개 인 정 보 보 호 위 원 회
심의·의결

의 안 번 호 제2022-013-093호 (사건번호 : 2021조총0039)

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2022. 8. 10.

주 문

피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 피심인의 일반 현황

피심인은 제1조에 따라 은행권·주화 및 국채·공채, 각종 유가증권 및 정부·지방자치단체 등이 사용할 특수제품의 제조 및 이와 관련된 사업을 하는 기관으로, 「개인정보 보호법」(이하 ‘보호법‘) 제2조

제5호에 따른 개인정보처리자이며, 일반현황은 다음과 같다.

< 피심인 일반현황 >

대표자	설립일자	상시 종업원 수	사업자등록번호 (법인등록번호)

Ⅱ. 사실조사 결과

개인정보보호위원회는 2021. 6월 개인정보보호 포털에 유출 신고가 접수된 건과 관련하여 서면 및 현장조사('22. 2. 18.~ 4. 22.)를 실시하고, 다음과 같은 사실을 확인하였다.

1. 개인정보 유출 경위

가. 사고 경위 및 규모

피심인은 0000상품권 시스템을 한국조폐공사 통합 데이터센터로 이전(‘21.5.20.~25.) 시, 데이터베이스관리시스템(DBMS)을 변경하면서, 변경된 시스템에서 가입자 회원번호 부여와 관련하여 DB 설정을 변경하는 조치를 누락하여, 서로 다른 가입자간 동일한 회원 번호가 부여됨으로 ’21.6.8. ~ ‘21.6.9. 기간 동안 ’ 0000상품권 앱 ‘의 ’ 내정보 변경’ 화면에서 일부 회원의 개인정보가 유출되는 사고가 발생하였다.

나. 사고인지 및 대응

○ **(‘21.6.9.)** 콜센터로 본인정보 오류 민원 접수

○ **(‘21.6.9.)** 개발팀에서 시스템 오류원인 분석, 데이터베이스 관리시스템 오류 수정 및 회원정보 복원

○ **(‘21.6.11.)** 정보주체에게 개인정보 유출 통지(124명, 이메일, 문자발송)

○ **(‘21.6.11.)** 개인정보보호포털에 개인정보 유출 신고

2. 개인정보보호 법규 위반 행위 사실

○ 개인정보 안전성 확보조치를 소홀히 한 행위

피심인은 취급중인 개인정보가 인터넷 홈페이지 등을 통하여 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 하나,

지역사랑상품권 시스템의 개인정보파일이 저장된 오라클DB에서 순서번호 재시작 사이클 설정 변경 조치 누락으로, 서로 다른 회원의 회원번호를 동일하게 중복 생성함으로써, 일부 회원의 개인정보가 ‘지역사랑상품권 앱’의 ‘내정보변경‘ 화면에서 동일한 회원번호가 부여된 다른 회원에게 유출되도록 한 사실이 있다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022. 7. 15. ~ 2022. 7. 29. ’보호법 위반 기관에 대한 행정처분 등 사전통지’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 위반 사실을 인정하고, 교육 등 재발방지를 위해 노력하고 있다는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 관련법 규정

보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”고 규정하고 있다.

같은 법 시행령 제30조제1항은 법 제29조에 따른 안전성 확보 조치로서, 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치를 하도록 규정하고 있으며,

시행령 제30조제1항에 따른 안전성 확보 조치의 세부기준인「개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2020-2호)」에서 개인정보처리자의 안전성 확보 조치 내용을 다음과 같이 구체적으로 정하고 있다.

③ 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 접근통제 등에 관한 조치를 하여야 한다. (제6조제3항)

나. 위법성 판단

피심인이 취급중인 개인정보가 인터넷 홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 하는 등의 필요한 기

술적 조치를 취하지 않은 사실은 보호법 제29조, 같은 법 시행령 제30조제1항제2호 및 고시 제6조제3항을 위반한 것이다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 따라 같은법 제75조제2항제6호 및 같은 법 시행령 제63조의 [별표2] 「과태료 부과기준」에 따라 300만원의 과태료를 부과한다.

가. 기준금액 산정

최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 금액 총 600만원을 적용한다.

< [별표 2] 과태료의 부과기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(단위:만원)		
		1회	2회	3회 이상
타. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 **제29조를 위반**하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중

「개인정보 보호법 위반에 대한 과태료 부과기준」(개인정보보호위원회 지침 2021. 1.27. 제정, 이하 ‘과태료 부과지침’) 제8조(과태료의 가중)에 해당하지 않아 기준금액을 유지한다.

다. 과태료의 감경

사전통지 의견제출 기간이 종료되기 이전에 위반행위를 시정완료했고, 자료제출 등 조사에 적극 협력한 점을 고려하여, 아래와 같이 감경 사유가 인정되어 과태료 부과기준에 따라 기준금액의 50%인 300만원을 감경한다.

<과태료의 감경기준>

기준	감경사유	감경비율
조사협조·자진시정 등	1. 과태료의 사전통지 및 의견 제출 기간이 종료되기 이전에 위반 행위를 중지하는 등 시정을 완료한 경우	기준금액의 50%이내

※ 과태료 부과지침 제7조(과태료의 감경기준)에 따라 과태료의 감경은 기준금액의 50%을 초과할 수 없음

라. 최종 과태료

피심인의 개인정보 보호법 위반 사항에 대하여 총 300만원의 과태료를 부과한다.

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반행위에 대하여 같은 법 제75조(과태료)제2항제6호에 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.

2022년 8월 10일

위 원 장　윤 종 인　(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　이 희 정　(서 명)

위　원　지 성 우　(서 명)