개인정보보호위원회 | 보도자료 | 대체불가 대한민국

보도시점 2026. 7. 8.(수) 10:00 배포 2026. 7. 8.(수) 7:30

개인정보위, 응용프로그램 인터페이스(API) 활용 확대에 따른 개인정보 유출 예방 당부

- 응용프로그램 인터페이스 기획·설계 단계부터 개인정보 최소화, 기본 차단 원칙 적용
- 서비스 변경 시에도 개인정보 필요 여부를 한번 더 점검하고 변경

개인정보보호위원회(위원장 송경희, 이하 '개인정보위')는 웹·앱 서비스 고도화, 플랫폼 연계, 제휴사 서비스 연동 등에서 응용프로그램 인터페이스(Application Programming Interface, 'API')를 통한 데이터 처리가 확대*됨에 따라, 이를 통한 개인정보 처리시 권한 관리와 개인정보 최소 전송 등 보호조치를 강화할 것을 사업자에게 당부했다.

* 트래픽 관리 서비스 '클라우드플레어' 처리 트래픽 기준 API가 57% 비중 차지

최근 국내외에서 권한 관리가 미흡한 API를 통한 개인정보 유출 사고가 잇따라 발생하고 있다. 로그인 여부만 확인하고 개인정보 조회 권한을 확인하지 않거나, 서비스 제공에 필요하지 않은 개인정보까지 API 응답 데이터에 포함하는 경우, 비정상적인 API 호출만으로도 대규모 개인정보 유출로 이어질 수 있다. 따라서, 사업자는 현재 운영 중인 API를 지속적으로 식별, 관리하고 개인정보를 처리하는 API는 이용자, 취급자, 고객사 등 권한 범위에 따라 접근을 제한하는 등 API 운영 전반에 대한 점검이 필요하다.

< API 권한 관리 미흡으로 인한 개인정보 유출 사례 >

▶ (A사) 권한 관리가 이루어지지 않은 API에 대한 비정상 접근으로 약 3,700만여명의 이름, 주소, 이메일, 전화번호, 생년월일 등 유출
▶ (B사) 개인정보 보호를 위해 이용자의 휴대전화번호 대신 안심번호만 전송하는 것으로 정책을 변경했으나, 실제 API는 휴대전화번호도 함께 전송하고 있었고, 타사 시스템에 약 13.5만여명의 이용자 개인정보가 보관된 사실도 확인됨
▶ (C사) 최신 API는 다중 인증 방식(MFA) 등으로 권한 관리가 이루어지고 있었으나, 계속 동작하는 오래된 API를 통해 별도 권한 확인 없이 고객 데이터 조회 가능하였음

이에 개인정보위는 API를 통해 개인정보를 처리하는 사업자에게 다음 사항을 중점적으로 점검하고 조치할 것을 권고했다.

첫째, 설계 단계부터 **개인정보 최소화 원칙을 준수**해야 한다.

○ 이용자 화면에서 보이지 않는 개인정보나 서비스 제공 목적에 필요하지 않은 정보는 **API 응답 데이터에서도 제외하도록 설계**

○ API로 **대규모 정보 조회 또는 반복 호출** 등을 **제한**하여 대규모 개인정보 조회·유출 방지

둘째, 최소 권한 원칙에 부합하게 **API 권한을 부여하고 관리**해야 한다.

○ 이용자용, 관리자용, 제휴 협력사용 등 주체별로 접근 가능한 API와 개인정보 범위를 **필요 최소한으로 차등 부여**

○ 인증·권한이 없거나 정책에 맞지 않는 요청은 **기본적으로 차단 설정**

○ **모든 API 요청에 대해** 요청한 이용자가 해당 개인정보를 조회하거나 수정할 **권한이 있는지 서버에서 확인**

○ **접근 가능한 정보**도 기간 경과 후에는 **일부 비식별 처리** 등 추가 조치

셋째, **운영 중인 API 목록을 식별, 현행화**하고 **점검**해야 한다.

○ 기능 개선, 테스트 완료 또는 서비스 개편 후 **외부에서 호출 가능한 API가 남아 있는지, 불필요 정보가 API 응답에 포함되지 않았는지 점검**하고 **불필요 정보 등 삭제 조치**

○ API 권한을 정기 점검하여 **장기 미사용 API 키·토큰·계정 등 자격증명은 즉시 회수**

○ **접속기록을 점검**하며 새벽시간 접속, 대량 조회 등 **이상행위 탐지·대응**

아울러 API를 제공받아 서비스를 운영하는 사업자도 응답 데이터에 서비스와 무관한 개인정보가 포함되어 있는지 확인하고 불필요한 개인정보는 즉시 제거해야 한다. API 키·토큰 등 자격증명은 담당자별로 발급하고 최소 권한 원칙에 따라 API로 조회·전송받는 데이터 범위를 제한하거나, 업무 절차나 시기에 따라 조회할 수 있는 개인정보를 제한하는 등 안전하게 관리하는 것이 바람직하다.

양청삼 개인정보위 사무처장은 “API는 서비스 화면에 표시되지 않는 개인정보도 함께 전송할 수 있으므로 서비스 제공에 필요한 최소한의 개인정보만 처리되도록 설계하고 운영해야 한다”라고 말했다.

담당 부서	예방조정심의관	책임자	과 장	김해숙 (02-2100-3060)
	사전실태점검과	담당자	사무관	전이루 (02-2100-2448)

붙임 | **API 제공 사업자 개인정보 보호 수칙 및 점검사항**

개인정보 유출 예방을 위한

API 권한 관리 점검사항

개인정보보호위원회

1 개인정보 최소화

API가 반환하는 개인정보 항목과 제공 규모를 줄입니다.

필요한 데이터만 응답

화면에 보여주지 않거나
목적에 필요 없는 개인정보는
API 응답 데이터에서 제외

대량조회·응답량 제한

계정, IP, 자격증명 등을 기준으로
반복 호출, 대량 검색 등에 제한을 두어
대규모 개인정보 조회·유출 등 방지

2 최소 권한 기반 접근통제

허용된 주체·기능·범위만 개인정보에 접근하도록 합니다.

접근범위 분리

이용자, 취급자, 고객사 등
주체별로 사용 가능한 API 및
개인정보 항목을 필요 최소한의
범위로 차등 부여

기본 차단

로그인 여부만 확인하는
것으로는 충분하지 않으며,
권한 정책을 따르지 않는
비정상 요청은 기본적으로 차단

서버 권한검사

이용자 화면에서
보이지 않는 것만으로는
충분하지 않으며, 서버에서 요청
데이터에 대한 접속 권한 확인

3 운영 API 지속 점검

운영 현황, 자격증명, 접속기록을 주기적으로 확인합니다.

오래된 API 관리

서비스 개편,
기능 종료 후 남아 있는
구버전·미사용 API
차단 또는 폐기

자격증명 회수

장기 미사용
API 키·토큰 등
자격증명 및 권한
정기적으로 점검 및 회수

이상징후 대응

접속기록을 점검하고
대량조회·반복 실패, 새벽시간 등
업무 외 시간 접속, 외국 등에서의
접속 등 비정상 패턴 탐지