

방 송 통 신 위 원 회

심의 · 의결

안건번호 제2020-28-121호

안 건 명 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2020년 5월 19일

주 문

1. 피심인은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 '유출등이 된 개인정보 항목', '유출등이 발생한 시점', '이용자가 취할 수 있는 조치', '정보통신서비스 제공자등의 대응 조치', '이용자가 상담 등을 접수할 수 있는 부서 및 연락처' 등 위의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.

2. 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. 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 것



나. 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터를 물리적 또는 논리적으로 망분리 적용할 것

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 : 18,000,000원

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

1 (이하 '피심인'이라 한다)은 지상파방송사업자로 홈페이지 ()를 통해 시청자의 개인정보를 수집·이용하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제67조에 따른 정보통신서비스 제공자이고, 피심인의 일반현황 및 최근 3년간 매출액은 다음과 같다.

< 피심인의 일반현황 >

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

대표이사	설립일자	자본금	주요서비스	종업원 수

〈 피심인의 최근 3년간 매출액 현황 〉

(단위 : 천원)

구 분	2016년	2017년	2018년	평 균
매출액 (정보통신 매출액)				

※ 매출액 : 피심인이 제출한 자료

II. 사실조사 결과

1. 조사 대상

- 2 방송통신위원회는 개인정보보호 포털에 유출 신고한 사업자에 대하여 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사(2019.9.17.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집·이용 현황

- 3 피심인은 뉴스, TV, 라디오 다시보기 및 시청자 의견 수렴 등을 위해 홈페이지 ()를 운영하면서 2019.9.17. 기준 건의 이용자 정보를 수집·보관하고 있다.

〈 개인정보 수집·이용 현황 〉

구분	항목	수집일	건수
회원 정보	아이디, 비밀번호, 이름, 연락처, 이메일, 직업, 생년월일		건
총 계			건

나. 개인정보 유출 관련 사실관계

4 (개인정보 유출 경과 및 대응)

일시		피심인의 유출인지·대응 내용
2019.8.1.	15:29	피심인의 홈페이지 회원 장기 미사용자를 대상으로 메일 전체발송
2019.8.14.	15:00	한국인터넷진흥원 유출신고 공문 접수를 통해 유출 사실 인지
2019.8.14~15.		메일 발송처리 내역 확인 및 수신자 명단 확보
2019.8.17.	17:00	정보주체 개별 통지문 발송 및 홈페이지를 통한 개인정보 유출 사실 공지
	19:04, 19:21	개인정보보호 종합포탈 및 개인정보보호 포탈을 통한 유출 신고

5 (유출 규모 및 항목) 피심인의 홈페이지()회원 이메일 정보 1,683건

6 (유출 경위) 피심인이 운영하는 홈페이지() 회원을 대상으로 장기 미사용자에게 회원정리(2019.12. 31. 회원 삭제예정) 안내메일을 2019.8.1. 발송하는 과정에서 개인정보처리 담당자의 실수로 안내메일을 개별수신이 아닌 전체 수신으로 발송

3. 개인정보의 기술적·관리적 보호조치 등 사실관계

가. 개인정보의 분실·도난·유출 사실을 지연 통지·신고한 행위

7 피심인은 2019.8.14. 15:00 한국인터넷진흥원의 유출신고 공문접수를 통해 개인정보 유출을 인지하였으나, 약 2일이 경과한 2019.8.17. 17:00 개인정보 유출 통지문 발송 및 홈페이지 통해 개인정보 유출사실을 공지한 사실이 있다.

나. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제를 소홀히 한 행위



- 8 (안전한 인증수단) 피심인은 개인정보취급자가 정보통신망을 통해 외부에서 관리자페이지()에 접속이 필요한 경우 별도의 인증수단을 적용하지 않고, 아이디와 비밀번호만으로 접속이 가능하도록 운영한 사실이 있다.
- 9 (망분리) 피심인은 2018년도 매출액이 163억원으로 개인정보처리시스템 망분리 적용 대상 사업자이나, 관리자 페이지()에 일반회원 및 취급자의 권한을 부여할 수 있는 기능을 운영하면서 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리하지 않은 사실이 있다.

<관리자 페이지 및 DB접속 시 외부망 미적용>

다. 처분의 사전통지 및 의견 수렴

- 10 방송통신위원회는 2020. 2. 25. '개인정보보호 법규 위반사업자 시정조치(안)사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2020. 3. 9. 의견을 제출하였다.



III. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제27조의3제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체 없이 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.”라고 규정하고 있다.

11 정보통신망법 시행령 제14조의2제1항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제27조의3제1항 각 호의 모든 사항을 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.”고 규정하고 있으며, 제2항은 “정보통신서비스 제공자등은 제1항에 따른 통지·신고를 하려는 경우 법 제27조의3제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 아니하였으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.”라고 규정하고 있다.

12 「정보통신망법 해설서」는 정보통신망법 제27조의3제1항의 ‘지체 없이’에 대해서 정보통신망법에 별도로 규정된 정의는 없으나, 관련 판례에서는 ‘합리적인 이유 및 근거가 없는 한 즉시’로 해석하고 있다.

나. 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)’을 하여야 한다.”라고 규정하고 있다.

13 정보통신망법 시행령 제15조제2항은 “개인정보에 대한 불법적인 접근을 차단하기 위하여 ‘개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행(제1호)’, ‘전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자의 경우 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단(제3호)’, ‘그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)’ 등의 조치를 하여야 한다.”라고 규정하고 있다.

14 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「(구)개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 ‘고시’) 제4조제4항은 “정보통신서비스 제공자 등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다.”고 규정하고 있고, 제4조제6항은 “전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자 등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다.”고 규정하고 있다.

15 ‘고시 해설서’는 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 인증수단의 적용이 필요하다고 해설하고 있고, 제4조제6항에 대해 개인정보처리시스템에 접근하여 다운로드, 파기 또는 접근권한 설정이 가능한 개인정보취급자는 외부 인터넷망이 차단된 업무망에서 업



무를 수행하여야 하며, 업무망과 외부 인터넷망은 서로의 영역에 접근할 수 없도록 물리적이거나 논리적으로 망분리하여 차단하여야 한다고 해설하고 있다.

다. 정보통신망법 제64조제3항은 “방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속 공무원에게 정보통신서비스 제공자등, 해당 법 위반 사실과 관련한 관계인의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다.”라고 규정하고 있다.

2. 위법성 판단

가. 개인정보의 분실·도난·유출 사실을 지연 통지·신고{정보통신망법 제27조의3(개인정보 유출등의 통지·신고)}한 행위

16 피심인이 개인정보의 유출 사실을 안 때(2019.8.14.)로부터 2일이 경과한 2019.8.17.에 개인정보 유출 통지 및 신고를 한 행위는 정보통신망법 제27조의 3제1항, 같은 법 시행령 제14조의2제1항을 위반한 것이다.

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

17 (안전한 인증수단) 피심인이 개인정보취급자가 외부에서 피심인의 개인정보 처리시스템에 접속 시 단순히 아이디와 비밀번호만으로 접속할 수 있도록 하고 추가적으로 안전한 인증수단(ex. 보안토큰, 휴대폰인증, 일회용 비밀번호, 바이오정보, 단말기 IP인증 등)을 적용하지 않은 행위는 정보통신망법 제28조제1항 제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제4항을 위반한 것이다.

18 (망분리) 피심인이 개인정보처리시스템에서 일반회원 및 취급자의 권한을 부여할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리를 하지 않은 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항, 고시 제4조제6항을 위반한 것이다.



< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	지연 통지	§27조의3①	§14조의2①	개인정보의 유출 사실을 안 때로부터 24시간을 경과하여 해당 이용자에게 통지한 행위
	접근 통제	§28①2호	§15②1호	외부에서 개인정보처리시스템에 접속 시 단순히 아이디/패스워드만을 이용토록 하여 안전한 인증 수단을 적용하지 아니한 행위(고시§4④)
	접근 통제	§28①2호	§15②3호	개인정보처리자의 접근 권한을 부여할 수 있는 개인정보취급자의 컴퓨터를 망분리하지 아니한 행위(고시§4⑥)

IV. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 '유출등이 된 개인정보 항목', '유출등이 발생한 시점', '이용자가 취할 수 있는 조치', '정보통신서비스 제공자등의 대응 조치', '이용자가 상담 등을 접수할 수 있는 부서 및 연락처' 등 위의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다.

나. 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) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 것 2) 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터를 물리적 또는 논리적으로 망분리 적용할 것



2. 시정명령 이행결과의 보고

- 19 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.

V. 과태료 부과

- 20 피심인의 정보통신망법 제27조의3(개인정보 유출등의 통지·신고)제1항, 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제2호의 3·제3호, 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

- 21 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 1,000만원을 각 적용한다.

〈 위반 횟수별 과태료 금액 〉

ㄱ ㄴ ㄷ ㄹ ㄺ ㄻ ㄼ ㄽ ㄾ ㄿ ㅀ ㅁ ㅂ ㅃ ㅄ ㅅ ㅆ ㅈ ㅊ ㅋ ㅌ ㅍ ㅎ

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
하. 법 제27조의3제1항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·방송통신위원회 및 한국인터넷진흥원에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제76조 제1항제2호의3	1,000	2,000	3,000
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

1) (과태료의 가중) 과태료 부과지침 제8조는 ▲증거인멸, 조작, 허위의 정보 제공 등 조사방해, ▲위반의 정도, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 가중할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 가중할 수 있다고 규정하고 있다.

22 이에 따라 피심인의 정보통신망법 제27조의3제1항 위반행위는 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하므로 기준금액의 30%인 300 만원을 가중하고, 같은 법 제28조제1항 위반행위에 대해서는 특별히 가중사유가 없으므로 가중하지 않는다.

< 과태료 부과지침 [별표2] ‘과태료의 가중기준’ >

기준	가중사유	가중비율
위반의 정도	나. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내
	제3호 정보통신망법 시행령 제74조 별표 9 제2호 하목	
	가. 정보통신망법 제27조의3제1항을 위반하여 이용자에게 통지하지 아니하거나 정당한 사유 없이 24시간을 경과하여 통지한 경우 나. 정보통신망법 제27조의3제1항을 위반하여 방송통신위원회 또는 한국인터넷진흥원에 신고하지 아니하거나 정당한 사유 없이 24시간을 경과하여 신고한 경우	

2) (과태료의 감경) 과태료 부과지침 제7조는 ▲당사자 환경, ▲사업규모와 자금사정, ▲개인(위치)정보보호 노력정도, ▲조사협조 및 자진시정, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 감경할 수 있다고 규정하고 있다.

23 이에 따라 피심인의 정보통신망법 제28조제1항 위반행위는 시정조치(안) 사전통지 및 의견제출 기간 이내에 법규 위반행위에 대하여 시정을 완료한 점을 고려하여 기준금액의 50%인 500만원을 감경하고, 같은 법 제27조의3제1항 위반행위에 대해서는 특별히 감경사유가 없으므로 감경하지 않는다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§27의3①	1,000만원	300만원	없음	1,300만원
§28①4호	1,000만원	없음	500만원	500만원
계				1,800만원

다. 최종 과태료

24 이에 따라 피심인의 정보통신망법 제27조의3제1항, 제28조제1항 위반행위에 대해 18,000,000원의 과태료를 부과한다.

VII. 결론

25 피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제2호의3·제3호(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.

2020년 5월 19일

위원장 한 상 혁 

부위원장 표 철 수 

위 원 허 욱 

위 원 김 창 룡



위 원 안 형 환

