

개 인 정 보 보 호 위 원 회

심의 · 의결

의 안 번 호 제2023-013-179호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2023. 7. 26.

주 문

피심인에 대하여 다음과 같이 과징금을 부과한다.

가. 과 징 금 : 12,500,000원

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

II. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인의 개인정보 유출 신고('22.2.24.)에 따라 개인정보 관리실태에 대한 사실조사('22. 2. 7. ~ 5. 3.)를 실시하였으며, 피심인의 보호법규 위반행위와 관련하여 다음과 같은 사실을 확인하였다.

2 행위 사실

가. 개인정보 수집·이용 현황

피심인은 시스템()을 운영하면서 '22.2.7. 기준 아래와 같이 개인정보를 수집·보관하고 있다.

구분	수집·이용 항목	수집일	건수

나. 개인정보 유출 관련 사실관계

1) 유출규모 및 항목

839명의

항목*이 유출되었다.

* 성명, 주민등록번호, 건강보험, 국민연금, 보장성보험, 의료비, 교육비, 신용카드·직불카드·현금영수증, 연금저축, 주택자금·월세액, 주택마련저축, 기부금 등

※ 839명 중 자료 내려받기 시 '정보제공에 동의'하면서 '주민등록번호 전체표시' 옵션을 선택한 67명의 자료에는 주민등록번호가 포함되어 다운로드 됨

※ 정보제공이란 이 을 수행하는 에게 자신의 정보를 주는 것을 말하며, 개인정보 공개는 불특정 다수에게 열람토록 하는 것은 아니고, 을 수행하는 에게 자신의 주민등록번호 뒷자리 마스킹을 해제하는 것임

2) 유출 인지 및 대응

일시		피심인의 유출인지·대응 내용
'21.12.22. 00:00		▶ 행안부 지침에 따라 민간인증모듈 업그레이드(버전 1.0 ⇒ 1.5)
'22.1.15. 00:00		▶ 서비스 개시
'21.1.16.	19:00	▶ 카카오톡 개발자가 인터넷 커뮤니티 '클리앙'에 로그인 취약점* 내용이 게시된 것을 인지하고 이를 에 제보 → 피심인 유출사실 인지 * 타인의 이름과 주민등록번호를 입력하고 카카오톡 본인 인증시 타인의 정보로 로그인 가능
	19:10	▶ 상황대응 및 피해확산 방지를 위한 TF 구성
	20:00	▶ 민간인증서 7종 이용 차단
	23:00	▶ 민간인증서 로그인 오류 조치* 및 서비스 재개 * 화면에 입력한 주민등록번호와 민간인증기관에서 리턴받은 개인식별번호(CI)로부터 추출한 주민등록번호를 비교 검증하는 로직을 추가·반영하여, 로그인창과 민간인증 팝업창에 입력된 인적사항이 동일한 경우에만 로그인 되도록 조치
'22.1.26. ~ 2.8.		▶ 민간인증 오류 관련, 타인의 인증서로 열람된 정보주체 773명 1차 확인(2.3.) 및 66명 2차 추가확인(2.8.) ※ 서비스 로그인 기록과 민간인증 기록을 대조하여 본인의 인증서가 아닌 타인의 인증서로 열람된 정보주체 확인
'22.2.3. ~ 9.		▶ (2.3.~4.) 1차 확인된 정보주체 777명에게 유출 통지 (문자·카카오톡 등) ▶ (2.8.~9.) 2차 추가 확인된 정보주체 66명에게 유출 통지 (문자·카카오톡 등)
'22.2.4.		▶ 개인정보 보호 포털에 유출 신고 * 유출 규모는 839건으로 보호법 제34조제3항에 의한 유출신고 대상은 아님

3) 유출경위

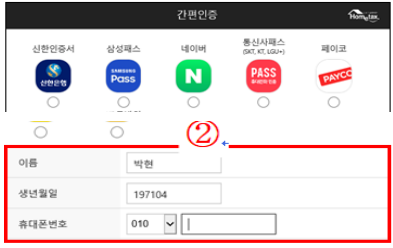
피심인이 민간인증서 연결을 위해 행정안전부에서 배포하는 「민간인증공통 모듈」 1.0버전을 1.5버전으로 업그레이드하여 민간인증 2종을 추가하였으나, 주민등록번호를 입력하는 것에서 생년월일을 입력하는 것으로 변경이 있었고,

[행정안전부 제공 민간인증 공통모듈 버전 비교]

▶ 민간인증 공통 프로그램 1.0v	▶ 민간인증 공통 프로그램 1.5v
- (입 력) 이름, <u>주민등록번호</u> , 핸드폰번호	- (입 력) 이름, <u>생년월일</u> , 핸드폰 번호
- (서비스) PC용	- (서비스) PC 및 모바일용
- (인증서) <u>카카오톡, PASS, 페이코, 삼성패스, 국민은행</u>	- (인증서) 5종 + <u>네이버, 신한은행</u>

이로 인해 1.0버전 당시 로그인 화면과 본인인증 요청화면에서 입력한 주민등록번호 간 일치여부를 확인하는 로직을 적용할 수 없게 되자, 전산 업체는 대체 비교수단을 마련하지 않고 해당 로직을 삭제함에 따라,

※ 행안부는 이용기관이 시스템 사양에 맞게 개인정보 처리가 필요함을 안내하였음

로그인 화면 이용자 인적사항	민간인증 팝업 인적사항
	

로그인 화면의 이용자 인적사항에 타인의 성명과 주민등록번호를 입력하고, 본인인증 시 자신의 정보로 인증을 하면, 타인의 계정으로 로그인이 되는 오류가 발생하였다.

※ 수검기관은 다양한 브라우저 및 핸드폰기기에서 새로운 민간인증이 제대로 작동 하는지에 대한 기능테스트는 수행하고, 유출사건과 같은 비정상 케이스에 대한 테스트는 수행하지 않음

다. 개인정보의 취급·운영 관련 사실관계

1) 고유식별정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 에 민간인증을 통한 로그인 시 본인인증 로직이 제대로 작동하도록 시스템을 구축하지 않았고 그에 대한 검증을 하지 않아, 제3자가 에 로그인 시 가족·지인 등 타인의 성명과 주민등록번호를 입력하고 본인인증 하여 타인의 계정으로 로그인한 후 해당 타인의 등 839명*에 대한 자료를 열람하게 한 사실이 있다.

* 839명의 정보는 불특정 다수가 아닌, 성명과 주민등록번호를 함께 알고 있는 가족·지인 등에 의해 부분적으로 노출됨

피심인은 제3자가 민간인증을 통한 로그인 오류를 이용하여 타인의 자료를 열람함으로써, 67명의 주민등록번호가 유출되게 한 사실이 있다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 5. 9. 피심인에게 예정된 처분에 대한 사전 통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 5. 19. 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 안전성 확보에 필요한 조치를 하여야 한다.”라고 규정하고 있고, 같은 법 시행령 제30조제1항은 “개인정보처리자는 법 제29조에 따라 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)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 있다.

나. 위법성 판단

개인정보처리자는 고유식별정보를 처리하는 경우에는 그 고유식별정보가 유출 등이 되지 않도록 안전성 확보에 필요한 조치를 하여야 하고, 취급 중인 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등에 관한 조치를 하여야 하나,

피심인이 에 민간인증을 통한 로그인 시 본인인증 로직이 제대로 작동하도록 시스템을 구축하지 않았고 그에 대한 검증을 하지 않아, 제3자가 에 로그인 시 가족·지인 등 타인의 성명과 주민등록번호를 입력하고 본인인증 하여 타인의 계정으로 로그인한 후 해당 타인의 등 839명에 대한 자료를 열람하게 한 행위는 보호법 제24조 제3항, 시행령 제30조제1항, 고시 제6조제3항 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 1.2점에 해당하므로, <1차 조정 기준표>에 따라 기준금액의 50%인 5,000만 원을 감경한다.

< 세부평가 기준표 >

부과점수		고려사항	비중	3점	2점	1점
안 전 성 확 보 조 치	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	
	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	개인정보가 유출되었음을 알게 된 때로부터 5일 이내에 다음 각 호의 조치 사항 중 두 가지 이상을 하지 아니한 경우	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 1점에 해당하므로, <2차 조정 기준표>에 따라 1차 조정된 금액의 50%인 2,500만원을 감정한다.

< 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*(1호 ISO)

* 피심인은 ISO 27001, ISO27701 인증을 받음

< 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

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.

면제 기준 (§8②)	1. 위반행위자가 객관적으로 과징금을 낼 능력이 없다고 인정되는 경우 2. 정보주체에게 피해가 발생하지 않았거나 경미한 경우로서 다음 어느 하나에 해당하는 경우 가. 2차 조정된 금액이 300만 원 이하인 경우 나. 사소한 부주의나 오류로 인한 위반행위인 경우 다. 개인정보가 유출된 경우로서 유출된 정보주체의 수가 100명 미만인 경우 3. 위반행위자 본인의 행위가 위법하지 않은 것으로 잘못 인식할 만한 정당한 사유가 있는 경우
-------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

이 사건의 유출된 주민등록번호는 100건 미만으로 과징금 면제를 검토할 수 있으나, 면제 여부는 위원회의 재량인 점, 는 대량의 개인정보를 처리하는 공공기관의 집중관리시스템*으로 다른 개인정보처리자에 비해 강화된 보호조치 의무가 요구된다는 점을 고려할 때 과징금 면제 대상으로 삼을 수는 없다.

* 개인정보위는 ‘22.7월 발표한 「공공부문 개인정보 유출 방지대책」에서 시정권고를 중심으로 조치하던 지자체 등 공공기관에 과태료·과징금을 적극 부과하기로 결정함

다만, 유출에 따른 정보주체의 피해가 발생하지 않았거나 경미한 경우로서 위반행위로 인하여 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 점(과징금 부과기준 제8조제1항제4호) 등을 종합적으로 고려하여 2차 조정된 금액의 50%인 1,250만 원을 감경한다.

마. 최종 과징금의 결정

피심인의 보호법 제24조제3항 위반행위에 대하여 기준금액에서 1차·2차 조정 및 부과과징금의 결정을 통하여 1,250만원의 과징금을 부과한다.

기준금액	1차 조정	2차 조정	부과 과징금 결정	최종 과징금
1억원	5,000만 원	2,500만 원	1,250만 원	1,250만원
일반 위반행위 ※ 10만 건 미만	1차 산정점수 1.2점 ⇒ 50%(5,000만 원) 감경	2차 산정점수 1점 ⇒ 50%(2,500만 원) 감경	2차 조정금액이 과중하다고 인정⇒ 50%(1,250만 원) 감경	

2. 과태료 미부과

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.

V. 결론

피심인의 보호법 제24조제3항 위반행위에 대하여 같은 법 제34조의2에 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.

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)