개 인 정 보 보 호 위 원 회
심의·의결

안건번호 제2022-005-023호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2022. 3. 23.

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 휴양콘도 운영업을 운영하면서 개인정보를 처리하는 자로서 「개인정보 보호법」(법률 제16930호, 이하 "보호법"이라 함) 제2조제5호에 따른 개인정보처리자의 지위를 가지며, 일반현황은 다음과 같다.

< 피심인의 일반현황 >

대 표	설립일자	매출액('20년)	당기순이익('20년)	종업원 수

Ⅱ. 사실조사 결과

개인정보보호위원회는 2021. 11월 개인정보보호 포털에 유출 신고가 접수된 건과 관련하여 현장조사 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 유출 경위

가. 유출 경과 및 대응

일시		인지 및 대응
’21.11.24.	17:06	KISA로부터 회원정보가 다크웹에 판매되고 있다는 안내 메일 수신
’21.11.29.	15:02	KISA로부터 공개된 개인정보 데이터 샘플에 대한 안내 메일 수신(다크웹 링크 제공)
’21.11.30.	09:21	KISA로부터 다크웹에 공개된 썸네일 수신
’21.11.30.	16:30	現시스템과 비교하여 개인정보 유출을 추정
’21.11.30.	18:00	유출 데이터와 舊시스템 테이블 정보가 일치함을 확인
’21.11.30.	18:12	개인정보보호 포털에 개인정보 유출 신고
’21.12. 1.	10:43	개인정보 유출 사실을 홈페이지에 공지
‘22.2.11. ~ 2.17.		개인정보 유출 사실을 통지(이메일, 문자)

나. 유출 규모 및 경위

썸네일에 있는 도메인은 그룹이 그룹으로부터 을 인수하기 전에 사용하던 것으로 인수 후 리브랜딩을 통해 새로운 도메인으로 변경하였는데 썸네일에 있는 파일명과 데이터구조가 舊시스템(‘18.12월까지 사용) 정보와 일치하였다.

도메인 변경 이력을 통해 개인정보 유출이 ’16.11월 이전에 발생한 것으로 추정되나 舊시스템이 폐기(‘18.12.)되어 정확한 유출시점과 유출경위를 알 수 없고 舊시스템의 안전조치의무 위반 여부도 확인할 수 없었다.

피심인은 썸네일에 성명, 생년월일, 주소 등 개인정보가 유출된 명 중 現시스템에 개인정보가 일치하는 명에 대한 유출통지를 하지 않았다. (홈페이지 공지만 실시)

피심인은 외부 전문기관에 의뢰하여 現시스템에 대한 대내·외 서비스 모의해킹, 서버 취약점 진단 등을 실시하고 취약점에 대한 보완조치를 진행하고 있다.

2. 개인정보보호 법규 위반 행위 사실

가. 개인정보 유출 사실의 통지를 지연한 행위

피심인은 개인정보의 유출 사실을 홈페이지에 공지하였으나 유출된 파일과 現시스템에서 개인정보가 일치하는 정보주체에게 5일 이내에 유출통지를 하지 않았다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022.2.17. ‘개인정보보호 법규 위반에 대한 행정처분 사전통지’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 2022.2.22. 피심인은 의견을 제출하였다.

Ⅲ. 위법성 판단

가. 관련 법령의 규정

보호법 제34조제1항은 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 [1호]유출된 개인정보의 항목, [2호]유출된 시점과 그 경위, [3호]유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, [4호]개인정보처리자의 대응조치 및 피해 구제절차, [5호]정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당 부서 및 연락처 등의 사실을 알려야 한다고 규정하고 있다.

같은 법 시행령 제40조제1항은 개인정보처리자는 개인정보가 유출되었음을 알게

되었을 때에는 서면등의 방법으로 지체 없이 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다고 규정하고 있다.

「표준 개인정보 보호지침」(고시 제2020-1호) 제26조제1항은 개인정보처리자는 개인정보처리자는 개인정보가 유출되었음을 알게 된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 법 제34조제1항 각 호의 사항을 알려야 한다고 규정하고 있다.

나. 위법성 판단

피심인이 '21.11.30. 개인정보 유출 사실을 인지하였으나 70여 일이 지나서 '22.2.11.~2.15. 정보주체에게 개인정보 유출 사실을 통지한 행위는 보호법 제34조제1항 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제34조제1항 위반에 대해 같은 법 제75조제2항제8호, 같은 법 시행령 제63조 [별표2]「과태료의 부과기준」에 따라 300만원의 과태료를 부과한다.

가. 기준금액 산정

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

< 과태료의 부과기준 >

위반행위	근거 법조문	위반횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
처. 법 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	제75조 제2항제8호	600	1200	2400

나. 과태료의 가중

피심인의 위반행위가 과태료의 부과기준에 따른 가중사유가 없으므로 기준금액을 유지한다.

다. 과태료의 감경

피심인이 위반행위에 대하여 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료하였으므로 기준금액의 50%인 300만원을 감경한다.

라. 최종 과태료

피심인이 보호법 제34조제1항을 위반한 행위에 대해 300만원의 과태료를 부과한다.

< 최종 과태료 산출내역 >

과태료 처분의 근거		과태료 금액 (단위:만원)			
위반조항	처분조항	기준 금액(A)	가중액 (B)	감경액 (C)	**최종액 (D=A+B+C)**
제34조제1항	제75조제2항제8호	600	-	△300	**300**

Ⅴ. 결론

피심인이 보호법 제34조제1항을 위반한 행위에 대하여 같은 법 제75조제2항제8호에 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 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

2022년 3월 23일

위 원 장 윤 종 인 (서 명)

부위원장 최 영 진 (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 흥 열 (서 명)

위 원 지 성 우 (서 명)