SHEARMAN & STERLING LLP

# The EU General Data Protection Regulation

Shearman & Sterling LLP is a limited liability partnership organized under the laws of the State of Delaware, with an affiliated limited liability partnership organized for the practice of law in the United Kingdom and Italy and an affiliated partnership organized for the practice of law in Hong Kong.

Attorney Advertising — Prior results do not guarantee a similar outcome.

# EU General Data Protection Regulation: Are You Prepared?

On 27 April 2016, the European Council and Parliament finally adopted a new data protection law: the General Data Protection Regulation (GDPR). The following is a summary of key issues and a checklist of initial tasks to help you prepare for the new regulation.

## When Will the GDPR Take Effect?

It will apply directly in all EU Member States from 25 May 2018. It will repeal and replace Directive 95/46EC and its Member State implementing legislation.

## Expanded Territorial Scope

The GDPR rules (like the Directive) will apply to both controllers and processors in the EU.

The GDPR will also apply to data controllers and processors outside the EU whose processing activities relate to:

- The offering of goods or services to EU residents (even if for free)
- The monitoring of EU residents

## Consequence of Non-Compliance

The maximum fine for a violation of the GDPR are substantial. Regulators can impose fines of up to 4% of total annual worldwide turnover or €20,000,000.

## Questions to Ask

To prepare for the new GDPR, an important first step will be to assess personal data risks and identify compliance gaps:

- What is the definition of Personal Data under GDPR?
- Where is such Personal Data stored across the organisation?
- Where is it transferred from and to (including third parties)?
- How is it secured throughout its lifecycle?
- What policies and procedures need to be revised or created to achieve compliance with the GDPR?

# Key Changes Proposed by the EU GDPR

The GDPR is part of a more general European cybersecurity and digital market framework. It aims to harmonise the differing data protection laws in force across the EU. With its enhanced enforcement regimes and a greater emphasis on rights of individuals and accountability, the GDPR presents ambitious and comprehensive changes to data protection rules.

## 1. Expanded Scope

### Territorial Scope, "Main Establishment", and the New Definition of Personal Data

The scope of the GDPR is expanded to include companies based outside the EU that are processing personal data about persons who are in the EU. Where the controller or processor is not established in the EU but is now within the scope of the GDPR, the controller or processor must designate in writing a representative in a Member State. If controllers or processors have establishments in more than one Member State, they must determine which of the establishments is the "main establishment." The new definition of personal data, which now includes pseudonymised data and online identifiers (such as IP addresses and cookie IDs), may also bring in scope certain processors that may not have needed to comply with data protection rules previously.

## 2. Formalised Recordkeeping Requirements

### Privacy Impact Assessments, Data Processing Register, Data Breach Register, and New Obligations for Processors

The concept of accountability is at the heart of the GDPR rules. Your organisation will need to demonstrate that it has analysed the GDPR requirements and implemented a data protection programme to achieve compliance. The requirement to conduct privacy impact assessments is now formalised under the GDPR, as well as the requirement for controllers to maintain a formal, written record of processing activities (data processing register) and a personal data breach register. Certain of these obligations will require a review and change to existing agreements with processors as not only do processors now have direct obligations under the GDPR and can be liable to claims from data subjects but compliance with GDPR rules will require controllers to understand data risks posed by processors.

## 3. New Rights

### The Right to Data Portability, the Right to Erasure, and the Right to Object

Individuals will have new rights to not only obtain a copy of his data from the data controller (the right of "access" currently in the Directive and the GDPR), but also to require the controller to have it transmitted to another controller or erased. Complying with these new requirements will mean the organisation needs to have a policy for determining when certain data is no longer necessary to be retained, how data subjects may withdraw his consent, and how to deal with data subject requests when he objects to the processing of his data. You will also want to pay attention to any new online businesses or consumer facing businesses, such as mobile apps or fintech initiatives where data is provided directly from the data subject, to formulate policies that identify how certain data can be stopped from being processed or can be transferred to a replacement provider upon request (especially when the recipient of the data could likely be a competitor).

# Take Action to Prepare

Organisations have a two-year window to conduct risk assessments and prepare for the GDPR. Our checklist outlines key initial tasks to begin assessing compliance gaps.

| | |
|---|---|
| Personal Data | Identify where personal data is stored across the organisation<br>❑ Create a personal data inventory<br>❑ Identify businesses that rely on pseudonymisation techniques and engage in monitoring activities based on IP addresses and cookies and analyse the impact of the new definition of personal data |
| Third Party Management | Identify the third parties from whom personal data is collected or to whom personal data is transferred<br>❑ Review the third party risk management programme to assess the number of third parties with whom personal data is shared and the volume of data handled by each third party<br>❑ Review existing contracts and begin the process for replacing them to reflect new requirements |
| Privacy Impact Assessments | Institute a systemic and formalised PIA process<br>❑ Develop a process for determining when a PIA is required and when results of a PIA should be referred to a Supervisory Authority |
| Data Processing | Map and risk rank the current data processing activities<br>❑ Review whether data subject consent forms, privacy notices and policies, and data transfer mechanisms are adequate to meet data processing requirements and develop a plan to replace them<br>❑ Seek to limit liability by baking into contracts minimum required data processing obligations, including provisions restricting appointment of subprocessors without the consent of controllers |
| Breach Notification | Design data breach response plans and notification procedures to meet the 72-hour deadline<br>❑ Prepare template letters and test effectiveness of response plans regularly (i.e. quarterly)<br>❑ Ensure processor agreements include appropriate breach notification provisions<br>❑ Evaluate how data breach incidents are recorded and develop a data breach register to meet the new GDPR requirements |
| Data Subject Rights | Develop policies and procedures to respond to data subject requests<br>❑ Revisit existing procedures and create new procedures to respond to data subject requests, including requests related to: subject access, rectification, erasure, data portability, and objection to certain types of processing<br>❑ Conduct training to implement new procedures |

# Key Contacts

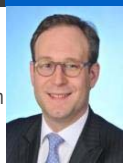

Richard Hsu
Menlo Park
+1 650 838 3774
richard.hsu@shearman.com

Jeewon Kim Serrato
Washington, DC
+1 202 508 8032
*jeewon.serrato@shearman.com*

Barney Reynolds
London
+44 20 7655 5528
barney.reynolds@shearman.com

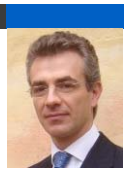
Thomas Donegan
London
+44 20 7655 5566
thomas.donegan@shearman.com

Andreas Löhdefink
Frankfurt
+49 69 9711 1622
andreas.loehdefink@shearman.com



Mathias Stöcker
Frankfurt
+49 69 9711 1215
mathias.stoecker@shearman.com

Tobia Croff
Milan / Rome
+39 02 0064 1509
tobia.croff@shearman.com




Our global reach — from North and South America to Europe, the Middle East and Asia — enables the team to meet the demands of multinational clients and provide sophisticated up-to-the-minute advice in multiple jurisdictions with varying data privacy regulations.

ABU DHABI

BEIJING

BRUSSELS

DUBAI

FRANKFURT

HONG KONG

LONDON

MENLO PARK

MILAN

NEW YORK

PARIS

ROME

SAN FRANCISCO

SÃO PAULO

SAUDI ARABIA*

SHANGHAI

SINGAPORE

TOKYO

TORONTO

WASHINGTON, DC

*Dr. Sultan Almasoud & Partners in association with Shearman & Sterling LLP

shearman.com

Copyright © 2016 Shearman & Sterling LLP