EU Data Protection Gains a Sword to Go With Its Shield

Compliance and Ethics

Technology, Privacy, and eCommerce


EUROPEAN UNION
PASSPORT

CHEAT SHEET

- ***From directives to regulation.*** In 2016, the European Union will adopt firm, binding regulation to replace the patchwork of provisions governing data security.
- ***A wide net gets wider.*** The newfangled regulation will affect businesses operating outside the European Union if they store information in Europe, which may interfere with discovery in American courts.
- ***A clash of principles.*** The rigorous demands of e-discovery in US courts will face off with the newly defended right to privacy of European litigants.
- ***Prepare yourself.*** This regulation will add to the difficulty experienced by those gathering electronically stored information from international sources.

In a digital age with a free flow of information, it is easy to diminish the value of personal data. The European Commission, however, is set to solidify and unify data protection laws within the European Union under the *General Data Protection Regulation (the Regulation)*, and American companies with operations or customers in the European Union will soon find themselves having to comply with a new set of laws that could increase the cost of doing business, as well as significantly impact business operations. Corporate counsel and law firms must understand the changes coming and the potential impact on their organizations.

After over two decades under Data Protection Directive 95/45/EC (the Directive), which has attempted to harmonize 28 different data protection regimes in each member state in the European Union (EU), the European Commission decided there was a need for wholesale reform. The new Regulation seeks to harmonize the member states' differing approaches to data protection under a single law, as well as address issues not taken into account under the Directive, including developments in globalization, technological advancements and the digital economy. The European Commission aims to strengthen the rights of data subjects, give consumers greater control over their personal data, introduce stricter sanctions for data protection breaches, and make the new data protection law applicable to foreign companies with customers in the European Union.

In 2012, the European Commission published draft legislation to meet these criteria. As a Regulation, rather than a Directive, this comprehensive law will have a binding effect on all the member states and will replace the current patchwork of data protection laws. The European Parliament proposed numerous amendments to the Regulation, as has the Council of the EU (the Council of Ministers), and today the draft Regulation is finally taking shape in Trilogue meetings between the Council of the EU (the Council of Ministers), the European Parliament and the European Commission. Both the draft Regulation and the draft Directive will need to be approved before implementation.

The Trilogue process will hopefully be completed this year and there will be a two-year implementation process before the new law takes effect. The Trilogue negotiation process could extend beyond 2015, because the proposed Regulation is one of — if not *the* — most debated laws in the history of the European Union. Topics ranging from applicability to foreign data controllers and processors, the introduction of a "One Stop Shop" data protection agency across the entire European Union, protection of employee data for enterprises, increased sanctions, and new requirements to obtain consent rules are just some of the most contested aspects of the Regulation.

The passage of the General Data Protection Regulation will not only bring advantages for individual data subjects, but will also place additional burdens on organizations operating within and outside of the borders of the European Union. The harmonization of data protection laws across all member states will make international data transfers simpler. However, the Regulation also gives new and strengthened rights to data subjects, such as the right to be forgotten which reflects the rights of individuals to have certain data about them deleted, and makes profiling stricter. Other important features of the new Regulation include increased fines, privacy impact assessments and the requirement for a data protection officer (DPO).

Corporate counsel and law firms need to prepare for this changed European data protection regime. In particular, lawyers will play significant roles ensuring compliance with the Regulation by confirming that an organization's policies, procedures, documentation and organizational structures are in accordance with EU law. With the clock ticking on the adoption of the Regulation, organizations need to understand the potential impact this law will have on their business.

Background

The 1995 Data Protection Directive was passed in response to the widespread use of computing that threatened the right to privacy and aimed to unify data protection laws among member states. The Directive aimed to shield EU citizens from overzealous data collection and processing by requiring member states to implement the data protection framework in the Directive, including the creation of an independent enforcement body to oversee and regulate the automated processing of personal data and to help protect the rights of individuals.

The Directive could not anticipate the technological advancements that are now commonplace in daily life, such as internet, big data, smart phones, social media or cloud computing. The European Commission determined that new guidelines were required for data protection and privacy, and proposed the General Data Protection Regulation in 2012 to replace the Directive. The EU aims to adopt the Regulation in 2015 or 2016, and it will take effect after a transitional period of two years. While the Directive left room for member states to interpret how to achieve their goals of data protection, the Regulation will not require any enabling legislation to be passed by members. When the Regulation comes into force, only one single set of data protection rules will be in force in the European Union. The current Directive and the data protection legislation in the member states will no longer apply.

The US discovery and EU privacy conflict: Fundamental principles collide

In US litigation, the fundamental principle of broad discovery conflicts with the wide-ranging privacy framework of the European Union. US civil litigation under the Federal Rules of Civil Procedure (FRCP) is premised on the idea that expansive pre-trial discovery cuts to the heart of a dispute because it allows judges to focus on the legal issues with a well-developed record. European law is founded on the idea that citizens have a broad right to privacy, with little government intervention. While the discovery rules of the United States and the privacy laws of the European Union reflect a fundamental conflict between legal systems, the way that they have up until now clashed has been relatively narrow. The problem of discovery and privacy typically arose when a litigant in the United States requested documents stored in a European jurisdiction. The European Union and its member states apply their own privacy laws, based on the Directive, over all data stored within their borders. The Directive affords a broad protection for personal data, including information like financial data, addresses, health status, racial or ethnic identity, and email addresses. Requested electronically stored information almost always contains this type of information. European laws, from the Directive to member states' blocking statutes, have blocked unwanted data collections from jurisdictions like the United States that do not offer an adequate data protection framework. The United States and European countries have developed the Safe Harbor agreement that allows US organizations to self-certify to the US Department of Commerce that they will provide privacy protections that meet the Directive's adequacy standards when transferring personal data outside of the European Union. The Safe Harbor agreement has been criticized in Europe and rejected by Germany.

Under the new Regulation, one change looks to be especially troubling for non-EU countries. The scope of the draft Regulation has been extended to apply to businesses operating outside of the European Union when they process personal data related to individuals living within the member states by offering goods or services to such individuals or monitoring their behavior. Businesses outside the European Union (such as those in the United States), face a legal regime where they are subject to EU privacy laws even if they are not located, or doing business, within the European Union

— so long as they are processing or storing personal information of individuals residing in the European Union. For example, a company headquartered in the United States may store and process employee records containing personal information about European Union residents at a subsidiary in Europe or even with a European-based cloud services provider and therefore be subject to the requirements of the Regulation. The extraterritoriality of the new Regulation is particularly worrisome for discovery in the United States. The Directive, and now the strengthened Regulation, prohibits the transfer of any personal data processed in the European Union to a country whose privacy laws are considered inadequate by the EU's determination such as the United States, which poses a significant conflict with US discovery obligations.

This has been the crux of the problem — litigants request documents in American courts, but European law may prevent the responding party from transferring the documents to the United States. The Regulation will undoubtedly further the frustration of lawyers who gather electronically stored information from international sources, but the extraterritoriality adds a new twist. While the European Union has strengthened its shield against data collectors with the Regulation, it has also equipped itself with a shiny new sword. When the fundamental principles of American discovery and European privacy collide in a US court judges must choose between adhering to the traditional discovery rules of the FRCP and respecting an EU litigant's legitimate right to privacy. American litigants clash against EU laws in a quest to obtain data that would otherwise be discoverable and now face a new, nightmarish prospect of being dragged into the EU's jurisdiction for non-compliance with the Regulation.

Practical impact of the regulation on e-discovery

In international cases potentially relevant data is typically scattered across multiple countries and needs to be collected, searched and reviewed efficiently to identify relevant documents for discovery purposes and generally to prepare the case.

Collection usually happens onsite but the processing of data is most effective if the data is transferred to a central e-discovery processing engine where it can be aggregated and filtered by date and key words. If data is located in Europe, a debate begins about how best to handle data that needs to be transferred to ensure compliance data protection laws. Should the data be processed and filtered in the initial country first, before it is transferred to a central database in another country? Can data be transferred to a central data processing engine and be processed with other data, and what steps must be taken to ensure the transfer is lawful? If the data is stored in a database in one country, can lawyers from other countries, who are experts in their particular fields, log into the database and review the documents or does this constitute a data transfer that is regulated? These are some of the questions which typically arise.

Under the current European Data Protection Directive the answers to these questions have not always been clear-cut, even though the regime has been in place for a long time. In the context of e-discovery. Some of the key issues that need to be addressed by litigants and their legal and e-discovery providers and on which legal guidance is often sought are the set out below.

What constitutes personal data?

Personal data is defined in the Regulation as any information relating to a natural person who can be identified, directly or indirectly, by reference to an identifier. These include names, identification numbers, location data, online identifiers or other factors related to the physical, physiological,

genetic, mental, economic, cultural or social identity of a person.

In the context of e-discovery, personal data is likely to be contained in *any* email or other document that is handled during the process of pre-trial discovery or produced in response to a regulatory enquiry. This personal data pertains not only to the person whose computer or data is under investigation (the *first party data subject*) but also to the third parties who he or she has corresponded with and to any third party individual referred to or about whom the correspondence or document pertains (*third party data subjects*).

What does processing data mean?

In the Regulation, “processing” is described broadly as any operation that is performed on personal data whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction. This definition is very similar to the current definition in section 2(a) of Directive 95/46/EC.

The wide scope of this definition means that *all* operations performed on data that contain personal data will be subject to European data protection laws. All electronic information handled in investigations or in litigation by companies, their lawyers and e-discovery providers is being processed when it is collected, filtered and loaded into document review tools for analysis.

What steps must be taken to ensure that data is handled for e-discovery in compliance with the Regulation?

Consent

Under the Directive, data processing requires a legal justification — in other words a legally recognised “ground for processing.” This remains unchanged in the Regulation but the standard for complying with the various grounds for processing is expected to be set higher, especially in relation to consent.

The main justifications for processing include consent, where necessary for performance of a contract or for the fulfillment of a legal obligation, where it is in the vital interests of the data subject or the public interest, or for the legitimate interests of the data controller.

Consent as a ground for processing personal data has caused difficulties over the years due to differences in the way that different countries in the European Union has interpreted it. In addition, consent is now often implied in online scenarios and the concept has been eroded. The Regulation aims to harmonize and bolster the approach to consent. It requires consent to the processing of personal data to be freely given, informed and specific. It is not yet clear whether implied consent will be valid or whether explicit consent to processing is required for all or some categories of data. This means data subjects must be given sufficiently detailed notice of an e-discovery exercise for them to make an informed choice (and in some cases explicit consent may be required) and that they are entitled to withdraw consent at any time.

If consent is sought, but one or more data subjects refuse to give it, it can be practically difficult in the face of a later data protection authority inquiry to make a claim that another exception applies and that the consent was not needed or was only sought as a “precautionary” measure.

In addition, third party data subjects are also data subjects within the scope of the Directive and it will, in most cases, be unrealistic to obtain their consent to an e-discovery exercise.

As a general rule consent should not be implied. It requires a statement by the data subject or a clear affirmative action. If the consent appears in a written document like a contract the data controller must present the mechanism for obtaining consent in a distinguishable way, meaning that a separate clause.

If there is an imbalance between the position of the data controller and data subject such as in an employment relationship, then consent may not be relied upon as grounds for processing personal data.

Legal obligation

Compliance with a legal obligation appears to be the most obvious exemption upon which to legitimise an e-discovery exercise. However, the law is drafted so that this exception only applies to European legal obligations and not, for example, to obligations arising from US law such as the FCPA or Sarbanes-Oxley.* Theoretically, even requests for information from regulators or law enforcement may not satisfy the legal obligation test because the request is often “voluntary” but backed up with sanctions if not complied with. Therefore, it may not, strictly speaking, be a “legal” obligation that the controller is required to comply with.

* This was made clear in the WP29’s Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, 1.2.2006, WP 117, page 8: “an obligation imposed by a foreign legal statute or regulation (…) may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. Any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive”.

Legitimate interests

Both the Directive and the Regulation permit the processing of personal data when it is necessary for the legitimate interests of a data controller provided there is no overriding interest of the individual. A company’s *legitimate interest* is currently and is likely to continue to be the most common justification for carrying out an e-discovery exercise. However, the draft Regulation, like the Directive, requires the legitimate interests of the employer to be balanced against the fundamental rights and freedoms of the individual. This means that it is important that, as far as reasonably possible, individuals receive comprehensive notice about how their personal data is to be processed, that personal data is only processed within the scope of that notice and that their rights (i.e., to be able to access or correct personal data or object to the processing) are preserved.

How should cross border transfers be handled?

Under the Regulation, data may only be transferred outside the European Union if conditions are met including the Commission finding the country’s data protections adequate, if appropriate safeguards are in place (like standard contract clauses or binding corporate rules) or if one of the derogations in Article 44 of the draft Regulation are present.

In a nutshell, the existing adequacy findings and Safe Harbor (for US companies only) will, in principle, continue to be valid and the Regulation seeks to extend the options available to legitimize

international data transfers (such as through the use of standard and ad hoc contractual clauses and codes of conduct adopted or authorised by Data Protection Authorities). The exact mechanisms for legitimizing transfers are, however, still being debated and the draft texts of the Commission, the Parliament and the Council differ significantly.

The Commission has so far recognised a dozen countries, along with the US Department of Commerce's US-EU Safe Harbor Framework as providing adequate protection.

The derogations in Article 44 are similar to those in the Data Protection Directive and include the following:

- The data subject has explicitly consented to the transfer after being informed that such transfers may involve risks for the data subject due to the absence of an adequacy decision and appropriate safeguards.
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken at the data subject's request.
- 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 person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary to protect the vital interest of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- The transfer is made from a register that intended to provide information to the public that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest
- The transfer, which is not large scale or frequent, is necessary for the purposes of legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject and where the controller has assessed all the circumstances surrounding the data transfer operation adduced suitable safeguards for the protection of personal data. The data controller must also keep a full record of the transfer and the further processing operations.

Some commentators believe we will see an increase in data transfers based on this derogation. This will particularly be the case where transfers only take place occasionally and not on a large scale, and no other derogations are reasonably available.

While under the current Directive a number of member states require that a transfer to third countries outside the European Union must be notified to or authorized by local Data Protection Authorities, in particular where based on EU Model Clauses or BCRs, the Regulation explicitly provides that this will no longer be the case so long as the other requirements of the Regulation are met. For multinational companies relying on EU Model Contracts or BCRs to legitimize their transfers, this will drastically reduce the administrative burden.

From a practical point of view, where data sets are is large, e-discovery providers can assist their client's compliance with the Directive by conducting initial filtering immediately so that the client can claim that they are being proportionate in their approach to e-discovery and data transfers.

In relation to the processing, filtering and interrogating of data in discovery, the Article 29 Working Party provides in WP158 that any filtering activity of personal data should be carried out locally *in the*

country where the data is found before the data is transferred outside the EEA. The Article 29 Data Protection Working Party was set up under Article 29 of the Data Protection Directive. It is an independent European advisory body on data protection and privacy and its Opinions and Working Documents are not binding but are influential. The Article 29 Working Party will become the EU Data Protection Board under the new Regulation.

Issues to consider when collecting evidence in Europe

US law firms and their clients typically consider the following issues when the need to collect European data arises.

WHAT LEGAL MECHANISMS CAN BE USED TO TRANSFER DATA LAWFULLY ACROSS BORDERS?

These might include legal exemptions in data protection law which allow data to be transferred where it is needed in legal proceedings, although in some countries like Germany discovery is not recognized as a legal obligation.

HOW CAN TECHNOLOGY BE USED TO TARGET THE DATA NEEDED AND REDUCE THE RISK OF UNLAWFUL DATA TRANSFERS?

Computer forensic experts can harvest data onsite in a very targeted way. Filtering either onsite or in Europe can be used to search across potentially relevant data and identify key data. Advanced review tools allow reviewers to identify and remove personal data from a data set or redact personal references.

IS IT NECESSARY TO NOTIFY OR OBTAIN THE EXPRESSED CONSENT OF DATA CUSTODIANS BEFORE COLLECTING THEIR DATA?

Data subjects must be given notice of an e-discovery exercise and enough information for them to make an informed choice (and in some cases explicit consent may be required). Obtaining consent of the individuals whose personal data is to be transferred can be logistically difficult and time-consuming.

Accountability

Article 22.1 of the Regulation currently states that: “Taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals, the controller shall implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.”

The various drafts of the Regulation in circulation differ on what is required by Article 22, including:

- The adoption of privacy policies.
- The adoption of internal or external audit processes to ensure that an organization’s processing of personal data complies with the Regulation.

- The implementation of technical and organizational methods to protect data against unauthorised or unlawful processing.

Keeping records of the processing of personal data which the organization carries out.

Under the Regulation, e-discovery providers will need to help their clients carry out the necessary audits, ensure that adequate mechanisms are in place to safeguard data, and that required audit trails are in place about the data processed. Whilst it is not yet clear what detail is required in records kept it is expected to include the reason for processing data, the categories of data subjects and data, the recipients or categories of recipients of data and when data should be deleted.

Impact on e-discovery service providers

The current Directive only applies to data controllers, but the Regulation introduces a number of detailed obligations and restrictions on data processors and is therefore likely to have a significant impact on e-discovery service providers (i.e., data processors) and those that engage them. In the future, penalties can be imposed on data processors that do not comply with their new responsibilities and, if they act outside of the instructions received from data controllers, they could be held to be joint controllers subject to higher standards of accountability.

The new obligations include the following:

- **Maintain documentation** about the processing operations under their responsibility.
- **Implement appropriate security measures** and alert controllers immediately after the establishment of a personal data breach.
- **Carry out data protection impact assessments**. The Regulation requires impact assessments to be carried out when processing operations present certain specified risks, either by the data controller or the data processor acting on their behalf. For example, they may be required when data processing involves large scale filing systems on children, genetic data or biometric data. There may also be situations where processing data for e-discovery purposes will require privacy impact assessments.
- **Obtain prior authorization or undertake prior consultation.** The data processor will be required to consult or obtain prior authorization from the relevant supervisory authority prior to certain processing activities being undertaken.
- **Comply with the international data transfer requirements.**
- **Cooperate with a supervisory authority** if requested to do so, for example, by submitting documentation to demonstrate compliance with the above responsibilities.

The Regulation also encourages the drawing up of codes of conduct and certification mechanisms so processors stand to gain a competitive advantage if they can show that they comply with new privacy codes of conduct.

Conclusion

Given that the European Union’s adoption of the Regulation in early 2016 is imminent, corporate counsel, their law firms and e-discovery providers will need to ensure compliance with the Regulation to avoid sanctions and ensure that an organization’s policies, procedures, documentation and organizational structures are in accordance with EU law. There is no doubt that the Regulation will add to the difficulty experienced by those gathering electronically stored information from international sources. The need for a legal justification for processing personal data remains

unchanged in the Regulation but the standard for complying with the various grounds for processing is expected to be set higher, especially in relation to consent. In terms of practical solutions, the obstacles experienced with cross border transfers of data can be overcome if transfers are not large scale or frequent and are necessary for the purposes of legitimate interests pursued by the controller that are not overridden by the interests or rights and freedoms of the data subject. Technology can also be relied on to ensure that, where necessary, data is processed onsite or in-country and that only that which is strictly necessary is transferred across national borders or outside of Europe in line with the Article 29 Working Party guidance.

It is important that the data subject receives good information about how personal data is to be processed, that it is only processed within the scope of that notice and that their rights to access or correct personal data are preserved.

Start preparing for these changes in the European data protection regime.

Further Reading

See European Parliament, Q&A on EU Data Protection Reform (Mar. 4, 2014).

See Proposal for a Regulation 9565/15 of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation).

Id. at paragraph 63.

Article 4(1) and (2). It is worth noting that this definition is from the Council of the EU's draft and may not be the definitive definition the EU agrees on.

Article 4 (3).

Article 6.

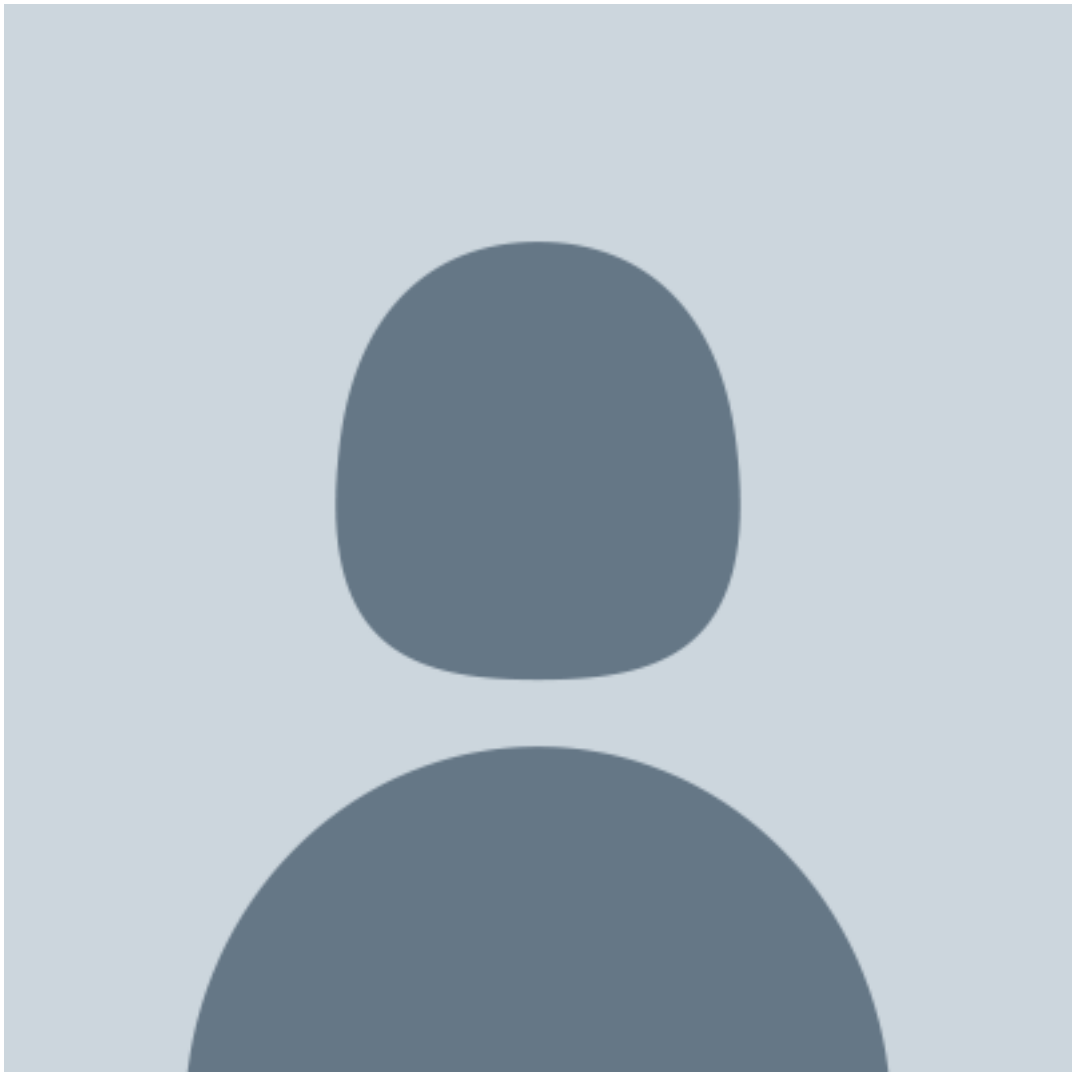
Article 7(4).

See, for example, Article 18 of Council Regulation 1/2003.

Future Proofing Privacy, A Guide to Preparing for the EU Data Protection Regulation, .

See Working Document 1/2009 on pre-trial discovery for cross-border civil litigation (WP 158), page 11 which states the following: "When personal data are needed the "filtering" activity should be carried out locally in the country in which the personal data is found before the personal data that is deemed to be relevant to the litigation is transferred to another jurisdiction outside the EU."

Lawrence Ryz

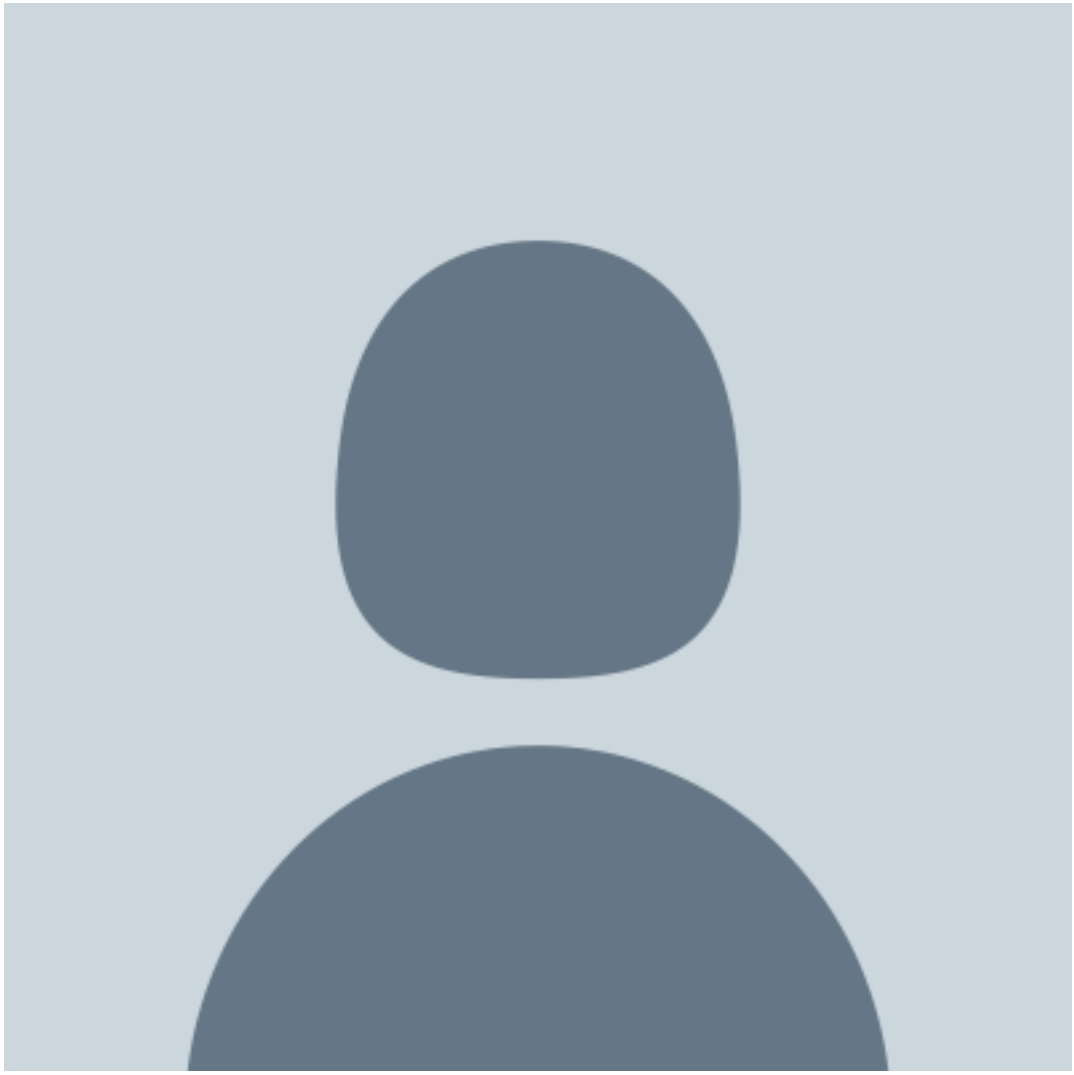


Legal Counsel

Kroll Ontrack in the UK

He advises on a range of legal issues in Europe and Asia related to data recovery, computer forensics and legal technologies. He provides expertise around data protection laws, commercial laws and legal compliance issues that affect the various jurisdictions in which Kroll Ontrack’s business operates.

Tracey Stretton



Legal Consultant

Kroll Ontrack in the UK

She advises lawyers and their clients on the use of technology in legal practice and has provided consultative expertise on a large number of cases in a variety of international jurisdictions.