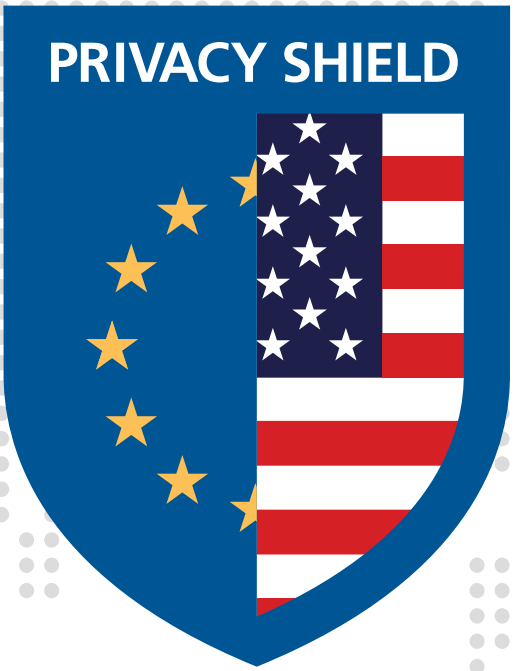
SEYFARTH SHAW

Data Privacy & Protection in the EU-U.S.

What Companies Need to Know Now



2017–2018 EDITION

On May 25, 2018, the EU General Data Protection Regulation (GDPR) will impose significant new obligations on all U.S. companies that handle personal data of any EU individual. U.S. companies can be fined up to €20 million or 4% of their global annual revenue for the most egregious violations.

Many U.S. companies are neither aware of, nor ready for GDPR compliance. According to a recent global Dell Survey, only 38% of U.S. multinationals were even aware of GDPR, and only 3% had a plan to prepare for GDPR[1]. A PwC global survey reflects that GDPR compliance is only one of several priorities for 38% of U.S. companies, and not a priority at all for 8%[2]. Further, a Data Threat Report based upon an audit of over 15,000 cloud applications revealed that only 2% of them are GDPR ready[3].

Seyfarth's Global Privacy and Security Team and eDiscovery and Information Governance Practice Group help clients safely prepare for GDPR, while also carving a secure and practical roadmap for U.S. cross-border transfers of EU personal data for both regular business and litigation obligations. We are uniquely suited for this task based upon our experience and expertise with (1) EU data protection and cross-border discovery practice since 1995; (2) our team's attorneys that have technology backgrounds, significant in-house experience, and high stakes international litigation experience; (3) our awards for innovative and practical technology solutions; (4) our extensive data security, cybersecurity, and ethical hacking expertise and experience; and (5) our longstanding thought leadership in this area, including extensive publishing, speaking and participation in numerous industry and regulatory initiatives, such as The Sedona Conference® International Working Group.

Seyfarth's Global Privacy and Security Team and eDiscovery and Information Governance Practice Group

Seyfarth's Global Privacy and Security and eDiscovery and Information Governance attorneys provide our clients with practical and innovative legal advice and solutions in all facets of data privacy and protection, including enterprise-wide, multi-jurisdictional information governance and electronic discovery. Clients rely on Seyfarth as trusted advisors and advocates for global eDiscovery issues, including conflicts between data protection regulations and U.S. discovery and business requirements, and for information governance issues including data security, privacy and records management.

For more information, please visit our Carpe Datum Law and Global Privacy Watch blogs (www.carpedatumlaw.com and www.globalprivacywatch.com). We are happy to discuss these developments, and the impact on your company at any time, via phone, in person, or webcast. For more information, please contact Scott A. Carlson at scarlson@seyfarth.com, John P. Tomaszewski at jptomaszewski@seyfarth.com, Darren G. Gardner at dgardner@seyfarth.com, or Peter Talibart at ptalibart@seyfarth.com, or visit our webpage at www.seyfarth.com.

---

[1] "Dell Survey Shows Organizations Lack Awareness and Preparation for New European Union General Data Protection," Business Wire, October 11, 2016, http://www.businesswire.com/news/home/20161011005445/en/Dell-Survey-Shows-Organizations-Lack-Awareness-Preparation.

[2] "GDPR Awareness, Readiness and Compliance in the U.S.," I-Scoop Compliance and Regulation, January 31, 2017, https://www.i-scoop.eu/general-data-protection-regulation-readiness/.

[3] "Most Cloud Applications are not GDPR Ready," Computer Weekly, July 28, 2016, http://www.computerweekly.com/news/450301241/Most-cloud-applications-not-GDPR-ready-report-reveals.

A Brief History of GDPR

"The GDPR imposes dramatic changes in how, going forward, all U.S. organizations, must treat EU Personal Data (i.e., data that can be used alone or in combination to identify any EU citizen)."

The adoption of The EU General Data Protection Regulation (GDPR) and EU-U.S. Privacy Shield Framework in 2016 represent a landmark shift in U.S./EU data privacy and protection. **There is no time to waste, given the significant human and IT resources and time and cost necessary to achieve GDPR compliance.**

According to a recent global survey by Dimensional Research on behalf of Dell, fewer than 33% of U.S. companies are prepared for the GDPR; only 3% have a GDPR plan in place; 27% are still unsure of GDPR requirements; and 33% have not started planning at all.[4]

First, the GDPR applies to all U.S. organizations that access EU personal data, whether in print or electronic format. This is true whether the data is in Europe or the United States; and whether it is available via website, email or remote Internet link. It applies regardless of size or type of industry, and regardless of context (e.g., business, litigation, regulatory). Unlike the current EU Data Protection Directive (95/46/EC), the GDPR, effective May 25, 2018, applies a uniform set of significant sanctions across all EU member States. Its provisions are mandatory and will supersede the current Directive. GDPR includes significant new data privacy and data protection requirements, including, among others:

(a) Exposure to penalties of up to €20 million or up to 4% of the organization's global gross annual revenue, whichever is greater;

(b) Notice to EU Data Protection Authorities officials within 72 hours of any data breach;

(c) Embedding "Privacy by Design" controls, by default, into all IT systems that handle EU Personal Data;

(d) Granting a "Right to be Forgotten," which requires EU personal data to be erased, upon request of the data subject;

(e) Granting a right of "Data Portability," requiring EU personal data to be removed and delivered to the data subject, upon request;

(f) The requirement of a Data Protection Officer for large and data-intensive businesses;

(g) The use of Data Protection Risk Assessments (DPRA) for each type of processing that has the potential to put an individual's privacy at risk.

[4] "Dell Survey Shows Organizations Lack Awareness and Preparation for New European Union General Data Protection," Business Wire, October 11, 2016, http://www.businesswire.com/news/home/20161011005445/en/Dell-Survey-Shows-Organizations-Lack-Awareness-Preparation.

“Organizations need to either certify under the Privacy Shield Framework, or implement alternative EU-approved mechanisms for complying with the provisions of the Directive, an imminent GDPR.”

Second, on August 1, 2016, the U.S. implemented the EU-U.S. Privacy Shield Framework, replacing the prior U.S.-EU Safe Harbor Framework, as a voluntary mechanism for transfers of personal data from the EU to the United States. The Privacy Shield Framework requires U.S. companies to accept significant data privacy and protection requirements, including:

(a) Public commitment (via a link to the Department of Commerce Privacy Shield Page) expressly representing that they will comply with all Privacy Shield provisions, under penalty of enforcement by the FTC;

(b) Creating a company Privacy Shield Complaint Recourse Process to receive and investigate Privacy Shield complaints, and to provide a written response to them within 45 days, and including a link to this process and related forms in the internal and external privacy policies;

(c) Giving notice of an individual’s right to complain under Privacy Shield also applies to processing undertaken by third parties;

(d) Giving notice whether the company has retained a third-party arbitrator as an additional recourse mechanism for resolving Privacy Shield complaints that cannot be resolved using the company’s independent recourse mechanism – and if so, providing a link in their internal and external privacy policies to the arbitrator and necessary forms; or in the alternative, designating the EU Data Protection Commissioner to resolve such complaints, in consultation with the company, the complainant and the FTC;

(e) Conducting regular company audits or monitoring of Privacy Shield compliance, and maintaining records of same, making them available for inspection by the FTC and EU Data Protection Authorities; and

(f) Identifying a company Privacy Shield point of contact to receive, investigate and rule on complaints, and to communicate and coordinate with the FTC and EU Data Protection Authorities regarding any complaints, concerns, or requesting information or an audit of Privacy Shield controls or compliance.

Significant Provisions of the GDPR

As a Regulation (as opposed to a Directive), the GDPR has the direct force and effect of law in all EU jurisdictions. Following is more detail regarding the principal GDPR provisions. A table is provided in Appendix A that compares the EU Data Protection Directive requirements with those of the GDPR. The principal provisions of the GDPR include:

- **Expanded territorial reach.** The GDPR applies to data controllers and processors whose processing activities relate to the offering of goods or services to EU data subjects, or monitoring the behavior of EU data subjects within the EU, regardless of whether the processing takes place in the EU.
- **Broader definition of "personal data."** Under the GDPR, personal data includes a name, an identification number, location data, or any online identifier; as well as factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person. "Sensitive Personal Data" will also include two new categories of data: genetic and biometric data.
- **New and enhanced rights for data subjects.** The GDPR provides data subjects with several expanded and new rights: such as the right to take their data with them (data portability); the right not to be evaluated on the basis of automated processing; and the right to be forgotten (or the right to erasure).
- **Lead DPA (the "One-Stop-Shop" provision).** Where a company operates in more than one Member State, the Data Protection Authority (DPA) for the main establishment of the company will be the company's lead DPA.
- **Fines.** The GDPR will impose substantial fines for non-compliance. Depending on the type of infringement, GDPR violators can be fined up to €20 million, or up to 4% of total worldwide annual turnover, whichever is higher.
- **Data breach reporting.** Data breach must be reported to the local DPA within 72 hours, and to the affected individuals "without undue delay" if there is high risk to their privacy rights. While there is an exception to the reporting requirement where a company can demonstrate that the breach "is unlikely to result in a risk for the rights and freedoms of individuals", the mere violation of the right will likely be seen as "risk".
- **Data protection "by design" and "by default."** To achieve privacy "by design," organizations are expected to operationally weave privacy into their services and business processes, both at the time of creation, and through implementation. To demonstrate privacy "by default," organizations should automatically take steps to limit the data collected, used, or disclosed during each interaction with an individual. Where there may be a need for a secondary use from the purpose of the original collection, companies should undertake a Data Privacy Impact Assessment ("DPIA") to ensure the individual's privacy rights are preserved.

- **Cross-Border Transfers.** All cross-border transfers have to fit within a specific set of legitimate bases for such transfers. These bases are more limited than the "fair and lawful" bases for merely processing.
- **Joint liability.** Data controllers and data processors are jointly liable under the GDPR, and controllers are responsible for contractually ensuring third-party GDPR compliance.
- **Data Protection Officers.** A company must appoint a Data Protection Officer ("DPO") in situations involving (1) regular and systematic monitoring of data subjects on a large scale; and (2) large scale processing of special categories of personal sensitive data, such as medical, financial, political, or union membership (among others). Further, the DPO should be independent and competent at both the privacy rules applicable to all the data of the business, and also the business' operational realities.
- **Data Privacy Impact Assessment.** The GDPR requires an annual mandatory Data Protection Impact Assessments ("DPIAs") where there is a high risk to the rights and freedoms of natural persons, taking into account nature, scope, context, and purposes of processing. This is required even if the processing is permissible under the GDPR. There needs to be documentation of the evaluation.
- **Privacy Notice.** The GDPR requires more detailed privacy notices, with specific wording, that are also clear, understandable, and accessible.
- **Consent.** Under the GDPR, all consent for processing personal data must be express, "freely given, specific, informed and unambiguous." Directive 95/46/EC does not specify modes of acceptable consent, which has resulted in inconsistent application across the EU.
- **Contracts.** Data processing contracts are now required for any entity processing a company's data. Even where a vendor is under the Privacy Shield framework, GDPR-compliance contractual language is required. Further, these contracts are required between companies in the EU. Merely relying on the location of a vendor in an "adequate" jurisdiction is no longer a prudent course of action.

Next Steps: What Should Companies Do Now?

U.S. organizations that have not already begun GDPR preparations should do so immediately. GDPR preparation involves significant time, money, and human resources. It requires additional staffing; new processes for handling, storing, processing and transferring EU personal data; and "baking in" data privacy controls into IT systems that manage such data. In addition, immediate attention needs to be given to ensuring proper mechanisms are in place now for cross-border transfers of EU personal data (e.g., data transfer and processing agreements that incorporate EU Model Contract Clauses, Binding Corporate Rules, if applicable, and Privacy Shield certification).

"Organizations should prepare for GDPR in strategic, team fashion, involving representatives from IT, Legal Privacy, Risk Management, and Business Units that handle EU personal data."

GDPR Preparation

- **Conduct a proportionally detailed Risk Assessment.** Evaluate whether your operations involve processing of EU personal data that is likely to result in a high risk to the rights and freedoms of natural persons, taking into account nature, scope, context, and purposes of processing. Once an enterprise risk assessment is complete, only then will your company need to execute more detailed DPIAs. Do not wait until the GDPR takes effect to undertake this effort.
- **Appoint a Data Protection Officer, if required.** Most companies that process personal data on a large scale will be required to appoint a Data Protection Officer, and will need to undertake an annual Data Privacy Risk Assessment, as part of their due diligence compliance monitoring.
- **Prepare to address data subjects' rights under the GDPR.** This includes developing policies, procedures and process workflows for the following requirements:
  - The new **right to data portability** – a data subject's right to receive his/her personal data and to move and store it for further personal use on a private device, or to transmit that data to another controller.
  - The expanded **right of access and correction** to personal data, that includes more information that must be provided, on request, to a data subject; as well as having embedded procedures for ensuring the stored data is accurate, relevant, and proportional.
  - The **right to erasure** (the **"right to be forgotten"**). Organizations will need to be prepared to meet an even greater administrative burden in relation to these rights.
  - **The right to object to processing.** The GDPR transfers the burden of proof from the data subject to the organization for showing that it either has compelling grounds for continuing the processing or that the processing is necessary in connection with its legal rights.
- **Immediately begin planning for implementing privacy "by design" and "by default."** Companies must ensure that privacy protections are built into current and future IT systems that service or process EU personal data. These privacy controls must exist "by default" and companies must demonstrate that they have adequate data security, and compliance monitoring processes in

GDPR Preparation continued –

place. Companies should implement appropriate technical and organizational measures to ensure that, by default, only EU personal data that are necessary for each specific purpose of the processing are processed.

- **Build a data breach reporting protocol.** Under the GDPR, any breach of EU personal data generally must be reported to the local Data Protection Authority (DPA) within 72 hours, unless the organization conducts and documents a speedy and thorough data breach investigation that demonstrates "that the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals."

Preparation for Privacy Shield Framework Certification

If a company chooses to self-certify with the U.S. Department of Commerce under the Privacy Shield Framework, it is important that before it does so, it has taken the steps below. Compliance with the framework is required ***at the time of filing***. A table is provided in Appendix B that compares the Safe Harbor requirements with those of the Privacy Shield. The company will need to demonstrate compliance with these steps as part of their Privacy Shield application.

> *"Designate a Privacy Shield contact who must administer a process workflow to respond to direct complaints from individuals within 45 days of receipt, and interface directly with the Department of Commerce, the FTC and EU Data Protection Authorities."*

- **Adopt a Privacy Policy.** Adopt a clear, concise and easy-to-understand privacy policy that complies with the Privacy Shield Principles, and that incorporates their specific language and requirements
- **Designate a Privacy Shield contact.** Designate a Privacy Shield contact who must administer a process workflow to respond to direct complaints from individuals within 45 days of receipt, and interface directly with the Department of Commerce, the FTC and EU Data Protection Authorities.
- **Implement an Independent Recourse Mechanism.** Designate an independent recourse mechanism to further investigate individuals' unresolved complaints regarding the organization's compliance with the Privacy Shield.
- **Amend existing onward-transfer contracts.** Amend existing data transfer and processing agreements to provide for joint liability for data controllers and data processors, and to ensure that onward transfers are supported by authorized mechanisms (Model Contract Clauses, Binding Corporate Rules, Privacy Shield) that require the same level of data protection as required by the EU Data Directive, and soon, the GDPR.
- **MOST IMPORTANTLY:** Make sure that your company is ready to comply with the GDPR's policy, procedure, process, technical, and compliance requirements. The clock is ticking toward May 25, 2018; there is no time to waste in preparing for compliance with these significant GDPR provisions.

Appendix A

Comparison of EU Data Protection Directive 95/46/EC and GDPR

	Directive 95/46/EC	vs.	GDPR
Authority	Required Member States to implement its principles through national legislation		GDPR is directly applicable across all Member States; no national implementation is required
Application	Applied to data controllers and direct processors only		Applies to data controllers, processors, and sub-processors
Enforcement	Inconsistent enforcement from state to state; low penalties		Bet-the-company sanctions
Data Protection Officers	Not required		Required for companies meeting certain criteria (under which most large companies will qualify)
Consent	Varying types of consent		Prior, express consent only
Definition of Personal Data	Broad, but didn't include some of the usual kinds of data		Expanded to include location data, online identifiers, and genetic data
Data Privacy Impact Assessment	Suggested		Required when collecting and processing sensitive or great in volume personal data
Privacy Notice	Required with suggested language		Required with specific language
Breach Notification	Not required		Required within 72 hours

Appendix B

Differences Between U.S. - EU Safe Harbor and EU-U.S. Privacy Shield

The table below outlines the major differences between the former Safe Harbor Framework and the current Privacy Shield Framework:

	Safe Harbor	vs.	Privacy Shield
Privacy Policy	Companies must post a privacy policy that discloses: types of personal data collected, purpose for collection, contact information for questions and complaints, categories of third-party onward recipients, data subject choices for limiting use, statement of compliance with the Framework, disclose independent recourse mechanism, ability to opt-out of onward disclosure (except for service providers), and opt-in for sensitive information, offer ability to opt-out of uses for materially different purposes, and opt-in when the information to be shared is sensitive.		Same. Additionally, a company must provide the following newly required information: link to Department of Commerce Program List, the right of data subjects to access data, acknowledgment of jurisdiction of FTC, DOT, or another U.S. enforcement agency, obligation to disclose personal data in response to lawful requests from law enforcement, acknowledge liability in relation to onward data transfers. Further, the new obligations under Privacy Shield (e.g., binding arbitration) need to be disclosed in the Privacy Policy.
Onward transfers to controllers	Give data subject notice of the transfer and the opportunity to opt out.		Notice and opt-out generally are still required. Enter contract stating that data can only be processed for limited and specific purposes consistent with data subject's consent and require the third-party controller to notify the organization if it makes a determination that it can no longer meet privacy principles.
Onward transfers to processors (service providers)	Confirm service provider has subscribed to the Safe Harbor Principles, is subject to Directive or another adequacy determination, or agrees to provide the level of protection in the Safe Harbor Principles by contract.		In addition to confirming the processor's commitment to the Privacy Shield Principles, the controller must contract with the processor to comply with the obligations set out in the Privacy Shield Principles.
Security	Organization must implement reasonable precautions to protect from loss, misuse, unauthorized access, disclosure, alteration, and destruction.		Same.
Data integrity	Organization must take reasonable steps to ensure that personal data is reliable for its intended use, and that it is accurate, complete, and current.		Same. Additionally, organization must take data minimization steps to retain information only for as long as it serves the processing purpose(s).
Access	Organization must provide: data subject's right to correct information about them, except when unduly burdensome to do so or third-party rights are implicated, data subject's right to erase information about them if inaccurate, except when unduly burdensome to do so or third-party rights implicated.		Same. Additionally, organization must provide data subject's right to obtain confirmation of whether organization has data about them.
Regulatory oversight	Independent recourse mechanisms for consumer complaints are required. Where those are insufficient, FTC jurisdiction may be invoked. Organization is required to respond directly to DPAs in the limited circumstance that human resource data is transferred.		Participants must provide independent recourse mechanism for free (as opposed to affordably), accept binding arbitration, and accept potential liability to data subject for violation. Additionally, organization is required to respond to inquiries and requests from the Department of Commerce, along with the FTC.

Additional Information

For more information about the GDPR and Privacy Shield, and how they interact, please visit our ***Carpe Datum Law*** and ***Global Privacy Watch*** blogs (www.carpedatumlaw.com and www.globalprivacywatch.com). We are happy to discuss these developments, and the impact on your company at any time, via phone, in person, or webcast. For more information, please contact Scott A. Carlson at scarlson@seyfarth.com, John P. Tomaszewski at jptomaszewski@seyfarth.com, Darren G. Gardner at dgardner@seyfarth.com, or Peter Talibart at ptalibart@seyfarth.com.

Seyfarth's eDiscovery and Information Governance Practice Group

The attorneys of the eDiscovery and Information Governance practice group provide advice and innovative solutions in all facets of electronic discovery and information governance. Clients rely on Seyfarth Shaw's eDiscovery and Information Governance practice group for counsel on eDiscovery issues including pre-litigation preparedness and the preservation, collection, review and production of electronic information in litigation, as well as information governance issues related to data security, privacy and records management. We work diligently to ensure that our clients' data privacy and security policies, procedures, and practices are compliant with all applicable laws both in the United States and abroad.

Seyfarth's Global Privacy and Security (GPS) Team

The attorneys of the Global Privacy and Security (GPS) Team help clients address a wide variety of domestic and international data privacy, data security, and cybersecurity legal issues relating to data breach response and remediation, data privacy and security risk assessments, data and data privacy and data security policies, processes, and technology. Seyfarth Shaw's GPS Team works closely with corporate chief information security officers (CISOs) and their staffs to reduce legal risk and cost in such incidents, including working as trusted "quarterback" to manage development and implementation of a communication plan, as well as notices to authorities and affected individuals in particular cases. Seyfarth Shaw's GPS Team is often asked to participate in data privacy, data security, and cybersecurity testing and trial exercises with clients. Our GPS Team attorneys who are certified ethical hackers work closely with internal and external information security professionals to ensure use of state-of-the-art tools and strategies that are reasonable and legally defensible. The GPS Team as well as the eDiscovery and Information Governance Practice Group coordinate closely to handle these issues in the context of both day-to-day business operations as well as specific litigations and regulatory proceedings.

SEYFARTH SHAW

Atlanta	**London**	**San Francisco**
Boston	**Los Angeles**	**Shanghai**
Chicago	**Melbourne**	**Sydney**
Hong Kong	**New York**	**Washington, D.C.**
Houston	**Sacramento**	