

개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의 · 의결

안 건 번 호 제2024-221-667호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인

의결연월일 2024. 11. 4.

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

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

이 유

I. 기초 사실

피심인은 해외구매대행 서비스 홈페이지()를 운영하는 「舊 개인정보 보호법」¹⁾(이하 '舊 보호법'이라 한다)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. 2. 8.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('23. 6. 3. ~ '24. 5. 17.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 해외구매대행 서비스 홈페이지()를 운영하면서 '23. 6. 3. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

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

< 개인정보 수집현황 >

구분	항목	수집일	건수

나. 개인정보 유출 관련 사실관계

‘23. 2. 6. 신원 미상의 자(이하 ‘해커’)가 알 수 없는 방법으로 취득한 피심인의 관리자 계정으로 홈페이지에 접속하고 게시판에 웹셀을 업로드하여 DB 접속 및 개인정보를 다운로드한 후 일부 이용자 대상으로 스팸문자를 발송하였다.

피심인은 ‘22. 6. 15. ~ ‘23. 2. 8. 동안 DB 접속 권한을 IP 주소 등으로 제한하지 않는 등 침입탐지·차단시스템 설치·운영을 소홀히 하였고, 외부에서 관리자 페이지 접속시 아이디, 비밀번호 외에 안전한 인증수단을 적용하지 않았다.

1) (유출 규모 및 항목) 이용자 19,403명의 개인정보*가 유출되었다.

* 아이디, 비밀번호(SHA-512 암호화), 이름, 이메일, 주소, 전화번호, 주문내역

2) (유출 인지 및 대응) 유출 인지 후 24시간을 경과하여 유출 신고하였다.

일시		피심인의 유출 인지·대응 내용
‘23. 2. 6.	12:50	개인정보를 유출한 해커로부터 협박 메일 수신 및 개인정보 유출 인지
‘23. 2. 6.	15:31	유출 사실 홈페이지 공지
‘23. 2. 7.	15:42	유출 사실 통지(이메일)
‘23. 2. 8.	23:24	개인정보 유출 신고
‘23. 2. 8.	-	관리자 페이지 기본 경로 변경 및 접근통제 설정
‘23. 2. 9.	-	관리자 페이지 로그인 시 2차 인증 적용

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 '22. 6. 15. ~ '23. 2. 8. 동안 개인정보처리시스템(DB) 접속 권한을 IP 주소 등으로 제한하지 않는 등 침입탐지·차단시스템 설치·운영을 소홀히 하였고, 외부에서 개인정보 처리시스템(관리자 페이지)에 접속할 경우 아이디, 비밀번호 외에 안전한 인증수단을 적용하지 않고 운영한 사실이 있다.

나. 개인정보 유출 신고를 소홀히 한 행위

피심인은 '23. 2. 6. 해커로부터 협박 메일을 수신하여 이용자의 개인정보가 유출된 사실을 인지하였으나, 정당한 사유 없이 24시간 경과한 '23. 2. 8. 23:24 유출 신고한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '24. 5. 20. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '24. 5. 24. 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 시행령²⁾(이하 '舊 시행령') 제48조의2제1항제2호는 “개인정보에 대한 불법

적인 접근을 차단하기 위해 '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)' 등의 조치를 하여야 한다."라고 규정하고 있다.

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 기준³⁾(이하 '舊 기술적 보호조치 기준') 제4조제4항은 "개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야" 하고, 제4조제5항은 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능(1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한)을 포함한 시스템을 설치·운영하여야 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 사

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

3) 개인정보보호위원회 고시 제2021-3호, 2021. 9. 15. 시행

항에 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.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

피심인이 '22. 6. 15. ~ '23. 2. 8. 동안 개인정보처리시스템(DB) 접속 권한을 IP 주소 등으로 제한하지 않는 등 침입탐지·차단시스템 설치·운영을 소홀히 하고, 외부에서 개인정보 처리시스템(관리자 페이지)에 접속하는 경우 아이디, 비밀번호 외 안전한 인증수단을 적용하지 않고 운영한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제4항·제5항을 위반한 것이다.

나. 개인정보 유출 통지를 소홀히 한 행위

[舊 보호법 제39조의4제1항(개인정보의 유출등의 통지·신고에 대한 특례)]

피심인은 '23. 2. 6. 12:50 해커로부터 협박 메일을 수신하여 이용자의 개인정보가 유출된 사실을 인지하였으나, 정당한 사유 없이 24시간 경과한 '23. 2. 8. 23:24 유출 신고한 행위는 舊 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	舊 시행령	세부내용(고시 등)
안전조치의무	舊 보호법 §29	舊 시행령 §48의2①	<ul style="list-style-type: none"> 외부에서 개인정보처리시스템 접속시 안전한 인증수단을 적용하지 않은 행위 (舊 기술적 보호조치 기준 §4④) 개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하지 않은 행위 (舊 기술적 보호조치 기준 §4⑤)
개인정보 유출등의 통지·신고에 대한 특례	舊 보호법 §39의4①	舊 시행령 §48조의4	<ul style="list-style-type: none"> 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 유출 신고한 행위

IV. 처분 및 결정

1. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4제1항(개인정보 유출 등의 통지·신고에 대한 특례) 위반행위에 대한 과태료는 같은 법 제75조제2항제6호·12호의3, 舊 시행령 제63조, 舊 시행령 [별표2] '과태료의 부과기준' 및 개인정보 보호법 위반에 대한 과태료 부과기준⁴⁾(이하 '과태료 부과기준'이라 한다)에 따라 다음과 같이 과태료를 부과한다.

※ '질서위반행위규제법' 제3조(법 적용의 시간적 범위)제2항에 따라 '질서위반행위 후 법률이 변경되어 과태료가 변경되기 전의 법률보다 가볍게 된 때'에 해당하므로 과태료 부과 시 피심인에게 유리하게 변경된 「개인정보 보호법 위반에 대한 과태료 부과기준(개인정보위 지침, '23.9.15.시행)」을 적용함

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 위반행위 기준 금액을 600만원으로 산정한다.

< 舊 시행령 [별표2] 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
도. 법 제39조의4제1항(제39조의14에 따라 준용되는 경우를 포함 한다)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

4) 개인정보보호위원회 지침, 2023. 9. 15. 시행

나. 과태료의 가중 및 감경

1) (과태료의 가중) 과태료 부과기준 제7조는 '사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표3]의 가중기준(▲위반의 정도, ▲위반 기간, ▲조사 방해, ▲위반 주도)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.'라고 규정하고 있다.

피심인의 경우, 가중 사유에 해당하지 않아 기준금액을 유지한다.

2) (과태료의 감경) 과태료 부과기준 제6조는 '사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 감경기준(▲당사자 환경, ▲위반정도, ▲업무형태 및 규모, ▲개인정보보호 노력정도, ▲조사 협조 및 자진 시정 등)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있으며, 감경사유가 2개 이상 해당되는 경우에는 합산하여 감경하되 기준금액의 100분의 90을 초과할 수 없다.'라고 규정하고 있다.

피심인의 경우, 舊 보호법 제29조(안전조치의무) 및 제39조의4제1항(개인정보 유출등의 통지·신고에 대한 특례) 위반행위에 대해 ▲「중소기업기본법」제2조에 따른 소기업(小企業)인 경우, ▲시정을 완료한 경우, ▲조사에 적극 협력한 경우에 해당하여 기준금액의 70%를 각각 감경한다.

다. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4제1항(개인정보 유출등의 통지·신고에 대한 특례) 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 360만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제)	600만원	-	420만원	180만원
개인정보 유출통지·신고 특례 (신고 지연)	600만원	-	420만원	180만원
계				360만원

2. 결과 공표

舊 보호법 제66조제1항 및 '舊 개인정보 보호위원회 처분결과 공표기준5)」제2조(공표요건)에 따라, 피심인의 위반행위는 舊 보호법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우(제4호), 위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)에 해당하므로, 과태료를 부과받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다. 다만, 개정된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침6)」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 (접근통제)	2024. 11. 4.	과태료 180만 원
		舊 보호법 제39조의4	개인정보 유출통지·신고 특례		과태료 180만 원
* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호					
2024년 11월 4일 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.

5) 개인정보보호위원회지침, 2020. 11. 18. 시행

6) 개인정보보호위원회지침, 2023. 10. 11. 시행

이의제기 방법 및 기간

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제 20조의 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 11월 4일

위 원 장 이 문 한 (서 명)

위 원 박 상 희 (서 명)

위 원 조 소 영 (서 명)