개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 제2024-221-666호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인

의결연월일 2024. 11. 4.

주 문

1. 피심인에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보처리시스템에 대한 접근통제, 접근권한 제한, 접속기록 보존·관리, 비밀번호 일방향 암호화 조치 등 보호법 제29조를 준수해야 한다.

나. 피심인은 보호법 제37조제1항을 준수하여 회원 탈퇴(동의철회) 기능을 마련해야 한다.

다. 피심인은 가., 나.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출해야 한다.

이 유

Ⅰ. 기초 사실

피심인은 66개 학회의 홈페이지와 42개 학회의 논문 투고 시스템을 구축·운영하는 「舊 개인정보 보호법」[1](이하 '舊 보호법'이라 한다)에 따른 개인정보 처리업무 수탁자이며, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

홈페이지 변조로 해킹 사실을 인지한 피심인이 유출 신고('23.1.27.)해옴에 따라 개인정보보호위원회는 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('23. 10. 16. ~ '24. 8. 13.) 하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 서비스를 운영하면서 '23. 1. 25. 기준 건의 개인정보를 수집하여 보관하고 있다.

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

< 개인정보 수집현황 >

구분	항목	기간	건수
계			

나. 개인정보 유출 관련 사실관계

피심인은 담당자 실수로 서버 접속정보(관리자 계정, 비밀번호 등)가 포함된 파일( )을 웹서버에 업로드하였는데, 해커가 노출되어 있던 해당 파일( ) 내 관리자 계정( )으로 접속하여 DB 접속정보(DB 관리자계정, 비밀번호)를 확인하고 DB 내 개인정보를 유출 후 삭제하였다. 또, 일부를 텔레그램에 게시하였다.

조사 결과, 피심인은 관리자 권한으로 접속할 수 있는 IP 주소 제한 등의 정책을 침입차단시스템에 설정하지 않았으며, 학회 담당자가 외부에서 관리자 페이지에 접속할 경우 아이디·비밀번호 외 안전한 인증수단을 적용하지 않았다.

개인정보취급자의 DB 접속기록을 보존·관리하지 않고, 비밀번호를 보안 강도가 낮은 암호 알고리즘(MD5 등)으로 암호화하여 저장하였다.

또, 논문투고시스템은 온라인 회원가입을 통해 개인정보를 수집했음에도 불구하고, 회원 탈퇴 기능을 마련하지 않은 사실이 있다.

1) (유출 규모 및 항목) 텔레그램에 공개된 22,245명의 개인정보**

* 해커가 조회했을 가능성이 있는 개인정보는 최대 42,244명

** ID, 암호화된 비밀번호, 이름, 이메일, 성별, 생일, 전화번호, 휴대전화, 주소, 소속

2) 유출 인지 및 대응

일시		피심인의 유출 인지·대응 내용
‘23. 1. 24	06:00	KISA에서 해킹 탐지 후 사실 확인 요청
‘23. 1. 25	08:57~	유출 인지, DB가 삭제되어 서비스 중지 및 원인 파악
’23. 1. 25	09:16	피심인이 등에서 KISA의 확인 요청 메일을 전달받음
‘23. 1. 25	09:20~	홈페이지 접속 차단, 서버 이미지 백업
‘23. 1. 27.	11:40	개인정보 유출 신고
’23. 2. 14.		KISA 분석보고서로 홈페이지 변조 및 개인정보 유출 등 피해경위 및 범위 확인
~’23. 2. 17.		시스템 관련 재발 방지조치
‘23. 2. 15.	16:59	32개 학회에 개인정보 유출사실 통지(이메일)
‘23. 2. 17.	13:10	개인정보 유출 통지(, 이메일)

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보의 안전조치 의무를 소홀히 한 사실

피심인은 서버에 대한 불법적인 접근 및 침해사고 방지를 위한 침입탐지·차단 시스템 정책 설정 등 운영을 소홀히 했으며, 학회 담당자가 외부에서 정보통신망을 통해 관리자 페이지에 접속할 때 안전한 인증수단을 적용하지 않고 시스템을 운영한 사실이 있다.

피심인은 관리자 계정 정보가 포함된 파일이 외부에 노출되는 취약점이 있었으나 조치하지 않고 운영하는 등 취약점 점검 및 개선 조치를 소홀히 하고 개인정보취급자가 시스템에 접속한 기록을 최소 1년 이상 접속기록을 보존·관리하지 않은 사실이 있다.

또, 피심인은 홈페이지 및 논문투고시스템 회원의 비밀번호 저장 시 보안 강도가 낮은 암호 알고리즘을 사용해 저장했으며 웹과 DB 관리자 계정의 비밀번호를 평문으로 설정 파일에 저장한 사실이 있다.

나. 개인정보 유출의 통지·신고를 소홀히 한 사실

피심인이 유출 사실 인지 후 유출통지 기한(처리자 기준 7일)을 경과하여 학회에 유출된 정보주체 명단, 유출 규모, 유출 항목 등을 메일로 알리고, 일부 학회 회원에게만 직접 유출통지한 사실이 있다.

다. 이용자 권리 보호를 소홀히 한 사실

피심인이 학회 홈페이지와 논문투고시스템을 개발·운영하면서 논문투고시스템에는 회원 탈퇴 기능을 마련하지 않은 사실이 있다.

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 '24. 8. 20. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 8. 22. 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 시행령[2](이하 '舊 시행령'이라 한다) 제48조의2제1항제2호는 "개인정보에 대한 불법적인 접근을 차단하기 위해 '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)' 등의 조치를 하여야 한다."라고 규정하고 있다. 또한, 같은 조 제3항은 "제1항에 따른 안전성 확보조치에 관한 세부 기준은 보호

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

위원회가 정하여 고시한다.”라고 규정하고 있다.

한편, 舊 시행령 제48조의2제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 舊 개인정보의 기술적·관리적 보호조치 기준[3](이하 ‘舊 기술적 보호조치 기준’이라 한다) 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있다.

또, 舊 기술적 보호조치 기준 제4조제4항은 “정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.”라고 규정하고 있다.

舊 기술적 보호조치 기준 제4조제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있다.

舊 기술적 보호조치 기준 해설서는 舊 기술적 보호조치 기준 제4조제9항에 대해 “인터넷 홈페이지를 통한 개인정보 유·노출 방지를 위해 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안기술 적용, 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.

그리고, 舊 기술적 보호조치 기준 제5조제1항은 “정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속

3) 개인정보보호위원회고시 제2021-3호, 2021. 9. 15. 시행

기록을 보존·관리하여야 한다.”라고 규정하고 있다.

舊 기술적 보호조치 기준 제6조제1항은 “정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.”라고 규정하고 있다.

나. 舊 보호법 제34조제1항은 “개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 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 피해 구제절차, 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처를 알려야 한다.라고 규정하고 있다.

다. 舊 보호법 제37조제1항은 ”정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다. 이 경우 공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.“라고 규정하고 있다.

같은 법 시행령 제44조제1항은 ”정보주체는 법 제37조제1항에 따라 개인정보처리자에게 자신의 개인정보 처리의 정지를 요구하려면 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다. 이 경우 개인정보처리자가 개인정보의 처리 정지 요구 방법과 절차를 마련할 때에는 제41조제2항을 준용하되, “열람”은 “처리 정지”로 본다.“라고 규정하고 있으며,

같은 법 시행령 제41조제2항은 ”개인정보처리자는 제1항에 따른 열람 요구 방법과 절차를 마련하는 경우 해당 개인정보의 수집 방법과 절차에 비하여 어렵지 아니하도록 다음 각 호의 사항을 준수하여야 한다.“라고 규정하면서, 제3호에서 ”인터넷 홈페이지를 운영하는 개인정보처리자는 홈페이지에 열람 요구 방법과 절차를 공개할 것“이라고 규정하고 있다.

2. 위법성 판단

가. 개인정보의 안전조치 의무를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

피심인이 서버에 대한 불법적인 접근 및 침해사고 방지를 위한 침입탐지·차단 시스템 정책 설정 등 운영을 소홀히 한 행위는 舊 보호법 제29조, 같은 법 시행령 제48조의2제1항 및 舊 기술적 보호조치 기준 제4조제5항 위반으로 판단되며 개인정보취급자인 학회 담당자가 외부에서 정보통신망을 통해 관리자 페이지에 접속 후 개인정보를 처리할 때, 안전한 인증수단을 적용하지 않고 시스템을 운영한 행위는 舊 기술적 보호조치 기준 제4조제4항 위반으로 판단된다.

관리자 계정 정보가 포함된 파일이 외부에 노출되는 취약점이 있었으나 조치하지 않고 운영하는 등 취약점 점검 및 개선 조치를 소홀히 한 행위는 舊 기술적 보호조치 기준 제4조제9항 위반으로 판단되고 개인정보취급자가 시스템에 접속한 기록을 최소 1년 이상 접속기록을 보존·관리하지 않은 행위는 舊 기술적 보호조치 기준 제5조제1항 위반으로 판단된다.

또, 홈페이지 및 논문투고시스템 회원의 비밀번호 저장 시 보안 강도가 낮은 암호 알고리즘을 사용해 저장하고 웹과 DB 관리자 계정의 비밀번호를 평문으로 설정 파일에 저장한 행위는 舊 기술적 보호조치 기준 제6조제1항 위반으로 판단된다.

나. 개인정보 유출의 통지·신고를 소홀히 한 행위

[舊 보호법 제34조(개인정보 유출 통지 등) 제1항]

피심인이 유출 사실 인지 후 유출통지 기한(처리자 기준 7일)을 경과하여 학회에 유출된 정보주체 명단, 유출 규모, 유출 항목 등 자세한 사항을 알리고 일부 학회 회원에게만 직접 유출통지한 사실을 고려할 때, 舊 보호법 제34조제1항 위반으로 판단된다.

다. 이용자 권리 보호를 소홀히 한 행위

[舊 보호법 제37조(개인정보의 처리정지 등) 제1항]

피심인이 학회 홈페이지와 논문투고시스템을 개발·운영하면서 회원 탈퇴 기능을 마련하지 않은 행위는 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다라고 규정한 舊 보호법 제37조제1항 위반으로 판단된다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(舊 기술적 보호조치 기준 등)
안전조치의무 위반	舊 보호법 §29	舊 시행령 §28의2①	• 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 처리시스템 등에 필요한 조치를 소홀히 함
개인정보 유출 통지 등	舊 보호법 §34①		• 개인정보 유출 사실 인지 이후 정당한 사유 없이 7일을 경과하여 유출 통지함
개인정보의 처리정지 위반	舊 보호법 §37①		• 회원 탈퇴 기능을 마련하지 않음

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인에 대하여 다음과 같이 시정조치를 명한다.

1) 피심인은 개인정보처리시스템에 대한 접근통제, 접근권한 제한, 접속기록 보존·관리, 비밀번호 일방향 암호화 조치 등 보호법 제29조를 준수할 것

2) 피심인은 보호법 제37조제1항을 준수하여 회원 탈퇴(동의철회) 기능을 마련할 것

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출해야 한다.

Ⅴ. 결론

피심인의 舊 보호법 제29조(안전조치의무), 제34조(개인정보 유출 통지 등) 제1항, 제37조(개인정보 처리정지 등) 제1항 위반행위에 대해 같은 법 제64조(시정조치 등)제1항에 따라 시정조치 명령을 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정조치 명령에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

이상과 같은 이유로 주문과 같이 의결한다.

2024년 11월 4일

위 원 장 이 문 한 (서 명)

위 원 박 상 희 (서 명)

위 원 조 소 영 (서 명)