EU General Data Protection Regulation (GDPR)
Practical Guidance and Checklists
Series of 10 Monthly Alerts
The EU's General Data Protection Regulation goes into effect on May 25, 2018. GDPR replaces the EU Data Protection Directive. GDPR can apply to US-based businesses even if they do not have offices or employees in the EU. It can also reach activities conducted outside the EU.

The Directive did not regulate US businesses unless the collection or processing occurred within the EU (e.g., if a US-based company had a data center in the EU). Now GDPR clearly has stronger extraterritorial reach than its predecessor.

Businesses collecting and using personal data should know their GDPR obligations. Violators of GDPR face steep penalties. Regulators can fine a company up to 20,000,000 euros or 4% of worldwide annual turnover, whichever is higher.

Follow our three-question flowchart to see if GDPR applies to your company.

**Personal data** means information relating to an identified or identifiable natural person. A person can be identified from information such as name, ID number, location data, online identifier (like an IP or MAC address), or other specific factors.

An offer has to be more than mere internet access (e.g., Do you target customers in an EU Member State? Do you offer your service in the language of an EU Member State? Do you accept euros? Do you offer to ship products to buyers in an EU Member State?).

Monitoring refers to tracking individuals on the internet and any subsequent use of the data to profile an individual (e.g., Do you collect location information about users in the EU? Do you follow EU users as they browse the internet? Do you predict a user’s behaviors based on that information?).

1. Does your company have a branch, office, subsidiary or other establishment in the EU that collects, receives, transmits, uses, stores or otherwise processes personal data (processing need not take place in the EU)?
   - No
   - Yes

2. Does your company offer goods or services to individuals in the EU (paid or free)?
   - No
   - Yes

3. Does your company monitor behavior of individuals in the EU?
   - No
   - Yes

GDPR Applies

GDPR Does Not Apply

---

Contact Us

Our GDPR Compliance Task Force, along with our international network, including our relationships with Lex Mundi member firms, is available to assist and advise clients in efficiently addressing GDPR-related issues. To learn more about the issues in this client alert, please contact Ted Claypoole at ted.claypoole@wbd-us.com or +1 404.879.2410, or Andrew Kimble at andrew.kimble@wbd-uk.com or +44 (0)238 020 8422.
Follow our three-question flowchart to answer the question: “Does GDPR Apply to You?” If “Yes” then you may be required to designate a Data Protection Officer (“DPO”) by May 25, 2018, when the GDPR applies.

Follow our five-step flowchart below to see if you need to designate a DPO:

1. Is your organization a public authority or public body under the applicable EU Member State law?
   - Yes, You Must Designate a DPO
   - No

2. Do your company’s core activities consist of regular and systematic monitoring of EU individuals on a large scale?
   - Yes, You Must Designate a DPO
   - No

3. Do your company’s core activities consist of processing (i) special categories of personal data of EU individuals on a large scale or (ii) personal data relating to criminal offenses and convictions?
   - Yes, You Must Designate a DPO
   - No

4. Even if the answer is “No” to the three questions above, does the law of an individual EU Member State require your company to designate a DPO?
   - Yes
   - No

5. Even if not required under the GDPR to designate a DPO, your company may voluntarily appoint a DPO, and there are benefits to doing so. However, if a company decides to voluntarily appoint a DPO, the company should be aware that EU guidance suggests that the company will be subject to the same obligations and compliance requirements concerning a DPO under the GDPR (and the DPO gets all the same protections) as for mandatory appointments.

Core activities are a company’s key operations to achieve its business goals. A hospital must designate a DPO because processing of special categories of personal data (health records) is a key operation of a hospital and may require regular systematic monitoring of individuals on a large-scale. But if a company collects personal data about its employees to process pay checks, then this activity alone may be an ancillary service (rather than a key operation), and would not alone trigger the requirement to designate a DPO.

Large scale is not defined in the GDPR, but factors to consider include the number of individuals concerned, volume of data and range of data items, duration and/or permanence of data processing, and geographic territory covered (e.g., regional, national, or international).

Special categories of data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data and biometric data used to uniquely identify a natural person, and data concerning health or a person’s sex life or sexual orientation.

Contact Us
Our GDPR Compliance Task Force is available to assist and advise clients in efficiently addressing GDPR-related issues. To learn more about the issues in this client alert, please contact Ted Claypoole at ted.claypoole@wbd-us.com or +1 404.879.2410, or Amy Eames at amy.eames@wbd-uk.com or +44 (0)238 020 8379.
A major change with the GDPR is that data processors now have direct legal obligations under EU privacy law. This is a significant shift from the current EU Directive which only directly obligates the data controllers. Non-compliant data processors face significant fines of up to 4% of global annual turnover or 20,000,000 euros, whichever is higher, and may be directly liable to individuals for damages.

### If the GDPR applies to you, review our checklist below summarizing the data processor's obligations:

- **Appoint a Data Protection Officer** (See: Are You Required to Designate a Data Protection Officer?)
- **Appoint a local representative** (if not established in the EU)
- **Implement appropriate technical and organizational measures to account for security risks and to assist controller in responding to requests of individuals**
- **Keep personal data confidential and obligate personnel to similar confidentiality obligations**
- **Keep meticulous written records and make records available to controller and regulators as required**
- **Notify controller of a data breach incident as soon as possible and provide support**
- **Only process personal data to the extent authorized by controller**
- **Obtain controller’s written permission before engaging sub-processors**
- **Enter into contracts with sub-processors providing the same level of protection as the principal contract with controller**
- **Notify controller if controller’s instructions infringe EU data protection laws**
- **Assist controller in Data Protection Impact Assessment**
- **Delete or return to controller (at controller’s choice) all personal data when no longer providing services**
- **Ensure that GDPR-approved safeguards are in place before transferring personal data across borders (or confirm that the “receiving” country is on the EU Commission’s list of approved countries)**
- **Assist controller in responding to an individual’s exercise of their privacy rights**
- **Cooperate with requests of EU member state regulators**
- **Train employees on GDPR and create company policies on compliance and non-compliance**
- **Update company policies (e.g., online privacy policy and written information security policy)**

### Contact Us

If you have questions about this checklist or for additional information on the GDPR, contact Orla O’Hannaidh at orla.ohannaidh@wbd-us.com or +1 919.484.2339, or Ben Gibson at ben.gibson@wbd-uk.com or +44 (0)2380 20 8449, or any member of our GDPR Compliance Task Force.
Any entity processing personal data on your behalf (i.e., your vendors) must have a written contract in place. The GDPR requires specific language in your vendor contracts. Review steps 1–4 below to bring your vendor contracts in compliance with the GDPR.

1. Do we need to amend our existing vendor contracts? If you answer “yes” to the questions below, then you will be required to update your vendor contracts (see step 4 below).
   - Does the GDPR apply to our company?
   - Does our company use third parties to process personal data on our behalf?
   - Will the contract be in place on and from May 25, 2018 when the GDPR applies?

2. How do we amend our existing vendor contracts? The amendment could take the form of a letter agreement or a more formal amendment. The amendment can take any form so long as it is in writing (including in electronic form), and it binds the processor to the controller.

3. What about any new vendor contracts? You should also incorporate the requirements of Article 28 (see step 4 below) into any new contracts. You can include the required language in any form, such as in a schedule or in the main body of the contract.

4. What language must we add to our existing or new vendor contracts? You must describe the scope of the permitted processing, including the:
   - Subject-matter and duration of the processing
   - Nature and purpose of the processing
   - Type of personal data to be processed and categories of data subjects
   - Obligations and rights of the controller

Vendor must agree to:
   - process the personal data only on documented instructions from you, unless otherwise required by applicable EU or Member State law
   - ensure that persons authorized to process the personal data have committed to confidentiality obligations
   - take all security measures required pursuant to Article 32
   - not use a sub-processor without your prior written authorization
   - assist you with responding to requests from data subjects
   - assist you with your obligations relating to security, data breach notification requirements and data protection impact assessments
   - return to you or delete, at your request, all personal data when services are completed, unless otherwise required by applicable EU or Member State law
   - make information available to you to demonstrate vendor’s compliance with the requirements of Article 28.
   - contribute to audits and inspections you or your auditors carry out.

Contact Us
If you have questions about this checklist or for additional information on the GDPR, contact Orla O’Hannaidh at orla.ohannaidh@wbd-us.com or +1 919.484.2339, or Amy Eames at amy.eames@wbd-uk.com or +44 (0)238 020 8379, or any member of our GDPR Compliance Task Force.

Controller is the entity which determines the purposes and means of the processing of personal data.

Processor is the entity which processes personal data on behalf of the controller.

Processing is any set of operations performed on personal data, such as collection, storage, use and disclosure.

Personal Data means information relating to an identified or identifiable natural person. A person can be identified from information such as name, ID number, location data, online identifier or other factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
U.S. companies already face a panoply of data breach notification laws enacted by 48 States and numerous regulators. Those subject to the GDPR may soon have yet another breach notification requirement to worry about.

Follow our chart below to determine if and when you must provide notice, who you must notify, and what your notice should include.

<table>
<thead>
<tr>
<th>Who Required</th>
<th>When Obliged</th>
<th>Who to Notify</th>
<th>How Quickly</th>
<th>What Notice Must Include</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>“Personal data breach” that is likely to result in a risk to the rights and freedoms of natural persons</td>
<td>“Competent supervisory authority”</td>
<td>“Without undue delay” once the controller becomes aware of the personal data breach</td>
<td>• Nature of the breach (including types and approximate number of individuals and records) • Name and contact details for the data protection officer or alternate point of contact • Likely consequences of it • Measures taken or proposed by the controller to address it • (Reason for delay if notifying after 72 hours)</td>
</tr>
<tr>
<td></td>
<td>“Personal data breach” that is “likely to result in a high risk to the rights and freedoms of natural persons”</td>
<td>Affected individuals If such notice would involve disproportionate effort, then controller may notify via “public communication or similar measure”</td>
<td>“Without undue delay”</td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>“Personal data breach”</td>
<td>Controller</td>
<td>“Without undue delay”</td>
<td>(Unspecified)</td>
</tr>
</tbody>
</table>

NOTE: controllers can address this as a matter of contract and should consider specifying the content to be included in these notices in their contracts with processors.
What is a “personal data breach”?  
“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”

When could a breach be “unlikely to result in a risk to the rights and freedoms of natural person”?  
For example, where the data was already publicly available, or where the data was encrypted and remains accessible to the controller (or adequately backed-up); however, each personal data breach will need to be assessed on its facts

What is the difference between “risk” and “high risk” to persons’ rights and freedoms?  
“High risk” would exist where “the breach may lead to physical, material or non-material damage for the individuals whose data have been breached,” such as “discrimination, identity theft or fraud, financial loss and damage to reputation”

When does the controller become “aware” of the breach?  
“When that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised,” depending on the circumstances, this may allow for “a short period of investigation in order to establish whether or not a breach has in fact occurred”

What is “without undue delay”?  
“As soon as possible” (or immediately, in the case of a processor giving notice to a controller)

Who is the “competent” supervisory authority” when a personal data breach affects individuals in more than one EU Member State?  
The “lead supervisory authority,” i.e., “the supervisory authority of the main establishment or of the single establishment of the controller or processor”

This text leaves open plenty of questions. However, on October 3, 2017, the Article 29 Working Party issued guidelines interpreting these data breach notification requirements. Here are some of the answers:

Key Contacts

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allen O’Rourke</td>
<td>Of Counsel</td>
<td>t: 704.350.6357 e: <a href="mailto:allen.orourke@wbd-us.com">allen.orourke@wbd-us.com</a></td>
</tr>
<tr>
<td>Peter Given</td>
<td>Legal Director</td>
<td>t: +44 (0)238 020 8194 e: <a href="mailto:peter.given@wbd-uk.com">peter.given@wbd-uk.com</a></td>
</tr>
</tbody>
</table>

Contact Us

If you have any questions about the checklist above, contact Allen O’Rourke at 704.350.6357 or allen.orourke@wbd-us.com or any member of our GDPR Compliance Task Force.
The GDPR provides enhanced rights for individuals. Below we summarize the general principles companies must follow when interacting with individuals and we identify the specific rights granted to individuals under the GDPR. We also suggest some practical steps to assist your company’s compliance with this portion of the GDPR.

### General Principles

- Your information and communications with individuals must be concise, transparent, intelligible, accessible and in clear/plain language.
- Rights can be exercised free of charge, unless manifestly unfounded/excessive.
- You must respond to requests and provide information promptly and, generally, within one month (exemptions may apply).

### Individual Rights

- **Right of access to personal data.** An individual has the right to access personal data held by an organization.
- **Right of rectification.** An individual has the right to request the correction of personal data held by an organization to the extent that it is inaccurate or incomplete.
- **Right to data portability.** An individual has the right to request the deletion of personal data where there is no compelling reason for its continued processing.
- **Right to withdraw consent.** An individual has the right to object to automated decision making (including profiling), an individual has the right to withdraw consent at any time, and the process to withdraw consent must be as easy as the process to give consent.
- **Right to object.** An individual has the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling). This right also applies to direct marketing and processing for purposes of scientific/historical research and statistics.
- **Right to restrict processing.** An individual has the right (in certain circumstances) to “block” or suppress the processing of their personal data.
- **Right to object to automated decision making (including profiling).** An individual has the right (in certain circumstances) to object to automated decisions (including profiling) based upon the processing of personal data and request human involvement.
- **Right to erasure/to be forgotten.** An individual has the right (in certain circumstances) to request the deletion of personal data where there is no compelling reason for its continued processing.

### Practical Steps

1. **Review, create and/or update protocols for dealing with individual rights.** Ask and answer questions such as: Can we respond to requests within a month? Will we need any assistance from our processors?

2. **Ensure existing and new internal systems (HR, IT, etc.) are designed to give effect to and comply with these rights.** Ask and answer questions such as: Do we have the ability to correct data? What is the process if an individual requests a copy of their data?

3. **Review and update your existing communications with individuals.** Ask and answer questions such as: Are our public facing policies (e.g., privacy policies) and communications concise, transparent, intelligible, accessible and in clear/plain language?

### Contact Us

If you have any questions about the guidance above or for additional information on the GDPR, contact [Matt Harris](mailto:matt.harris@wbd-uk.com) at +44 2380 20 8146 or [Orla O’Hannaidh](mailto:orla.ohannaidh@wbd-us.com) at 919.484.2339 or orla.ohannaidh@wbd-us.com, or any member of our [GDPR Compliance Task Force](mailto:GDPR_Compliance_Task_Force).
If your company is a controller or processor under the GDPR (for US companies, review this flowchart), then your company must comply with the GDPR’s requirements regarding the transfer of personal data of EU individuals to any country outside of the EU/EEA.

In the absence of an adequacy decision (explained below) and subject to very limited exceptions, controllers and processors are required to ensure that an “appropriate safeguard” or another GDPR-approved mechanism is in place before sending personal data of EU individuals outside of the EU/EEA.

The table below describes the mechanisms commonly used to lawfully transfer personal data of EU individuals outside of the EU/EEA. A full list of the transfer mechanisms can be found in Article 46.

<table>
<thead>
<tr>
<th>Transfer Mechanism</th>
<th>Requirements</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adequacy Decision</strong></td>
<td>• Transfer to a country (or sector within a country) on the European Commission’s (EC) approved list</td>
<td>• No additional steps required (i.e., no requirement to put a contract in place)</td>
<td>• EC periodically reviews these adequacy decisions and may not renew the decision</td>
</tr>
<tr>
<td><strong>Binding Corporate Rules (BCRs)</strong></td>
<td>• Prepare BCRs, which are an intracompany code of conduct, and submit to DPA for approval</td>
<td>• No additional steps required • Can potentially transfer to many different countries not otherwise approved (particularly helpful for multinational companies)</td>
<td>• Only covers intra-group transfers • DPA approval is required • Length of time for approval varies and is uncertain</td>
</tr>
<tr>
<td><strong>Model Contractual Clauses (Model Clauses)</strong></td>
<td>• Include EC-approved Model Clauses in contracts for the transfer of data</td>
<td>• Standard language • Approved by the EC</td>
<td>• EC may update or replace Model Clauses • Current versions of Model Clauses are subject to court review (may be invalidated)</td>
</tr>
</tbody>
</table>

These requirements also apply to the transfer of personal data outside of the 3 EEA countries that are not in the EU (Iceland, Liechtenstein and Norway).
<table>
<thead>
<tr>
<th>Transfer Mechanism</th>
<th>Requirements</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| EU-US and Swiss-US Privacy Shield                      | • Must comply with the Privacy Shield principles, such as transparency in data practices, accountability for transfer of data to third parties and maintenance of data security practices  
• Must also post a Privacy Shield-compliant privacy policy, implement an appropriate recourse mechanism, pay applicable fees, have compliance verification procedures in place, and have a designated contact person for Privacy Shield questions | • Relatively quick approval process  
• Fees to the Privacy Shield and the required payment to the arbitral fund are available on the Privacy Shield website and are based on annual revenue | • Only covers transfer from the EU to the US or Switzerland to the US  
• Must become Privacy Shield certified as a US business  
• Only allowed for businesses regulated by the US Department of Transportation or the US Federal Trade Commission |
| Derogations (see row below on consent – one type of derogation) | • Article 49 outlines a few instances where cross-border transfers are permitted in the absence of an adequacy decision or appropriate safeguards (like Model Clauses and BCRs) | • Allows for transfer in absence of adequacy decision or appropriate safeguard | • Reliance on a derogation is not without risk (and can be challenging to rely on in practice)  
• A company should conduct a careful analysis before opting to rely on a derogation |
| Consent from Individual                                | • Requires explicit consent from the individual authorizing cross-border transfer; must inform the individuals of possible risks of transfer due to absence of adequacy decision and appropriate safeguards | • Allows for transfer in absence of adequacy decision or appropriate safeguard | • Consent under the GDPR must meet very specific requirements  
• Requires detailed record keeping of obtained consent and specific disclosures needed  
• Requires internal processes and procedures in place  
• Individual can withdraw consent |

Contact Us

If you have questions about the guidance or for additional information on the GDPR, contact Orla O’Hannaigh at orla.ohannaigh@wbd-us.com or +1 919.484.2339, Taylor Ey at taylor.ey@wbd-us.com or +1 919.484.2306, or Becca Stringer at rebecca.stringer@wbd-uk.com or +44 (0)113 290 4420, or Matt Harris at matt.harris@wbd-uk.com or +44 2380 20 8146, or any member of our GDPR Compliance Task Force.
If your company is a data controller under the GDPR (for US companies, follow this flowchart), then your company will need to update its privacy policy or privacy notice. Under the GDPR privacy policies must contain more detailed disclosures, while also being understandable and accessible. Even under the current privacy laws, EU regulators have demonstrated they will enforce rules on transparency in privacy disclosures. On February 16, 2018, a Belgian court threatened to fine Facebook US $125 million for failure to disclose its personal data collection practices. These fines may be steeper after May 25th since the GDPR increases the maximum penalties.

Use the checklist below to identify the key disclosure requirements for privacy policies.

### Information about processing of personal data
- Purpose of processing
- Legal basis for processing (e.g., consent, performance of a contract, necessary for the purposes of the legitimate interests of the data controller)
- Legitimate interests of the controller (if any)
- Whether automated decision-making, including profiling, will take place (this includes details of the significance and the potential consequences of such processing for the individual)

### Details about collection and use of personal data
- Categories of personal data collected
- Recipients or categories of recipients that receive personal data
- Any transfers of personal data to countries outside of the EEA (and the applicable safeguards in place)
- Data retention policy (i.e., how long the data will be stored for or the criteria used to determine that period)
- Any automated processing of personal data that will take place (including profiling) and how decisions will be made, the significance and any consequences of such processing
- Whether provision of personal data is part of a statutory or contractual requirement and possible consequences if individual refuses to provide personal data

### Existence of individual rights
- Right of access to personal data
- Right to rectification of personal data held where it is incorrect or incomplete
- Right of erasure of personal data (“right to be forgotten”) if certain grounds are met
- Right to restrict/suspend processing of personal data
- Right to complain to a supervisory authority
- Additional rights that may apply in certain instances:
  - Right of data portability (if processing is based on consent and automated means)
  - Right to withdraw consent at any time (if processing is based on consent)
  - Right to object to processing (if processing is based on legitimate interests)
  - Right to object to processing of personal data for direct marketing purposes

### Contact information
- Name and contact details for data controller (and any representative)
- Name and contact details for data protection officer (“DPO”), if a DPO is appointed

---

**Contact Us**

If you have questions about the checklist or for additional information on the GDPR, contact Ted Claypoole at ted.claypoole@wbd-us.com, Orla O’Hannaidh at orla.o hannaidh@wbd-us.com, or Darryl Webb at darryl.webb@wbd-uk.com, or any member of our GDPR Compliance Task Force.
Q: What Is Brexit and When Is It Due to Happen?
A: Following the referendum of 23 June 2016 and the United Kingdom’s subsequent notification under Article 50 of the Lisbon Treaty, the UK’s membership of the European Union is due to end on 29 March 2019, subject to any transitional or implementation period that may be agreed with the EU (and ratified by its continuing member states).

Q: Will Brexit Stop the GDPR Applying in the UK?
A: No, the GDPR will apply in the UK on and from 25 May 2018. The UK still will be a Member State of the European Union at that point. Brexit does not take effect until 29 March 2019.

Q: How Will Data Protection Law Operate in the UK post-Brexit?
A: The Data Protection Bill (the “Bill”) will replace the Data Protection Act 1998 and will implement the GDPR into the law of England and Wales. The Bill is currently under legislative review. The Bill performs two core functions: (1) it will implement the GDPR into the law of England and Wales, including the UK’s “derogations” under the GDPR (Derogations are elements of the GDPR which can be adapted by each Member State.); and (2) it will ensure that at the point the UK exits the EU, and GDPR ceases to apply directly, the UK will have a data protection regime which is largely aligned with that of the remaining EU member states.

Q: What is the Current Status of the Bill?
A: A consolidated version of the Bill was published on 23 March 2018 and captures the debates that have taken place to date.

Brexit, an Unprecedented Event

Whether Brexit takes place on 29 March 2019 or is effectively deferred until end of a transitional period (31 December 2020) the UK will likely adopt data protection legislation which largely tracks the GDPR. There is no precedent for Brexit and it is impossible for companies to foresee every scenario that may arise and the impact it may have on data protection law in the UK. Companies which process the personal data of citizens of the UK or have operations in the UK will need to keep a close watch on the law over the coming months.

Q: What Is the Impact on Data Transfers to the US post-Brexit?
A: When the UK exits the EU, it will, for the purposes of the GDPR, become a “third country” (a country outside of the European Economic Area). The Bill provides a similar data transfer protection regime to that of the GDPR. See our previous alert describing cross-border data transfers under the GDPR.

Based on the current draft of the Bill, following Brexit, the transfer of personal data to a third country (e.g., the United States) from the UK can be carried out using a transfer mechanism which has been approved by the European Commission (i.e., subject to an adequacy decision). Such transfer mechanisms include Standard Contractual Clauses and the Privacy Shield. The Secretary of State will have the power to prevent the transfer of personal data to specific third countries where there is an important public interest to prevent the transfer.

The Bill provides the framework to preserve the use of current compliance mechanisms (for transferring data from the UK to third countries), however, companies should keep the position under review: (1) the Privacy Shield is subject to an annual review and therefore subject to periodic challenge; and (2) the future of the Standard Contractual Clauses remains uncertain given that the validity of the Standard Contractual Clauses has been called into question by Data Protection Commission v. Facebook & Schrems.

Contact Us

If you have questions about this alert or for additional information on the GDPR, contact Jackie Gray at jackie.gray@wbd-uk.com, Malcolm Dowden at malcolm.dowden@wbd-uk.com, or Matthew Harris at matt.harris@wbd-uk.com, or any member of our GDPR Compliance Task Force.
At this point, it is no secret that many US companies will be subject to the GDPR. Under the GDPR, EU regulators will have the authority to punish noncompliance by imposing hefty fines, issuing injunctions, assessing bans on processing, and suspending international data transfers.

The practical impact of such enforcement measures is the ability to devastate a product, service, or business. Many US companies may still be wondering:

How can regulators enforce the GDPR on companies in the United States?

The answer, at this point, depends on principles of jurisdiction and international law. In general, international law distinguishes between the ability to apply law versus enforce law extraterritorially. As such, even if the GDPR is applicable to certain conduct of US companies, enforcement of penalties for violating the law may or may not reach beyond EU member states.

- For US companies with a physical establishment in the EU — the GDPR can be enforced directly against them by EU regulators.
- For US companies subject to the GDPR that lack a physical presence in the EU — a local EU representative must be appointed unless an exemption in Article 27 applies. This EU representative may be held liable for non-compliance of overseas entities, although the contract with the representative may shift liability back to the US company.
- For US companies with no EU physical location or local representative — EU regulators will have to rely on US cooperation or international law to punish GDPR noncompliance.

- While a US-EU civil enforcement mechanism for the GDPR doesn’t yet exist, a cooperation agreement is possible in the future.
- Without such an agreement, through the doctrine of comity, US courts will grant extraterritorial effect to the valid judgments of foreign courts. However, the US court must first be satisfied that the foreign court properly had jurisdiction over the matter and that the judgment was not contrary to public policy.
- Only time will tell whether the GDPR satisfies these requirements.

This analysis relates to enforcement for GDPR noncompliance in general. However, some violations of the GDPR may also be violations of the EU-US Privacy Shield Framework for the transfer of personal information from the EU to the US. In those instances, the FTC has indicated that it will enforce the Privacy Shield against US companies.

Contact Us

If you have questions about the client alert or for additional information on the GDPR, contact Whitney Kamerzel at whitney.kamerzel@wbd-us.com, Allen O’Rourke at allen.orourke@wbd-us.com, or Malcolm Dowden at malcolm.dowden@wbd-uk.com, or any member of our GDPR Compliance Task Force.
We live in a new world of EU privacy rules shaking US businesses. As of 10 months ago, many of you had not heard about the GDPR when we explained how the GDPR applies to US companies (see flowchart). By now your company may be on its way to GDPR compliance (but beware: see #3 below).

For those of us who have been immersed in GDPR compliance projects over the last year, it was refreshing to hear so many of our colleagues, family members and news outlets around the world pay attention to the GDPR on May 25th. But we also heard a lot of misunderstandings about the GDPR. Here are our five takeaways from the past year:

1. Do NOT rely on consent for all data collection. Despite what almost every news story stated the week of May 25, consent is not required in all instances. Consent is one of many ways to lawfully collect personal data. In fact, we only recommend that companies obtain consent when another ground is not available.

2. If you do rely on consent, be careful. Almost every proposed consent mechanism we reviewed did not meet GDPR-level consent. For example, most consent mechanisms did not require an affirmative action or did not disclose that consent can be withdrawn at any time.

3. Do not call yourself 100% or completely GDPR compliant. Many companies claim to be “100% GDPR compliant” in their privacy notices. We caution against such a claim because no one truly knows what a 100% compliant company looks like. There are still too many questions unanswered and the law has not been tested (see #4 below).

4. Data Processing Addendums or “DPAs” (i.e., controller to processor agreements) are taking many forms. Of the DPAs we reviewed from both controllers and processors, about 50% of them stuck very close to the Article 28 required provisions. About 25% took a more aggressive approach, adding an indemnity by the other party for breach of the DPA (some were silent on the limitation of liability or expressly stated that the indemnity is not capped by the limitation of liability provisions in the underlying agreement). Other DPAs were more expansive, shifting the liability allocation of the underlying agreement on claims outside of the GDPR and adding obligation much more robust than those of Article 28.

5. Companies have varied approaches in their privacy policies. We have seen a wide range of privacy policies. Some cover the exact disclosure requirements of Articles 13 and 14, while others (even those of very large data-focused players) are taking a more risk-based approach and do not provide the granularity required under the GDPR. Some companies apply GDPR-based benefits to all consumers, and others limit them to individuals in the EU and EEA.

We promised 5 takeaways. But we will add one as a bread crumb for our future alerts on the GDPR post-May 25th.

6. There are many, many unanswered questions.

What exactly does a controller-to-controller “arrangement” need to cover? Can a data protection officer be “accessible” and located outside of the EU? When analyzing the mandatory DPO requirement, what does “large scale” mean? When and how can you rely on consent for the transfer of data outside of the EU/EEA? How granular do we need to be in setting forth our legal bases for data use? Who is serving as a local representative?

Contact Us

If you have any questions on your organization’s GDPR compliance plan, contact Ted Claypoole at ted.claypoole@wbd-us.com, Orla O’Hannaidh at orla.ohannaidh@wbd-us.com, Taylor Ey at taylor.ey@wbd-us.com or any member of our GDPR Compliance Task Force.

“Womble Bond Dickinson,” the “law firm” or the “firm” refers to the network of member firms of Womble Bond Dickinson (International) Limited, consisting of Womble Bond Dickinson (UK) LLP and Womble Bond Dickinson (US) LLP. Each of Womble Bond Dickinson (UK) LLP and Womble Bond Dickinson (US) LLP is a separate legal entity operating as an independent law firm. Womble Bond Dickinson (International) Limited does not practice law. Please see www.womblebond dickinson.com/us/legal-notice for further details.