개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 제2024-221-668호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인

의결연월일 2024. 11. 4.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 8,700,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보처리시스템에 대한 접근통제, 이용자의 비밀번호 일방향 암호화 조치 등 보호법 제29조를 준수해야 한다.

나. 피심인은 舊 보호법 제39조의4제1항을 준수하여 이번 유출사고 피해 정보주체에게 법정고지사항을 통지하여야 한다.

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

이 유

Ⅰ. 기초 사실

피심인은 컴퓨터 관련 교육 강의 홈페이지( )를 운영하는 「舊 개인정보 보호법」[1](이하 '舊 보호법'이라 한다)에 따른 정보통신서비스 제공자이며, 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호	대표자 성명	주소	종업원 수 (명)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보 포털(privacy.go.kr)에 유출 신고('22. 12. 6.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('23. 3. 14. ~ '24. 5. 29.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 컴퓨터 관련 교육 강의 홈페이지( )를 운영하면서 '23. 3. 27. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

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

< 개인정보 수집현황 >

구분	항목	수집일*	건수
합 계			

나. 개인정보 유출 관련 사실관계

‘20. 11. 22. ~ ‘22. 12. 9. 동안 해커가 피심인이 운영중인 홈페이지를 대상으로 SQL 인젝션 공격(약 320만 회)을 통해 이용자의 개인정보를 유출하였다.

1) **(유출내용)** 최대 이용자 23,355명의 개인정보*가 유출되었을 가능성이 있으며, 유출 데이터를 확보하지 못해 정확한 유출 규모를 확인하지 못함

* 이메일, 비밀번호(평문)

2) **(유출 인지 및 대응)** 피심인은 유출 사실을 인지 후 24시간 이내에 유출 신고 및 홈페이지에 유출 사실을 게시하였으나, 정보주체에게 개별 통지하지 않았다.

일시		피심인의 유출 인지·대응 내용
‘22. 12. 6.	13:17	한국인터넷진흥원을 통해 개인정보 유출 관련 메일 수신 및 개인정보 **유출 인지**
‘22. 12. 6.	15:55	개인정보 **유출 신고**
‘22. 12. 8.	13:17	홈페이지 공지를 통한 개인정보 **유출 통지**(7일간)

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

피심인은 ‘22. 11. 23.부터 불법적인 접근 및 침해사고 방지를 위한 침입탐지·차단시스템 등을 설치하지 않고 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하지 않고 운영한 사실이 있다.

피심인은 ‘22. 11. 23.부터 SQL 쿼리와 같은 웹서버 입력값에 대한 검증과정이 없는 취약점에 대해 점검을 소홀히 한 사실이 있다.

또한, 피심인은 이용자의 비밀번호를 복호화 되지 아니하도록 안전한 방식으로 일방향 암호화하여 저장하지 않은 사실이 있다.

피심인은 심의일 현재까지 안전성 확보에 필요한 조치를 시정조치하지 않은 사실이 있다.

나. 개인정보 유출 통지를 소홀히 한 행위

피심인은 ‘22. 12. 6. 13:17 한국인터넷진흥원으로부터 유출 관련 메일을 수신하고 개인정보 유출을 인지하였으나, 정당한 사유 없이 이용자 대상 유출 통지하지 않은 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’24. 5. 30., 10. 15. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’24. 5. 30., 10. 15. 개인정보보호위원회에 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가.「개인정보 보호법」[2](이하 ’보호법‘) 제29조는 “개인정보처리자는 개인정보

가 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[3](이하 ‘시행령’이라 한다) 제30조제1항제3호는 “개인정보에 대한 접근을 통제하기 위해 ‘그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치(다목)’ 등을 하여야 한다.” 라고 규정하고 있으며, 제30조제1항4호는 “개인정보를 안전하게 저장하기 위해 ‘비밀번호의 일방향 암호화 저장 등 이에 상응하는 조치(가목)’를 하여야 한다.”,라고 규정하고 있다. 또한, 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)[4](이하 ‘안전성 확보조치 기준’이라 한다) 제6조제1항은 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한해야 하고(1호)’, ‘개인정보처리시스템에 접속한 IP 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응하여야 한다(2호)’.”라고 규정하고 있고, 제6조제3항은 “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 있으며, 제7조제1항은 “개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송ㆍ수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 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 조

2) 법률 제19234호, 2023. 3. 14., 일부개정, 2024. 3. 15. 시행
3) 대통령령 제34309호, 2024. 3. 12. 일부개정, 2024. 9. 15. 시행
4) 개인정보보호위원회고시 제2023-6호, 2023. 9. 22. 시행

치(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.

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. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[보호법 제29조(안전조치의무)]

피심인이 ‘22. 11. 23.부터 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하지 않고 운영한 행위, SQL 쿼리와 같은 웹서버 입력값에 대한 검증과정이 없는 취약점에 대해 점검을 소홀히 한 행위는 보호법 제29조, 시행령 제30조제1항, 안전성 확보 조치 기준 제6조제1항·제3항을 위반한 것이다.

또한, 피심인이 이용자의 비밀번호를 복호화 되지 아니하도록 안전한 방식으로 일방향 암호화하여 저장하지 않은 행위는 보호법 제29조, 보호법 제29조, 시행령 제30조제1항, 안전성 확보 조치 기준 제7조제1항을 위반한 것이다.

나. 개인정보 유출 통지를 소홀히 한 행위

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

피심인은 '22. 12. 6. 13:17 한국인터넷진흥원으로부터 유출 관련 메일을 수신하고 개인정보 유출을 인지하였으나, 정당한 사유 없이 이용자 대상 유출 통지하지 않은 행위는 舊 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	舊 시행령	세부내용(고시 등)
안전조치의무	보호법 §29	시행령 §30①	・개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하지 않고 운영한 행위 (안전성 확보조치 기준§6①) ・열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위 (안전성 확보조치 기준§6③) ・비밀번호를 복호화되지 않도록 안전하게 일방향 암호화하여 저장·보관하지 않은 행위 (안전성 확보조치 기준§7①)
개인정보 유출등의 통지·신고에 대한 특례	舊 보호법 §39의4①	舊 시행령 §48조의4	・유출 사실을 인지하였으나 정당한 사유 없이 이용자에게 유출 통지하지 않은 행위

Ⅳ. 처분 및 결정

1. 과태료 부과

가. 보호법 제29조 안전조치의무 위반 관련

피심인의 보호법 제29조(안전조치의무) 위반행위에 대한 과태료는 보호법 제75조제2항5호, 시행령 제63조 및 [별표2] '과태료의 부과기준'을, 및 「개인정보 보호법 위반에 대한 과태료 부과기준」[5](이하 '과태료 부과기준')에 따라 다음과 같이 부과한다.

5) 개인정보보호위원회 지침, '23. 9. 15. 시행

1) 기준금액

시행령 [별표2] 및 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.

< 시행령 [별표2] 2. 개별기준 >

(단위: 만 원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액		
		1회	2회	3회 이상
아. 법 제23조제2항·제24조제3항·제25조제6항(법 제25조의2제4항에 따라 준용되는 경우를 포함한다)·제28조의4제1항·**제29조**(법 제26조제8항에 따라 준용되는 경우를 포함한다)**를 위반**하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제5호	600	1,200	2,400

2) 과태료의 가중 및 감경

가) 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 보호법 제29조(안전조치의무) 위반행위에 대해서 ▲위반행위별 각 목의 세부기준에서 정한 행위가 2개 이상인 경우에 해당하므로 기준금액의 15%를 가중하고, ▲법 위반상태의 기간이 1년을 초과하고 2년 미만인 경우에 해당하므로 기준금액의 15%를 가중하여, 기준금액의 30%를 가중한다.

※ 위반기간 : '22.11.23. ~ 진행중
※ 위반행위 : 시행령 제30조제1항제3호(접근통제), 제4호(암호화)

나) 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 노력정도, ▲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 경우, ▲「중소기업기본법」제2조에 따른 소기업(小企業)인 경우, ▲ 일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료를 제출 또는 진술하는 등 조사에 적극적으로 협력한 점 등을 종합적으로 고려하여 과태료 부과기준 제6조에 따라 기준금액의 50%를 감경한다.

3) 최종 과태료

피심인의 보호법 제29조(안전조치의무) 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 480만 원의 과태료를 부과한다.

나. 舊 보호법 제39조의4제1항 유출등의 통지·신고에 대한 특례 위반 관련

피심인의 舊 보호법 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항 위반행위에 대한 과태료는 같은 법 제75제2항제12호의3, 舊 시행령 제63조, [별표2] '과태료의 부과기준' 및 과태료 부과기준에 따라 다음과 같이 부과한다.

1) 기준금액

舊 시행령 [별표2] 및 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 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
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

2) 과태료의 가중 및 감경

가) 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 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항 위반행위에 대해서 ▲법 위반상태의 기간이 1년을 초과하고 2년 미만인 경우에 해당하므로 기준금액의 15%를 가중한다.

※ 위반기간 : '22.12.6. ~ 진행중

나) 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 노력정도, ▲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 경우, ▲「중소기업기본법」제2조에 따른 소기업(小企業)인 경우, ▲일관되게 행위 사실을 인정하면서 위법성 판단에 도움 되는 자료를 제출 또는 진술하는 등 조사에 적극적으로 협력한 점 등을 종합적으로 고려하여 과태료 부

과기준 제6조에 따라 기준금액의 50%를 감경한다.

3) 최종 과태료

피심인의 舊 보호법 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 390만 원의 과태료를 부과한다.

다. 최종 과태료

피심인의 보호법 제29조(안전조치의무) 및 舊 보호법 제39조의4(개인정보 유출등의 통지 · 신고에 대한 특례)제1항 위반행위에 대해 기준금액에서 가중·감경을 거쳐 총 870만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제, 암호화)	600만원	180만원	300만원	**480만원**
개인정보 유출등의 통지·신고에 대한 특례 (유출 통지)	600만원	90만원	300만원	**390만원**
합 계				**870만원**

2. 시정조치 명령

가. 피심인의 보호법 제29조(안전조치의무) 및 舊 보호법 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항 위반에 대해 피심인에 대하여 다음과 같이 시정조치를 명한다.

1) 피심인은 개인정보처리시스템에 대한 접근통제, 이용자의 비밀번호 일방향 암호화 조치 등 보호법 제29조를 준수할 것

2) 피심인은 舊 보호법 제39조의4제1항을 준수하여 이번 유출사고 피해 정보주체에게 법정고지사항을 통지할 것

나. 피심인은 1)부터 2)까지의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출할 것

Ⅴ. 결론

피심인의 보호법 제29조(안전조치의무), 舊 보호법 제39조의4제1항(개인정보 유출등의 통지·신고에 대한 특례) 위반행위에 대해 보호법 제64조(시정조치 등) 제1항, 제75조(과태료)제2항제5호 및 舊 보호법 제75조(과태료)제12호의3에따라 시정조치 명령, 과태료 부과를 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.

피심인은 이 시정조치 명령에 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.

2024년 11월 4일

위 원 장 이 문 한 (서 명)

위 원 박 상 희 (서 명)

위 원 조 소 영 (서 명)