CORPORATE COUNSEL
An ALM Website
corpcounsel.com | March 23, 2018

The Six Data Privacy Principles of the GDPR

Amy Lewis

Data privacy and personal data breaches have been in the news a lot recently. Over the past few years, companies have been collecting and processing ever-increasing amounts of data about their customers, employees, and users. As personal data becomes more valuable, governments around the world have begun the debate surrounding whether this data collection should be limited in favor of individuals' fundamental right to privacy.

The Global Data Protection Regulation (GDPR) is the European Union's answer to these debates. This new regulation strives to take the decisions regarding some uses of personal data out of the hands of companies and return control to the individuals that the data refer to—the data subjects. Any company that has a European presence or handles European residents' personal data is subject to the GDPR. These companies will likely need to upgrade their data security and privacy procedures to meet the personal data handling requirements of the GDPR.

The GDPR's data privacy goals can be summarized in six personal data processing principles: Lawfulness, Fairness and Transparency; Purpose Limitation; Data Minimization; Accuracy; Integrity and Confidentiality; and Storage Limitation.

Lawfulness, Fairness and Transparency

"Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject." – GDPR Article 5(1)(a)

Under the GDPR, companies must ensure that personal data collection or processing is justified and permitted by law.

In some cases, companies may process personal data without asking for consent, such as when the processing is required by law or is necessary in order to conduct business. For example, companies with a European presence need to process their employees' tax ID numbers to file required employment and tax paperwork with governments.

Unless covered under another legal justification, companies must obtain informed, explicit consent from the data subject before their data can be collected or used. This consent has to be obtained on an opt-in basis using straightforward language, and individuals must separately consent to each use of their data. This ensures that individuals truly approve of a company's use of their personal information before processing occurs.

Purpose Limitation

"Personal data shall be collected for specified, explicit and

legitimate purposes and not further processed in a manner that is incompatible with those purposes …" – GDPR Article 5(1)(b)

Any time a company collects or processes personal data, it must be limited to a specific, legitimate purpose. Companies can no longer conduct blanket personal data collection in the hopes that the data becomes useful someday; the reason for collecting the data must be explicit and determined at the time of collection. This also means that companies cannot collect more data than is required for the specified purpose.

Once companies collect the personal data, they cannot then process it in a way that is incompatible with the reason for which it was initially collected. For instance, a company that collects customers' contact information for invoicing purposes cannot then use this information for marketing campaigns. Exceptions to this limitation must be examined and approved by a company's data protection officer (DPO) before the data is reused to ensure there is a justifiable and legal basis for the new processing.

Data Minimization

"Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed." – GDPR Article 5(1)(c)

Once a company has collected a set of data for a specified purpose, its use must be limited to only the specific pieces of information required for the task. For example, if a company legitimately collects a list of names, email addresses, and phone numbers for marketing purposes, the phone numbers should be excluded from processing involved in an email marketing campaign.

Minimizing personal data often involves anonymizing or pseudonymizing the data before processing. Anonymizing data involves fully stripping any identifiers from the data, ensuring that it can never be retraced to individual persons even if combined with other information. This is ideal since anonymous data is no longer considered 'personal,' so it is not subject to the same level of privacy and security restrictions.

Pseudonymization involves substituting a 'key,' such as an ID number, for the personal identifiers in the data to minimize contact with the most sensitive personal elements of the data. However, since the data can still be linked back to the personal identifiers by using the 'key,' the data is still subject to the strict privacy and security restrictions of the GDPR.

Accuracy

"Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay." – GDPR Article 5(1)(d)

The GDPR requires companies to ensure that the personal data they process is accurate, especially in the case where it is used for building profiles of data subjects. Maintaining accurate data is of course a best practice for data handling or processing regardless of regulation. However, under the GDPR, if data inaccuracies are discovered, the company must quickly fix the inaccuracy or erase the data.

Companies also have to pass these change requests along to affiliates, partners, or vendors that handle the same data. This requirement to propagate data updates helps maintain accurate profiles and protects individuals from harm caused by inaccurate profiling due to data errors.

In an effort to meet this requirement, companies should consider building a comprehensive map of where personal data lives within their systems and with their business partners. If personal data must be updated or deleted, this map will help identify instances of that data and improve the company's ability to comply with the GDPR.

Integrity and Confidentiality

"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or

organizational measures." – GDPR Article 5(1)(f)

Controllers of sensitive personal data have an obligation under the GDPR to prevent theft, leaks, breaches, or inappropriate alteration of that data. This generally involves establishing data-handling procedures that limit unnecessary access to and use of personal data, as well as technical security measures like encryption to reduce the chance of theft or breach. These measures also help companies uphold the principles of Purpose Limitation and Data Minimization by restricting access to personal data except when appropriate.

Companies should work to improve their data organization and consider building a comprehensive personal data map to ensure they place appropriate security measures and process controls around any systems containing personal data. Companies must also conduct regular training for employees who handle personal data so they know how to maintain the confidentiality and integrity of that data.

Storage Limitation

"Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed…" – GDPR Article 5(1)(e)

The principle of Storage Limitation is closely related to the principles of Data Minimization and Purpose Limitation. Once personal data has served its purpose, it must be removed to protect the rights of the individuals it concerns.

This does not mean companies are necessarily obligated to delete personal data once it has served its purpose; they may also uphold the Storage Limitation principle if they anonymize the data. Anonymization makes the data impossible to retrace to specific individuals, which means it is no longer considered personal data and is not subject to the same level of privacy and security restrictions. Anonymous data can be especially useful for future statistical analysis, but companies must take special care to ensure that anonymization is performed correctly to protect themselves as well as the individuals whose data they handle.

What Does This Mean for Your Company?

"The [data] controller shall be responsible for, and be able to demonstrate compliance with" the above principles. – GDPR Article 5(2)

The GDPR is changing the way global companies collect, process, and handle personal data. If your company processes the personal data of European residents or has a European presence, you have a duty to protect the privacy rights of the individuals whose data you control or process, and to demonstrate compliance with data privacy regulations.

By striving to uphold these six principles of the GDPR, you will be doing your part to protect the rights and privileges of the individuals whose personal information you process in your efforts to provide better and more effective products and services.

Amy Lewis *is a member of Berkeley Research Group's Information Governance and Technology practice. She helps clients' corporate legal and IT teams develop comprehensive data privacy and security compliance initiatives to mitigate information-related risk, with a particular focus on readiness programs for Europe's General Data Protection Regulation (GDPR). These programs emphasize strengthening the human element of information privacy and security, empowering the client's workforce with the tools, knowledge and motivation to assist in achieving compliance with personal data handling and privacy regulations.*

The views and opinions expressed in this article are those of the author and do not necessarily reflect the opinions, position, or policy of Berkeley Research Group, LLC or its other employees and affiliates.