방 송 통 신 위 원 회
심의·의결

안건번호 제2018 - 35 - 384호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2018. 7. 11.

주 문

1. 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

2. 피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

3. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 금 액 : 10,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

라. 과태료를 내지 않으면 질서위반행위규제법 제24조, 제52조, 제53조제1항 및 제54조에 따라 불이익이 부과될 수 있음

이 유

Ⅰ. 기초 사실

피심인은 영리를 목적으로 홈페이지( ) 및 모바일 애플리케이션( )을 통해 판매 서비스를 제공하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법' 이라 한다) 제2조 제1항 제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황 및 최근 3년간 매출액은 다음과 같다.

〈참고 1〉 피심인의 일반현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수

〈참고 2〉 피심인의 최근 3년간 매출액 현황

(단위 : 백만원)

구 분	2015년	2016년	2017년	평 균
매출액				
정보통신서비스 매출액				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 고객정보가 노출되었다는 피심인의 개인정보 노출신고(2018.2.21.)가 개인정보보호 포털(i-privacy.kr, KISA)에 접수됨에 따라, 피심인을 대상으로 정보통신망법 위반여부에 대한 개인정보 취급·운영 실태를 현장조사(2018.3.26. ~ 2018.3.27.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 ‘ 판매’ 서비스를 운영하면서 2018. 3. 26. 기준으로 5,222,918건의 회원정보를 보유하고 있다.

〈참고 3〉 피심인의 개인정보 수집 현황

구 분	항 목	수집기간	건수
웹사이트 회원	[필수] 성명, 생년월일, 성별, 아이디, 비밀번호, 휴대전화번호, 이메일 주소 [선택] 주소, 닉네임	'12.12.23. ~	**5,222,918건** (휴면회원 1,381,317건 포함)
회원	[필수] 카드 번호, 카드 핀번호 *회원가입 후 회원 신청		
비회원	성명, 전화번호, 이메일 주소 *신규 입점 상담, 협력 고객사 등록 신청 등		

나. 개인정보 노출 규모 및 경로

(1) 개인정보 노출규모

피심인이 ‘ 판매’ 서비스를 운영하면서 수집한 회원의 개인정보 약 537건이 모바일 애플리케이션 내 소스코드 설정 오류로 인해 외부에 노출되었다.

〈참고 4〉 피심인의 개인정보 노출 현황

구 분	노 출 항 목	건 수
모바일 APP 회원	아이디, 닉네임, 휴대전화번호	537건

(2) 노출 경로

피심인은 2018.2.20. 모바일 애플리케이션 로그인 인증 보안 강화를 위해 실시한 엡데이트 프로그램 내 소스코드 오류로 인해 로그인 인증 정보가 타인의 계정으로 전송되어 회원정보(아이디, 닉네임, 휴대전화번호) 537건이 노출되었다.

(3) 노출 신고

피심인은 2018.2.21. 고객센터에 타인에게 계정이 노출되어 충전금액이 사용되었다는 고객 민원(17건) 신고를 접수하면서 노출 사고를 인지하였다.

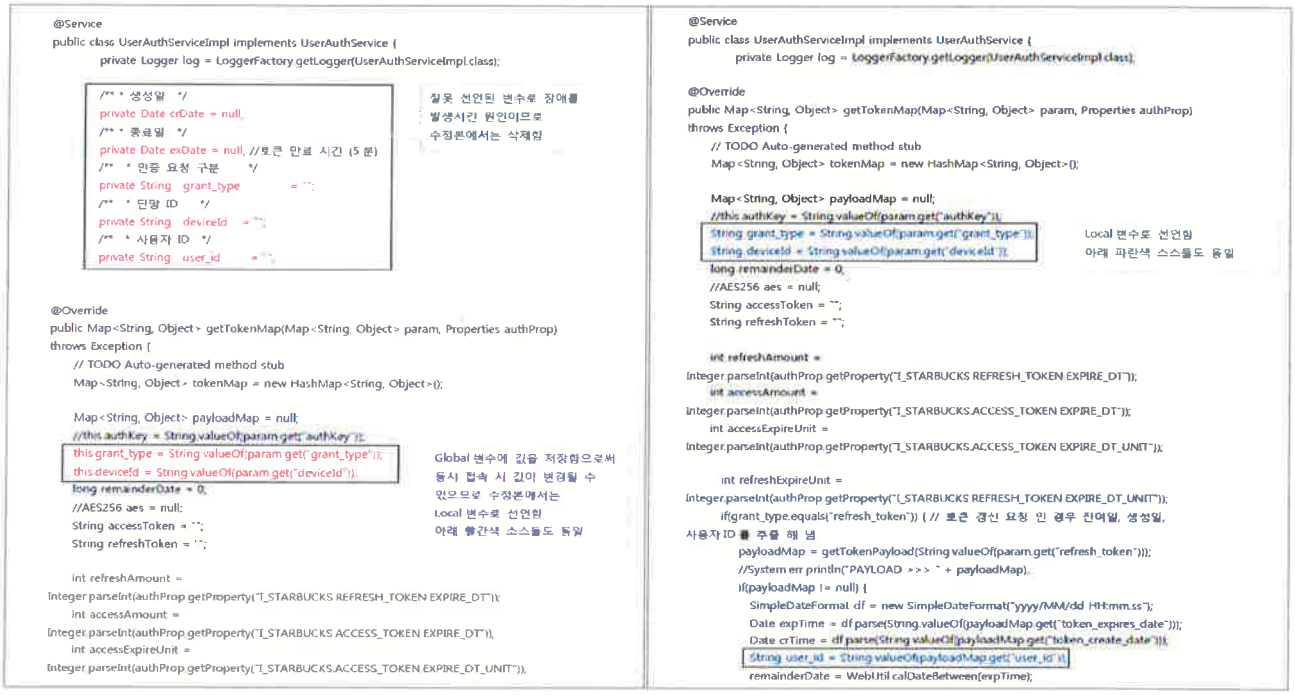
이에 피심인은 2018.2.22. 개인정보보호 포털(www.i-privacy.kr)에 개인정보 노출을 신고하였고, 2018.2.23. 노출가능 대상자를 특정(3,102명)하여 이메일(3,100명)과 앱 개인 팝업에 공지(2명)하였다.

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

가. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}**를 소홀히 한 행위**

피심인이 운영 중인 모바일 애플리케이션 로그인 인증 프로세스 강화를 위해 2018.2.20. 배포한 신규 버전(16.2.5.) 애플리케이션에 프로그램 오류가 포함되어 있었고, 해당 버전(16.2.5.) 애플리케이션을 다운로드해 로그인 한 회원

중 타인의 인증토큰이 전송되어 타인의 계정으로 로그인되어 열람권한이 없는 자의 개인정보가 공개되어 외부에 유출되었다.



```
@Service
public class UserAuthServiceImpl implements UserAuthService {
        private Logger log = LoggerFactory.getLogger(UserAuthServiceImpl.class);

    /** * 생성일 */
    private Date crDate = null;
    /** * 종료일 */
    private Date exDate = null; //토큰 만료 시간 (5 분)
    /** * 인증 요청 구분 */
    private String grant_type = "";
    /** * 단말 ID */
    private String deviceId = "";
    /** * 사용자 ID */
    private String user_id = "";

@Override
public Map<String, Object> getTokenMap(Map<String, Object> param, Properties authProp)
throws Exception {
    // TODO Auto-generated method stub
    Map<String, Object> tokenMap = new HashMap<String, Object>();

    Map<String, Object> payloadMap = null;
    //this.authKey = String.valueOf(param.get("authKey"));
    this.grant_type = String.valueOf(param.get("grant_type"));
    this.deviceId = String.valueOf(param.get("deviceId"));
    long remainderDate = 0;
    //AES256 aes = null;
    String accessToken = "";
    String refreshToken = "";

    int refreshAmount =
Integer.parseInt(authProp.getProperty("I_STARBUCKS.REFRESH_TOKEN.EXPIRE_DT"));
    int accessAmount =
Integer.parseInt(authProp.getProperty("I_STARBUCKS.ACCESS_TOKEN.EXPIRE_DT"));
    int accessExpireUnit =
Integer.parseInt(authProp.getProperty("I_STARBUCKS.ACCESS_TOKEN.EXPIRE_DT_UNIT"));
```

정적 선언된 변수로 장애를 발생시킨 원인이므로 수정본에서는 삭제함

Global 변수에 값을 저장함으로써 동시 접속 시 값이 변경될 수 있으므로 수정본에서는 Local 변수로 선언함 아래 빨간색 소스들도 동일

```
@Service
public class UserAuthServiceImpl implements UserAuthService {
        private Logger log = LoggerFactory.getLogger(UserAuthServiceImpl.class);

@Override
public Map<String, Object> getTokenMap(Map<String, Object> param, Properties authProp)
throws Exception {
    // TODO Auto-generated method stub
    Map<String, Object> tokenMap = new HashMap<String, Object>();

    Map<String, Object> payloadMap = null;
    //this.authKey = String.valueOf(param.get("authKey"));
    String grant_type = String.valueOf(param.get("grant_type"));
    String deviceId = String.valueOf(param.get("deviceId"));
    long remainderDate = 0;
    //AES256 aes = null;
    String accessToken = "";
    String refreshToken = "";

    int refreshAmount =
Integer.parseInt(authProp.getProperty("I_STARBUCKS.REFRESH_TOKEN.EXPIRE_DT"));
    int accessAmount =
Integer.parseInt(authProp.getProperty("I_STARBUCKS.ACCESS_TOKEN.EXPIRE_DT"));
    int accessExpireUnit =
Integer.parseInt(authProp.getProperty("I_STARBUCKS.ACCESS_TOKEN.EXPIRE_DT_UNIT"));

        int refreshExpireUnit =
Integer.parseInt(authProp.getProperty("I_STARBUCKS.REFRESH_TOKEN.EXPIRE_DT_UNIT"));
        if(grant_type.equals("refresh_token")) { // 토큰 갱신 요청 인 경우 잔여일, 생성일,
사용자 ID 를 추출 해 냄
            payloadMap = getTokenPayload(String.valueOf(param.get("refresh_token")));
            //System.err.println("PAYLOAD >>> " + payloadMap);
            if(payloadMap != null) {
              SimpleDateFormat df = new SimpleDateFormat("yyyy/MM/dd HH:mm:ss");
              Date expTime = df.parse(String.valueOf(payloadMap.get("token_expires_date")));
              Date crTime = df.parse(String.valueOf(payloadMap.get("token_create_date")));
              String user_id = String.valueOf(payloadMap.get("user_id"));
              remainderDate = WebUtil.calDateBetween(expTime);
```

Local 변수로 선언함 아래 파란색 스스들도 동일

나. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2018. 4. 26. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 5. 17. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제28조제1항은 "정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령이 정하는 기준에 따라 '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·

운영(제2호)' 를 하여야 한다." 라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 의 조치를 하여야 한다." 라고 규정하고 있다.

정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시') 제4조제9항은 "정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보 취급자의 컴퓨터에 조치를 취하여야 한다." 라고 규정하고 있다.

나. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자등의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다." 라고 규정하고 있다.

2. 위법성 판단

가. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}**를 소홀히 한 행위**

고시 제4조제9항의 입법 목적은 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 에러, 오류 상황이 처리되지 않거나 불충분하게 처리되지 않도록 구성하는 등 보안대책을 마련하여야 한다는 것이다.

피심인이 모바일 애플리케이션 에러, 오류 등의 위험요소를 분석해 개인정보가 유·노출되지 않도록 처리하지 않아 열람권한이 없는 자에게 이용자의 개인

정보 537건이 공개(노출)되도록 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.

〈참고 5〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②5호	취급중인 개인정보가 열람권한이 없는 자에게 공개·유출되지 않도록 조치를 취하지 행위(고시§4⑨)

Ⅳ. 시정조치 명령

1. 시정명령

피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

2. 시정명령 이행결과의 보고

피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

3. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 위반에 대한 과태료는

같은 법 제76조제1항제3호, 같은 법 시행령 제74조의 [별표9] 및 「개인정보보호 의무위반자 과태료 부과 등 처리지침」(이하 '과태료 부과 등 처리지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 부과 등 처리지침 제7조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피심인의 위반행위가 첫 번째에 해당하므로 1회 위반 과태료인 1,000만원을 적용한다.

〈참고 6〉 위반 횟수별 과태료 금액

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
너. 법 제28조제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 않은 경우	법 제76조 제1항제3호	1,000	2,000	3,000

나. 과태료의 가중 및 감경

특별히 가중·감경할 사유가 없어 기준 금액을 유지한다.

〈참고 7〉 과태료 산출내역

위반조문	기준금액	가중	감경	최종 과태료
§28①2호	1,000만원	없음	없음	**1,000만원**

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 1,000만원의 과태료를 부과한다.

V. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조(과태료)제1항제3호에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

피심인은 이 시정명령 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 방송통신위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 방송통신위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 방송통신위원회의 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.

위 원 장 이 효 성 (인)

부위원장 허 욱 (인)

위 원 김 석 진 (인)

위 원 표 철 수 (인)

위 원 고 삼 석 (인)