 일반현황 >

사업자 등록번호	대표자 성명	주소	직원 수

Ⅱ. 사실조사 결과

개인정보보호위원회는 개인정보 유출신고 건과 관련하여 피심인의 「개인정보 보호법」위반 여부에 대한 사실조사( ) 결과, 다음과 같은 사실을 확인하였다.

1. 행위 사실

가. 개인정보 수집 · 이용 현황

피심인은 기준 아래와 같이 개인정보를 수집·보유하고 있다.

	개인정보파일 (처리시스템)	수집·이용 항목	목적	수집 방법	수집일	보유기간	보유건수
1							
2							
3							

나. 개인정보 유출 관련 사실관계

개인정보보호위원회는 1차 유출 조사를 진행하면서, 2차·3차 추가 유출 사실을 확인하였다.(경찰청 협조)

① 내부망 업무용 PC 공유폴더 파일 유출

1) 유출 항목 및 규모

- 내부망 업무용 PC 및 서버에 보관하고 있던 정보 및 정보

2) 유출경위

- 신원미상의 자가 피심인의 파일 업로드 취약점을 이용하여 웹셸[1])( )을 업로드하였고,

- 웹셸을 이용하여 웹서버에서 원격데스크톱 서비스로 유휴 서버인 서버*에 연결( )한 후

  * 사업 종료( ) 후 네트워크가 연결된 채로 DMZ에 방치됨
    - (구) 서버 내부 디스크에서 1,025개 업무관련 파일을 확인함

- 네트워크 스캔을 통해 윈도우 공유폴더 기능이 활성화*된 내부망 업무용 PC 및 서버 를 발견하고 공유폴더에 있던 업무파일 일부를 열람하였으며,

  * 피심인의 「 지침( )」은 '공유폴더는 필요한 경우에만 설정하였다가 공유목적 달성 후 해제하여야 하고 전체 공유로 설정하지 않아야 하며 목적에 해당하는 폴더만 최소한으로 공유하는 한편 공유폴더 접근시 인증절차를 설정하여야 한다'고 규정

- 공유폴더 업무파일들을 (구) 서버로 복사하고, 중복 제거 및 분할압축(1기가 단위) 한 뒤, 약 213G의 자료(문서, 이미지, 엑셀파일 등)를 국외서버(, 독일)와 국내서버(, 한국)로 전송하고 해당 파일을 삭제하였다

1) 공격대상 웹 사이트의 게시판, 자료실 등과 같은 파일 업로드 기능을 이용해 웹셸을 업로드한 후 실행하여 해당 웹서버 정보를 수집하여 공격하는 기법으로 서버 명령을 실행할 수 있는 JSP(Java Server Pages) 등이 이에 해당함

3) 유출인지 및 대응

일시	피심인의 유출인지·대응 내용
	피심인, 외부기관의 위협징후 통보를 받고 자체분석* 진행 * 신원 미상의 자가 파일을 삭제하여 정확한 유출내역을 확인하지 못함
	피심인, 내부정보 유출 의심에 따라 신고
	, 피심인에 대한 현장점검 실시
	피심인, 개인정보 **유출사실 인지*** * 침해사고 분석보고서로부터 유출정황이 매우 높다는 내용을 수신
	인터넷 홈페이지에 유출사실 게재
	정보주체에게 **유출사실 통지**(문자, 우편)
	개인정보 **유출신고**

2 데이터

1) 유출 항목 및 규모

- 판독용 서버( )와 백업용 ( )에 저장되어 있던 정보 및 데이터

· 규모 : 총 652,930명의 정보 및 데이터

2) 유출경위

- 미상의 자는 부터 공격을 시도하다가 (구) 서버 등에서 확보한 계정정보를 사용하여 외부망에 노출된 피심인의 통합커뮤니케이션( ) 서비스의 제어판 관리센터( ) 로그인에 성공하고

- 판독용 서버와 백업용 를 네트워크 드라이브로 연결한 것으로 추정되며

- 판독용 서버의 'DB_Backup' 폴더 내 있던 SQL파일과 백업용 에 있던 파일(SQL파일)을 MS 익스체인지 서버( )의 'ecp' 폴더에 분할 압축 저장(200메가 단위)하고

- MS 리버스 프록시 서버(, 단순 포워딩 및 외부접속 서버)를 거쳐 국외서버(, 독일)로 개인정보를 전송하였다.

3) 유출인지 및 대응

일시	피심인의 유출인지·대응 내용
	피심인, 경찰청의 해킹징후 통보를 받고 자체분석 진행
	개인정보 유출사실 **인지**
	개인정보 **유출 신고**
	정보주체에게 **유출사실 통지**(문자, 우편)
	인터넷 홈페이지에 유출사실 게재

3 직원정보

1) 유출 항목 및 규모

- 부문 홈페이지( ) 로그인을 위해 홈페이지에 가입한 , 일반직원, 정보

· 항목 : 이름, 생년월일, 성별, ID, 비밀번호, 이메일, 휴대폰번호, 전화번호, 주소, 사원번호, 번호

· 규모 : 총 1,953건 (1에서 유출된 1,550건 포함)

2) 유출경위

- 미상의 자는 웹서버에 파일 업로드 취약점을 악용하여 웹쉘(JspSpy 등)을 업로드(1과 동일경로)하였고,

웹쉘( )을 이용하여 내부망 DB(오라클, IP:)에 접속한 후 직원정보를 추출하고, 외부 경유서버에 파일(5개)을 저장하였다.

3) 유출인지 및 대응

일시	피심인의 유출인지·대응 내용
	경찰청, 국내 경유서버에서 개인정보가 발견됨을 통보
	개인정보 **유출사실 인지**
	개인정보 유출 대책회의 개최
	홈페이지 외부공격에 대한 차단 등 대응
	정보주체에게 **유출 통지**(문자, 이메일)*

* ①과 동일한 공격자(IP:)가 동일한 경로(웹서버)를 통해 직원정보를 유출한 사안으로, 추가 유출된 직원(403건) 대상 유출통지만 진행

다. 기초 사실

① 내부망 업무용 PC 공유폴더 파일 유출

1) 주민등록번호를 암호화하지 않고 보관한 행위

피심인은 '19년 ', ' ' 등 주민등록번호(10,089명)가 포함된 엑셀파일을 암호화하여 저장하지 않은 사실이 있다.

2) 고유식별정보를 암호화하지 않고 보관한 행위

피심인은 피부과 내부망 업무용 PC에 여권번호(2명)를 암호화하지 않고 저장한 사실이 있다.

3) 개인정보 안전조치 의무를 소홀히 한 행위

(접근권한) 피심인은 공용 PC에 , 등 개인정보 취급자의 정보시스템( )의 비밀번호를 텍스트파일에 기재하고 상호 공유하여 사용한 사실이 있다.

(접근통제) 피심인이 내부망 업무용 PC 및 서버에 공유폴더 등에 대한 권한 설정 등의 조치를 하지 않아, 미상의 자가 (구) 서버를

통해 공유폴더가 설정되어 있던 PC 및 서버에 접근하여 저장된 파일을 열람 및 외부로 전송한 사실이 있다.

(암호화) 피심인은 내부망 업무용 PC에 및 들의 정보시스템 비밀번호를 평문으로 저장한 사실이 있다.

2 데이터

1) 개인정보 안전조치 의무를 소홀히 한 행위

(악성프로그램) 피심인은 MS에서 보안취약점을 발표('20.2.11.)하고 인터넷진흥원 '보호나라&KrCERT'에서 보안공지('20.3.2.)를 하였음에도 MS익스체인지2013 서버에 즉시 패치를 적용하지 않고 '21.6월 공격 당시까지 업데이트를 실시하지 않은 사실이 있다.

(접근권한) 피심인은 시스템에서 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하지 않고, 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 기능이 없다.

(접근통제) 피심인은 판독용 서버 및 에서 윈도우 공유폴더 기능을 활성화한 사실이 있다.

(암호화) 피심인은 시스템에서 개인정보취급자의 비밀번호를 평문으로 저장한 사실이 있다.

(접속기록) 피심인은 시스템에서 개인정보처리시스템에 접속한 기록을 보관.관리하지 않은 사실이 있다.

3 직원정보

1) 정보주체에게 유출사실을 지체없이 통지하지 않은 행위

피심인은 ( ) 회원정보(직원정보)가 국내 경유 서버에서 발견되어, 개인정보가 유출된 사실을 인지('21. 11. 24.)하였음에도 정보주체에게 즉시 통지하지 않은 사실이 있다.('21. 12. 7. 통지 시작)

2. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 2. 6. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 2. 23. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 보호법 제24조의2제2항은 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다고 규정하고 있다.

나. 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 한다고 규정하고 있다.

같은 법 시행령 제21조제1항은 법 제24조제3항에 따른 고유식별정보의 안전성 확보조치에 관하여는 제30조 또는 제48조의2를 준용한다. 이 경우 '법 제29조'는 '법 제24조제3항'으로, '개인정보'는 '고유식별정보'로 본다고 규정하고 있다.

보호법 제29조는 개인정보처리자는 개인정보가 분실·도난·유출·위조·

변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다고 규정하고 있다.

같은 법 시행령 제30조제1항은 개인정보처리자는 법 제29조에 따라 '개인정보에 대한 접근통제 및 접근권한의 제한 조치(제2호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화기술의 적용 또는 이에 상응하는 조치(제3호)', '개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)', 개인정보에 대한 보안프로그램의 설치 및 갱신(제5호)' 등의 안전성 확보조치를 하여야 한다고 규정하고 있다.

같은 법 시행령 제30조제3항에 따라 안전성 확보조치에 관한 세부기준을 구체적으로 정하고 있는 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호, 이하 '고시') 제5조제3항은 '개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 3년간 보관하여야 한다'고 규정하고 있고, 제4항은 '개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자별로 사용자계정을 발급해야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다'고 규정하고 있으며, 제6항은 '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'고 규정하고 있다.

고시 제6조제3항은 '개인정보처리자는 취급중인 개인정보가 인터넷홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근통제 등에 관한 조치를 하여야 한다'고 규정하고 있다.

고시 제7조제2항은 ‘개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우 일방향 암호화하여 저장하여야 한다’고 규정하고 있다.

고시 제8조제1항은 ‘개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다’고 규정하고 있다.

고시 제9조는 개인정보처리자는 악성프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안프로그램을 설치·운영하여야 하며, 보안프로그램의 자동 업데이트 기능을 사용하거나 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지(1호), 악성프로그램 관련 경보가 발령된 경우 또는 사용중인 응용프로그램이나 운영체제 소프트웨어 제작업체에서 보안업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시(2호), 발견된 악성프로그램에 대해 삭제 등 대응 조치(3호) 등 각호의 사항을 준수하여야 한다‘고 규정하고 있다.

다. 보호법 제34조제1항은 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 ’유출된 개인정보의 항목‘(제1호), ’유출된 시점과 그 경위‘(제2호), ’유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보‘(제3호), ’개인정보처리자의 대응조치 및 피해구제절차‘(제4호), ’정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처‘(제5호) 등 각 호의 사실을 알려야 한다고 규정하고 있다.

같은 법 시행령 제40조는 개인정보처리자는 개인정보가 유출되었음을 알게되었을 때에는 서면 등의 방법으로 지체없이 법 제34조제1항 각호의 사항을 정보주체에게 알려야 한다고 규정하고 있다.

2. 위법성 판단

가. 주민등록번호를 암호화하지 않고 보관한 행위

피심인이 ‘19년도 ’, ‘ ’ 등 주민등록번호가 포함된 엑셀파일을 암호화하여 저장하지 않은 것은 개인정보보호법 제24조의2제2항을 위반한 것이다.

나. 고유식별정보를 암호화하지 않고 보관한 행위

피심인이 내부망 업무용 PC에 여권번호를 암호화하지 않고 저장한 것은 개인정보보호법 제24조제3항을 위반한 것이다.

다. 개인정보에 대한 안전성 확보조치를 소홀히 한 행위

피심인이 시스템에서 개인정보취급자의 접근권한 부여·변경·말소에 대한 내역을 기록·보관하지 않은 것은 보호법 제29조(고시 제5조제3항)를 위반한 것이다.

피심인이 공용PC(IP:)에 전공의, 교수 등 개인정보취급자의 정보시스템( )의 비밀번호를 텍스트 파일 등에 기재하고 상호 공유하여 사용한 것은 보호법 제29조(고시 제5조제4항)를 위반한 것이다.

피심인이 시스템에서 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하지 않은 것은 보호법 제29조(고시 제5조제6항)를 위반한 것이다.

피심인이 내부망 업무용 PC 및 서버에 공유폴더에 권한 설정 등의 조치를 하지 않고, 판독용 서버 및 에서 윈도우 공유폴더 기능을 활성화한 것은 보호법 제29조(고시 제6조제3항)를 위반한 것이다.

피심인이 내부망 업무용 PC에서 와 들의 시스템( ) 비밀번호를, 시스템에서 개인정보취급자의 비밀번호를 평문으로 저장한 것은 보호법 제29조(고시 제7조제2항)를 위반한 것이다.

피심인이 시스템에서 개인정보처리시스템에 접속한 기록을 보관.관리하지 않은 것은 보호법 제29조(고시 제8조제1항)를 위반한 것이다.

피심인이 마이크로소프트(MS)에서 보안취약점을 발표('20.2.11.)하고, 인터넷진흥원 '보호나라&KrCERT'에서 보안공지('20.3.2.)를 하였음에도, MS 익스체인지 2013 서버에 즉시 패치를 적용하지 않고, '21.6월 공격 당시까지 업데이트를 실시하지 않은 것은 보호법 제29조(고시 제9조)를 위반한 것이다.

라. 정보주체에게 유출사실을 지체없이 통지하지 않은 행위

피심인이 홈페이지( ) 회원정보(직원정보)가 국내 경유서버에서 발견되어, 개인정보가 유출된 사실을 인지하였음에도 정보주체에게 즉시 통지하지 않은 것은 보호법 제34조를 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
• 주민등록번호의 처리 제한	법§24의2②	§21의2	주민등록번호를 암호화조치를 통해 안전하게 보관하지 않은 행위
• 고유식별정보 처리 제한	법§24③	§21①	고유식별정보에 안전성 확보에 필요한 조치를 하지 않은 행위
• 안전성 확보조치	법 §29	§30①	외부에서 정보통신망을 통해 개인정보처리시스템에 접속하려는 경우 안전한 접속수단이나 안전한 인증수단을 적용하지 않은 행위(고시§6②)
접근권한	법 §29	§30①	접근권한의 부여·변경·말소에 대한 내역을 기록·보관하지 않은 행위(고시§5③) 개인정보취급자별로 사용자계정을 발급하여 다른 취급자와 공유되지 않도록 하지 않은 행위(고시§5④) 계정정보 또는 비밀번호를 일정횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하지 않은 행위(고시§5⑥)
접근통제	법 §29	§30①	공유폴더에 권한 설정 등의 조치를 하지 않은 행위(고시§6③)
암호화	법 §29	§30①	비밀번호를 암호화하여 저장하지 않은 행위(§7②)
접속기록	법 §29	§30①	개인정보취급자가 개인정보처리시스템에 접속한 기록을 보관·관리하지 않은 행위(§8①)
악성프로그램	법 §29	§30①	보안업데이트 공지가 있었음에도 보안 업데이트를 실시하지 않은 행위(§9)
• 개인정보의 유출 통지	법 §34①	§40①	개인정보 유출을 인지하였음에도 정보주체에게 즉시 유출통지를 하지 않은 행위

Ⅳ. 처분 및 결정

○ 주민등록번호 유출로 인한 과징금 부과(법 제34조의2) 대상에 해당하는 피심인의 위반행위(1차 유출, 내부망 업무용PC 공유폴더 파일)에 대하여는 보호법 제76조[2]에 따라 과태료를 부과하지 아니한다.

보호법 제34조의2*에 따라 과징금을 부과한 행위에 대하여는 과태료를 부과할 수 없다고 규정한 보호법 제76조에 따라, 피심인의 1~3차 유출 중 1차 유출**당시 법 위반사항에 대해서는 법 제75조의 과태료를 미부과 * 주민등록번호가 유출된 경우 등에 대한 과징금 부과조항 ** 내부망 업무용 PC 공유폴더 파일 유출

1. 과징금 부과

보호법 제34조의2에 따라 주민등록번호가 유출된 경우로서 법 제24조 제3항에 따른 안전성 확보에 필요한 조치를 다하지 않은 경우에는 과징금을 부과할 수 있다.

피심인의 보호법 제24조제3항 위반행위에 대해 같은 법 제34조의2제1항, 같은 법 시행령 제40조의2 [별표1의3], 주민등록번호 유출 등에 대한 과징금 부과기준(고시 제2022-4호, 2022.10.20., 이하 '과징금 부과기준')에 따라 다음과 같이 부과한다.

가. 기준금액

보호법 시행령 제40조의2 [별표1의3]은 고의·중과실·경과실 여부 및 유출 주민등록번호 규모에 따라 산정기준액을 규정하고 있고, 피심인은 중과실로 인하여 10만 건 미만의 주민등록번호가 유출되었으므로, '중대한 위반행위'에 해당하는 금액인 2억3천만원을 적용한다.

2) 제76조(과태료에 관한 규정 적용의 특례) 제75조의 과태료에 관한 규정을 적용할 때 제34조의2에 따라 과징금을 부과한 행위에 대하여는 과태료를 부과할 수 없다.

<보호법 시행령 제40조의2 [별표 1의3] >

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

* 위반행위의 고의 또는 중과실 여부는 위반행위의 목적, 동기, 당해 행위에 이른 경위 등을 종합적으로 고려하여 판단(과징금부과기준 §4②)

나. 1차 조정

과징금 부과기준 제5조(1차 조정)는 "1차 조정금액은 산정기준액에 따라 <1차 조정 기준표>에서 정한 1차 조정비율을 곱한 금액으로 정한다. 1차 조정 비율은 <세부평가 기준표>에 따라 산정한다"고 규정하고 있다.

피심인의 위반행위는 과징금 부과기준 제5조의 <세부평가 기준표>에 따른 산정 점수가 1.6점에 해당하므로, <1차 조정 기준표>에 따라 기준금액의 35%인 8,050만원을 감경한다.

< 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

< 세부평가 기준표 >

고려사항		부과점수 / 비중	3점	2점	1점
안전성확보	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

조치	암호화	0.2	주민등록번호의 송신·전달·저장 시 이를 암호화 하지 아니한 경우	주민등록번호를 안전한 암호화 알고리즘으로 암호화하지 않은 경우	3점 또는 2점에 해당되지 않는 경우
	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
	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

다. 2차 조정

과징금 부과기준 제6조(2차 조정)는 "2차 조정금액은 1차 조정된 금액에 <2차 조정 기준표>에서 정한 2차 조정비율을 곱한 금액으로 정한다. 2차 조정 비율은 <세부평가 기준표>에 따라 산정한다"고 규정하고 있다.

피심인의 위반행위는 과징금 부과기준 제6조의 <세부평가 기준표>에 따른 산정 점수가 1점에 해당하므로, <2차 조정 기준표>에 따라 1차 조정된 금액(1억 4,950만원)의 50%인 7,475만 원을 감경한다.

< 2차 조정 기준표 >

세부평가 기준표에 따른 산정 점수	1차 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

< 세부평가 기준표 >

고려사항 \ 부과점수	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 조사기간 내 자료 미제출, 조사자료 은폐 등 조사방해의 부당성이 현저히 큰 경우	위반행위 조사 시 조사기간 내 자료 미제출, 조사자료 은폐 등 조사방해의 부당성이 경미하지 않은 경우	3점 또는 2점에 해당되지 않는 경우
2차 피해	0.2	위반행위로 인해 보이스 피싱 등 2차 피해가 발생한 경우	위반행위로 인해 보이스 피싱 등 2차 피해 발생할 우려가 상당히 큰 경우	3점 또는 2점에 해당되지 않는 경우
개인정보 보호를 위한 노력	0.2	참작할 사유가 없는 경우	개인정보보호 관련 직원 교육을 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 1. 개인정보보호 인증*을 받은 경우 등

라. 부과과징금의 결정

과징금 부과기준 제8조(부과과징금의 결정)제1항은 “위반행위자의 현실적인 부담능력, 위반행위로 발생한 정보주체의 피해 및 배상의 정도, 위반행위자가 속한 시장 · 산업 여건 등을 고려하여 2차 조정된 과징금이 과중하다고 인정되는 경우에는 해당 금액의 100분의 90 범위에서 감경할 수 있다.”고 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”고 규정하고 있다.

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

마. 최종 과징금

피심인의 위반행위에 대하여 기준금액에서 1차·2차 조정 및 부과과징금의 결정을 거쳐 총 7,475만원의 과징금을 부과한다.

2. 과태료 부과

피심인의 1차 유출(내부망 업무용PC 공유폴더 파일) 관련 보호법 위반행위에 대하여는 과징금이 부과되므로 법 제76조에 따라 과태료를 부과하지 아니하고, 2·3차 유출 관련 위반행위에 대하여 과태료를 부과한다.

피심인의 보호법 제29조(안전조치 의무), 제34조제1항(개인정보 유출통지) 위반행위에 대한 과태료는 같은 법 제75조제2항제6호·제8호 및 같은 법 시행령 제63조의 [별표2] 「과태료 부과기준」에 따라 다음과 같이 부과한다.

가. 기준금액

최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 금액 총 600만원을 적용한다.

위반행위	근거 법조문	과태료 금액(만원)		
		1회 위반	2회 위반	3회 이상 위반
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
처. 법 **제34조제1항을 위반하여 정보주체에게 같은 항 각호의 사실을 알리지 않은 경우**	법 제75조 제2항제8호	600	1,200	2,400

나. 과태료의 가중·감경

1) (과태료의 가중) 「개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보보호위원회 지침 '23. 3. 8. 일부개정, 이하 '과태료 부과지침') 제8조(과태료의 가중)는 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 법 제29조 위반행위에 대하여는 경우 과태료 부과지침 제8조(과태료 가중) [별표2] 가중기준에 따라 위반행위별 각 목의 세부기준에서 정한 행위가 3개인 점을 고려하여 기준금액의 10%인 60만원을 가중한다.

< 과태료의 가중기준(제8조 관련) >

기준	가중사유	가중비율
위반의 정도	1. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개에 해당하는 경우	기준금액의 50% 이내
	2. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내

피심인의 법 제34조 위반행위에 대하여는 가중기준에 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 과태료 부과지침 제7조(과태료 감경)에 따라 의견제출 기간내 법규 위반행위를 시정하고, 자료제출 등 조사에 적극 협력한 점을 고려하여 기준금액의 50%인 300만원을 각각 감경한다.

< 과태료의 감경기준(제7조 관련) >

기준	감경사유	감경비율
조사 협조·자진 시정 등	1. 과태료의 사전 통지 및 의견 제출 기간 내에 법규 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

※ 과태료 부과지침 제7조에 따라 과태료의 감경은 기준금액의 50%를 초과할 수 없음

다. 최종 과태료

피심인이 보호법 제29조 및 제34조제1항을 위반한 행위에 대해 가중 및 감경사유를 적용한 금액인 360만원, 300만원을 합산하여 총 660만원의 과태료를 부과한다.

< 최종 과태료 산출내역(안) >

개인정보보호법		과태료 금액 (단위:만원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
법 제29조(안전조치의무) 위반	제75조제2항제6호	600	60	300	**360**
법 제34조(개인정보 유출통지등) 제1항 위반	제75조제2항제8호	600	-	300	**300**
계		1,200	60	600	**660**

☞ 피심인이 과태료 고지서를 송달받은 날부터 14일 이내에 과태료를 자진납부 하는 경우, 100분의 20을 감경함 (질서위반행위규제법 제18조 및 같은 법 시행령 제5조 준용)

3. 처분결과의 공표

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

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	안전조치의무 위반 (접근권한, 접근통제, 암호화, 접속기록, 악성프로그램)	2023. 5. 10.	과태료 360만 원
		법 제34조 제1항	개인정보 유출통지 위반		과태료 300만 원
2023년 5월 10일 개 인 정 보 보 호 위 원 회					

Ⅴ. 결론

피심인의 「개인정보 보호법」제24조제3항, 제24조의2제2항, 제29조, 제34조제1항 위반행위에 대하여 같은 법 제34조의2(과징금의 부과 등), 제66조(결과의 공표), 제75조(과태료) 제2항에 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.

2023년 5월 10일

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 홍 열　(서 명)

위　　원　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)