# 개 인 정 보 보 호 위 원 회
# 심의·의결

**안 건 번 호** 제2025-015-229호
**안 건 명** 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
**피 심 인** ㈜비와이엔블랙야크

**의결연월일** 2025. 7. 9.

## 주 문

1. 피심인에 대하여 다음과 같이 과징금을 부과한다.

   가. 과 징 금 : 1,391,000,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인은 처분등에 대한 통지를 받은 날부터 1개월 이내 당해 처분등을 받은 사실 등을 피심인의 홈페이지(모바일 어플리케이션 포함)에 2일 이상 5일 미만 게시하여야 한다. 이때, 구체적인 공표내용과 방법 등은 개인정보보호위원회와 미리 문서로 협의를 거쳐야 한다.

# 이 유

## Ⅰ. 기초 사실

피심인은 의류용품 제조·판매 서비스를 운영하는 「개인정보 보호법」[1](이하 '보호법')에 따른 개인정보처리자이며, 피심인의 일반현황은 다음과 같다.

**< 피심인의 일반현황 >**

| 피심인명 | 사업자등록번호 (법인등록번호) | 대표자 성명 | 주소 | 종업원 수 (명) |
|---|---|---|---|---|
| ㈜비와이엔 블랙야크 | | | | |

## Ⅱ. 사실조사 결과

### 1. 조사 배경

개인정보보호위원회는 피심인이 개인정보 유출신고('25. 3. 4.)함에 따라 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('25. 3. 7. ~ '25. 5. 16.)하였으며, 다음과 같은 사실을 확인하였다.

### 2. 행위 사실

#### 가. 개인정보 수집현황

피심인은 의류용품 제조·판매 서비스를 운영하면서 '25. 3. 21.(자료제출일) 기준 아래와 같이 개인정보를 수집하여 보관하고 있다.

1) 법률 제19234호, 2023. 3. 14. 일부개정, 2024. 3. 15. 시행

**< 개인정보 수집현황 >**

| 구분 | 항목 | 기간 | 건수 |
|---|---|---|---|
| | | | |
| | | | |

## 나. 개인정보 유출 관련 사실관계

### 1) 유출 경위

해커가 '25. 3. 1. ~ 3. 4. 동안 피심인이 운영 중인 웹사이트 내 고객 상담 페이지(  )에 SQL Injection 공격으로 DB에 저장된 관리자 계정 정보*를 탈취하였고,

* SQL injection 공격으로 관리자 계정명과 암호화(SHA-256)된 비밀번호(64자리 해시값)를 탈취한 사실은 확인되나, 해커가 평문 비밀번호를 확보한 방법은 확인되지 않음

탈취한 최고 관리자 계정(  ) 정보를 악용하여 피심인의 관리자 페이지에 로그인 후, '엑셀 다운로드' 기능으로 이용자의 개인정보를 다운로드 받아 유출하고 쇼핑몰 배너 이미지를 변경함

### 2) 유출내용

해커가 다운로드 받은 엑셀 파일 데이터 분석 결과, 342,253명의 개인정보가 유출되었으며, 유출 항목은 이름, 성별, 생년월일, 휴대폰 번호, 주소 일부(동·호수 등)가 포함되어있다.

### 3) 유출 인지 및 대응

| 일 시 | | 유출 인지 및 대응 내용 |
|---|---|---|
| ’25. 3. 4. | 11:31 | • 웹사이트에 잘못된 배너 이미지 노출 사실 인지 |
| ’25. 3. 4. | 11:41 | • 관리자 페이지 접속권한을 사내 IP로 제한, 최고 관리자 계정 비밀번호 변경 |
| ’25. 3. 4. | 13:20 | • 외부 IP가 회원정보를 다운로드 받은 사실을 확인하여 **개인정보 유출 인지** |
| ’25. 3. 5. | 10:40 | • 경찰청 사이버수사대 신고 |
| ’25. 3. 5. | 10:40 | • 개인정보 **유출 신고** |
| ’25. 3. 6. | 09:30 | • 개인정보 **유출 통지**(문자) |
| ’25. 3. 7. | 17:30 | • 관리자 페이지 OTP 2차 인증 조치 |
| ’25. 3. 13. | 21:28 | • 웹사이트 SQL 인젝션 취약 페이지 개선 조치 |
| ’25. 3. 19. | 17:00 | • 웹방화벽 설치 및 SQL 인젝션 차단 정책 설정 |

## 3. 개인정보의 취급.운영 관련 사실관계

### 가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 ’21. 10월부터 웹사이트 내 고객상담 페이지( )를 운영하면서, SQL 입력값에 대한 검증 절차를 적용하지 않았으며, ’23. 8. 28.부터 웹방화벽( )을 운영하였으나, SQL Injection 공격을 탐지·차단하는 등 대응할 수 있는 정책을 적용하지 않은 사실이 있다.

또한, 피심인은 외부 행사 진행, 재택 근무 등의 사유로 외부에서 관리자 페이지 접근이 가능하도록 허용하였으나, 관리자 페이지 로그인 시 ID, PW 외 OTP 등 안전한 인증수단을 적용하지 않고 운영한 사실이 있다.

### 4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 ‘25. 5 26. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’25. 6. 10 개인정보보호위원회에 의견을 제출하였다.

## Ⅲ. 위법성 판단

### 1. 관련법 규정

가. 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[2](이하 ‘시행령’) 제30조제1항제3호는 “개인정보에 대한 접근을 통제하기 위해 ‘개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치(가목)’, ‘그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치(다목)’를 하여야 한다.”라고 규정하고 있으며, 같은 조 제3항은 “제1항에 따른 안전성 확보조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

한편, 시행령 제30조제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 개인정보의 안전성 확보조치 기준[3](이하 ‘고시’) 제6조1항은 “정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)’, ‘개인정보처리시스템에 접속한 IP 주소 등을 분석하여 개인정보 유출 시도를 탐

2) 개인정보 보호법 시행령(대통령령 제33723호, 2023. 9. 12. 일부개정, 2023. 9. 15. 시행)
3) 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2023-6호, 2023. 9. 22. 시행)

지 및 대응(제2호)’하는 등의 안전조치를 하여야”하고, 제6조제2항은 “개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다.” 라고 규정하고 있으며, 제3항은 “개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.”라고 규정하고 있다.

## 2. 위법성 판단

### 가. 개인정보처리시스템에 대한 안전조치 의무를 소홀히 한 사실

[보호법 제29조(안전조치의무)]

피심인이 ’21. 10월. ~ ’25. 3. 12. 동안 운영중인 웹사이트의 고객상담 페이지( )에 SQL 입력값에 대한 검증 절차 누락 등 취약점 점검·조치를 소홀히 한 행위는 보호법 제29조, 시행령 제30조제1항제3호, 안전성 확보조치 기준 제6조제3항을 위반한 것이다.

피심인이 웹방화벽( )를 운영하였으나, SQL Injection 공격을 방지하기 위한 보안정책 설정을 적용하지 않고, IP 주소 등을 재분석하여 이상행위 대응 등 개인정보 유출시도에 대한 침입탐지 및 대응 조치를 소홀히 한 행위는 보호법 제29조, 시행령 제30조제1항제3호, 안전성 확보조치 기준 제6조제1항을 위반한 것이다.

피심인이 외부 행사 진행 및 재택 근무 등 목적으로 개인정보취급자가 외부에서 개인정보처리시스템에 접근할 수 있도록 운영하였으나, 외부에서 개인정보처리시스템 접속 시 ID, PW 외 OTP 등 안전한 인증 수단을 적용하지 않고 운영한 행위는 보호법 제29조, 시행령 제30조제1항제2호, 안전성 확보조치 기준 제6조제2항을 위반한 것이다.

< 피심인의 위반사항 >

| 위반행위 | 법률 | 시행령 | 세부내용(고시 등) |
|---|---|---|---|
| 안전조치의무 위반 | 보호법 §29 | §30① 3호 | ・개인정보처리시스템에 접속한 IP 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응을 소홀히 한 행위(고시§6①) |
| | | | ・정보통신망을 통해 외부에서 개인정보처리시스템에 접속하는 경우 안전한 인증수단을 적용하지 않은 행위(고시§6②) |
| | | | ・처리하는 개인정보가 인터넷 홈페이지 등을 통하여 권한이 없는자에게 공개되거나 유출되지 않도록 조치를 취하지 않은 행위(고시§6③) |

# Ⅳ. 처분 및 결정

## 1. 과징금 부과

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 같은 법 제64조의2제1항 제9호, 시행령 제60조의2 [별표 1의5] 및「개인정보보호 법규 위반에 대한 과징금 부과기준[4]」(이하 '과징금 부과기준')에 따라 다음과 같이 부과한다.

### 가. 과징금 상한액

피심인의 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제64조의2제1항, 시행령 제60조의2에 따라 위반행위가 있었던 사업연도 직전 3개 사업연도의 연평균 매출액의 100분의 3을 초과하지 아니하는 범위에서 부과할 수 있다.

### 나. 기준금액

#### 1) 중대성의 판단

과징금 부과기준 제8조제1항은 '시행령 [별표 1의5] 2. 가. 1) 및 2)에 따른 위반

4) 개인정보보호 법규 위반에 대한 과징금 부과기준(개인정보보호위원회 고시 제2023-3호, 2023. 9. 15. 시행)

행위의 중대성의 정도는 [별표] 위반행위의 중대성 판단기준을 기준으로 정한다.’라고 규정하고 있다.

[별표] 위반행위의 중대성 판단기준에 따르면 ‘위반행위의 중대성의 정도는 고려사항별 부과기준을 종합적으로 고려하여 판단’하고, ‘고려사항별 부과수준 중 두 가지 이상에 해당하는 경우에는 높은 부과수준을 적용한다.’라고 규정하고 있으며, ‘고려사항별 부과수준의 판단기준은 ▲(고의 · 과실) 위반행위의 목적, 동기, 당해 행위에 이른 경위, 영리 목적의 유무 등을 종합적으로 고려, ▲(위반행위의 방법) 안전성 확보 조치 이행 노력 여부, 개인정보 보호책임자 등 개인정보 보호 조직, 위반행위가 내부에서 조직적으로 이루어졌는지 여부, 사업주, 대표자 또는 임원의 책임·관여 여부 등을 종합적으로 고려하고, 개인정보가 유출등이 된 경우에는 개인정보의 유출등과 안전성 확보 조치 위반행위와의 관련성을 포함하여 판단, ▲(위반행위로 인한 정보주체의 피해 규모 및 정보주체에게 미치는 영향) 피해 개인정보의 규모, 위반기간, 정보주체의 권리 · 이익이나 사생활 등에 미치는 영향 등을 종합적으로 고려하고, 개인정보가 유출등이 된 경우에는 유출등의 규모 및 공중에 노출되었는지 여부를 포함하여 판단한다.’라고 규정하고 있다.

피심인의 고의·과실, 위반행위의 방법, 처리하는 개인정보의 유형, 정보주체의 피해 규모 및 정보주체에게 미치는 영향 등을 종합적으로 고려하여, 위반행위의 중대성을 ’중대한 위반행위‘로 판단한다.

**2) 기준금액 산출**

과징금 부과기준 제6조제1항은 ‘기준금액은 전체 매출액에서 위반행위와 관련이 없는 매출액을 제외한 매출액에 부과기준율을 곱한 금액으로 정한다’라고 규정하고 있다.

피심인의 경우, 과징금 부과기준 제7조제3항에 따라 위반행위와 관련이 없는 매출액은 매출액으로 하고, 직전 3개 사업년도의 연평균 전체 매

출액에서 관련 없는 매출액을 제외한 천 원에 시행령 [별표 1의5] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의의 를 적용하여 기준금액을 천 원으로 한다.

**< 피심인의 위반행위 관련 매출액 >**

(단위 : 천 원)

| 구 분 | 2022년 | 2023년 | 2024년 | 평 균 |
|---|---|---|---|---|
| ①전체 매출액 | | | | |
| ②관련 없는 매출액 | | | | |
| ①에서 ②를 제외한 매출액 | | | | |

※ 피심인이 제출한 회계자료를 토대로 작성

**<시행령 [별표 1의5] 2. 가. 1)에 따른 부과기준율>**

| 위반행위의 중대성 | 부과기준율 |
|---|---|
| 매우 중대한 위반행위 | 2.1% 이상 2.7% 이하 |
| 중대한 위반행위 | 1.5% 이상 2.1% 미만 |
| 보통 위반행위 | 0.9% 이상 1.5% 미만 |
| 약한 위반행위 | 0.03% 이상 0.9% 미만 |

### 다. 1차 조정

과징금 부과기준 제9조에 따라 피심인이 ▲위반기간이 2년을 초과하므로 기준금액의 100분의 50에 해당하는 천 원을 가중하고, ▲위반행위로 인하여 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 경우에 해당하여 기준금액의 100분의 30에 해당하는 금액인 천 원을 감경한다.

### 라. 2차 조정

과징금 부과기준 제10조에 따라 피심인이 ▲조사에 적극 협력한 경우, ▲사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하고 시정을 완료한 경우에 해당하여 1차 조정을 거친 금액의 100분의 30에 해당하는 천 원을 감경한다.

## 마. 과징금의 결정

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제64조의2제1항제9호, 시행령 제60조의2, [별표 1의5] '과징금의 산정기준과 산정절차' 2. 가. 1) 및 '과징금 부과기준'에 따라 위와 같이 단계별로 산출한 금액인 13억 9,100만 원을 최종 과징금으로 결정한다.

**<과징금 산출 내역>**

| ①기준금액 | ②1차 조정 | ③2차 조정 | ④최종 과징금 |
|---|---|---|---|
| •직전 3개 사업연도 연평균 매출액<br>( 천 원)<br>•연평균 매출액에 % 적용 (중대한 위반*) | •위반기간** 2년 초과 50% 가중<br>( 천 원)<br>•취득이익 없으므로 30% 감경<br>( 천 원) | •시정완료, 조사협력 사유로 30% 감경***<br>( 천 원) | **1,391,000천 원**** |
| ⇒ 천 원 | ⇒ 천 원 | ⇒ 천 원 | |

* ①(고의·과실:**중**) ▲중과실, ▲영리 목적 없음, ▲내부 모니터링 중 사고 인지, 유출 인지 후 위반행위 자진시정 완료(일부 참작)

②(부당성:**중**) ▲안전조치의무(접근통제) 위반이 유출과 직접적 관련이 있으나, ▲개인정보 보호책임자 지정, ▲조직적인 행위 미해당, ▲대표자·임원의 관여 미해당 등 고려

③(개인정보 유형:**하**) ▲고유식별정보, 민감정보 미포함

④(피해규모:**중**) ▲위반기간 약 3년 6개월, ▲약 34만명의 온라인 회원 전체 유출(전체 회원의 약 26% 유출) ▲휴대폰 번호, 성별, 생년월일, 이름 유출로 스팸 문자 등 추가피해가 우려되는 점 등을 종합 고려

** 위반기간 : '21. 10월(홈페이지 게시) ~ '25. 3. 19.(접근통제 최종 조치일자)

*** 최초 조사 시점부터 위법사실을 모두 인정하고 위법성 판단에 도움이 되는 자료를 제출하는 등 적극 협력한 점을 고려하여 조사협력 사유로 감경하며, 사고 이후 위반행위를 자진 시정한 점을 고려하여 감경함

**** 과징금 부과기준 제11조제5항에 따라 1억원 이상인 경우에는 1백만원 단위 미만의 금액을 버림

### 2. 과태료 부과

피심인의 보호법 제29조(안전조치의무) 위반행위는 같은 법 제75조(과태료)제2항제5호에 따라 과태료 부과 대상에 해당하나, 제76조(과태료에 관한 규정 적용의 특례)에 따라 과징금을 부과한 행위와 동일하여 과태료를 부과하지 않는다.

### 3. 처분 결과 공표명령

피심인의 위반행위는 보호법 제66조제2항 및 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」[5](이하 '공표 및 공표명령 지침') 제6조제1항제7호·8호에 해당하고 위반행위가 인터넷을 통하여 이루어졌으므로, 제8조 및 제11조에 따라 처분등에 대한 통지를 받은 날부터 1개월 이내에 당해 처분등을 받은 사실을 피심인의 홈페이지(모바일 어플리케이션 포함)의 초기화면 팝업창에 전체화면의 6분의1 크기로 2일 이상 5일 미만의 기간 동안(휴업일 포함) 공표하도록 명한다.

이때 제7조제1항, 제8조제3항에 따라 원칙적으로 공표지침 [별표]의 표준 공표문안을 따르되, 공표 문안 등에 관하여 보호위원회와 미리 문서로 협의해야 하고, 제11조제3항에 따라 글자크기·모양·색상 등에 대해서는 해당 홈페이지 특성을 고려하여 보호위원회와 협의하여 정한다.

## Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 위반행위에 대하여 같은 법 제64조의2(과징금의 부과)제1항제9호, 시행령 제60조의2(과징금의 산정기준 등), 제66조(결과의 공표)에 따라 과징금, 공표명령을 주문과 같이 의결한다.

5) 개인정보 보호법 위반에 대한 공표 및 공표명령 지침(개인정보보호위원회 지침, 2023. 10. 11. 시행)

## 이의제기 방법 및 기간

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

이상과 같은 이유로 주문과 같이 의결한다.

2025년 7월 9일

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 김 휘 강 (서 명)

위 원 박 상 희 (서 명)

위 원 윤 영 미 (서 명)

위 원 이 문 한 (서 명)