제 12 회 개 인 정 보 보 호 위 원 회

제 2 소 위 원 회

심의·의결

안 건 번 호 제2023-212-217호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표자

의결연월일 2023. 6. 14.

주 문

1. 피심인 에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 10,800,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인 에 대한 과태료 부과의 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 기초 사실

PC 등을 판매하는 온라인 쇼핑몰을 운영하는 피심인은 「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16930호, 이하 '보호법'이라 한다.)에 따른 개인정보처리자 및 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수(명)
㈜커넥트웨이브	117-81-40065 (110111-2551996)	김기록, 정재웅, 김상혁	서울특별시 양천구 목동동로 233-1, 5층 501호 (목동, 현대드림타워)	282명

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보포털(privacy.go.kr)에 유출 신고('21. 11. 2., '21. 11. 16.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('22. 12. 27. ~ '23. 4. 11., '23. 3. 14. ~ '23. 5. 2.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 PC 등을 판매하는 온라인 쇼핑몰( )를 운영하면서 '23. 1. 9. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
회원 정보	(필수) 아이디, 비밀번호, 이름, 닉네임, 이메일 주소 (선택) 휴대전화번호, 주소, 계좌번호 등	'00. 12. 21. ~ 계속	(유효) (분리)
합 계			

나. 개인정보 유출 경위

< ① 개인정보 유출 사건('21. 11. 2. 유출 신고 건) **>**

1) 유출 경과 및 대응

일시		피심인의 유출 인지·대응 내용
'21. 10. 19.	16:20	내부 모니터링 과정에서 장바구니 상품 조회 실패 등 이상 로그 발생 인지
'21. 10. 29.	09:25	로그 분석을 위해 수정한 소스코드 배포
'21. 11. 1.	17:44	상세한 오류 발생 원인 파악을 위해 소스코드 재수정
'21. 11. 2.	09:12	추가 수정한 소스코드(오류가 포함된 코드) 배포
'21. 11. 2.	09:21	시스템 장애 관련 로그를 통해 개인정보 유출 인지 및 소스코드 수정 이전 버전으로 롤백
'21. 11. 2.	17:35	개인정보 유출 고객 대상 유출 통지
'21. 11. 2.	18:25	개인정보포털에 개인정보 유출 신고

2) 유출항목 및 규모

이용자 10명*의 이름, 주소, 휴대전화번호, 추가 연락처, 주문 상품 정보 등이 유출되었다.

* 로그 분석 결과, 주문자 회원정보와 해당 주문정보를 열람한 자의 회원정보가 일치하지 않아 개인정보가 유출된 이용자는 총 10명으로 확인

3) 유출 경위

피심인의 소스코드 설정 오류*로 '21. 11. 2. 09:12부터 '21. 11. 2. 09:21.까지 주문목록 페이지( )에 접근한 이용자가 본인의 주문정보뿐만 아니라 로그인된 다른 회원들의 주문정보에도 접근할 수 있게 되어 개인정보가 유출되었다.

* 담당자 실수로 $marketPlaceMember[marketPlaceMemberSeq] = 0 ; 코드가 삽입된 채 소스코드가 배포되어 주문 목록 페이지에 접근한 회원의 고유번호가 0으로 변환되면서 당시 로그인된 모든 회원들의 주문정보에 접근이 가능해졌음

< ② 개인정보 유출 사건('21. 11. 16. 유출 신고 건) **>**

1) 유출 경과 및 대응

일시		피심인의 유출 인지·대응 내용
'21. 6. 30.	-	고객센터를 통해 주문한 상품이 아닌 다른 상품 주문 관련 알림톡을 수신했다는 민원 접수(1차 인지)
'21. 7. 8.	09:12	원인 분석을 위해 수정한 소스 코드 배포
'21. 7. 15.	-	본인 주문내역에 다른 사람 주문정보가 등록되는 문제가 발생했다는 민원 접수(2차 인지)
'21. 7. 27.	16:43	로그 확인을 위해 소스 코드 수정 후 배포
'21. 11. 8.	13:55	판매점으로부터 상품 오배송 관련 민원 접수(3차 인지)
'21. 11. 9.	16:16	장애 원인 파악을 위해 로그 분석 진행
'21. 11. 16.	12:46	개인정보 유출 고객 3명 대상 유출 통지
'21. 11. 16.	12:52	개인정보포털에 개인정보 유출 신고
'21. 11. 17.	10:04	결제 전·후 개인정보의 동일성 여부를 확인하는 기능을 추가한 소스코드 배포
'21. 11. 23.	09:24	배송정보가 저장되는 전역변수를 지역변수로 변경한 소스코드 배포

2) 유출규모 및 규모

이용자 3명의 주소, 연락처, 이메일 주소가 유출되었다.

※ 로그 분석 결과, 이용자 2명의 상품 주문 시각이 100분의 1초 단위까지 동일한 경우, 전역변수에 동시 접근하여 개인정보가 공유되는 문제가 발생하였음

3) 유출 경위

피심인은 '21. 6. 29. 개인정보 암호화 관련 개발 언어를 변경하는 과정에서 소스코드 설정 오류*로 인해 해당 상품을 주문한 회원이 아닌 다른 회원이 입력한 배송정보가 주문자의 배송정보로 저장되었으며, 이를 주문자가 열람하여 개인정보가 유출되었다.

* 분석 결과, 전역변수에 주소·연락처·이메일 주소가 저장되도록 구현하여, 이용자 2명이

동시에 상품 주문을 하는 경우, 전역변수에 동시 접근하여 개인정보가 공유되는 문제가 발생

3. 개인정보의 취급.운영 관련 사실관계

< ① 개인정보 유출 사건('21. 11. 2. 유출 신고 건) **>**

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인의 소스코드 설정 오류로 인해 '21. 11. 2. 09:12부터 '21. 11. 2. 09:21.까지 약 9분 동안 이용자 10명의 개인정보가 유출되었으며, 피심인은 취약점 점검 및 테스트 없이 해당 소스코드를 운영 서버에 배포한 사실이 있다.

< ② 개인정보 유출 사건('21. 11. 16. 유출 신고 건) **>**

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 '21.6.29. 개인정보 암호화 관련 개발 언어를 변경하는 과정에서 소스코드 설정 오류로 인해 이용자 3명의 개인정보가 유출되었으며, 피심인은 해당 소스코드 배포 전 수정한 암·복호화 기능의 작동 여부에 대한 테스트는 진행하였다고 소명하였으나 동시 주문 테스트 및 취약점 점검은 실시하지 않은 사실이 있다.

나. 개인정보 유출 통지·신고를 소홀히 한 행위

피심인은 세 차례에 걸친 개인정보 유출 관련 민원('21. 6. 30., '21. 7. 15., '21. 11. 8.)을 통해 개인정보가 유출된 사실을 각각 인지하였으나, '21. 11. 16. 유출 통지·신고한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '23. 4. 17., '23. 5. 2. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 '23. 5. 2., '23. 5. 4. 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 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위해 ’그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제48조의2제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

같은 법 시행령 제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(개인정보보호위원회 고시 제2021-3호, 이하 ‘고시’) 제4조제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있다.

나. 보호법 제39조의4제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체 없이 유출등이 된 개인정보 항목(제1호), 유출등이 발생한 시점(제2호), 이용자가 취할 수 있는 조치(제3호), 정보통신서비스 제공자등의 대응 조치(제4호), 이용자가 상담 등을 접수할 수 있는 부서 및 연락처(제5호)를 해당 이용자에게 알리고 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는

조치를 취할 수 있다.”라고 규정하고 있다.

같은 법 시행령 제48조의4제2항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제39조의4제1항 각 호의 모든 사항을 서면등의 방법으로 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고해야 한다.”라고 규정하고 있으며, 제3항은 “정보통신서비스 제공자등은 제2항에 따른 통지·신고를 하려는 경우에는 법 제39조의4제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.”라고 규정하고 있다.

2. 위법성 판단

< ① 개인정보 유출 사건(’21. 11. 2. 유출 신고 건) **>**

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

피심인이 주문 목록 페이지에 접근한 회원의 고유번호가 ‘0’으로 변환되도록 소스코드를 설정하고, 해당 소스코드 배포 전 취약점 점검 및 테스트 등을 소홀히 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항, 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반	보호법 §29	§48의2①	・열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위(고시§4⑨)

< ② 개인정보 유출 사건(’21. 11. 16. 유출 신고 건) **>**

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

피심인이 전역변수에 주문자의 배송정보(주소·연락처·이메일 주소)가 저장되도록 구현하고, 해당 소스코드 배포 전 취약점 점검 및 테스트 등을 소홀히 한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항, 고시 제4조제9항을 위반한 것이다.

나. 개인정보 유출 통지·신고를 소홀히 한 행위

[보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항]

피심인이 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 통지·신고한 행위는 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반	보호법 §29	§48의2①	• 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위(고시§4⑨)
개인정보 유출등의 통지·신고에 대한 특례 위반	보호법 §39의4①	§48조의4	• 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 유출 통지·신고한 행위

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 보호법 제29조(안전조치의무) 및 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항 위반행위에 대한 과태료는 같은 법 제75조제2항제6호·제12호의3, 같은 법 시행령 제63조, 같은 법 시행령 [별표2] '과태료의 부과기준' 및 '개인정보 보호법 위반에 대한 과태료 부과기준'(이하, '과태료 부과지침')에

따라 다음과 같이 부과한다.

< ① 개인정보 유출 사건('21. 11. 2. 유출 신고 건) >

가. 기준금액

보호법 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 보호법 제29조 위반행위에 대해 기준금액을 1회 위반에 해당하는 600만원으로 산정한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 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

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 경우, 과태료 부과지침 제8조 및 [별표2] 과태료의 가중기준에서 정한 가중사유가 없으므로 보호법 제29조 위반행위에 대해 기준금액을 유지한다.

2) 과태료의 감경

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 경우, 보호법 제29조 위반행위는 과태료 부과지침 제7조 및 [별표1] 과태료의 감경기준에 따라, '위반행위에 대해 시정을 완료한 경우' 및 '조사에 적극 협력한 경우'에 해당하여 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 300만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제)	600만원	-	300만원	**300만원**
계				**300만원**

< ② 개인정보 유출 사건('21. 11. 16. 유출 신고 건) **>**

가. 기준금액

보호법 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 보호법 제29조 위반행위 및 같은 법 제39조의4 제1항 위반행위에 대해 기준금액을 1회 위반에 해당하는 600만원으로 산정한다.

< 보호법 시행령 [별표2] 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
도. 법 제39조의4제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·보호위원회 및 전문기관에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제75조 제2항제12호의3	600	1,200	2,400

나. 과태료의 가중 및 감경

1) 과태료의 가중

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 경우, 보호법 제29조 위반행위는 과태료 부과지침 제8조 및 [별표2] 과태료의 가중기준에 따라 '법 위반상태의 기간이 3개월 이상인 경우'에 해당하여 기준금액의 10%를 가중하고, 같은 법 제39조의4제1항 위반행위는 과태료 부과지침 제8조 및 [별표2] 과태료의 가중기준에 따라 '법 위반상태의 기간이 3개월 이상인 경우' 및 '제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우'에 해당하여 기준금액의 20%를 가중한다.

2) 과태료의 감경

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 경우, 보호법 제29조 위반행위 및 같은 법 제39조의4제1항 위반행위는 과태료 부과지침 제7조 및 [별표1] 과태료의 감경기준에 따라, ‘위반행위에 대해 시정을 완료한 경우’ 및 ‘조사에 적극 협력한 경우’에 해당하여 기준금액의 50%를 각각 감경한다.

다. 최종 과태료

피심인의 보호법 제29조 위반행위 및 같은 법 제39조의4제1항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 780만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제)	600만원	60	300만원	**360만원**
개인정보 유출등의 통지·신고에 대한 특례	600만원	120	300만원	**420만원**
계				**780만원**

2. 결과 공표

< ② 개인정보 유출 사건(’21. 11. 16. 유출 신고 건) **>**

보호법 제66조제1항 및 ‘개인정보보호위원회 처분결과 공표기준’(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따르면 피심인의 위반행위는 ‘보호법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우(제4호)’에 해당하므로 피심인이 과태료 부과를 받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다.

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		법 제29조	안전조치의무 위반 (접근통제)	2023. 6. 14.	과태료 360만 원
		법 제39조의4 제1항	개인정보 유출통지·신고 위반(지연통지·신고)		과태료 420만 원
2023년 6월 14일 개 인 정 보 보 호 위 원 회					

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무) 및 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대하여 같은 법 제75조(과태료)제2항 제6호·제12호의3, 같은 법 제66조(결과의 공표)제1항에 따라 과태료 부과 및 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

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

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

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 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.

이상과 같은 이유로 주문과 같이 의결한다.

2023년 6월 14일

위 원 장　　지 성 우 (서명)

위　　원　　강 정 화 (서명)

위　　원　　염 흥 열 (서명)