개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2023-008-077호 (사건번호 : 2020조총0004)

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2023. 5. 10.

주 문

피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

피심인은 「개인정보 보호법」(‘이하 “보호법”이라 한다.) 제2조제6호에 따른 공공기관으로, 같은 법 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

개인정보보호위원회는 개인정보 유출신고와 관련하여 피심인의 「개인정보 보호법」 위반 여부에 대한 사실조사(’20.12.4.~’21.2.17.) 결과, 다음과 같은 사실을 확인하였다.

1. 행위 사실

가. 개인정보 수집 현황

피심인은 전자연구노트시스템을 운영하면서 ’20. 12. 9. 기준 30,616건의 개인정보를 수집·보관하고 있다.

< 개인정보 수집현황 >

개인정보파일	수집·이용 항목	수집기간	보유건수(명)
연구노트 이용자 정보 (전자연구노트시스템*)	(필수) 이름, 이메일, 아이디, 학번/사번, 부서/학과, 신분(직급)	‘16.12.15 ~ 20.12.8	30,616

* 근거 법령 : 「국가연구개발 혁신법」 제35조, 「국가연구개발사업 연구노트 지침」 제10조 등

나. 개인정보 유출 관련 사실관계

1) 유출 규모 및 항목

①총 30,607명의 이름, 아이디, 이메일, 부서/학과, 사번/학번, 신분(직급), ②총 63개의 이메일 계정(아이디, 비밀번호)

2) 유출 경위

미상의 해커가 피싱 메일 11종*을 피심인의 교직원·학생 등 125개 이메일 계정에 발송('20.11.4~11.24)하여 이 중 63개 계정에서 비정상** 로그인 형태를 보였으며, 해커는 탈취한 이메일 계정에 접속하여 VPN 계정***, 서버접속 정보 등을 획득한 것으로 추정된다.

* **(8종)** 클릭 시 접속장애 메시지 현출, 이후 다시 이메일 로그인 화면(피싱 페이지)이 뜨면서 ID·PW 입력 유도
(3종) 정보유출을 위한 악성코드가 담긴 첨부파일(v3, 보안플러그인) 설치 유도

** ① 한 개의 IP에서 30분 내 여러 메일 계정으로 로그인, ② 여러 IP에서 동시에 한 메일 계정으로 로그인, ③ 확보한 악성 IP 그룹에서 로그인 성공(블랙리스트, 특정국가IP, 특정 C&C IP), ④ 다수 국가에서 30분 내 메일 계정으로 로그인

*** 학술정보개발팀 유지보수 계정(kaist_diane813)

탈취한 VPN 계정을 이용하여 전자연구노트시스템이 속한 서버팜 내로 접속한 후 SVN 서버*를 경유하여 회의시스템 웹서버에 접속하여 DB클라이언트로 '연구노트 이용자 정보' 30,607건 탈취하여 개인정보가 유출되었다.

* '16년 11월, 외부작업을 위해 KVPN_group IP, 학술정보개발팀 대역 IP에 한하여 서버접근제어 시스템(Gateone) 경유 없이 SVN 서버에 접속할 수 있도록 허용하였으나, 같은 해 작업종료 후 즉시 삭제하지 않고, 유출 의심 사고 발생 후 '20.11.12. 삭제함

유출 추정 경로
(전자연구노트시스템)

①해커가 탈취한 VPN 계정* 이용 VPN 접속	⇒	②서버팜 내로 접속	⇒	③SVN서버를 경유하여 '회의시스템 웹서버에 접속	⇒	④ DB 클라인언트(Navicat)로 **도서관DB서버**의 테이블(PN_USER)* **30,607명 개인정보 탈취**
* _diane813		- '16년에 특정 IP*에 한해 서버접근제어시스템(Gateone)을 경유하지 않고 SVN서버에 접속할 수 있도록 허용 후 '20.11.12까지 미조치				* 전자연구노트시스템 이용자
'20.11.7. 22:09		SVN서버 접속 일시는 확인 불가		**11.10. 09:50**		**11.10. 10:41**

※ **(서버팜)** SVN서버, 회의시스템 웹서버, 도서관 DB서버 등 **총 114개로 구성**

※ **(SVN서버)** 도서관운영 WAS 소스 버전 관리 서버(libsource.kaist.ac.kr)

※ **(도서관DB서버)** **전자연구노트시스템**, 전자도서관, 연구성과관리(RIMS), 논문학술연구자료 공개시스템( ) 등 4개 시스템의 데이터 관리

3) 유출 인지 및 대응

일시		피심인의 유출 인지·대응 내용
2020.	11. 5.	으로부터 웜바이러스 피해(추정) 탐지 통보를 받아 공격 대상자를 특정하여 악성 IP 차단 등 조치
	11. 9.	공격자 확인 등 정밀 분석 실시
	11. 10.~ 11. 11.	전자연구노트시스템을 운영하는 학술정보개발팀 그룹에 속한 모든 VPN 계정 삭제(총 82개), 국정원 조사 시작
	11. 12.	SVN 서버에 적용되어 있던 'KVPN_Group IP, 학술정보개발팀 대역 IP' 방화벽 허용 정책 삭제
	11. 16.	전자연구노트시스템 서비스를 교내 IP 대역으로 축소
	11. 20.	VPN 접속 시 2차 인증수단(Google OTP) 추가
	11. 25.	교내 메일시스템 취약점 점검 후 JavaScript, 메일 Session 처리 SSO 연동 개선
	11. 26.	국정원에서 유출 의심 엑셀파일 일부를 보여주며 피심인의 것인지 문의
	11. 27.	국정원에서 문의한 파일이 피심인의 학술정보개발팀이 운영하는 서버 중 한 군데에 있는 사실 확인 / 국정원에 추가자료 요청
	12. 3.	국정원으로부터 유출 정보 엑셀화면 캡처파일을 전달받아 **유출사실 인지**
		개인정보 **유출 신고** 및 정보주체에게 **유출 통지**(이메일, 홈페이지 공지)
	12. 19.	전자연구노트시스템이 속한 도서관DB서버에 DB접근제어시스템 적용

2. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 2. 7. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 2. 27. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련 법 규정

가. 보호법 제26조제2항은 “개인정보의 처리 업무를 위탁하는 경우에는 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개하여야 한다”라고 규정하고 있다.

나. 보호법 제29조는 “개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 않도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다”라고 규정하고 있다.

같은 법 시행령 제30조제1항은 안전성 확보조치로 개인정보에 대한 접근 통제 및 접근권한의 제한 조치(2호), 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(4호)를 하도록 하고 있다.

같은 법 시행령 제30조제3항에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호, 이하 ‘고시’라고 한다.)에서는 “개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을

발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.“(제5조제4항), ”개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.“(제6조제1항), ”개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다.“(제8조제1항)라고 규정하고 있다.

2. 위법성 판단

가. 업무위탁에 따른 개인정보 처리제한 조치를 소홀히 한 행위

피심인은 개인정보의 처리 업무를 위탁하는 경우에는 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개하여야 하나, 전자연구노트시스템 유지보수를 목적으로 개인정보 처리 업무가 포함된 시스템 유지보수 업무를 위탁하면서 위탁하는 업무의 내용과 수탁자를 공개하지 않은 사실은「개인정보 보호법」제26조제2항 위반에 해당한다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용
업무위탁에 따른 개인정보의 처리제한	보호법 §26②	§28②	· 개인정보처리 업무를 위탁하는 개인정보처리자가 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개하지 않은 행위

나. 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며 다른 개인정보취급자와 공유되지 않도록 하여야 하고, 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP(Interner Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한하는

기능을 포함한 조치를 하여야 하고, 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 하나,

VPN 계정 “ _diane813”을 학술정보개발팀 직원 3명과 유지보수 업체 2곳(아르고넷, 비네아)이 공유하여 사용한 사실, ’16년 11월에 외부작업을 위하여 SVN 서버(114개 서버가 모인 서버팜 내 위치) 접근 시 특정 IP에 대하여 서버접근제한시스템(Gateone)을 거치지 않고 접근할 수 있게 허용하고 작업 종료 이후 즉시 삭제하지 않지 않은 사실, ’21.2.1. 이전까지 전자연구노트시스템 접속기록 중 ‘처리한 정보주체 정보, 수행업무’를 보관·관리하지 않은 사실은 보호법 제29조 위반에 해당한다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보 보호조치 위반(접근권한, 접근통제, 접속기록)	보호법 §29	§30①	· 개인정보처리시스템에 접속할 수 있는 사용자 계정을 다른 개인정보취급자와 공유한 행위(고시§5④) · 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하지않아 인가받지 않은 접근이 가능하도록 한 행위(고시§6①) · 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하지 않은 행위(고시§11②)

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조 위반행위에 대해 같은 법 제75조제2항제6호, 같은 법 시행령 제63조의 [별표2]「과태료 부과기준」에 따라 다음과 같이 총 360만 원의 과태료를 부과한다.

제26조제2항(업무위탁에 따른 개인정보의 처리 제한) 위반행위에 대해서는 의안번호 제2023-008-085(사건번호 2020조총0047)에서 같은 조항 위반행위와 병합하여 처분한다.

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 제29조(안전조치의무) 위반에 대해서 1회 위반에 해당하는 과태료인 600만 원을 적용한다.

< 과태료 부과기준, 개인정보보호법 시행령 제63조 [별표 2] >

위반행위	근거 법조문	과태료 금액(단위 : 만원)		
		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

나. 과태료의 가중

「개인정보보호법 위반에 대한 과태료 부과기준」(개인정보위 2023. 3. 8. 이하 '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 경우, 안전조치의무 위반에 대해 '제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상인 경우'에 해당하여 보호법 제29조 위반행위에 대해 기준금액의 10%인 60만 원을 가중한다.

< 과태료 가중기준(제8조 관련) >

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

다. 과태료의 감경

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.

피심인의 경우, 사전통지 전 위반사항에 대해 시정을 완료하고, 조사 기간 중 자료제출·진술 등 조사에 적극 협력한 점을 고려하여 과태료 부과지침 제7조의 과태료 감경기준에 따라 기준금액의 50%를 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

라. 최종 과태료

피심인의 개인정보 보호법 제29조 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 총 360만 원의 과태료를 부과한다.

< 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
제29조(안전성확보 조치 의무 위반)	법 제75조제2항제6호	600	60	300	**360**

V. 결론

피심인의 「개인정보 보호법」 제29조 위반행위에 대하여 같은 법 제75조(과태료)제2항제6호에 따라 과태료 부과 명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

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)