

개 인 정 보 보 호 위 원 회

심의 · 의결

의 안 번 호 제2023-018-234호

안 건 명 공공기관의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의 결 연 월 일 2023. 11. 8.

주 문

1. 피심인에 대하여 다음과 같이 과징금을 부과한다.

가. 과 징 금 : 16,250,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 개선을 권고한다.

가. 피심인은 주민등록번호 처리와 관련된 보호실태를 점검하여 적법한 절차와 수단을 마련하는 등 미흡한 사항을 개선하고, 개인정보취급자 등을 대상으로 정기적인 개인정보 보호교육을 실시하여야 한다.

나. 피심인은 가.의 개선권고에 따른 조치를 이행하고, 통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

I. 기초 사실

피심인은 「舊 개인정보 보호법¹⁾」(이하 ‘舊보호법’) 제2조제6호에 따른 공공기관으로, 같은 법 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

사업자 등록번호	대표자 성명	주소

II. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 유출 신고(23. 4. 21.)가 접수되어 개인정보

1) 법률 제16930호, 2020. 2. 4. 일부개정, 2020. 8. 5. 시행

관리실태에 대한 조사('23. 4. 28. ~ '23. 8. 14.)를 실시하였으며, 피심인의 舊보호법 위반행위와 관련된 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

피심인은 소속 학생 장학금 수여 등 관리를 위해 '23. 5. 15. 기준 아래와 같이 개인정보를 수집·보관하고 있다.

개인정보파일	수집·이용 항목	수집일	보유건수
학적정보 등록 양식 (엑셀 파일)	성명, 주민등록번호	23.4.17.~ 5.12.	1,203명

나. 개인정보 유출 관련 사실관계

1) 유출 규모 및 항목

장학금 수혜 및 학자금 대출 관련 재학생·졸업생 1,203명의 개인정보가 유출되었고, 유출된 정보에는 성명과 주민등록번호가 포함된 사실을 확인하였다.

2) 유출 인지 및 대응

일시		피심인의 유출 인지·대응 내용
2023.	4.17.	개인정보가 포함된 파일을 홈페이지에 게시
	4.18.	재학생이 홈페이지를 통해 민원 제보, 최초 인지 / 대응 TF팀 구성 게시글 삭제 및 홈페이지에 유출 사실 게시
	4.19.	정보주체에게 유출 통지(이메일)
	4.21.	한국인터넷진흥원에 유출 신고

3) 유출 경위

피심인은 「한국장학재단 설립 등에 관한 법률」 제50조의2제10호에 따라 ○○○○○○ 측에서 학자금 대출 상환 및 장학금 환수 등 수혜자 관리 목적으로 학자금 대출 지원자에 대한 학사정보 제출을 요청할 경우 이에 따라야 하며, 이 경우 통상적으로 ○○○○측 전용 시스템에 접속하여 학자금 대출 지원자 관련 주민등록번호를 다운로드한 후 해당 자료에 학사정보를 매칭·현행화하여 다시 시스템에 업로드하는 방식으로 자료를 제출하고 있다.

피심인은 2023. 4. 14. ○○○○○○ 측으로부터 학자금 대출 지원자 학사정보 제출 요청을 받았으며, 이에 따라 ○○○○측 시스템에 접속하여 학자금 지원자 1,203명의 주민등록번호를 다운로드 받아 해당 자료에 학사정보를 매칭·현행화하여 제출용 자료를 가공하였다. 해당 자료를 ○○○○○○ 측에 제출하기 전 학자금 대출 지원자들에게 관련 절차가 진행된다는 사실을 알리기 위해 피심인 홈페이지에 안내 글을 게시하는 과정에서, 담당자 부주의로 ○○○○○○ 측에 제출하기 위해 가공 중이던 엑셀 파일을 잘못 첨부·게시하여, 학자금 대출 지원자들의 성명·주민등록번호가 유출되었다.

다. 개인정보의 취급·운영 관련 사실관계

1) 고유식별정보의 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 홈페이지에 학자금 대출 지원자들의 주민등록번호가 포함된 엑셀파일을 암호화하지 않고 첨부하여 열람 권한이 없는 자들이 접근하도록 하였으며, 해당 자료에 18개의 IP가 접근한 사실을 확인하였다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023. 8. 18. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023. 8. 30. 개인정보보호위원회에 “사실을 인정하고 위반행위를 시정 완료하였다.”며 선처를 요청하는 내용의 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 고유식별정보의 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련 법 규정

舊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 시행령²⁾(이하 ‘舊시행령’) 제30조제1항은 “개인정보처리자는 법 제29조에 따라 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)를 하여야 한다.”라고 규정하고 있다.

또한 「舊 개인정보의 안전성 확보조치 기준³⁾」(이하 ‘舊고시’) 제6조제3항은 “개인정보처리자는 취급 중인 개인정보가 인터넷 홈페이지 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 등에 접근 통제 등에 관한 조치를 하여야 한다.”라고 규정하고 있고, 제7조제1항은 “개인정보처리자는 고유식별정보, 비밀번호, 생체인식정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.”라고 규정하고 있다.

나. 위법성 판단

개인정보처리자는 취급 중인 개인정보가 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등의 조치를 하여야 하나, 피심인이 업무부주의로 주민등록번호가 포함된 파일을 홈페이지에 게시하여 열람 권한이 없는 자에게 공개되도록 한 행위는 舊보호법 제24조제3항, 제29조, 舊시행령 제30조제1항, 舊고시 제6조제3항 위반에 해당한다.

2) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2022. 10. 20. 시행

3) 개인정보보호위원회고시 제2021-2호, 2021. 9. 15., 시행

또한, 개인정보처리자는 고유식별정보를 정보통신망을 통하여 송신하는 경우 이를 암호화하여야 하나, 피심인이 재학생들의 주민등록번호가 포함된 엑셀 파일을 암호화하지 않은 상태로 홈페이지에 게시한 행위는 舊보호법 제24조 제3항, 제29조, 舊시행령 제30조제1항, 舊고시 제7조제1항 위반에 해당한다.

IV. 처분 및 결정

1. 과징금 부과

피심인의 舊보호법 제24조제3항, 제29조 위반행위에 대해 같은 법 제34조의2 제1항, 같은 법 舊시행령 제40조의2 [별표 1의3], 「舊 주민등록번호 유출 등에 대한 과징금 부과기준⁴⁾」(이하 '舊 과징금 부과기준')에 따라 다음과 같이 과징금을 부과한다.

가. 기준금액

舊보호법 舊시행령 제40조의2 [별표 1의3]은 고의·중과실·경과실 여부 및 유출 주민등록번호 규모에 따라 산정기준액을 규정하고 있는데, 피심인의 위반행위는 경과실로 인하여 10만 건 미만의 주민등록번호가 유출된 경우로서, '일반 위반행위'에 해당하는 금액인 1억 원을 적용한다.

<舊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

4) 개인정보보호위원회고시 제2022-4호, 2022. 10. 20. 시행

나. 1차 조정

‘舊 과징금 부과기준’ 제5조는 “1차 조정금액은 산정기준액에 따라 <1차 조정 기준표>에서 정한 1차 조정비율을 곱한 금액으로 정한다. 1차 조정 비율은 <세부평가 기준표>에 따라 산정한다.”라고 규정하고 있다.

피심인의 舊보호법 제24조제3항 위반행위는 ‘舊 과징금 부과기준’ 제5조의 <세부평가 기준표>에 따른 산정 점수가 1.6점에 해당하므로, <1차 조정 기준표>에 따라 기준금액의 35%인 3,500만 원을 감경한다.

< 세부평가 기준표 >

부과점수		고려사항	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. 접근통제 2. 접근권한의 관리	3점 또는 2점에 해당되지 않는 경우	
	암호화	0.2	주민등록번호의 송신·전달·저장 시 이를 암호화하지 아니한 경우	주민등록번호를 안전한 암호화알고리즘으로 암호화하지 않은 경우	3점 또는 2점에 해당되지 않는 경우	
안전성 확보 조치	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	

< 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

‘舊 과징금 부과기준’ 제6조는 “2차 조정금액은 1차 조정된 금액에 <2차 조정 기준표>에서 정한 2차 조정비율을 곱한 금액으로 정한다. 2차 조정 비율은 <세부평가 기준표>에 따라 산정한다.”라고 규정하고 있다.

피심인의 舊보호법 제24조제3항 위반행위는 ‘舊 과징금 부과기준’ 제6조의 <세부평가 기준표>에 따른 산정 점수가 1.2점에 해당하므로, <2차 조정 기준표>에 따라 1차 조정된 금액의 50%인 3,250만 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

부과점수		3점	2점	1점
고려사항	비중			
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*	개인정보 보호를 위한 노력이 현저히 큰 경우

* 직원 대상 7회 개인정보 교육 실시, 전직원 정보보호교육센터 주관 온라인 교육 이수 / 개인정보보호 영향평가 시행 / 개인정보 Clean Day 시행 및 월 1회 점검 등

< 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

‘舊 과징금 부과기준’ 제8조제1항은 “위반행위자의 현실적인 부담 능력, 위반행위로 발생한 정보주체의 피해 및 배상의 정도, 위반행위자가 속한 시장·산업 여건 등을 고려하여 2차 조정된 과징금이 과중하다고 인정되는 경우 해당 금액의 100분의 90 범위에서 감경할 수 있다.”라고 규정하고 있으며, 제8조제2항은 “객관적으로 과징금을 낼 능력이 없다고 인정되는 경우(제1호), 정보주체에게 피해가 발생하지 않았거나 경미한 경우(제2호), 본인의 행위가 위법하지 않은 것으로 잘못 인식할 만한 정당한 사유가 있는 경우(제3호)에 2차 조정된 금액을 면제할 수 있다.”라고 규정하고 있다.

이 사건의 주민등록번호 유출이 담당 직원의 사소한 부주의로 발생했다고 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(舊 과징금 부과기준 제8조제1항 제4호) 등을 종합적으로 고려하여 2차 조정된 금액의 50%인 1,625만 원을 감경한다.

마. 최종 과징금

피심인의 舊보호법 제24조제3항 및 제29조 위반행위에 대하여 기준금액에서 1차·2차 조정 및 부과과징금의 결정을 거쳐 총 1,625만 원의 과징금을 부과한다.

< 과징금 산출내역 >

기준금액	1차 조정	2차 조정	부과 과징금 결정	최종 과징금
1억원	6,500만 원	3,250만 원	1,625만 원	1,625만 원
일반 위반행위 ※ 주민등록번호 10만 건 미만	1차 산정점수 1.6점 ⇒ 35%(3,500만 원) 감경	2차 산정점수 1.2점 ⇒ 50%(3,250만 원) 감경	2차 조정금액이 과중하다고 인정 ⇒ 50%(1,625만 원) 감경	

2. 과태료 미부과

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

피심인의 舊보호법 제24조제3항 및 제29조 위반행위는 같은 법 제75조제2항 제6호, 같은 법 舊시행령 제63조의 [별표2]에 따라 과태료 부과 사유에 해당하나, 舊보호법 제76조에 따라 과태료를 부과하지 아니한다.

3. 개선권고

피심인에 대하여 舊보호법 제61조제2항에 따라 다음과 같이 개선을 권고한다.

가. 피심인은 주민등록번호 처리와 관련된 보호실태를 점검하여 적법한 절차와 수단을 마련하는 등 미흡한 사항을 개선하고, 개인정보취급자들을 대상으로 정기적인 개인정보 보호교육을 실시하여야 한다.

나. 피심인은 가.의 개선권고에 따른 조치를 이행하고, 통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

4. 처분 결과의 공표

舊보호법 제66조제1항에 따라 피심인의 처분 결과를 개인정보보호위원회 홈페이지에 공표한다.

* 「舊 개인정보 보호위원회 처분결과 공표기준(2020.11.18. 시행)」 제2조(공표요건) 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우 처분 결과를 공표할 수 있다.

2. 1천 명 이상 정보주체의 주민등록번호 등 고유식별정보 또는 민감정보를 분실,도난,유출,위조,변조,훼손한 행위로 개선권고, 시정조치 명령, 고발, 징계권고, 과태료 부과 처분을 받은 경우

* 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침(2023.10.11. 시행)」 제5조(공표기간) 보호위원회가 인터넷 홈페이지 등에 공표하는 경우 기간은 1년으로 한다.

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	○○○○학교	법 제24조 제3항	고유식별정보의 처리 제한 위반	2023. 11. 8.	개선권고 (주민등록번호 처리 보호실태 개선 및 교육 실시)
		법 제29조	안전조치 의무 위반		
2023년 11월 8일 개 인 정 보 보 호 위 원 회					

V. 결론

피심인의 舊보호법 제24조제3항, 제29조 위반행위에 대하여 같은 법 제34조의2제1항, 제61조제2항, 제66조제1항에 따라 주문과 같이 의결한다.