개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 제2024-219-622호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인

의결연월일 2024. 9. 25.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 7,200,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대한 과태료 부과의 내용 및 결과를 개인정보보호위원회 홈페이지에 1년간 공표한다.

이 유

Ⅰ. 기초 사실

웹( )·앱( )으로 여행상품 예약 서비스를 운영하는 피심인은 「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 개인정보 포털(privacy.go.kr)에 유출 신고('23. 4. 17.)한 피심인에 대하여 개인정보 취급·운영 실태 및 舊 보호법 위반 여부를 조사('23. 11. 7. ~ '24. 4. 17.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 여행상품 예약 서비스를 운영하면서, '24. 4. 12. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

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

< 개인정보 수집 현황 >

구분	항목	수집일	건수

나. 개인정보 유출 관련 사실관계

’23. 4. 17. 10:00 경 피심인이 운영중인 앱에서 진행한 여행상품 이벤트 직후 이용자가 크게 증가하자 오류*가 발생하여 일부 이용자가 다른 이용자의 정보로 중복 로그인 처리되어 개인정보가 유출되었다.

* 이용자가 로그인 하는 경우 웹 서버에서 세션 확인을 위해 세션키( )를 생성 후 이용자 ID와 매칭하나, 이벤트 직후 이용자 접속이 크게 증가하자 동일한 세션키가 다수의 이용자에게 매칭되는 오류가 발생하여 첫 번째로 세션키를 받은 이용자의 정보로 다른 이용자가 중복 로그인 처리되었음

1) (유출 규모 및 항목) 이용자의 명의 개인정보*가 유출되었다.

* 이름, 핸드폰 번호

2) 유출 인지 및 대응

일 시		유출 인지 및 대응 내용
’23. 4. 17.	10:00	피심인 여행상품 이벤트 시작
’23. 4. 17.	10:06	고객센터로 타인의 개인정보가 보인다는 민원이 접수되어 **개인정보 유출 인지**
’23. 4. 17.	10:55	이벤트 중지, 세션키 중복으로 인한 개인정보 유출 원인분석 및 해당 이용자 로그아웃 처리
’23. 4. 17.	11:54	세션키 중복 전달 방지를 위한 소스코드 변경
’23. 4. 17.	17:00	개인정보 포털에 개인정보 **유출신고**
’23. 5. 15.	15:47	개인정보 **유출 통지**(이메일)
’24. 4. 23.	11:01	개인정보 **유출 추가 통지**(이메일)

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인이 여행상품 앱 서비스를 운영하면서 앱 접속자 증가에 따른 세션 중복 오류 발생 가능성 등에 대한 사전 검증 없이 시스템에 적용하는 등 유출방지 조치를 소홀히 한 사실이 있다.

나. 개인정보 유출 통지를 소홀히 한 행위

피심인은 ’23. 4. 17.에 개인정보 유출 사실을 인지하였으나, 정당한 사유 없이 24시간이 경과한 ’23. 5. 15., ’24. 4. 23. 이용자 대상 유출 통지한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’24. 4. 19. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’24. 5. 7. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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 불법적인 접근을 차단하기 위하여 ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등을 하여야 한다.”라고 규정하고 있다.

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

舊 시행령 제48조의2제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

舊 시행령 제48조의2제3항에 따라 위 기준 수립·시행의 내용을 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.

나. 舊 보호법 제39조의4제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체 없이 유출등이 된 개인정보 항목(제1호), 유출등이 발생한 시점(제2호), 이용자가 취할 수 있는 조치(제3호), 정보통신서비스 제공자등의 대응 조치(제4호), 이용자가 상담 등을 접수할 수 있는 부서 및 연락처(제5호)를 해당 이용자에게 알리고 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.”라고 규정하고 있다.

舊 시행령 제48조의4제2항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제39조의4제1항 각 호의 모든 사항을 서면등의 방법으로 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고해야 한다.”라고 규정하고 있으며, 제3항은 “정보통신서비스 제공자등은 제2항에 따른 통지·신고를 하려는 경우에는 법 제39조의4제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.”라고 규정하고 있다.

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

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

피심인이 ’21. 6. 23.* ~ ’23. 4. 17. 동안 여행상품 앱 서비스를 운영하면서 앱 접속자 증가에 따른 세션 중복 오류 발생 가능성 등에 대한 사전 검증 없이 시스템에 적용하는 등 개인정보 유출 방지조치를 소홀히 한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제9항을 위반한 것이다.

* 문제가 된 소스코드 변경 이력은 피심인이 형상관리시스템을 구축한 '21.6.23.부터 확인이 가능하였음

나. 개인정보 유출 통지를 소홀히 한 행위

[舊 보호법 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항)]

피심인이 ’23. 4. 17. 개인정보 유출 사실을 인지하였으나, 정당한 사유 없이 24시간을 경과하여 ’23. 5. 15., ’24. 4. 23. 유출 통지를 한 행위는 舊 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반	舊 보호법 §29	舊 시행령 §48의2①	• 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위 (舊 기술적 보호조치 기준 §4⑨)
개인정보 유출등의 통지·신고에 대한 특례 위반	舊 보호법 §39의4①	舊 시행령 §48조의4	• 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 유출 통지한 행위

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무) 및 제39조의4(개인정보의 유출등의

통지·신고에 대한 특례)제1항 위반행위에 대한 과태료는 같은 법 제75조제2항제6호·제12호의3, 舊 시행령 제63조, 舊 시행령 [별표2] '과태료의 부과기준' 및 '舊 개인정보 보호법 위반에 대한 과태료 부과기준[4]'(이하 '舊 과태료 부과지침')에 따라 다음과 같이 부과한다.

가. 기준금액

舊 시행령 제63조와 [별표2] '과태료의 부과기준'은 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 위반행위의 기준금액을 600만 원으로 산정한다.

< 舊 시행령 [별표2] 과태료의 부과기준 중 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 **제29조**를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
도. 법 **제39조의4제1항**(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·보호위원회 및 전문기관에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제75조 제2항제12호의3	600	1,200	2,400

나. 과태료의 가중 및 감경

1) 과태료의 가중

舊 과태료 부과지침 제8조는 '사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여, 舊 과태료 부과지침의 '[별표2] 과태료의 가중기준(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인

4) 개인정보보호위원회지침, 2023. 3. 8. 시행

정되는 경우)‘에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.’라고 규정하고 있다.

피심인의 舊 보호법 제29조(안전조치의무) 위반행위 및 같은 법 제39조의4(개인정보 유출 등의 통지·신고에 대한 특례)제1항 위반행위에 대해 ▲법 위반상태의 기간이 3개월 이상 지속된 경우에 해당하여 기준금액의 10%를 각각 가중한다.

※ 위반기간 : §29(’21.6.23. ~ ’23.4.17.), §39의4①(’23.4.17. ~ ‘24.4.23.)

2) 과태료의 감경

舊 과태료 부과지침 제7조는 ‘사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여, 舊 과태료 부과지침의 ’[별표1] 과태료의 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.

피심인은 ▲과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우(50% 이내), ▲조사에 협조한 경우(40% 이내)에 해당하여 최대 감경 범위인 기준금액의 50%를 각각 감경한다.

다. 최종 과태료

피심인이 舊 보호법 제29조(안전조치의무) 및 제39조의4(개인정보 유출 등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 720만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만원	60만원	300만원	**360만원**
개인정보 유출등의 통지·신고에 대한 특례 위반 (통지 지연)	600만원	60만원	300만원	**360만원**
합 계				**720만원**

2. 결과 공표

舊 보호법 제66조제1항 및 「舊 개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 '위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)'에 해당하므로, 피심인이 舊 보호법 제29조(안전조치의무) 위반으로 과태료를 부과받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다. 다만, 개정된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침(2023. 10. 11. 개인정보보호위원회 의결)」에 따라 공표 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		舊 보호법* 제29조	안전조치의무 위반 (접근통제)	2024. 9. 25.	과태료 360만 원

* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호

2024년 9월 25일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4제1항(개인정보 유출등의 통지 · 신고에 대한 특례) 위반행위에 대해 같은 법 제75조(과태료)제2항제6호·제12호의3, 제66조(결과의 공표)제1항에 따라 과태료 부과, 결과 공표를 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 9월 25일

위 원 장 김 진 욱 (서 명)

위 원 김 진 환 (서 명)

위 원 박 상 희 (서 명)