Building a better working world

Practical considerations for cross-border discovery under the General Data Protection Regulation (GDPR)

Author:

Eric Schwarz, CIPM, CIPP/E, SCERS
Principal
Forensic & Integrity Services
Ernst & Young LLP

We are living in a world where individuals, companies and markets are much more interconnected than ever before. Even the smallest companies can have direct access to a global customer base over the internet, and multinationals have globalized operations that can cross many borders. All of this is facilitated by an explosion in new forms of communication and enormous global flows of electronically stored information (ESI).[1] These developments have happened very quickly and, while beneficial in many ways, they have presented some new challenges. There is a natural tension that exists between the benefits of improved information flows and the necessity of protecting individual privacy.

The GDPR[2] takes effect on 25 May 2018, and it will have wide-ranging effects on commerce, entertainment and communications around the world. This paper will focus on the practical impact of the GDPR on cross-border discovery. We use the term cross-border discovery broadly to cover those situations in which a party is obligated to disclose information in one jurisdiction that is located in another jurisdiction. In today's interconnected world, this is becoming an increasingly common situation, as ESI is more likely than not to be distributed globally, either on mobile devices or in an electronic storage cloud. Different jurisdictions have different cultures, expectations and laws with respect to the protection of personal information and what compromises are "fair" for a given situation and purpose.

---

[1] In a recent report, a market research firm reported that the number of worldwide emails in 2017 will exceed 3.7 billion and they expected the number of worldwide email users in 2021 will be over 4.1 billion. They also noted that in 2017 over half of the world's population used email. See *Email Statistics Report, 2017-2021*, http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf, accessed 6 April 2018.

[2] *General Data Protection Regulation GDPR*, https://gdpr-info.eu/, accessed 10 April 2018.

The United States of America (the "United States" or US) and the European Union (the "Union" or US) have very different expectations when it comes to the protection of personal information. The protection of one's privacy and personal information is a fundamental human right in the Union. Both Article 8(1) of the Charter of Fundamental Rights of the European Union[3] and Article 16(1) of the Treaty on the Functioning of the European Union[4] provide that everyone has the right to the protection of personal information concerning him or her. In addition, all European Union member states implemented the 1995 Data Protection Directive (the Directive),[5] the predecessor to the GDPR. This "right to be left alone" is as important to Europeans as the right to free speech is to Americans.

What data is covered by the GDPR?

The GDPR lays down rules for the protection of natural persons in relation to the processing of personal data and rules relating to the free movement of personal data within the Union.

Personal data is a very broad concept under both the GDPR and the Directive. Article 4.1 of the GDPR defines personal data as *". . . any information relating to an identified or identifiable natural person ('data subject')."*[6] This 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 that results in the ability to identify individuals, even if only by estimation. If the individual can be identified using *"all the means likely reasonably to be used,"*[7] the data is considered to be personal data and entitled to protection.

The territorial scope of the GDPR is also quite broad. Under Article 3(1),[8] the GDPR applies to the processing of personal data by a processor "established" in the European Union, regardless of where the processing takes place. Article 3(2)[9] expands that scope to cover processing by a controller based outside of the European Union if the processing is in connection with the offering of goods or services to data subjects or the monitoring of data subjects' behavior in the Union. If you are doing business of any kind in the Union, you are likely covered by the GDPR.

Processing of personal data under the GDPR

Now that we know what is included in the definition of personal data under the GDPR, we need to understand what is meant by "processing." Under the GDPR, anything you do with data is considered processing. The definition of processing in Article 4(2) includes, among other things, collection, retrieval, consultation, use, transmission, erasure and even storage, or "preservation," in the lexicon of civil discovery in the United States.[10]

Since anything we do with personal data can be considered processing under the GDPR, we must next ask what constitutes lawful processing of such data under the GDPR. Article 6(1) states that processing shall be lawful *only if* and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[11]

The bases for lawful processing of personal data under Article 6 of the GDPR are very similar to those under Article 7 of the Directive.[12] As a result, we have a good deal of 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.[13] It will continue as

---

3 *EU Charter of Fundamental Rights Article 8 – Protection of personal data,* http://fra.europa.eu/en/charterpedia/article/8-protection-personal-data, accessed 6 April 2018.

4 *The Lisbon Treaty Article 16,* http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-the-functioning-of-the-european-union-and-comments/part-1-principles/title-ii-provisions-having-general-application/158-article-16.html, accessed 6 April 2018.

5 *DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en, accessed 6 April 2018.

6 *Art. 4 GDPR Definitions,* https://gdpr-info.eu/art-4-gdpr/, accessed 6 April 2018.

7 Ibid. See also *Opinion 4/2007 on the concept of personal data,* http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, accessed 6 April 2018.

8 *Art. 3 GDPR – Territorial scope,* https://gdpr-info.eu/art-3-gdpr/, accessed 6 April 2018.

9 Ibid.

10 *Art. 4 Definitions,* https://gdpr-info.eu/art-3-gdpr/, accessed 6 April 2018.

11 *Art. 6 GDPR – Lawfulness of processing,* https://gdpr-info.eu/art-6-gdpr/, accessed 6 April 2018.

12 *DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en, accessed 6 April 2018.

13 *Article 29 Data Protection Working Party,* https://en.wikipedia.org/wiki/Article_29_Data_Protection_Working_Party, accessed 6 April 2018.

the European Data Protection Board under the GDPR. Because it is the simplest and the most direct, it is tempting to look to consent of the data subject under Article 6(1)(a)[14] as a lawful basis for processing of personal data but this is generally not a good option for cross-border discovery. Under Article 7 of the GDPR and the suitable recitals, consent must be freely given, unambiguous, specific, informed and it can be withdrawn at any time. In addition, consent is not considered valid where there is a clear imbalance between the data subject and the controller. The Article 29 Working Party considers such an imbalance to be highly likely in an employee-employer relationship. [15]

Article 6(1)(c) may seem appropriate for cross-border discovery as it relates to compliance with a legal obligation the controller is subject to, however, Recital 45 and previous guidance from the WP29 seems to limit the scope of that basis to legal obligations that have a foundation in either the Union or member state law.[16]

The only remaining suitable basis for processing of personal data in the context of cross-border discovery is under Article 6(1)(f), which allows for processing of personal data for the *"legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject."* While the Article 29 Working Party has not yet opined on Article 6(1)(f) of the GDPR, in its opinion on Article 7(f) of the Directive, it clearly states that the need to comply with a foreign legal obligation *"may represent a legitimate interest of the controller"* [17] 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."* In that same opinion, WP29 provides considerable guidance regarding elements to consider in conducting the balancing test, and states that the purpose of the balancing exercise is *"not to prevent any negative impact on the data subject"* but to prevent *"disproportionate impact."* [18] In their Document 1/2009, the Article 29 Working Party has provided further guidance as to the application of this balancing test in the context of civil discovery.[19] More specifically, the balancing test *"should take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject. Adequate safeguards would also have to be put in place."*

In order to comply with the regulation, when responding to cross-border discovery, controllers should first consider the use of anonymized data and if that is not sufficient, pseudonymized 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 prior to export so that any personal data ultimately disclosed to a tribunal or authority outside of the EU is adequate, relevant and not excessive. In addition, adequate safeguards must be in place to ensure, among other things, the security and accuracy of the data.

Finally, WP29 stipulates 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."* It is noted by the Article 29 Working Party that *"this right could give rise to a conflict with the requirements of the litigation process to retain data as at a particular date in time and any changes (whilst for correction purposes only), would have the effect of altering the evidence in the litigation."*[20]

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

In the first part of this paper, we examined the requirements for the processing of personal data covered by the GDPR in the context of cross-border discovery. While there are derogations to allow for such processing, it must be limited to only that which is reasonable and necessary for the purposes of the litigation, and that the rights of data subjects must be maintained throughout the litigation process. Now that we understand the requirements for the Processing of Personal Data under the GDPR in the context of cross-border discovery, we must turn our attention to understanding the requirements for transferring that data out of the European Union and ultimately to the tribunal or regulator requesting it.

Under the GDPR, personal data can be transferred outside of the EU only under the conditions of Chapter V, the provisions of which are to be applied *"in order to ensure that the level of protection of natural persons guaranteed by this regulation is*

---

[14] *Art. 6 GDPR – Lawfulness of processing,* https://gdpr-info.eu/art-6-gdpr/, accessed 6 April 2018.

[15] *Art. 7 GDPR – Conditions for consent,* https://gdpr-info.eu/art-7-gdpr/, accessed 6 April 2018. For a discussion of consent as it applies under the Directive, see *Opinion 15/2011 on the definition of consent,* http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, accessed April 6, 2018. On January 21 of this year, the Article 29 Working Party adopted guidelines on consent under GDPR but they have not yet been finalized. See *[adopted, but still to be finalized] Guidelines on Consent under Regulation 2016/679 (wp259),* http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615239, accessed 6 April 2018.

[16] *Recital 45 – Fulfillment of legal obligations,* https://gdpr-info.eu/recitals/no-45/, accessed 6 April 2018. See also *Working Document 1/2009 on pre-trial discovery for cross border civil litigation,* http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf, accessed 10 April 2018.

[17] 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.

[18] Section III.3.4 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.

[19] *Working Document 1/2009 on pre-trial discovery for cross border civil Litigation,* http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf, accessed 6 April 2018.

[20] Ibid.

not undermined."[21] This is especially challenging when dealing with cross-border discovery involving the European Union and the United States as the United States is deemed by the European Union as a country with inadequate mechanisms for the protection of personal data. In the absence of such an adequacy decision, transfers of personal data to the United States can take place only if the appropriate safeguards are in place.[22]

Article 46 and Recital 108 of the GDPR outlines the requirements for appropriate safeguards to allow transfers from the Union to countries such as the United States, which are not deemed to have adequate protection of Personal Data. There are a number of such mechanisms, the most popular of which are Privacy Shield, standard data protection clauses and binding corporate rules. We will look at each of these in turn.

The EU-US Privacy Shield data protection framework (Privacy Shield) is a self-certification mechanism for companies based in the United States that allows for the transfer of personal data to any company subscribing to the Privacy Shield framework. Notably, Privacy Shield is not available to all American companies. As enforcement is key to any adequacy decision by the European Commission, the Privacy Shield 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.[23]

Under the Privacy Shield framework, signatory companies are able to move personal data covered by the GDPR from the EU to the US but the data must stay within the protections of the Privacy Shield framework. Notably, the signatory companies must agree to have policies and agreements in place to make sure *"that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data."* While the Privacy Shield does allow for the transfer of personal data outside of the Union, it does this 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. This can be very useful for filtering or review of personal data prior to ultimate production to a tribunal or third party. It is not helpful for the ultimate production to a tribunal or third party as they are unlikely to agree to the protections required by Privacy Shield.

Binding Corporate Rules (BCRs) are similar in function to Privacy Shield in that legally binding agreements are used to ensure continued protection of personal data and data subjects' rights when data covered by the GDPR is transferred to a jurisdiction, such as the United States, that does not offer adequate protection of that data. The BCRs must be approved by European Union data supervisory authorities, but once they are in place, the corporate family or group of undertakings covered by the BCRs can move personal data among themselves. While the BCRs do allow for the transfer of personal data outside of the EU, they do this by expanding the "bubble of protection" of the GDPR; and any transfer of data beyond the entities covered by the BCRs require standard data protection clauses, which require any recipient of the data to secure all of the requisite safeguards and data subjects' rights. Notably, they must agree to, among other things, ensure the application of the general data protection principles, which are specifically noted again under Article 47(2)(d) to make sure there is no misunderstanding.[24] As is the case with the Privacy Shield, the BCRs can be very useful for filtering or review of personal data prior to ultimate production to a tribunal or third party but they are not helpful for that production to a tribunal or third party as they are unlikely to agree to the protections required by the Privacy Shield.

The practicalities of enforcing many of the required data subjects' rights may conflict with the needs of responding to either civil discovery or regulatory inquiries in the United States. Therefore, it is not sufficient to rely on the above justifications for the transfer of personal data to the US in the context of cross-border discovery.

Article 49 — derogations for specific situations

Article 49 is very clear that when none of the transfer mechanisms described above are applicable, a transfer of personal data to a third country or an international organization is only allowable if one of the following conditions applies:[25]

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

d) the transfer is necessary for important reasons of public interest;

e) the transfer is necessary for the establishment, exercise or defense of legal claims;

f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

[21] *Article 44 GDPR — General principle for transfers*, https://gdpr-info.eu/art-44-gdpr/, accessed 9 April 2018.

[22] *Article 46 GPDR — Transfers subject to appropriate safeguards,* https://gdpr-info.eu/art-46-gdpr/, accessed 9 April 2018.

[23] *EU-US PRIVACY SHIELD F.A.Q. FOR EUROPEAN BUSINESSES*, https://ec.europa.eu/newsroom/document.cfm?doc_id=40933, accessed 9 April 2018.

[24] *Article 47 GDPR — Binding corporate rules,* https://gdpr-info.eu/art-47-gdpr/, accessed 9 April 2018.

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

g) the transfer is made from a register which, according to the Union or member state law, is intended to provide information to the public and which is open to consultation, either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by the Union or member state law for consultation are fulfilled in the particular case.

Article 48 appears to clearly limit the application of Article 49(e) by excluding from allowable legal claim "*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data*"[26] unless such judgment or decision is supported by an international agreement like the Hague Convention.[27] If the derogations under Article 49(1)(a) through 49(1)(g) described above do not apply, which would be the case if Article 48 truly does exclude third-party judgments and decisions as valid legal claims, the second paragraph of Article 49(1) contains only one remaining possibility for transfer of the data but, in the context of cross-border discovery, it would be very difficult to comply with it in practice.

Of particular note, to qualify under the second sentence of Article 49 requires a fairly comprehensive balancing test in that the transfer "*may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.*"[28] Moreover, the controller is also required to inform both the data supervisory authority and the data subject regarding "*the transfer and on the compelling legitimate interests pursued.*"[29]

There are a number of conditions here that are qualitative judgments that are open to interpretation, and some that could cause significant conflicts with the needs of cross-border discovery. Thankfully, we do have some additional guidance from the Article 29 Working Party which recently adopted Guidelines on interpreting Article 49 of the GDPR.[30]

In that guidance, the Article 29 Working Party makes it very clear that the intention of Article 48 is not to eliminate foreign legal claims as legitimate grounds for data transfer to third countries but to ensure that *"decisions from third-country authorities, courts, or tribunals are not in themselves legitimate grounds for data transfers to third countries."*[31] Importantly, it also states that while not sufficient, Article 48 does allow for a transfer in response to third-country authorities *"if in line with the conditions set out in Chapter V,"*[32] which includes Articles 44 through 50 and governs the transfer of personal data to third countries or international organizations.

There is very good news for controllers responding to the types of cross-border discovery requests in that the new guidance clearly 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.*[33]

In their guidance, the Article 29 Working Party reminds us that any data transferred under this exemption must be *"adequate, relevant and limited to what is necessary"*[34] and it has set out a layered approach to this guidance, which we have discussed in more detail above.

It should be noted that it is not yet clear if this guidance will allow for the justification of the processing of personal data in connection with cross-border discovery under Article 6(1)(c) of the GDPR instead of under the much more burdensome Article 6(1)(f). While this may seem to make intuitive sense, in allowing transfers for cross-border discovery purposes as described above under Article 49(1)(e), Article 29 Working Party bases its opinion on Recital 11, which appears to be limited to data transfers. If, in the future, Article 6(1)(c) can be used as a basis for the processing of personal data in connection with cross-border discovery, responding parties would be relieved of the balancing test required under Article 6(1)(f).

---

[26] *Article 48 GDPR – Transfers or disclosures not authorized by Union law,* https://gdpr-info.eu/art-48-gdpr/, accessed 9 April 2018.

[27] *Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters,* https://www.hcch.net/en/instruments/conventions/full-text/?cid=82, accessed 9 April 2018.

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

[29] Idem.

[30] Guidelines, https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49771, accessed 9 April 2018.

[31] Section I of *Article 48 GDPR – Transfers or disclosures not authorised by Union law,* https://gdpr-info.eu/art-48-gdpr/, accessed 9 April 2018.

[32] Idem.

[33] Section II.5 of *Article 48 GDPR – Transfers or disclosures not authorised by Union law,* https://gdpr-info.eu/art-48-gdpr/, accessed 9 April 2018.

[34] Idem.

Conclusion

While it is certainly true that 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 GDPR provided that the processing is limited to only that data which is adequate, relevant and limited to what is necessary. Controllers should first consider the use of anonymized data and, if that is not sufficient, pseudonymized data, where the controller maintains the ability to reverse the anonymization if necessary. To the extent anonymized or pseudonymized data are not sufficient, data should be filtered so that any personal data ultimately disclosed is adequate, relevant and not excessive. Adequate safeguards must be in place to make sure of, among other things, the security and accuracy of the data.

If available, Binding Corporate Rules, standard data protection clauses and Privacy Shield can be used to facilitate the access to, and movement of data out of, the European Union 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 that which is relevant and necessary. That much more limited set can then 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 over 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 02552-181Gbl
1804-2666417

ED None

ey.com