개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2022-019-156호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인

의결연월일 2022. 11. 30.

주 문

1. 피심인에 대하여 다음과 같이 시정조치를 명한다.

   가. 피심인은 개인정보의 유출 사실을 안 때에는 지체 없이 유출된 개인정보 항목, 유출이 발생한 시점, 이용자가 취할 수 있는 조치, 정보통신서비스 제공자등의 대응 조치, 이용자가 상담 등을 접수할 수 있는 부서 및 연락처 등을 해당 이용자에게 알려야 한다.

   나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 8,400,000원

   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

문자발송 서비스( )를 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)

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 개인정보종합포털(privacy.go.kr)에 유출 신고('21. 6. 18.)한 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사('21. 6. 28. ~ '22. 6. 7.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 문자발송 서비스를 운영하면서 '21. 7. 8. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수
회원 정보	(필수) 이름, 아이디, 비밀번호, 생년월일, 이메일, 휴대전화번호 (선택) 주소	'10. 12. 7. ~ '21. 7. 8.	
합 계			

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출 인지·대응 내용
’21. 5. 8.	11:36	신원미상의 자(이하, 해커)의 1차 스팸문자 발송
’21. 5. 9.	18:05	해커의 2차 스팸문자 발송
’21. 6. 18.	10:35	개인정보보호포털에 개인정보 유출 신고
’22. 4. 26. ~ 4. 27.	-	일부 이용자(18개 계정)에게 유출 통지

2) 유출규모 및 경위

(유출항목 및 규모) 문자발송 서비스 이용자 48명의 아이디·비밀번호가 유출된 것으로 추정된다.

(유출 경위) 해커는 ’21. 5. 6.부터 ’21. 5. 9.까지 SQL 인젝션 공격을 하여 피심인이 운영하는 문자발송 서비스의 이용자 계정정보를 탈취한 후, 스팸문자(약 29만건)를 발송하였다.

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

1) 피심인은 ’10. 12. 7.부터 ’22. 5. 23.까지 불법적인 개인정보 유출 시도를 탐지하기 위한 IDS, IPS 등과 같은 보안 장비를 설치·운영하지 않았으며, ’10. 12. 7.부터 ’21. 6. 14.까지 해커가 입력한 SQL 쿼리와 같은 입력값에 대한 검증과정을 마련하지 않은 사실이 있다.

2) 피심인은 ’10. 12. 7.부터 ’22. 4. 20.까지 개인정보취급자가 개인정보처리시스템에 접속한 기록 중 식별자와 수행업무를 보존하지 않은 사실이 있다.

3) 피심인은 ’10. 12. 7.부터 ’21. 6. 21.까지 비밀번호를 안전하지 않은 MD5 알고리듬으로 암호화하여 저장한 사실이 있다.

나. 유출 통지·신고를 소홀히 한 행위

피심인은 유출된 계정 48개 중 30개 계정 이용자에게 유출 통지를 하지 않았으며, 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 신고한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 ’22. 6. 8. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 ’22. 6. 29. 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 위하여 ‘침입차단시스템 및 침입탐지시스템의 설치·운영(나목)’, ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제48조의2제1항제3호는 “접속기록의 위조·변조 방지를 위하여 ‘개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등을 저장 및 이의 확인·감독(가목)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령 제48조의2제1항제4호는 “개인정보가 안전하게 저장 · 전송될 수 있도록 비밀번호의 일방향 암호화 저장(나목)을 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 제2020-5호, 이하 ‘고시’) 제4조제5항제2호는 “정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지할 수 있는 시스템을 설치·운영하여야 한다.”라고 규정하고 있고, 고시 제4조제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있다.

고시 제5조제1항은 “정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존.관리하여야 한다.” 라고 규정하고 있다.

고시 제6조제1항은 “정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.”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.

2. 위법성 판단

가. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위{보호법 제29조 (안전조치의무)}

피심인이 피심인은 불법적인 개인정보 유출 시도를 탐지하기 위한 IDS, IPS 등과 같은 보안 장비를 설치·운영하지 않고, 해커가 입력한 SQL 쿼리와 같은 입력값에 대한 검증과정을 마련하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2 제1항제2호, 고시 제4조제5항·제9항을 위반한 것이다.

피심인이 접속기록을 1년 이상 보존·관리하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제3호, 고시 제5조제1항을 위반한 것이다.

피심인이 비밀번호를 안전하지 않은 MD5 알고리듬으로 암호화하여 저장한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제4호, 고시 제6조제1항을 위반한 것이다.

나. 유출 통지·신고를 소홀히 한 행위{보호법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항}

피심인이 유출된 계정 48개 중 30개 계정 이용자에게 유출 통지를 하지 않고, 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 신고한 행위는 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반	보호법 §29	§48의2① 제2호·제3호·제4호	• 침입 차단·탐지시스템을 설치·운영하지 않은 행위(고시§4⑤) • 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위(고시§4⑨) • 개인정보취급자의 개인정보처리시스템의 접속기록을 보관하지 않은 행위(고시§5①) • 비밀번호를 복호화되지 아니하도록 일방향 암호화하여 저장하지 않은 행위(고시§6①)

개인정보 유출등의 통지·신고에 대한 특례 위반	보호법 §39의4①	-	• 유출 통지를 하지 않고, 정당한 사유 없이 유출 사실을 안 때부터 24시간을 경과하여 신고한 행위

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보의 유출 사실을 안 때에는 지체 없이 유출된 개인정보 항목, 유출이 발생한 시점, 이용자가 취할 수 있는 조치, 정보통신서비스 제공자 등의 대응 조치, 이용자가 상담 등을 접수할 수 있는 부서 및 연락처 등을 해당 이용자에게 알려야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

2. 과태료 부과

피심인의 보호법 제29조(안전조치의무) 및 같은 법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대하여 같은 법 제75조제2항제6호·제12호의3, 같은 법 시행령 제63조, 같은 법 시행령 [별표2] '과태료의 부과기준' 및 '개인정보 보호법 위반에 대한 과태료 부과기준'(2021. 1. 27. 개인정보보호위원회 의결, 이하 '과태료 부과지침')에 따라 다음과 같이 과태료를 부과한다.

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 각 위반행위별 기준 금액을 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, 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위는 '제3호 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상에 해당하는 경우' 및 '법 위반행위의 상태가 3개월 이상인 경우'에 해당하여 기준금액의 20%를 가중하고, 유출 통지·신고를 소홀히 한 행위는 '제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우' 및 '법 위반행위의 상태가 3개월 이상인 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, 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위는 ‘위반행위에 대해 시정을 완료한 경우’, ‘조사에 적극 협력한 경우’ 및 ‘「중소기업기본법」 제2조에 따른 소기업인 경우’에 해당하여 기준금액의 50%를 감경하고, 유출 통지·신고를 소홀히 한 행위는 ‘조사에 적극 협력한 경우’ 및 ‘「중소기업기본법」 제2조에 따른 소기업인 경우’에 해당하여 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조 및 같은 법 제39조의4제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 840만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제, 접속기록, 암호화)	600만원	120만원	300만원	**420만원**
개인정보 유출등의 통지·신고에 대한 특례 위반	600만원	120만원	300만원	**420만원**
계				**840만원**

3. 결과 공표

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), 위반행위 기간이 6개월 이상 지속된 경우(제5호)에 해당하므로 보호법 제66조제1항에 따라 피심인이 시정조치 명령을 받은 사실과 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다.

개인정보보호법 위반 행정처분 결과 공표				
위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	위반조항	위반내용	처분일자	처분내용
	법 제29조	안전조치의무 위반	2022.11.30	과태료 부과 420만원
	법 제39조의4제1항	유출 통지·신고에 대한 특례 위반	2022.11.30	시정조치 명령 과태료 부과 420만원

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 제64조(시정조치 등)제1항 및 같은 법 제66조(결과의 공표) 제1항에 따라 과태료, 시정조치 명령 및 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 시정명령 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.

2022년 11월 30일

부위원장 최 장 혁 (서 명)

위 원 강 정 화 (서 명)

위 원 고 성 학 (서 명)

위 원 백 대 용 (서 명)

위 원 서 종 식 (서 명)

위 원 염 흥 열 (서 명)

위 원 이 희 정 (서 명)

위 원 지 성 우 (서 명)