Sponsored by EY Forensic & Integrity Services

Practical considerations of GDPR compliance in US-based investigation and litigation

Of special interest to:

General counsel
Outside counsel
Chief legal officer
Legal technology executives
Chief compliance officer

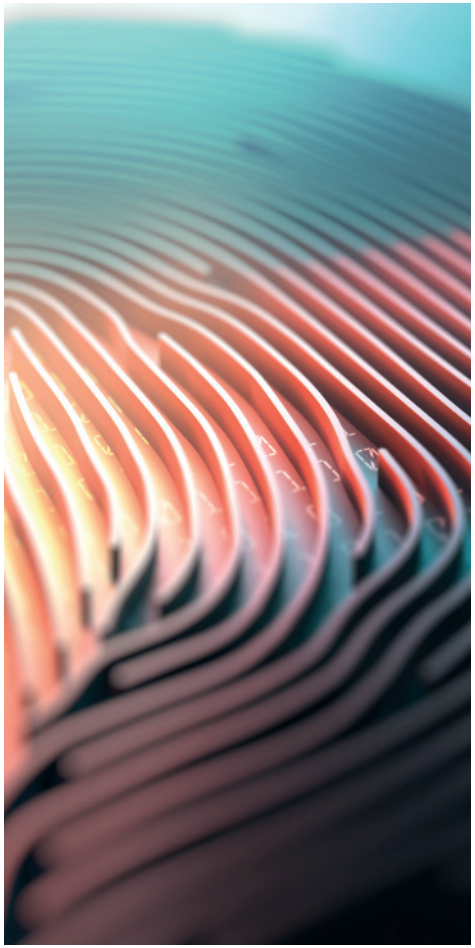
Legal, Compliance and Technology Executive Series

The General Data Protection Regulation (GDPR) , which goes into effect on 25 May 2018, is designed to protect the personal data and privacy of European Union (EU) residents. It aims to enhance enforcement and unify the existing data protection and privacy regulations within the EU such as the 1995 Data Protection Directive (the "Directive"). Given its broad outreach, the GDPR will have profound effects on the ability of global businesses to process and transfer personal data in the context of investigation or litigation.

This document is extracted from "Practical considerations for cross-border discovery under the general data protection regulation (GDPR),"[1] authored by Eric Schwarz, principal of EY Forensic & Integrity Services.

[1] The complete paper can be accessed at: ey.com/us/FIDS.

EY
Building a better working world



Author

- Eric Schwarz , CIPM, CIPP/E, SCERS
  Principal, Forensic & Integrity Services
  Ernst & Young LLP
  eric.schwarz@ey.com

What data is covered by the GDPR?

Under both the GDPR and the Directive, personal data is very broadly interpreted as any information that would allow an individual to be identified from the data. This could be as simple as a name or identification number, or as complex as a sophisticated analysis of the data.

The territorial scope of the GDPR is also quite broad. The GDPR applies to any data processing that is in connection with the offering of goods or services to data subjects in the EU or the monitoring of data subjects' behavior in the EU, regardless of where the processing takes place.

Processing of personal data

The definition of processing in the GDPR includes, among other things, collection, retrieval, consultation, use, transmission, erasure, storage and preservation of data. The bases for lawful processing of personal data under the GDPR are very similar to those under the Directive. As a result, organizations can draw previous experience and guidance from the Article 29 Working Party (WP29) regarding the application of these principles. WP29 is an advisory body established under Article 29 of the Directive and consists of a representative of the data protection authority of each European Union member state, the European Data Protection Supervisor and the European Commission. In the end of 2017, WP29 published updated guidelines on consent to address the requirements set out in the GDPR.

Under the GDPR, consent to processing must be freely given, informed, unambiguous, specific, and it can be withdrawn at any time. Moreover, consent is not considered valid where there is a clear imbalance between the data subject and the controller. WP29 considers such an imbalance to be highly likely in an employee-employer relationship.

In the context of cross-border discovery, the GDPR allows for processing of personal data for the "*legitimate interests pursued by the controller or by a third party, except where such interest are overridden by the interests or fundamental rights and freedoms of the data subject*." WP29 states that the need to comply with a foreign legal obligation, such as a document request from a US tribunal, "*may represent a legitimate interest of the controller,*"[2] but only subject to the balancing test of the controllers' obligation against the interests of the data subject and, "*provided that appropriate safeguards are put in place*." WP29 provides considerable guidance regarding elements to consider in conducting the balancing test.

[2] Sections III.2.3 and III.3 of *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, accessed 6 April 2018.

According to WP29, for the purposes of cross-border discovery, and in order of preference, controllers should consider the use of anonymized data and if that is not sufficient peseudonymized data where the controller maintains the ability to reverse the anonymization if necessary (they keep a "key"). To the extent anonymized or pseudonymized data is not sufficient, data should be filtered within the EU where it was collected so that any personal data ultimately disclosed to a tribunal or authority outside of the EU is adequate, relevant and not excessive. Adequate safeguards must be in place to ensure, among other things, the security and accuracy of the data.

WP29 clarifies that notice must be given to the data subjects and this notice should include "the identity of any recipients, the purposes of the processing, the categories of data concerned, and the existence of their rights." Moreover, "the rights of the data subject continue to exist during the litigation process and there is no general waiver of the rights to access or amend."

As with any effort to comply with complex regulations, the controller should document the decisions and analyses made in connection with the processing of personal data in connection with cross-border discovery. In the event that a decision is questioned at a later date, documentation demonstrating the above analyses and, most importantly, the consideration of the data subject's rights, may well be beneficial in demonstrating reasonable good faith efforts of the controller.

Transfer of personal data out of the EU

Once data has been processed and filtered down to only which is reasonable and necessary, the GDPR outlines the legal bases to allow transfers of personal data out of the EU. There are a number of such mechanisms, the most popular of which are the EU-US Privacy Shield data protection framework (Privacy Shield), standard data protection clauses and the Binding Corporate Rules (BCRs).

The Privacy Shield is a self-certification mechanism for companies based in the US and is only available to companies subject to the jurisdiction of the United States Federal Trade Commission or the Department of Transportation. Companies not subject to those agencies, such as nonprofits, banks, insurance companies and telecommunications service providers, cannot take advantage of the Privacy Shield framework. The Privacy Shield allows for the transfer of personal data outside of the US by expanding the "bubble of protection" of the GDPR to the entities covered by the Privacy Shield agreements. Any transfer of data outside of the Privacy-Shield-certified entities requires standard data protection clauses, which require any recipient of the data to agree to ensure all of the requisite safeguards and data subjects' rights.

The BCRs are similar in function to the Privacy Shield in that legally binding agreements are used for data transfer out of the EU. The BCRs must be approved by EU data supervisory authorities, but once they are in place, the corporate family or group of undertaking the BCRs can move personal data among any entities covered by the BCRs. As is the case with the Privacy Shield, any transfer of data beyond the entities covered by the BCRs requires standard data protection clauses for any onward transfers of data to third parties, which require any recipient of the data to ensure all of the requisite safeguards and data subject's rights.

It is important to note that the practicalities of enforcing many of the required data subject's rights can conflict with the needs of responding to either civil discovery or regulatory inquiries in the US. Therefore, it is impractical to resort solely to the above justifications for the transfer of personal data to the US in the context of cross-border discovery.

Derogations for specific situations

When none of the transfer mechanisms described above are applicable, the GDPR offers certain conditions to allow the transfer of personal data out of the EU under Article 49.[3] There is very good news for controllers responding to the types of cross-border

[3] Article 49 GDPR – Derogations for specific situations, https://gdpr-info.eu/art-49-gdpr/, accessed 9 April 2018.

discovery requests in that new guidance from WP29 includes most cross-border discovery under the derogation of Article 49(1)(e):

This covers a range of activities, for example, in the context of a criminal or administrative investigation in a third country (i.e., antitrust law, corruption, insider trading or similar situations), where the derogation may apply to a transfer of data for the purpose of defending oneself or for obtaining a reduction or waiver of a fine legally foreseen, e.g., in antitrust investigations. As well, data transfers for the purposes of formal pre-trial discovery procedures in civil litigation may fall under this derogation. It can also cover actions by the data controller to institute procedures in a third country, for example, commencing litigation or seeking approval for a merger.

In its guidance, WP29 reminds us that any data transferred under this exemption must be "*adequate, relevant and limited to what is necessary*" and it has set out the layered approach to this guidance, which we have discussed above.

Conclusion

While it is certainly true that the GDPR enhances the rights of data subjects and places much greater responsibility on both controllers and processors of personal data, there is enhanced clarity for cross-border activities thanks to the derogation for data transfers now available under Article 49(e). After 25 May 2018, when faced with a request from a tribunal or administrative body in the US to disclose information that is located in another jurisdiction, one must engage in a multi-step analysis to fully consider compliance under the GDPR.

First, as is more fully discussed above, processing of personal data for the purposes of cross-border discovery can be allowable under the GDPR provided that the processing is limited to only that data which is adequate, relevant and limited to what is necessary. In addition, adequate safeguards must be in place to make sure of, among other things, the security and accuracy of the data.

If available, the BCRs, standard data protection clauses and the Privacy Shield can be used to facilitate the access to, and movement of data out of, the EU prior to production to any third party. This can greatly facilitate the application of technologies, efficient processes and diverse resources to analyze and filter data to only data that is relevant and necessary. As a result, a much more limited data set can be produced, subject to appropriate safeguards and security, which can be provided through protective orders and technical means.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

EYG 02554-181GbI
1807-2805276

ED None

ey.com