

# 개 인 정 보 보 호 위 원 회

## 심의 · 의결

안 건 번 호 제2024-017-239호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (주)네오팜 (사업자등록번호 : )

대표자

의결연월일 2024. 10. 23.

## 주 문

1. 피심인에 대하여 다음과 같이 과징금, 과태료를 부과한다.

가. 과 징 금 : 105,173,000원

나. 과 태 료 : 7,200,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인 (주)네오팜에 대한 과태료 부과 내용 및 결과를 개인정보보호위원회 홈페이지에 1년간 공표한다.

# 이 유

## I. 기초 사실

피심인은 화장품 등 제품 판매 온라인 쇼핑몰(네오팜샵, neopharmshop.co.kr)을 운영하는 「舊 개인정보 보호법<sup>1)</sup>」(이하 '舊 보호법')에 따른 정보통신서비스 제공자에 해당하며, 피심인의 일반현황은 다음과 같다.

### < 피심인의 일반현황 >

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

## II. 사실조사 결과

### 1. 조사 배경

피심인이 신원 미상의 자(이하 '해커')의 해킹 공격으로 개인정보가 유출된 정황을 인지하고 유출 신고('23. 8. 18.)해움에 따라 개인정보보호위원회는 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('24. 1. 12. ~ '24. 2. 27.) 하였으며, 다음과 같은 사실을 확인하였다.

### 2. 행위 사실

#### 가. 개인정보 수집현황

피심인은 화장품 등 제품 판매 쇼핑몰(네오팜샵, neopharmshop.co.kr)을 운영하면서 '24. 1. 24.(자료제출일) 기준,           건의 개인정보를 수집·보관하고 있다.

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

**< 개인정보 수집현황 >**

구분	항목	기간	건수
회 원			
계			

**나. 개인정보 유출 관련 사실관계**

해커는 '23. 8. 5. 17:13 사전에 획득한 계정 정보로 피심인의 관리자 페이지( )에 접근하여 로그인에 성공하였다.

※ 해커가 웹 관리자 페이지에 1회 접속시도로 로그인 성공한 것을 고려했을 때, 사전에 관리자 계정정보를 획득한 것으로 추정됨

이후, '23. 8. 5. ~ 8. 17. 동안 29개(중복 제거)의 IP 주소에서 피심인의 웹 관리자용 회원정보 조회 페이지( )에 759회 접근하여 293,723명(유효 226,620명, 휴면 67,463명)의 개인정보를 조회하였다.

※ 해커는 회원정보 조회 페이지( )에 1회 500명씩 회원정보를 출력하도록 설정( )하여 총 759회 회원정보를 조회함

또, 동 기간('23.8.5.~8.17.) 동안 25개(중복 제거)의 IP 주소에서 회원정보 조회 페이지의 '엑셀 내보내기 기능\*( )'을 이용해 226,260명의 개인정보 파일을 다운로드하여 유출하였다.

\* '엑셀 내보내기 기능'은 유효회원(226,260건)에 대해서만 다운로드될 수 있도록 설정

한편, 해커는 '23. 8. 14. 웹 관리자 페이지 내 문자 발송 기능을 이용해 스팸문자 테스트 발송 이후 '23. 8. 17.까지 4회에 걸쳐 피심인 이용자 대상 약 442,821건의 스팸문자를 발송하였다.

※ 해커는 관리자 페이지에서 문자발송 기능 이용 시 회원 리스트를 선택하여 스팸문자를 발송한 것으로 확인

1) (유출 규모 및 항목) 이용자 293,723명\*의 개인정보\*\*

\* (개인정보 조회) 293,723명(유효회원(226,260명) 및 휴면회원(67,463명))  
(엑셀파일 다운로드) 226,260명(유효회원)

\*\* 아이디, 성명, 성별, 생년월일, 휴대전화번호, 주소, 이메일

2) 유출 인지 및 대응

일 시	유출인지 및 대응 내용
'23. 8. 14. ~ 8. 17.	해커는 네오팜 회원 대상 스팸 문자(총 442,821건) 발송
'23. 8. 17. 22:00	비정상 스팸문자 발송 사실 확인
'23. 8. 17. 22:05	관리자 페이지의 관리자 계정 비밀번호 변경
'23. 8. 17. 23:00 ~	관리자 페이지 웹서버 로그 확인 ※ 사내 IP 및 일부 외부 IP에서 관리자 페이지 로그인한 이력 확인
'23. 8. 18. 00:00	관리자 페이지의 IP 주소 접근 제한 ※ 사내 IP, VPN 이용자 이외에 접근이 불가능하도록 설정
'23. 8. 18. 10시경	웹로그 분석을 통해 외부 IP 주소에서 회원정보를 다운로드한 사실 확인 및 개인정보 <u>유출 인지</u>
'23. 8. 18. ~ 9. 23.	홈페이지 내 개인정보 유출 사실 안내 팝업 게시
'23. 8. 18. 11:04	개인정보 포털에 개인정보 <u>유출 신고</u>
'23. 8. 23. 12:00	관리자 페이지에 2차 인증(SMS) 기능 적용 및 사용자별 계정 분리 생성, 계정 부여·변경·말소 내역 보관·관리
'23. 8. 29. 17:00	유출 이용자 대상 개인정보 <u>유출 통지</u> (이메일)
'23. 9. 5.	관리자 페이지의 개인정보취급자의 접속기록 보관·관리 시행

3. 개인정보의 취급·운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 웹 관리자 페이지의 개인정보 열람·수정·다운로드 등의 모든 권한을 사용할 수 있는 계정을 부서별(온라인전략팀, CS팀, 마케팅팀)로 1개 계정( )만 생성·공유하였고, 권한 부여·변경·말소에 대한 내역을 기록·보관하지 않은 사실이 있다.

피심인은 외부에서 정보통신망을 통해 웹 관리자 페이지에 접속 시 안전한 인증 수단을 적용하지 않고, 아이디·비밀번호만으로 접속이 가능하도록 운영한 사실이 있다.

피심인은 웹 관리자 페이지에 대한 접속 권한을 IP 주소 등으로 제한하거나 접속한 IP 주소 등을 재분석하여 대량의 개인정보 유출 시도를 탐지·차단하는 등 침입 차단·탐지 시스템 운영을 소홀히 한 사실이 있다.

피심인은 개인정보취급자가 관리자 페이지에 접속한 기록을 보존·관리하지 않은 사실이 있다.

#### **나. 개인정보 유출 통지를 소홀히 한 행위**

피심인은 '23. 8. 18. 10시경 웹로그 분석을 통해 외부 IP 주소에서 회원정보 엑셀 파일을 다운로드한 사실을 확인하여 개인정보 유출 사실을 인지했음에도, 정당한 사유 없이 24시간을 경과한 '23. 8. 29. 17:00 이용자 대상 개인정보 유출 통지를 한 사실이 있다.

#### **4. 처분의 사전통지 및 의견수렴**

개인정보보호위원회는 '24. 2. 28. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 4. 1. 개인정보 보호위원회에 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<sup>2)</sup>(이하 ‘舊 시행령’) 제48조의2제1항제2호는 “개인정보에 대한 불법적인 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 기준<sup>3)</sup>(이하 ‘舊 기술적 보호조치 기준’) 제4조제1항은 “정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보 보호책임자 또는 개인정보취급자에게만 부여한다.”라고 규정하고 있고, 제4조제2항은 “정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.”라고 규정하고 있으며, 제4조제3항은 “정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.”라고 규정하고 있다.

舊 기술적 보호조치 기준 제4조제4항은 “정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.”라고 규정하고 있고, 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인

---

2) 舊 개인정보 보호법 시행령(대통령령 제32813호, 2022. 7. 19. 일부개정, 2022. 10. 20. 시행)

3) 舊 개인정보의 기술적·관리적 보호조치 기준(개인정보보호위원회고시 제2021-3호, 2021. 9. 15. 시행)

가받지 않은 접근을 제한(1호)', '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(2호)' 기능을 포함한 시스템을 설치·운영하여야 한다.”라고 규정하고 있다.

舊 기술적 보호조치 기준 제5조제1항은 “정보통신서비스 제공자등은 개인정보 취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 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(1호), 유출등이 발생한 시점(2호), 이용자가 취할 수 있는 조치(3호), 정보통신서비스 제공자등의 대응 조치(4호), 이용자가 상담 등을 접수할 수 있는 부서 및 연락처(5호)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 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 항제3호부터 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)]

피심인은 웹 관리자 페이지의 개인정보 열람·수정·다운로드 등의 모든 권한을 사용할 수 있는 계정을 부서별 1개 계정만 생성·공유하고 있어, 웹 관리자 페이지 접속을 위해 필요한 개인정보취급자별로 접근 권한을 부여하거나 최소 인원에게 필요한 범위 내에서 권한을 차등화하지 않았으며, 취급자의 인사이동에 따른 접근 권한 변경 또는 말소하거나, 접근 권한 부여·변경·말소에 대한 내역을 기록하고 보관하지 않은 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제1항·제2항·제3항을 위반한 것이다.

피심인은 외부에서 정보통신망을 통해 웹 관리자 페이지 접속 시 안전한 인증 수단을 적용하지 않고 아이디·비밀번호만으로 접속할 수 있게 운영한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제4항을 위반한 것이다.

피심인은 웹 관리자 페이지에 대한 접속 권한을 IP 주소 등으로 제한하여 인가 받지 않은 접속을 차단하는 등 침입 차단·탐지 시스템 운영을 소홀히 한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제5항을 위반한 것이다.

피심인은 개인정보취급자가 처리시스템인 웹 관리자 페이지에 접속한 접속기록을 보존·관리하지 않은 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제5조제1항을 위반한 것이다.

## 나. 개인정보 유출 통지를 소홀히 한 행위

피심인은 '23. 8. 18. 10시경 웹로그 분석을 통해 외부 IP 주소에서 회원정보



엑셀 파일을 다운로드한 사실을 확인하여 개인정보 유출 사실을 인지했음에도, 정당한 사유 없이 24시간을 경과하여 '23. 8. 29. 17:00 이용자 대상 개인정보 유출 통지를 한 행위는 舊 보호법 제39조의4제1항을 위반한 것이다.

#### < 피심인의 위반사항 >

위반행위	법률	舊 시행령	세부내용(고시 등)
안전조치의무	舊 보호법 §29	§48의2① 제2호·제3호	<ul style="list-style-type: none"> <li>개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보 보호책임자 또는 개인정보취급자에게만 부여하지 않은 행위 (舊 기술적 보호조치 기준§4①)</li> <li>개인정보취급자 변경 시 개인정보처리시스템의 접근 권한을 변경 또는 말소하지 않은 행위 (舊 기술적 보호조치 기준§4②)</li> <li>권한 부여, 변경 또는 말소에 대한 내역을 기록·보관하지 않은 행위(舊 기술적 보호조치 기준§4③)</li> <li>정보통신망을 통해 외부에서 개인정보처리시스템 접속 시 안전한 인증수단 미적용 (舊 기술적 보호조치 기준 §4④)</li> <li>불법적인 접근 및 침해사고 방지를 위한 개인정보 처리 시스템에 대한 침입 탐지·차단 시스템 운영 소홀 (舊 기술적 보호조치 기준§4⑤)</li> <li>개인정보취급자가 개인정보처리시스템의 접속기록을 보존·관리하지 않은 행위(舊 기술적 보호조치 기준§5①)</li> </ul>
개인정보 유출등의 통지·신고에 대한 특례	舊 보호법 §39의4①	§48조의4	<ul style="list-style-type: none"> <li>정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 유출 통지한 행위</li> </ul>

## IV. 처분 및 결정

### 1. 과징금 부과

피심인의 舊 보호법 제29조(안전조치의무) 위반에 대한 과징금은 같은 법 제39조의15제1항제5호, 舊 시행령 제48조의11제1항과 제4항, [별표 1의5] '과징금의 산정기준과 산정절차' 및 舊 개인정보보호 법규 위반에 대한 과징금 부과기준<sup>4)</sup> (이하 '舊 과징금 부과기준')에 따라 다음과 같이 부과한다.

4) 舊 개인정보보호 법규 위반에 대한 과징금 부과기준(개인정보보호위원회 고시 제2022-3호, 2022. 10. 20. 시행)

## 가. 과징금 상한액

피심인의 舊 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제39조의15, 舊 시행령 제48조의11에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업 연도 연평균 매출액의 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 따라, 舊 보호법 제29조(안전조치의무), 舊 시행령 제48조의2(개인정보의 안전성 확보 조치에 관한 특례)를 소홀히 한 피심인에게 이용자 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 경

우 ‘보통 위반행위’로, 1개 이상 2개 이하에 해당하는 경우 ‘중대한 위반행위’로 감경하도록 규정하고 있다.

피심인의 경우, 해킹으로 인해 보유 중인 개인정보 대부분이 유출되었으므로 ‘피해규모가 100분의 5 이내인 경우(제2호)’에 해당하지 않으나, ‘공중에 노출되지 않은 경우(제3호)’ 및 안전조치의무 위반으로 인해 ‘직접적으로 이득을 취하지 않은 경우(제1호)’에 해당(총 2개 호에 해당)하여 ‘중대한 위반행위’로 판단한다.

### 3) 기준금액 산출

舊 과징금 부과기준 제4조제1항은 “관련 매출액은 위반 정보통신서비스 제공자 등의 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 서비스의 직전 3개 사업년도의 연평균 매출액으로 한다.”라고 규정하고 있다.

피심인이 화장품 등 제품 판매 쇼핑몰(neopharmshop.co.kr) 서비스인 ‘네오팜샵’ 자사몰에서 발생한 매출을 위반행위 관련 매출로 하고, 직전 3개 사업년도의 연평균 매출액                    천 원에 舊 시행령 [별표 1의5] 2. 가. 1)에 따른 ‘중대한 위반행위’의 부과기준을 1천분의 21을 적용하여 기준금액을                    천 원으로 한다.

#### < 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2020년	2021년	2022년	평 균
관련 매출액*				

\* 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

#### <舊 시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준>

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
<b>중대한 위반행위</b>	<b>1천분의 21</b>
보통 위반행위	1천분의 15

#### 다. 필수적 가중 및 감경

舊 과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 2년을 초과하는 경우에 해당하므로 '장기 위반행위'에 해당하여 기준금액의 100분의 50에 해당하는          천 원을 가중하고, 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          천 원을 최종 과징금으로 결정한다.

### <과징금 산출 내역>

①기준금액	②필수적 가중·감경	③추가적 가중·감경	④최종 과징금
<ul style="list-style-type: none"> <li>•직전 3개 사업연도 연평균 매출액 (            천 원)</li> <li>•연평균 매출액에 2.1% 적용 (중대한 위반*)</li> </ul>	<ul style="list-style-type: none"> <li>•장기위반으로 50% 가중 (            천 원)</li> <li>•최초위반으로 50% 감경 (            천 원)</li> </ul>	<ul style="list-style-type: none"> <li>•조사협력, 자진신고로 20% 감경 (            천 원)</li> </ul>	

\* 중대한 위반 : 고의·중과실이 있는 경우, 매우 중대한 위반행위로 판단하나, ▲위반행위로 직접 취한 이득이 없는 경우, ▲이용자의 개인정보가 공중에 노출되지 않은 경우에 해당하여 중대한 위반행위로 판단함

## 2. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무), 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<sup>5)</sup>(이하 ‘舊 과태료 부과기준’)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) 舊 개인정보 보호법 위반에 대한 과태료 부과기준(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 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 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 따라 舊 보호법 제29조(안전조치의무) 위반행위는 ‘제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상에 해당하는 경우’, ‘법 위반상태의 기간이 3개월 이상인 경우’에 해당하여 기준금액의 20%를 가중하고, 같은 법 제39조의4(개인 정보 유출등의 통지·신고에 대한 특례)제1항 위반행위는 가중사유가 없으므로 기준금액을 유지한다.

**2) (과태료의 감경)** 舊 과태료 부과기준 제7조는 ‘사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의

감정기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감정할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감정할 수 있다.’라고 규정하고 있다.

피심인의 경우, 舊 과태료 부과기준 제7조 및 [별표1] 과태료의 감정기준에 따라 舊 보호법 제29조(안전조치의무) 위반행위는 ‘과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우’, ‘조사에 적극 협력한 경우’에 해당하여 기준금액의 50%를 감정하고, 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항 위반행위는 ‘과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우’, ‘조사에 적극 협력한 경우’에 해당하여 기준금액의 50%를 감정한다.

#### 다. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대해 기준금액에서 가중·감정을 거쳐 총 720만 원의 과태료를 부과한다.

#### < 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감정액	최종 과태료
안전조치의무 (접근통제, 접속기록)	600만원	120만원	300만원	420만원
개인정보 유출등의 통지·신고에 대한 특례	600만원	-	300만원	300만원
계				720만원

### 3. 결과 공표

舊 보호법 제66조제1항 및 「舊 개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 ‘법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우(제4호)’, ‘위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)’, ‘개인정보 유출 및 침해사고로 인한 피해자 수가 10만 명 이상인 경우(제7호)’에 해당하므로 舊 보호법 제66조제1항에 따라 피심인이 시정조치 명령과 과태료 부과를 받은 사실을 개인정보보호위원회 홈페이지에 공표한다. 다만, 개정된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」(2023. 10. 11. 시행)에 따라 공표 기간은 1년으로 한다.

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

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	위 반내용	처분일자	처분내용
1	(주)네오팜	舊 보호법* 제29조	안전 조치의무	2024. 10. 23.	과태료 부과 420만원
		舊 보호법 제39조의4 제1항	개인정보 유출등의 통지·신고에 대한 특례	2024. 10. 23.	과태료 부과 300만원
* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호					
2024년 10월 23일 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 제39조의15(과징금 부과 등에 대한 특례)제1항제5호, 제75조(과태료)제2항제6호·제12호의3, 제66조(결과의 공표)제1항에 따라 과징금 부과, 과태료 부과 및 결과 공표를 주문과 같이 의결한다.



## 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.

2024년 10월 23일

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      박 상 희    (서 명)

위      원      윤 영 미    (서 명)

위      원      이 문 한    (서 명)

위      원      조 소 영    (서 명)