# 개 인 정 보
# 보 호 위 원 회
# 제 2 소 위 원 회

# 심의·의결

**안 건 번 호** 제2025-209-223호

**안 건 명** 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

**피 심 인**

**의결연월일** 2025. 5. 14.

## 주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 1,800,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

# 이 유

## Ⅰ. 기초 사실

피심인은 건설업 관련 조사 및 연구를 수행하는 비영리법인으로 홈페이지를 통해 온라인 소식지 구독을 신청한 자의 개인정보를 처리하고 있어 「개인정보 보호법」[1](이하 '舊 보호법')에 따른 개인정보처리자로, 피심인의 일반현황은 다음과 같다.

**< 피심인의 일반현황 >**

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

## Ⅱ. 사실조사 결과

### 1. 조사 배경

개인정보보호위원회는 피심인이 한국인터넷진흥원으로부터 연락을 받아 개인정보 유출 사실을 인지하고 유출 신고('23.1.26.)해옴에 따라 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('23.2.3.～'24.2.6.)하였으며, 다음과 같은 사실을 확인하였다.

### 2. 행위 사실

#### 가. 개인정보 수집 현황

피심인은 '23. 3. 7.(자료제출일) 기준 아래와 같이 개인정보를 수집하여 보관하고 있다.

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

**< 개인정보 수집현황 >**

| 구 분 | 수집 항목 | 기간 | 규모(명) |
|---|---|---|---|
| | | | |

## 나. 개인정보 유출 관련 사실관계

해커*는 피심인의 홈페이지 게시판에서 SQL Injection 공격으로 획득한 홈페이지 관리자계정(아이디/비밀번호) 정보를 이용하여 관리자페이지에 접속**한 후 피심인이 관리하는 온라인소식지 구독 신청자의 개인정보를 유출('23.1.21.)하였다.

* (IP주소) 5.28.34.201(유럽)

** 외부에서 접속 가능한 관리자페이지에는 안전한 접속수단 또는 인증수단이 적용되어 있지 않았으며, "웹진 구독 신청자 정보" 다운로드 기능을 통해 회원정보를 유출함

**1) (유출 내용)** 온라인소식지 구독 신청자 55명*의 개인정보**

* 총 69건이 유출되었으나, 중복 신청자 등 제외

** 이름, 이메일주소, 소속, 직위 등이 유출되었으며, 정보주체별 유출 항목이 다름

**2) (유출 인지 및 대응)** 유출사실 인지 후 5일 내 유출 통지 및 신고 완료

| 일 시 | | 피심인의 유출 인지·대응 내용 |
|---|---|---|
| '23. 01. 21. | | 중국 해커조직(샤오치잉)이 브리치드 포럼에 피심인의 홈페이지 주소와 개인정보 69건을 공개 |
| '23. 01. 22. | 10:00 | 한국인터넷진흥원으로부터 연락을 받아 개인정보 **유출 인지** 및 관련 조치(외부에서 작업/접속차단, 게시물 삭제, 피해신고 접수 등) |
| '23. 01. 25. | 09:00 | 개인정보 유출사실 확인 및 이사장 등 내부 보고<br>※ 1.21.~1.24. 설 연휴 |
| '23. 01. 26 | 16:00 | 소식지 구독신청자 대상 개인정보 **유출 통지** 및 사과문 발송(이메일) |
| | 17:00 | 개인정보 포털에 **유출 신고** |
| '23. 01. 27 | 13:00 | 관리자 페이지( ) 비밀번호 변경 및 소식지 구독 신청자 정보 삭제<br>※ 홈페이지 소식지 구독 신청자 정보는 엑셀 파일로 이관 후 삭제 |

### 3. 개인정보의 취급.운영 관련 사실관계

#### 가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 홈페이지를 운영하면서 외부에서 개인정보취급자가 관리자페이지에 접속하는 경우, IP주소 등으로 접근을 제한하거나 안전한 접속수단 또는 인증수단을 적용하지 않은 상태로 운영한 사실이 있다.

또한, 홈페이지 관리자페이지에 대하여 입력값 검증 등 SQL Injection 공격을 방어할 수 있는 조치를 적용하지 아니한 사실이 있다.

### 4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 '24. 6. 10. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 6. 27. 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') 제30조제1항제2호는 "개인정보에 대한 접근 통제 및 접근 권한의 제한 조치를 하여야 한다."라고 규정하고 있다.

한편, 舊 개인정보의 안전성 확보조치 기준[3](이하 '舊 안전성 확보조치 기준'이라 한다.) 제6조제1항은 "개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으

2) 대통령령 제30892호, 2020. 8. 4. 일부개정, 2021. 2. 5. 시행
3) 개인정보보호위원회고시 제2021-2호, 2021. 9. 15. 일부개정, 2021. 9. 15. 시행

로 제한하여 인가받지 않은 접근을 제한(1호)', '개인정보처리시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응(2호)' 기능을 포함한 조치를 하여야 한다."라고 규정하고 있으며,

같은 조 제2항은 "개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다."라고 규정하고 있으며,

같은 조 제3항은 "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 있다.

다만, 舊 안전성 확보조치 기준 제6조제8항은 "[별표]의 유형1에 해당하는 개인정보처리자는 舊 안전성 확보조치 기준 제6조 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다."라고 규정하고 있다.

## 2. 위법성 판단

### 가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

피심인이 홈페이지 관리자 페이지에 외부에서 접속하는 경우 IP 주소 등으로 접근을 제한하지 않았고, 관리자 로그인 페이지에 대하여 입력값 검증 등 SQL Injection 공격에 대한 방어조치를 적용하지 아니하여 열람권한이 없는 자에게 온라인소식지 구독 신청자의 개인정보가 유출된 것은 舊 보호법 제29조, 같은 법 시행령 제30조제1항제2호, 舊 안전성 확보조치 기준 제6조(접근통제)를 위반한 것이다.

※ 피심인은 舊 안전성 확보조치 기준 제6조제8항의 [별표]의 유형1(1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인)에 해당하는 개인정보처리자로, 舊 안전성 확보조치 기준 제6조제2항에 따른 안전한 접속수단 또는 안전한 인증수단을 적용하지 아니할 수 있음

## Ⅳ. 처분 및 결정

### 1. 과태료 부과

피심인의 舊 보호법 제29조 위반에 대해 같은 법 제75조제2항제6호, 舊 시행령 제63조 [별표2] '과태료의 부과기준' 및 개인정보 보호법 위반에 대한 과태료 부과기준[4](이하 '과태료 부과기준')에 따라 다음과 같이 180만 원의 과태료를 부과한다.

### 가. 기준금액

舊 시행령 제63조 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 기준금액 600만 원을 적용한다.

**< 舊 보호법 시행령 [별표2] 2. 개별기준 >**

| 위반행위 | 근거 법조문 | 과태료 금액(단위 : 만 원) | | |
|---|---|---|---|---|
| | | 1회 위반 | 2회 위반 | 3회 이상 위반 |
| 자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우 | 舊 법 제75조제2항제6호 | 600 | 1,200 | 2,400 |

### 나. 과태료의 가중

과태료 부과기준 제7조제1항은 "당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 3]의 가중기준(▲위반의 정도, ▲위반기간, ▲조사방해, ▲위반주도)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다"라고 규정하고 있다.

피심인의 경우 과태료 부과기준에 규정된 과태료를 가중할 수 있는 사유에 해당하는 사항이 없으므로 기준금액을 유지한다.

4)「질서위반행위규제법」제3조제2항에 따라 과태료 부과 시 피심인에게 유리하게 변경된 지침(2023. 9. 15. 시행) 적용

### 다. 과태료의 감경

과태료 부과기준 제6조제1항은 “당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 감경기준(▲당사자 환경, ▲위반정도, ▲개인정보 보호 노력 정도, ▲조사협조 및 자진 시정 등을 고려하여 감경사유가 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.” 라고 규정하고 있으며,

같은 조 제2항은 “[별표 2]의 각 기준에 따른 과태료 감경 시 그 사유가 2개 이상 해당되는 경우에는 합산하여 감경하되, 제2호 1) 및 2)에 해당하는 사유가 각 2개 이상 해당되는 경우에는 기준금액의 100분의 50을 초과할 수 없고, 최종 합산 결과 기준금액의 100분의 90을 초과할 수 없다.”라고 규정하고 있다.

피심인의 경우 과태료 부과기준 제6조 및 [별표 2] 과태료의 감경기준에 따라, ‘비영리법인인 점(30%이내)’, ‘사전통지 및 의견제출 기간 내에 위반행위를 시정 완료한 경우(20%이내)’, ‘일관되게 행위 사실을 인정하면서 위법성 판단에 도움되는 자료를 제출 또는 진술하는 등 조사에 적극적으로 협력한 경우(20%이내)’에 해당하여 과태료 부과기준 제6조에 따라 기준금액의 70%를 감경한다.

### 라. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 180만 원의 과태료를 부과한다.

**< 과태료 산출내역 >**

| 과태료 처분 | | 과태료 금액 (단위:만 원) | | | |
|---|---|---|---|---|---|
| 위반조항 | 처분 조항 | 기준 금액(A) | 가중액 (B) | 감경액 (C) | 최종액(D) D=(A+B-C) |
| 舊 보호법 제29조(안전조치의무) | 舊 보호법 제75조제2항제6호 | 600 | - | 420 | **180** |

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

## Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반에 대하여 같은 법 제75조(과태료) 제2항제6호에 의한 과태료 부과를 의결한다.

# 이의제기 방법 및 기간

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조제1항에 따라 과태료 부과 통지를 받은 날부터 60일 이내에 개인정보보호위원회에 서면으로 이의제기를 할 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 납부 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다.

**2025년 5월 14일**

위 원 장　　김 진 환

위　　원　　김 일 환

위　　원　　김 휘 강