# GDPR Impact on U.S. Litigation: What You Need to Know

In April 2016, the European Union (EU) adopted a major overhaul of its data privacy laws to better address new technologies and provide a more coherent approach across different EU Member States. The new law, known as the General Data Protection Regulation (EU) 2016/679 ("GDPR") takes effect on May 25, 2018. It will replace the patchwork of national laws created under the old Directive 95/46/EC with a more unified law directly binding each Member State and threatening significant fines amounting to four percent of a company's global turnover for noncompliance. This document provides (1) a glossary of key terms; (2) an overview of key GDPR provisions and impact on litigation; and (3) a litigation checklist.

## Glossary:

**Data Subject** – A person identified in the data.
**Data Processor** – A company that processes data under the direction/control of another company.
**Data Controller** – A company that makes decisions about how, why, when and by whom data is processed.
**Supervisory Authorities** – Regulatory bodies in each EU member state that enforce the GDPR.

## GDPR Key Provisions:

### Increased Territorial Scope

The GDPR will apply to all companies processing the personal data of people residing in the European Union and European Economic Area (EU/EEA), regardless of the company's location. That means GDPR applies whether the processing takes place in the EU or not. For example, if a company has offices in the EU, it is covered by the GDPR, even if it is storing the data elsewhere. Conversely, if a company is only located in the United States, but it is offering goods or services to EU residents and/or monitoring behavior that takes place within the EU, it is also covered.

*Example of Impact on Litigation: In many situations, responsive emails containing the email addresses of EU-based employees stored on a server in the U.S. by a U.S. company would be covered by the GDPR and could thus not be collected, reviewed or produced in discovery without first complying with the GDPR.*

### Penalties

Organizations found to be in violation of the GDPR can be fined up to four percent of annual global turnover or €20 million, whichever is ***greater***. In other words, the GDPR has teeth. This provision makes clear penalties are intended to be significant and potentially in excess of €20 million.

*Example of Impact on Litigation: If you start collecting, reviewing and producing data without following the steps mandated by the GDPR, your client and your law firm could be exposed to direct liability and fines.*

### Right to Be Forgotten

The right to be forgotten entitles individuals to have his/her personal data erased, limit or cease dissemination of their data, and empowers them to halt processing of the data.

*Example of Impact on Litigation: In theory, an EU resident could contact you or your client and demand immediate destruction of all personal data related to them despite the fact that the data was on a litigation hold – creating a potential conflict between the obligation to preserve evidence and the GDPR.*

### Data Portability

Individuals now have the right to receive personal data concerning themselves and transmit it to others if they so desire.

*Example of Impact on Litigation: In theory, a person residing in the EU could contact your law firm and demand a transportable copy of all personal data you have concerns them.*

## Consent

Consent is generally required prior to collecting personal data, and the GDPR has increased these requirements. Companies are now required to draft consent forms in simple language and are prohibited from using forms filled with vague, overbroad terms that would allow just about any future use.

*Example of Impact on Litigation: Based on these heightened requirements, it will be increasingly difficult to rely on consent as a basis for working with personal data in the context of litigation.*

## Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to impact individuals in that jurisdiction and must be done within 72 hours of first having become aware of the breach. Depending on the risks associated with the breach, notification may need to go directly to the data subjects or may be limited to only the relevant Supervisory Authority.

*Example of Impact on Litigation: If a law firm's eDiscovery vendor or law firm itself suffers a data breach, the law firm may be required to notify EU regulators and/or EU data subjects.*

## Right to Access

Individuals can now obtain confirmation from data controllers as to whether or not personal data concerning them is being processed, where, and for what purpose. Further, controllers must provide a copy of the personal data, free of charge, in an electronic format.

*Example of Impact on Litigation: After hearing their employer or a company they do business with is involved in U.S. litigation, a person in the EU could contact the law firm directly or its eDiscovery vendor and demand to know whether or not his/her personal data was being used in conjunction with the lawsuit, where that data was located, and what was being done with it.*

## Privacy by Design

At its core, privacy by design calls for the inclusion of data protection from the onset of system design rather than an update or patch down the road. Among other things, Article 23 calls for companies to hold and process only the data absolutely necessary for the completion of their duties (data minimization), as well as limiting the access to personal data to those needing to act out the processing.

*Example of Impact on Litigation: This will likely require that more narrow collection criteria be used when collecting data covered by the GDPR than are typically used during discovery. It may also require that at least some processing and filtering be done in-country.*

## Enhanced Internal Record-Keeping Requirements

In order to ensure accountability, the GDPR requires companies to keep detailed records regarding all data processing activities, including records indicating the date and contents of notices sent to data subjects, records of each data subject's consent (if consent is required), records indicating where and how data is being processed, and records of any safeguards or steps taken to minimize the risk of infringing the data subject's rights.

*Example of Impact on Litigation: It will be important to maintain records documenting compliance with the GDPR throughout the life of the litigation, including copies of any notices sent to custodians and notes detailing data minimization steps and access restrictions.*

## Audit Rights & Private Right of Action

The GDPR gives EU Supervisory Authorities ("SAs") the right to audit entities processing data covered by the law, including U.S.-based entities. It also creates a private right of action for data subjects to sue data controllers and/or processors for alleged violations. Damages can include material and nonmaterial harm, such as emotional distress.

*Example of Impact on Litigation: A disgruntled former employee who was terminated after an internal investigation conducted by a law firm could file a complaint with an SA triggering an audit of both the employer's and the law firm's GDPR compliance. In addition, with or without an audit, the disgruntled former employee could file suit directly against the employer and the law firm for alleged violations of his/her data privacy rights under the GDPR.*

## GDPR Cross-Border Litigation and Investigation Checklist:

- Determine whether or not the GDPR applies to the data in question by asking these questions:
    a. Can the data be used to identify individual people, e.g., names, email addresses, etc.?
    b. Does the data identify any people residing in the EU?
    c. Is the data being collected from a company with any offices/employees in the EU?
    d. Was the data collected as a result of offering goods or services to people residing in the EU, or as a result of monitoring the behavior of people residing in the EU?
- Contact company/client privacy officer.
- Determine whether it is necessary to retain privacy or eDiscovery counsel to advise on issues.
- Determine whether company policies or other contractual agreements apply to the data in question, e.g.:
    a. Privacy Shield Restrictions
    b. EU Standard Contractual Clauses
    c. Binder Corporate Rules (BCRs)
    d. Employment Contracts or Union Contracts
    e. Computer Use Policies
    f. Vendor/customer Agreements
    g. Confidentiality Agreements
- Determine whether a national blocking statute or employment law also applies, such as the French Blocking Statute.
- Identify a legal basis under the GDPR for processing the data:
    a. Does the company have legitimate grounds for processing the data?
    b. Does the new processing required for the lawsuit or investigation pass the balancing of interests test?
    c. Are other legal bases for processing available, such as consent?
- In addition to the legal basis for processing above, identify a separate legal basis for accessing or transferring the data from/to a third country (or transferring it to a third country), e.g.:
    a. Privacy Shield
    b. Standard Contractual Clause Agreements
    c. Legal Necessity Derogation

    *Note: More than one may be necessary.*
- Ensure you have the necessary legal agreements in place with your discovery vendor, counsel and co-counsel:
    a. Standard Contractual Clauses
    b. GDPR-compliant Data Processing Agreement
- Provide and document necessary notices to the custodians. This may require changes to current and future preservation notices.
- Take steps to minimize the data, limit access rights and adopt technical security safeguards prior to processing or accessing the data.
    a. Narrow document collection
    b. Date limitations or targeting only certain folders
    c. In-country filtering with search terms and other data analytics techniques
    d. Restrictions on further transfers or access by new people/entities
    e. Protective Order
- Document all the steps you took and comply with the GDPR's specific record-keeping requirements.
- Access or transfer the data in question.

**Wendy Butler Curtis**
Chief Innovation Officer
Washington, D.C.
E wcurtis@orrick.com
T +1 202 339 8584

**Jeffrey McKenna**
Senior Attorney
eDiscovery & Privacy
San Francisco
E jmckenna@orrick.com
T +1 415 773 4152