THE
NATIONAL LAW REVIEW

The GDPR – One Year and Counting

jackson lewis.

Article By
Mary T. Costigan
Joseph J. Lazzarotti
Jason C. Gavejian
Jackson Lewis P.C.
Workplace Privacy Blog

- Administrative & Regulatory
- Communications, Media & Internet
- Global

- All Federal
- European Union

Tuesday, May 28, 2019

The GDPR is wrapping up its first year and moving full steam ahead. This principles-based regulation has had a global impact on organizations as well as individuals. While there continue to be many questions about its application and scope, anticipated European Data Protection Board guidance and Data Protection Authority enforcement activity should provide further clarity in the upcoming year. In the meantime, here are a few frequently asked questions – some reminders of key principles under the GDPR and others addressing challenges for implementation and what lies ahead.

Can US organizations be subject to the jurisdiction of the GDPR?

Whether a US organization is subject to the GDPR is a fact-based determination. Jurisdiction may apply where the US organization has human or technical resources located in the EU and processes EU personal data in the context of activities performed by those resources. In cases where the US organization does not have human or technical resources located in the EU, it may be subject to the GDPR's jurisdiction in two instances: if the organization targets individuals in the EU (not businesses) by offering goods or services to them, regardless of whether payment is required, or if it monitors the behavior of individuals in the EU and uses that personal data for purposes such as profiling (e.g. website cookies, wearable devices). The GDPR may also apply indirectly to a US organization through a data processing agreement.

If we execute a data processing agreement, does that make our US organization subject to the GDPR?

When an organization subject to the GDPR engages a third party to process its EU data, the GDPR requires that the organization impose contractual obligations on the third party to implement certain GDPR-based safeguards. If you are not otherwise subject to the GDPR, executing a data processing agreement will not directly subject you to the GDPR. Instead, it will contractually obligate you to follow a limited, specific set of GDPR-based provisions. Your GDPR-based obligations will be indirect in that they are contractual in nature.

Does the GDPR apply only to the data of EU citizens?

No, the GDPR applies to the processing of the personal data of data subjects who are in the EU regardless of their nationality or residence.

Is our organization subject to the GDPR if EU individuals access our website and make purchases?

If your organization does not have human or technical resources in the EU, the mere accessibility of your website to EU visitors, alone, will not subject you to the GDPR. However, if your website is designed to *target* EU individuals (e.g. through features such as translation to local language, currency converters, local contact information, references to EU purchasers, or other accommodations for EU individuals) your activities may be viewed as targeting individuals in the EU and subject you to the GDPR.

Are we required to delete an individual's personal data if they request it?

If your organization is subject to the GDPR, an individual may request that you delete their personal data. However, this is not an absolute right. Your organization is not required to delete the individual's personal data if it is necessary

- for compliance with a legal obligation or the establishment, exercise or defense of a legal claim
- for reasons of public interest (e.g. public health, scientific, statistical or historical research purposes)
- to exercise the right of freedom of expression or information
- where there is a legal obligation to keep the data
- or where you have anonymized the data.

Additional consideration should be given to any response when the individual's data is also contained in your back-ups.

GDPR principles have started to influence law in the U.S. In fact, many have

been watching developments regarding the California Consumer Privacy Act (CCPA), which shares a right to delete as it pertains to the personal information of a California resident. Similar to the GDPR, it is not an absolute right and in certain cases, an exception may apply. For instances, both laws contain an exception from the right to have personal information deleted when the information is needed to comply with certain laws.

Does the GDPR apply to an EU citizen who works in the US?

If your organization is not subject to the GDPR and you hire an EU citizen to work in the US, the GDPR may not apply to the processing of their personal data in the US. However, depending on the circumstances, the answer may be different if the EU citizen is in the US on temporary assignment from an EU parent. In that scenario, their data may be subject to the GDPR if the US entity's relationship with the parent creates an establishment in the EU, and it processes this data in the context of the activities of that establishment. To the extent the EU parent transfers the EU employee's personal data from the EU to the US entity, that transfer may require EU-US Privacy Shield certification, the execution of binding corporate rules, or standard contractual clauses. These measures are designed to ensure data is protected when it is transferred to a country, such as the US, that is not deemed to have reasonable safeguards.

Do we need to obtain an EU individual's consent every time we collect their personal data?

If your organization is subject to the GDPR and processes an EU individual's information, you must have a "legal basis" to do so. Consent is just one legal basis. In addition to consent, two of the most commonly used legal basis are the "legitimate interests" of your organization and the performance of a contract with the individual. A legitimate interest is a business or operational need that is not outweighed by the individual's rights (e.g. processing personal data for website security, conducting background checks, or coordinating travel arrangements). Processing necessary to the performance of a contract is activity that enables you to perform a contract entered into with the individual (e.g. processing employee data for payroll pursuant to the employment contract or processing consumer data for shipping goods under a purchase order.)

Should we obtain an employee's consent to process their personal data?

The GDPR requires that the individual's consent be freely given, specific, informed, and revocable. Due to nature of the employment relationship, employers should rely on a legal basis other than consent for processing the employee's personal data, where possible. When there is an imbalance of power between the party obtaining the consent and the individual giving it (as is regularly the case in the employment relationship), it is likely that the consent is not freely given and thus not valid. Employers should review whether alternative legal bases for processing apply, such as legitimate interest, performance of the employment contract, or compliance with a legal obligation.

Does the GDPR have specific security requirements?

The GDPR is a privacy regulation and while it does not include specific security standards, it does require the implementation of technical and organizational measures designed to provide a level of security appropriate to the risks. This may include, where appropriate, adopting and implementing internal policies and procedures to minimize the processing of personal data; pseudonymizing or encrypting personal data; ensuring the confidentiality, integrity, availability and resilience of your processing systems and services; maintaining data backups and an incident response plan; and adopting a process to regularly test, assess and evaluate these measures.

What impact has the GDPR had in its first year?

EU Data Protection Authorities saw a significant increase in the public's awareness of data privacy as they fielded over 144,000 questions and complaints regarding individual rights. This awareness further resulted in organizations reporting approximately 89,000 data breaches. In the UK, the Information Commissioner's Office determined that one-third of reported incidents did not trigger a notification obligation, suggesting that over-reporting is a concern. In order to avoid undertaking unnecessary response activity, incurring needless costs, and causing employees or customers undue concern, organizations should consider consulting counsel to identify whether an incident is reportable.

DPAs have brought enforcement actions against organizations of all sizes and issued a number of fines for violations including failing to secure users' data, lack of consent for advertisements, failing to inform citizens that their data was being processed, unlawful video surveillance, and failing to implement necessary security for data processing. Each of these actions has provided greater understanding of how the GDPR should be applied and what the DPAs are addressing.

The impact of the GDPR was also felt beyond the borders of the EU as numerous countries have adopted data protection regulations. Here in the US, multiple states have proposed or enacted data privacy and security legislation based on transparency and choice principles including the California Consumer Privacy Act (CCPA), the Massachusetts Consumer Data Privacy Bill, and New Jersey's Assembly Bill 4902.

What can we expect for the GDPR's second year?

In its first year, the GDPR raised global awareness of data privacy. As it enters its second year, organizations should expect this awareness to generate increased requests from individuals to access or delete data and greater demand for appropriate data security. This may present unique challenges to employers as they navigate complying with the GDPR as well as applicable US or EU member state employment laws.

Fairness and data security featured prominently in enforcement activity this year and likely will continue. Organizations will have to address these issues by maintaining transparent processing practices and conducting regular risk

assessments. Those involved in e-commerce will likely face continuing compliance challenges presented by the data collection activities of first or third party website cookies and tracking technologies. The Bavarian DPA randomly audited 40 companies to determine whether their websites provided visitors with transparent notice of data processing and tracking activity of third-party cookies. None of the companies was in compliance. To facilitate GDPR and e-Privacy Directive compliance in the digital advertising ecosystem, the iab.EU (Interactive Advertising Bureau) has released TCF v2.0 for public comment. TCF is a framework designed to provide consumers with greater choice over the processing of their data, including opportunities to opt out, among other features.

Finally, the European Data Protection Board (EDPB) issued several draft guidelines for public consultation during the year. Once reviewed and finalized, these documents should offer guidance and clarity in several areas including processing personal data obtained in the context of providing online services to data subjects, creating Codes of Conduct and Monitoring Bodies, the jurisdictional reach of the GDPR, and exemptions for the transfer of personal data to third countries.

During the next year, US companies will continue to identify and address their obligations under the GDPR. As they do so, they will likely find that many of these data protection practices can be leveraged to meet compliance challenges imposed by recently enacted or proposed US state laws. For those US companies not subject to the GDPR, the adoption of the GDPR's underlying data protection principles might make sense.

Source URL: https://www.natlawreview.com/article/gdpr-one-year-and-counting