개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2025-013-042호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인 머크㈜

의결연월일 2025. 6. 11.

주 문

1. 피심인에 대하여 다음과 같이 과징금, 과태료를 부과한다.

   가. 과 징 금 : 80,000,000원

   나. 과 태 료 : 6,000,000원

   다. 납부기한 : 고지서에 명시된 납부기한 이내

   라. 납부장소 : 한국은행 국고수납 대리점

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

이 유

Ⅰ. 기초 사실

피심인은 제조·판매하는 의약품에 대한 투약내역 기록 등 편의 서비스를 제공하는 「舊 개인정보 보호법」[1](이하 '舊 보호법'이라 한다)에 따른 정보통신서비스제공자에 해당하며, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인이 제조·판매하는 의약품 투약 기록 편의 제공 관련 신규 서비스인 ' '를 출시하면서 시스템 오류로 이용자의 개인정보 유출 인지 후 유출 신고('23. 3. 30.)해옴에 따라 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('24. 1. 9. ~ '25. 2. 19.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 '23. 3. 29. 기준, 아래와 같이 개인정보를 수집하여 보관하고 있다.

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

<개인정보 수집·보유 현황 >

구분	항목	기간	건수(명)

나. 개인정보 유출 관련 사실관계

피심인은 환자들이 병원에서 치료제를 처방받으면서 안내받은 프로그램에 희망자에 한해 개별적으로 등록 요청(전화) 하는 경우, 이메일을 통해 치료제 투약기록 등 건강에 관한 민감정보를 포함하여 개인정보 수집·이용 동의에 대한 동의(민감정보 별도 동의 포함)를 받은 후, 해당 환자 또는 보호자에게 카카오톡 채널 가입 안내메세지를 발송하고 있다.

피심인은 '23. 3. 29. ‘ ’ 카카오톡 채널 내에 이용자들이 투약내역을 기록 할 수 있도록 투약 기록 편의 제공 관련 신규 서비스인 ‘ ’를 출시하면서, 수신 동의한 이용자들에게 ‘ 바로가기’ 기능이 포함된 알림톡을 발송하였다.

피심인이 이용자들에게 발송한 ‘ 바로가기’(/?userkey=)에 접속시 이용자별로 고유값이 부여되게 하지 않고, ‘{유저키}’라는 고정된 파라미터값이 부여되었다.

이로 인해 ‘바로가기’ 기능을 통해 ‘ ’에 접속하는 이용자가 모두 동일인으로 처리되어, 먼저 ‘ ’에 접속하여 정보를 입력한 이용자의 개인정보를 이후 접속한 이용자들이 열람할 수 있었고, 이후 다른 이용자가 추가로 입력하는 경우 덮어쓰기되어 추가 입력한 이용자의 개인정보가 노출되었다.

1) (유출 내용) DB레코드에 투약기록이 54번 업데이트 되어 있어 각각 다른 이용자가 자신의 정보를 입력했을 경우 최대 108명의 개인정보(민감정보 포함)가 유출되었을 가능성이 있으며, 타인의 개인정보(민감정보 포함)를 열람하였다고 주장하는 민원이 4건(이용자 정보 기준 8명) 접수되었다.

1건의 투약기록당 2명(환자, 보호자)의 개인정보가 포함되어 있으며, 유출된 개인정보에는 이름(환자, 보호자) 및 환자의 키, 몸무게, 처방정보(하루 처방 용량, 투약 횟수, 처방일자, 투약시작일자, 요일별 투약량 등)가 포함되어 있다.

2) 유출 인지 및 대응

일 시		유출 인지 및 대응 내용
'23. 03. 29.	14:37	• URL이 잘못 설정된 ' 바로가기' 버튼 추가
'23. 03. 29.	15시경	• ' 바로가기' 버튼이 포함된 알림 메시지를 이용자에게 발송
'23. 03. 29.	17:20	• 피심인은 ' 바로가기'에 접속한 이용자가 타인의 개인정보가 보인다는 민원 최초 접수
'23. 03. 29.	18시경	• 유출 사실 인지 후 ' 접속 차단 조치
'23. 03. 30.	17:10	• 개인정보 포털에 개인정보 유출 신고
'23. 03. 30.	17:56	• 이용자 90명* 대상 개인정보 유출 통지(문자) * '바로가기' 기능이 아닌 정상적으로 접속 후 투약기록을 입력한 인원
'23. 04. 07.	-	• 유출 원인 분석을 통해 " " 바로가기 버튼을 통해 접속한 이용자들의 정보가 DB에 덮어쓰기 되어 다음 이용자에게 노출된 사실 확인 및 유출 대상자를 특정하기 위한 분석(지속)
'23. 04. 18.	17:51	• 민원('23.3.29. 접수)을 통해 개인정보 유출이 확인된 이용자 8명(환자, 보호자 각 4명) 대상 개인정보 유출 통지(문자)

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 ‘ ’ 신규 서비스 개발 과정에서 ‘ 바로가기’ 기능에 대한 파라미터값 설정 오류 등 취약점 점검을 소홀히 하고 이에 대한 사전 테스트 등 검증 없이 적용한 사실이 있다.

나. 개인정보 유출 통지를 소홀히 한 행위

피심인은 ‘23. 3. 29. 민원을 통해 이용자의 개인정보 유출을 인지하였으나, 정당한 사유 없이 24시간을 경과한 ‘24. 4. 18. 이용자 대상 유출 통지한 사실이 있다.

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 ‘25. 3. 5. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 4. 3. 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 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.

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.

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 제48조의4제4항은 "정보통신서비스 제공자등은 법 제39조의4제1항 각 호 외의 부분 단서에 따른 정당한 사유가 있는 경우에는 법 제39조의4제1항 각 호의 사항을 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제2항의 통지를 갈음할 수 있다."라고 규정하고 있다.

---

2) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2022. 10. 20. 시행
3) 개인정보보호위원회고시 제2021-3호, 2021. 9. 15. 시행

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

피심인은 의약품 투약기록 등 건강에 관한 민감정보를 수집·이용하면서 보다 높은 수준의 보호 조치가 기대됨에도 불구하고, ‘ ’ 신규 서비스 개발 과정에서 ‘ 바로가기 기능’의 파라미터값 오류에 대한 취약점 점검을 소홀히 하고 이에 대한 사전 테스트 등 검증 없이 적용하여 이용자의 개인정보가 열람 권한이 없는 자에게 유출된 행위는 舊 보호법 제29조, 舊 시행령 제48조의2 제1항, 舊 기술적 보호조치 기준 제4조제9항을 위반한 것이다.

※ ’23. 3. 29. 15:00 서비스 오픈 직전인 ’23. 3. 29. 14:37 ‘ 바로가기 기능’을 추가

나. 개인정보 유출 통지를 소홀히 한 행위

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

피심인이 ’23. 3. 29. 17:54 민원이 접수되어 개인정보 유출을 인지하였으나, 민원을 통해 유출을 확인한 이용자에게 정당한 사유 없이 24시간을 경과하여 ’23. 4. 18. 유출 통지한 행위는 舊 보호법 제39조의4제1항 및 舊 시행령 제48조의4제4항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무	舊 보호법 §29	舊 시행령 §48의2①	·처리중인 개인정보가 인터넷 홈페이지 등을 통해 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 조치를 취하지 않은 행위 (舊 기술적 보호조치 기준 §4⑨)
개인정보 유출등의 통지·신고에 대한 특례	舊 보호법 §39의4①	舊 시행령 §48조의4 ④	·정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 유출 통지한 행위

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 舊 보호법 제29조 위반에 대한 과징금은 같은 법 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 규정하고 있다.

이에 따를 때, 舊 보호법 제29조의 안전조치의무를 소홀히 한 피심인에게 이용자

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

개인정보 유출에 대한 중과실이 있다고 판단한다.

2) 중대성의 판단

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.

피심인의 경우, '　　' 신규 서비스 개발 과정에서 '　　바로가기 기능'에 대한 취약점 점검을 소홀히 하고 이에 대한 사전 테스트 등 검증 없이 적용하여 이용자의 개인정보가 열람 권한이 없는 자에게 유출된 경우로 '위반행위로 인해 직접적으로 이득을 취하지 않은 경우(제1호)', '피해규모가 100분의 5 이내인 경우(제2호)', '이용자의 개인정보가 공중에 노출되지 않은 경우(제3호)'에 해당(총 3개 '호'에 해당)하여 '보통 위반행위'로 판단한다.

※ 사고 당시 가입자 수는　　명으로, 유출 피해 규모(최대 108명)는 보유한 개인정보의 5% 이내에 해당

3) 기준금액 산출

피심인이 처리하는 이용자의 개인정보가 유출된 '　　' 서비스는 영업실적이 없거나 객관적인 매출액 산정이 곤란한 경우로 舊 시행령 [별표 1의5] 2. 가. 2)에 따른 '보통 위반행위'의 부과 기준금액을 적용하여 기준 금액을　　천 원으로 한다.

<舊 시행령 [별표 1의5] 2. 가. 2)에 따른 부과기준율>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	3억 6천만 원
중대한 위반행위	2억 8천만 원
보통 위반행위	**2억 원**

다. 필수적 가중 및 감경

舊 과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 1년 이내('23. 3. 29. 14:37(바로가기 기능 추가) ~ '23. 3. 29. 18시(서비스 차단)) 이므로 '단기 위반행위'에 해당하여 기준금액을 유지하고,

최근 3년 이내 舊 보호법 제39조의15제1항 각 호에 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 자진 신고한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 20에 해당하는 천 원을 감경한다.

마. 과징금의 결정

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 80,000천원을 최종 과징금으로 결정한다.

<과징금 산출 내역>

①기준금액	②필수적 가중·감경	③추가적 가중·감경	④최종과징금
•직전 3개 사업연도 연평균 매출액(없음) •기준금액 적용 (보통위반*)	•최초위반으로 50% 감경 (천 원)	•조사협력, 자진신고로 20% 감경 (천 원)	**80,000천 원**
⇒ 천 원	⇒ 천 원	⇒ 천 원	

* 보통위반 : ▲위반행위로 직접 이득을 취하지 않은 경우(해당), ▲개인정보가 공중에 노출되지 않은 경우(해당), ▲유출피해 규모가 보유하고 있는 개인정보의 5% 이내인 경우(해당)

2. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무) 및 보호법 제39조의4(개인정보의 유출 등의 통지·신고에 대한 특례)제1항 위반행위에 대한 과태료는 같은 법 제75조제2항 제6호·12호의3, 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.

5) 개인정보보호위원회지침, 2023. 3. 8. 시행

< 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 위반**하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
도. 법 **제39조의4제1항**(제39조의14에 따라 준용되는 경우를 포함한다)을 **위반**하여 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 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 중

지하는 등 시정을 완료한 경우', '조사에 적극 협력한 경우'에 해당하여 기준금액의 50%를 각각 감경한다.

다. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 600만 원의 과태료를 부과한다.

< 과태료 산출내역 >

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

3. 결과 공표

舊 보호법 제66조제1항 및 舊 개인정보 보호위원회 처분결과 공표기준[6](이하 '舊 공표 기준') 제2조(공표요건)에 따르면 피심인의 위반행위는 '법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우(제4호)'에 해당하므로 舊 보호법 제66조제1항에 따라 피심인이 과태료 부과를 받은 사실에 대해 개인정보보호위원회 홈페이지에 1년간 공표한다.

6) 개인정보보호위원회지침, 2020. 11. 18. 시행

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	머크(주)	舊 보호법* 제29조	안전조치의무 위반	2025. 6. 11.	과태료 부과 300만원
		舊 보호법* 제39조의4	개인정보 유출등의 통지·신고 특례 위반		과태료 부과 300만원

* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호

2025년 6월 11일

개 인 정 보 보 호 위 원 회

이의제기 방법 및 기간

피심인은 이 과징금 부과처분, 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 6월 11일

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 김 휘 강 (서 명)

위 원 박 상 희 (서 명)

위 원 윤 영 미 (서 명)

위 원 이 문 한 (서 명)