**구글·메타 개인정보 과징금 , 빅테크 규제 범위를 가늠할 항소심**

2022 년 9 월, 개인정보보호위원회는 구글과 메타가 이용자의 동의 없이 행태정보를 수집해 맞춤형 광고에 활용한 사실을 적발하고, 개인정보보호법 위반으로 역대 최대 규모인 1,000 억 원대 과징금을 부과했다. 구글에 692 억 원, 메타에 308 억 원이 각각 부과됐으며, 두 회사는 이에 불복해 처분 취소를 구하는 행정소송을 제기했다. 2025 년 1 월 23 일 1 심에서는 개인정보위가 승소했고, 현재 2 심이 진행 중이다.

개인정보위에 따르면 구글과 메타는 이용자가 자사 플랫폼 밖에서 활동한 정보, 즉 쿠팡·11 번가 등 메타의 픽셀, SDK, 페이스북 로그인, 소셜 플러그인 등이 설치된 다수의 사업자 웹사이트와 앱에서 발생한 타사 행태정보를 이용자의 단말기에서 수집해 맞춤형 광고에 활용했다. 또한 이러한 수집 사실을 이용자에게 명확히 알리지 않았고, 사전 동의도 받지 않았다. 구글과 메타는 정보 수집 동의의 주체가 자신들이 아니라 웹사이트·애플리케이션 운영 사업자라고 주장하지만, 개인정보위는 이들 회사가 실질적인 수집·이용 주체라고 본다.

행태정보에는 웹사이트 방문 기록, 앱 설치·사용 이력 등 온라인 활동 기록이 포함된다. 동의 절차 역시 문제로 지적됐다. 구글은 '옵션 더보기'를 숨겨 동의를 기본값처럼 유도했고, 메타는 694 줄에 달하는 관련 내용을 한 화면에 5 줄만 보이도록 구성해 형식적인 동의를 받았다는 비판을 받았다. 이에 대해 구글과 메타는 웹사이트 또는 앱 운영 사업자가 개인정보 수집 주체이므로 이용자의 동의를 받아야 하며, 설령 자신들이 동의받아야 하는 주체라고 하더라도 개인정보 처리방침 등을 통해 충분히 알리고 동의를 받았다고 반박하고 있다.

메타의 글로벌 제재 이력도 이 문제의 연장선에 있다. 2020 년 한국에서는 이용자 동의 없이 제 3 자에게 개인정보를 제공한 사건으로 67 억 원의 과징금을 부과받았고, 대법원은 2025 년 이를 적법하다고 최종 확정했다. 2021 년에는 얼굴인식 템플릿을 동의 없이 생성·수집한 행위로 64 억 원대 과징금이 부과됐으며, 이는 생체정보 역시 강하게 보호된다는 점을 보여준다. 2022 년 미국 텍사스주가 메타의 얼굴인식 기술 사용을 문제 삼아 소송을 제기했고, 메타는 2024 년 14 억 달러, 약 2 조 원에 합의했다. 같은 흐름에서 미국 일리노이주도 안면인식 데이터 무단 수집을 이유로 집단소송을 제기해 2020 년

6 억 5 천만 달러에 합의했으며, 메타의 프라이버시 리스크가 특정 국가에 국한되지 않고 여러 법역에서 반복적으로 현실화되고 있음을 보여준다.

개별 위반행위별로 과징금이 부과되는 구조이기 때문에, 2020 년 한국의 과징금 규모는 2022 년 텍사스주 합의액에 비해 상대적으로 작지만, 법 위반 인정과 시정명령이 분명하다는 점에서 의미가 크다.

2025 년 6 월 11 일에는 구글이 개인정보위를 상대로 과징금과 시정명령 처분 취소를 구한 소송의 2 심 첫 변론이 열릴 예정이다. 이 소송은 국내 개인정보보호법이 미국 빅테크에 실제로 적용될 수 있는지를 가늠하는 사건으로, 2 심 결과는 향후 빅테크 규제의 중요한 선례가 될 가능성이 높다. 개인정보위가 승소할 경우 국내 플랫폼 기업 전반에 규제 강화와 동의 절차 개선 압박이 커지고, 개인정보위의 규제 권위도 한층 강화될 것으로 보인다. 반대로 일부 감액이 이뤄지면 규제 강도는 다소 완화되겠지만, 개인정보위는 일정한 규제 입지를 유지하며 기업과 정부 간의 긴장도도 완만해질 가능성이 있다. 만약 빅테크가 승소한다면 규제 경직성은 완화되겠지만, 개인정보 규제 전반에 대한 신뢰와 집행력에는 적지 않은 영향을 줄 수 있다.

여러 나라의 규제가 시사하는 바는, 개인정보 보호가 더 이상 한 나라의 로컬 규범이 아니라 글로벌 비즈니스의 기본 인프라가 되었다는 점이다. 국가마다 방식은 다르지만 공통적으로 동의의 실질성, 목적 제한, 최소 수집, 투명성, 책임성을 핵심 원칙으로 삼고 있다. 결국 이러한 규제는 억압을 위한 장치가 아니라 소비자와 자국민을 보호하기 위한 필수 수단이며, 기존의 사후 대응형 규제에서 벗어나 선제적 규제 체계를 만드는 계기가 될 수 있다. 그런 점에서 이번 2 심은 단순한 금전 분쟁을 넘어, 향후 개인정보 규제의 방향을 가늠하는 중요한 분기점으로 주목할 필요가 있다.

**Korea's Record Privacy Penalty Against Google and Meta Heads to Appeal**

In September 2022, the Personal Information Protection Commission (PIPC) found that Google and Meta had collected behavioral data without users' consent and used it for targeted advertising. As a result, the commission-imposed fines totaling approximately KRW 100 billion—the largest penalty ever under the Personal Information Protection Act. Google was fined KRW 69.2 billion, and Meta KRW 30.8 billion. Both companies challenged the decision and filed administrative lawsuits seeking to revoke the sanctions. On January 23, 2025, the PIPC prevailed in the first-instance ruling, and the case is currently under appeal.

According to the PIPC, Google and Meta collected and used third-party behavioral data generated from users' activities outside their own platforms. This included data gathered through Meta Pixel, SDKs, Facebook Login, and social plugins installed on numerous third-party websites and apps such as Coupang and 11st. The companies collected this information from users' devices and used it for targeted advertising. They neither clearly informed users of such data collection nor obtained prior consent. While Google and Meta argue that website and app operators are the entities responsible for obtaining user consent, the PIPC considers the two companies to be the substantive entities responsible for data collection and use.

Behavioral data includes records of online activities such as website visits and app installation and usage history. The consent procedures themselves were also criticized. Google was found to have effectively nudged users toward consent by hiding the "more options" feature, while Meta displayed only five lines of a 694-line disclosure on a single screen, resulting in what critics described as merely formal consent. In response, Google and Meta maintain that website or app operators are responsible for obtaining user consent, and that even if they themselves were required to obtain consent, they had sufficiently informed users and obtained consent through their privacy policies.

Meta's global enforcement history reflects a continuation of these issues. In 2020, South Korea imposed a KRW 6.7 billion fine for providing personal data to third parties without user consent, and the Supreme Court upheld the decision as lawful in 2025. In 2021, Meta was fined approximately KRW 6.4 billion for generating and collecting facial recognition templates without consent, demonstrating that biometric data is also subject to strong protection. In 2022, the U.S. state of Texas filed a lawsuit over Meta's use of facial recognition technology, which was settled in 2024 for USD 1.4 billion (approximately KRW 2 trillion). Similarly, in Illinois, a class action lawsuit over unauthorized collection of facial recognition data was settled in 2020 for USD 650 million. These cases show that Meta's privacy risks are not confined to a single jurisdiction but have repeatedly materialized across multiple legal systems.

Because fines are imposed per violation, the scale of Korea's 2020 penalty is relatively small compared to the Texas settlement in 2022. However, it is significant in that it clearly established legal violations and corrective orders.

On June 11, 2025, the first hearing of the second-instance trial in Google's lawsuit seeking to revoke the PIPC's fines and corrective orders is scheduled to take place. This case is expected to serve as a key test of whether Korea's Personal Information Protection Act can be effectively

applied to U.S. Big Tech companies. The outcome of the appeal is likely to become an important precedent for future regulation of Big Tech. If the PIPC prevails, regulatory pressure on domestic platform companies will increase, particularly in strengthening consent procedures, and the authority of the PIPC will be further reinforced. If the fines are partially reduced, regulatory intensity may be somewhat eased, while the PIPC would still retain a certain level of regulatory standing, potentially reducing tensions between companies and the government. If Big Tech prevails, regulatory rigidity may be relaxed, but this could significantly affect trust in and enforcement of personal data protection overall.

What regulations across various countries suggest is that personal data protection is no longer a local norm confined to a single country but has become a fundamental infrastructure of global business. Although approaches differ by country, core principles consistently include meaningful consent, purpose limitation, data minimization, transparency, and accountability. Ultimately, such regulations are not tools of suppression but essential mechanisms to protect consumers and citizens. They also provide an opportunity to move away from reactive regulatory approaches toward more proactive frameworks. In this regard, the current appellate case should be seen not merely as a financial dispute, but as a critical turning point in determining the future direction of personal data regulation.