개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 제2025-208-197호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인 ㈜모우다 (사업자등록번호 :)

대표자
의결연월일 2025. 4. 23.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 5,400,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

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

이 유

Ⅰ. 기초 사실

피심인은 병의원 전용 신용대출상품 등 의료금융 분야에서 대출자와 투자자를 연결하는 플랫폼( )을 운영하는 「개인정보 보호법」[1](이하 '보호법')에 따른 개인정보처리자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	종업원 수(명)
㈜모우다				

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 포털(privacy.go.kr)에 유출 신고('24. 5. 9.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('24. 5. 29. ~ '24. 7. 10.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 의료금융 분야의 투자 중개 플랫폼을 운영하면서, '24. 5. 31. 기준, 15,618건의 개인정보*를 수집하여 보관하고 있다.

* 이메일, 주민등록번호, 주소, 성별, 생년월일, 계좌번호 등

나. 개인정보 유출 관련 사실관계

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

’24.5.3. 피심인은 제보자로부터 피심인 플랫폼의 개인정보 유출 정황 관련 화면 스크린샷(5장)을 제공받았고 이메일로 사실 확인을 요청받았다. 확인 결과 제공 화면은 피심인 플랫폼 이용자의 데이터 샘플이었으며, 피심인의 DB 테이블 구조 및 이용자 개인정보와 일치하였다.

제공 화면을 분석한 결과, ’19.1.22. ~ ’20.6.18.* 사이에 캡쳐된 것으로 추정되나, 피심인은 서버 이전(’21.7.) 및 시스템 변경**으로 해당 시점의 서버 로그기록, 시스템 운영 환경 등을 파악할 수 없어 유출 경위 확인에 어려움이 있었다.

* 제공 화면3에는 ’19.1.22. 발송한 이메일 소스코드가 캡쳐되어 있고, 화면4의 경우 공지사항 소스코드가 캡쳐되어 있는데 피심인은 해당 테이블 구조를 ’20.6.18. 변경했다고 소명(테이블 항목에 type 추가)

** 망분리, 클라우드로 서버 이전 등(’21.7.~8.말)

※ 피심인은 이전 서버 업체에 로그를 요청했으나, 방화벽 로그는 보관기간 최대 1년, WAF 로그는 계약 해지 시 삭제되어 로그를 받지 못하였다고 소명함

1) (유출 내용) 확인된 이메일 주소 165건

※ 제공 화면3(이메일 발송 제목 및 일부 이메일주소 리스트(17건) 표시)을 토대로 확인한 결과, 당시 피심인의 이메일 발송 대상자는 총 165건인 것으로 확인됨

- 다만, 유출 경위 확인이 어려워 정확한 유출 항목 및 규모는 미상

2) 유출 인지 및 대응

일시		피심인의 유출 인지·대응 내용
’24.5.3.	11:32	피심인은 제보자로부터 피심인 플랫폼의 개인정보 유출 관련 화면 스크린샷(5장)을 제공받았고 이메일로 사실 확인을 요청받았음
’24.5.3.		제공 화면1의 회원 DB 테이블 구조가 실제 DB 테이블 구조와 일치함 확인
’24.5.7.		제공 화면3의 개인정보(이메일 주소 17개)와 보유 개인정보가 일치함을 확인하여 **개인정보 유출 인지**
’24.5.9.	22:52	**개인정보 유출 신고**
’24.5.9.		홈페이지에 개인정보 유출사실 게시 ※ (피심인 소명) 피해 확산 방지를 위해 우선 유출 가능성이 있음을 알리는 것이 필요하다고 판단하여 신고
‘25.3.7.		**개인정보 유출 통지**

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 '16.10. ~ '21.7. 주민번호, 계좌번호 등을 안전하지 않은 알고리즘(RSA-512)으로 암호화하여 저장한 사실이 있다.

※ '21.7. 이전 시스템은 피심인이 보안업체 제출을 위해 보관중이던 캡쳐 파일, 내부 직원 간 주고받은 이메일 내역 등을 토대로 분석

나. 개인정보 유출 통지를 소홀히 한 행위

피심인은 '24. 5. 7. 개인정보 유출 사고가 발생한 사실을 인지하였음에도 불구하고 정당한 사유 없이 72시간을 경과하여 유출을 통지한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '24. 12. 3. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '24. 12. 17. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 舊 보호법[2] 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[3](이하 '시행령') 제48조의2제1항제4호는 "개인정보가 안전하게 저장 · 전송될 수 있도록 하기 위해 '주민등록번호, 계좌정보 및 제18조제3호에 따

2) 개인정보 보호법(법률 제16930호, 2020. 2. 4. 일부개정, 2020. 8. 5. 시행)
3) 개인정보 보호법 시행령(대통령령 제32813호, 2022. 7. 19. 일부개정, 2022. 10. 20. 시행)

른 정보 등 보호위원회가 정하여 고시하는 정보의 암호화 저장(나목)' 등을 해야 한다"라고 규정하고 있다.

한편, 시행령 제30조제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준[4]」(이하 '보호조치 기준') 제6조제2항은 "정보통신서비스 제공자등은 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다."라고 규정하고 있다.

나. 보호법 제34조제1항은 "개인정보처리자는 개인정보가 분실 · 도난 · 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 1. 유출등이 된 개인정보의 항목, 2. 유출등이 된 시점과 그 경위, 3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, 4. 개인정보처리자의 대응조치 및 피해 구제절차, 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처를 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다."라고 규정하고 있다.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

피심인이 '16.10. ~ '21.7. 기간 동안 주민번호, 계좌번호 등을 안전하지 않은 알고리즘으로 암호화하여 저장한 것은 보호조치 기준 제6조제2항 위반으로 판단된다.

나. 개인정보 유출 통지를 소홀히 한 행위

[보호법 제34조(개인정보 유출 등의 통지)제1항]

피심인은 '24. 5. 7. 개인정보 유출 사고가 발생한 사실을 인지하였음에도 불구하고 정당한 사유 없이 72시간을 경과하여 유출을 통지한 행위는 보호법 제34조제1항 및 시행령 제39조제1항을 위반한 것이다.

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

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반	舊 보호법 §29	舊 시행령 §48의2①	• 주민등록번호, 계좌번호 등을 안전한 암호알고리즘으로 암호화하여 저장하지 않은 행위
개인정보 유출등의 통지	보호법 §34①	§39①	• 정당한 사유 없이 유출 사실을 안 때부터 72시간을 경과하여 유출 통지한 행위

Ⅳ. 처분 및 결정

1. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

가. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제6호, 舊 시행령 제63조 [별표2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[5](이하 舊 '과태료 부과기준')에 따라 다음과 같이 부과한다.

※ 서버 이전 및 시스템 변경으로 해당 시점의 서버 로그기록, 시스템 운영 환경 등을 파악할 수 없어 유출 경위 확인이 어려운 점, 확인된 유출내용도 165건의 이메일주소인 점 등을 고려하여 과징금 부과 면제

1) 기준금액

舊 시행령 제63조 [별표2]는 최근 3년간 같은 위반 행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 舊 보호법 제29조(안전조치의무) 위반 행위에 대해 1회 위반에 해당하는 과태료인 600만 원을 기준금액으로 적용한다.

< 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 **제29조**를 **위반하여 안전성 확보에 필요한 조치를 하지 않은 경우**	舊보호법 제75조 제2항제6호	600	1,200	2,400

5) 개인정보 보호법 위반에 대한 과태료 부과기준(개인정보보호위원회 지침, 2021. 1. 27. 시행)

2) 과태료의 가중 및 감경

가) 과태료의 가중

舊 과태료 부과기준 제8조는 '당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 가중기준에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.'라고 규정하고 있다.

피심인의 舊 보호법 제29조(안전조치의무) 위반행위는 '법 위반 상태의 기간이 3개월 이상* 경우'에 해당하여 기준금액의 10%를 가중한다.

* '16.10. ~ '21.7.

나) 과태료의 감경

舊 과태료 부과기준 제7조는 '당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다.'라고 규정하고 있고, [별표 1]의 각 기준에 따른 과태료 감경 시 그 사유가 2개 이상에 해당되는 경우에는 기준금액의 50을 초과할 수 없다.'라고 규정하고 있다.

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대해 '소기업인 경우', '시정을 완료한 경우', '조사에 적극 협력한 경우'에 해당하여 기준금액의 50%를 감경한다.

3) 최종 과태료

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

나. 결과 공표

舊 보호법 제66조제1항 및 '舊 개인정보보호위원회 처분결과 공표기준[6](이하 '

6) 개인정보보호위원회 지침, 2020. 11. 18. 시행

舊 공표기준') 제2조(공표요건)에 따르면 피심인의 위반행위는 '위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)'에 해당하므로 피심인이 과태료를 부과받은 사실을 개인정보보호위원회 홈페이지에 1년간 공표한다.

* 질서위반행위규제법에 근거하여 피심인에게 유리하게 변경된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침(2023.10.11. 시행)」에 따라 공표기간 1년을 소급 적용

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	㈜모우다	舊 보호법* 제29조	안전조치의무	2025. 4. 23.	과태료 360만 원

* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호

2025년 4월 23일

개 인 정 보 보 호 위 원 회

2. 개인정보 유출 통지를 소홀히 한 행위

가. 과태료 부과

피심인의 보호법 제34조(개인정보 유출 등의 통지)제1항 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제17호, 시행령 제63조 [별표2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[7](이하 '과태료 부과기준')에 따라 다음과 같이 부과한다.

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

1) 기준금액

시행령 제63조 [별표2]는 최근 3년간 같은 위반 행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 보호법 제34조(개인정보 유출 등의 통지)제1항 위반 행위에 대해 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
노. 법 **제34조제1항**(법 제26조제8항에 따라 준용되는 경우를 포함한다)을 **위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우**	보호법 제75조 제2항제17호	600	1,200	2,400

2) 과태료의 가중 및 감경

가) 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 제34조(개인정보 유출 등의 통지)제1항 위반행위는 과태료 부과기준 제7조에 해당하지 않아 가중없이 기준금액을 유지한다.

나) 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 이상 해당되는 경우에는 합산하여 감경하되, 제2호 1) 및 2)에 해당하는 사유가 각 2개 이상 해당되는

경우에는 기준금액의 100분의 50을 초과할 수 없고, 최종 합산 결과 기준금액의 100분의 90을 초과할 수 없다.“라고 규정하고 있다.

피심인의 보호법 제34조(개인정보 유출 등의 통지)제1항 위반행위에 대해 ‘소기업인 경우’, ‘과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우’, ‘조사에 적극 협력한 경우’에 해당하여 기준금액의 70%를 감경한다.

3) 최종 과태료

피심인의 보호법 제34조(개인정보 유출 등의 통지)제1항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 180만 원의 과태료를 부과한다.

다. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무) 및 보호법 제34조(개인정보 유출 등의 통지)제1항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 540만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무	600만 원	60만 원	300만 원	**360만 원**
개인정보 유출 통지 지연	600만 원	-	420만 원	**180만 원**
계				**540만 원**

Ⅴ. 결론

피심인의 舊 보호법 제29조(안전조치의무) 및 보호법 제34조(개인정보 유출 등의 통지)제1항 위반행위에 대하여 舊 보호법 제75조(과태료)제2항제6호 및 보호법 제75조(과태료)제2항제17호, 舊 보호법 제66조(결과의 공표)제1항에 따라 과태료 부과, 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 공표에 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.

2025년 4월 23일

위 원 장 김 진 환 (서 명)

위 원 김 일 환 (서 명)

위 원 김 휘 강 (서 명)