

# 개 인 정 보 보 호 위 원 회

## 심의 · 의결

안전번호 제2022-005-015호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 Zynga Game Ireland Limited  
25-28 North Wall Quay, Dublin 1, Ireland

의결연월일 2022. 3. 23.

## 주 문

1. 피심인에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 5,300,000원

가. 과 태 료 : 13,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

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

# 이 유

## I. 피심인의 일반 현황

피심인은 영리를 목적으로 정보통신망을 통해 게임 서비스를 제공하는 자로서 舊정보통신망이용 촉진 및 정보보호 등에 관한 법률(법률 제16021호, 이하 “정보통신망법”이라 함) 제2조제1항제3호에 따른 정보통신서비스 제공자이며, 일반현황은 다음과 같다.

### < 피심인의 일반현황 >

대표자	주소	설립일자
	25-28 North Wall Quay, Dublin 1, Ireland	2010.3.11.

## II. 사실조사 결과

### 1. 개인정보 유출 경위

#### 가. 유출 경로 및 규모

신원 미상자가 알 수 없는 방법으로 AWS의 개인정보처리시스템에 접근할 수 있는 AWS Key를 탈취하였다. 신원미상자는 '19.8.29. AWS에 무단 접근하여 시스템 구성, 접근 권한 등의 시스템 정보를 확인하고, '19.8.31. ~ 9.2. 특정 게임의 AWS 데이터베이스와 Poker 게임의 특정 회원 정보가 저장된 Private GitHub 서버에 접근하였다. 이를 통해 한국 이용자의 개인정보(이름, 생년월일, 이메일 주소, ID, 비밀번호 등)가 유출되었다.

피심인은 AWS 데이터베이스와 GitHub 서버 모두 금융 정보나 민감한 개인정보는 보관되어 있지 않고, GitHub 서버는 외부 인터넷에서 접속이 불가능하나 AWS 접속을 통해 접근이 가능하였다고 소명하였다.

피심인은 AWS Key를 교체하고 악성 IP주소를 차단, 무단 접근에 대한 실시간 감시를 포함한 모니터링과 경보를 강화하고, 네트워크에 FireEye(악성 활동을 탐지·차단하는 전문 툴) 배치하고 AWS 접근의 다중 인증을 강화하였다.

## 나. 경과 및 대응

일 시	인지 및 대응
'19. 9. 1.	비정상적인 네트워크 활동을 감지
'19. 9. 2.	특정 회원 계정정보의 유출 가능성 인지
'19. 9. 16.	한국 이용자 개인정보의 유출 가능성 인지
'19. 9. 30.	한국 이용자 약 1명에게 1차 이메일 통지
'19. 10. 23.	한국 이용자 약 2명에게 2차 이메일 통지

## 2. 행위 사실

### 가. 개인정보에 대한 접근통제를 소홀히 한 행위

피심인은 외부에서 이용자 데이터베이스에 접속하려는 경우 안전한 인증수단을 적용하지 않아, 신원 미상자가 탈취한 AWS Access Key로 데이터베이스에 무단 접근하여 개인정보를 유출하였다.

### 나. 개인정보 유출 신고 및 통지를 지연한 행위

피심인은 '19.9.2. 비정상적 네트워크 활동을 감지하고 개인정보 유출 가능성을 인지하였으나, '19.9.30.·10.23 한국 이용자에게 통지하고 개인정보보호 포털에 '19.10.1. 신고하였다.

## 3. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2021.7.20. '개인정보보호 법규 위반에 대한 행정처분 사전 통지' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였다.

2021.10.29. 피심인은 의견을 제출하였고, 개인정보보호위원회는 검토하였다.

### Ⅲ. 위법성 판단

#### 1. 개인정보에 대한 접근통제를 소홀히 한 행위

##### 가. 관련 법령의 규정

정보통신망법 제28조제1항은 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 유출을 방지하고 개인정보의 안전성을 확보하기 위하여 다음 각 호의 기술적·관리적 조치를 하여야 한다고 규정하고 있고, 제2호는 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영을 규정하고 있다.

같은 법 시행령 제15조제2항은 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다고 규정하고 있고, 제1호는 개인정보처리시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행을 규정하고 있다.

「(舊)개인정보의 기술적·관리적 보호조치 기준」(방통위 고시, '15.5.19.) 제4조 제4항은 정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다고 규정하고 있다.

##### 나. 위법성 판단

외부에서 개인정보처리시스템에 접속하려는 경우 안전한 인증수단을 적용하여야 하나 피심인이 이를 적용하지 않아 개인정보가 유출되어 정보통신망법 제28조 제1항 위반에 해당한다.

#### 2. 개인정보 유출 신고 및 통지를 지연한 행위

##### 가. 관련 법령의 규정

정보통신망법 제27조의3제1항은 정보통신 서비스 제공자들은 개인정보의 유출 사실을 안 때 지체 없이 해당 이용자에게 알리고 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다고 규정하고 있다.

#### 나. 위법성 판단

개인정보 유출 사실을 안 때에는 지체 없이(24시간 이내) 이용자에게 알리고 한국인터넷진흥원에 신고하여야 하나 피심인이 24시간을 경과하여 신고한 피심인의 행위는 정보통신망법 제27조의3제1항 위반에 해당한다.

### IV. 처분 및 결정

#### 1. 과징금 부과

피심인의 정보통신망법 제28조제1항제2호 위반에 대해 같은 법 제64조의3제1항, 시행령 제69조의2 [별표8] 및 「(舊)개인정보보호 법규 위반에 대한 과징금 부과 기준」(방통위 고시, '15.8.27.)에 따라 530만원의 과징금을 부과한다.

#### 가. 관련 매출액

피심인의 위반행위와 관련한 매출액은 사건이 발생한 게임의 한국 매출로서 직전 3개 사업연도의 연평균 매출액이다.

##### <직전 3년간 한국 매출액 현황>

구분	2016년	2017년	2018년	평균
한국 매출액(달러)				

#### 나. 기본 과징금

피심인의 위반행위가 과징금 부과기준 제5조에 따라 직접적인 이득을 취득하지 않았고 피해규모가 한국인 개인정보의 100분의 5 이내이고 유출 개인정보가 외부에 공개되지 않아 '보통 위반행위'이므로 관련 매출액에 1천분의 15 부과

기준율을 적용하여 기본과징금은            이다.

#### 다. 의무적 조정

피심인의 위반행위가 과징금 부과기준 제6조에 따라 위반기간이 1년 이내인 경우라서 가중 사유는 없고, 최근 3년간 과징금 처분을 받은 적이 없으므로 기준 금액의 50%인            를 감경한다.

#### 라. 임의적 조정

피심인의 위반행위가 과징금 부과기준 제8조에 따라 가중 사유는 없고, 조사에 적극 협력하고 개인정보 유출사실을 자진 신고하였으므로 의무적 조정을 거친 금액의 30%인            를 감경한다.

#### 마. 최종 과징금

피심인의 정보통신망법 제28조제1항 위반에 대하여 530만원의 과징금을 부과한다.

##### <과징금 산출내역>

기본과징금	의무적 조정	임의적 조정	최종액
			4,474 달러 (3.1. 기준 환율 적용)

※ 과징금 산출액이 1억원 미만이면 십만원 미만은 절사

## 2. 과태료 부과

피심인의 정보통신망법 제27조의3제1항 및 제28조제1항 위반에 대해 같은 법 제76조제1항 및 시행령 제74조 [별표9]에 따라 1,300만원의 과태료를 부과한다.

#### 가. 기준금액 산정

피심인이 최근 3년간 같은 각 위반행위로 과태료 처분을 받은 사실이 없으므로 2개의 위반행위에 대해 기준금액은 1회 위반에 해당하는 1,000만원을 각각 적용한다.

< 과태료의 부과기준 >

위반행위	근거 법조문	위반횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
하. 법 제27조의3제1항을 위반하여 이용자·방송통신위원회 및 한국인터넷진흥원에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제76조제1항 제2호의3	1,000	2,000	3,000
너. 법 제28조제1항에 따른 기술적·관리적 조치를 하지 않은 경우	법 제76조제1항 제3호	1,000	2,000	3,000
계		2,000		

**나. 과태료의 가중**

피심인의 제27조의3제1항 위반행위에 대해 개인정보 유출 사실을 정당한 사유 없이 24시간을 경과하여 통지·신고하였으므로 기준금액의 30%인 300만원을 가중한다.

**다. 과태료의 감경**

피심인은 각 위반행위에 대해 사전 통지 기간 전에 시정을 완료하고 조사기간 중 일관되게 행위사실을 인정하면서 조사에 적극 협력하였으며 위반행위의 정도나 동기 등을 고려하여 기준금액의 50%인 500만원을 각각 감경한다.

**라. 최종 금액**

피심인의 정보통신망법 제27조의3제1항 및 제28조제1항 위반에 대하여 기준금액 2,000만원에서 700만원을 감경하여 총 1,300만원의 과태료를 부과한다.

< 최종 과태료 산출내역 >

과태료 처분의 근거		과태료 금액 (단위:만원)			
위반조항	처분조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액 (D=A+B+C)
제27조의3제1항	제76조제1항제2호의3	1,000	300	△500	800
제28조제1항	제76조제1항제3호	1,000	-	△500	500
합 계		2,000	300	△1,000	1,300

### 3. 결과 공표

피심인의 위반행위가 개인정보보호법 제66조 및 같은 법 시행령 제61조에 해당하므로 피심인의 처분결과를 다음과 같이 개인정보보호위원회 홈페이지에 공표한다.

「(舊)정보통신망 이용촉진 및 정보보호 등에 관한 법률」 위반 행정처분 결과 공표					
(舊)정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.					
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

피심인이 정보통신망법 제28조제1항을 위반한 행위에 대하여 같은 법 제64조의3제1항에 의한 과징금 부과, 정보통신망법 제27조의3제1항 및 제28조제1항을 위반한 행위에 대하여 같은 법 제76조제1항에 의한 과태료 부과, 개인정보 보호법 제66조에 의한 공표를 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 중 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 중 식     (서 명)

위     원     염 홍 열     (서 명)

위     원     지 성 우     (서 명)