

# 개 인 정 보 보 호 위 원 회

## 심의 · 의결

의 안 번 호 제2023-008-076호 (사건번호 : 2021조총0035)

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의 결 연 월 일 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 유출신고('21.6.14.)와 관련하여 조사를 진행하여, 피심인의 개인정보보호 법규 위반행위와 관련된 다음과 같은 사실을 확인하였다.

### 1. 행위 사실

#### 가. 개인정보 수집 현황

피심인은 위탁 계약을 맺은 학교법인 을 통해 육아서비스 등 제공을 목적으로 '21. 11. 29. 기준 아래와 같이 개인정보를 수집·보관하고 있다.

개인정보파일	수집·이용 항목	수집기간	보유건수(명)
홈페이지 회원 정보 (대여관리시스템)	(필수) 이름, 아이디, 비밀번호, 생년월일, 휴대폰 번호, 이메일 주소, 집주소 (선택) 집 전화번호, 자녀 정보(이름, 생년월일)	'12.7.1 ~ 계속	8,659

## 나. 개인정보 유출 관련 사실관계

### 1) 유출 규모 및 항목

대여 신청자의 개인정보 15,460건이 유출되었으며, 성명·ID·휴대폰 번호·집 주소 등이 포함되어 있었다.

### 2) 유출 인지 및 대응

일시		피심인의 유출 인지·대응 내용
2021.	6.7.~6.8.	유지보수업체를 통해 홈페이지 프로그램 수정 작업 진행
	6. 8.	민원 신고를 접수한 한국인터넷진흥원으로부터 개인정보 노출 안내문 수신, <b>유출 사실 최초 인지</b> / 관리자페이지 로그인 프로그램 시정
	6.10.	한국인터넷진흥원에 <b>침해신고</b>
	6.11.	로그 분석 결과 유출 사실 확인, 노출 URL 삭제 조치
	6.14.	개인정보 포털에 <b>유출신고</b>
		홈페이지에 개인정보 유출 공지
	6.15.~6.17.	개인정보 <b>유출 통지</b> (이메일 및 문자 메시지)
	6.17.	개인정보 보호 교육 실시

### 3) 유출 경위

대여 신청자 명단 관리자페이지 URL이 접근통제가 해제 (해제시기 불상)된 상태로 외부 검색 엔진(MS Bing)에 노출되었으며, 해당 URL을 클릭하면 별도 로그인 과정 없이 관리자페이지로 접근이 가능하였고, 로그 분석 결과 '21.5.9.~6.8. 외부 검색 엔진을 통해 165개 페이지의 접근을 허용한 사실을 확인하였다.

## 다. 개인정보의 취급·운영 관련 사실관계

### 1) 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 개인정보처리시스템에 접속한 IP 주소 등을 분석하여 불법적인 유출 시도를 탐지하거나 대응하지 않은 사실이 있고, 관리자페이지 URL이 외부 검색 엔진에 노출된 것과 관련 접근 통제 등 조치를 소홀히 한 사실이 있으며, 홈페이지 관련 '처리한 정보주체 정보' 및 '수행업무' 등 접속 기록을 보관·관리하지 않은 사실이 있다.

## 2. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 1. 26. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 2. 15. 개인정보보호위원회에 의견을 제출하였다.

## Ⅲ. 위법성 판단

### 1. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

#### 가. 관련 법 규정

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.”고 규정하고 있으며, 보호법 시행령 제30조제1항은 “개인정보처리자는 법 제29조에 따라 개인정보에 대한 접근 통제 및 접근

권한의 제한 조치(제2호) 및 개인정보 침해사고 발생에 대응하기 위한 접속 기록의 보관 및 위조·변조 방지를 위한 조치(제4호)를 하여야 한다”고 규정하고 있다.

또한 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호, 이하 ‘고시’) 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응을 하여야 한다”고 규정하고 있고, 제6조제3항은 “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.”고 규정하고 있으며, 제8조제1항은 “개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다.”고 규정하고 있다.

## 나. 위법성 판단

1) 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지하고 대응하여야 하나, 피심인이 홈페이지에 대한 불법적인 개인정보 유출 시도 탐지 및 대응을 하지 않은 행위는 보호법 제29조, 시행령 제30조제1항, 고시 제6조제1항 위반에 해당한다.

2) 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템 등에 접근 통제 등에 관한 조치를 하여야 하나, 피심인이 관리자페이지 URL이 외부

검색 엔진에 노출된 것과 관련 접근 통제 조치를 소홀히 한 행위는 보호법 제29조, 시행령 제30조제1항, 고시 제6조제3항 위반에 해당한다.

3) 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 하나, 피심인이 홈페이지 관련 ‘처리한 정보주체 정보’ 및 ‘수행업무’ 등 접속 기록을 보관·관리하지 않은 행위는 보호법 제29조, 시행령 제30조제1항, 고시 제8조제1항 위반에 해당한다.

## IV. 처분 및 결정

### 1. 과태료 부과

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

#### 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 위반에 대해서 1회 위반에 해당하는 과태료인 600만 원을 적용한다.

#### < 과태료 부과기준, 보호법 시행령 제63조 [별표 2] >

위반행위	근거 법조문	과태료 금액(단위 : 만원)		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 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 보호법 제29조 위반행위는 과태료 부과지침 제8조 [별표2]의 가중기준에 따라 ‘위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우’로서 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.

피심인은 의견제출 기간내 법규 위반행위를 시정 완료하고, 자료제출 등 조사에 적극 협력하였으므로, 과태료 부과지침 제7조 [별표1] 감경기준에 따라 기준금액의 50%인 300만 원을 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 보호법 제29조 위반 행위에 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(안전조치의무)	법 제75조제2항제6호	600	60	300	360

**V. 결론**

피심인의 보호법 제29조 위반행위에 대하여 같은 법 제75조제2항제6호에 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 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)