개인정보보호위원회 보도자료 국민이 만든 대전환의 길

보도시점 배포 즉시

개인정보위, '㈜KT의 개인정보 유출사고' 제재처분 의결

▷ KT의 불법 펨토셀을 통한 개인정보 유출에 대해 안전조치 의무 위반으로 과징금 539억 7,900만 원 부과

▷ 위원회 조사 결과, 펨토셀을 통한 이동통신 핵심 네트워크·시스템 접근통제 관리 소홀로 16,647명의 개인정보(휴대전화번호, IMSI, IMEI) 유출 및 이동통신망 문자·전화 탈취 확인

※ 해킹으로 개인정보가 유출된 데 그치지 않고 소액결제 인증에 사용된 SMS·ARS까지 탈취돼 약 2.4억 원 부정 결제가 발생하는 등 실제 피해로 이어지며 국민 불안이 커짐

▷ 재발 방지를 위해 펨토셀 등 통신설비 전반의 취약점 점검, 개인정보보호책임자(CPO)의 실질적 역할 수행을 포함한 대책을 3개월 내 수립·보고하도록 시정명령하고, 사고가 발생한 이동통신 네트워크·시스템에 대해 개인정보보호 관리체계(ISMS-P) 인증을 받도록 개선권고

▷ '24.3월 악성코드 감염 사실을 신고하지 않고 로그 삭제, 거짓 자료 제출 등으로 조사를 방해한 KT는 고발 조치하고, '25.8월 조사 착수전 서버 폐기 등 증거를 인멸한 LGU+는 수사의뢰

▷ 증거 은닉·폐기 등 조사방해 행위를 막기 위한 제도개선을 연내 추진

개인정보보호위원회(위원장 송경희, 이하 '개인정보위')는 7월 29일(수) 제15회 전체회의를 열고, 「개인정보 보호법」(이하 '보호법')을 위반한 ㈜KT(이하 'KT')에 대해 **과징금 539억 7,900만 원을 부과**하고, **시정명령, 개선권고, 공표, 공표 명령하고,** 조사과정에서 거짓자료 제출 등으로 조사를 방해한 행위에 대해 **고발**을 **의결하였**다. 아울러 조사 착수 전 서버를 폐기해 증거를 인멸한 ㈜**LGU+**(이하 'LGU+')**는 수사기관에 수사의뢰**하기로 결정하였다.

1 KT의 펨토셀을 통한 개인정보 유출

가. 사실관계

개인정보위는 KT 소액결제로 인한 피해사례 접수 및 언론보도 등에 따라 개인정보 유출가능성을 인지하고 2025년 9월 10일 조사에 **선제적으로 착수**하였다. KT는 다음날인 **9월 11일** 5,561명의 **개인정보 유출을 신고**했고, 이후 조사 과정에서 추가 유출이 확인되어 9월 18일과 10월 17일 두 차례 더 신고하였다.

조사 결과, 해커는 유실된 KT 펨토셀에서 인증서를 빼내 이를 자체 제작한 펨토셀에 심은 뒤 이를 통해 KT 이동통신망에 접속하였다. 이후 이용자 단말이 해커의 펨토셀을 경유하도록 유도하여 단말과 내부망 간 송·수신 정보를 가로챘고, 이를 추가적으로 확보한 개인정보(이름, 성별, 생년월일)와 결합하여 휴대폰 소액결제를 요청한 뒤 결제인증코드가 포함된 ARS·SMS를 탈취하여 무단 소액결제에 성공하였다.

* 펨토셀: 무선통신 품질 개선을 위해 가정이나 사무실, 지하 등 무선통신 신호가 약한 음영지역 해소를 위한 소형기지국

이 과정에서 **KT 이용자 16,647명***(알뜰폰 포함, 중복제거)의 **개인정보(휴대전화번호, 가입자식별번호(IMSI), 단말기식별번호(IMEI))**가 유출되었으며, **총 368명을 대상으로 약 2.4억 원 상당의 무단 소액결제 피해**가 발생한 것으로 확인되었다.

* 당초 유출신고한 22,227명 중 법인 및 다중회선 등 중복을 제거한 실제 정보주체 규모 산정

그동안 다수의 개인정보 유출사고는 개인정보가 제3자에게 유출되었음에도 직접적인 피해가 명확히 확인되지 않은 경우가 많았으나, 이번 사건은 단순한 개인정보 유출에 그치지 않고, 펨토셀을 통해 **유출된 개인정보가 실제 금전적 피해로 이어진 사례**라는 점에서 그 심각성이 매우 크다.

나. 펨토셀 운영 주체 및 KT의 관리통제 범위

펨토셀은 KT가 2016년 11월부터 무선통신 신호가 약한 음영지역 해소를 위해 도입·운영한 소형기지국으로 KT 인터넷을 사용하는 고객을 대상으로 KT 설치기사가 직접 설치해주며, 이용자에게 판매되지 않는 KT의 자산이다.

펨토셀이 KT 무선통신망에 접근하기 위한 망 접속 승인, 인증체계 관리, 내부망 접속 허용, 보안통제 및 운영은 KT가 수행한다. 반면, 이용자는 펨토셀의 설치 장소 등 운영환경 제공 역할만 수행하는 바, 개인정보위는 **펨토셀의 실질적인 운영 주체는 KT**이며, **펨토셀의 이동통신망 접속 및 서비스 제공을 위한 이용자 인증과정, 이 과정에서의 개인정보 전송에 대한 관리통제권**은 **KT**에 속한다고 판단하였다.

다. 개인정보 보호법 위반 사항

KT의 개인정보 처리·운영 실태와 개인정보 보호법 준수 여부를 조사한 결과, 이번 사고는 KT가 초소형 기지국인 펨토셀을 관리·운영하면서 **KT 내부망에 대한 기본적인 접근통제 관리를 소홀히** 하여 발생한 것으로 확인되었다.

이동통신 서비스를 위해 KT 내부망 내 개인정보 처리시스템인 홈가입자 서버(HSS) 등은 이용자 단말과 개인정보(휴대전화번호, 가입자식별번호(IMSI), 단말기 식별번호(IMEI) 등)를 전송하면서 가입자 및 기기를 인증하고, 음성·문자서비스를 연결한다. 이때, 음영지역의 이용자 단말은 펨토셀을 반드시 거치게 되므로, **KT 내부망에는 인가된 펨토셀만 접속하도록 엄격하게 통제·관리**할 필요가 있다.

그러나, 사고 당시 KT의 펨토셀 관리체계는 전반적으로 부실하여 인가받지 않은 펨토셀이 KT 내부망에 쉽게 접속할 수 있는 상태였다. KT는 내부망 접속을 위해 부여하는 펨토셀 인증서의 유효기간을 10년으로 장기간 설정하였으며, 내부망에 접속하는 펨토셀에 대해 **접속 아이피(IP) 제한을 하지 않아 타사 또는 해외 아이피(IP)에서도 접속 가능**하도록 운영하였다.

또한, 펨토셀 관리서버를 우회하는 경로가 존재하였으며, 펨토셀이 코어망 접속시 부여되는 식별자인 셀 아이디(Cell ID)를 관리하지 않아 **비인가 셀 아이디(Cell ID)의 이상접속 행위에 대한 탐지·대응체계가 부재**한 상태로 운영하는 등 **펨토셀을 통한 KT 내부망의 개인정보처리시스템에 대한 접근통제 관리를 소홀히** 하고 있음을 확인하였다.

이로 인해 해커는 유실된 KT 펨토셀에 존재하는 인증서를 복사하여 자체 제작한 펨토셀에 삽입하였고, 별도의 인증절차 없이 **KT의 내부망에 약 11개월간 (2024.10.8. ~ 2025.9.5.) 접속**하여 이용자의 개인정보를 유출하는 동안 KT는 이러한 **이상접속 행위를 탐지하지 못하였다.** 이로 인해, 소액결제 등 2차 피해가 발생하여 다수의 민원이 접수된 후에야 비정상 접속을 식별할 수 있었다.

이에 대해 개인정보위는 KT가 개인정보 보호법에서 부여하고 있는 정보통신망을 통한 **불법적인 접근 및 침해사고 방지를 위한 안전조치 의무를 위반**한 것으로 판단하였다.

라. 처분 내용

개인정보위는 KT가 대규모 개인정보를 처리하는 이동통신사업자로서 안전조치의무를 소홀히 하여 개인정보가 유출된 행위에 대해 **과징금 539억 7,900만 원을 부과**하고, KT가 운영 중인 홈페이지에 위와 같이 **처분받은 사실을 공표하도록 명령**하였다.

아울러, 유사사고 재발 방지를 위해 펨토셀 등 무선통신망 장비에 대한 **취약점 점검 및 통신망 내 개인정보에 대한 불법적인 접근통제 등 안전조치를 강화**하는 한편, 회사 전반의 개인정보 처리 업무에 대해 개인정보 보호책임자(CPO)의 책임과 역할을 명확히 하는 등 **거버넌스 체계를 정비**할 것을 시정명령하였다.

또한, 일부 IT서비스를 대상으로 획득한 **개인정보보호 관리체계(ISMS-P)의 인증범위를 이동통신 네트워크 시스템까지 확대**하여 개인정보 보호수준을 제고할 것을 **개선 권고**하였다.

2 KT 악성코드 감염 및 LGU+ 개인정보 유출

가. KT의 악성코드 감염 관련

개인정보위는 펨토셀 사건 조사과정에서 2024년 3월 KT IT서비스 네트워크 내 38대* 서버가 해킹으로 BPFDoor** 등 **다수의 악성코드에 감염**된 사실을 확인하고, 개인정보 유출 가능성이 있다고 보아 **조사를 확대**하였다.(2025.11.6.~)

* 과기정통부 민관합동조사단은 조사결과(2025.12.29.) 41대 서버 감염을 발표함. 다만, 이 중 3대는 별도의 네트워크에서 발생하였고 개인정보처리시스템에 해당하지 않아 위원회 조사 대상에서 제외

** BPFDoor(Berkeley Packet Filter) : 리눅스 시스템을 타깃으로하는 백도어 악성코드

확인 결과, 해커는 2024년 3월 KT 로밍렌탈서비스 홈페이지 내 취약점을 이용해 네트워크에 침투한 뒤 **악성코드 파일을 업로드하여 다수 서버를 감염**시켰으며, **로밍렌탈서비스 관리자페이지에 대한 SQL 삽입공격***으로 **KT 임직원 및 협력사 일부직원의 개인정보**(이름, 전화번호, 계정)를 조회·유출한 정황을 확인하였다.

* SQL(Structured Query Language) 삽입 공격 : 웹사이트 취약점을 이용해 악의적인 SQL(데이터베이스 명령어) 문을 실행되게 함으로써 DB를 비정상적으로 조작하는 공격 기법

다만, 개인정보위는 사건 발생 이후 조사가 진행되는 시점에 **사고 당시의 네트워크 로그 부재 등으로 사실관계 확인에 한계**가 존재하여 해커의 공격이 발생한 38대 서버의 개인정보 처리시스템에 대한 이용자 개인정보의 추가 유출은 확인할 수 없었다.

KT는 2024년 3월 자사 서버의 악성코드 감염 사실을 최초로 인지하고도 정부에 **침해사실을 신고하지 않았고, 개인정보 유출 여부에 대한 상세 분석을 진행하지 않은 채 자체적으로 조치**(2024년 3월 ~ 7월)하였다. 당시 감염 서버 중에는 **이용자 개인정보를 처리하는 시스템이 다수** 포함되어 있는 상황이었다.

또한, 2025년 4월 타 통신사 개인정보 유출 사고를 계기로 **KT 서버에 대한 악성코드 감염 여부를 전수 점검**하는 과정에서, **침해 발생 서버 일부(10대)의 로그를 삭제**하는 등 **조직적으로 침해사실을 은폐한 정황**도 확인하였다.

아울러, 개인정보위 조사과정에서 초기에는 **감염서버에 대한 보존 자료가 없다고 거짓 진술**하였으나, 위원회가 디지털포렌식을 통해 조사착수 전 관련 로그를 삭제한 정황을 적발해 내자, 진술을 번복하고 별도로 보관중인 로그를 뒤늦게 제출하여 조사를 지연시키는 등 **위원회의 사고조사를 실질적으로 방해**한 사실이 있다.

나. LGU+ 개인정보 유출

개인정보위는 2025년 8월 **미국 보안 전문지 'Phrack'**에서 발표한 **LGU+의 개인정보 유출** 사실을 인지하고 같은 해 9월 10일 조사에 착수하여 개인정보 유출관련 사실관계를 검토하였다.

조사 과정에서 **LGU+ 임직원·협력사 직원의 이름, 계정** 등이 포함된 텍스트 파일의 유출 여부를 점검했고, 해당 정보가 **LGU+의 통합 비밀번호 관리시스템**(Automated Process Policy Management, 이하 'APPM')에서 실제 LGU+가 보유·관리하던 정보로 확인되었다.

다만, LGU+는 위원회의 조사 착수 전 **APPM 서버 등 관련 서버의 운영체제(OS)를 재설치**(2025.8.12., 8.14.)**하거나 폐기**(2025.8.25.)하여 위원회가 조사를 통해 정확한 유출 경위 및 추가 유출 여부 등을 확인할 수 없도록 하였다.

다. KT 및 LGU+에 대한 대응

개인정보위는 KT가 2024년 3월 악성코드 감염 사고 발생 당시 개인정보 유출 분석을 소홀히 하고 정부에 미신고하였으며, 이후 사고 서버의 로그 일부를 삭제하고 위원회 조사과정에서 거짓 자료제출 및 번복 등으로 **위원회 조사를 방해한 행위**에 대해서는 **고발하기로 결정**하였다.

아울러, **LGU+**가 **관련 서버 OS 재설치 및 폐기 행위**로 개인정보 유출 관련 사실관계 확인을 어렵게 한 바, 이를 공무집행방해 행위로 판단하고 **수사기관에 수사 의뢰**하기로 하였다.

3 조사 실효성 강화를 위한 제도개선 계획

개인정보위는 KT와 LGU+ 같이 개인정보 유출 가능성이 존재함에도 조사·제재 회피 목적으로 관련 **증거를 은닉·폐기하여 위원회 조사를 방해**하는 행위에 엄정 대응하고 **조사의 실효성을 강화하기 위한 제도개선**을 추진한다.

현행 규정상, ‘조사 중’ 은닉 등 행위에 대해서는 형사처벌·과태료 부과가 가능하나, ‘조사 착수 전’ 행위에 대해서는 제재 규정이 미비하여 사업자가 사고 발생 시 증거를 미리 은닉·폐기하는 것이 오히려 유리할 수 있는 규제 사각지대가 있다.

이에 개인정보위는 개인정보 유출사고가 발생하면 적기에 신고하여 2차 피해를 최소화할 수 있도록 ① ‘조사 착수 전’ 은닉·폐기 행위에 대해 **형사처벌 규정** 마련, ② 증거 은닉·폐기시 **과징금(전체 매출액의 3%) 부과**, ③ 증거 은닉·폐기를 신고하여 조사·처분에 기여한 경우, **신고포상금 지급** 등 제도 개선을 추진한다.

아울러, 사업자의 비협조로 인해 조사가 지연되는 문제를 막기 위해 ④ 조사 비협조 또는 시정명령 미 이행시 **이행강제금(일 매출액 0.3%) 부과**, ⑤ **침해사고 발생시 자료보전명령 등**이 가능하도록 **보호법을 개정**할 계획이다.

4 이번 조사·처분의 의의

개인정보위는 이번 조사와 처분을 통해, 국민 생활과 밀접한 서비스를 제공하는 대규모 개인정보처리자의 유출사고에 대해 **위반행위의 중대성에 상응하는 경제적 제재로 책임성을 제고**하고, **국민의 개인정보를 두텁게 보호**하겠다는 원칙을 다시 한번 확인했다. 아울러, 개인정보처리자는 **개인정보 유출이 국민의 생명·재산에 직접적인 피해**로 이어질 수 있다는 점을 무겁게 인식하고 유출사고가 발생하지 않도록 책임 있는 노력을 다해야 한다.

또한, 사고를 은폐하더라도 끝까지 법적 책임을 묻는다는 원칙을 확인하여 '**사고 은폐와 조사 방해**'라는 일부 기업의 고질적인 관행에 대해 경종을 울리고, **제도 개선**을 통해 이런 행위가 더 이상 기업에 유리한 선택이 아니라는 인식을 정착시켜 나갈 계획이다.

송경희 개인정보위 위원장은 "이번 처분이 **국민 생활에 필수적인 서비스를 제공하는 통신 업계 전반의 보안 역량을 한층 강화**하는 계기가 되어야 한다"라고 강조하면서, "특히, 사고 발생 시 자료를 은폐하거나 축소하는 행위가 기업에 중대한 불이익으로 돌아가도록 제도를 개선하여, 앞으로는 **투명한 공개가 가장 합리적인 선택이라는 인식**을 업계 전반에 뿌리내리도록 하겠다"라고 밝혔다.

붙임 : 주요 질의 답변

담당 부서 <총괄>	개인정보보호위원회 조사2과	책임자	과 장	이정은 (02-2100-3121)
		담당자	조사관	조근환 (02-2100-3157)
담당 부서 <공동>	한국인터넷진흥원 개인정보조사단	책임자	단 장	임진수 (061-820-2800)
		담당자	팀 장	손기종 (061-820-2850)
		담당자	선 임	한미정 (061-820-2830)
		담당자	주 임	나정용 (061-820-2830)

붙임	주요 질의 답변

1. 민관합동조사단 조사결과 22,227건 유출과 차이가 있는 이유?

□ 과기정통부 민관합동조사단이 발표한 유출 규모는 해커의 펨토셀을 통해 유출된 정보의 전체 규모를 산정한 것이며,

○ 위원회는 유출된 정보 중 법인 및 다중회선 등 중복을 제외한 실제 정보주체의 규모로 산정하였음

□ 그 결과, KT 이동통신서비스 이용자 16,647명의 개인정보가 유출된 것으로 확인하였음

※ (유출내용) KT통신망(알뜰폰 포함) 이용자 16,647명의 개인정보(휴대전화번호, IMSI, IMEI)

2 과징금 산정 과정

□ **(산정기준)** 개인정보 유출 사고 발생 시, 안전조치 의무 위반이 확인될 경우, 전체 매출액의 3%를 초과하지 않는 범위에서, 위반행위와 관련없는 매출액을 제외한 매출액을 기준으로 과징금을 산정하게 되며,

○ 법 위반행위의 중대성과, 정보주체의 피해 규모 및 영향, 조사협조 및 시정완료 여부 등의 요소를 고려한 가중·감경을 거쳐 최종 과징금을 산정하게 됨

□ **(고려사항)** 무단 소액결제 사고가 발생한 KT 이동통신서비스의 5G·LTE 통신 매출을 기준으로 과징금을 산정하였고, IPTV·인터넷 통신 등 관련 없는 독립적인 매출액은 관련 매출액에서 제외

○ 국민의 생활에 필수적인 이동통신 서비스를 제공하는 기간통신사업자로서, 내부망에 대한 접근통제 관리 소홀로 공격자의 불법적인 접근을 제한하지 못하고 지속적인 접근에도 이상행위를 탐지하지 못해 실제 금전적 피해로 이어지는 등 개인정보 침해 수준이 상당히 높다는 점에서 중대한 위반행위로 판단하였고,

○ 위반기간 및 위반행위의 시정 여부, 피해 회복 노력 등 다양한 요소를 고려하여 최종 과징금액을 산정하였음

3. 이번 심의 과정에서 KT의 주요 주장은?

□ KT는 본 유출 사고가 해커가 펨토셀을 제작하여 단말기에서 송출되는 통신신호를 가로채는 방식으로 발생한 전례 없는 신유형의 사고로 예측 및 대응이 불가능하였다고 주장함

□ 이에 대해 위원회는 펨토셀은 단순한 말단 통신장비가 아닌 이동통신 서비스를 이용하기 위해 반드시 경유해야 하는 필수적인 장비로 펨토셀 장비에 대한 관리 부실 및 펨토셀을 통한 내부망 접속에 대한 접근통제 미흡으로 발생한 사고라는 점에서 안전조치의무 준수시 충분히 예방이 가능한 사고이며,

○ 펨토셀을 통한 해킹 공격은 해외사례 및 학계에서 보안 취약점에 대한 지적이 지속적으로 제기되어온 사안으로 판단함

4. KT 고발과 LGU+ 수사의뢰 차이가 발생하는 이유는?

□ KT의 경우 위원회 **조사착수 이후**, 위원회 조사과정에서 거짓 자료 제출 등을 통해 위원회 조사를 방해한 행위에 해당하여 **보호법 제73조(벌칙)** 및 '개인정보 보호 법규 위반에 대한 **고발기준'에 따라 고발**하기로 결정하였음

○ 다만, LGU+의 경우, 위원회 **조사착수 전** 서버 폐기 등 증거 은닉·폐기가 이루어져 보호법상 조사방해 요건에 해당하지 않아, 형법상 공무집행 방해로 수사기관에 수사 의뢰하기로 함

□ 아울러, 위원회는 이러한 **규제 사각지대 및 행정조사의 한계**를 인지하고, 조사실효성 확보를 위한 제도개선을 추진 중에 있음

5. 증거 은닉·폐기 과징금 등 제도개선 계획은?

□ 개인정보 침해 사고 발생 시, 조사 실효성 강화를 위해 **증거 은닉·폐기에 대한 제재 규정** 및 **이행강제금·증거보전명령 제도 도입**을 추진하고 있음

○ 이행강제금·증거보전명령 도입 관련 법안은 이미 국회에 발의*되어 있으며,

* 한정애·김용만·박범계 의원안('26.2.12.발의) / 한창민 의원안('26.4.9.발의)

○ 증거 은닉·폐기 제재규정 관련 법안은 하반기 국회 통과를 목표로 현재 발의를 추진하고 있음

□ 관련 법안이 연내에 통과될 수 있도록 하여, 향후 개인정보 유출 사고 발생 시 신속한 조사를 통해 정보주체의 권리가 보호될 수 있도록 하겠음