pillsbury

# Overview of Key Points

### What is changing and when?

A new data protection framework (the GDPR) has been adopted, significantly changing current EU laws. It will take the form of a Regulation and so will be directly applicable in all EU Member States from 25 May 2018. Once in effect, the current Data Protection Directive 95/46/EC will be repealed.

### Who is caught by the GDPR?

Organisations operating in the EU will be caught. Importantly, organisations outside the EU who nonetheless target consumers in the EU will now also be caught.

The GDPR applies to "controllers" and "processors". Those currently subject to EU data protection laws will almost certainly be subject to the GDPR. Processors have significantly more legal liability under the GDPR than was the case under the prior Directive and new obligations which do not currently exist.

The GDPR does not apply to certain activities, e.g., processing for national security purposes.

### I am a U.S. company. Do I need to comply?

Being U.S.-based will not save you from complying if you are targeting consumers in the EU, monitoring EU citizens or otherwise offering goods/services to EU consumers, (even if for free).

### What about the UK after Brexit?

It is generally accepted that even after the UK leaves the EU, the GDPR will nevertheless apply (via some form of implementing legislation or a new UK law which effectively mirrors the GDPR). In other words, even if you are purely a UK company, or you are outside the UK and targeting UK consumers only, you should still comply and not ignore these changes. The UK government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

### What are the key changes?

- **Accountability** – data controllers must show compliance e.g. (i) maintain certain documents; (ii) carry out Privacy Impact Assessments; (iii) implement Privacy by Design and Default (in all activities).
- **Data Protection Officers (DPOs)** – in many circumstances, controllers and processors will need to appoint DPOs.
- **Data Processors** – will have direct liability/obligations for the first time.
- **Consent** – new rules are introduced relating to the collection of data, e.g., consent must be "explicit" for certain categories. Existing consents may no longer be valid.
- **Privacy Policies** – fair processing notices now need to be more detailed, e.g., new information needs to be given about new enhanced rights. Policies will need updating.
- **Enhanced Rights for Individuals** – new rights are introduced around (i) subject access; (ii) objecting to processing; (iii) data portability; and (iv) objecting to profiling, amongst others.
- **International Transfers** – BCRs for controllers and processors as a means of legitimizing transfers are expressly recognized.
- **Breach Notification** – new rules requiring breach reporting within 72 hours (subject to conditions) are introduced.

## What key things should I do now to prepare?

- **Review Privacy Notices and Policies** – ensure these are GDPR compliant. Do they provide for the new rights individuals have?
- **Prepare/Update the Data Security Breach Plan** – to ensure new rules can be met if needed.
- **Audit your Consents** – are you lawfully processing data? Will you be permitted to continue processing data under the GDPR?
- **Set Up an Accountability Framework** – e.g., monitor processes, procedures, train staff.
- **Appoint a DPO where required.**
- **Consider if you have New Obligations as a Processor** – is your contractual documentation adequate? Review contracts and consider what changes will be required.
- **Audit your International Transfers** – do you have a lawful basis to transfer data?

## Why is this important? Huge Fines

A failure to comply could attract a fine of up to the greater of 20m Euros or 4% of annual worldwide revenue (whichever higher) and so consequences for non-compliance are severe.

## About Pillsbury

Pillsbury is a major, full service, international law firm. Our Data Privacy & Cybersecurity Team is recognized by Chambers Global as one of the world's foremost practices in the area. We are one of only a small number of firms to have successfully secured BCRs for clients, we have handled multi-billion dollar cyber breaches and we regularly advise on all aspects of data use including issues relating to HR, marketing, websites, customer profiling, social media, transfers and privacy policies.

## To learn more, please contact one of the lawyers below:

**Rafi Azim-Khan** | Partner
+44 20 7847 9519
rafi@pillsburylaw.com

**Steven Farmer** | Counsel
+44 20 7847 9526
steven.farmer@pillsburylaw.com