개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2024-014-195호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인

의결연월일 2024. 8. 28.

주 문

1. 피심인에 대하여 다음과 같이 과징금, 과태료를 부과한다.

가. 과 징 금 : 원

나. 과 태 료 : 3,000,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

이 유

Ⅰ. 기초 사실

피심인은 온라인 숙박 예약을 위한 웹( )·앱 서비스를 제공하는 「舊 개인정보 보호법」[1](이하 '舊 보호법')에 따른 정보통신서비스 제공자이며, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인이 이용자의 개인정보가 다른 이용자에게 노출된 사실을 인지하고 개인정보 유출신고('23. 4. 7.)함에 따라 개인정보 취급·운영 실태 및 舊 보호법 위반 여부를 조사('23. 11. 21. ~ '24. 6. 7.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 온라인 숙박 예약 서비스를 운영하면서 '23. 11. 30.(자료제출일) 기준 건의 개인정보를 수집하여 보관하고 있다.

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

< 개인정보 수집현황 >

구분	항목	기간	건수(명)

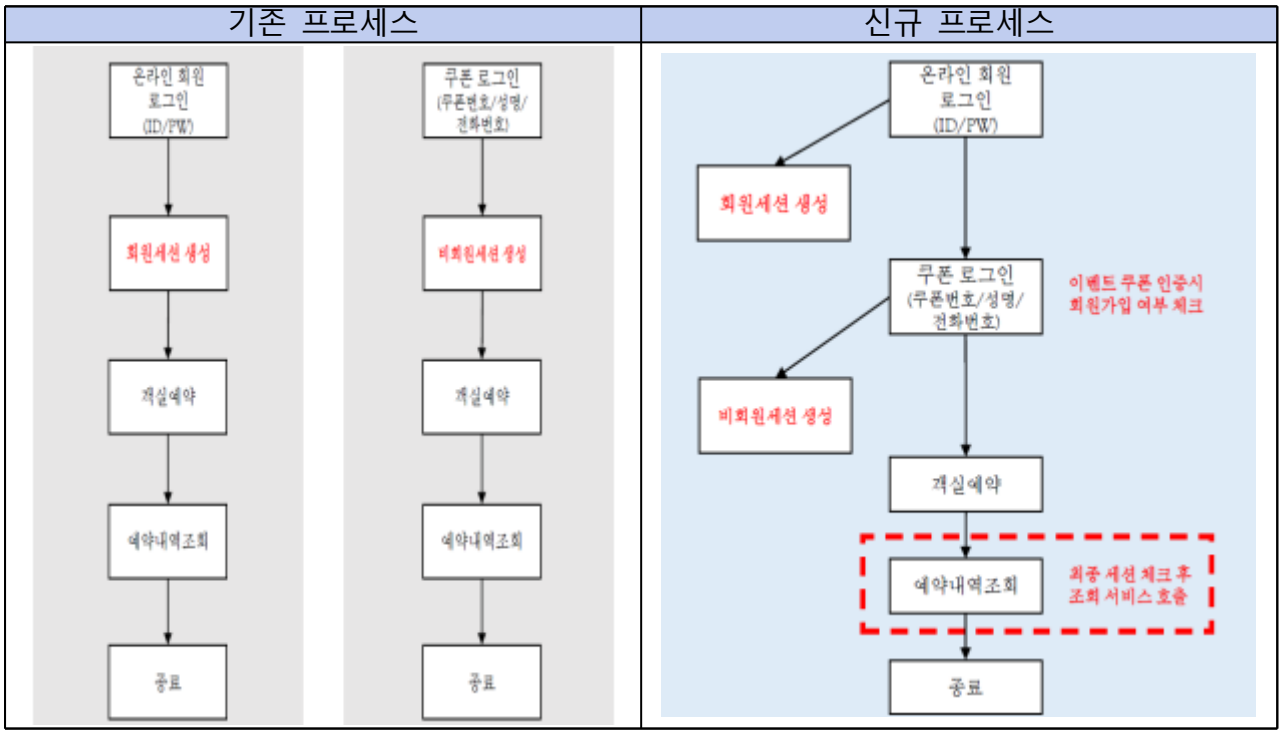
※ 수집일은 멤버십 서비스 시작일

나. 개인정보 유출 관련 사실관계

'23.3.23. 피심인이 적용한 새로운 쿠폰 사용 프로세스*에 따른 회원 로그인과 쿠폰 로그인 간 세션 오류로 '23.4.6. ~ 4.7. 이용자(20개 계정)가 홈페이지상의 '예약 내역' 조회 시 타인의 예약 정보가 노출되었다.

* (기존) 쿠폰 사용은 비회원 상태에서만 이용(쿠폰 로그인)
→ (변경) 회원 로그인 후 쿠폰 사용 가능

<숙박 예약 프로세스 흐름도(피심인 제출 자료)>



<사고 상세 내역>

①회원 로그인 후 예약 내역 조회 페이지에 대기 상태 유지
②신규 브라우저/새창을 통해 회원 로그인 및 쿠폰 로그인
③대기 상태에 있던 예약 조회 화면에서 조회 처리
④쿠폰 사용을 위해 쿠폰 로그인한 회원은 회원 고객번호가 아닌 쿠폰 판매 대행사의 고객번호로 세션 처리
⑤해당 대행사가 발행한 쿠폰으로 예약한 내역 모두 조회 가능

※ 피심인은 쿠폰 판매 대행사에도 고객번호를 부여하고 있으며, 이용자가 쿠폰 로그인 시 해당 대행사의 고객번호가 세션 정보로 저장됨

또한, '23.4.6. 이용자 명은 예약 목록(엑셀파일)을 다운로드*하였다.

* 피심인은 기업 회원의 편의를 위해 소속 직원의 예약 정보를 일괄 다운로드할 수 있는 기능을 제공 중이었음

1) (유출 항목 및 규모) ①예약내역 페이지에서 열람 가능한 이용자 명의 개인정보* 건, ②개인회원이 엑셀파일로 다운로드한 이용자 명의 개인정보**

* (항목) 이름, 예약 내역(숙박일, 리조트, 객실, 요금)
(규모) 해당 페이지 접근 건수(건) × 페이지당 열람 가능 건수(건) = 건

** (항목) 이름, 휴대전화번호, 예약 내역(숙박일, 리조트, 객실, 요금)
(규모) 이름 및 휴대전화번호를 기준으로 중복 제거

2) 유출 인지 및 대응

일 시		유출 인지 및 대응 내용
'23. 4. 6.	18:11	타인의 개인정보 노출 관련 고객 민원 제기
'23. 4. 7.	08:44	고객 민원 확인하여 **유출 인지**
	14:14	개인정보 포털에 **개인정보 유출 신고**
	17:30	피심인의 홈페이지에 **유출 사실 공지**
	18:55	유출 가능성이 있었던 전체 이용자(해당 기간 예약자 명(중복 제거). 건 발송 실패)에게 **개인정보 유출 통지**

일 시	유출 인지 및 대응 내용
’23. 4. 7.	예약 내역 조회 시 비밀번호 인증 추가, 로그인 세션 인증 로직 보완, 엑셀파일 다운로드 기능 일시 정지
‘23. 4. 8. ~ 4. 18.	예약 저장·변경 시 비밀번호 추가 인증 적용, 엑셀파일 다운로드 제한(기업 고객 한정, 비밀번호 인증 추가), 홈페이지 다중 브라우저 및 새창 열기 제한
’23. 4. 12.	

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 ’23. 3. 23.에 쿠폰 활용 회원 로그인 프로세스를 변경하면서 타인의 개인정보 열람 가능성에 대한 사전 검증을 소홀히 한 사실이 있다.

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 ‘24. 6. 10. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’24. 6. 26. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

舊 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 ‘舊 시행령’) 제48조의2제1항제2호는 “개인정보에 대한

2) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2020. 10. 20. 시행

불법적인 접근을 차단하기 위해 ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다. 또한, 舊 시행령 제48조의2제3항은 “제1항에 따른 안전성 확보조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다

한편, 舊 시행령 제48조의2제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 舊 개인정보의 기술적·관리적 보호조치 기준[3](이하 ‘舊 기술적 보호조치 기준’) 제4조제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있다.

舊 기술적 보호조치 기준 해설서는 고시 제4조제9항에 대해 “인터넷 홈페이지를 통한 개인정보 유·노출 방지를 위해 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안기술 적용, 운영 및 관리 측면에서의 개인정보 유·노출 방지 조치를 하여야 하며, 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등에 관한 보호조치를 하여야 한다.”다고 규정하고 있다.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

피심인이 타인의 개인정보 열람 가능성이 있는 형태로 시스템을 개발하고도 운영 전 검증을 소홀히 한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제9항을 위반한 것이다.

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

< 피심인의 위반사항 >

위반행위	법률	舊 시행령	세부내용(고시 등)
안전조치의무	舊 보호법 §29	§48의2① 제2호	・열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위 (舊 기술적 보호조치 기준 §4⑨)

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 舊 보호법 제29조 위반에 대한 과징금은 舊 보호법 제39조의15제1항제5호, 舊 시행령 제48조의11제1항과 제4항, [별표 1의5] (과징금의 산정기준과 산정절차) 및 舊 개인정보보호 법규 위반에 대한 과징금 부과기준[4](이하 '舊 과징금 부과기준')에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 위반행위와 관련된 舊 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제39조의15, 舊 시행령 제48조의11에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도 연평균 매출액(다만, 해당 사업연도 첫날 현재 사업을 개시한지 3년이 되지 않은 경우에는 그 사업개시일부터 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액)의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의·중과실 여부

舊 과징금 부과기준 제5조제1항은, 舊 시행령 [별표 1의5] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 舊 시행령 제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단하도록 규정

4) 개인정보보호위원회고시 제2022-3호, 2022. 10. 20. 시행

하고 있다.

이에 따를 때, 피심인의 행위가 고의성이 없고 단순 과실로 보이는 점을 고려하면 피심인에게 중과실이 있다고 보기 어렵다.

2) 중대성의 판단

舊 정보통신망법상 과징금 부과기준 제5조제2항은 '정보통신서비스 제공자등에게 고의·중과실이 없으면 위반행위의 중대성을 보통 위반행위로 판단한다.'라고 규정하고 있다.

또한, 舊 과징금 부과기준 제5조제3항은 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하도록 규정하고 있다. 다만, 舊 과징금 부과기준 제5조제3항 단서에서 위반행위의 결과가 ▲위반 정보통신서비스 제공자등이 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ▲이용자의 개인정보가 공중에 노출되지 않은 경우(제3호) 중 모두에 해당하는 경우 '보통 위반행위'로, 1개 이상 2개 이하에 해당하는 경우 '중대한 위반행위'로 감경하도록 규정하고 있다.

피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단하더라도 수집·보유 중인 이용자의 개인정보 % 미만이 개별적으로 다른 이용자에게 노출된 점을 고려하였을 때, '위반행위로 인해 직접적으로 이득을 취하지 않은 경우(제1호)', 피해규모가 보유 중인 개인정보의 5% 이내(제2호), 공중에 노출되지 않은 경우(제3호)에 모두 해당하여 '보통 위반행위'로 판단한다.

3) 기준금액 산출

피심인의 관련 매출액은 피심인이 운영하는 홈페이지( )를 통해 발생한 매출액으로 하고, 직전 3개 사업년도의 연평균 매출액 천 원에 舊 보호법 시행령 [별표 1의5] 2. 가. 1)에 따른 '보통 위반행위'의 부과기준율 1천분의 15을

적용하여 기준금액을 천 원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천 원)

구 분	2020년	2021년	2022년	평 균

* 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

<舊 시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
보통 위반행위	**1천분의 15**

다. 필수적 가중 및 감경

舊 과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 1년 이내('23. 3. 23. ~ '23. 4. 6.)이므로 '단기 위반행위'에 해당하므로 기준금액을 유지하고,

최근 3년 이내 舊 보호법 제39조의15제1항 각호에 해당하는 행위로 과징금 처분을 받은 적이 없으므로 기준금액의 100분의 50에 해당하는 천 원을 감경한다.

라. 추가적 가중 및 감경

舊 과징금 부과기준 제8조는 사업자의 위반행위의 주도 여부, 조사 협력 여부 등을 고려하여 필수적 가중 · 감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

이에 따를 때, 피심인이 ▲조사에 적극 협력한 점, ▲개인정보 유출사실을 자진신고한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의

100분의 20에 해당하는 천 원을 감경한다.

마. 부과과징금의 결정

舊 과징금 부과기준 제9조제1항은 ▲위반행위자의 현실적인 부담 능력, ▲위반행위로 발생한 정보주체의 피해 및 배상의 정도, ▲위반행위자가 속한 시장·산업 여건 등(1. 위반행위자의 자산, 자기자본 등 재무상황에 비추어 위반행위자가 과징금을 부담할 능력이 현저히 부족하다고 객관적으로 인정되는 경우, 2. 개인정보 분쟁조정, 민사조정 등을 통해 정보주체에게 발생한 피해에 대한 원상회복, 손해배상 또는 이에 상당하는 필요한 피해구제 조치를 한 경우, 3. 경제위기 등으로 위반행위자가 속한 시장·산업 여건이 현저하게 변동되거나 지속적으로 악화된 상태인 경우)을 고려하여 제8조에 따라 산정된 과징금이 과중하다고 인정되는 경우에는 해당 금액의 100분의 90 범위에서 감경할 수 있다’라고 규정하고 있다.

피심인은 유출 가능성이 있었던 전체 이용자( )에게 총 원 이상의 피해 보상( )을 완료하고, 정보보안 시스템 운영, 매년 2회이상 취약점 모의침투 테스트 실시 등 개인정보 보호 활동을 적극적으로 이행하고 있는 점을 종합적으로 고려하여 舊 과징금 부과기준 제9조제1항제2호에 따라 추가적 가중 및 감경을 거친 금액의 100분의 30에 해당하는 천 원을 감경한다.

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15제1항제5호, 舊 시행령 제48조의11, [별표 1의5] 2. 가. 1)(과징금의 산정기준과 산정절차) 및 舊 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액인 천 원을 최종 과징금으로 결정한다.

< 과징금 산출 내역(안) >

①기준금액	②필수적 가중·감경	③추가적 가중·감경	④부과과징금의 결정	⑤최종과징금

* 보통 위반 : 고의·중과실 없음, ▲위반행위로 직접 취한 이득 없음, ▲피해 규모 5% 이내, ▲공중 미노출 3개 요건에 해당

2. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대한 과태료는 같은 법 제75조제2항제6호, 舊 시행령 제63조, 舊 시행령 [별표2] '과태료의 부과기준' 및 舊 개인정보 보호법 위반에 대한 과태료 부과기준[5](이하 '舊 과태료 부과기준'이라 한다)에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

舊 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 각 위반행위별 기준금액을 600만원으로 산정한다.

< 舊 시행령 [별표2] 2. 개별기준 >

(단위: 만 원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 또는 **제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우**	법 제75조 제2항제6호	600	1,200	2,400

5) 개인정보보호위원회지침, 2023. 3. 8. 시행

나. 과태료의 가중 및 감경

1) (과태료의 가중) 舊 과태료 부과기준 제8조는 '사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정하고 있다.

피심인의 경우, 舊 과태료 부과기준 제8조 및 [별표2] 과태료의 가중기준에 해당하지 않아 가중없이 기준금액을 유지한다.

2) (과태료의 감경) 舊 과태료 부과기준 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.'라고 규정하고 있다.

피심인의 경우, 舊 과태료 부과기준 제7조 및 [별표1] 과태료의 감경기준에 따라 '과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우', '조사에 적극 협력한 경우'에 해당하여 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 300만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무(접근통제)	600만 원	-	300만 원	**300만 원**
계				**300만 원**

Ⅴ. 결론

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대해 같은 법 제39조의15(과징금 부과 등에 대한 특례)제1항제5호, 제75조(과태료)제2항제6호에 따라 과징금 부과, 과태료 부과를 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.

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 8월 28일

위 원 장 고 학 수 (서 명)

부위원장 최 장 혁 (서 명)

위 원 김 일 환 (서 명)

위 원 김 진 욱 (서 명)

위 원 김 진 환 (서 명)

위 원 박 상 희 (서 명)

위 원 윤 영 미 (서 명)

위 원 이 문 한 (서 명)

위 원 조 소 영 (서 명)