개 인 정 보 보 호 위 원 회

심의・의결

안건번호 제2022-005-017호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 ㈜하우빌드
서울특별시 강남구

의결연월일 2022. 3. 23.

주 문

1. 피심인에 대하여 다음과 같이 시정조치를 명한다.

   가.「개인정보 보호법」 제24조의2(주민등록번호 처리의 제한)제1항을 준수할 것
   나. 법률 등에 근거 없이 수집·저장·보유한 주민등록번호를 지체 없이 파기할 것
   다. 위 가·나의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출할 것

2. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

   가. 과 징 금 : 5,900,000원
   나. 과 태 료 : 9,000,000원
   다. 납부기한 : 고지서에 명시된 납부기한 이내
   라. 납부장소 : 한국은행 국고수납 대리점

3. 피심인의 법 위반행위에 따른 행정처분의 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 피심인의 일반 현황

피심인은 영리를 목적으로 정보통신망을 통해 서비스를 제공하는 「개인정보 보호법」(법률 제16930호, 이하 “보호법”이라 함) 제18조제2항에 규정된 정보통신서비스 제공자이며 일반현황은 다음과 같다.

< 피심인의 일반현황 >

사업자등록번호 (법인등록번호)	대표자 성명	주 소	상시 종업원 수

Ⅱ. 사실조사 결과

개인정보보호위원회는 2021.11월 개인정보보호 포털에 유출 신고가 접수된 건과 관련하여 현장조사 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 유출 경위

가. 유출 경로 및 규모

피심인이 자사 서비스를 운영하기 위해 이용하는 아마존 클라우드서비스(AWS) 관리자 접근권한(Access Key)을 미상의 해커가 탈취하여 AWS내 개인정보 DB를 전체 삭제하고, 스캔문서 파일 내 이용자의 개인정보* 건(중복포함)을 다크웹에 유출하였다.

* 이름, 생년월일, 주민등록번호(평문), 계좌번호(평문), 휴대폰번호, 주소, 이메일 등

나. 경과 및 대응

일 시		유출 인지·대응
2021.11.10.	10:00	이상징후 발견후 에서 AWS 저장소 의 모든 파일이 다운로드 된 후 삭제됨을 확인
2021.11.10. ~		탈취된 AWS Access Key 폐기, 변경, 취약점 보완
2021.11.11.	09:55	개인정보보호포털에 개인정보 유출 신고
	09:56	정보주체에게 개인정보 유출 통지 (이메일, 휴대폰)
2021.11.24.	04:15	다크웹에 개인정보 업로드됨

2. 개인정보보호 법규 위반 행위 사실

가. 법률 등에 근거 없이 주민등록번호를 수집한 행위

피심인은 법률 등에 근거 없이 등에 포함된 주민등록번호(건)를 수집하였다.

나. 개인정보처리시스템에 대한 접근통제를 소홀히 한 행위

피심인은 개인정보처리시스템을 관리·운영할 수 있는 AWS 접근권한(Access Key)을 개인정보취급자에게 허용된 IP로 제한하거나 안전한 인증수단을 적용하지 않았다.

다. 개인정보처리시스템에 접속한 기록 보관을 소홀히 한 행위

피심인은 이용자의 개인정보를 DB에 저장하면서 개인정보취급자의 접속기록(식별자, 접속일시, 접속지, 수행업무 등)을 1년 이상 보관하지 않았다.

라. 개인정보의 암호화 조치를 소홀히 한 행위

피심인은 주민등록번호(건)와 계좌번호(건)가 포함된 문서 스캔 파일을 암호화하지 않은 채 DB에 저장하였다.

3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2022.2.18. ‘개인정보보호 법규 위반 행정처분 사전통지’

공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 2022.3.3. 피심인은 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 법률 등에 근거 없이 주민등록번호를 수집한 행위

가. 관련 법령의 규정

보호법 제24조의2제1항은 “제24조제1항에도 불구하고 개인정보처리자는 다음 각 호*의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다”라고 규정하고 있다.

* 1호. 법률 · 대통령령 · 국회규칙 · 대법원규칙 · 헌법재판소규칙 · 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우

2호. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우

3호. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

나. 위법성 판단

피심인이 법률 등에 근거 없이 이용자의 주민등록번호 건을 수집하여 저장·보유한 것은 보호법 제24조의2제1항 위반에 해당한다.

2. 안전성 확보 조치를 소홀히 한 행위

가. 관련 법령의 규정

보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”라고 규정하고 있고,

같은 법 시행령 제48조의2제1항은 정보통신서비스 제공자는 이용자의 개인정보를 처리하는 경우에는 제30조에도 불구하고 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 하고, 개인정보에 대한 불법적인 접근을 차단하기 위한 접근

통제를 위하여 필요한 조치(제2호), 접속기록의 위조·변조 방지를 위해 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(제3호), 개인정보가 안전하게 저장·전송될 수 있도록 주민등록번호, 계좌번호 등 보호위원회가 정하여 고시하는 정보의 암호화 저장(제4호) 등을 해야 한다고 규정하고 있다.

「개인정보의 기술적·관리적 보호조치 기준」(고시 제2020-5호) 제4조제5항에서 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하는 기능을 포함한 시스템을 설치·운영하여야" 하고, 제5조제1항에서 "개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야" 하고, 제6조제2항에서 "주민등록번호, 계좌번호 등 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장해야 한다"라고 규정하고 있다.

나. 위법성 판단

피심인이 AWS 접근권한을 개인정보취급자에게 허용된 IP로 제한하지 않고 외부 인터넷 어디서나 접속 가능하도록 운영하고, 개인정보취급자가 접속한 기록을 1년 이상 보존·관리하지 않고, 이용자의 주민등록번호, 계좌번호를 안전한 암호알고리즘으로 암호화 저장하지 않은 것은 보호법 제29조 위반에 해당한다.

Ⅳ. 처분 및 결정

1. 시정명령

피심인의 보호법 제24조의2제1항 위반에 대해 제64조제1항에 따라 다음과 같이 시정조치를 명한다.

가.「개인정보 보호법」제24조의2(주민등록번호 처리의 제한)제1항을 준수할 것

나. 법률 등에 근거 없이 수집·저장·보유한 주민등록번호를 지체 없이 파기할 것

다. 위 가·나의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행결과를 개인정보보호위원회에 제출할 것

2. 과징금 부과

이용자의 개인정보가 유출된 경우로서 안전성 확보조치를 하지 아니한 피심인의 제39조의15제1항제5호 행위에 대해 같은 법 제39조의15제4항, 같은 법 시행령 제48조의11제1항 및 제4항 [별표 1의5],「개인정보보호 법규 위반에 대한 과징금 부과기준」(고시 제2020-6호, 이하 '과징금 부과기준')에 따라 **590만원의 과징금을 부과한다.**

가. 관련 매출액 산정

피심인의 위반행위와 관련한 매출액은 유출 사고가 발생한 온라인 서비스의 직전 3개 사업연도의 연평균 매출액이므로 **천원**으로 산정한다.

< 피심인의 위반행위 매출액 >

(단위 : 천원)

구 분	2018년	2019년	2020년	평 균

※ 자료 출처 : 피심인이 제출한 재무제표 등 회계자료

나. 기준금액 산정

피심인의 위반행위는 미상의 해커에 의해 다크웹에 개인정보가 유출되었으므로 이용자의 개인정보가 공중에 노출된 경우로서 과징금 부과기준 제5조를 적용하여 '중대한 위반행위'로 보아 관련 매출액에 부과기준율 1천분의 21을 곱하여 **기준금액을 천원으로 산정**한다.

다. 필수적 가중·감경

과징금 부과기준 제6조에 따라 위반기간이 1년 이내인 경우라서 가중없이 기준금액을 유지하고, 최근 3년간 과징금 처분을 받은 적이 없으므로 기준금액의 50%인 **천원을 감경**한다.

라. 추가적 가중·감경

과징금 부과기준 제8조에 따라 특별히 가중할 사유는 없고, 피심인이 조사에 적극 협력한 점, 개인정보 유출사실을 자진 신고한 점을 고려하여 필수적 가중·감경을 거친 금액의 30%인 **천원을 감경**한다.

마. 최종 과징금

피심인에게 590만원의 과징금을 부과한다.

< 최종 과징금 산출내역 >

사업자명	기준금액	필수적 가중·감경	추가적 가중·감경	최종 과징금
㈜하우빌드		① 기준금액 유지(단기위반) ② 기준금액의 50% 감경 (최초위반 : 천원 감경)	필수적 가중·감경 거친 금액의 30% 감경 (천원 감경)	**590만원**

* 최종 과징금 산출액이 1억원 미만은 십만원 미만 절사, 1억원 이상은 백만원 미만 절사함

2. 과태료 부과

피심인의 보호법 제24조의2제1항 및 제29조 위반에 대해서 같은 법 제75조제2항 제4호의2·제6호, 같은 법 시행령 제63조의 [별표2]「과태료의 부과기준」에 따라 다음과 같이 **총 900만원의 과태료를 부과**한다.

가. 기준금액

피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 위반행위별 1회 위반에 해당하는 600만원(총 1,200만원)을 적용한다.

< 과태료 부과기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만원)		
		1회 위반	2회 위반	3회 이상 위반
자. 법 제24조의2제1항을 위반하여 주민등록번호를 처리한 경우	법 제75조 제2항제4호의2	**600**	1,200	2,400
자. 법 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	**600**	1,200	2,400
계		**1,200**		

나. 과태료의 가중

피심인의 제29조에 따른 안전성 확보에 필요한 조치 위반행위의 정도가 중대하여 과태료의 부과기준에 따라 기준금액(600만원)의 50%인 300만원을 가중한다.

* ①개인정보에 대한 불법적인 접근 차단 미조치, ②접속기록 미보관, ③주민등록번호, 계좌번호 등 암호화 저장 미조치

다. 과태료의 감경

피심인의 위반행위는 사소한 부주의로 인한 것이며, 행위사실을 인정하면서 조사에 적극 협력한 점, 「중소기업기본법」제2조에 따른 소기업인 점 등을 고려하여 위반행위별 기준금액의 50%인 300만원(총 600만원)을 감경한다.

라. 최종 과태료

피심인의 보호법 제24조의2제1항 및 제29조 위반행위에 대해 총 900만원의 과태료를 부과한다.

< 최종 과태료 산출내역 >

위반조항	위반내용	과태료 금액 (단위 : 만원)			
		기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) =(A+B+C)
법 §24의2①	법률 등에 근거없이 주민등록번호를 처리함	600	-	△300	**300**
법 §29	안전성 확보에 필요한 조치를 하지 않음	600	300	△300	**600**
계		**1,200**	**300**	**△600**	**900**

3. 결과 공표

피심인의 위반행위가 보호법 제66조 및 같은 법 시행령 제61조에 해당함에 따라 처분결과를 다음과 같이 개인정보보호위원회 홈페이지에 공표한다.

「개인정보 보호법」 위반 행정처분 결과 공표					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용

Ⅴ. 결론

피심인의 보호법 제24조의2(주민등록번호 처리의 제한)제1항, 제29조(안전조치 의무) 위반행위에 대하여 같은 법 제39조의15(과징금의 부과 등에 대한 특례), 제75조(과태료) 제2항제4호의2·제6호, 제64조(시정조치 등), 제66조(결과의 공표) 제1항 각각에 의한 과징금·과태료 부과, 시정조치 명령, 결과공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 과징금 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 그 처분을 받은 날부터 90일 이내에 중앙행정심판위원회에 행정심판청구 또는 관할법원에 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(피심인 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

2022년 3월 23일

위 원 장　　윤 종 인　(서 명)

부위원장　　최 영 진　(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　　지 성 우　(서 명)