개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 제2024-220-644호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인 (사업자등록번호 :)

대표자
의결연월일 2024. 10. 23.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

피심인은 여행 상품, 항공권, 호텔 등 예약 서비스를 제공하는 「개인정보 보호법」[1](이하 '보호법')에 따른 개인정보처리자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수(명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인이 서비스 제공 중 통신장애로 인해 고객의 개인정보가 타인에게 노출되었다고 신고('23.10.13.)해옴에 따라 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('23. 11. 15. ~ '24. 8. 16.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 '23. 11. 28. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

1) 개인정보 보호법(법률 제19234호, 2023. 3. 14. 일부개정, 2023. 9. 15. 시행)

< 개인정보 수집현황 >

구분	항목	기간	건수
계			

나. 개인정보 유출 관련 사실관계

피심인은 통합인증(통합회원) 서버와 피심인의 홈페이지 로그인 서버를 연동하여 운영 중이며, 통합인증 서버의 인증서를 업데이트했으나 피심인의 홈페이지 로그인 서버 1대(#2 서버)의 인증서를 업데이트하지 않아, 서버 간 인증서 불일치로 인해 홈페이지 로그인 서버(#2 서버)가 통합인증 서버에서 고객 코드를 받아오는 중 통신 오류가 발생하였다.

오류가 발생한 서버로 로그인한 이용자(A)는 통합인증 서버에서 고객 코드 값을 받아 오지 못해 고객 코드가 "null"로 처리되면서 이용자 A의 예약정보 내 고객 코드도 'null'로 등록되었고, 이후 이용자(B)도 해당 로그인 서버로 로그인하여 고객 코드가 'null'로 처리되면서 예약정보 조회시 A가 예약한 개인정보를 열람하였다.

1) (유출 규모 및 항목) 민원 내용과 로그기록*으로 1명의 개인정보 유출 확인

* 이름, 영문이름, 생년월일, 국적, 예약번호, 현지 연락처, 이메일, 핸드폰 번호, 여권번호, 여권 만료일, 여권 발행국, 항공사 마일리지 번호, 항공권 운임 정보(항공사 예약번호, 항공권 편명, 출발일 등), 결제정보(카드 소유주명, 신용카드번호, 결제금액 등)

2) 유출 인지 및 대응

일시		피심인의 유출 인지·대응 내용
'23. 10. 13.	11:15	로그인 서버#2가 LPOINT 통합회원 서버에서 고객 코드를 받아오지 못하는 오류 확인
'23. 10. 13.	11:40	로그인 서버#2 운영 중지하고 로그인 서버#1 단일 운영 실시
'23. 10. 13.	15:29	LPOINT 통합회원 서버에서 고객 코드를 받아오지 못하면(고객 코드 NULL) 로그인이 안 되도록 소스 코드 수정
'23. 10. 13	17:24, 17:32	개인정보 유출 통지(유선) 및 신고
'23. 10. 15.	18:46	로그인 서버#2의 인증서 갱신

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

서버 간 인증서 업데이트를 제대로 이행하지 않아 인증서 버전 불일치로 인한 통신 오류로 인해 타인에게 이용자의 개인정보가 노출되었으며, 열람권한이 없는 자에게 개인정보가 공개되지 않도록 처리시스템 등에 필요한 조치를 충분히 하지 않은 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '24. 8. 20. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '24. 9. 4. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

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

같은 법 시행령[2](이하 '시행령') 제30조제1항제3호는 "개인정보에 대한 접근을

통제하기 위해 ‘개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치(가목)’, ‘개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등으로서 보호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷망의 차단(나목)’, ‘그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치(다목)’를 해야 한다”라고 규정하고 있다.

한편, 시행령 제30조제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 「개인정보의 안전성 확보조치 기준[3]」(이하 ‘안전성 확보조치 기준’) 제6조제3항은 “개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

서버 간 인증서 업데이트를 제대로 이행하지 않아 인증서 버전 불일치로 인한 통신 오류로 타인에게 이용자의 개인정보가 노출되었으며, 피심인이 열람권한이 없는 자에게 개인정보가 공개되지 않도록 처리시스템 등에 필요한 조치를 충분히 하였다고 볼 수 없어 보호법 제29조, 같은 법 시행령 제48조의2제1항 및 안전성 확보조치 기준 제6조제3항 위반으로 판단된다.

< 피심인의 위반사항 >

위반행위	법률	舊 시행령	세부내용(고시 등)
안전조치의무	보호법 §29	§30① 제3호	• 처리 중인 개인정보가 열람 권한이 없는 자에게 공개되지 않도옥 조치를 취하지 않은 행위 (안전성 확보조치 기준 §6③)

Ⅳ. 처분 및 결정

2) 개인정보 보호법 시행령(대통령령 제33723호, 2023. 9. 12. 일부개정, 2023. 9. 15. 시행)
3) 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2023-6호, 2023. 9. 22. 시행)

1. 과태료 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제5호, 시행령 제63조 [별표2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[4](이하 '과태료 부과기준')에 따라 다음과 같이 부과한다.

가. 기준금액

시행령 제63조 [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) 위반에 대해서는 1회 위반에 해당하는 과태료인 600만 원을 기준금액으로 적용한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

(단위: 만 원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액		
		1회	2회	3회 이상
아. 법 제23조제2항·제24조제3항·제25조제6항(법 제25조의2 제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·**제29조(법 제26조제8항에 따라 준용되는 경우를 포함한다)를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우**	법 제75조 제2항제5호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) 과태료의 가중

1) **(과태료의 가중)** 과태료 부과기준 제7조는 '당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표3]의 가중기준(▲위반의 정도, ▲위반기간, ▲조사방해, ▲위반주도 등을 고려하여 가중사유가 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.'라고 규정하고 있다.

피심인의 보호법 제29조(안전조치의무) 위반행위는 과태료 부과기준 제7조 및 [별표3] 과태료의 가중기준에 해당하지 않아 가중없이 기준금액을 유지한다.

4) 개인정보 보호법 위반에 대한 과태료 부과기준(개인정보보호위원회 지침, 2023. 9. 15. 시행)

2) 과태료의 감경

과태료 부과기준 제6조는 “당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 감경기준(▲당사자 환경, ▲위반정도, ▲개인정보보호 노력정도, ▲조사협조 및 자진시정 등을 고려하여 감경사유가 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.“라고 규정하고 있고, 제6조제2항은 ”[별표2]의 각 기준에 따른 과태료 감경 시 그 사유가 2개 이상에 해당되는 경우에는 기준금액의 50을 초과할 수 없다.‘라고 규정하고 있다.

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 ‘과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우’, ‘조사에 적극 협력한 경우’에 해당하여 기준금액의 40%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 360만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제)	600만 원	-	240만 원	**360만 원**
계				**360만 원**

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무)를 위반한 행위에 대하여 같은 법 제75조(과태료)제2항제6호·12호의3에 따라 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(당사자 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료 납입 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다.

2024년 10월 23일

위 원 장 이 문 한 (서 명)

위 원 박 상 희 (서 명)

위 원 조 소 영 (서 명)