방 송 통 신 위 원 회
심의 · 의결

안건번호 제2018 - 47 - 438호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2018. 9. 4.

주 문

1. 피심인은 개인정보를 처리할 때에는 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적 · 관리적 보호조치를 취하여야 한다.

가. 개인정보취급자의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 5년간 보관할 것

나. 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인 · 감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존 · 관리할 것

다. 개인정보취급자가 개인정보처리시스템에 접속한 접속기록이 위 · 변조되지 않도록 별도의 물리적인 저장장치에 보관하여야 하며 정기적인 백업을 수행할 것

라. 이용자의 계좌번호, 신용카드번호를 저장할 때는 암호알고리즘으로 암호화할 것

2. 피심인은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리 위탁·보관(이전)할 경우 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.

3. 피심인은 제1항부터 제2항까지의 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.

4. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 금　　액 : 17,800,000원

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 홈페이지(　　)를 통해 영유아 영어교육 교재 등을 판매하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 최근 3년간 매출액은 다음과 같다.

〈 의 매출액 현황 〉

(단위 : 백만원)

구 분	2015년	2016년	2017년	평 균
매출액				

※ 자료 출처 : 피심인이 제출한 자료, (사업개시일 :)

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 피심인에 대한 이용자 민원(국외이전)이 국민신문고에 접수(2018.3.10.)됨에 따라 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 현장조사(2018.4.12.~13.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보의 분실·도난·유출·변조 또는 훼손을 방지하기 위하여 기술적·관리적 조치를 하지 아니한 행위

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

피심인은 개인정보처리시스템에 대하여 개인정보관리책임자 및 개인정보취급자의 접근 권한 부여 및 변경 또는 말소에 관한 내역을 최소 5년간 보관하여야 하나 2017. 04. 23.일부터 권한 부여 기록만 보관한 사실이 있다.

2) 개인정보처리시스템에 접속한 기록의 보관 및 점검{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}**을 소홀히 한 행위**

피심인은 개인정보취급자가 DB 및 관리자페이지 등 개인정보처리시스템에 접속한 처리일시, 처리내역 등 접속기록을 보존·관리하지 아니하였고, 접속기록이 위·변조되지 않도록 별도의 물리적인 저장장치에 보관하고 정기적인 백업을 수행하지 않았으며, 개인정보처리시스템의 접속기록을 월1회 이상 정기적으로 확인·감독한 사실이 없다.

3) 개인정보의 암호화{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**를 소홀히 한 행위**

피심인은 이용자의 계좌번호 5,253건 및 신용카드번호 546건을 암호화하지 않고 평문으로 DB에 저장한 사실이 있다.

나. 개인정보의 국외 이전을 이용자에게 고지{정보통신망법 제63조(국외 이전 개인정보의 보호) 중 국외 제공 고지}**하지 않은 행위**

피심인은 2012. 02. 16.부터 214,423건의 개인정보를 일본 소재 “ ”로 데이터 보관 및 서비스운영을 처리 위탁하고 있다는 사실을 개인정보 처리방침에 추가(2017. 03. 31.)하여 이용자에게 고지하기 전까지 이용자의 개인정보를 국외에 처리 위탁·보관하고 있다는 사실을 이용자에게 고지하지 않은 사실이 있다.

※ 피심인은 2017. 04. 24.부터 고객정보를 국내 IDC센터로 다시 이전하여 보관·관리하고 있음(처리방침 상 국외이전 부분 삭제)

다. 처분의 사전통지 및 의견수렴

방송통신위원회는 2018. 7. 17. ‘개인정보보호 법규 위반사업자 시정조치(안) 사전통지 및 의견수렴’ 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 7. 27. 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)', '접속기록의 위조·변조 방지를 위한 조치(제3호)', '개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)' 하여야 한다." 라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)' 등의 조치를 하여야 한다." 라고 규정하고 있고, 제3항은 "정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 '개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(제1호)' 등의 조치를 하여야 한다." 라고 규정하고 있고, 제4항은 "정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '주민등록번호, 계좌번호 및 바이오정보 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장(제2호)' 을 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' 라 한다.) 제4조제3항은 "정보통신서비스 제공자등은 개인정보처리시스템의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다." 라고 규정하고 있다.

고시 제5조제1항은 "정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 한다." 라고 규정하고 있고, 제3항은 "정보통신서비스 제공자등은 개인정보취급자의 접속기록이 위·변조되지 않도록 별도의 물리적인 저장 장치에 보관하여야 하며 정기적인 백업을 수행하여야 한다." 라고 규정하고 있다.

고시 제6조제2항은 "정보통신서비스 제공자등은 계좌번호, 신용카드번호 등 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다." 라고 규정하고 있다.

'고시 해설서' 는 고시 제4조제3항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 접근권한 부여, 변경, 말소 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 5년간 보관하여야 하며, 관리대장 등에는 신청자 정보, 신청 및 적용 일시, 승인자 및 발급자 정보, 신청 및 발급 사유 등의 내용이 포함되어야 하며 공식적인 절차를 통하여 관리하도록 한다고 해설하고 있다.

고시 제5조제1항에 대해 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여 개인정보 처리를 위한 업무수행과 관련이 없거나 과도한 개인정보의 조회, 정정, 다운로드, 삭제 등 비정상적인 행위를 탐지하고 적절한 대응조치를 하여야 한다고 해설하고 있으며,

개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무의 확인을 위해 ⅰ)식별자(개인정보처리시스템에서 개인정보취급자를 식별할 수 있도록 부여된 ID 등), ⅱ)접속일시(개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시점) 〈년-월-일, 시:분:초〉, ⅲ)접속지(개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등), ⅳ)수행업무(개인정보처리시스템에서 개인정보취급자가 처리한 내용을 알

수 있는 정보)〈개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위〉 등을 포함하는 접속기록을 최소 6개월 이상 보존·관리하여야 한다고 해설하고 있다.

고시 제5조제3항에 대해 정보통신서비스 제공자등은 개인정보처리시스템에 접속한 기록이 위·변조되지 않도록 ⅰ)정기적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 물리적인 저장장치에 보관, ⅱ)접속기록을 수정 가능한 매체(하드디스크, 자기 테이프 등)에 백업할 때에는 위·변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관·관리, ⅲ) 다양한 접속기록 위·변조 방지 기술의 적용 등의 보호조치를 취하여야 한다고 해설하고 있다.

고시 제6조제2항에 대해 개인정보 유·노출 시에 2차 피해가 발생할 확률이 높은 계좌번호, 신용카드번호 등에 대해서는 안전한 알고리즘(128비트 이상)으로 암호화하여 저장·관리해야 한다고 해설하고 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 "과학기술정보통신부장관 또는 방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반 한 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·변조 또는 훼손을 방지하기 위하여 기술적·관리적 조치를 하지 아니한 행위

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

피심인이 개인정보처리시스템에 대한 접근 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관하지 아니한 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항제1호, 고시 제4조제3항을 위반한 것이다.

2) 개인정보처리시스템에 접속한 기록의 보관 및 점검{정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지}**을 소홀히 한 행위**

피심인이 개인정보취급자의 개인정보처리시스템 접속일시·처리내역 등 접속기록을 작성하여 월1회 이상 이를 확인·감독하지 않고 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 개인정보처리시스템의 접속기록(로그기록)을 보존·관리하지 않은 행위는 정보통신망법 제28조제1항제3호(기술적·관리적 보호조치 중 접속기록), 같은 법 시행령 제15조제3항제1호, 고시 제5조제1항, 고시 제5조제3항을 위반한 것이다.

3) 개인정보의 암호화{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**를 소홀히 한 행위**

피심인이 이용자의 계좌번호 및 신용카드번호를 안전한 암호알고리즘으로 암호화하지 않고 평문으로 DB에 저장한 행위는 정보통신망법 제28조제1항제4호(기술적·관리적 보호조치 중 암호화), 같은 법 시행령 제15조제4항제2호, 고시 제6조제2항을 위반한 것이다.

나. 개인정보의 국외 이전을 이용자에게 고지{정보통신망법 제63조(국외 이전 개인정보의 보호) 중 국외 제공 고지}**하지 않은 행위**

피심인이 이용자의 개인정보를 국외에 처리 위탁·보관하고 있다는 사실을 이용자에게 고지하지 않은 행위는 정보통신망법 제63조제2항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②1호	개인정보취급자에 대한 권한부여·변경·말소내역을 기록하고 그 기록을 최소5년간 보관하지 아니한 행위(고시§4③)
	접속 기록	§28①3호	§15③1호	개인정보취급자의 개인정보처리시스템 접속기록을 작성하여 월1회 이상 감독하지 않고, 최소 6개월 이상 개인정보처리시스템의 접속기록을 보존하지 아니한 행위(고시§5①·③)
	암호화	§28①4호	§15④2호	이용자의 계좌번호 등에 대해 안전한 알고리즘으로 암호화하지 않고 평문으로 DB에 저장한 행위 (고시§6②)
	국외 이전	§63②		이용자의 개인정보를 국외에 처리 위탁·보관하고 있다는 사실을 이용자에게 고지하지 않은 행위

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다. 1)개인정보취급자의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 5년간 보관할 것 2) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로

확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리할 것 3)개인정보취급자가 개인정보처리시스템에 접속한 접속기록이 위·변조되지 않도록 별도의 물리적인 저장장치에 보관하여야 하며 정기적인 백업을 수행할 것 4)이용자의 계좌번호, 신용카드번호를 저장할 때에는 안전한 암호알고리즘으로 암호화할 것

나. 피심인인 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이전)할 경우 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 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

3. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 및 제63조제2항에 대한 과태료는 같은 법 제76조제1항제3호, 제76조제2항제5호 같은 법 시행령 제74조의 〔별표9〕 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 부과지침 제6조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피심인의 위반행위가 첫 번째에 해당하므로 1회 위반 과태료인 1,000만원과 600만원을 각 적용한다.

〈 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
우. 법 제63조제2항 단서를 위반하여 법 제63조제3항 각 호의 사항 모두를 공개하거나 이용자에게 알리지 않고 이용자의 개인정보를 국외에 처리위탁·보관한 경우	법 제76조 제2항제5호	600	1,200	2,000

나. 과태료의 가중 및 감경

1) **(과태료의 가중)** 과태료 부과지침 제8조는 ▲증거인멸·조작, 허위 정보 제공 등 조사방해, ▲위반의 정도, ▲ 기타 위반행위의 동기, 사업규모, 그 결과 등을 고려하여 과태료를 가중 부과할 필요가 있다고 인정되는 경우에는, 과태료 부과지침 제8조에 따른 과태료 금액을 2분의 1까지 가중하여 부과할 수 있다고 규정하고 있다.

이에 의할 때, 피심인의 정보통신망법 제28조제1항 위반행위가 3개인 경우에 해당하므로 기준 금액의 50%를 가중하고, 제63조제2항 위반행위에 대해서는 특별히 해당사항이 없으므로 과태료를 가중하지 않는다.

2) **(과태료의 감경)** 과태료 부과지침 제7조는 ▲당사자의 환경, ▲사업규모와 자금사정, ▲개인(위치)정보보호 노력정도, ▲ 조사협조와 자진시정 ▲기타 위반행위의 정도, 동기, 사업규모, 그 결과 등을 고려하여 과태료를 감경 부과할 필요가 있다고 인정되는 경우에는 과태료 부과지침 제7조에 따른 과태료 금액을 2분의 1까지

감경하여 부과할 수 있다고 규정하고 있다.

이에 의할 때, 제28조제1항 위반에 대해서는 중기업으로서 직전 3개 사업연도 평균 당기순이익이 적자인 점을 고려하여 기준금액에서 20%를 감경하고, 조사 과정 중 법규 위반 행위를 중지하고 시정을 완료한 정보통신망법 제63조제2항 위반 행위에 대해서 기준금액에서 20%를 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§28①6호	1,000만원	500만원	200만원	**1,300만원**
§63②	600만원	없음	120만원	**480만원**
계				**1,780만원**

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제28조제1항과 제63조제2항 위반행위에 대해 1,780만원의 과태료를 부과한다.

Ⅴ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제3호(과태료)에 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.

이에 주문과 같이 의결한다.

2018년 9월 4일

위 원 장 이 효 성 (인)

부위원장 허 욱 (인)

(국회 참석 관계로 회의 불참)

위 원 김 석 진 (인)

위 원 표 철 수 (인)

위 원 고 삼 석 (인)