On May 25, 2018, the EU General Data Protection Regulation 2016/679 (GDPR) came into force. It applies to any organisation, anywhere in the world, that offers goods or services in the EU or that monitors EU citizens.

The new law takes the form of a “Regulation” and is directly applicable in all EU Member States from its implementation date. The previous EU legislative framework with respect to data protection, the Data Protection Directive 95/46/EC, has been repealed.

The GDPR requires those caught by it to take certain key steps with respect to their data processing activities, even if they are based outside the EU. A failure to comply could attract a fine of up to 20M Euros or 4 percent of annual worldwide revenue (whichever is higher) per breach, and so consequences for non-compliance are severe.

10 Steps to Compliance (and how we can help)

1. Data Mapping
Determine What Data You Hold and Why

   Background
   
   • The principle of accountability is at the very core of the GDPR. Organisations must consider and document how and why they process personal data and must be able to demonstrate compliance (Article 5(2)).
2. Legal Basis for Processing

Analyse the Legal Basis for Processing and Reviewing Consents

- **Background**
  - Organisations must process personal data lawfully, fairly and in a transparent manner under Article 5(1). Processing is only lawful where one of the six bases set out in Articles 6(1) (in relation to personal data) and 9(2) (in relation to special categories of personal data) apply.

  - The GDPR requires organisations to closely review processing and decide what is the most appropriate lawful basis on which they can rely in order to process data, i.e. consent, performance of a contract, legitimate interest etc. The definition of “consent” under the GDPR is more restrictive than the previous legislation so organisations will need to review their processes and existing consents to ensure these can be relied upon after May 2018.

- **How We Can Help**
  - We can analyse existing consents and suggest where updated consent should be sought and how best to achieve that (e.g., in a marketing or employment context).

  - We can work with our clients to undertake a data mapping process to identify what data processing is taking place, providing decision trees/check lists to determine what lawful basis/secondary basis could be used to process data.

3. Risk Assessments

Conduct DPIA Where Required

- **Background**
  - Data Protection Impact Assessments (DPIA) have long been a recommendation of supervisory authorities and will now be a legal requirement under Article 35 of the GDPR. A documented DPIA is required for processing which uses new technologies, or where there is a “high risk to the
4. International Transfers
Consider the Lawfulness of International Transfers

● Where a DPIA reveals high residual risks, the GDPR also requires organisations to seek prior consultation for the processing from a supervisory authority.

**How We Can Help**

● We can assist clients in identifying all data processes and technologies currently in use and identify high risk data sets and technologies which require urgent address.

● We can offer a standard template DPIA, conduct the highest risk assessments on our clients’ behalf, and put a policy in place to highlight when processes should be subject to a DPIA and where consultation with a supervisory authority is required.

4. International Transfers
Consider the Lawfulness of International Transfers

**Background**

● In order to transfer personal data from a country within the European Economic Area to a “third country”, organisations must: (1) comply with the wider requirements of the GDPR; and (2) in the absence of an adequacy decision by the European Commission, implement appropriate safeguards as listed in Article 46(2).

● The various safeguards will not be appropriate in all cases and some are facing challenge in the courts. As a result, there is uncertainty.

**How We Can Help**

● We can work with clients to identify what data is transferred outside of the EEA and the reason.

● We can advise on the best method for lawful transfer of personal data outside of the EEA, and we can apply the most appropriate safeguard where required.

5. Third-Party Providers
Review Data Processing Contracts and Ensure Third-Party Providers Are Responsible

**Background**

● Organisations acting as “Data Controllers” must take responsibility for ensuring that any processing activities are performed in compliance with the GDPR (Article 24) and may only instruct third-party vendors (or, “Data Processors”) which provide sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the GDPR.

● Although Data Controllers and Data Processors will be liable for their own breach of the GDPR, there is a risk that a supervisory authority would pursue a Data Controller for a breach committed
by their third-party vendor acting as a data processor, where the Data Controller failed to undertake the necessary background checks to confirm compliance.

- The relationship between the Data Controller and Data Processor must be governed by a contract (Article 28(3)) which must contain the specific obligations set out in Article 28 (3).

**How We Can Help**

- We can review contracts in place with customers or suppliers to ensure the requirements of the GDPR are met.

### 6. Data Governance

**Review Data Governance and How You Can Respond to New Data Subject Rights**

**Background**

- The first step to GDPR compliance is developing an understanding of what data is held within your organisation and the business need for collecting and processing it. This understanding will then inform data governance policies such as data classification and retention, and the necessary technical and organisational measure required, such as access privileges and multi-factor authentication.

- Under the GDPR, processing must be transparent outward facing privacy policies should be readily available, written in plain English and be in sufficient detail to allow data subject consent to be lawful. Articles 13 and 14 list certain information which must be included, such as the names/categories of those third parties who will receive the data (such as payment providers) and the period for which information will be stored.

**How We Can Help**

- We can review policies to ensure outward facing information is compliant, produce guidance on what data is subject to the new rights, and offer a data subject access request service to assist with access requests.

- We can work with clients to identify what profiling is taking place, the logic of the profiling and the effect of the profiling on data subjects.

- We can undertake privacy impact assessments of the high-risk profiling and review policies for dealing with contested profiling decisions and for dealing with data access requests.

### 7. Security

**Ensure Appropriate Security Policies and Procedures Are in Place**

**Background**

- The GDPR requires organisations to take a risk-based approach to data security. Deciding what
security measures should be introduced depends on the technology available and its costs, the inherent risk of the processing and the nature of the data.

- **How We Can Help**
  - We can work with clients to identify what data is stored and under what security measures and recommend appropriate code of conduct/certification mechanisms.
  
  - Using a thorough data mapping process, we can work with our clients to identify what data they hold and where pseudonymisation is sufficient or inadequate.

  - We can review internal policies for handling personal/special personal data and pseudonymisation of personal/special personal data.

8. Data Breach Response
Review Data Incident Policy and Prepare for Notification

- **Background**
  - The GDPR includes a wide definition of “Personal Data Breach” which includes any “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to [Personal Data].” This definition would include an employee leaving a laptop on the train or, arguably, a bank sending a paper statement to a customer’s previous postal address, which is then “returned to sender.”

  - A Personal Data Breach can have a profound reputational and financial impact on an organisation. This will only be increased by the introduction of breach notification rules under the GDPR.

- **How We Can Help**
  - We can review policies, training documents, draft notification letters and provide breach notification check lists to enable clients to document the decision on whether to notify an authority/data subject following a breach.

9. Privacy by Design and Default
Introduce Culture of Privacy by Design and Default

- **Background**
  - The principle of “data protection by design” (Article 24) requires organisations to think about data protection at the outset and throughout the development of a new process or technology. Organisation must assess the risk associated with all processing and introduce appropriate safeguards.

  - The principle of ‘data protection by default’ (Article 25) requires products and services which contain multiple setting options, to default to the most data restrictive settings. The default position is
that only personal data which is required should be processed. This applies to the amount of personal data collected, the extent of their processing, the period of storage and accessibility.

- **How We Can Help**

  - We can advise clients on how to meet the new requirements for considering data protection in all design stages.

**10. Data Protection Officer**

Improve Awareness and Consider Appointing a Data Protection Officer

- **Background**

  - Compliance with the GDPR requires managerial oversight and co-operation from many different departments including legal, compliance, IT, marketing and procurement.

  - Supervisory Authorities have emphasised that there are no quick fixes and compliance cannot be a box-ticking exercise. Organisations must review their processes and introduce policies and processes which might be missing.

  - Organisations should designate someone to take responsibility for data protection compliance and set out the parameters of this role. Organisations which undertake systematic data processing on a large scale may be required to formally designate a Data Protection Officer (Article 37). Organisations should appoint a data specialist or DPO as early in the compliance process as possible.

- **How We Can Help**

  - Pillsbury can advise on the risks presented by the GDPR and help clients create a business case for a compliance project. We can offer training and updates on the new provisions and additional guidance released by Supervisory Authorities.

  - We can identify whether your organisation will need to formally appoint a DPO and advise on the legal power and responsibilities they will have.