KILPATRICK TOWNSEND

General Data Protection Regulation (GDPR)

GDPR
At a Glance

What Is the General Data Protection Regulation (GDPR)?

The GDPR will replace the current EU Data Protection Directive 95/46/EC and significantly change EU Data Protection law. The GDPR will apply directly in all EU member states and significantly impact companies processing personal data, including many companies located outside of the EU.

When is the GDPR Effective?

The GDPR comes into force on May 25, 2018.

Does the GDPR Apply to Your Company?

The GDPR applies to any company that:

- Is established in the EU that process personal data, regardless of whether the processing takes place in the EU or outside the EU.
- Is based outside of the EU:
  - Processes activities related to offering goods or services to data subjects in the EU (regardless of whether payment is required)
  - Monitors an individual's behavior if the behavior takes place within the EU.
- Sells goods to data subjects located in the EU through online stores, accordingly these companies are subject to the GDPR (including portfolio companies).

Why Does the GDPR Matter?

The GDPR will significantly affect the way companies collect, store and protect the personal information of customers, clients and visitors to a company website. The Data Protection Authorities (DPAs) will have the power to levy fines for non-compliance with increasing levels of severity, up to €20,000,000 or 4% of the total worldwide annual turnover for the previous financial year (whichever is higher).

What Are the New Compliance Obligations?

The GDPR's new obligations:

- Broader applicability than the EU Data Protection Directive, reaching companies beyond the borders of the EU.
- Create direct statutory obligations for data processors.
- Establish a duty to perform Data Protection Impact Assessment in cases of high-risk processing activities.
- Mandate the duty to appoint a Data Protection Officer (DPO) in certain cases.
- Expand rights of individuals, to include the right to be forgotten and right to data portability.
- Introduce stricter consent requirements.
- Require notifications to the relevant supervisory authority, and in specific situations, the data subjects, of any security breaches of personal data within 72 hours.

What Does Your Company Need to Do to Prepare for the GDPR?

Below is a list of high-level considerations that your company should address prior to May 25, 2018:

- **Data Mapping.** Document key information about the EU personal data your company holds, including where it came from, where it is stored, with whom it is shared, and how long it is maintained.
- **Records of Processing Activities.** Identify key business processes and determine your company's status as a controller, processor or joint-controller with respect to each key business process. Document information required by Article 30 for each processing activity.
- L**awful Basis.** Identify and document Your company's lawful basis for each processing activity involving EU personal data.
- **Privacy Notices.** Review and update current privacy notices to comply with enhanced GDPR notice requirements.
- **Contracts.** Update vendor contracts with all GDPR-required provisions.
- **Consents.** Identify where your company relies on consent as a legal basis for processing EU personal data. Ensure that consent is valid under the GDPR, including that it is freely given, unambiguous, specific and informed.
- **Breach Response.** Update/implement breach response procedures to ensure your company complies with GDPR breach reporting timelines and notification requirements and implements appropriate security safeguards.
- **Individual Rights.** Ensure your company has procedures in place for responding to a data subject's requests to exercise their rights under the GDPR including rights of erasure, restriction of processing, data portability, access, rectification, objection and not to be subject to automated decision making.
- **Cross-Border Data Transfers.** Ensure a lawful mechanism is in place for international data transfers.
- **Privacy by Design and Data Protection Impact Assessment.** Ensure that your company has implemented procedures for complying with the GDPR's requirements for Privacy by Design and by Default. Additionally, a process must be in place for conducting Data Protection Impact Assessments on all high-risk processing.
- **Data Protection Officer.** Determine whether your company is required to appoint a Data Protection Officer ("DPO"). The GDPR requires the appointment of a DPO at a minimum where processing involves regular and systemic monitoring of individuals on a large scale, or where sensitive personal data is processed on a large scale.

Understanding the GDPR

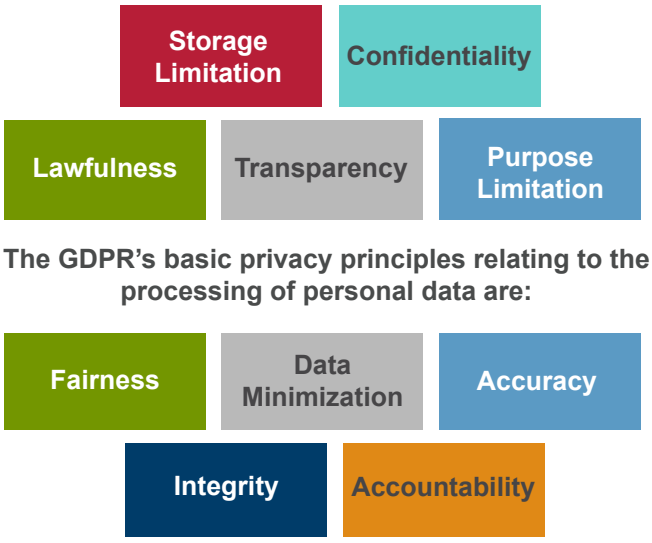
I. What Is the GDPR?

The General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016 (the "GDPR") is the European Union ("EU") Regulation regulating the processing of personal data that will become effective on May 25, 2018. The GDPR replaces the current data protection framework as set out in the Data Protection Directive 95/46/EC (the "Directive").

The Directive does not apply automatically in EU Member States and instead must be adopted into each Member State's national law. As a result of lawmakers in each of the Member States applying their own interpretation to the Directive, the existing EU data protection landscape is a "patchwork" of varying requirements and enforcement patterns. Consequently, companies trying to do business in the EU face inconsistent data protection compliance requirements between different Member States.

The GDPR is intended to harmonize data protection law in the EU by removing the requirement for each Member State to implement the law individually:

- Reinforce individuals' rights.
- Strengthen the EU internal market.
- Ensure stronger enforcement of the rules.
- Streamline international transfers of personal data.
- Set global data protection standards.



The GDPR's basic privacy principles relating to the processing of personal data are:

Key Definitions

According to Article 4(2) of the GDPR, "Processing" means any operation or set of operations which is performed on personal data or on sets of 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, restriction, erasure or destruction.

Under the GDPR, "Personal Data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. It is important to note that more types of data are now in-scope for the regulation. Under the GDPR, the definition of personal data now explicitly includes location data, online identifiers and genetic data. Additionally, the GDPR also includes a broader definition of "special categories" of personal data, commonly known as sensitive personal data, to include the processing of genetic data and biometric data.

II. When Does the GDPR come into Effect?

The effective date for the GDPR is rapidly approaching. The GDPR will come into full force on **May 25, 2018** and there will not be a compliance "grace period," so it is critical that organizations that are subject to the GDPR begin their preparations now.

III. What Do Companies Need to Know about the GDPR?

With its extraterritorial reach, wide scope, direct liability for processors and high fines, the GDPR will represent a significant compliance challenge for many companies. It is critical that U.S. companies assess and understand how the GDPR may apply to them and, if applicable, what will be required for compliance. Below is an overview of key requirements and considerations.

A. The GDPR Applies Broadly

The GDPR has a broader extraterritorial reach than the Directive - it applies to any processing of personal data related to EU citizens and non-EU citizens living in the EU, even where the data controller is located in a country outside of the EU, if processing relates to (i) the offering of goods or services to such individuals or (ii) monitoring their behavior.

B. The Stakes Are High

The GDPR tasks EU supervisory authorities (i.e., Data Protection Authorities ("DPAs")) with "monitoring and enforcing the application" of the Regulation in their respective territories. In order to do this, DPAs are granted a number of investigative powers under the GDPR. These investigatory powers are supplemented by certain corrective measures (including fines) which DPAs may exercise to sanction or remediate any violations of the GDPR. Under the GDPR, DPAs may impose administrative fines for violations of the GDPR that are "effective, proportionate and dissuasive." The GDPR sets out two tiers of fines.

Tier 1	Tier 1 fines amounts up to €10,000,000 or 2% of total worldwide annual turnover (whichever is the greatest).

Examples of GDPR Articles Related to Tier 1 Fines

- Provisions on the obligation to obtain consent from a parent or legal guardian where information society services are provided directly to a minor (Article 8)
- Data protection by design/by default (Article 25)
- Obligation for controllers to enter into an agreement with their processors setting out the responsibilities of processors (Article 28)
- Obligation for controllers and processors to implement appropriate technical and organizational measures to ensure the security of the data that is being processed (Article 32)

Does the GDPR Apply to Your Organization?

Does your organization:

1. Have an established presence in the EU?
2. Process personal data of data subjects in the EU in connection with offering such individuals goods or services?
3. Process personal data on data subjects in the EU in connection with monitoring their behavior (including e.g., online through your website)?

What Companies Should Do

- ☑ Raise awareness internally among key stakeholders.
- ☑ Educate senior management about GDPR requirements and potential impacts of non-compliance.
- ☑ Begin compliance initiatives now; do not wait until spring!

Tier 2	Tier 2 fines can be up to €20,000,000 or 4% of total worldwide annual turnover (whichever is the greatest).

Examples of GDPR Articles Related to Tier 2 Fines

- Provisions on the basic data processing principles (Article 5)
- Lawful conditions for processing personal data (Article 6)
- Conditions for obtaining valid consent (Article 7)
- Special categories of data (i.e. sensitive personal data) (Article 9)
- Data subjects' rights (Articles 12-22)
- International data transfers

C. Data Processors Now Have Direct Liability

Although the concept of "data controllers" and "data processors" are fundamentally the same under the GDPR and the Directive, the GDPR now imposes direct obligations on processors, whereas under the Directive, the responsibility for data protection fell primarily on the data controller.

Under the GDPR, data processors are directly required to:

- Maintain records of their processing activities.
- Comply with breach notification requirements.
- Implement appropriate security measures.
- Cooperate with data protection authorities.
- Appoint a Data Protection Officer where required.
- Comply with cross-border data transfer requirements.

Significantly, data subjects can now bring claims directly against data processors. A processor will be liable for the damage caused by its processing activities where it has not complied with obligations under the GDPR that are specifically directed to processors or where it acted outside or contrary to lawful instructions from the controller.

What Companies Should Do

- ☑ Identify where they operate as a controller or joint controller versus a processor.
- ☑ Ensure compliance with additional processor obligations.
- ☑ Update contracts as necessary to address direct liability.

Companies need to be aware of their new responsibilities and increased risk profile while they are acting solely as a processor of EU personal data.

D. Companies Must Keep Records of Their Processing Activities

Both controllers and processors are required by Article 30 of the GDPR to keep records of their data processing activities.

Controllers Must:

- Name and provide contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer.
- Document purposes of the processing.
- Describe the categories of data subjects and of the categories of personal data.
- Specify categories of recipients to whom the personal data has been or will be disclosed including recipients in third countries or international organizations.
- Identify transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards.
- Indicate envisaged time limits for erasures time limits for erasure of the different categories of data.
- Provide a general description of the technical and organizational security measures referred to in Article 32(1).

Processors Must:

- Name and provide contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer.
- Describe the categories of processing carried out on behalf of each controller.
- Identify transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards
- Provide a general description of the technical and organizational security measures referred to in Article 32(1).

What Companies Should Do

- ☑ Conduct a data mapping/inventory exercise to document key business processes that involve collection, use, storage, transfer or other processing of EU personal data.
- ☑ Determine which categories of EU personal data are used in connection with each processing activity.
- ☑ Determine whether the organization is a controller or a processor with respect to each processing activity.
- ☑ Understand and document data flows, including cross-border data flows, in connection with each processing activity.
- ☑ Understand and document the information lifecycle of personal data processed in connection with each processing activity.

E. Companies Need a Lawful Basis to Process Personal Data

The GDPR requires that companies have a lawful basis for all processing of personal data. Pursuant to Article 6 of the GDPR, processing shall be lawful only if processing:

- Is consented to by the data subject for one or more specific purposes (for more information about consent see below).
- 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.
- Is essential for compliance with a legal obligation to which the controller is subject.
- Protects the vital interests of the data subject or of another natural person.
- 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 in a third party to whom the data are disclosed.
- Is required for the purposes of the legitimate interests pursued by the controller or by the 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.

What Companies Should Do

- ☑ Understand and document the legal basis on which they collect and use data.
- ☑ Assess whether these basis remain valid under the GDPR and, if not, revisit and adapt them as necessary.
- ☑ Where relying on legitimate interests as the legal basis for processing, conduct an assessment and document how the company determined that its legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child.

F. Consent Is More Difficult to Obtain

The GDPR imposes stricter rules on obtaining consent. Companies will no longer be able to rely on “opt-outs“ or pre-checked boxes to justify data processing. As under the Directive, consent must be freely given, specific, and informed. However, the GDPR now also requires that consent be unambiguous, given by a statement or a clear affirmative action. Additionally, under the GDPR, the processing of sensitive personal data, and transferring personal data to a third country in the absence of an adequacy decision or appropriate safeguards, requires “explicit” consent. It will no longer be sufficient to infer consent on the basis that notice was provided in a privacy policy or terms of use and a data subject’s continued use of the service.

To be specific, the controller must clearly and precisely explain the scope and the consequences of the data processing. Consent cannot apply to an open-ended set of processing activities and must be clearly distinguishable from other matters. With regard to consent for cross-border data transfer outside of the EEA, the data subject must be informed of the possible risk of such transfer due to the absence of an adequacy decision or appropriate safeguards.

To be freely given, the data subject must have genuine free choice. Where there is a clear imbalance between the controller and the data subject, consent is presumed not to have been freely given. The employer/employee relationship is the most common example of an imbalance between the controller and the data subject, but there is some risk that a doctor/patient relationship would be viewed as an imbalance. The data controller would have to make it clear to the data subject that he/she can refuse to give consent, or may withdraw his/her consent at any time, without impacting his/her treatment.

In order for consent to be informed, the GDPR provides that the nature of the processing should be explained in an intelligible and easily accessible form, using clear and plain language which does not contain unfair terms. Moreover, the data subject should be aware of at least of the identity of the controller and the purposes for which the personal data will be processed.

If the consent is given in a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

The data subject has the right to withdraw his or her consent at any time. Such withdraw will not affect the data that was processed on the basis of consent before it was withdrawn. The data subject must be informed of this right prior to giving consent.

The controller must be able to demonstrate that the data subject has consented to the processing of his or her personal data.

What Companies Should Do

- ☑ Identify where consent is relied on as the basis for processing personal data.
- ☑ Determine if another legal basis can more appropriately be relied upon.
- ☑ If consent is required, review existing consent processes and determine if they are valid under the GDPR.
- ☑ Implement new mechanisms for obtaining valid consent and allowing individuals to withdraw consent, as required.
- ☑ Ensure processes/capabilities are in place to retain records of consents obtained and withdrawn.
- ☑ Update privacy notices as required.

G. Individuals Have More Expansive Rights

The GDPR will give individuals more control over their personal data and will make it easier for them to access it. Controllers and processors will need to ensure that they will be able to comply if a data subject lawfully requests to exercise his or her rights under the GDPR. Individual rights under the GDPR give data subjects the right to:

- **Transparency.** Receive certain information from the data controller in a concise, intelligible and easily accessible form that uses clear and plain language (for more information, see Privacy Notices below).
- **Access.** Access their personal data.
- **Rectification.** Have personal data about them that is incorrect corrected.
- **Objection.** Object to the processing of their personal data where the lawful basis for processing is either "public interest" or "legitimate interests." Data subjects also have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.
- **Erasure (Right to be Forgotten).** Have data deleted when the individual no longer wants his or her personal data to be processed, and provided that there are no legitimate grounds for retaining it, the data must be deleted.
- **Restriction of Processing.** Restrict the processing of personal data in certain circumstances (e.g., the accuracy of the data is contested, the processing is unlawful etc.).
- **Data Portability.** Receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have their personal data transmitted directly between controllers.
- **Right Not to Be Evaluated on the Basis of Automated Decision Making.** Be the subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her.

What Companies Should Do

- ☑ Ensure processes and procedures are in place for responding to requests from data subjects to exercise their rights.
- ☑ Conduct training with relevant staff on responding to data subjects' requests.
- ☑ Implement any process or system changes necessary to comply with the new requirements.

H. Restrictions on Profiling

As mentioned above, under the GDPR, individuals have a right not to be subject to decisions based solely on automated processing, including profiling, which produce legal effects concerning him or her or significantly affects him or her. 'Profiling' is defined under Article 4 of the GDPR as "any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." Data subjects also have the right to be informed of the "consequences" of profiling decisions. Articles 13 and 14 of the GDPR require disclosure of "the existence of automated decision making including profiling" along with "the significance and the envisaged consequences of such processing for the data subject."

The profiling is authorized by law if the controller is subject to a law in one of the European Economic Area ("EEA") member states that authorizes the profiling activity (e.g., to monitor and prevent).

Profiling may be permitted if the activity is necessary for the purpose of entering into (or performing) a contract with the individual, and the controller is capable of demonstrating (a) the existence of a contract or pre-contractual arrangements between the data subject and the controller and (b) that it is necessary to profile the individual in order to enter into or perform such contract.

Finally, profiling may be permissible if the individual concerned has given his/her explicit consent to use his/her personal data for profiling purposes. If the data subject provides his/her explicit consent, then the controller may use his/her personal data for profiling purposes.

What Companies Should Do

- ☑ Conduct Data Protection Impact Assessments on profiling activities to determine where profiling restrictions apply.
- ☑ Determine whether human interventions can be introduced such that individuals are no longer subject to processing based solely on automated decisions.
- ☑ Obtain consent for profiling activities when necessary.
- ☑ Update privacy notices as required to provide data subjects with information about the right to object to profiling.

I. Privacy Notices Must Be More Detailed in Order to Meet Transparency Requirements

The GDPR requires that controllers be transparent with data subjects regarding the processing of their personal data. Controllers must provide certain minimum information to data subjects, regarding the collection and further processing of personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Any information provided to children should be in such a clear and plain language that the child can easily understand. When collecting personal data relating to a data subject from the data subject, a controller must provide the data subject with the following information at the time the personal data is collected.

- Identity and contact details of the controller and, where applicable, of the controller's representative.
- Contact details of the Data Protection Officer.
- Purposes of processing and the legal basis for the processing.
- Recipients, or categories of recipients, of the personal data.
- Details of data transfers outside the EU, including how the data will be protected (e.g., the recipient is in an adequate country; Binding Corporate Rules or Standard Company Clauses are in place etc.); and how the individual can obtain a copy of the BCRs or other safeguards, or where such safeguards have been made available.
- Retention period for which the personal data will be stored, or if that is not possible, then the criteria used to determine that period.
- Individual's right to access and port data, to rectify, erase and restrict his or her personal data, to object to processing and, if processing is based on consent, to withdraw consent.
- Individual's right to complain to a supervisory authority.
- Whether there is a statutory or contractual requirement to provide the data and the consequences of not providing the data.
- If there will be any automated decision making – together with information about the logic involved and the significance and consequences of the processing for the individual.

J. Vendor Contracts May Require Updates

The GDPR will require many companies to amend their vendor contracts. Under the GDPR, where a controller appoints a processor to process personal data on its behalf, the processing must be governed by a binding written contract (or equivalent legal act) that sets forth the subject matter and duration for processing, nature of the processing, and type of personal data and categories of data subjects, and imposes certain obligations on the processor, including that the processor:

- Implement appropriate technical and organizational measures.
- Obtain prior specific or written general authorization for subprocessing.
- Flow down of terms to subprocessors.
- Remain fully liable for the performance of subprocessors.
- Process only personal data in accordance with the controller's instructions.
- Notify the controller if the processor believes the controller's instructions violate applicable data protection law or if it will be unable to comply.
- Ensure all persons authorized to process personal data are subject to confidentiality requirements.
- Allow for and contribute to audits by the controller.
- Transfer only personal data to non-EEA locations with appropriate safeguards.
- Assist the controller with responding to data subjects' requests to exercise their rights.
- Assist the controller with complying with its data breach notification obligations.
- Make available to the controller all information necessary to demonstrate compliance with these obligations.
- Delete or return all personal data upon termination of the contract.

What Companies Should Do

- ☑ Review and update existing privacy notices to include GDPR-required information.

What Companies Should Do

- ☑ Inventory vendor contracts that are subject to the GDPR.
- ☑ Prioritize key vendor contracts.
- ☑ Prepare GDPR-compliant contract addendum.
- ☑ Negotiate contract amendments with vendors.

K. Cross-Border Data Transfers Are Stricter

Under the Directive and the GDPR, personal data may be transferred outside of the EEA when jurisdiction in which the data importer is located is deemed to provide an adequate level of data protection; the data exporter puts in place appropriate safeguards; or if derogation or exemption applies.

The European Commission has recognized 11 jurisdictions as adequate. The United States is not considered to provide an adequate level of data protection. At present, standard contractual clauses (also known as model contract clauses), Privacy Shield certification and binding corporate rules ("BCRs") are the means by which an adequate level of protection can be ensured when transferring personal data to the U.S. or another non-adequate country absent an applicable derogation. The GDPR will introduce new instruments (e.g., approved codes of conduct, approved certification mechanism and additional means of contractual clauses) and derogations (e.g., one-time transfers in the event of a compelling legitimate interests of the controller).

What Companies Should Do

- ☑ Determine cross-border data transfers based on data mapping analysis.
- ☑ Assess whether current data transfer mechanisms are adequate.
- ☑ Where necessary, implement appropriate cross-border data transfer solutions.
- ☑ Review notices and consents in order to ensure that they accurately describe cross-border data transfers.
- ☑ Ensure relevant obligations are flowed down through subcontractor chains.

L. Data Impact Assessments Must Be Conducted on High-Risk Processing

The GDPR contains requirements pertaining to conducting Data Protection Impact Assessments (DPIAs), to identify and minimize non-compliance risks. Specifically, controllers must ensure that DPIAs has been conducted on any "high-risk" processing activity before it is commenced – focused on the risk of infringing a natural person's rights and freedoms. "Large scale" processing of sensitive data, or profiling activities, are cited as illustrative examples of high-risk processing. The GDPR also requires that data controllers consult DPIAs when they cannot find sufficient measures to mitigate the risks of a processing activity and the residual risks are still high, as well as in specific cases where required by EU Member State law.

At a minimum, the GDPR requires that DPIAs:

- Describe the processing activities and their purpose.
- Assess the need for, and proportionality of, the processing, and the risks arising and measures adopted to mitigate those risks, in particular safeguards and security measures to protect personal data and comply with the GDPR.

M. Breach Notification Requirements Are Enhanced

The GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." Controllers must notify the supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it." If not made within 72 hours, controllers must provide a "reasoned justification" for the delay. Article 33(1) contains a key exception to the supervisory authority notification requirement: notice is not required if "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." In the event of a data breach that presents a high risk to data subjects, the controller must notify the affected data subjects without undue delay.

When a data processor experiences a personal data breach, it has an obligation to notify the data controller without undue delay.

What Companies Should Do

- ☑ Develop a process for conducting DPIAs on high-risk processing activities.
- ☑ Develop DPIAs template and policy/ identify third party DPIAs solutions.
- ☑ Conduct DPIAs on any existing high-risk processing activities.

What Companies Should Do

- ☑ Review existing breach response policies.
- ☑ Update/draft breach response policy to comply with GDPR requirements.
- ☑ Prepare template breach notification letters.
- ☑ Test breach response policy (e.g., by carrying out table top exercises).
- ☑ Conduct security audit.

N. Appointment of a Data Protection Officer (DPO) Is Required for Some Organizations

The GDPR requires a controller or processor to appoint a DPO if its data processing activities:

- Involve regular and systematic monitoring of data subjects on a large scale.
- Process Sensitive Personal Data on a large scale.

The EU's Article 29 Working Party has published Guidelines on the role of DPOs under the GDPR. To determine whether a given processing activity is "large scale," the guidelines recommend businesses:

- Consider the number of individuals affected (either in abstract, or as a percentage of the relevant population).
- Evaluate the volume of data, and/or the number of categories of data, being processed.
- Identify the duration or permanence of the processing activities.
- Assess the geographic scope of the processing activities.

The DPO's tasks should, as a minimum, include: advising their colleagues and monitoring their organization's GDPR/privacy law/policy compliance, including via training and awareness raising, running audits, advising regarding DPIAs, and cooperating with supervisory authorities.

What Companies Should Do

- ☑ Conduct an assessment to determine whether the organization is required to appoint a DPO.
- ☑ Determine if the organization will appoint a DPO voluntarily.
- ☑ Consider whether to appoint an internal DPO or outsource the role.
- ☑ Determine how the DPO will fit into the organization. Where will they be located geographically? What department and team will they be on? Will you have one DPO or a DPO supported by a team?
- ☑ Ensure the DPO will report to the highest level of management.
- ☑ Ensure that the DPO's tasks are consistent with GDPR requirements.
- ☑ Ensure the DPO is free from conflicts of interests.
- ☑ Consider how to provide the DPO with the necessary resources.
- ☑ Publish the DPO's contact details and notify the supervisory authority.

O. Appointment of a Representative Is Required for Some Organizations

A controller established outside of the EU must appoint a representative in one of the Member States in which the controller offers goods or services or monitors EU residents, unless the processing is occasional, small-scale and does not involve Sensitive Personal Data. A representative may be subject to enforcement actions by data protection authorities in the event of non-compliance by the controller. Controllers (and their representatives, if any) are required to cooperate, on request, with DPAs in the performance of their tasks.

What Companies Should Do

- ☑ Evaluate whether non-EU companies that track or target EU data subjects need to have an EU representative or whether an exception applies.

P. Concepts of Privacy by Design and by Default Is Codified

The GDPR codifies the new concepts of "privacy by design" and "privacy by default." Data controllers are required to implement appropriate technical and organizational measures, which are designed to integrate the necessary safeguards into the processing. Specifically, controllers must ensure that, both in the planning phase of processing activities and during the processing, Data Protection Principles and appropriate safeguards, are addressed and implemented.

What Companies Should Do

- ☑ Adopt policies and procedures relating to pseudonymization and data minimization.
- ☑ Ensure product development teams receive privacy training.
- ☑ Require consultation with the privacy office early in the product development lifecycle.

EU GDPR
Topic Guide

Topic	Sub-topic	References
Accountability, Security and Breach Notification	Privacy by design and security	Recitals: 74–78 Article: 25, 32, 33, 34
	Pseudonymization	Recitals: 26, 28, 29, 156 Articles: 25, 40, 89
	Personal data breach notification standards	Recitals: 85–88 Articles: 33, 34, 70, 83, 84
	Information notices	Recitals: 58, 60, 61, 62 Articles: 12, 13, 14
Certifications, Seals, and Marks	Voluntary compliance-signaling tool	Recitals: 46, 57, 58, 64, 70, 83, 100 Articles: 24, 25, 28, 32, 42, 43, 83
Codes of Conduct	Voluntary compliance-signaling tool	Recitals: 77, 81, 98, 99, 148, 168 Articles: 24, 28, 32, 40, 41, 83
Consent	Affirmative consent requirement	Recitals: 32, 33, 40, 42, 43 Articles: 7, 8, 9
	Consent for children's data processing/principles for children	Recitals: 38, 58, 75 Articles: 8, 12, 40, 57
	Personal data processing	Recitals: 50, 51 Articles: 5, 6, 9, 14
Consequences for GDPR Violations	Higher penalties and fines imposed by supervisory authorities	Recitals: 146, 148–152 Article: 58, 82, 83, 84
Cross-border Data Transfers	Transfers subject to an adequacy decision	Recitals: 104, 106, 108, 112 Article: 45
	Transfers subject to appropriate safeguards (including binding corporate rules)	Recitals: 107, 108, 110, 168 Articles: 46, 47
	Public interest derogations	Recitals: 10, 50–56, 65, 69, 73, 111, 112, 115, 154, 156, 158 Articles: 5, 6, 9, 14, 17, 21, 49, 89
	Legitimate interest derogations	Recitals: 47–50, 69, 88, 111, 113 Articles: 6, 13, 14, 22, 49
Data Protection Officer (DPO)	Required for all public authorities or large controllers or processors of personal data	Recital: 97 Articles: 9, 10, 37, 38, 39
Individual Rights	Right to erasure and right to restriction of processing	Recitals: 65, 66, 67, 73 Articles: 17, 18, 19
	Right to object/rectification	Recitals: 57, 59, 63, 65, 69, 70 Articles: 15, 16, 21
	Right to data portability	Recitals: 58–63, 68 Articles: 12–15, 20
	Right to legal remedy	Recitals: 4, 141, 142, 143 Articles: 77–80, 82
Profiling	Automated decision making; rights of data subjects	Recitals: 24, 60, 63, 70–73 Articles: 13, 15, 22, 35, 47

Topic	Sub-topic	References
Responsibilities of the Controller	Data protection impact assessment (DPIA)—required for automated data processing and other high risk processing activities	Recitals: 84, 89–94 Articles: 35, 36
	Record of processing activities	Recital: 82 Article: 30
	Data breach notification requirements	Recitals: 85, 86, 88 Articles: 33, 34
	Responsibility to appoint a representative (if not established in the Union)	Recitals: 23, 24, 25, 80 Articles: 3, 27
	Other obligations (data protection, cooperating with supervisory authorities, etc.)	Articles: 12, 13, 14, 24, 25, 26, 29, 31, 32, 82
Responsibilities of the Processor	Record of processing activities	Recital: 82 Article: 30
	Data breach notification requirements	Recitals: 85, 86, 88 Articles: 33, 34
	Responsibility to appoint a representative (if not established in the Union)	Recitals: 23, 24, 25, 80 Articles: 3, 27
	Other obligations (data protection, cooperating with supervisory authorities, etc.)	Articles: 28, 29, 31, 32, 33, 82
Supervisory Authorities/Data Protection Authorities (DPA)	Competence of the supervisory authority	Recitals: 116–123 Articles: 55–59
	Main Establishment Definition	Recital 36
	“One-stop-shop” (Lead DPA) based on location of its “main establishment”	Recitals: 124–138 Articles: 60–66

KILPATRICK TOWNSEND

ANCHORAGE
ATLANTA
AUGUSTA
CHARLOTTE
DALLAS
DENVER
HOUSTON
LOS ANGELES
NEW YORK
RALEIGH
SAN DIEGO
SAN FRANCISCO
SEATTLE
SHANGHAI
SILICON VALLEY
STOCKHOLM
TOKYO
WALNUT CREEK
WASHINGTON D.C.
WINSTON-SALEM

Counsel to Innovative Companies & Brands Around the World

We help leaders create, expand, and protect the value of their businesses and most prized assets. Our attorneys bring a balance of business savvy, technical skills, and creative thinking to the opportunities and issues our clients face daily. From the most complex challenges to the routine, we work together to make businesses better, smarter, more protected, and more successful.

www.kilpatricktownsend.com