

방 송 통 신 위 원 회

심의 · 의결

안전번호 제2017 - 45 - 272호

안 건 명 O2O사업자 개인정보보호 법규 위반에 대한 시정조치에 관한 건

피 심 인 ㈜ (사업자등록번호 :)

대표이사

의 결 일 2017. 12. 12.

주 문

1. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하기 위하여 ①개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 개인정보처리시스템의 접근권한을 변경 또는 말소, ②외부에서 개인정보처리시스템에 접속이 필요한 경우에는 아이디와 비밀번호를 통한 개인정보처리자 식별·인증과 별도로 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용, ③이용자의 계좌번호에 대해 안전한 암호알고리즘으로 암호화하여 저장, ④정보통신서비스를 1년 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 위 1년이 경과한 후 위 이용자의 개인정보를 즉시 파기하거나 정보통신서비스를 이용하고 있는 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.



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

3. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 25,000,000원

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 숙박 온라인 예약대행 서비스를 제공하는 홈페이지 () 및 모바일앱(,)를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조 제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 최근 3년간 매출액은 다음과 같다.

〈 피심인 일반 현황 〉

구 분	2014년	2015년	2016년	평 균
매출액(단위 : 백만원)				

※ 자료 출처 : 피심인이 제출한 자료



II. 사실조사 결과

1. 조사 대상

방송통신위원회는 온라인과 오프라인을 연계하여 서비스를 제공하는 주요한 O2O(Online to Offline) 사업자를 대상으로 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 기획조사 하였고, 피심인에 대한 현장조사(2017.6.22.~2017.6.23.) 결과 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하기 위한 기술적·관리적 보호조치를 아니한 행위

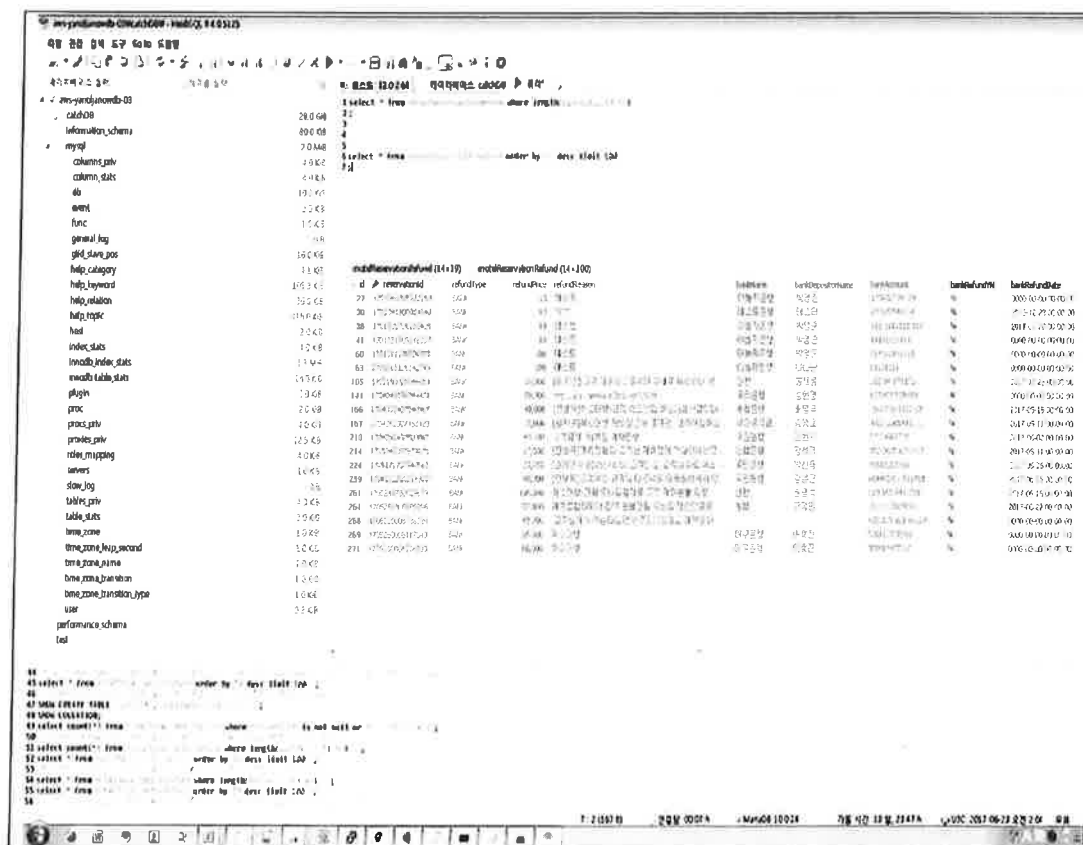
(1) 피심인은 2017. 6. 22. 현재 개인정보처리시스템인 관리자페이지(admin. .com)의 전체 접근권한 418개 중 이용자의 회원정보 및 예약정보를 열람 등 처리할 수 있는 개인정보취급자의 접근권한을 288개 부여하였고, 이 중 퇴사한 개인정보취급자의 접근권한 44개를 말소하지 않았으며, 접근권한이 1개월 동안 접속이 없는 경우 차단되도록 조치하고 있었으나 퇴사한 개인정보취급자 중 4명은 1개월 이내 퇴사한 직원으로 해당 접근권한이 사용이 가능하도록 하였다.

(2) 피심인은 개의 제휴점이 예약내역(이름, 휴대전화번호, 숙박예약날짜 등) 및 정산내역 등 이용자의 개인정보에 접근·다운로드 할 수 있는 개인정보처리시스템(.com)을 운영하고 있으나, 이들 제휴점을 포함한 개인정보취급자가 정보통신망을 통해 외부에서 동 개인정보처리시스템에 접속하는 경우 별도의 안전한 인증수단 없이 아이디와 비밀번호만으로 접속이 가능하도록 하였다.





(3) 피싱인은 환불 처리를 위해 수집한 이용자의 계좌번호를 개인정보처리 시스템에 저장하면서 안전한 암호알고리즘으로 암호화하지 않았다.



나. 정보통신서비스를 1년 동안 이용하지 않는 이용자의 개인정보를 즉시 파기 또는 별도로 저장·관리하지 아니한 행위

(1) 피심인은 운영 중인 모바일앱()을 이용하는 이용자로부터 이름, 이메일, 닉네임, 비밀번호, 휴대번호 등 을 수집하여 2017. 6. 22. 현재 명의 이용자 정보를 피심인의 개인정보처리시스템 내 회원DB에 저장·관리하고 있으며, 이 중 2016. 6. 22. 이후 서비스를 이용한 사실이 없어 1년 동안 서비스를 이용하지 아니한 이용자 명의 개인정보를 파기하거나 서비스를 이용하고 있는 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 사실이 있다.

다. 방송통신위원회는 2017. 8. 10. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청 하였으며, 피심인은 의견을 제출하지 않았다.

III. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제28조제1항은 “정보통신서비스 제공자등이 개인정보를 처리 할 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)’, ‘개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)’를 하여야 한다.”라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 “개인정보에 대한 불법적인 접근을 차단 하기 위하여 ‘개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시 스템(개인정보처리시스템)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의



수립·시행(제1호)',을 하여야 한다.”고 규정하고 있고, 제4항은 “주민등록번호, 계좌번호 및 바이오정보 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장(제2호)' 등의 조치를 하여야 한다.”고 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') 제4조제2항은 “정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다”고 규정하고 있으며,

제4조제4항은 “정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.”고 규정하고 있으며,

제6조제2항은 “정보통신서비스 제공자등은 계좌번호에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장한다(제6호).”고 규정하고 있다.

「개인정보의 기술적·관리적 보호조치 기준 해설서」는 고시 제4조제2항에 대해 내부 인력의 퇴직시 해당 인력의 계정 뿐만 아니라 해당 인력이 알고 있는 공용 계정에 대한 위험도 존재하게 되므로, 내부 인력의 퇴직 시에는 해당 인력의 계정을 삭제하고 내부 인력들이 공용으로 사용하는 계정의 비밀번호를 즉시 변경 하도록 지침에 반영하여 이행하여야 한다고 해설하고 있고,

고시 제4조제4항에 대해 외부에서 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만을 이용할 경우 유출 위험이 커지기 때문에 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증 수단의 적용이 필요하다고 해설하고 있고,

고시 제6조제2항에 대해 개인정보 유·노출 시에 2차 피해가 발생할 확률이



높은 계좌번호 등에 대해서는 안전한 알고리즘(128비트 이상)으로 암호화하여 저장·관리해야 한다고 해설하고 있다.

나. 정보통신망법 제29조제2항은 “정보통신서비스 제공자등은 정보통신서비스를 1년의 기간동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다”라고 규정하고 있다.

정보통신망법 시행령 제16조제2항은 “정보통신서비스 제공자등은 이용자가 정보통신서비스를 법 제29조의제2항의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다”라고 규정하고 있다.

다. 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. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하기 위한 기술적·관리적 보호조치를 아니한 행위

피심인이 개인정보처리시스템에서 퇴사한 개인정보취급자의 접근 권한 44개를 말소하지 않은 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항, 고시 제4조제2항을 위반하였고,

피심인이 제휴점이 외부에서 개인정보처리시스템에 접속시 단순히 아이디와 비밀번호 이외 추가적으로 안전한 인증수단(ex. 보안토큰, 휴대폰인증, 일회용



비밀번호, 바이오정보, 단말기 IP인증 등)을 적용하지 않은 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 15조제2항제1호, 고시 제4조제4항을 위반하였고,

피심인이 이용자의 계좌번호를 개인정보처리시스템에 저장하면서 안전한 암호 알고리즘으로 암호화하지 않은 행위는 정보통신망법 제28조제1항제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제4항제2호, 고시 제6조제2항을 위반하였다.

나. 정보통신서비스를 1년 동안 이용하지 않는 이용자의 개인정보를 즉시 파기 또는 별도로 저장·관리하지 아니한 행위

피심인이 정보통신서비스를 1년의 기간 동안 이용하지 않는 이용자의 개인정보를 즉시 파기하거나 또는 별도로 저장·관리하지 않은 행위는 정보통신망법 제29조제2항(개인정보의 파기 중 개인정보 유효기간제), 시행령 제16조제2항을 위반하였다.

〈참고〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
(주)	접근 통제	§28①2호	§15②1호	퇴사한 개인정보취급자의 개인정보처리시스템 접근권한을 말소하지 아니한 행위(고시§4②)
	접근 통제	§28①2호	§15②1호	외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증수단을 적용하지 아니한 행위(고시§4④)
	암호화	§28①4호	§15④2호	이용자의 계좌번호를 개인정보처리시스템에 저장하면서 안전한 암호알고리즘으로 암호화하지 아니한 행위(고시§6②)
	유효 기간제	§29②	§16②	1년 동안 서비스를 이용하지 않은 이용자의 개인정보를 파기하지도 않았고, 서비스를 이용하고 있는 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하지도 아니한 행위

IV. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하기 위하여 ①개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 개인정보처리시스템의 접근권한을 변경 또는 말소, ②외부에서 개인정보처리시스템에 접속이 필요한 경우에는 아이디와 비밀번호를 통한 개인정보처리자 식별·인증과 별도로 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용, ③이용자의 계좌번호에 대해 안전한 암호알고리즘으로 암호화하여 저장, ④ 정보통신서비스를 1년 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 위 1년이 경과한 후 위 이용자의 개인정보를 즉시 파기하거나 정보통신서비스를 이용하고 있는 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

2. 시정명령 이행결과의 보고

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

3. 과태료 부과

피심인의 정보통신망법 제28조제1항 및 제29조(개인정보의 파기)제2항 위반에 대한 과태료는 같은 법 제76조제1항제3호·제4호, 같은 법 시행령 제74조의 [별표 9]



및 「개인정보보호 의무위반자 과태료 부과 등 처리지침」(이하 '처리지침')에 따라 다음과 같이 부과한다.

가. 기준금액

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

〈 위반 횟수별 과태료 금액 〉

위반사항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
○ 법 제28조제1항(법 제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 않은 경우	법 제76조 제1항제3호	1,000	2,000	3,000
○ 법 제29조제2항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 파기 등의 조치를 취하지 않은 경우	법 제76조 제1항제4호	1,000	2,000	3,000

나. 과태료의 가중 및 감경

1) (과태료의 가중) '처리지침' 제9조는 ▲위반행위가 2개 이상인 경우, ▲위반행위가 2개 이상에 해당하지 아니하는 경우로서 위반 행위자의 사업 규모, 위반의 동기·정도, 사회·경제적 파급 효과 등을 고려하여 과태료를 가중 부과할 필요가 있다고 인정되는 경우에는, '처리지침' 제7조에 따른 과태료 금액을 2분의 1까지 가중하여 부과할 수 있다고 규정하고 있다.

이에 의할 때, 피심인의 정보통신망법 제28조제1항 위반행위가 2개 이상인 경우이므로 기준 금액의 50%를 가중한다.



2) (과태료의 감경) '처리지침' 제8조는 ▲위반행위의 결과가 과실에 의한 경우, ▲위반행위의 결과가 경미한 경우, ▲위 두 가지 규정에 해당하지 아니하는 경우로서 위반 행위자의 사업 규모, 위반의 동기 등을 고려하여 과태료를 감경 부과할 필요가 있다고 인정되는 경우에는 '처리지침' 제7조에 따른 과태료 금액을 2분의 1까지 감경하여 부과할 수 있다고 규정하고 있다.

이에 의할 때, 피심인의 정보통신망법 제28조제1항 및 제29조제2항 위반 행위 대해서 특별히 해당사항이 없으므로 과태료를 감경하지 않는다.

< 과태료 산출내역 >

위반조문	기준금액	과태료 가중	과태료 감경	최종 과태료
§28①	1,000만원	500	없음	1,500만원
§29②	1,000만원	없음	없음	1,000만원
계				2,500만원

다. 최종 과태료

이에 따라, 피심인의 정보통신망법 제28조제1항 및 제29조제2항 위반에 대해 2,500만원의 과태료를 부과한다.

V. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제4호(과태료)에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

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

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조 규정에 의하여 처분을 받은 날로부터 60일 이내에 방송통신위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 방송통신위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항 규정에 의하여 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 과태료를 납부하여야 한다.

위원장

이 효 성



부위원장

허 욱



위원

김 석 진



위원

표 철 수



위원

고 삼 석

