# 개 인 정 보 보 호 위 원 회
# 심의·의결

**안건번호** 제2022-005-021호

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

**피 심 인**

**의결연월일** 2022. 3. 23.

## 주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 4,800,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

## 이 유

### Ⅰ. 피심인의 일반 현황

피심인은 항공운수업을 운영하면서 개인정보를 처리하는 사업자로서 「개인정보 보호법」(법률 제16930호, 이하 “보호법”이라 함) 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

| 대 표 | 설립일자 | 매출액('20년) | 당기순이익('20년) | 종업원 수 |
|---|---|---|---|---|
| | | | | |

## Ⅱ. 사실조사 결과

개인정보보호위원회는 2021.10월 개인정보보호 포털에 유출 신고가 접수된 건과 관련하여 현장조사 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

### 1. 개인정보 유출 경위

#### 가. 유출 경과 및 대응

| 일시 | 인지 및 대응 |
|---|---|
| '21.9.27. | 신원 미상자가 舊홈페이지로 접근하여 웹서버의 파일 업로드 취약점을 이용하여 웹셸을 업로드 |
| '21.9.29. ~ 10.9. | 舊웹서버에서 피심인의 서버로 WebLogic 취약점을 통해 공격을 시도 |
| '21.10.9. ~ 10.11. | 신원 미상자가 DB에 접근하여 개인정보를 조회 |
| '21.10.12. | 악성코드 모니터링 탐지 안내 메일이 발송되었으나 연휴로 인해 확인이 지연 |
| '21.10.12. | 舊웹서버는 폐기하고 피심인 서버의 WebLogic 취약점에 대한 패치를 적용 |
| '21.10.13. | DB 쿼리 내역을 점검하여 개인정보가 조회된 것을 인지하고 개인정보보호 포털에 신고 |
| '21.10.14. | 개인정보 유출 사실을 정보주체에게 통지(이메일, 유선)하고 홈페이지에 공지 |
| '21.10.14. ~ 11.15. | WebLogic 설치 서버들에 대한 전수 조사를 진행 |

### 나. 유출 규모 및 경위

’19.9월 홈페이지를 새롭게 오픈하였고 새로운 홈페이지가 안정화될 때까지 舊 홈페이지는 유지한 후 서비스를 종료할 예정이었으나 사고가 발생할 때까지 오픈되어 있었다.

그룹 계열사 간 통합 관리 및 운영 효율을 위해 신뢰할 수 있는 구간을 바탕으로 네트워크가 구축되어 망에서 망으로 접근이 가능한 상태였고, 네트워크에 방화벽이 도입되어 있었으나 악의적인 접근만 차단하고 그 외에는 모두 허용하는 블랙리스트 방식으로 보안 정책이 설정되어 있었다.

피심인은 서버의 WebLogic 취약점에 대한 보안 업데이트를 하지 않았고, 이를 통해 성명, 생년월일, 예약번호 등 명(국적, 여권번호 명은 중복)의 개인정보가 유출되었을 것으로 추정된다.

피심인은 생성된 웹셸 및 악성파일 삭제, 서버 폐기, No-Show 서버의 WebLogic 취약점 패치 적용, 내부 서버 간 이상 징후 탐지를 위한 보안관제 체계 및 정책 강화 등 개선조치를 실시하였다.

## 2. 행위 사실

### 가. 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 침입 탐지·차단시스템, 방화벽을 설치·운영하고 있으나 웹서버를 통해 이루어진 비인가된 접근을 제한하지 않았고, No-Show Penalty 서버의 WebLogic 취약점에 대한 보안 업데이트를 하지 않았다.

## 3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022.2.17. ‘개인정보보호 법규 위반에 대한 행정처분 사전통지’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 2022.3.2. 피심인은 위반상태를 모두 시정하였고 ISMS 인증을 취득한 점 등을 고려하여 선처를 요청하였다.

## Ⅲ. 위법성 판단

### 1. 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련 법령의 규정

보호법 제29조는 개인정보처리자는 개인정보가 유출 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다고 규정하고 있고,

같은 법 시행령 제30조제1항은 개인정보처리자는 법 제29조에 따라 제2호개인정보에 대한 접근 통제 및 접근 권한의 제한 조치, 제5호개인정보에 대한 보안 프로그램의 설치·갱신을 하여야 한다고 규정하고 있다.

「개인정보의 안전성 확보조치 기준」(고시 제2020-2호) 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 제1호개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한하는 기능을 포함한 조치를 하여야” 하고 제9조는 “개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 제2호악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시하여야 한다”라고 규정하고 있다.

나. 위법성 판단

피심인이 개인정보처리시스템에 대한 접속 권한을 제한하여 인가받지 않은 접근을 제한하지 않은 것과 서버 취약점에 대한 보안 업데이트를 하지 않은 것은 보호법 제29조 위반에 해당한다.

## Ⅳ. 처분 및 결정

### 1. 과태료 부과

피심인의 보호법 제29조 위반에 대해 같은 법 제75조제2항제6호, 같은 법 시행령 제63조 [별표2]「과태료의 부과기준」에 따라 480만원의 과태료를 부과한다.

#### 가. 기준금액

피심인이 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 기준금액은 1회 위반에 해당하는 600만원을 적용한다.

< 과태료 부과기준 2. 개별기준 >

| 위반행위 | 근거 법조문 | 과태료 금액(단위 : 만원) | | |
|---|---|---|---|---|
| | | 1회 위반 | 2회 위반 | 3회 이상 위반 |
| 자. 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우 | 법 제75조 제2항제6호 | 600 | 1,200 | 2,400 |
| 계 | | 600 | | |

#### 나. 과태료의 가중

피심인의 제29조에 따른 안전성 확보에 필요한 조치 위반행위의 정도가 중대하여 과태료의 부과기준에 따라 기준금액의 30%인 180만원을 가중한다.

* ①개인정보에 대한 접근 통제 및 접근권한 제한 미조치, ②보안프로그램의 설치 및 갱신 미조치

#### 다. 과태료의 감경

피심인이 위반행위에 대하여 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료하였으므로 기준금액의 50%인 300만원을 감경한다.

### 라. 최종 과태료

피심인이 보호법 제29조를 위반한 행위에 대해 480만원의 과태료를 부과한다.

< 최종 과태료 산출내역 >

| 과태료 처분의 근거 | | 과태료 금액 (단위:만원) | | | |
|---|---|---|---|---|---|
| 위반조항 | 처분조항 | 기준 금액(A) | 가중액 (B) | 감경액 (C) | **최종액 (D=A+B+C)** |
| 제29조 | 제75조제2항제6호 | 600 | 180 | △300 | **480** |

## Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반에 대해서 같은 법 제75조(과태료) 제2항제6호에 의한 과태료 부과를 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 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

2022년 3월 23일

위 원 장　　윤 종 인　(서 명)

부위원장　　최 영 진　(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　　지 성 우　(서 명)