LEGAL ALERTS | AUG 13, 2018

Public Agencies and GDPR Compliance

Government Entities Should Evaluate Data Collection and Use Practices

The European Union's General Data Protection Regulation (commonly known as GDPR) has broad implications that reach even local public agencies in the United States. GDPR, which took effect May 25, is a sweeping global privacy law that for many entities transforms the way personal data must be collected, processed, stored and shared.

Do Public Agencies Need to Comply with GDPR?

Privacy Law Applies to Government Agencies that "Process" Certain Personal Data

Public agencies in the U.S. that engage in certain data collection, use and storage practices with respect to people in the EU are expected to comply with GDPR — and may face consequences for failing to do so. GDPR provides new privacy rights to natural persons in the EU, including the rights to require the deletion of personal data, obtain a restriction on the processing of their personal data and, in certain instances, obtain personal data held by an entity regulated by GDPR. Further, GDPR places substantive data security, transparency, and breach notification requirements on those entities under its purview—along with many other compliance requirements designed to regulate the use and transfer of personal data.

GDPR applies to the collection of "personal data," which is defined broadly as "any information relating to an identified or identifiable natural person." Personal data includes a data subject's name, identification numbers, location data and online identifiers such as an IP address, cookie or an RFID tag. GDPR also includes "special" data categories, like genetic and biometric data.

While its impact on private companies is being broadly discussed, little attention has been paid to public authorities that fall within its scope.

People

Leeann Habte
PARTNER
(213) 787-2572

Todd R. Leishman
OF COUNSEL
(949) 263-6576

Related Practices

- ARC: Advanced Records Center
- Health Care
- Telecommunications

Related Industries

- Education
- Health Care
- Municipal
- Special Districts

Unlike its predecessor, the European Union Data Privacy Directive, GDPR's "territorial scope" reaches certain private entities and "public authorities" *outside the EU* — including federal, state and local government agencies. For a public authority or private entity in the United States, GDPR will apply in two instances:

1. Where the entity processes personal data of natural persons *in the EU* (including the United Kingdom) where the processing relates to "the offering of goods or services," even if no payment is required or
2. Where the entity's processing of personal data relates to monitoring a person's behavior *as far as that behavior takes place in the EU.*

When Might Public Agencies Fall Under GDPR?

Many public agencies in the United States might "process" data within the scope of GDPR .

Processing Related to Offering Goods and Services to People in the EU

Regarding whether processing relates to "the offering of goods or services" to individuals in the EU, GDPR provides some guidance as to what factors a court might consider when deciding whether a U.S. public or private entity has made such an "offer." For example, a court might consider whether advertised goods or services can be purchased in an EU Member State language and/or currency, or whether the context of the advertisement is clearly designed to reach an overseas audience—but overall there are no bright line rules.

A local public agency might process data within the meaning of GDPR by, for example:

- Hosting tourism websites (i.e., websites for conference centers, hotels or special events) with content advertising to a global or EU audience.
- Providing an option to purchase certain goods (i.e., tickets or hotel bookings) in an EU Member State currency or language.
- Publishing testimonials of EU residents or organizations that have used the advertised goods or services

Processing Related to Monitoring Behavior in the EU

If a public agency is collecting information on EU residents through advertising or online tracking operations, the agency is likely processing "personal data" under GDPR. If a public agency gathers personal data through a website or a mobile app, or provides a third party with access to personal data it gathers through such sources, it may be wise to investigate as to whether any persons in the EU are "monitored" within the meaning of GDPR. GDPR does not define "monitoring," but its accompanying regulations indicate that monitoring occurs when "natural persons are tracked on the internet." This includes the use of personal data processing techniques like "profiling" a person, which may entail

analyzing or predicting his or her personal preferences, behaviors and attitudes based on the personal data gathered. Far less technical practices, however, appear to constitute “monitoring” within the meaning of GDPR.
It is possible a public agency is “monitoring” people in the EU by:

- Utilizing website analytics tools or behavior-based ad-retargeting programs,
- Employing tracking technology, such as using cookies on a website or collecting a visitor’s IP address,
- Profiling users for fraud prevention purposes,
- Engaging in location-based data gathering (for instance, through a mobile app associated with a particular local authority, or an app connected with a third-party offering services in partnership with the local authority, such as a bike-share program) or
- Passing on personal data to third parties for monitoring or profiling purposes.

Since GDPR applies when these actions are taken with respect to behavior “in the EU,” it appears to protect every person there regardless of their nationality or domicile. This may mean a US citizen is endowed with new rights when in the EU, and adds another layer of complication to compliance efforts.

What Should Public Agencies Do to Facilitate Compliance?
GDPR, in many instances, raises more questions than it answers. Deloitte recently reported that a scant 35 percent of nearly 500 professionals involved in GDPR compliance efforts say their organizations can defensibly demonstrate compliance today. Public agencies should view GDPR as a call to action, and an opportunity to increase and clarify internal controls and policies for data gathering, use and storage activities. Key decision-makers should be made aware of potential GDPR compliance obligations. As public authorities increasingly gather and utilize data for official and commercial purposes — including in partnership with private third-party entities — GDPR compliance will likely comprise an important step toward institutionalizing appropriate privacy and data security practices.

GDPR has established new norms for privacy and data security that have already shaped California law and public perception regarding privacy rights. For example, in June, Gov. Jerry Brown signed into law Assembly Bill 375, the California Consumer Privacy Act of 2018. The Act is designed to grant California residents additional privacy rights and increase consumer control over the collection, purchase and sale of their personal information. The Act, which goes into effect in 2020, does not appear to apply to local governments. But, it otherwise borrows heavily from GDPR, requiring businesses to disclose the categories of collected personal information, explain why it is shared, to delete collected personal information on request and, generally, to allow consumers to “opt out” of any data collection and sale programs without penalty.

Privacy laws are evolving at a rapid clip, and local governments must diligently assess compliance obligations. For more information about GDPR and privacy

compliance, please contact the authors of this Legal Alert listed at right in the firm's Telecommunications and Business practice groups, or your BB&K attorney.

Please feel free to share this Legal Alert or subscribe by clicking here. Follow us on Facebook @BestBestKrieger and on Twitter @BBKlaw.

Disclaimer: BB&K Legal Alerts are not intended as legal advice. Additional facts or future developments may affect subjects contained herein. Seek the advice of an attorney before acting or relying upon any information in this communiqué.