개 인 정 보 보 호 위 원 회

심의·의결

안 건 번 호 제2022-018-153호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

의결연월일 2022. 11. 16.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체없이 ‘유출등이 된 개인정보 항목’, ‘유출등이 발생한 시점’, ‘이용자가 취할 수 있는 조치’, ‘정보통신서비스 제공자등의 대응조치’, ‘이용자 상담 등을 접수할 수 있는 부서 및 연락처’의 사항을 해당 이용자에게 알려야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.

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

2. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 7,800,000원

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

피심인은 사업자 전용(B2B) 문자발송 웹사이트를 운영하는「개인정보 보호법」(2020. 8. 5. 시행, 법률 제16930호, 이하 '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

개인정보보호위원회는 피심인이 신원 미상자(이하 '해커'라 한다)에 의한 이용자 계정 탈취 사실을 인지하고 유출신고(2021. 12. 22.)함에 따라 피심인에 대하여 개인정보 취급·운영 실태 및 보호법 위반 여부를 조사(2022. 4. 8. ~ 2022. 7. 8.)하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 사업자 전용(B2B) 문자발송 웹사이트를 운영하면서 '22. 6. 23. 기준 건의 이용자 정보를 수집하여 보관하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수(건)
회원정보	(필수) 아이디, 비밀번호, 이메일, 이름(계정명) (선택) 전화번호(휴대폰번호)		

나. 개인정보 유출 경위

1) 유출 경과 및 대응

일시		피심인의 유출인지·대응 내용
'21. 12. 9.	16:00	KISA로부터 '스팸문자 신고' 관련 이메일 수신 후, 해당 내용 파악 중 해킹에 의한 유출 사실 인지
'21. 12. 10.	09:33	개인정보 유출 사실 홈페이지 게시
	15:30 ~16:00	일부 이용자(4명)에게 스팸문자 발송에 따른 피해복구 방안 이메일 발송
'21. 12. 22.	15:53	개인정보보호 포털에 개인정보 유출 신고

2) 유출규모 및 경위

(유출항목 및 규모) 이용자 9명의 개인정보*

* 아이디, 비밀번호, 이메일, 이름(계정명), 전화번호(휴대폰번호)

(유출경위) 해커는 피심인의 문자발송 홈페이지( ) 디렉터리 접근 설정 취약점*을 이용하여, 웹서버에 접속하고 데이터베이스 연동 설정파일 등을 다운로드**한 후 이용자 계정을 탈취함

* 디렉터리 접근 공격 : 웹브라우저를 이용해 웹서버의 파일 목록과 파일에 접근할 수 있는 취약점

**

- '21. 12. 6. 00:29 : 해커가 디렉터리 접근 공격으로 ' ' 홈페이지 웹서버(이하 '사고서버')의 파일( )을 다운로드함

- '21. 12. 6. 00:35 : 해커는 SSH*를 통해 사고서버에 ' ' 계정으로 접속 성공함

* SSH(Secure Shell) : 원격 서버(호스트)에 접속하기 위해 사용되는 보안 프로토콜

- '21. 12. 6. 00:58 : 해커는 디렉터리 접근 공격으로 사고서버에서 데이터베이스 연동정보가 저장되어 있는 ' ' 파일을 다운로드함

- '21. 12. 6. 02:15 : 해커는 사고서버에 등 웹셸 파일을 생성하여 실행하였고, 이를 통해 데이터베이스 내 계정정보를 탈취한 것으로 추정

- '21. 12. 7. 09:29~ : 해커는 이용자 계정 9개에 로그인 성공하였으며, 이 중 6개 계정을 통해 스팸문자(약 97만 건)를 발송함

3. 개인정보의 취급.운영 관련 사실관계

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 정보통신망을 통해 외부에서 개인정보처리시스템(웹서버)에 접속 시 안전한 인증수단을 적용하지 않고 아이디·비밀번호만으로 접속하도록 하거나 접속 권한을 아이피(IP) 주소 등으로 제한하지 않았고, 웹사이트 취약점 점검 등 보안 조치를 하지 않아 해커의 디렉터리 접근 공격을 허용하여 이용자의 개인정보가 유출된 사실이 있다.

나. 개인정보처리시스템의 접속기록 보관을 소홀히 한 행위

피심인은 홈페이지 최초 개발 시부터 데이터베이스 서버 접속기록을 최소 1년 이상 저장·관리하지 않고 운영한 사실이 있다.

다. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위

피심인은 이용자의 비밀번호를 보안 강도가 낮은 SHA-1으로 암호화하여 저장한 사실이 있다.

라. 개인정보 유출통지 및 유출신고를 소홀히 한 행위

피심인은 이용자에게 유출 사실을 통지하지 않고, 정당한 사유 없이 24시간을 경과하여 유출 사실을 신고한 사실이 있다.

※ 피심인은 유출 사실을 인지(2021. 12. 9.)하고 홈페이지에 유출 사실을 공지하였으나, 유출된 이용자(9개 계정)에 대해 유출 사실을 통지하지 않았으며(일부 이용자에게 문자 발송 비용 미청구 메일만 발송), 2021. 12. 22.에 유출 신고함

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022. 7. 13. 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2022. 7. 22. 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 저장ㆍ전송될 수 있도록 ‘비밀번호의 일방향 암호화 저장(가목)’ 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'라 한다) 제4조제4항은 "개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다."라고 규정하고 있고, 제4조제5항은 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)'하는 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있다. 또한, 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.

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 복호화되지 아니하도록 일방향 암호화하여 저장한다."라고 규정하고 있다.

'고시 해설서'는 고시 제6조제1항에 대해 비밀번호를 암호화 할 때에는 국내.외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호 알고리듬으로 암호화하여 저장하도록 하고, MD5, SHA-1 등 보안 강도가 낮은 것으로 판명된 암호 알고리듬을 사용하여서는 안된다고 해설하고 있다.

나. 보호법 제39조의4제1항은 "정보통신서비스 제공자등은 개인정보의 유출등 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)'의 사항을 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

가. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위[보호법 제29조(안전조치의무) 중 접근통제]

1) (안전한 인증수단 및 침입차단·탐지시스템 운영) 피심인이 외부에서 개인정보처리시스템에 접속 시 안전한 인증수단을 적용하지 않고 아이디·비밀번호만으로 접속하도록 하거나, 개인정보처리시스템에 대한 접속 권한을 아이피(IP) 주소 등으로 제한하지 않고 외부 인터넷 어디서나 접속할 수 있도록 운영한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제4항·제5항을 위반한 것이다.

2) (개인정보 유·노출 방지) 피심인이 인터넷 홈페이지를 통한 개인정보 유출을 방지하기 위해 보안기술 적용 등 조치를 취하여야 하나, 웹 취약점 점검 등 보안 조치를 하지 않아 해커의 공격을 허용한 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 고시 제4조제9항을 위반한 것이다.

나. 개인정보처리시스템의 접속기록 보관을 소홀히 한 행위[보호법 제29조(안전조치의무) 중 접속기록의 위조ㆍ변조 방지]

피심인이 개인정보가 저장되는 데이터베이스 서버에 접속하는 개인정보취급자의 접속기록을 최소 1년 이상 보존·관리하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제3호, 고시 제5조제1항을 위반한 것이다.

다. 개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위[보호법 제29조(안전조치의무) 중 개인정보의 암호화]

피심인이 이용자의 비밀번호를 복호화되지 아니하도록 일방향 암호화하여 저장하지 않은 행위는 보호법 제29조, 같은 법 시행령 제48조의2제1항제4호, 고시 제6조제1항을 위반한 것이다.

라. 개인정보 유출통지 및 유출신고를 소홀히 한 행위[보호법 제39조의4(개인정보 유출등의 통지ㆍ신고에 대한 특례)제1항]

피심인이 개인정보가 유출된 이용자 대상 별도의 유출통지를 하지 않고, 정당한 사유 없이 24시간을 경과하여 유출 사실을 신고한 행위는 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	시행령	세부내용(고시 등)
안전조치의무 위반 (접근통제, 접속기록, 암호화)	보호법 §29	§48조의2① 제2·3·4호	・개인정보처리시스템에 대한 접근통제를 소홀히 한 행위(고시§4④,⑤,⑨) ・개인정보처리시스템의 접속기록 보존·관리를 소홀히 한 행위(고시§5①) ・개인정보의 암호화기술 등을 이용한 보안조치를 소홀히 한 행위(고시§6①)
개인정보 유출 통지・신고 위반	보호법 §39조의4①	§48조의4	・개인정보 유출통지 및 유출신고를 소홀히 한 행위

Ⅳ. 처분 및 결정

1. 시정조치 명령

가. 피심인은 개인정보의 유출등 사실을 안 때에는 지체 없이 '유출등이 된 개인정보 항목', '유출등이 발생한 시점', '이용자가 취할 수 있는 조치', '정보통신서비스 제공자등의 대응조치', '이용자가 상담 등을 접수할 수 있는 부서 및 연락처'의 사항을 해당 이용자에게 알려야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.

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, 제39조의4제1항 위반행위에 대한 과태료는 같은 법 제75조(과태료)제2항제6호·제12호의3, 같은 법 시행령 제63조의 [별표2] '과태료 부과기준' 및「개인정보 보호법 위반에 대한 과태료 부과기준(2021. 1. 27. 개인정보보호위원회 의결, 이하 '과태료 부과기준'이라 한다)」에 따라 다음과 같이 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 1회 위반에 해당하는 과태료인 600만원을 각각 적용한다.

< 「보호법」 시행령 [별표2] 2. 개별기준 >

(단위:만원)

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4 제1항 또는 **제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우**	법 제75조 제2항제6호	600	1,200	2,400
도. 법 **제39조의4제1항**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 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 '안전성 확보에 필요한 조치를 하지 않은 행위'에 대하여 법 위반상태의 기간이 3개월 이상인 경우 및 위반행위별 각 목의 세부기준에서 정한 행위가 3개 이상인 경우에 해당하여 기준금액의 20%를 가중하고, '이용자에게 유출통지를 하지 않고 정당한 사유 없이 24시간을 경과하여 유출 신고한 행위'에 대하여 법 위반상태의 기간이 3개월 이상인 경우에 해당하여 기준금액의 10%를 가중한다.

2) **(과태료의 감경)** 과태료 부과기준 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 '안전성 확보에 필요한 조치를 하지 않은 행위'에 대하여 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위에 대한 시정을 완료한 점, 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 점, 사업규모가 「중소기업기본법」에 따른 중기업(中企業)인 점을 고려하여 기준금액의 50%를 감경하고, '이용자에게 유출통지를 하지 않고 정당한 사유 없이 24시간을 경과하여 유출 신고한 행위'에 대하여 조사기간 중에 일관되게 행위사실을 인정하면서 위법성 판단에 도움이 되는 자료를 제출하거나 진술하는 등 조사에 적극 협력한 점, 사업규모가 「중소기업기본법」에 따른 중기업(中企業)인 점을 고려하여 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 보호법 제29조, 제39조의4제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 780만원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 위반 (접근통제, 접속기록, 암호화)	600만원	120만원	300만원	**420만원**
개인정보 유출 통지·신고 위반	600만원	60만원	300만원	**360만원**
계				**780만원**

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 시점을 기준으로 위반 상태가 6개월 이상 지속된 경우(제5호)에 해당하므로, 피심인이 시정조치 명령을 받은 사실과 피심인에 대한 과태료 부과 사실에 대해 개인정보보호위원회 홈페이지에 공표한다.

<table>
<tr><td colspan="5">개인정보보호법 위반 행정처분 결과 공표
개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.</td></tr>
<tr><td>위반행위를 한 자</td><td colspan="2">위반행위의 내용</td><td colspan="2">행정처분의 내용 및 결과</td></tr>
<tr><td>명칭</td><td>위반조항</td><td>위반내용</td><td>처분일자</td><td>처분내용</td></tr>
<tr><td rowspan="2"></td><td>법 제29조</td><td>안전조치의무</td><td rowspan="2">2022.11.16.</td><td>과태료 부과 420만원</td></tr>
<tr><td>법 제39조의4 제1항</td><td>개인정보 유출등의 통지·신고에 대한 특례</td><td>시정조치 명령
과태료 부과 360만원</td></tr>
</table>

Ⅴ. 결론

피심인의 보호법 제29조, 제39조의4제1항 위반행위에 대하여 같은 법 제75조(과태료) 제2항 제6호·제12호의3, 제64조(시정조치 등)제1항, 제66조(결과의 공표)제1항에 따라 과태료, 시정조치 명령, 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 16일

위 원 장　　고 학 수　(서 명)

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)