

# 개 인 정 보 보 호 위 원 회

## 심의 · 의결

의 안 번 호 제2023-013-170호

안 전 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의 결 연 월 일 2023. 7. 26.

### 주 문

1. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 20,000,000원

나. 과 태 료 : 6,000,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표 한다.

# 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

### 1. 조사 배경

개인정보보호위원회는 개인정보 침해신고('21. 2. 18.)가 접수되어 개인정보 관리실태에 대한 조사('22. 4. 22. ~ '23. 5. 26.)를 실시하였으며, 피심인의 보호법규 위반행위와 관련된 다음과 같은 사실을 확인하였다.

### 2 행위 사실

#### 가. 개인정보 수집·이용 현황

피심인은 '21년도 의 실거주 확인 및 보험 가입 등을 위해 '21. 3. 12. 기준 아래와 같이 개인정보를 수집·보관하고 있다.

개인정보파일	수집 · 이용 항목	수집일	보유건수(명)



## 2) 유출 사실의 통지·신고를 지체없이 하지 않은 행위

피심인은 '21. 2. 10. 홈페이지 게시 직후 신원미상 민원인의 개인정보 유출 제보 등을 통해 상황을 인지하고 게시물을 삭제하는 등의 조치를 하였으나, 유출 사실을 인지한 날로부터 16일이 지난 '21. 2. 26. 정보 주체에게 유출 사실을 통지하고, 같은 날 개인정보 포털을 통해 해당 내용을 신고한 사실이 있다.

## 3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 5. 16. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 5. 31. 개인정보보호위원회에 의견을 제출하였다.

# III. 위법성 판단

## 1. 고유식별정보 안전성 확보에 필요한 조치를 소홀히 한 행위

### 가. 관련 법 규정

보호법 제24조제3항은 “개인정보처리자가 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.”라고 규정하고 있고, 같은 법 시행령 제30조제1항은 “개인정보 처리자는 법 제29조에 따라 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호) 및 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)를 하여야 한다”라고 규정하고 있다.

또한 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2020-2호, 이하 '고시') 제6조제3항은 “개인정보처리자는 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.”라고 규정하고 있으며, 제7조제1항은 “개인정보처리자는 고유식별정보, 비밀번호, 생체인식정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.”라고 규정하고 있다.

## 나. 위법성 판단

1) 개인정보처리자는 고유식별정보를 정보통신망을 통하여 송신하는 경우 이를 암호화하여야 하나, 피심인이 공고용 엑셀파일에 고유식별정보(주민등록번호)가 숨김 처리되어 포함된 사실을 확인하지 않고, 이를 암호화하지 않은 상태로 홈페이지에 게시한 행위는 보호법 제24조제3항, 시행령 제30조제1항, 고시 제7조제1항 위반에 해당한다.

2) 개인정보처리자는 취급 중인 개인정보가 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등의 조치를 하여야 하나, 피심인이 고유식별정보가 포함된 파일을 홈페이지에 게시하여 열람 권한이 없는 자에게 공개되도록 한 행위는 보호법 제24조제3항, 시행령 제30조제1항, 고시 제6조제3항 위반에 해당한다.

## 2. 개인정보 유출 통지·신고 의무를 소홀히 한 행위

### 가. 관련 법 규정

1) 보호법 제34조제1항은 “개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체없이 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 대응 조치 및 구제절차, 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처 등을 알려야 한다.”라고 규정하고 있다.

2) 보호법 제34조제3항은 “대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 통지 및 조치 결과를 지체없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다”라고 규정하고 있고, 같은 법 시행령 제39조제1항은 “법 제34조제3항 전단에서 대통령령으로 정한 규모 이상의 개인정보란 1천명 이상의 정보주체에 관한 개인정보를 말한다”라고 규정하고 있으며, 같은 법 시행령 제39조제3항은 “법 제34조제3항 전단 및 후단에서 대통령령으로 정하는 전문기관이란 각각 한국인터넷진흥원을 말한다”라고 규정하고 있다.

## 나. 위법성 판단

1) 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때 지체없이 해당 정보주체에게 관련 사실을 알려야 하나, 피심인이 유출 사실을 '21. 2. 10. 인지하고도 정보주체에게 관련 내용을 16일이 경과한 '21. 2. 26. 통지한 행위는 보호법 제34조제1항 위반에 해당한다.

2) 개인정보처리자는 1천명 이상의 개인정보가 유출된 경우 통지 및 피해 최소화 조치 등 결과를 개인정보위나 한국인터넷진흥원으로 지체없이 신고하여야 하나, 피심인이 유출 사실을 '21. 2. 10. 인지하고도, 16일이 지나 개인정보 포털을 통해 '21. 2. 26. 신고한 행위는 보호법 제34조제3항 위반에 해당한다.

## IV. 처분 및 결정

### 1. 과징금 부과

주민등록번호가 유출되었고, 보호법 제24조제3항에 따른 안전성 확보에 필요한 조치를 다하지 않은 피심인의 보호법 위반에 대해 같은 법 제34조의2 제1항, 같은 법 시행령 제40조의2 [별표 1의3], 「주민등록번호 유출 등에 대한 과징금 부과기준(고시 제2022-4호, 2022.10.20., 이하 ‘과징금 부과기준’)」에 따라 다음과 같이 과징금을 부과한다.

#### 가. 기준금액

보호법 시행령 제40조의2 [별표1의3]은 고의·중과실·경과실 여부 및 유출 주민등록번호 규모에 따라 산정기준액을 규정하고 있고, 피심인은 경과실로 인하여 10만 건 미만의 주민등록번호가 유출되었으므로, ‘일반 위반행위’에 해당하는 금액인 1억 원을 적용한다.

**<보호법 시행령 제40조의2 [별표 1의3] >**

위반 정도	산정 기준액	비고
매우 중대한 위반행위	3억 5천만 원	고의 또는 중과실로 인하여 10만 건 이상의 주민등록번호가 분실·도난·유출·변조 또는 훼손(이하 ‘분실 등’이라 한다)된 경우
중대한 위반행위	2억 3천만 원	고의 또는 중과실로 인하여 10만 건 미만의 주민등록번호가 분실 등이 된 경우 및 경과실로 인하여 10만 건 이상의 주민등록번호가 분실 등이 된 경우
일반 위반행위	1억 원	경과실로 인하여 10만 건 미만의 주민등록번호가 분실 등이 된 경우

#### 나. 1차 조정

과징금 부과기준 제5조(1차 조정)는 “1차 조정금액은 산정기준액에 따라 <1차 조정 기준표>에서 정한 1차 조정비율을 곱한 금액으로 정한다. 1차 조정 비율은 <세부평가 기준표>에 따라 산정한다”고 규정하고 있다.

피심인의 보호법 제24조제3항 위반행위는 과징금 부과기준 제5조의 <세부평가 기준표>에 따른 산정 점수가 1.8점에 해당하므로, <1차 조정 기준표>에 따라 기준금액의 20%인 2,000만 원을 감경한다.

< 세부평가 기준표 >

고려사항		부과점수 비중	3점	2점	1점
안전성 확보 조치	개인정보에 대한 접근	0.2	주민등록번호에 대하여 다음 각 호의 조치를 모두 하지 아니하거나 현저히 부실하게 한 경우 1. 접근통제 2. 접근권한의 관리	주민등록번호에 대하여 다음 각 호의 조치 중 한 가지를 하지 아니하거나 현저히 부실하게 한 경우 1. <u>접근통제</u> 2. 접근권한의 관리	3점 또는 2점에 해당되지 않는 경우
안전성 확보 조치	암호화	0.2	<u>주민등록번호의 송신·전달·저장 시 이를 암호화 하지 아니한 경우</u>	주민등록번호를 안전한 암호화알고리즘으로 암호화하지 않은 경우	3점 또는 2점에 해당되지 않는 경우
	보안 프로그램	0.2	악성프로그램 등을 방지·치료할 수 있는 보안프로그램을 설치·운영하지 않은 경우	보안프로그램에 대한 업데이트를 실시하지 아니하여 최신의 상태로 유지하지 않은 경우	3점 또는 2점에 해당되지 않는 경우
	접속기록의 보관 등	0.2	개인정보처리시스템의 접속기록 보관 및 위조·변조 등 방지를 위한 조치를 하지 아니하고, 주민등록번호를 보관하는 물리적 보관장소를 별도로 두지 아니하거나 잠금장치를 하지 않은 경우	개인정보처리시스템의 접속기록 보관 및 위조·변조 등 방지를 위한 조치를 하지 아니하거나, 주민등록번호에 대한 물리적 보관장소를 별도로 두지 않는 등 물리적 안전조치가 없는 경우	3점 또는 2점에 해당되지 않는 경우
피해 방지 후속 조치 등		0.2	개인정보가 유출되었음을 알게 된 때로부터 5일 이내에 다음 각 호의 조치를 모두 하지 아니한 경우 1. 정보주체에게 통지 2. 피해 최소화를 위한 대책 마련 및 조치 3. 조치결과를 신고	개인정보가 유출되었음을 알게 된 때로부터 5일 이내에 다음 각 호의 조치 사항 중 두 가지 이상을 하지 아니한 경우 1. <u>정보주체에게 통지</u> 2. 피해 최소화를 위한 대책 마련 및 조치 3. <u>조치결과를 신고</u>	3점 또는 2점에 해당되지 않는 경우

< 1차 조정 기준표 >

세부평가 기준표에 따른 산정 점수	1차 조정 비율
2.5이상	+100분의 50
2.3이상 2.5미만	+100분의 35
2.1이상 2.3미만	+100분의 20
1.9이상 2.1미만	-
1.7이상 1.9미만	-100분의 20
1.5이상 1.7미만	-100분의 35
1.5미만	-100분의 50



## 다. 2차 조정

과징금 부과기준 제6조(2차 조정)는 “2차 조정금액은 1차 조정된 금액에 <2차 조정 기준표>에서 정한 2차 조정비율을 곱한 금액으로 정한다. 2차 조정 비율은 <세부평가 기준표>에 따라 산정한다”고 규정하고 있다.

피심인의 보호법 제24조제3항 위반행위는 과징금 부과기준 제6조의 <세부평가 기준표>에 따른 산정 점수가 1.0점에 해당하므로, <2차 조정 기준표>에 따라 1차 조정된 금액의 50%인 4,000만 원을 감경한다.

**< 세부평가 기준표 >**

고려사항	부과점수 비중	3점	2점	1점
위반기간	0.2	위반기간이 6개월을 초과하는 경우	위반기간이 3개월 초과 6개월 이내인 경우	3점 또는 2점에 해당되지 않는 경우
위반횟수	0.2	최근 3년 내 주민등록번호 유출로 과징금 부과 처분을 2회 이상 받은 경우	최근 3년 내 주민등록번호 유출로 과징금 부과 처분을 1회 이상 받은 경우	3점 또는 2점에 해당되지 않는 경우
조사협조	0.2	위반행위 조사 시 조사기간내 자료 미제출, 조사자료 은폐 등 조사방해의 부당성이 현저히 큰 경우	위반행위 조사 시 조사기간내 자료 미제출, 조사자료 은폐 등 조사방해의 부당성이 경미하지 않은 경우	3점 또는 2점에 해당되지 않는 경우
2차 피해	0.2	위반행위로 인해 보이스 피싱 등 2차 피해가 발생한 경우	위반행위로 인해 보이스 피싱 등 2차 피해 발생할 우려가 상당히 큰 경우	3점 또는 2점에 해당되지 않는 경우
개인정보 보호를 위한 노력	0.2	참작할 사유가 없는 경우	개인정보 보호 관련 직원교육을 하거나 표창을 받는 등 개인정보 보호를 위한 노력이 상당히 있는 경우	다음 각 호의 어느 하나에 해당하는 경우 등 개인정보 보호를 위한 노력이 현저히 큰 경우*

\* 대표 홈페이지 등 6개 개인정보 처리시스템을 대상으로 개인정보 보호 인증(ISMS-P)을 획득, 위원회 주관 관리수준 진단 결과 3년 연속 ‘양호 평가’(19년 90.34점/20년 100점/21년 98.68점)

**< 2차 조정 기준표 >**

세부평가 기준표에 따른 산정 점수	2차 조정 비율
2.5이상	+100분의 50
2.1이상 2.5미만	+100분의 25
1.7이상 2.1미만	-
1.3이상 1.7미만	-100분의 25
1.3미만	-100분의 50

## 라. 부과과징금의 결정

보호법 제34조의2제1항은 “주민등록번호가 유출된 경우 5억원 이하의 과징금을 부과할 수 있다.”고 하면서, 단서로 “제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.”라고 규정하고 있다.

과징금 부과기준 제8조(부과과징금의 결정)는 “위반행위자의 현실적인 부담 능력, 위반행위로 발생한 정보주체의 피해 및 배상의 정도, 위반행위자가 속한 시장·산업 여건 등을 고려하여 2차 조정된 과징금이 과중하다고 인정 되는 경우 해당 금액의 100분의 90 범위에서 감경할 수 있고(제1항), 정보주체에게 피해가 발생하지 않았거나 경미한 경우로서 사소한 부주의나 오류로 인한 위반행위인 경우 과징금을 면제할 수 있다.(제2항)”고 규정하고 있다.

이 사건의 주민등록번호 유출 사고가 ‘담당 직원이 엑셀 파일에 숨김처리 된 시트를 확인하지 못한 사소한 부주의로 발생했다’ 하더라도, 유출된 해당 엑셀 파일은 보호법이 특별히 규율하고 있는 주민등록번호 암호화 조치를 하지 않은 것으로서 과징금 면제 대상으로 삼을 수는 없다.

다만, 유출에 따른 정보주체의 피해가 발생하지 않았거나 경미한 경우로서 사소한 부주의로 유출된 점과 위반행위로 인하여 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 점(과징금 부과기준 제8조제1항제4호) 등을 종합적으로 고려하여 2차 조정된 금액의 50%인 2,000만 원을 감경한다.

※ (추가 고려사항) 유출 직후 약 2분만에 해당 사실을 인지하고 시정 조치를 진행하여 개인정보가 유출된 시간이 약 7분으로 짧은 점, 추가 피해 접수 사례가 없는 점 등

## 마. 최종 과징금

피심인의 보호법 제24조제3항 위반행위에 대하여 기준금액에서 1차·2차 조정 및 부과과징금의 결정을 거쳐 총 2,000만 원의 과징금을 부과한다.

기준금액	1차 조정	2차 조정	부과 과징금 결정	최종 과징금
1억원	8,000만 원	4,000만 원	2,000만 원	2,000만 원
일반 위반행위 ※ 10만 건 미만	1차 산정점수 1.8점 ⇒ 20%(2,000만 원) 감경	2차 산정점수 1.0점 ⇒ 50%(4,000만 원) 감경	2차 조정금액이 과중하다고 인정 ⇒ 50%(2,000만 원) 감경	

## 2. 과태료 부과

보호법 제76조는 “제75조의 과태료에 관한 규정을 적용할 때 제34조의2에 따라 과징금을 부과한 행위에 대하여는 과태료를 부과할 수 없다”라고 규정하고 있다.

피심인의 보호법 제24조제3항 위반행위는 같은 법 제75조제2항제6호, 같은 법 시행령 제63조의 [별표2] 「과태료 부과기준」에 따라 과태료 부과 사유에 해당하나, 보호법 제76조에 따라 과태료를 부과하지 아니한다.

피심인의 보호법 제34조제1항 및 제3항 위반행위에 대해 같은 법 제75조제2항제8호 및 제9호, 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 제34조제1항 및 제3항 위반행위에 대해 1회 위반에 해당하는 과태료인 1,200만원(각 600만 원)을 적용한다.

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

위반행위	근거 법조문	과태료 금액(단위 : 만원)		
		1회 위반	2회 위반	3회 이상 위반
처. 법 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제8호	600	1,200	2,400
커. 법 제34조제3항을 위반하여 조치 결과를 신고하지 않은 경우	법 제75조 제2항제9호	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 제34조제1항 및 제3항 위반행위는 과태료 부과지침 제8조 [별표2]의 가중기준에 해당하지 않아 기준금액을 유지한다.

## 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 노력 정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 내에서 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 600만 원(각 300만 원)을 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 제34조제1항 및 제3항 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 총 600만 원의 과태료를 부과한다.

### < 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) $D=(A+B-C)$
제34조제1항(통지 의무)	법 제75조제2항제8호	600		300	300
제34조제3항(신고 의무)	법 제75조제2항제9호	600		300	300
계		1,200		600	600

## 3. 처분 결과의 공표

보호법 제66조제1항에 따라 피심인이 과태료를 부과받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표					
개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1	서울특별시	법 제34조 제1항	개인정보 유출통지 위반	2023. 7. 26.	과태료 300만 원
		법 제34조 제3항	개인정보 유출신고 위반		과태료 300만 원
2023년 7월 26일 개 인 정 보 보 호 위 원 회					

## V. 결론

피심인의 보호법 제24조제3항, 제34조제1항 및 제3항 위반행위에 대하여 같은 법 제34조의2제1항, 제75조제2항, 제66조제1항에 따라 주문과 같이 의결한다.

## 이의제기 방법 및 기간

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

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 7월 26일

위 원 장    고 학 수    (서 명)

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)