개 인 정 보 보 호 위 원 회
제 2 소 위 원 회

심의·의결

안 건 번 호 **제2024-212-422호**

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

피 심 인 **주식회사 비플스** (사업자등록번호 :)

대표자

의결연월일 **2024. 6. 12.**

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 6,000,000원

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 청첩장 제작·판매 서비스를 제공하는 홈페이지를 운영하는 사업자로, 의 개인정보를 처리하는 「舊 개인정보 보호법」[1](이하 '舊 보호법') 제2조제5호에 따른 개인정보처리자이다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	상시 종업원 수
㈜비플스				

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 포털(privacy.go.kr)에 유출 신고('23.3.2.)한 피심인에 대하여 개인정보보호 법규 위반 여부를 조사('23.5.15.~'23.9.5.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 홈페이지 관리를 위하여 '23. 7. 17.(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

한국인터넷진흥원에서 타 기업 해킹사고 관련 분석 중 피심인의 직원정보가 담긴 데이터가 확인되었다.

* 피심인은 접근권한 내역 및 접속기록을 단기간(3개월)만 보관하여 정확한 유출경로 확인은 불가

1) (유출규모 및 항목) 직원 및 퇴사자의 개인정보* **163건**

* 성명, 전화번호, 이메일, 주소, 직책 등

2) 유출인지 및 대응

일 시	유출 인지·대응 내용	비고
'23.2.27.	한국인터넷진흥원은 피심인의 유출정보를 발견하고 이메일로 안내	
'23.3.1.	피심인의 회신 부재로 유선 재안내	인지
'23.3.2.	개인정보 유출 통지 (대면, 사내 공지, 이메일, 문자 등)	통지
	개인정보 포털에 개인정보 유출 신고	신고
'23.3.6-10.	정보유출 대응방안 보고서에 따른 검토 및 보안 강화조치	후속조치

3) 사후 조치

피심인은 유출 사고 인지 후 관리자 계정의 비밀번호를 변경하고 이를 암호화하였으며, 보유기간이 경과한 불필요한 데이터를 삭제하고, 접근 권한에 대한 기록과 개인정보처리시스템에 접속한 기록 보관 등을 실시하였다.

3. 개인정보의 취급·운영 관련 사실관계

가. 보유기간이 경과한 개인정보를 파기하지 않은 사실

피심인은 퇴사한 홈페이지 관리자의 계정정보(118건)을 파기하지 않고 개인정보처리시스템에 지속 보관한 사실이 있다.

나. 안전성 확보에 필요한 조치를 소홀히 한 사실

피심인은 홈페이지 관리자 계정 비밀번호를 암호화하지 않은 평문으로 DB에 저장하였으며, 개인정보처리시스템에 대한 개인정보취급자의 접근 권한 내역과 접속 기록을 각각 3개월만 보관한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2023.9.22. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2023.9.25.에 법 위반 사실을 인정하고 선처를 요청하는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련 법 규정

舊 보호법 제21조제1항은 “개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.”라고 규정하고 있다.

舊 보호법 제29조는 안전조치의무에 관한 규정으로 “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 있고,

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 상응

2) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2020. 10. 20. 시행

하는 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’) 제5조제3항은 “개인정보처리시스템의 접근권한 부여, 변경, 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야”하고, 제8조제1항은 “개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야”하며, 제7조제2항은 “비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다”라고 규정하고 있다.

2. 위법성 판단

가. 보유기간이 경과한 개인정보를 파기하지 않은 사실

[舊 보호법 제21조(개인정보의 파기)제1항]

피심인이 퇴사한 홈페이지 관리자의 계정정보(118건)을 지체 없이 파기하지 않고 개인정보처리시스템에 지속 보관한 행위는 舊 보호법 제21조제1항을 위반한 것이다.

나. 안전성확보조치를 소홀히 한 사실

[舊 보호법 제29조(안전조치의무)]

피심인이 비밀번호를 일방향 암호화하지 않고 평문으로 저장한 행위와 개인정보처리시스템에 대한 접근 권한 부여, 변경 또는 말소에 대한 내역을 3년간 보관하지 않고, 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하지 않은 행위는 舊 보호법 제29조, 舊 시행령 제30조1항, 舊 안전조치기준 제7조제2항, 제5조제3항 및 제8조제1항 위반에 해당한다.

Ⅳ. 처분 및 결정

3) 개인정보보호위원회고시 제2021-2호, 2021. 9. 15. 시행

1. 과태료 부과

피심인의 舊 보호법 제21조제1항 및 제29조 위반에 대해 같은 법 제75조제2항제4호 및 제6호, 舊 시행령 제63조 [별표2] 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[4] (이하 '과태료 부과기준')에 따라 다음과 같이 600만 원의 과태료를 부과한다.

※ '질서위반행위규제법' 제3조(법 적용의 시간적 범위)제2항에 따라 '질서위반행위 후 법률이 변경되어 과태료가 변경되기 전의 법률보다 가볍게 된 때'에 해당하므로 과태료 부과 시 피심인에게 유리하게 변경된 「개인정보 보호법 위반에 대한 과태료 부과기준(개인정보위 지침, '23.9.15.시행)을 적용함

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
마. 법 제21조제1항을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우	舊 법 제75조 제2항제4호	600	1,200	2,400
자. 법 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	舊 법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중

과태료 부과기준 제7조는 '당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 3]의 가중기준(위반의 정도, 위반기간, 조사방해, 위반 주도)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다'라고 규정

4) 개인정보보호위원회지침, 2023. 9. 11. 일부개정, 2023. 9. 15. 시행

하고 있고, 제7조2항은 '[별표 3]의 각 기준에 따른 과태료 가중 시 그 사유가 2개 이상 해당되는 경우에는 합산하여 가중하되, 기준금액의 100분의 50을 초과할 수 없다'라고 규정하고 있다.

피심인의 경우, 舊 보호법 제21조제1항 위반행위에 대해 '법 위반 상태의 기간이 2년을 초과하는 경우'에 해당하여 기준금액(600만 원)의 30%(180만 원)를 가중하고, 제29조 위반행위에 대해 '제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우*'에 해당하여 기준금액(600만 원)의 30%(180만 원)를 가중한다.

* 개인정보에 대한 접근 권한을 제한하지 않은 경우, 개인정보를 안전하게 저장·전송하는데 필요한 조치를 하지 않은 경우, 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관을 하지 않은 경우

다. 과태료의 감경

과태료 부과기준 제6조제1항은 '당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 2]의 감경기준(당사자 환경, 위반정도, 개인정보처리자의 업무형태 및 규모, 개인정보 보호인증, 자율규제규약 등, 개인정보 보호활동, 조사협조, 자진시정 등, 피해회복·피해확산방지, 자진신고)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다. 다만, 과태료를 체납하고 있는 경우는 제외한다"라고 규정하고 있고, 제6조제2항은 '[별표 2]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 경우 과태료 부과기준 제6조 및 [별표 2] 과태료의 감경기준에 따라, '「중소기업기본법」제2조에 따른 소기업인 경우', '조사에 적극 협력한 경우', '자진 시정을 완료한 경우', '위반행위 사실을 자진신고 한 경우'에 해당하여 기준금액(600만 원)의 80%(480만 원)를 각각 감경한다.

라. 최종 과태료

피심인의 舊 보호법 제21조제1항 및 제29조 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 600만 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 제21조(개인정보의 파기)제1항	舊 보호법 제75조제2항제4호	600	180	480	**300**
舊 보호법 제29조(안전조치의무)	舊 보호법 제75조제2항제6호	600	180	480	**300**
합계		1200	360	960	**600**

※ 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 제21조제1항 및 제29조 위반에 대해 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 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	㈜비플스	법 제21조 제1항	개인정보 파기 위반	2024. 6. 12.	과태료 600만 원
		법 제29조	안전조치의무 위반		
2024년 6월 12일 개 인 정 보 보 호 위 원 회					

Ⅴ. 결론

피심인의 舊 보호법 제21조(개인정보의 파기)제1항, 제29조(안전조치의무) 위반에 대하여 같은 법 제75조(과태료)제2항제4호 및 제6호, 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 6월 12일

위 원 장 김 진 욱

위 원 김 진 환

위 원 박 상 희