

# 개 인 정 보 보 호 위 원 회

## 심의 · 의결

안전번호 제2022-005-018호  
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건  
피 심 인 정보공업(주)  
인천 서구  
의결연월일 2022. 3. 23.

## 주 문

1. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 12,500,000원

나. 과 태 료 : 9,000,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

2. 피심인의 법 위반의 내용 및 처분 결과를 개인정보보호위원회 홈페이지에  
공표한다.

# 이 유

## I. 피심인의 일반 현황

피심인은 중소기업으로 「개인정보 보호법」(법률 제16930호, 이하 “보호법”이라 함) 제2조제5호에 따른 개인정보처리자이며 일반현황은 다음과 같다.

### < 피심인의 일반현황 >

대 표	설립일자	자본금	매출액('20년)	주요서비스	종업원 수

피심인은 (이하 “수탁사”라 함)과 홈페이지 유지·보수 계약을 체결하고 웹호스팅, 사이트 유지보수 업무를 위탁하였다.

## II. 사실조사 결과

개인정보보호위원회는 2021.6월 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

신원 미상자가 SQL 인젝션\*을 통해 데이터베이스(DB)에 접속하여 개인정보를 조회하였고, 입사지원자, 협력사, 고객 등의 성명, 전화번호, 이메일주소, 주민등록번호 등 개인정보 건을 텔레그램에 유출하였다.

\* SQL 인젝션(Structured Query Language Injection) : DB에 대한 질의값을 조작해 해커가 원하는 자료를 DB로부터 유출하는 공격 기법

## **나. 경과 및 대응**

- '21.5.24. 한국인터넷진흥원(KISA)으로부터 텔레그램에 개인정보가 게재된 사실을 통보받고 유출 사실을 인지
- '21.5.24. 수탁사는 데이터를 DB에서 삭제하고, 로그를 백업·분석하고 KISA 보호나라에 해킹사고를 신고
- '21.5.27.~31. 수탁사는 SQL 인젝션 차단을 설정
- '21.6.18. 개인정보보호 포털에 개인정보 유출 신고(1천건 미만)
- '21.10.22., 11.2. 정보주체에게 유출 통지 \* 사전통지 기간 중 통지

## **3. 개인정보보호 법규 위반 행위 사실**

### **가. 개인정보를 파기하지 않은 행위**

피심인은 입사지원이 종료되거나 홈페이지 입사지원 기능이 삭제되어 불필요하게 된 입사지원자의 개인정보 건을 파기하지 않고 DB서버에 보관하였다.

### **나. 법률 등에 근거 없이 주민등록번호 처리 및 암호화 미조치한 행위**

피심인은 법률 등에 근거 없이 입사지원자의 주민등록번호 건을 보유하여 암호화하지 않고 DB서버에 보관하였으며, 암호화하지 않은 주민등록번호가 포함된 개인정보파일이 텔레그램에 유출되었다.

### **다. 개인정보 유출 사실을 통지하지 않은 행위**

피심인은 개인정보 유출 사실을 인지하고도 즉시 정보주체에게 유출통지를 하지 않았다.

## **4. 처분의 사전통지 및 의견 수렴**

개인정보보호위원회는 2021.10.25. 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 의견을 2021.11.8.에 제출하였다.

### Ⅲ. 위법성 판단

#### 1. 개인정보를 파기하지 않은 행위

##### 가. 관련 법령의 규정

보호법 제21조제1항은 “개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.”라고 규정하고 있다.

##### 나. 위법성 판단

피심인이 입사지원 종료 등으로 개인정보가 불필요하게 되었는데도 DB서버에 개인정보를 보관하고 파기하지 않은 것은 보호법 제21조제1항 위반에 해당한다.

#### 2. 법률 등에 근거 없이 주민등록번호를 처리한 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

보호법 부칙 <법률 제11990호, 2013. 8. 6.> 제2조제1항은 “이 법 시행 당시 주민등록번호를 처리하고 있는 개인정보처리자는 이 법 시행일(‘14.8.6.)부터 2년 이내에 보유하고 있는 주민등록번호를 파기하여야 한다”라고, 제2항에서는 “제1항에 따른 기간 이내에 보유하고 있는 주민등록번호를 파기하지 아니한 경우에는 제24조의2 제1항의 개정규정을 위반한 것으로 본다”라고 규정하고 있다.

#### 나. 위법성 판단

피심인이 보호법 시행(‘14.8.6.) 당시 법률 등에 근거 없이 입사지원자의 주민등록번호     건을 보유하고 있으나 보호법 부칙에 따라 ’16.8.6.까지 파기하지 않고 DB 서버에 지속 보관한 것은 보호법 제24조의2제1항 위반에 해당한다.

### 3. 주민등록번호 암호화 조치를 하지 않은 행위

#### 가. 관련 법령의 규정

보호법 제24조의2제2항은 “개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다”라고 규정하고 있다.

#### 나. 위법성 판단

피심인이 입사지원자의 주민등록번호     건을 DB 서버에 보관하면서 암호화 조치 등 안전성 확보에 필요한 조치를 다 하지 않아 텔레그램에 유출된 것은 보호법 제24조의2제2항 위반에 해당한다.

### 4. 개인정보 유출 미통지 행위

#### 가. 관련 법령의 규정

보호법 제34조제1항은 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 관련 사실을 알리도록 규정하고 있고,

「표준 개인정보 보호지침」(고시 제2020-1호) 제26조제1항은 개인정보처리자는 개인정보가 유출되었음을 알게 된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 알리도록 규정하고 있다.

#### 나. 위법성 판단

피심인이 개인정보 유출 사실을 인지하고도 지체 없이 정보주체에게 유출통지하지 않은 것은 보호법 제34조제1항 위반에 해당한다.

## IV. 처분 및 결정

### 1. 과징금 부과

주민등록번호가 유출된 경우로서 보호법 제24조의2제2항에 따른 안전성 확보에 필요한 조치를 다하지 않은 피심인에게 같은 법 제34조의2제1항, 같은 법 시행령 제40조의2제1항 [별표 1의3] 과징금의 부과기준(이하 “과징금 부과기준”이라 함)에 따라 다음과 같이 1,250만원의 과징금을 부과한다.

#### 가. 기준금액 산정

피심인의 위반행위는 고의 또는 중과실이 없고 건의 주민등록번호가 유출된 경우로, 과징금 부과기준 2. 가. 기본 산정기준에 따른 일반 위반행위에 해당하여 100,000천원으로 산정한다.

#### 나. 1차 조정

과징금 부과기준 2. 나.에 따라 안전성 확보조치 중 주민등록번호 저장 시 암호화하지 않은 점을 고려하여 기준금액의 50%인 50,000천원을 감액한다.

#### 다. 2차 조정

피심인의 위반행위는 위반 기간이 3개월 이내이며, 최근 3년 이내에 동일한 처분을 받은 적이 없고, 조사에 적극 협조한 점, 2차 피해 우려가 적은 점, 개인 정보 보호를 위한 노력이 상당한 점 등을 고려하여 과징금 부과기준 2. 다.에 따라 1차 조정된 금액의 50%인 25,000천원을 감액한다.

#### 라. 최종 조정

피심인은 「중소기업기본법」제2조에 따른 중소기업으로 과징금 부담 능력이 낮고, 주민등록번호 유출행위가 사소한 부주의로서 정보주체 등에 미치는 영향이 미미하고, 이를 통해 피심인이 경제적·비경제적 이득을 취하지 아니하였거나 취할 가능성이 현저히 낮은 경우에 해당하여 과징금 부과기준 2. 라.에 따라 2차 조정된 금액의 50%인 12,500천원을 감액한다.

## 마. 최종 금액

피심인이 보호법 제24조의2제2항을 위반한 행위에 대해 12,500천원의 과징금을 부과한다.

### < 최종 과징금 산출내역 >

(단위 : 천원)

기준 금액(A)	1차 조정액 (B)	2차 조정액 (C)	최종 조정액 (D)	최종액(E) E=(A+B+C+D)
100,000	△50,000	△25,000	△12,500	12,500

## 2. 과태료 부과

피심인의 보호법 제21조제1항, 제24조의2제1항 및 제34조제1항 위반에 대해서 같은 법 제75조제2항제4호, 제4호의2 및 제8호, 같은 법 시행령 제63조의 [별표2] 「과태료의 부과기준」에 따라 다음과 같이 총 900만원의 과태료를 부과한다.

### 가. 기준금액

피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 위반행위별 1회 위반에 해당하는 600만원(총 1,800만원)을 적용한다.

### < 과태료 부과기준 2. 개별기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만원)		
		1회 위반	2회 위반	3회 이상 위반
마. 법 제21조제1항을 위반하여 개인정보를 파기하지 않는 경우	법 제75조 제2항제4호	600	1,200	2,400
차. 법 제24조의2제1항을 위반하여 주민등록번호를 처리한 경우	법 제75조 제2항제4호의2	600	1,200	2,400
처. 법 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제8호	600	1,200	2,400
계		1,800		

### 나. 과태료의 가중

피심인의 위반행위는 보호법 시행령 [별표2] 과태료 부과기준 1. 일반기준 라.에 규정된 가중할 수 있는 사유에 해당하는 사항이 없으므로 가중 없이 기준금액을 유지한다.

## 다. 과태료의 감경

피심인의 위반행위는 부주의로 인한 것이며 추가피해 발생이 없었고, 사전통지 의견제출 기간이 종료되기 이전에 위반상태를 모두 시정한 점, 행위사실을 인정하면서 조사에 적극 협력한 점, 「중소기업기본법」제2조에 따른 중소기업인 점 등을 고려하여 위반행위별 기준금액의 50%인 300만원(총 900만원)을 감경한다.

## 라. 최종 과태료

피심인의 보호법 제21조제1항, 제24조의2제1항 및 제34조제1항 위반행위별 기준금액 600만원에서 50%를 감경한 300만원(총 900만원)을 부과한다.

### < 최종 과태료 산출내역 >

위반조항	위반내용	과태료 금액 (단위 : 만원)			
		기준금액 (A)	가중액 (B)	감경액 (C)	최종액(D) =(A+B+C)
법 §21①	개인정보를 파기하지 않음	600	-	△300	300
법 §24의2①	법률 등에 근거없이 주민등록번호를 처리함	600	-	△300	300
법 §34①	유출 시 정보주체에게 같은 항 각 호의 사실을 지체없이 알리지 않음	600	-	△300	300
계		1,800	-	△900	900

## 3. 결과 공표

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

개인정보보호법 위반 행정처분 결과 공표					
순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
2022년 월 일 개 인 정 보 보 호 위 원 회					



## V. 결론

피심인의 보호법 제21조(개인정보의 파기)제1항, 제24조의2(주민등록번호 처리의 제한)제1항·제2항 및 제34조(개인정보 유출 통지 등)제1항 위반행위에 대하여 같은 법 제34조의2(과징금의 부과 등)제1항, 제75조(과태료)제2항제4호·제4호의2·제8호, 제66조(결과의 공표)제1항 각각에 의한 과징금·과태료 부과, 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)