

개 인 정 보 보 호 위 원 회

심의 · 의결

안 건 번 호 제2025-001-001호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 법원행정처 (사업자등록번호 :)

의결연월일 2025. 1. 8.

주 문

1. 피심인 법원행정처에 대하여 다음과 같이 과징금과 과태료를 부과한다.
 - 가. 과 징 금 : 207,000,000원
 - 나. 과 태 료 : 6,000,000원
 - 다. 납부기한 : 고지서에 명시된 납부기한 이내
 - 라. 납부장소 : 한국은행 국고수납 대리점
2. 피심인 법원행정처에 대한 과태료 부과 내용 및 결과를 개인정보보호 위원회 홈페이지에 1년간 공표한다.

3. 피심인 법원행정처에 대하여 다음과 같이 징계를 권고한다.

가. 피심인은 본 건의 개인정보 보호법규 위반 행위에 책임이 있는 자에 대해 징계할 것.

나. 피심인은 가.의 징계권고에 따른 조치를 이행하고, 징계권고 통지를 받은 날로부터 30일 이내에 그 결과를 개인정보보호위원회에 통보할 것. 다만, 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보할 것.

4. 피심인 법원행정처에 대하여 다음과 같이 개선을 권고한다.

가. 피심인은 개인정보처리시스템 운영체계 및 조직·인력·예산, 관련 규정 등 보호체계 전반에 걸쳐 안전조치 실태를 점검하고, 개인정보 보호조치 수준 향상 방안을 마련할 것.

나. 피심인은 가.의 개선권고에 따른 조치를 이행하고, 개선권고 통지를 받은 날로부터 60일 이내에 개인정보보호위원회에 이행 결과 및 계획을 제출할 것. 다만, 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보할 것.

이 유

I. 기초 사실

피심인은 「舊 개인정보 보호법」(법률 제16930호, 2020.8.5. 시행, 이하 ‘보호법’이라 한다) 제2조제6호가목에 따른 공공기관으로, 같은 법 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	직원 수
법원행정처				

II. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인의 개인정보 유출신고('23. 12. 7.)에 따라 사실 조사를 진행('23. 12. 15.~'24. 12. 12.)하였으며, 피심인의 보호법 위반행위와 관련된 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 '24. 9. 13. 기준 아래와 같이 개인정보를 수집·보관하고 있다.

개인정보파일	수집·이용 항목	수집일	보유건수(명)

나. 개인정보 유출 관련 사실관계

1) **(유출 경위)** 신원 불상자(경찰,)가 '21. 1. 7. 이전 법원의 내·외부망이 연결된 포트를 이용해 내부망에 악성파일을 설치하고, '21. 6.~'23. 1. 서버(스토리지)에 저장된 데이터를 탈취한 것으로 추정되며

- 해킹에 이용된 외부 경유지 서버 8대(국내 4대, 국외 4대)로 약 1,014GB 분량의 데이터가 유출되었으며, 이 중 경찰 수사를 통해 국내 서버 1대에서 4.7GB의 파일(총 유출 데이터의 약 0.46% 분량)을 복원하였다.

2) **(유출 내용)** 문서에 기재된 정보주체의 개인정보*

* 이름(15,169명), 주민등록번호(2,010명), 생년월일(2,385명), 연락처(2,055명), 주소(4,275명), 나이(5,497명), 성별(943명) 등

※ 경찰이 복원에 성공한 4.7GB(5,171개 파일)을 전수조사한 결과, 자필 진술서, 등기사항전부증명서, 건강보험자격득실확인서, 혼인관계증명서, 진단서 등 총 731종 10,089개의 소송 관련 문서에서 17,998명의 개인정보 확인

<복원된 문서 예시>

3) (유출 인지 및 대응)

일시			유출 인지·대응 내용
2023	2.7.	00:01	서울중앙지법 스캔서버에서 악성파일(백도어) 탐지하여, 보안업체에 해당 악성파일 분석 의뢰
	2.7.		보안업체 분석 결과, 인터넷가상화웹서버에 웹쉘 추가 확인
	2.8.		인터넷가상화PC(외부망)에서 인터넷가상화웹서버(내부망)의 80포트 접근 차단
	2.9.		업무PC 3대, 인터넷가상화PC 4대에서 백도어 탐지
	3.10.		업무망과 인터넷망 간 대량의 데이터 통신 확인
	3.20.		인터넷가상화PC 2대에서 악성 사이트 접근 이력 확인
	4.7.		보안업체를 통해 침해사고 자체조사 결과 보고서 작성 ※ 내부망 스캔서버와 업무용PC 2대에서 데이터(관련 문서) 수집 흔적 및 335GB 이상의 내부 데이터의 외부 유출정황 인지
	11.30.		한 언론사가 관련 내용 보도
	12.7.	17:46	개인정보보호종합포털에 유출사실 신고 및 홈페이지에 유출사실 게시
2024	1.22.~ 5.19.		
	5.8.		
	6.13.~ 8.30.		유출 통지(문자 4,161명, 우편 9,016명) ※ 연락처가 확인되지 않는 4,821명은 홈페이지 공지로 갈음(8.30.~9.13.)

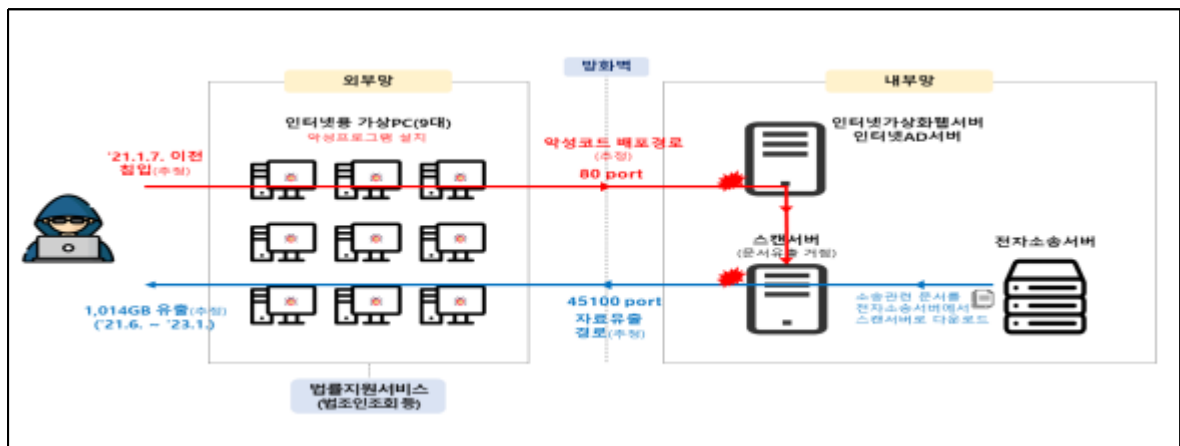
다. 기초사실

- 1) (고유식별정보<주민등록번호> 암호화 위반) 피심인은 소송 관련 문서를 PDF 파일로 변환하여 서버(스토리지)에 저장·보관하면서, 주민등록번호가 포함된 문서를 암호화하지 않은 사실이 있다.
- 2) (안전조치의무 위반) 피심인은 인터넷AD(Active Directory)서버 관리자 계정과 인터넷가상화PC 취급자 계정에 유추하기 쉬운 해당 계정의 초기 비밀번호를 변경없이 그대로 사용한 사실이 있다.

※

- 피심인은 IP주소 등의 분석 및 모니터링이 미흡하여 불법적인 개인정보 유출 시도를 탐지·차단하지 못한 사실이 있고
- 내부망-외부망 간 상호 접속이 가능하도록 불필요한 포트*를 개방하여 악성파일 배포 및 개인정보 유출 경로로 악용되게 한 사실이 있다.

* <80 포트> (내부망) 인터넷가상화웹(포털)서버-(외부망) 인터넷용가상PC 연결 (악성파일 배포 통로로 악용 / 소속직원 편의를 위해 인터넷용가상PC에서 법률지원서비스 등 배너를 별도 로그인 없이 사용 가능하도록 내부망 법원 업무포털 로그인 정보를 가져오기 위해 포트 개방, '14. 5. 7. 개방, '23. 2. 8. 차단
 <45100 포트> (내부망) 스캔서버-(외부망) 인터넷용가상PC 연결(개인정보 유출 경로로 악용) '14. 4. 17. 개방, '23. 3. 16. 차단



- 피심인은 내부망에 위치한 '인터넷 가상화 웹서버'에 백신 소프트웨어 등 보안프로그램을 설치하지 않고 운영한 사실이 있다.
- ※ 악성 파일이 탐지된 이후인 '23. 2. 8.부터 보안프로그램 설치·운영 중

3) (유출 통지·신고 의무 위반) 피심인은 보안업체를 통해 침해사고 자체 조사를 진행하여 '23. 4. 7. 보안업체 조사 결과 보고서*를 통해 법원 전산망에서 개인정보가 유출된 정황을 인지하였으나,

* 보안업체 보고서에는 내부망 스캔서버와 업무용PC 2대에서 데이터(관련 문서) 수집 흔적 및 335GB 이상의 내부 데이터 외부 유출 정황이 기재

- '23. 11. 30. 한 언론사에서 관련 내용이 보도된 이후인 '23. 12. 7. 개인정보 유출 사실을 신고하고 홈페이지에 유출 관련 안내문을 게시한 사실이 있다.

Ⅲ. 법령 근거 및 위법성 판단

1. 고유식별정보 처리 제한(§24③), 주민등록번호 처리 제한(§24의2②), 안전조치의무(§29) 위반

가. 법령 근거

보호법 제24조제3항은 “개인정보처리자가 제1항 각 호에 따라 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 제24조의2제2항은 “개인정보처리자가 제1항 각 호에 따라 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 있으며, 같은 법 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(대통령령 제32813호, 2022.10.20. 시행, 이하 ‘시행령’이라 한다) 제30조제1항은 “개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다”라고 규정하며 제2호에서 “개인정보에 대한 접근 통제 및 접근 권한의 제한 조치”, 제3호에서 “개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치”, 제5호에서 “개인정보에 대한 보안프로그램의 설치 및 갱신”을 규정하고 있다.

아울러, 舊 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회고시 제2021-2호, 2021.9.15. 시행, 이하 ‘고시’라 한다) 제5조제5항은 “개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수

있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.”라고 규정하고 있고, 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해 사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.”라고 규정하며 제2호에서 “개인정보처리시스템에 접속한 IP (Internet Protocol) 주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응”을 규정하고 있다. 또한, 제6조제3항은 “개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.”라고 규정하고 있고, 제9조는 “개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.”고 규정하고 있다.

나. 위법성 판단

1) 고유식별정보 처리 제한 및 주민등록번호 처리 제한 위반

[보호법 제24조(고유식별정보의 처리 제한), 제24조의2(주민등록번호 처리의 제한)]

피심인이 소송 관련 문서를 PDF 파일로 변환하여 서버(스토리지)에 저장·보관하면서, 주민등록번호가 포함된 문서를 암호화하지 않은 행위는 보호법 제24조제3항 및 제24조의2제2항을 위반한 것이다.

2) 고유식별정보 처리 제한 및 안전조치의무 위반

[보호법 제24조(고유식별정보의 처리 제한), 제29(안전조치의무)]

(접근권한) '16. 8. 13. ~ '23. 3. 20. 동안 피심인이 인터넷AD서버 관리자 계정과 인터넷가상화PC 취급자 계정의 비밀번호를 유추하기 쉬운 해당 계정의 초기 비밀번호를 변경 없이 그대로 사용한 행위는 보호법 제24조제3항 및 제29조, 같은 법 시행령 제30조제1항, 고시 제5조제5항을 위반한 것이다.

(접근통제) 피심인이 IP주소 등의 분석 및 모니터링이 미흡하여 불법적인 개인정보 유출 시도를 탐지·차단하지 못 한 행위는 보호법 제24조제3항 및 제29조, 시행령 제30조제1항, 고시 제6조제1항제2호를 위반한 것이고,

'14. 5. 7. ~ '23. 3. 16. 동안 내부망-외부망 간 상호 접속이 가능하도록 불필요한 포트를 개방하여 악성파일 배포 및 개인정보 유출 경로로 악용되게 한 행위는 보호법 제24조제3항 및 제29조, 시행령 제30조제1항, 고시 제6조제3항을 위반한 것이다.

(악성프로그램 방지) '16. 8. 13. ~ '23. 2. 8. 동안 피심인이 내부망에 위치한 '인터넷 가상화 웹서버'에 보안 프로그램을 설치하지 않고 운영한 행위는 보호법 제24조제3항 및 제29조, 시행령 제30조제1항, 고시 제9조를 위반한 것이다.

2. 유출 통지·신고 의무(§34①·③) 위반

가. 법령 근거

보호법 제34조제1항은 “개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.”라고 규정하고 있고, 같은 법 제34조제3항은 “개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다.”라고 규정하고 있다.

나. 위법성 판단

피심인이 보안업체를 통해 침해사고 자체조사를 진행하여 '23. 4. 7. 보안업체 보고서를 통해 법원 전산망에서 개인정보 유출 정황을 인지하였음에도, '23. 12. 7. 개인정보 유출 사실을 신고하고 홈페이지에 유출 관련 안내문을 게시한 행위는 보호법 제34조제1항·제3항을 위반한 것이다.

IV. 처분의 사전통지·의견 수렴 및 검토

개인정보보호위원회는 '24. 12. 13. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였고, 피심인은 '24. 12. 27. 개인정보보호위원회에 아래와 같이 의견을 제출하였다.

피심인은 본 건 개인정보 유출사고에 관하여 사안의 중대성과 심각성을 철저히 인식하고 있고, 이번 조사 과정에서 밝혀진 사실관계를 기초로 개인정보 보호법령의 위반의 점이 있다면 이를 적극적으로 시정하고 개선하겠다며, 과징금·과태료 처분 시 피심인이 개인정보보호위원회의 조사에 적극 협조하고 관련 자료를 성실히 제출한 점 등을 참작하여 감경·감액해 줄 것을 요청하였다.

※ 피심인은 과징금 산정 시 감경 기준 사유 중 하나인 '정보보호 관리체계(ISMS) 인증'('20. 5. 27. ~ '23. 5. 26.) 증빙자료도 제출

한편, 사전통지에 관하여 피심인이 자체 검토한 의견을 참작해 줄 것을 요청하였고, 주요 내용 및 개인정보보호위원회 검토 결과는 아래와 같다.

1. (피심인 의견 : 개인정보처리자 지위 관련) 법원행정처는 「민사소송 등에서의 전자문서 이용 등에 관한 법률」(이하 '민소전자문서법') 제4조(전산정보처리시스템의 운영)*에 따라 법률에 따른 재판업무를 수행하기 위하여 ' 시스템'을 운영하고 있을 뿐이며,

* **민소전자문서법 제4조**(전산정보처리시스템의 운영) 법원행정처장은 전산정보처리시스템을 설치·운영한다.

- 시스템은 재판사무를 전자적으로 수행하는 매개체에 불과하고, 자료에 포함된 개인정보의 처리 주체는 수소법원이며 법원행정처는 소송자료에 어떠한 개인정보가 있는지도 알 수 없으므로 개인정보처리자가 아니다.

- 한편, 최근 대법원은 “개개의 사건에 대하여 재판사무를 담당하는 법원(수소법원)은 개인정보처리자에서 제외된다”고 판시하였다.(대법원 2024.12.12. 선고 2021도12868 판결)

⇒ (검토 결과 : 불수용) 피심인은 법원조직법 제19조*에 근거하여 법원의 송무·등기·가족관계등록 등 사법행정사무를 관장하기 위하여 설치된 기관으로서 보호법 제2조제6호가목의 공공기관에 해당하고, 사법행정사무의 하나로 민소전자문서법 제4조에 따라 재판사무와 밀접하게 관련된 ‘시스템’을 설치·운영하면서 주민등록번호 등 개인정보가 포함된 문서를 처리하는 공공기관이므로 보호법 제2조제5호의 개인정보처리자에 해당하고

*** 법원조직법 제19조(법원행정처)**

- ① 사법행정사무를 관장하기 위하여 대법원에 법원행정처를 둔다.
- ② 법원행정처는 법원의 인사·예산·회계·시설·통계·**송무(訟務)**·**등기**·**가족관계등록**·공탁·집행관·법무사·법령조사 및 사법제도연구에 관한 사무를 관장한다.

- 피심인은 법원의 사법행정사무 수행을 목적으로 설립된 기관으로, 소송 과정에서 처리되는 자료에 주민등록번호 등 개인정보가 포함되어 있을 가능성을 충분히 인지할 수 있다.
- 피심인이 제시한 대법원 판례(대법원 2024.12.12. 선고 2021도12868 판결)는 “행정사무를 처리하는 기관”으로서의 법원과 ‘재판사무를 처리하는 기관’으로서의 법원의 구별 등을 종합하여 보면, 개개의 사건에 대하여 재판사무를 담당하는 법원(수소법원)은 개인정보처리자에서 제외된다”고 하여, 후자인 ‘재판사무를 처리하는 기관’으로서의 법원에 대해 개인정보처리자성을 부정한 것이지, 사법행정사무를 처리하는 법원행정처의 개인정보처리자성을 부정한 것은 아니며, 법원의 행정사무를 처리하는 기관인 법원행정처를 개인정보처리자로 보지 않을 경우 매우 민감한 개인정보가 다수 포함된 문서의 관리 및 보호법상 의무 이행에 있어 공백이 발생할 위험이 크고, 국민의 개인정보에 관한 권리를 보장함에 있어 큰 어려움이 예상되므로 피심인 의견을 불수용한다.

2. (피심인 의견 : 개인정보 처리 관련) 법원행정처는 시스템을 운영하면서 개인정보가 포함된 전자문서를 저장·유통하는 등을 지원 하는 역할을 할 뿐이지 전자문서에 포함된 개인정보를 ‘처리’하지 않는다.

※ 법원행정처는 ‘舊 개인정보 보호 법령 및 지침·고시 해설’의 “다른 사람이 처리하고 있는 개인정보를 단순히 전달, 전송 또는 통과만 시켜주는 행위는 처리에 해당하지 않는다” 문구를 인용하면서, ‘ 시스템’ 운영은 우편배달사업자, 인터넷서비스제공자 등과 같이 개인정보를 단순 전달, 전송하는 것에 불과하여 개인정보 처리가 아니라는 입장임

⇒ (검토 결과 : 불수용) 보호법 제2조제2호는 개인정보 ‘처리’의 개념을 폭 넓게 인정하고 있으며 개인정보의 저장·보유 행위도 ‘처리’로 정의하고 있고

- 피심인이 행정사무를 목적으로 시스템을 운영하면서 주민등록 번호 등 개인정보가 포함된 소송문서를 저장·보관, 관리한 것은 개인정보의 ‘처리’에 해당하므로 피심인 의견을 불수용한다.

※ 피심인이 인용한 해설서의 ‘단순 전달·전송 행위는 개인정보 처리에 해당 하지 않는다’는 문구는 ‘다른 사람’이 처리하고 있는 개인정보를 제3자가 전달·전송하는 것을 전제로 하며, 법원행정처는 법원조직법 제19조에 근거 하여 법원의 ‘행정사무를 처리하는 기관’으로서 법원 내 설립된 행정기관 으로, ‘재판사무를 처리하는 기관’인 법원과 ‘다른 사람’에 해당하지 않아 본 건에 적용하기 어려움

3. (피심인 의견 : 주민등록번호 암호화 관련) 시스템에 저장된 것은 소송자료인 전자문서이지 주민등록번호 자체를 전자적인 방법으로 보관하는 것이 아니므로 암호화 대상이 아니며, 전자문서에 개인정보가 포함되어 있다는 이유로 암호화해야 한다면 신속하고 효율적인 형태의 구현·유지가 어렵다.

⇒ (검토 결과 : 불수용) 주민등록번호 암호화 대상은 주민등록번호만을 별도로 전자적인 방법으로 보관하는 것에 한정되지 않고 주민등록번호가 포함된 문서 등의 형태도 포함한다.

- 법원행정처가 주민등록번호가 포함된 소송문서를 PDF 파일로 변환하여 서버에 저장·보관하는 행위는 주민등록번호를 전자적인 방법으로 보관하는 행위에 포함되고 보호법 제24조의2(주민등록번호 처리의 제한)의 암호화 대상이며
- 단순히 신속하고 효율적인 업무를 위해 주민등록번호가 포함된 소송문서를 암호화하기 어렵다는 주장은 수용하기 어려워 피심인 의견을 불수용한다.

4. (피심인 의견 : 유출 신고·통지 관련) 법원행정처는 '23. 4. 7. 보안업체를 통한 침해사고 자체조사 결과 보고서에서 해커가 사법부 전산망에 침입하여 사법부 내부망에 위치한 스캔서버 등에서 수집한 데이터 약 335GB가 외부로 유출된 정황은 확인하였으나, 유출 데이터의 상세 내용이 확인되지 않아 개인정보가 유출되었음을 알 수 없어 당시 유출 통지·신고 의무가 발생한 것은 아니며,

- '23. 12. 7. 개인정보 유출 신고를 하고 홈페이지에 유출 관련 안내문을 게시한 것은 선제적·자발적 조치를 취한 것일 뿐이다.

⇒ (검토 결과 : 불수용) 스캔서버에는 다량의 소송문서가 저장되어 있었으므로 유출된 데이터에는 당연히 다수 정보주체의 개인정보가 포함되어 있다는 것을 충분히 알 수 있었고,

- 피심인이 '23. 12. 7. 에서야 유출 신고 및 홈페이지를 통해 유출 안내문을 게시한 것은 '23. 11. 30. 보안업체 자체조사 결과 보고서를 입수한 한 언론사에서 관련 내용이 보도*되자 신고·통지한 것으로 유출 신고·통지 의무 위반이므로 피심인 의견을 불수용한다.

*

5. (피심인 의견 : 안전조치의무 위반 관련) 유추하기 쉬운 계정의 초기 비밀번호를 변경없이 그대로 사용한 인터넷AD서버와 인터넷가상화PC는

직접 개인정보를 보관하거나 처리하는 개인정보처리시스템에 해당하지 않아 보호법상 안전조치의무 대상이 아니다.

⇒ (검토 결과 : 불수용) 舊 「개인정보의 안전성 확보조치 기준」 제5조제5항은 개인정보처리시스템을 전제로 하지 않으므로 피심인 의견을 불수용한다.

*** (舊)개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)**

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

- 아울러, 인터넷AD서버는 개인정보취급자에 대한 접근권한을 부여하고 그 직원들의 개인정보를 처리한다는 측면에서 개인정보처리시스템에 해당하고, 인터넷가상화PC 역시 개인정보취급자가 사용하는 PC이므로 고시 제5조제5항에 따라 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

V. 처분 및 결정

1. 과징금 부과

보호법 제34조의2에 따라 주민등록번호가 유출된 경우로서 안전성 조치를 다하지 않은 경우에는 과징금을 부과할 수 있으며,

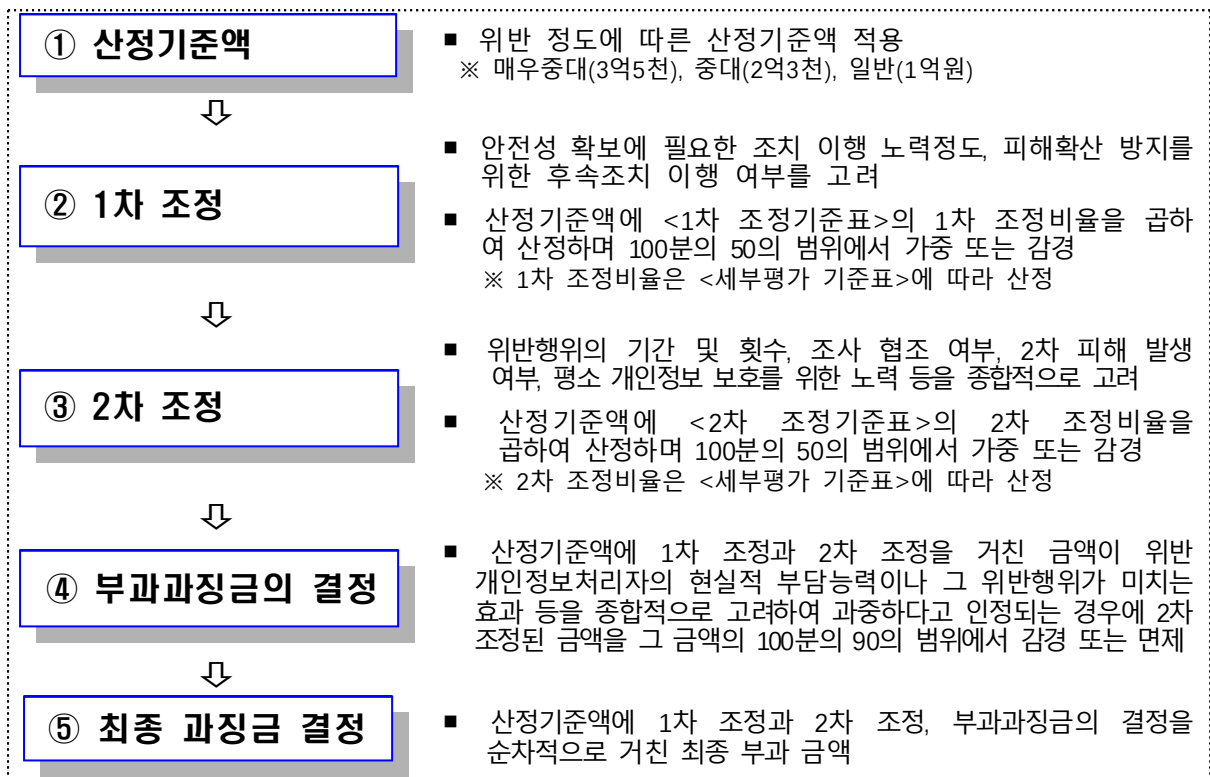
- 피심인의 보호법 제24조제3항(고유식별정보의 처리 제한), 제24조의2제2항(주민등록번호 처리의 제한), 제29조(안전조치의무) 위반행위에 대해 같은 법 제34조의2, 시행령 제40조의2제1항 [별표 1의3] 및 舊 「주민등록번호 유출 등에 대한 과징금 부과기준」에 따라 총 2억 700만원의 과징금을 부과함

※ <중과실 판단> 의도적으로 소속직원 편의를 위해 내부망-외부망 간 불필요한 포트를 개방하고, 내부망 인터넷가상화웹서버에 보안프로그램 미설치, 주민번호 암호화 미조치 등으로 인해 대량의 소송 문서가 유출된 점을 고려할 때 중대한 위반행위에 해당하는 중과실로 판단

<과징금 산출 내역>

①기준금액	②1차 조정	③2차 조정	④최종과징금
<ul style="list-style-type: none"> •중대한 위반 행위(고의 또는 중과실로 인하여 10만건 미만의 주민번호 유출) (2억 3천만원) 	<ul style="list-style-type: none"> •주민번호 접근통제, 접근 권한 관리 부실 •주민번호 저장 시 암호화 위반 •일부 서버 보안프로그램 미설치 •개인정보 유출 통지신고 위반 	<ul style="list-style-type: none"> •위반기간 6개월 초과 •개인정보 보호 노력 * 피심인은 '20. 5. 27. 정보 보호 관리체계(ISMS) 인증 (20. 5. 27.~'23. 5. 26.)을 받음 	2억 700만원
⇒ 2억 3천만원	⇒ 2억 7,600만원(20% 가중)	⇒ 2억 700만원(25% 감경)	

< 주민등록번호 유출 등에 대한 과징금 부과기준에 따른 과징금 산정 절차 >



① (기준금액 산정) 과징금 부과기준 제4조에 따라 위반 정도가 '중대한 위반행위'에 해당하여 2억3천만원을 적용함

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

- ② (1차 조정) 과징금 부과기준 제5조의 세부평가 기준표에 따른 산정 점수가 2.2점에 해당하여 기준금액의 20%인 4,600만원을 가중함

< 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 >

부과점수		고려사항	비중	3점	2점	1점
안 전 성 확 보 조 치	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 하 지 아니하거나 현저히 부실하 게 한 경우 1. 접근통제 2. 접근권한의 관리	3점 또는 2점에 해 당되지 않는 경우	
	암호화	0.2	주민등록번호의 송신·전달·저 장 시 이를 암호화 하지 아 니한 경우	주민등록번호를 안전한 암호화 알고리즘으로 암호화하지 않은 경우	3점 또는 2점에 해 당되지 않는 경우	
	보안 프로그램	0.2	악성프로그램 등을 방지·치료 할 수 있는 보안프로그램을 설치·운영하지 않은 경우	보안프로그램에 대한 업데이트 를 실시하지 아니하여 최신의 상태로 유지하지 않은 경우	3점 또는 2점에 해 당되지 않는 경우	
	접속기록의 보관 등	0.2	개인정보처리시스템의 접속 기록 보관 및 위조·변조 등 방지를 위한 조치를 하지 아 니하고, 주민등록번호를 보관 하는 물리적 보관장소를 별 도로 두지 아니하거나 잠금 장치를 하지 않은 경우	개인정보처리시스템의 접속기 록 보관 및 위조·변조 등 방지 를 위한 조치를 하지 아니하거 나, 주민등록번호에 대한 물리 적 보관장소를 별도로 두지 않 는 등 물리적 안전조치가 없는 경우	3점 또는 2점에 해 당되지 않는 경우	
피해 방지 후속 조치 등		0.2	개인정보가 유출되었음을 알 게 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 해 당되지 않는 경우	

- ③ (2차 조정) 과징금 부과기준 제6조의 세부평가 기준표에 따른 산정 점수가 1.4점에 해당하여 1차 조정된 금액(2억 7,600만원)의 25%인 6,900만원을 감액함

< 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 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 1. 개인정보보호 인증*을 받은 경우 등

* 피심인은 '20. 5. 27. 정보보호 관리체계(ISMS) 인증('20. 5. 27.~'23. 5. 26.)을 받음

- ④ (부과과징금의 결정) 과징금 부과기준 제8조(부과과징금의 결정)의 감경 또는 면제 기준에 해당하지 않아 2차 조정금액인 2억 700만원을 유지함

감경 기준 (§8①)	1. 위반행위자가 과징금을 부담할 능력이 현저히 부족하다고 객관적으로 인정되는 경우 2. 정보주체에게 발생한 피해에 대한 원상회복, 손해배상 등 피해구제 조치를 한 경우 3. 경제위기 등으로 위반행위자가 속한 시장·산업 여건이 지속적으로 악화된 상태인 경우 4. 위반행위로 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 경우 5. 기타 제1호 내지 제4호에 준하는 사유가 있어 과징금의 감액이 불가피하다고 인정되는 경우
면제 기준 (§8②)	1. 위반행위자가 객관적으로 과징금을 낼 능력이 없다고 인정되는 경우 2. 정보주체에게 피해가 발생하지 않았거나 경미한 경우로서 다음 어느 하나에 해당하는 경우 가. 2차 조정된 금액이 300만원 이하인 경우 나. 사소한 부주의나 오류로 인한 위반행위인 경우 다. 개인정보가 유출된 경우로서 유출된 정보주체의 수가 100명 미만인 경우 3. 위반행위자 본인의 행위가 위법하지 않은 것으로 잘못 인식할 만한 정당한 사유가 있는 경우

- ⑤ 피심인이 보호법 제24조제3항을 위반한 행위에 대해 1·2차 조정 및 부과과징금의 결정을 통하여 2억 700만원의 과징금을 부과함

기준 금액	1차 조정	2차 조정	부과 과징금 결정	최종 과징금
2억3천만원	2억 7,600만원	2억 700만원	2억 700만원	2억 700만원
중대한 위반행위	1차 산정점수 2.2점 ⇒ 20%(4,600만원) 가중	2차 산정점수 1.4점 ⇒ 25%(6,900만원) 감경	면제·감경 사유 없음 ⇒ 2차 조정금액 유지	

2. 과태료 부과

피심인의 보호법 제34조제1항·제3항(개인정보 유출 통지·신고) 위반행위에 대해 같은 법 제75조제2항제8호·제9호, 시행령 제63조 [별표2] 및 舊 「개인정보 보호법 위반에 대한 과태료 부과기준」에 따라 총 600만원의 과태료를 부과함

※ ‘보호법 제34조의2에 따라 과징금을 부과한 행위에 대해서는 과태료를 부과할 수 없다’고 규정한 보호법 제76조(과태료 특례)에 따라, 주민등록번호 유출로 인한 과징금 부과 대상에 해당하는 피심인의 위반행위(고유식별정보 <주민등록번호> 처리 제한 위반, 안전조치의무 위반)에 대한 과태료는 미부과

< 신규 과태료 산출내역 비교 >

구분	기준 금액	舊 과태료 부과기준			現 과태료 부과기준		
		가중	감경	소계	가중	감경	계
§34① (개인 정보 유출 통지)	적용 비중 600 만원	-	-50%(최대)	-50%	-	-40%	-40%
	적용 근거	-	▲시정 완료(50%이내) ▲조사 협조(40%이내)	-300만 원	-	▲시정 완료(20%이내) + 조사 협조(20%이내)	-240만 원
§34③ (개인 정보 유출 신고)	적용 비중 600 만원	-	-50%(최대)	-50%	-	-40%	-40%
	적용 근거	-	▲시정 완료(50%이내) ▲조사 협조(40%이내)	-300만 원	-	▲시정 완료(20%이내) + 조사 협조(20%이내)	-240만 원
총계		600만 원			720만 원		

※ 행위 당시 부과기준 우선 적용하되, 新 기준에 의한 부과금액이 더 적은 경우 新 기준 적용

3. 처분결과 공표

보호법 제66조(결과의 공표) 및 舊 「개인정보 보호위원회 처분결과 공표 기준」 제2조제4호(보호법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우)에 해당하는 피심인의 위반행위에 대해 과태료 부과 내용 및 결과를 개인정보보호위원회 홈페이지에 1년간 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	법원행정처	舊 보호법* 제34조 제1항	개인정보 유출통지 위반	2025. 1. 8.	과태료 300만 원
		舊 보호법 제34조 제3항	개인정보 유출신고 위반		과태료 300만 원
* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호					
2025년 1월 8일 개 인 정 보 보 호 위 원 회					

4. 징계권고

피심인에 대하여 피심인의 핵심적인 보호법 위반 사항으로 소속직원 편의를 위해 인터넷용가상PC에서 법률지원서비스 등 배너를 별도 로그인 없이 사용 가능하도록 내부망-외부망 간 불필요한 포트를 개방하고, 인터넷가상화웹 서버에 백신 소프트웨어 등 보안프로그램을 설치하지 않고 운영하는 등 안전 조치를 다하지 않아, 고유식별정보(주민등록번호) 등 개인정보가 포함된 대량의 소송 관련 문서가 유출되게 한 개인정보 보호법규 위반 행위에 대해 보호법 제65조제2항(고발 및 징계권고) 및 舊 「개인정보 보호 법규 위반에 대한 징계권고 기준」 제3조제1항제4호*에 따라 다음과 같이 징계를 권고한다.

* 위반행위의 대상이 된 개인정보가 제24조제1항에 따른 고유식별정보로서 정보 주체의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 경우

가. 피심인은 본 건의 개인정보 보호법규 위반 행위에 책임이 있는 자에 대해 징계할 것.

나. 피심인은 가.의 징계권고에 따른 조치를 이행하고, 징계권고 통지를 받은 날로부터 30일 이내에 그 결과를 개인정보보호위원회에 통보할 것. 다만, 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보할 것.

5. 개선권고

피심인이 다량의 개인정보를 처리하고 있는 점을 감안하여 보호법 제61조 제2항에 따라 다음과 같이 개선을 권고한다.

가. 피심인은 개인정보처리시스템 운영체계 및 조직·인력·예산, 관련 규정 등 보호체계 전반에 걸쳐 안전조치 실태를 점검하고, 개인정보 보호조치 수준 향상 방안을 마련할 것.

나. 피심인은 가.의 개선권고에 따른 조치를 이행하고, 개선권고 통지를 받은 날로부터 60일 이내에 개인정보보호위원회에 이행 결과 및 계획을 제출할 것. 다만, 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보할 것.

VI. 결론

피심인의 보호법 제24조제3항, 제24조의2제2항, 제29조, 제34조제1항·제3항 위반행위에 대하여 같은 법 제34조의2(과징금의 부과 등), 제61조(의견제시 및 개선권고), 제65조(고발 및 징계권고), 제66조(결과의 공표), 제75조(과태료)에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 과징금 부과처분, 공표에 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 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.

2025년 1월 8일

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 환 (서 명)

위 원 박 상 희 (서 명)

위 원 윤 영 미 (서 명)

위 원 이 문 한 (서 명)