개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 **제2024-220-639호**

안 건 명 **개인정보보호 법규 위반행위에 대한 시정조치에 관한 건**

피 심 인 주식회사 한독 (사업자등록번호 :)

대표자

의결연월일 **2024. 10. 23.**

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. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 의약품 제조 및 판매업을 하는 「舊 개인정보 보호법」[1](이하 '舊 보호법')에 따른 개인정보처리자에 해당한다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	종업원 수 (명)
주식회사 한독				

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 포털(privacy.go.kr)에 유출 신고('23.6.2.)한 피심인에 대하여 개인정보보호 법규 위반 여부를 조사('23.6.16.~'24.3.15.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 임직원 및 고객의 개인정보를 건 수집하여 보관하고 있다.

구 분	항 목	기 간	건 수(건)
계			

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

나. 개인정보 유출 관련 사실관계

피심인은 '19년 5월경 내·외부 메일 서버를 연동하기 위하여 외부의 접근을 허용하도록 방화벽 정책을 수정*하고, '23년 4월경 보안장비 교체를 위하여 IPS를 탐지모드로 설정하였으며, 외부에서 접근 가능한 메일 서버는 최신 보안 업데이트**가 적용되지 않아 외부의 비정상적인 행위를 차단하지 못하였음

* (외부->내부) 특정 IP, 포트로 접근을 제한하지 않고 모두 허용,
비정상적인 외부 접근(IP스캔, 포트 스캔행위 등)은 IPS로 차단

** 취약점(CVE-2020-1472) 보안패치는 '20.8.11. 가이드되었으나, '23.6.1.업데이트 함

1) (**유출 규모 및 항목**) 임직원 및 고객의 개인정보* 10,492건

* 성명, 전화번호, 이메일, 주소, 직책, 소속기관 등

2) 유출인지 및 대응

일 시	유출 인지·대응 내용
'19. 5월 경	내·외부 **메일서버**를 하이브리드로 **연동**하면서 **특정 IP 및 포트**로 **접근**을 **제한**하지 않고 **모두 허용***함 * 외부에서 내부로의 비정상적인 접근(IP스캔, 포트스캔 등)은 IPS(침입방지시스템)로 차단함
'23. 4. 22	IPS 장비를 **교체***하는 과정에서 **탐지모드**(**모니터링**)로 설정 * (기존 장비) -> (신규 장비) : 방화벽+IPS
'23. 4. 27. ~ '23. 5. 12	**메일서버**에 **취약점 공격** 발생* **AD관리자 계정****으로 **무단 원격접속**(**RDP**) 발생 * **외부**에서 **접근**이 가능하였던 메일 서버는 **최신 보안 업데이트**가 적용되지 않음 (취약점(CVE-2020-1472) 보안패치는 '20.8.11. 가이드 되었으나, '23.6.1.업데이트 함) ** 이전 **로그**가 **삭제**되어 **AD관리자 계정**이 **유출된 경위** 등은 확인할 수 없으나, IP·포트스캔 등을 통해 메일서버 및 RDP포트를 인지한 것으로 추정됨
'23. 5. 10.	시스템 **이상 징후** 인지, **외부 통신 차단** 등 **보안 조치** 진행
'23. 5. 11.	신원미상자로부터 **해킹** 관련 협박성 **메일 수신**
'23. 5. 16.	신원미상자로부터 **실제 데이터** 보유 확인을 위한 **파일 수신**
'23. 5. 19.	정보주체(**임직원 44명**)에게 **유출 통지**(**메일**)
'23. 6. 2.	**다크웹** 모니터링 중 "**Handok Inc.**"페이지 확인 및 일부 **다운로드**
	개인정보 **유출 신고**, 서울경찰청 및 한국인터넷진흥원에 자료 전달
'23. 6. 9.	유출사고 **홈페이지 게시** 및 대응 콜센터 개시, **유출 통지**(**메일, SMS**)

3) 사후조치

피심인은 IP제한 조치 및 메일 서버에 대한 보안 프로그램을 최신화 하였으며, 추가적인 보안 강화 프로젝트*를 실시하였다.

* 앤드포인트 탐지 및 대응, 보안강화, PC EDR

3. 개인정보의 취급·운영 관련 사실관계

가. 안전성 확보에 필요한 조치를 소홀히 한 사실

피심인은 ①메일 서버에 외부 IP 및 포트를 제한하지 아니하여 외부의 접근을 허용하고, ②외부접근이 가능하였던 메일 서버에 최신 보안 업데이트를 적용하지 아니한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

가. 피심인 의견

개인정보보호위원회는 '24. 3. 21. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '24. 4. 5. 의견을 제출하였다.

피심인은 피심인의 임직원과 정보통신서비스 이용관계를 맺고 있지 않은 점은 명백하며, 고객의 경우 피심인의 오프라인 고객으로서 해당 정보는 병·의원 및 행사장 등 오프라인에서 수집된 것이며 공식 홈페이지 및 웹사이트와 무관하여 정보통신서비스 이용관계가 성립하지 않아 과징금 대상이 아니라고 주장한다.

나. 검토의견 : 수용

피심인의 ①임직원은 정보통신서비스 이용 관계가 없으므로 이용자에 해당하지 않으며, 유출된 ②고객(의·약사)의 정보는 마케팅(행사 정보 안내 등)을 위해 SMS·이메일을 발송할 목적으로 현장에서 직접 수집하였고,

고객이 피조사자의 웹페이지에 회원으로 가입하였다거나, 웹페이지에 접속하여

상담을 하거나 구매·예약을 하는 등 서비스를 이용한 사실이 없으므로, 정보통신서비스 이용 관계가 성립하지 않는다는 피심인의 주장을 수용함

※ 유출된 DB는 공식 홈페이지 및 온라인몰 등 피조사자가 운영하는 웹페이지와 연결되지 않음

Ⅲ. 위법성 판단

1. 관련 법 규정

舊 보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 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’) 제30조제1항은 개인정보처리자는 보호법 제29조에 따라 ’개인정보에 대한 접근 통제 및 접근 권한의 제한 조치(제2호)‘, ’개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치(제3호)‘, ’개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치(제4호)‘ 등의 안전성 확보 조치를 하여야 한다고 규정하고 있다.

또한 舊 개인정보의 안전성 확보조치 기준[3](이하 ‘舊 안전조치 기준’) 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야”하고, 제9조제1호는 “개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지하여야 한다”라고 규정하고 있다.

2. 위법성 판단

가. 안전성확보조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

2) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2020. 10. 20. 시행
3) 개인정보보호위원회고시 제2021-2호, 2021. 9. 15. 시행

피심인이 ①메일 서버에 외부 IP 및 포트를 제한하지 아니하여 외부의 접근을 허용하고, ②외부접근이 가능하였던 메일 서버에 최신 보안 업데이트를 적용하지 아니한 행위는 舊보호법 제29조 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 舊 보호법 제29조 위반에 대해 같은 법 제75조제2항제6호, 「舊 개인정보 보호법 시행령」[4](이하 '舊 시행령') 제63조 [별표2] 및 舊 개인정보 보호법 위반에 대한 과태료 부과기준[5](이하 '舊 과태료 부과기준')에 따라 다음과 같이 420만 원의 과태료를 부과한다.

가. 기준금액

舊 시행령 제63조 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 기준금액 600만 원을 적용한다.

< 舊 보호법 시행령 [별표2] 2. 개별기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	舊 법 제75조제2항제6호	600	1,200	2,400

나. 과태료의 가중

舊 과태료 부과기준 제8조제1항은 '당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 2]의 가중기준(▲조사방해, ▲위반의 정도, ▲위반기간)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정하고 있다.

---

4) 대통령령 제30892호, 2020. 8. 4. 일부개정, 2021. 2. 5. 시행
5) 개인정보보호위원회지침, 2023. 3. 8. 시행

피심인의 경우 舊 과태료 부과기준 제8조 및 [별표 2] 과태료의 가중기준에 따라, ‘제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상에 해당하는 경우’, ‘법 위반상태의 기간이 3개월 이상인 경우’에 해당하여 기준금액(600만 원)의 20%(120만 원)를 가중한다.

다. 과태료의 감경

舊 과태료 부과기준 제7조제1항은 ‘당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사 협조, ▲자진시정, ▲개인정보 보호인증·자율규제규약 등 개인정보 보호활동, ▲사업 규모) 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다. 다만, 과태료를 체납하고 있는 경우는 제외한다’라고 규정하고 있고, 제7조제2항은 ‘[별표 1]의 각 기준에 따른 과태료 감경 시 그 사유가 2개 이상 해당되는 경우에는 합산하여 감경하되, 기준금액의 100분의 50을 초과할 수 없다’라고 규정하고 있다.

피심인의 경우 舊 과태료 부과기준 제7조 및 [별표 1] 과태료의 감경기준에 따라, ’조사에 적극 협력한 경우(40%이내)’, ’시정을 완료한 경우(50%이내)‘에 해당하여 최대 감경범위인 기준금액(600만 원)의 50%(300만 원)를 감경한다.

라. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 420만 원의 과태료를 부과한다.

< 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만 원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
舊 보호법 제29조(안전조치의무)	舊 보호법 제75조제2항제6호	600	120	300	**420**

※ 피심인이 과태료 고지서를 송달받은 날부터 14일 이내에 과태료를 자진납부 하는 경우, 100분의 20을 감경함(질서위반행위규제법 제18조 및 같은 법 시행령 제5조 준용)

2. 결과 공표

피심인의 舊 보호법 제29조 위반에 대해 舊 보호법 제66조제1항 및 「舊 개인정보 보호위원회 처분 결과 공표기준」 (2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우에 해당하므로, 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다. 다만, 개정된 「개인정보 보호위원회 처분결과 공표기준」(2023. 10. 11. 개인정보보호위원회 의결)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	주식회사 한독	舊 법 제29조	안전조치의무 위반	2024. 10. 23.	과태료 420만 원

2024년 10월 23일
개 인 정 보 보 호 위 원 회

Ⅵ. 결론

피심인의 舊 보호법 제29조 위반에 대하여 같은 법 제75조(과태료)제2항제6호 및 제66조제1항에 따라 과태료 부과 및 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조제1항에 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」 제20조제2항의 규정에 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 납부 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다.

2024년 10월 23일

위 원 장　　이 문 한

위　　원　　박 상 희

위　　원　　조 소 영