개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2023-019-238호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2024. 6. 12.

주 문

1. 피심인에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 개정된 「개인정보 보호법[1]」 제29조(안전조치의무), 같은 법 시행령[2] 제30조(개인정보의 안전성 확보 조치), 「개인정보의 안전성 확보조치 기준[3]」 제6조제3항을 준수하는 주기적인 계획을 수립하고 이행하여야 한다.

나. 피심인은 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 한다.

---

1) 개인정보 보호법(법률 제19234호, 2023. 3. 14. 일부개정, 2023. 9. 15. 시행)
2) 개인정보 보호법 시행령(대통령령 제33723호, 2023. 9. 12. 일부개정, 2023. 9. 15. 시행)
3) 개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시 제2023-6호, 2023. 9. 22. 시행)

다. 피심인은 가.부터 나.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 태 료 : 3,600,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

3. 피심인의 법 위반행위 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 영리를 목적으로 웹( )으로 조립PC 등을 판매하는 쇼핑몰 서비스를 제공하는 「舊 개인정보 보호법」[4](이하 '舊 보호법'이라 한다)에 따른 개인정보처리자이자 정보통신서비스 제공자이며, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 피심인이 신원미상의 자(이하 '해커'라 한다)의 협박 메일을 수신하고 개인정보 유출 사실을 인지하여 유출신고('23. 5. 30.) 함에 따라 개인정보 취급·운영 실태 및 舊 보호법 위반 여부를 조사('23. 6. 12. ~ '23. 10. 13.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

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

피심인은 조립PC 등을 판매하는 쇼핑몰 서비스를 제공하면서 ’23. 6. 23.(자료 제출일) 기준 건의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구 분	항 목	기 간	건 수(건)
계			

나. 개인정보 유출 관련 사실관계

피심인이 운영하는 조립PC 등 판매 쇼핑몰의 상품정보 페이지*에 해커가 SQL Injection 공격으로 이용자의 개인정보를 유출함(’23.5.16.)

* (상품정보 페이지)

1) **(유출 규모 및 항목)** 이용자의 개인정보 **건***

* 이름, 휴대전화번호, 아이디, 암호화된 비밀번호(SHA-256), 이메일, 주소, 생년월일, 암호화된 계좌번호(SEED)

2) 유출 인지 및 대응

일 시	유출 인지 및 대응 내용
’23. 5. 30. 01:12	해커의 협박 메일*을 수신 * 기자와 회원에게 해킹 사실을 유포하겠다고 협박하며 비트코인을 요구
’23. 5. 30. 08:10	해커의 협박 메일을 열람하고 해킹 사실 및 개인정보 유출 사실인지
’23. 5. 30. 10:20~	로그 분석을 통해 공격이 의심되는 페이지*에 대한 취약 소스코드 보완** * 상품정보 페이지 : ** 관련 SQL 입력값에 특수문자 미포함 되도록 조치 등 검증 절차 추가
’23. 5. 30. 15:30	개인정보 포털(privacy.go.kr)에 개인정보 유출 신고
’23. 5. 30. 15:43	유출 이용자 대상 개인정보 유출 통지(1차) ※ ‘23.5.30. 유출 사실을 홈페이지에도 공지하였으나, 시간은 확인 불가
’23. 6. 7. 16:52	유출 이용자 대상 개인정보 유출 통지(2차) ※ 1차 통지 후 확인된 유출항목 추가 통지

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보처리시스템에 대한 안전조치 의무를 소홀히 한 사실

피심인은 ’19. 6월 ~ ’23. 9. 15. 동안 운영 중인 웹사이트의 상품정보 페이지에 대해 SQL 입력값 검증 절차를 적용하지 않아, 해커의 SQL Injection 공격으로 회원 정보가 유출·공개된 사실이 있다.

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 2023. 10. 18. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 같은 해 10. 31. 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[5](이하 ‘舊 시행령’이라 한다) 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위해 ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다. 또한, 같은 조 제3항은 “제1항에 따른 안전성 확보조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

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

한편, 舊 시행령 제48조의2제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 「舊 개인정보의 기술적·관리적 보호조치 기준[6]」 (이하 '舊 기술적 보호조치 기준'이라 한다) 제4조제9항은 "처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다."라고 규정하고 있다.

舊 기술적 보호조치 기준 해설서는 제4조제9항에 대해 "인터넷 홈페이지를 통한 개인정보 유·노출 방지를 위해 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방지 조치를 하여야 하며, 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근통제 등에 관한 보호조치를 하여야 한다."라고 해설하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 안전조치 의무를 소홀히 한 사실

{舊 보호법 제29조(안전조치의무) 중 접근통제}

피심인이 '19. 6월 ~ '23. 9. 15. 동안 운영 중인 웹사이트의 상품정보 페이지에 대해 SQL 입력값 검증 절차를 적용하지 않아, 해커의 SQL Injection 공격으로 회원 정보가 유출·공개된 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(舊 기술적 보호조치 기준 등)
안전조치의무 위반	舊 보호법 §29	§48의2① 2호	• 처리 중인 개인정보가 인터넷 홈페이지 등을 통하여 열람 권한이 없는 자에게 유출되지 않도록 조치를 취하지 아니한 행위(舊 기술적 보호조치 기준§4⑨)

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

Ⅳ. 처분 및 결정

1. 과징금 면제

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15제1항제5호, 舊 시행령 제48조의11 [별표 1의5] 및 「舊 개인정보보호 법규 위반에 대한 과징금 부과기준」(개인정보보호위원회 고시 제2022-3호, 2022. 10. 20. 시행, 이하 '舊 과징금 부과기준'이라 한다) 제9조제2항제1호에 따라 과징금을 면제한다.

舊 과징금 부과기준 제9조제2항은 ▲위반행위자의 지급불능 · 지급정지 또는 자본잠식 등의 사유로 위반행위자가 객관적으로 과징금을 낼 능력이 없다고 인정되는 경우, ▲정보주체에게 피해가 발생하지 않았거나 경미한 경우로서 다음 각 목(가. 제8조에 따라 산정된 과징금이 300만원 이하인 경우, 나. 사소한 부주의나 오류로 인한 위반행위인 경우, 다. 개인정보가 유출된 경우로서 유출된 정보주체의 수가 100명 미만인 경우)의 어느 하나에 해당하는 경우, ▲위반행위자 본인의 행위가 위법하지 않은 것으로 잘못 인식할 만한 정당한 사유가 있는 경우의 어느 하나에 해당하는 경우에는 제8조에 따라 산정된 과징금을 면제할 수 있다고 규정하고 있다.

피심인은 완전자본잠식 등의 사유로 위반행위자가 객관적으로 과징금을 낼 능력이 없다고 인정되는 경우로 舊 과징금 부과기준 제9조제2항제1호에 해당한다고 판단되며, 추가로, 피심인이 속한 조립PC 시장·산업 여건 또한 현저하게 지속적으로 악화하는 상태임에도 불구하고, 조사에 적극 협조하였으며, 24시간 이내에 개인정보 유출·통지 신고를 완료하였으며 해킹 사실을 인지하고 해당 취약점에 대해 2시간여 만에 보완조치를 완료한 점, 사고를 계기로 운영중인 홈페이지 전반에 대해 취약점을 점검하고 발견된 취약점 항목에 대해 모두 이행한 점, 지속적으로 개인정보 보호조치를 하겠다고 의지를 표명하고 있는 점 등을 종합적으로 고려하여 산정된 과징금을 면제한다.

2. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대한 과태료는 같은 법 제75조(과태료) 제2항제6호 및 舊 시행령 제63조의〔별표2〕'과태료 부과기준' 및 「舊 개인정보 보호법 위반에 대한 과태료 부과기준」(2023. 3. 8. 일부 개정, 이하 '舊 과태료 부과지침'이라 한다)에 따라 다음과 같이 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 제29조(안전조치의무) 위반에 대해서는 1회 위반에 해당하는 과태료인 600만 원을 기준금액으로 적용한다.

< 舊 시행령 [별표2] 2. 개별기준 >

(단위: 만 원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 또는 **제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우**	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중 및 감경

1) (과태료의 가중) 舊 과태료 부과지침 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 舊 보호법 제29조(안전조치의무)에 대해서 ▲위반 기간이 3개월 이상인 경우에 해당하므로 기준금액의 10%를 가중한다.

2) (과태료의 감경) 舊 과태료 부과지침 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 舊 보호법 제29조(안전조치의무) 위반행위에 대하여, ▲사전통지 및 의견제출 기간 내에 위반행위를 시정 완료한 경우인 점, ▲일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료를 제출 또는 진술하는 등 조사에 적극적으로 협력한 점, ▲중기업인 점 등을 종합적으로 고려하여 舊 과태료 부과지침 제7조에 따라 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 360만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제)	600만 원	60만 원	300만 원	**360만 원**

3. 시정조치 명령

가. 피심인은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 개정된 「개인정보 보호법[7]」 제29조(안전조치의무), 같은 법 시행령[8] 제30조(개인정보의 안전성 확보 조치), 「개인정보의 안전성 확보조치 기준[9]」 제6조제3항을 준수하는 주기적인 계획을 수립하고 이행하여야 한다.

7) 개인정보 보호법(법률 제19234호, 2023. 3. 14. 일부개정, 2023. 9. 15. 시행)
8) 개인정보 보호법 시행령(대통령령 제33723호, 2023. 9. 12. 일부개정, 2023. 9. 15. 시행)
9) 개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시 제2023-6호, 2023. 9. 22. 시행)

나. 피심인은 대표자를 비롯하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 한다.

다. 피심인은 가.부터 나.까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출하여야 한다.

4. 결과 공표

舊 보호법 제66조제1항 및 「舊 개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, 피심인의 위반행위는 위반상태가 6개월 이상 지속된 경우(제5호)에 해당하므로, 피심인의 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		舊 보호법* 제29조	안전조치의무 위반 (접근통제)	2024. 6. 12.	시정명령 과태료 360만 원

* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호

2024년 6월 12일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대하여 같은 법 제64조(시정조치 등) 제1항, 제66조(결과의 공표) 제1항, 제75조(과태료) 제2항제6호에 따라 시정조치 명령, 공표, 과태료 부과를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분통지를 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분통지를 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조 제2항의 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.

2024년 6월 12일

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)