개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 **제2024-220-640호**

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

피 심 인 사회복지법인 월드비전 (사업자등록번호 :)

대표자

의결연월일 **2024. 10. 23.**

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 3,600,000원

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 사회복지사업을 운영하는 비영리단체로, 후원 등의 업무를 목적으로 대표 홈페이지 이용자의 개인정보를 처리하는 「舊 개인정보 보호법」[1](이하 '舊 보호법') 제2조제5호에 따른 개인정보처리자에 해당한다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	종업원 수(명)
사회복지법인 월드비전				

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 포털(privacy.go.kr)에 유출 신고('23.8.23.)한 피심인에 대하여 개인정보보호법규 위반 여부를 조사('23.9.18.~'24.4.25.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 후원 등의 목적으로 대표 홈페이지를 운영하면서 '23. 9. 27.(자료제출일) 기준 명의 개인정보를 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 대표 홈페이지에 평소 로그인 시도의 약 1,000배에 달하는 대량의 로그인 시도*(만 건 이상) 및 실패(99.9%)가 발생하였고, 단일 IP에서 1초에 건의 비정상적인 로그인 시도가 이루어졌음에도 이를 탐지·차단**하지 못하여, 신원미상자의 공격을 통해 홈페이지 회원 1,219명의 개인정보가 유출되었다.

* 개의 IP에서 로그인 시도가 발생하였으며, 1,219명의 회원ID로 로그인이 성공함

** 사고 당시 방화벽과 침입탐지·차단 시스템을 설치·운영하였으나, 임계치 등은 적용되지 않음

1) (유출규모 및 항목) 대표홈페이지 이용자의 개인정보* 1,219건

* 성명, 생년월일, 전화번호, 이메일, 주소 등

2) 유출인지 및 대응

일시		피심인의 유출 인지·대응 내용	비고
2023	7.25.	신원 미상의 자가 회원가입 시도(건) 및 문의글 게시	
	7.27. ~ 8.3.	신원 미상의 자로부터 로그인 시도* 발생	
	8.2.	수검 기관 내부 보고 및 보안 전문가 자문	
	8.8.	외부 공격(크리덴셜 스터핑) 확인 후 WAF정책 변경	
	8.9.	총 건의 로그인 성공(7.27.~8.3.) 확인	**인지**(1차)
	8.11.	이용자 명에게 유출 통지	통지(1차)
	8.13.	로그인 성공 추가(8.11.~8.12.) 확인	인지(2차)
	8.14.~17.	이용자에게 추가 유출 통지	통지(2차)
	8.22.	건의 로그인 성공(8.20.~8.21.) 추가 확인	인지(3차)
	8.23.	개인정보 유출 신고	**신고**
	8.24.	대표 홈페이지에 유출 통지문 게시	게시
	8.25.	이용자 명에게 유출 통지	통지(3차)

3) 사후 조치

피심인은 유출 사고 인지 후 동일계정 로그인 5회 시도시 계정을 잠금하도록 하고, 기존 회원 로그인 시 비밀번호을 필수로 변경하도록 하였으며, 중국 대역

IP차단 등을 조치하였다.

3. 개인정보의 취급·운영 관련 사실관계

가. 안전성 확보에 필요한 조치를 소홀히 한 사실

피심인은 대표 홈페이지에 단시간내 과다한 로그인 시도 등 비정상적인 로그인 시도가 발생하였음에도 이를 탐지·차단하지 못하는 등 정보통신망을 통한 불법적인 개인정보 유출 시도 탐지 및 대응을 소홀히 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

가. 피심인 의견

개인정보보호위원회는 2024.5.28. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023.6.18.에 의견을 제출하였다.

피심인은 과도하거나 급격한 로그인 시도를 모니터링 하고 있으며, 동일한 IP에서 연속적으로 공격하는 것이 탐지되는 경우 해당 IP를 차단함으로써 공격자에게 신속하게 대응하는 등 안전조치를 다하였다고 주장한다.

나. 검토의견 : 불수용

피심인은 2023년 7월 27일부터 대표 홈페이지에 평소 로그인 시도의 약 1,000배에 달하는 대량의 로그인 시도*(만 건 이상) 및 실패(99.9%)가 발생하였고, 단일IP에서 1초에 건의 비정상적인 로그인 시도가 이루어졌음에도 2023년 8월 2일까지 이를 탐지·차단하지 못하였으며, 2023년 8월 8일 17시 까지 아무런 조치를 취하지 않는 등 안전조치를 소홀히 한 사실이 있으므로 피심인의 주장을 수용하지 않는다.

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’) 제6조 제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고, 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응 조치를 하여야 한다”라고 규정하고 있다.

2. 위법성 판단

가. 안전성확보조치를 소홀히 한 사실

[舊 보호법 제29조(안전조치의무)]

피심인이 대표홈페이지에 IP주소 등을 분석하여 비정상적인 로그인 시도 등 불법적인 개인정보 유출 시도 탐지 및 대응을 소홀히 한 행위는 舊 보호법 제29조, 舊 시행령 제30조1항, 舊 안전조치기준 제6조제1항 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 舊 보호법 제29조 위반에 대해 같은 법 제75조제2항제6호, 舊 시행령 제63조 [별표2] 및 「舊 개인정보 보호법 위반에 대한 과태료 부과기준」[4] (이하 ‘舊 과태료 부과기준’)에 따라 다음과 같이 600만 원의 과태료를 부과한다.

---

2) 대통령령 제32813호, 2022. 10. 20. 일부개정, 2022. 7. 19. 시행
3) 개인정보보호위원회고시 제2021-2호, 2021. 9. 15. 시행
4) 개인정보 보호법 위반에 대한 과태료 부과기준(개인정보보호위원회 지침, 2023. 3. 8. 시행)

가. 기준금액

舊 시행령 [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 과태료인 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 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중

舊 과태료 부과기준 제8조는 '당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 2]의 가중기준(조사 방해, 위반의 정도, 위반기간 등)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정하고 있다.

피심인의 경우 舊 과태료 부과기준 제8조 및 [별표 2] 과태료의 가중기준에 따라, '법 위반 상태의 기간이 3개월 이상인 경우'에 해당하여 기준금액(600만 원)의 10%(60만 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 등, ▲개인정보 보호인증·자율규제규약 등 개인정보 보호활동, ▲사업 규모 등)에 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)’, ‘자진 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 360만 원의 과태료를 부과한다.

< 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만 원)			
위반 조항	처분 조항	기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
舊 보호법 제29조(안전조치의무)	舊 보호법 제75조제2항제6호	600	60	300	**360**

※ 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 개인정보보호위원회 처분 결과 공표기준」 (2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 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	사회복지법인 월드비전	舊 법 제29조	안전조치의무 위반	2024. 10. 23.	과태료 360만 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, 제66조제1항에 따라 과태료 부과 및 공표를 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　(서 명)

위　　원　　박 상 희　(서 명)

위　　원　　조 소 영　(서 명)