개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 제2024-220-642호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인 (사업자등록번호 :)

대표자
의결연월일 2024. 10. 23.

주 문

1. 피심인에 대하여 다음과 같이 시정조치를 명령한다.

가. 행사안내 알림톡을 발송하는 등 행사 관련 시스템을 운영할 경우, 시스템의 보안취약점 점검 및 개선 등 재발방지 대책을 마련하여야 한다.

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

이 유

Ⅰ. 기초 사실

피심인은 의 위탁으로 입장티켓 발송 등 행사 시스템을 개발·운영한 「舊 개인정보 보호법」[1](이하 '舊 보호법')에 따른 개인정보 처리업무 수탁자로, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

피심인이 한국인터넷진흥원으로부터 행사 URL을 통해 타인의 개인정보가 조회된다는 안내로 유출사실을 인지하여 유출신고('23. 3. 8.)해옴에 따라 개인정보보호위원회는 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('24. 1. 31. ~ '24. 8. 13.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 '24. 2. 20.(자료제출일) 기준 아래와 같이 개인정보를 수집하여 보관하고 있다.

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

< 개인정보 수집현황 >

구 분	항 목	기 간	건 수(건)

***** 행사 종료에 따라 수집 목적이 달성되어 '23. 2. 20.에 개인정보 파기

나. 개인정보 유출 관련 사실관계

피심인은 행사 사전등록자 편의를 위하여 '23. 2. 15. 19시부터 알림톡으로 입장티켓의 URL을 발송하였는데, URL에 포함된 개인코드는 200001번부터 시작하는 숫자 6자리로 유추하기 쉬운 형태였으며, URL에 포함된 개인코드를 변경하면 해당 개인코드를 부여받은 타인의 개인정보가 그대로 노출되었다.

1) **(유출 규모 및 항목)** 사고 당시 상세페이지 로그 기록이 없어 정확한 유출 규모 산정은 어려우나, 타인의 정보(이름, 휴대전화번호)를 볼 수 있다고 한국인터넷진흥원에 침해신고한 신고인의 증빙자료로 **3명의 개인정보 유출사실 확인**

※ '23년 에 등록한 회원은 17,409명

2) 유출 인지 및 대응

일 시	유출인지 및 대응 내용
'23. 3. 7. 14시경	인터넷진흥원 담당자가 유출 사실 안내
'23. 3. 7. 14시	주관사인 에 유출사실 통보
'23. 3. 7. 15시	해당 페이지 내 표출되는 개인정보 모두 마스킹 처리
'23. 3. 8. 18시	개인정보포털에 **유출 신고***

* 내부 보고 및 에 통지, 유출 원인이 된 페이지 조치 등으로 시간이 경과하였고, 피심인이 유출 사실을 연락받아 직접 신고했다고 소명

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보의 안전조치 의무를 소홀히 한 사실

피심인이 시스템을 개발·운영하면서 개인정보 유출에 취약한 파라미터 변조 취약점에 대한 점검 및 개선 조치를 소홀히 하여, 권한이 없는 타인에게 개인정보가 노출된 사실이 있다.

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 '24. 8. 20. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으나, 기한 내 의견을 제출하지 않았다.

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 보호위원회가 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) 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.

2) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2022. 10. 20. 시행
3) 개인정보보호위원회고시 제2021-3호, 2021. 9. 15. 시행

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.

2. 위법성 판단

가. 개인정보의 안전조치의무를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

피심인이 시스템을 개발·운영하면서 개인정보 유출에 취약한 파라미터 변조 취약점에 대한 점검 및 개선 조치를 소홀히 하여, 권한이 없는 타인에게 개인정보가 노출되었으므로, 舊 보호법 제29조, 같은 법 시행령 제48조의2제1항 및 舊 기술적 보호조치 기준 제4조제9항 위반에 해당한다.

※ ①피심인이 시스템 개발·운영을 책임지며, ②舊 보호법 제26조제7항에 따라 수탁자도 안전조치의무가 준용되고, ③표준 개인정보 보호지침도 수탁자에게 안전조치 책임이 있다고 규정, ④피심인의 위수탁 계약서도 안전조치 의무를 수탁자 책임으로 명시한 점 등을 고려하여, **안전조치 의무 위반의 책임은 피심인에게 있다고 판단**함

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용
안전조치의무 위반	舊 보호법 §29	舊 시행령 §28의2①	• 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 처리시스템 등에 필요한 조치를 소홀히 함

Ⅳ. 처분 및 결정

1. 시정 조치 명령

가. 행사안내 알림톡을 발송하는 등 행사 관련 시스템을 운영할 경우, 시스템

의 보안취약점 점검 및 개선 등 재발방지 대책을 마련하여야 한다.

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

Ⅴ. 결론

피심인의 舊 보호법 제29조(안전조치의무)를 위반한 행위에 대하여 같은 법 제64조(시정 조치 등)제1항에 따라 시정조치를 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(당사자 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.

2024년 10월 23일

위 원 장 이 문 한 (서 명)

위 원 박 상 희 (서 명)

위 원 조 소 영 (서 명)