개 인 정 보 보 호 위 원 회

제2소위원회

심의·의결

안 건 번 호 제2024-215-538호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치 등에 관한 건

피 심 인

의결연월일 2024. 7. 24.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 4,200,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 개인정보 처리 실태의 개선을 권고한다.

가. 피심인은 보호법 제34조제2항에 따라 개인정보 유출 및 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치*를 하여야 한다.

* 유출 대응체계 구축, 피해 최소화 및 긴급 조치, 피해 구제 및 재발 방지 등

※ 자세한 사항은「개인정보 유출 등 사고대응 매뉴얼」(2023.9.) 참고
(개인정보 포털(www.privacy.go.kr) → 자료 → 자료보기(지침자료)에서 검색 가능)

나. 가.의 개선권고를 이행하기 위하여 성실하게 노력하고, 개선권고 통지를 받은 날로부터 30일 이내에 그 조치 결과를 개인정보보호위원회에 제출하여야 한다.

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 온라인으로 유사 투자자문 서비스를 제공( )하는 「舊 정보통신망 이용촉진 및 정보보호 등에 관한 법률」[1](이하 '舊 정보통신망법'이라 한다) 및 「舊 개인정보 보호법」[2](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 서울경찰청에서 피심인의 개인정보 유출 발생 사실 통보('22. 2. 15.) 및 피심인이 개인정보 유출신고('21. 11. 22.)함에 따라 개인정보 취급·운영 실태 및 舊 보호법 위반 여부를 조사('22. 7. 6. ~ '24. 3. 18.) 하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

1) 법률 제16021호, 2018. 12. 24, 일부개정, 2019. 6. 25. 시행
2) 법률 제16930호, 2020. 2. 4. 일부개정, 2020. 8. 5. 시행

피심인은 온라인으로 유사 투자자문 서비스를 제공하면서 ’23. 1. 19. 기준 건의 개인정보를 수집하여 보관하고 있다.

구분	항목	기간	건수
계			

나. 개인정보 유출 관련 사실관계

경찰은 신원 미상의 자(이하 ‘해커’라 한다)가 최소 ‘20. 3. 22. ~ ’20. 4. 23.동안 매크로 프로그램으로 사전에 알고 있던 아이디와 비밀번호를 자동 입력하는 공격 기법으로 로그인에 성공하는 경우 해당 계정의 개인정보를 유출했다고 보았으나, 피의자 진술을 제외하고는 로그기록도 없는 등 증빙이 부족하여 해킹을 통해 개인정보가 유출되었다고 인정하기 어려운 상황이었다.

또, 경찰 참고인 조사 시점(‘21.11.)이 실제 해킹 시점(’20.3~4)보다 20개월 이상 경과되어 피심인은 개인정보 접근 여부를 확인할 수 있는 접속기록을 보존·관리하고 있지 않아, 해킹사고 당시 시스템 운영환경도 변경되어 세부 유출경위·시기 파악이 불가하고 안전조치 의무 준수 여부도 확인할 수 없었다.

※ 해커가 다른 사이트 계정에 침입할 당시 할당받은 IP 주소와 동일 IP 주소로 계정에 접근한 기록을 해커가 접근한 기록으로 판단

1) (유출 규모 및 항목)

※ 유출 규모는 경찰 통보 자료(해커 보유 자료)와 피심인이 보유한 정보 일치 여부를 통해 확인하였으며, 정보 일치 여부는 ID만 확인

2) 유출 인지 및 대응

일 시	유출 인지 및 대응 내용
’21. 11. 17.	경찰 참고인 조사
’21. 11. 22.	개인정보 포털에 개인정보 유출 신고
’23. 2. 1.	이용자에게 개인정보 유출 통지

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 유출 통지를 소홀히 한 사실

피심인은 ‘21. 11. 17.에 개인정보 유출 사실을 인지*했음에도 정당한 사유 없이 24시간을 경과하여 ’21. 11. 22.에 유출 신고 및 ’23. 2. 1.에 유출 통지를 한 사실이 있다.

* 경찰 참고인 조사 시 피심인으로부터 해커 보유 자료와 실제 고객정보 일치 여부를 확인하여 유출 여부를 확인했으므로 참고인 조사 시점을 인지 시점으로 판단

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 ‘24. 3. 18. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 4. 3. 개인정보보호위원회에 의견을 제출하였다.

피심인은 경찰 참고인 조사 당시 유출된 DB 대조가 아닌 담당 수사관이 로그인을 시도하는 방식으로 진행했고, 총 11건의 로그인 시도 중 5건을 실패(6건 성공)하여 즉시 인지하지 못했으며, 그럼에도 유출 신고했고, 유출 항목 및 규모를 알 수 없어 유출 통지는 하지 못하다가 ’23. 2. 1. 개인정보보호위원회로부터 유출된 DB 대조 결과 확인 즉시 유출 통지했으므로 유출 통지·신고 위반이 아니라고 주장하나,

경찰 진술조서 확인 결과, 담당 수사관은 피심인에게 유출된 DB(엑셀파일 2개)를 제시 및 유출된 DB상 개인정보로 로그인 성공 시 유출로 판단하기로 피심인과 합의하였고, 일부 로그인에 성공한 바(정확한 건수는 미기재), 피심인은 유출을 인지했다고 판단되며, 유출 항목 등을 확인하지 못한 경우에는 유출 사실을 우선 통지해야 하므로 피심인의 주장을 받아들이지 아니한다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 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.

같은법 시행령[3](이하 ‘舊 시행령’이라 한다) 제48조의4제2항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제39조의4제1항 각 호의 모든 사항을 서면 등의 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 한

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

다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보 유출 통지·신고를 소홀히 한 사실

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

피심인이 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 통지·신고를 한 행위는 舊 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
개인정보 유출등의 통지·신고에 대한 특례	舊 보호법 §39의4①	舊 §48조의4	• 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 유출 통지·신고한 행위

Ⅳ. 시정조치(안)

1. 과태료 부과

가. 舊보호법 제39조의4 개인정보의 유출등의 통지·신고 위반 관련

피심인의 舊 보호법 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항 위반행위에 대한 과태료는 같은 법 제75조제2항제12호의3, 舊 시행령 제63조, [별표2] ‘과태료의 부과기준’ 및 ‘舊 개인정보 보호법 위반에 대한 과태료 부과기준[4]’(이하 ‘舊 과태료 부과지침’)에 따라 다음과 같이 과태료를 부과한다.

1) 기준금액

舊 시행령 제63조, [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에

4) 개인정보보호위원회지침, 2023. 3. 8. 시행

따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 각 위반행위별 기준금액을 600만원으로 산정한다.

< 舊 시행령 [별표2] 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
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

2) 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 인정되는 경우)'에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.'라고 규정하고 있다.

피심인의 경우, '위반행위가 2개에 해당하는 경우', '위반기간이 3개월 이상인 경우'에 해당하여 기준금액의 20%를 가중한다.

(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, ▲개인정보 보호 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, '시정조치를 완료한 경우(50% 이내)', '조사에 적극 협력한 경우(40%

이내)’에 해당하여 최대 감경 범위인 기준금액의 50%를 감경한다.

3) 최종 과태료

피심인의 舊 보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 420만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
개인정보 유출등의 통지·신고에 대한 특례	600만원	120만원	300만원	**420만원**
계				**420만원**

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, 과태료 부과에 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.

개인정보 보호법 위반 행정처분 결과 공표 개인정보 보호법 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* 제39조의4	개인정보 유출통지·신고 위반	2024. 7. 24.	과태료 420만 원
* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호					
2024년 7월 24일 개 인 정 보 보 호 위 원 회					

Ⅴ. 개선권고(안)

피심인에 대해 개인정보 보호법[5](이하 '보호법') 제61조에 따라 다음과 같이 개인정보 처리의 실태를 개선하도록 권고한다.

가. 피심인은 보호법 제34조제2항에 따라 개인정보 유출 및 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치*를 하여야 한다.

* 유출 대응체계 구축, 피해 최소화 및 긴급 조치, 피해 구제 및 재발 방지 등

※ 자세한 사항은「개인정보 유출 등 사고대응 매뉴얼」(2023.9.) 참고
(개인정보 포털(www.privacy.go.kr) → 자료 → 자료보기(지침자료)에서 검색 가능)

나. 가.의 개선권고를 이행하기 위하여 성실하게 노력하고, 개선권고 통지를 받은 날로부터 30일 이내에 그 조치 결과를 개인정보보호위원회에 제출하여야 한다.

5) 법률 제19234호, 2023. 3. 14. 일부개정, 2023. 9. 15. 시행

이의제기 방법 및 기간

피심인은 이 공표에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조에 따라 처분이 있음을 알게 된 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조에 따라 과태료 부과 통지를 받은 날부터 60일 이내에 개인정보보호위원회에 서면으로 이의제기를 할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조 제2항에 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 과태료 납입 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다.

2024년 7월 24일

위 원 장 김 진 욱 (서 명)

위 원 김 진 환 (서 명)

위 원 박 상 희 (서 명)