개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 제2024-219-621호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인

의결연월일 2024. 9. 25.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 6,300,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대한 과태료 부과의 내용 및 결과를 개인정보보호위원회 홈페이지에 1년간 공표한다.

이 유

Ⅰ. 기초 사실

온라인 카페트 쇼핑몰( )을 운영하는 피심인은 「舊 개인정보 보호법」[1](이하 '舊 보호법'이라 한다)에 따른 정보통신서비스 제공자이며, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

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

Ⅱ. 사실조사 결과

1. 조사 배경

피심인이 한국인터넷진흥원으로부터 이용자의 개인정보가 다크웹에 유출된 정황을 전달받아 유출 신고('23. 2. 6.)함에 따라 개인정보보호위원회는 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('23. 4. 27. ~ '24. 4. 8.) 하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 카페트 쇼핑몰( )을 운영하면서 '23. 6. 23.(자료제출일) 기준 명의 개인정보를 수집하여 보관하고 있다.

1) 법률 제16930호, 2020. 2. 4. 일부개정, 2020. 8. 5. 시행

< 개인정보 수집현황 >

구 분	항 목	기 간*	건 수(건)

* 피심인은 이전 사업자에게 사업을 양도받아 '14.3.1.부터 홈페이지를 개설하여 서비스를 운영하였음

나. 개인정보 유출 관련 사실관계

'20. 8. 30. 신원 미상의 자(이하 '해커'라 한다)가 알 수 없는 방법으로 획득한 피심인의 카페트 쇼핑몰 회원정보를 다크웹에 게시하여 개인정보가 유출되었다.

1) (유출 규모 및 항목) 이용자 명의 개인정보*가 유출되었다.

* 휴대폰 번호, 유선번호, 이메일, 비밀번호, 회사 이메일

2) 유출 인지 및 대응

일 시		유출 인지 및 대응 내용
'23.2.3.	16:15	한국인터넷진흥원으로부터 다크웹 내 피심인의 회원정보 노출 의심 메일 수신
'23.2.6.	-	다크웹에 게시된 회원정보가 피심인의 회원정보임을 확인 및 **개인정보 유출 인지** ※ '23. 2. 3. 담당자 부재(휴가) 및 2. 4.~ 2. 5. 주말 휴무로 인해 메일 확인 및 회원정보 비교가 지연되었다고 소명
'23.2.6.	15:27	개인정보 **유출 신고**
'23.2.10.	00:00	홈페이지 내 개인정보 유출 안내 팝업 공지
'23.2.22.	14:08	개인정보 **유출 통지(이메일)** ※ 피심인은 다크웹에 게시된 이메일 건을 대상으로 유출통지 하였으나, 이메일 오류 및 중복가입에 따른 중복인원을 제외하여 발송된 인원이라고 소명

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보처리시스템에 대한 안전조치 의무를 소홀히 한 사실

피심인은 ’14. 3. 1. ~ ’23. 6. 13. 동안 외부에서 개인정보처리시스템에 접속하는 경우 안전한 인증수단을 적용하지 않고 운영한 사실이 있다.

피심인은 오픈소스 웹 방화벽( )을 운영하면서 신규 위협 대응 등을 위하여 접근 제한 및 유출 탐지 정책을 지속적으로 업데이트하지 않고, 인가받지 않은 접근을 제한하기 위한 모니터링을 소홀히 한 사실이 있다.

또한, 피심인은 이용자의 비밀번호를 일방향 암호화 방식(MD5)으로 암호화하여 저장하였다고 소명하였으나, 다크웹에 유출된 데이터에는 암호화되지 않은 비밀번호가 발견된 사실이 있다.

나. 개인정보 유출 통지를 소홀히 한 사실

피심인은 ’23. 2. 6. 개인정보 유출 사실을 인지하였으나, 정당한 사유 없이 24시간을 경과하여 ‘23. 2. 22. 14:08 이용자 대상 유출 통지를 한 사실이 있다.

4. 처분의 사전통지 및 의견수렴

개인정보보호위원회는 2024. 4. 9. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 별도 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 舊 보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변

조 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 ‘舊 시행령’이라 한다) 제48조의2제1항제2호는 “개인정보에 대한 불법적인 접근을 차단하기 위해 ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등을 하여야 한다.”라고 규정하고 있고, 같은 항 제4호는 개인정보가 안전하게 저장될 수 있도록 “비밀번호의 일방향 암호화 저장(가목)‘ 라고 규정하고 있다. 또한, 같은 조 제3항은 “제1항에 따른 안전성 확보조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.”라고 규정하고 있다.

한편, 舊 시행령 제48조의2제3항에 따라 안전성 확보조치에 관한 세부 기준을 구체적으로 정하고 있는 舊 개인정보의 기술적·관리적 보호조치 기준[3](이하 ‘舊 기술적 보호조치 기준’이라 한다) 제4조제4항은 “정보통신서비스 제공자등은 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용해야 한다.”라고 규정하고 있으며, 제4조제5항은 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(2호)하는 기능을 포함한 시스템을 설치·운영하여야 한다”라고 규정하고 있고, 제6조제1항은 “정보통신서비스 제공자등은 비밀번호가 복호화 되지 아니하도록 일방향 암호화 하여 저장해야 한다.” 라고 규정하고 있다.

나. 舊 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), 정보통신 서비스 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

2) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2022. 10. 20. 시행
3) 개인정보보호위원회고시 제2021-3호, 2021. 9. 15. 시행

바에 따라 통지를 갈음하는 조치를 취할 수 있다.”라고 규정하고 있다.

舊 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

가. 개인정보처리시스템에 대한 안전조치 의무를 소홀히 한 사실

[舊 보호법 제29조(안전조치의무)]

피심인이 ’14. 3. 1. ~ ’23. 6. 13. 동안 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하는 경우 ID, 비밀번호 외 안전한 인증수단을 적용하지 않고 운영한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제4항을 위반한 것이다.

피심인이 오픈소스 웹 방화벽( )을 사용하면서 신규 위협 대응 등을 위하여 접근 제한 및 유출 탐지 정책을 지속적으로 업데이트하지 않고, 인가받지 않은 접근을 제한하기 위한 모니터링을 소홀히 하는 등 침입탐지·차단시스템 운영을 소홀히 한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제5항을 위반한 것이다.

피심인이 이용자의 비밀번호를 안전하지 않은 일방향 암호화 알고리즘인 MD5로 암호화하여 저장한 행위는 舊 보호법 제29조, 舊 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제6조제1항을 위반한 것이다.

나. 개인정보 유출 통지를 소홀히 한 사실

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

피심인이 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 이용자 대상 유출 통지를 한 행위는 舊 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(舊 기술적 보호조치 기준 등)
안전조치의무 위반	舊 보호법 §29	舊 시행령 §48의2①	• 외부에서 개인정보처리시스템에 접속하는 경우 안전한 인증수단을 적용하지 않은 행위 (舊 기술적 보호조치 기준§4④) • 불법적인 접근 및 침해사고 방지를 위한 개인정보 처리 시스템에 대한 침입 탐지·차단 시스템 운영을 소홀히 한 행위 (舊 기술적 보호조치 기준§4⑤) • 이용자의 비밀번호를 안전하게 저장하지 아니한 행위 (舊 기술적 보호조치 기준§6①)
개인정보 유출등의 통지·신고에 대한 특례 위반	舊 보호법 §39의4①	舊 시행령 §48조의4	• 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 통지한 행위

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4제1항(개인정보의 유출등의 통지·신고에 대한 특례) 위반행위에 대한 과태료는 같은 법 제75조제2항제6호·제12호의3, 舊 시행령 제63조, 舊 시행령 [별표2] '과태료의 부과기준' 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[4](이하 '과태료 부과기준')에 따라 다음과 같이 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

4) 개인정보보호위원회 지침, '23. 9. 15. 시행

가. 기준금액

舊 시행령 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 위반행위를 하여 적발된 날을 기준으로 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 각 위반행위별 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, 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 부과기준 제7조는 '사전통지 및 의견제출 결과와 가중기준(▲위반의 정도, ▲위반 기간, ▲조사 방해, ▲위반 주도)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다.'라고 규정하고 있다.

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대해서 ▲위반 기간이 2년을 초과하므로 기준금액의 30%를 가중하고, ▲위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상인 경우에 해당하므로 기준금액의 15%를 가중하여 총 45%를 가중하고, 舊 보호법 제39조의4제1항(개인정보 유출등의 통지·신고에 대한 특례) 위반행위는 가중 사유에 해당하지 않아 기준금액을 유지한다.

※ 위반기간 : '14. 3. 1. ~ '23. 6. 13.

※ 위반행위 : 舊 시행령 제48조의2제1항제2호(접근통제), 제4호(암호화)

2) (과태료의 감경) 과태료 부과기준 제6조는 '사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의 감경기준(▲당사자 환경, ▲위반정도, ▲업무형태 및 규모, ▲개인정보보호 노력 정도, ▲조사 협조 및 자진 시정 등)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있으며, 감경사유가 2개 이상 해당되는 경우에는 합산하여 감경하되 기준금액의 100분의 90을 초과할 수 없다.'라고 규정하고 있다.

피심인의 舊 보호법 제29조(안전조치의무) 및 같은 법 제39조의4제1항(개인정보 유출 등의 통지·신고에 대한 특례) 위반행위에 대해 ▲「중소기업기본법」 제2조에 따른 인 경우(30% 이내), ▲일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료를 제출 또는 진술하는 등 조사에 적극적으로 협력한 점(20% 이내), ▲사전통지 및 의견제출 기간 내에 위반행위를 시정 완료한 경우(20% 이내)인 점 등을 종합적으로 고려하여 과태료 부과기준 제6조에 따라 기준금액의 70%를 각각 감경한다.

다. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무) 및 같은 법 제39조의4(개인정보 유출 등의 통지·신고에 대한 특례)제1항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 630만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제, 암호화)	600만 원	270만 원	420만 원	**450만 원**
개인정보 유출등의 통지·신고에 대한 특례 위반 (통지 지연)	600만 원	-	420만 원	**180만 원**
계				**630만 원**

2. 결과 공표

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)' 및 '위반행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)'에 해당하므로, 과태료를 부과받은 사실에 대해 개인정보보호위원회 홈페이지에 공표한다. 다만, 개정된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침(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, 암호화)	2024. 9. 25.	과태료 450만 원
		舊 보호법* 제39조의4제1항	유출 통지·신고에 대한 특례 위반 (통지 지연)		과태료 180만 원

* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호

2024년 9월 25일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4제1항(개인정보 유출등의 통지·신고에 대한 특례) 위반행위에 대해 같은 법 제75조(과태료)제2항제6호·제12호의3, 제66조(결과의 공표)제1항에 따라 과태료 부과, 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

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.

2024년 9월 25일

위 원 장 김 진 욱 (서 명)

위 원 김 진 환 (서 명)

위 원 박 상 희 (서 명)