방 송 통 신 위 원 회
심의 · 의결

안건번호 제2018 - 05 - 022호

안 건 명 개인정보보호 법규 위반에 대한 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2018. 1. 24.

주 문

1. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하고 개인정보의 안전성을 확보하기 위하여 ①정보통신망을 통해 개인정보처리시스템에 불법적인 접근을 방지·차단하기 위한 침입차단·탐지시스템 등 접근통제 장치를 설치·운영하여야 하며, ②개인정보처리시스템에 접근 할 수 있는 개인정보취급자의 비밀번호는 '영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성', '연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고', '비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경'하는 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 하며, ③이용자의 계좌번호를 개인정보처리시스템에 저장시 안전한 암호알고리즘으로 암호화 하여야 하며, ④이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이전)하려면

이용자의 동의를 받거나 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우 이전되는 개인정보의 항목과 이전되는 국가, 이전일시 및 이전방법, 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다.), 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용기간 등을 이용자에게 고지하여야 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 : 21,000,000원
  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 전기통신사업자의 전기통신역무를 이용하여 가상통화 거래 사이트( )를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이다.

피심인은 가상통화 거래 사이트( )를 운영하면서

기간 동안 명의 회원 개인정보(이메일(ID), 이름, 생년월일, 휴대폰번호, 계좌번호 등)를 수집하고 DB(Table명 :)에 저장·관리하고 있으며, 피심인의 최근 3년간 매출액은 다음과 같다.

〈 피심인 일반 현황 〉

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

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 가상통화 탈취를 위한 악성코드 유포·표적 공격 등이 성행함에 온라인 가상통화 거래 사이트를 운영하는 주요한 사업자를 대상으로 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 기획조사 하였고, 피심인에 대한 현장조사(2017. 10. 10. ~ 2017. 10. 16.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 접근통제시스템을 설치·운영하지 않은 행위

피심인은 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 접근통제 시스템을 설치·운영하지 않았다.

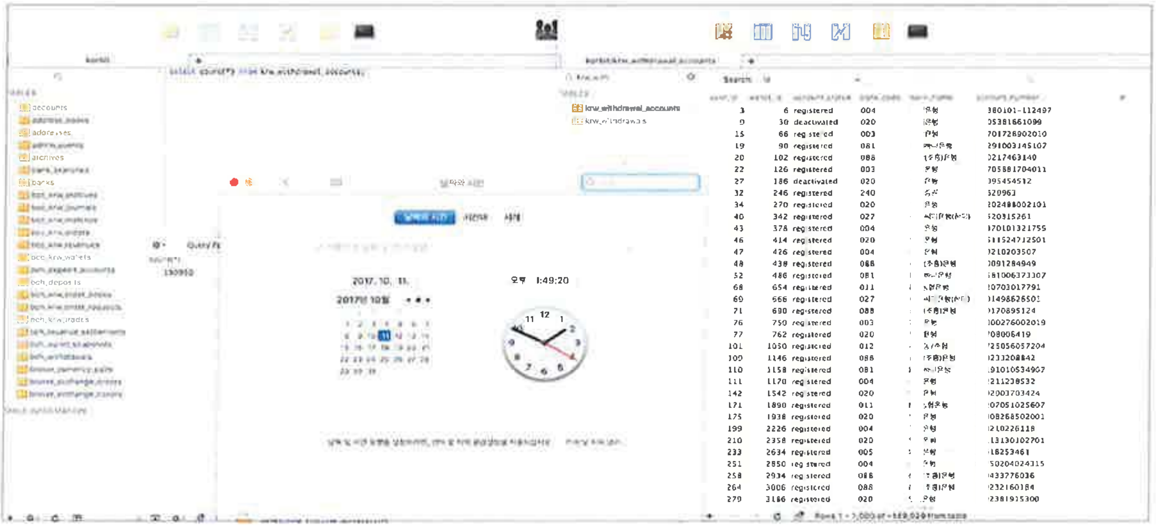
나. 개인정보취급자의 비밀번호 작성규칙을 수립하고 적용·운영하지 않은 행위

피심인은 2017. 10. 16. 개인정보 내부관리계획을 보완·수정하여 비밀번호 작성규칙을 수립하여 적용하기 전까지, 개인정보취급자를 대상으로 '영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성', '연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고', '비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경' 사항을 포함하는 비밀번호 작성규칙을 수립·운영(개인정보 내부관리계획에도 포함되지 않음)하지 않은 사실이 있다.

다. 이용자의 계좌번호를 암호화하지 않은 행위

피심인은 2017. 10. 16. 이용자의 계좌번호를 암호화하는 등 개선조치 하기 전까지, 이용자의 원화 환급 및 입금 등을 처리하기 위해 수집한 이용자의 계좌번호 건을 개인정보처리시스템에 안전한 암호알고리즘으로 암호화하여 저장하지 않고 평문으로 저장한 사실이 있다.

< 이용자 계좌번호 미암호화 화면 >



라. 국외 이전 개인정보의 이용자 고지{정보통신망법 제63조(국외 이전 개인정보의 보호) 중 고지}**하지 않은 행위**

피심인은 2017. 10. 16. 개인정보를 처리 위탁·보관하고 있다는 사실을 개인정보처리방침에 추가하여 이용자에게 고지하기 전까지, 클라우드 웹서비스 (서버위치 :)를 사용하면서 이용자의 개인정보를 국외에 처리 위탁·보관하고 있다는 사실을 이용자에게 고지하지 않은 사실이 있다.

마. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2018. 1. 4. 개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 1. 12. 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)', '개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)'를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영(제4호)'을 하여야 한다."라고 규정하고 있고, 제4항은 "개인정보를 안전하게

저장·전송될 수 있도록 보안조치를 하기 위하여 '주민등록번호, 계좌번호 및 바이오정보 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장(제2호)'을 하여야 한다."라고 규정하고 있으며, 제6항은 "개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 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') 제4조제5항은 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)', '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)' 기능을 포함한 시스템을 설치・운영하여야 한다."라고 규정하고 있으며

고시 해설서는 ▲"정보통신망을 통해 개인정보처리시스템에 불법적으로 접근하는 행위를 방지・차단하기 위해 침입차단기능 및 침입탐지기능을 갖는 시스템 등을 설치・운영함으로써 네트워크 보안을 강화하여야 한다."라고,

▲"침입차단 및 침입탐지 기능을 갖춘 설비의 설치 방법으로, 일정 규모 이상의 개인정보처리시스템을 운영하고 있는 사업자는 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치・운영하거나, 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템(IPS : Intrusion Prevention System), 웹방화벽 또는 보안 운영체제(Secure OS) 등을 도입할 수 있다."라고,

▲"전문 침입차단시스템 및 침입탐지시스템의 설치 운영이 곤란한 SOHO 등 소기업의 경우 인터넷데이터센터(IDC) 등에서 제공하는 보안서비스(방화벽, 침입방지, 웹방화벽 등)를 활용함으로써 초기 투자비용 등을 줄일 수 있다."라고,

▲"또한, 공개용(무료) S/W를 사용하여 해당 기능을 구현한 시스템을 설치・운영 할 수 있다. 다만, 공개용(무료) S/W를 사용하는 경우에는 적절한 보안이 이루어지는지를 사전에 점검할 필요가 있다."라고 설명하고 있다.

고시 제4조제8항은 “정보통신서비스 제공자등은 개인정보취급자를 대상으로 ‘영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성(제1호)’, ‘연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고(제2호)’, ‘비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경(제3호)’ 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다.”라고 규정하고 있으며

고시 해설서는 ▲“정보통신서비스 제공자등은 개인정보취급자가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음의 사항을 포함하는 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템 등에 적용하여야 한다.”라고,

▲ “비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합 · 구성하여야 한다.”라고,

▲ “개인정보처리시스템에 권한 없는 자의 접근을 방지하기 위하여 비밀번호 등을 일정 횟수 이상 잘못 입력할 때에는 개인정보처리시스템에 접근을 제한하는 등의 보호조치를 추가적으로 적용할 수 있다.”라고 설명하고 있다.

고시 제6조제2항은 “정보통신서비스 제공자등은 계좌번호에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다(제6호).”라고 규정하고 있으며

고시 해설서는 ▲“주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 바이오정보는 국내 및 미국, 일본, 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리듬으로 암호화하여 저장하여야 한다.”라고 설명하고 있다.

나. 정보통신망법 제63조제2항은 “정보통신서비스 제공자등은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이전)하려면 이용자의 동의를 받아야 한다. 다만 정보통신서비스의 제공에 관한 계약을 이행하고

이용자 편익 증진 등을 위하여 필요한 경우로서 제3항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁·보관에 따른 동의절차를 거치지 아니할 수 있다."라고 규정하고 있다.

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

2. 위법성 판단

가. 접근통제시스템을 설치 · 운영하지 않은 행위

피심인은 2017. 10. 16. 조사 당시 오픈소스(Snort)를 이용한 침입탐지를 적용 및 운영체제(Linux CentOS)에서 제공하는 기본 방화벽(iptables)을 사용하거나, 별도로 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하거나, 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템, 웹 방화벽 등의 보안장비를 도입하여 운영한 사실은 없었다. 피심인은 이에 대하여 확인서를 통하여 확인하였고, 2018. 2. 1.부터 침입차단 및 침입탐지시스템이 동시에 구현된 침입방지시스템을 설치 · 운영하고 있다고 소명하고 있다.

따라서 피심인은 2018. 2. 1. 침입통제시스템을 설치 · 운영하기 전까지 개인정보를 처리할 때에는 개인정보의 분실 · 도난 · 유출 · 변조 또는 훼손을 방지하기 위하여 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고, 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치 · 운영하여야 하나, 오픈소스(Snort)를 이용한 침입탐지 및 운영체제(Linux CentOS)에서 제공하는 기본 방화

벽(iptables)을 사용하지 않았고, 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치 · 운영하지 않음으로써 정보통신망법 제28조제1항제2호(기술적 · 관리적 보호조치 중 접근통제), 시행령 제15조제2항, 고시 제4조제5항을 위반하였다.

나. 개인정보취급자의 비밀번호 작성규칙을 수립하고 적용 · 운영하지 않은 행위

피심인은 2017. 10. 11. 조사 당시 개인정보취급자를 대상으로 '영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성', '연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고', '비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경' 사항을 포함하는 비밀번호 작성규칙을 수립하지 않고 이를 적용 · 운영하지 않았다. 피심인은 이에 대하여 확인서를 통하여 확인하였고, 2017. 10. 16. 비밀번호 작성 규칙을 수립 · 운영 조치 완료하였다고 소명하고 있다.

따라서 피심인은 2017. 10. 16. 비밀번호 작성규칙을 수립하여 적용하기 전까지, 개인정보취급자를 대상으로 '영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성', '연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고', '비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경' 사항을 포함하는 비밀번호 작성규칙을 수립하지 않고 이를 적용 · 운영하지 않음으로써 정보통신망법 제28조제1항제2호, 시행령 제15조제2항제4호, 고시 제4조제8항을 위반하였다.

다. 이용자의 계좌번호를 암호화하지 않은 행위

피심인은 이용자의 원화 환급 및 입금 등을 처리하기 위해 수집한 이용자의 계좌번호·   건을 개인정보처리시스템(DB)에 저장하면서 안전한 암호알고리즘으로 암호화하지 않고 있었다. 피심인은 이러한 위반사실에 대하여 확인서에서 확인하였으며, 2017. 10. 16. 개인정보처리시스템에 보관된 계좌번호를 암호화

조치 완료하였다고 소명하고 있다.

따라서 피심인은 2017. 10. 16. 이용자 계좌번호를 암호화 조치 완료 전까지 이용자의 계좌번호 건을 개인정보처리시스템(DB)에 저장하면서 안전한 암호알고리즘으로 암호화하지 않음으로써 정보통신망법 제28조제1항제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제4항제2호, 고시 제6조제2항을 위반하였다.

라. 국외 이전 개인정보를 이용자에게 고지하지 않은 행위

피심인은 클라우드 웹서비스(서버위치 :)를 사용하면서 이용자의 개인정보를 국외에 처리 위탁·보관하고 있으면서도 이용자의 개인정보를 국외에 처리위탁·보관하고 있다는 사실을 이용자에게 고지 및 동의를 받은 사실은 없다. 피심인은 이에 대하여 2017. 10. 11. 조사 당시 확인서를 통하여 확인하였으며 2017. 10. 16. 개인정보를 국외에 처리위탁·보관하고 있다는 사실을 개인정보처리방침에 추가하고 이용자에게 알리고 있다고 소명하고 있다.

따라서 피심인은 2017. 10. 16. 이용자의 개인정보를 국외에 처리위탁·보관하고 있다는 사실을 이용자에게 고지하기 전까지, 이용자의 개인정보를 국외에 처리위탁·보관하고 있다는 사실을 알리지 않음으로써 정보통신망법 제63조제2항을 위반하였다.

〈참고〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근통제	§28①2호	§15②2호	개인정보의 불법적인 접근을 차단하기 위한 침입차단 및 침입차단 시스템을 설치·운영하지 않은 행위(고시§4⑤)
	접근통제	§28①2호	§15②4호	개인정보취급자의 비밀번호 작성규칙을 수립·운영하지 않은 행위(고시§4⑧)
	암호화	§28①4호	§15④2호	이용자의 계좌번호를 개인정보처리시스템에 저장하면서 안전한 암호알고리즘으로 암호화하지 않은 행위(고시§6②)
	국외이전	§63②		이용자의 개인정보를 국외에 처리 위탁·보관하고 있다는 사실을 이용자에게 고지하지 않은 행위

Ⅳ. 시정조치 명령

1. 시정명령

피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하고 개인정보의 안전성을 확보하기 위하여 ①정보통신망을 통해 개인정보처리시스템에 불법적인 접근을 방지·차단하기 위한 침입차단·탐지시스템 등 접근통제 장치를 설치·운영하여야 하며, ②개인정보처리시스템에 접근 할 수 있는 개인정보취급자의 비밀번호는 '영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성', '연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고', '비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경'하는 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 하며, ③이용자의 계좌번호를 개인정보처리시스템에 저장시 안전한 암호알고리즘으로 암호화 하여야 하며, ④이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이전)하려면 이용자의 동의를 받거나 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우 이전되는 개인정보의 항목과 이전되는 국가, 이전일시 및 이전방법, 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다.), 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용기간 등을 이용자에게 고지하여야 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 제28조(개인정보의 보호조치)제1항 및 제63조(국외 이전 개인정보의 보호)제2항 위반에 대한 과태료는 같은 법 제76조제1항제3호 및 제76조제2항제5호 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 1,000만원과 600만원을 적용한다.

〈 위반 횟수별 과태료 금액 〉

위반사항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
너. 법 제28조제1항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 기술적·관리적 조치를 하지 아니한 자	법 제76조 제1항제3호	1,000	2,000	3,000
우. 법 제63조제2항 단서를 위반하여 제63조제3항 각 호의 사항 모두를 공개하거나 이용자에게 알리지 아니하고 이용자의 개인정보를 국외에 처리위탁·보관한 자	법 제76조 제2항제5호	600	1,200	2,000

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 기준금액의 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, 특별히 감경할 사유가 없으므로 과태료를 감경하지 않는다.

< 과태료 산출내역 >

위반조문	기준금액	과태료 가중	과태료 감경	최종 과태료
§28①	1,000만원	500만원	없음	**1,500만원**
§63②	600만원	없음	없음	**600만원**
계				**2,100만원**

다. 최종 과태료

이에 따라, 피심인의 정보통신망법 제28조제1항 및 제63조제2항 위반에 대해 2,100만원의 과태료를 부과한다.

Ⅴ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제3호(과태료),제76조제2항제5호(과태료) 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 이효성 (인)

부위원장 허 욱 (인)

위 원 김석진 (인)

위 원 표철수 (인)

위 원 고삼석 (인)