Updates
June 11, 2018
Use a Third-Party Platform? You Might Be a “Data Controller”

The European Union's top court ruled last week that the operator of a Facebook fan page is a "joint controller," along with Facebook, with respect to personal data collected on such pages. The decision has implications for the countless businesses who administer pages through third-party platforms.

The case concerns a German educational firm that ran a fan page on Facebook that placed cookies on visitors to that page. The educational firm was ordered by a local data protection authority to deactivate the page because, it alleged, neither the firm nor Facebook had informed users their personal data was being collected via those cookies. The firm objected, arguing that it had not processed or directed the processing of personal data. The German courts split on the core issue of whether the educational firm acted as a controller, and the courts certified several questions in that regard to the Court of Justice of the European Union (CJEU).

In reaching its decision, the CJEU reasoned that a page administrator acts as a data controller because it takes part "in the determination of the purposes and means of processing personal data of the visitors to its fan page," noting the firm's role in setting up the page as well as the anonymized demographic data that the firm could request. (By way of background, an organization acts as a controller when it determines 'why' and 'how' personal data should be processed. Organizations may act as 'joint controllers,' but under the General Data Protection Regulation (GDPR), they must enter into an arrangement setting out their respective responsibilities for complying with data protection rules.) Ultimately, the court determined that the firm could not benefit from the platform's service while also avoiding compliance obligations.

This ruling serves as an important reminder that companies may have compliance obligations even when collecting personal data solely through platforms provided by others and even when they have minimal say in the type of data collected on those platforms or insight into the data collected on them. The cost of noncompliance is high—it can run as much as €20 million or 4 percent of an organization's worldwide annual revenue.

Authors

Explore more in

General Data Protection Regulation (GDPR) Privacy & Security Technology Transactions & Privacy Law

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law