개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2023-006-049호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2023. 4. 12.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 6,000,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 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') 제2조 제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인의 개인정보 유출 신고('21.11.17.)에 따라 유출 사건을 조사('22.4.18. ~ 7.20.)하고 피심인의 개인정보 보호법규 위반행위와 관련하여 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용

피심인은 시스템(이하 '종합관리시스템')을 운영하면서 '22.7.29. 기준 아래와 같이 고객의 개인정보를 수집·보관하고 있다.

< 개인정보 수집현황 >

구분	수집·이용 항목	수집일	건수(명)

나. 개인정보 유출 관련 사실관계

1) 개인정보 유출 인지 및 대응

일시	피심인의 유출인지·대응 내용
’21. 11. 15.	권한없는 외부인(이하 ‘신고인’)이 제보(구글에서 특정 검색어 조합을 통해 종합관리시스템 내 자료 검색시 영수증, 출장비 등이 포함 된 파일을 다운로드 가능함)
’21. 11. 16.	피심인은 종합관리시스템 취약점과 신고인이 개인정보를 포함하는 문서 파일을 비정상 다운로드 받은 내역을 확인하고, 이를 근거로 본 사건을 개인정보 유출 사고로 확정 후 기관 개인정보 유출사고 대응 규정에 따라 위기대응본부 구성
’21. 11. 16.	URL 내 파일 식별정보에 대한 암호화 조치 완료
’21. 11. 17.	개인정보 포털에 개인정보 유출사고 신고
’21. 11. 18.	신고인으로부터 679건 문서를 다운로드 할 때 사용한 저장장치와 문서 전체 파기 및 외부 미유출에 대한 ‘사실확인서’ 수령
’21. 11. 19.	전달 받은 저장장치에 대한 디지털 포렌식 분석을 통해, 문서 전체가 삭제되었고, 외부 유출 가능성이 낮다는 사실을 재확인
’21. 11. 19.	정보주체에게 유출 사실 통지(이메일 및 홈페이지 팝업 게시(7일간)

2) (유출경위) 권한 없는 외부인(이하 ‘신고인’)이 ‘21. 10. 28. ~ 11. 15. 기간 동안 구글 검색을 통해 ‘종합관리시스템 내 파일 디렉토리에 직접 접근하여 679건의 문서를 다운로드하였으며, 이중 일부 문서에 개인정보가 포함됨

- 신고인은 URL에 포함된 파일 식별번호 값을 임의로 변경하면 시스템 내 파일에 접근 가능한 사실을 발견하고, 별도의 권한 없이 개인정보가 포함된 비공개 문서를 내려 받음

- 피심인은 신고인의 제보를 통해 이를 인지하였고, 구글 검색에 특정 검색어를 조합하여 지원시스템 내 파일 디렉토리에 직접 접근이 가능한 URL을 찾음

3) **(유출항목 및 규모)** 종사자의 이름, 주민등록번호*, 생년월일, 휴대 전화, E-Mail, 주요경력, 소속, 직위, 주소, 학력, 고용형태, 채용구분, 입사일, 계좌번호, 급여정보, 소득정보 등 4,087명 12,375건

* **주민등록번호 유출은 10건**이며, 이와 관련하여 피심인은 협약기업이 증빙문서 파일 제출시, 주민등록번호 뒷자리를 마스킹 처리하여 제출할 것을 요청하고 있으나, 일부 기업이 마스킹 처리를 하지 않고 제출하였다고 소명하였음

3. 개인정보의 취급·운영 관련 사실관계

1) 권한 없는 자에 대한 접근통제를 소홀히 한 행위

피심인은 종합관리시스템에 제3자가 구글 검색을 통해 접근 시 접근통제 등에 관한 조치를 하지 않아, 제3자가 개인정보가 포함된 비공개 문서 679건을 다운로드 한 사실이 있다.

2) 주민등록번호를 암호화하지 않고 보관한 행위

피심인은 주민등록번호가 포함된 문서를 전자문서시스템에 보관하면서, 해당 문서를 암호화하지 않은 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 2. 14. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 2. 21. 위반 사실을 인정하고 개인정보 보호를 위해 ISO27001 인증을 받은 점과 위반 사항에 대해 자진 시정을 완료하였다는 점을 고려하여 선처를 요청하였다.

Ⅲ. 위법성 판단

1. 관련 법 규정

가. 보호법 제29조는 “개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 않도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제30조제1항은 안전성 확보조치로 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(2호)를 하도록 하고 있다.

같은 법 시행령 제30조제3항에 따른 안전성 확보 조치의 세부기준인 「개인정보의 안전성 확보조치 기준」(이하 ‘고시’ 라고 한다.)에서는 “개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개 되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.(제6조제3항)”고 규정하고 있다.

나. 보호법 제24조의2제2항은 “개인정보처리자는 제24조제3항에도 불구하고 주민 등록번호가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

가. 권한 없는 자에 대한 접근통제를 소홀히 한 행위

피심인이 개인정보처리자로서 종합관리시스템에 대한 접근통제 조치를 하지 않아 개인정보가 유출된 행위는 보호법 제29조, 시행령 제30조 제1항 및 고시 제6조제3항을 위반한 것이다.

나. 주민등록번호를 암호화하지 않고 보관한 행위

피심인은 개인정보처리자로서 주민등록번호가 포함된 문서를 전자문서시스템에 보관할 때 암호화 조치를 통하여 안전하게 보관하지 않은 행위는 보호법 제24조의2제2항을 위반한 것이다.

Ⅳ. 처분 및 결정

1. 과징금 면제

피심인의 보호법 제24조의2(주민등록번호 처리의 제한)제2항 위반에 대해 부과하는 같은 법 제34조의2(과징금의 부과 등)제1항에 따른 과징금은 경미하고 피해가 없는 사유 등을 고려하여 「주민등록번호 유출 등에 대한 과징금 부과 기준」(이하 '과징금 부과기준')에 따라 다음과 같이 과징금을 면제한다.

가. 기준금액

과징금 부과기준 제4조에 따라 위반 정도가 일반 위반행위에 해당하여 1억원을 적용한다.

위반 정도	산정 기준액	비고
매우 중대한 위반행위	3억 5천만원	고의 또는 중과실로 인하여 10만건 이상의 주민등록번호가 분실·도난·유출·변조 또는 훼손(이하 '분실 등'이라 한다)된 경우
중대한 위반행위	2억 3천만원	고의 또는 중과실로 인하여 10만건 미만의 주민등록번호가 분실 등이 된 경우 및 경과실로 인하여 10만건 이상의 주민등록번호가 분실 등이 된 경우
일반 위반행위	**1억원**	**경과실로 인하여 10만건 미만의 주민등록번호가 분실등이 된 경우**

나. 1차 조정

과징금 부과기준 제5조의 세부평가 기준표에 따른 산정 점수가 1.2점에 해당하여 기준금액의 50%인 5천만원을 감액한다.

< 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**

< 세부평가 기준표 >

고려사항 \ 부과점수		비중	3점	2점	1점
안전성확보조치	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. 접근통제** 2. 접근권한의 관리	3점 또는 2점에 해당되지 않는 경우
	암호화	0.2	주민등록번호의 송신·전달·저장 시 이를 암호화 하지 아니한 경우	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. 정보주체에게 통지 2. 피해 최소화를 위한 대책 마련 및 조치 3. 조치결과를 신고	3점 또는 2점에 해당되지 않는 경우

나. 2차 조정

과징금 부과기준 제6조의 세부평가 기준표에 따른 산정 점수가 1점에 해당하여 1차 조정된 금액(5천만원)의 50%인 2천5백만 원을 감액한다.

< 2차 조정 기준표 >

세부평가 기준표에 따른 산정 점수	1차 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**

< 세부평가 기준표 >

부과점수 / 고려사항	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 조사기간 내 자료 미제출, 조사자료 은폐 등 조사방해의 부당성이 현저히 큰 경우	위반행위 조사 시 조사기간 내 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	개인정보보호 관련 직원 교육을 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 **1. 개인정보보호 인증을 받은 경우 등**

다. 부과과징금의 결정

과징금 부과기준 제8조제2항제2호에 따라 정보주체에게 피해가 발생하지 않았거나 경미한 경우로서 100명 미만 유출의 경우(다목)에 해당되어 2차 조정된 금액(2천5백만 원)을 면제한다.

* 유출된 주민등록번호는 10건으로, 최초 발견자(제보자) 1인에게만 유출되었으며, 유출된 자료는 파기되어 추가 피해로 확산되지 않음

2. 과태료 부과

피심인의 보호법 제29조(안전조치의무) 및 제24조의2(주민등록번호 처리의 제한) 제2항 위반에 대한 과태료는 같은 법 제75조(과태료)제2항제6호와 제4호의2, 같은 법 시행령 제63조의 [별표2]「과태료 부과기준」에 따라 다음과 같이 총 600만 원의 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(안전조치의무) 및 제24조의2(주민등록번호 처리의 제한)제2항 위반에 대해서 1회 위반에 해당하는 과태료인 600만 원을 각각 적용한다.

< 과태료 부과기준, 개인정보보호법 시행령 제63조 [별표 2] >

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
카. 법 제24조의2제2항을 위반하여 암호화 조치를 하지 않은 경우	법 제75조 제2항제4호의3	600	1,200	2,400

나. 과태료의 가중

피심인의 제29조(안전조치의무) 및 제24조의2(주민등록번호 처리의 제한)제2항 위반에 대해 과태료 부과지침 제8조 및 [별표2] 가중기준에 따른 과태료를 가중할 수 있는 사유에 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 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.

피심인의 경우, 사전통지 및 의견제출 기간이 종료되기 이전에 위반상태를 모두 시정을 완료한 점, 조사 기간 중 행위사실을 인정하면서 자료제출·진술 등 조사에 적극 협력한 점, ISO27001 인증을 받은 점 등을 종합적으로 고려하여 과태료 부과지침 제7조의 과태료 감경기준에 따라 기준금액의 50%인 300만 원을 각각 감경한다.

< 과태료의 감경기준(제7조 관련) >

기준	감경사유	감경비율
조사 협조 · 자진 시정 등	1. 과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 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
	3. 사전통지 및 의견제출 기간 내에 법규 위반행위를 시정 완료하지는 못하였으나 시정 중에 있는 것으로 인정되는 경우	기준금액의 30%이내
개인정보 보호 노력정도	3. 개인정보보호와 관련된 국제인증(ISO27001, ISO27701, BS10012)을 받은 경우	기준금액의 35%이내

라. 최종 과태료

피심인의 제29조(안전조치의무) 및 제24조의2(주민등록번호 처리의 제한)제2항 위반에 대해 기준금액 총 1,200만 원에서 가중·감경을 거쳐, 각 50%를 감경한 총 600만 원을 부과한다.

< 과태료 산출내역 >

개인정보보호법		과태료 금액 (단위:만원)			
위반조항	처분 조항	기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
제29조(안전조치의무)	제75조제2항제6호	600	-	300	**300**
제24조의2(주민등록번호 처리의 제한) 제2항	제75조제2항 제4호의3	600	-	300	**300**
계		1,200	-	600	**600**

3. 결과의 공표

「개인정보 보호법」 제66조제1항 및 「개인정보보호위원회 처분 결과 공표 기준」('20.11.18. 개인정보위 의결) 제2조(공표요건)에 따르면 피심인의 위반행위는 보호법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우(제4호)에 해당하므로, 피심인에 대한 과태료 부과에 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
2		법 제24조의2	주민등록번호의 암호화 조치	2023. 4. 12.	과태료 300만 원
		법 제29조	안전조치의무 위반 (접근통제)		과태료 300만 원

2023년 4월 12일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인의 개인정보 보호법 제29조 및 제24조의2제2항 위반행위에 대하여 같은 법 제75조(과태료)제2항제6호 및 제2항제4호의3에 따라 과태료 부과와 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날로부터 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 4월 12일

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)