개인정보보호위원회 보도자료 다시 대한민국! 새로운 국민의 나라

보도시점 2024. 5. 23.(목) 12:00 배포 2024. 5. 22.(수) 19:00

개인정보위, ㈜카카오에 과징금 151억 원, 과태료 780만 원 부과

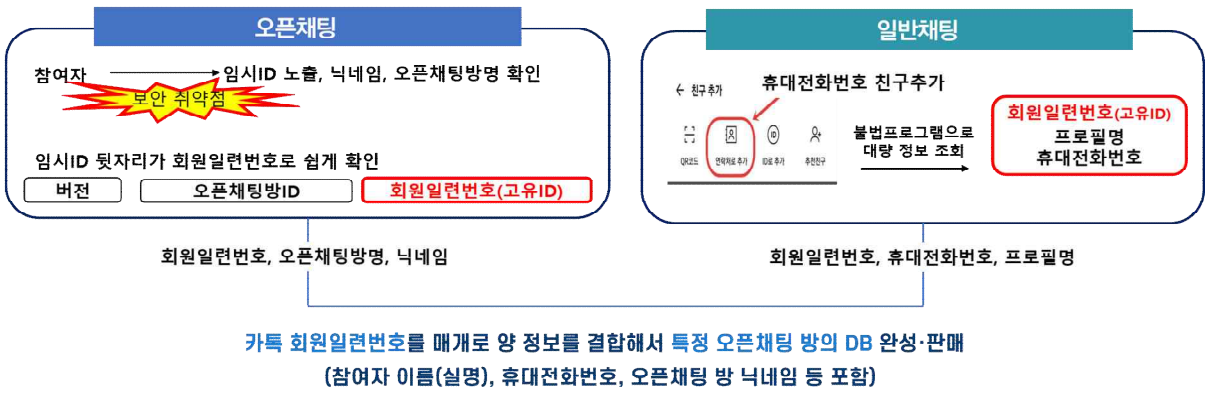
- 지난해 발생한 오픈채팅 이용자 개인정보 유출사고 관련
- 안전조치 의무위반 및 유출 신고·피해자 통지 소홀 등에 대해 제재, 시정명령과 결과 공표도 함께 처분

개인정보보호위원회(위원장 고학수, 이하 '개인정보위')는 5월 22일(수) 제9회 전체회의를 열고, 개인정보보호 법규를 위반한 ㈜카카오에 대해 151억 4,196만 원의 과징금과 780만 원의 과태료를 부과하고, 시정명령과 처분결과를 공표하기로 의결하였다.

개인정보위는 지난해 3월 카카오톡 오픈채팅 이용자의 개인정보가 불법 거래되고 있다는 언론보도에 따라 개인정보 보호법 위반 여부를 조사하였다.

조사 결과, 해커는 오픈채팅방의 취약점을 이용해 오픈채팅방 참여자 정보를 획득했고, 카카오톡의 친구추가 기능과 불법 프로그램 등을 이용해 이용자 정보를 확보하였으며, 이들 정보를 '회원일련번호'를 기준으로 결합해 개인정보 파일을 생성, 판매한 것으로 확인되었다.

< 개인정보 유출 과정 >



개인정보위는 ㈜카카오가 카카오톡 서비스를 제공하는 과정에서 다음과 같은 위반 사실을 확인하였다.

< 안전조치의무 위반 >

먼저, ㈜카카오는 익명채팅이라고 홍보하며 오픈채팅 서비스를 운영하였는데, 일반채팅과 오픈채팅을 이용하는 이용자를 동일한 회원일련번호로 식별할 수 있게 이용자 식별체계를 구현하였다. 다만, 오픈채팅 참여자는 오픈채팅방 정보(오픈채팅방 ID)와 회원일련번호로 구성한 임시ID를 메시지 송수신시 사용하였다.

’20. 8월 이전에 생성된 오픈채팅방은 참여자의 임시ID를 암호화하지 않아, 임시ID에서 회원일련번호를 쉽게 확인할 수 있었다.

또, ’20. 8월 이후에 생성된 오픈채팅방은 임시ID를 암호화하였지만, 오픈채팅방 게시판에 암호화된 임시ID를 입력하면 암호화를 해제하고 평문으로 임시ID를 노출하는 취약점이 있어, 참여자의 암호화된 임시ID도 쉽게 회원일련번호를 확인할 수 있었다.

이와 같이, ㈜카카오는 카카오톡 서비스 설계·운영 과정에서 회원일련번호와 임시ID가 연계되어 오픈채팅의 익명성이 훼손 또는 개인정보 노출될 가능성이 있음에도 그에 대한 검토와 개선 조치를 소홀히 한 것이다. 마찬가지로, 오픈채팅방 게시판에 있던 보안 취약점에 대한 점검과 개선조치를 소홀히 하였다.

회원일련번호 연계에 따른 익명성 훼손을 방지하려면 오픈채팅 이용자는 일반채팅과 다른 식별체계로 구성하거나, 임시ID를 암호화해 회원일련번호가 노출되지 않도록 하는 방법 등이 가능하다. ㈜카카오는 지난해 사고 발생 이후 모든 오픈채팅방 참여자의 임시ID를 암호화하였다.

또, 카카오톡 전송방식을 분석한 공개된 API를 이용하면 이용자 정보 추출 등이 가능하다는 지적이 개발자 커뮤니티 등에 공개되어 왔음에도 불구하고, ㈜카카오는 관련 내용이 카카오톡 서비스에 비치는 영향, 개인정보 유출 등 피해 가능성에 대한 검토와 개선 조치도 미흡하였다.

오픈채팅 서비스 설계·구현 과정에서의 과실과 카카오톡 전송방식을 분석해서 만든 해킹 프로그램을 이용한 악성행위에 대한 대응조치 미흡 등으로 인해서 ㈜카카오가 처리 중인 개인정보가 해커에게 공개·유출되었고, 따라서 ㈜카카오는 개인정보 보호법의 안전조치 의무를 위반하였다.

< 유출 신고·통지 의무 위반 >

또한, ㈜카카오는 '23. 3월 언론보도 및 개인정보위 조사과정에서 카카오톡 오픈채팅방 이용자의 개인정보가 유출되고 있다는 사실을 인지했음에도 유출 신고와 이용자 대상 유출 통지를 하지 않아 개인정보 보호법을 위반하였다.

개인정보위는 이용자 개인정보가 유출된 ㈜카카오에 대해 안전조치의무 위반으로 과징금을 부과하고, 유출 신고·통지의무 위반 등에 대해서는 과태료를 부과하기로 결정하였다.

또, ㈜카카오에 이용자 대상 유출 통지를 할 것을 시정명령하는 동시에, 개인정보위 홈페이지에 처분 결과를 공표하기로 결정하였다.

이번 처분을 계기로 카카오톡과 같이 대다수 국민이 이용하는 서비스의 경우 보안 취약점을 상시적으로 점검·개선하는 한편 설계·개발 과정에서 발생할 수 있는 개인정보 침해 가능성에 대해서도 지속적인 점검과 노력이 필수적이라는 인식이 자리잡기를 기대한다고 개인정보위는 밝혔다.

[붙임] 위반내용 및 시정조치

담당 부서 <총 괄>	개인정보보호위원회 조사2과	책임자	과 장	김해숙 (02-2100-3121)
		담당자	조사관	허재형 (02-2100-3129)
<공 동>	한국인터넷진흥원 플랫폼조사팀	책임자	팀 장	문봉주 (061-820-1496)
		담당자	선 임	한상원 (061-820-1418)

붙 임 위반내용 및 시정조치

사업자명	위반 내용	위반 조항	시정조치(안)
㈜카카오	• 안전조치의무 위반 • 개인정보 유출 신고·통지 의무 위반	舊 보호법* §29 §39의4①	• 과징금 151억 4,196만 원 • 과태료 780만 원 • 시정명령 • 결과공표

* 법률 제16930호, 2020. 8. 5. 시행