

# GDPR: An International Context

The global impact of the GDPR in  
relation to Brexit and the EU-US  
Privacy Shield

**Imprima White Paper**

Published 19 April 2018

The contents of this document are limited to general information and not detailed analyses of law or legal advice and are not intended to address specific legal queries arising in any particular set of circumstances.

# GDPR

## The clock is ticking

### Is your business ready?

With just over five weeks until the GDPR comes into effect and less than one year before the UK is scheduled to depart the EU, it is understandable that many organisations feel a high level of anxiety around these major and fundamental changes. With so many changes happening in parallel there has also been a lot of information presented around these topics.

However, there still appears to be a level of unpreparedness and confusion within companies on the impact these changes will ultimately have on the data protection and privacy landscape in Europe and beyond. To this end, Imprima will run a series of articles on the GDPR to help our clients deal with the new regulation in the context of sharing information via data storage and collaboration platforms.


In this first piece, we look at the GDPR not only in the European context, but also in-terms of the wider international data protection landscape. As such, we will focus on how it impacts on both the UK (pre and post

Brexit) and on data transfers between Europe and the US (EU-US Privacy Shield).

### What is the GDPR?

The General Data Protection Regulation (GDPR) represents the most important data protection regulation change in 20 years. The GDPR, approved and adopted by the EU Parliament in April 2016, replaces the Data Protection Directive 95/46/EC. The GDPR was designed to both update and harmonise data privacy and the various laws surrounding it across Europe. Its primary intent is to provide further data privacy protection and empowerment of all EU citizens' and as a result reshape the way organisations across the region approach it.

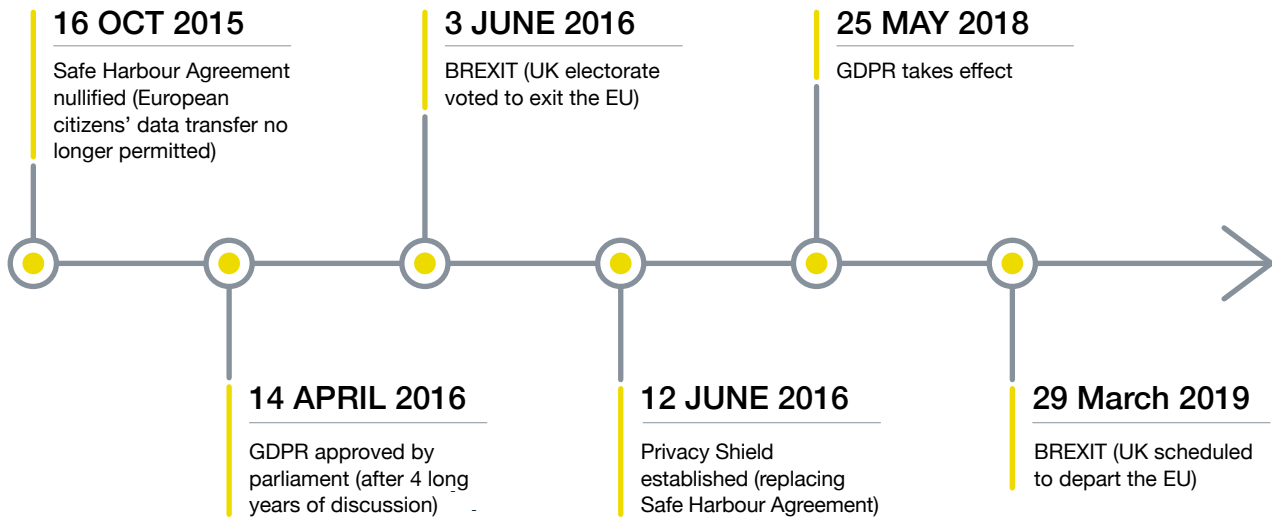
Furthermore, as the GDPR reduces 28 sets of different data protection laws to a single regulation with the aim of reducing compliance costs, complexity, risk and uncertainty over reporting for organisations; it should be seen as a benefit not only to EU citizens, but also all companies that need to embrace the change.



**!** Once the GDPR comes into effect on 25 May 2018, all companies processing and holding the personal data of subjects residing in the EU must comply with it, regardless of location.

# GDPR, Brexit and Privacy Shield

## Timeline of Key Data Protection Events



In order to fully appreciate the global consequences of the GDPR, it is essential to view it not in isolation, but against the backdrop of two other internationally significant items:

1. **The UK's exit from the EU**
2. **The EU-US Privacy Shield**

### What happens after GDPR comes into effect but before the UK departs the EU?

Once GDPR comes into force but before the UK leaves the EU (March 2019), businesses processing data in the EU can freely share data with the UK simply by virtue of the fact that the UK is still a member of the EU.

### What happens after the UK leaves the EU on 29th of March 2019?

After Brexit, the UK will become a 'third country'. This means that data controllers in the EU countries will have to identify a specific legal basis within the GDPR upon which it can legally transfer personal data to the UK.

The UK government initially declared it was aiming to get an adequacy ruling from the European Commission on the UK's data protection capabilities, by aligning UK

data protection law with the EU General Data Protection Regulation (GDPR) as closely as possible.

**!** **Adequacy decision – the EC has the power to determine whether a country offers an 'adequate' level of data protection**

Should the EC grant an adequacy decision to the UK, this would ensure the unhindered flow of data between the EU and the UK post-Brexit.

However, in a recent speech the UK Prime Minister, Theresa May, went a step further when declaring:

**“We will be seeking more than just an adequacy arrangement and want to see an appropriate ongoing role for the UK's Information Commissioner's Office (ICO). This will ensure UK businesses are effectively represented under the EU's new 'one stop shop' mechanism for resolving data protection disputes”.**

This crystal-clear commitment on data protection was warmly welcomed by the UK business community. The move to go further than the adequacy arrangement is seen by many as the right approach to support the UK's place as a leading tech economy.

## GDPR, Brexit and Privacy Shield (cont...)

---

### The GDPR and EU-US Privacy Shield

Under both the GDPR and its predecessor, the EU doesn't allow the transfer of data on its citizens outside of the country unless the country is deemed to have adequate data privacy laws. Unfortunately, the EU has deemed that the US does not have adequate data privacy laws. Organisations try to navigate this by adhering to the EU-US Privacy Shield.

### What is the EU-US Privacy Shield?

The EU-US Privacy Shield is a program where participating U.S. companies are considered to have adequate data protection and can therefore facilitate the transfer of EU data. The EU-US Privacy Shield's predecessor, the Safe Harbour Framework, was overhauled because the EU did not consider this agreement strict enough on data protection for their citizens. The GDPR protects the data of all EU citizens, regardless of whether they currently live in the EU.

### How does it link with the GDPR?

According to the EU-US Privacy Shield, to ensure that your company is meeting all requirements, you must include robust mechanisms for assuring compliance with the principles of the GDPR. Being certified under the EU-US Privacy Shield can give your company a jump-start on fulfilling the GDPR's standards and provides legal clarity and direction on the EU's data protection laws, but will not guarantee total GDPR compliance.

It is also important to note that the EU-US Privacy Shield will be revisited every year and could change, so it is important to have an assigned employee/person to stay current with all the updates. Many observers feel it is only a matter of time before the Privacy Shield falls to a similar fate as the "safe harbour" agreement by being invalidated by the European Court of Justice.



# GDPR: Key provisions

---

Now we understand the context, what **key new provisions** are included within the GDPR?



## **The definition of personal data is much wider**

It now includes online identifiers, such as the id of your mobile phone while you browse the internet, along with HR, customer and client records.



## **Expanded Territorial Scope**

The GDPR applies to all data controllers/data processors processing the personal data of data subjects residing in the EU, regardless of the data controller's/data processor's location. This means that many non-EU businesses that were not required to comply with the Data Protection Directive will be required to comply with the GDPR.



## **Increased Enforcement Powers**

Under the GDPR, data breaches could result in fines up to 4% of annual global turnover (or 20 Million Euros, whichever is greater). Data processing procedures should be monitored and reviewed with the aim of minimising data processing and retention of data.



## **Evidence of Consent**

The GDPR requires a very high standard of consent for the processing of personal data. The burden of demonstrating that the legal standard of "consent" has been achieved will lie with organisations, so businesses should review whether their documents and forms of consent are adequate, and check that consents are freely given, informed and specific. Businesses also must ensure that a data subject can withdraw his/her consent to the processing of their personal data at any time.



## **Right to be forgotten**

You must be able to delete the name and personal information of any EU citizen on request. This means from any place, including backups, where that information might happen to reside. This will require you to become aware of where your data is and what's in it something many companies probably can't do now. If there is no legal reason to keep the data, it needs to be erased. If you have passed the details to a third party, you need to contact the other party and make sure they also do it.

## GDPR: Key provisions (cont...)

---



### **Privacy by Design**

This is a central principle of the GDPR. Data protection considerations need to be considered from the outset of designing a new process, products or services, rather than treating it as an afterthought.



### **Reporting Security Breaches**

The GDPR requires that businesses will have to report breaches that are likely to harm individuals to national authorities e.g. the ICO in the UK within 72 hours. Organisations should develop a data breach response plan enabling them to respond quickly in the event of a data breach.



### **Regulation on Data Processors**

The GDPR directly regulates “data processors” for the first time. The current Data Protection Directive regulates data controllers rather than “data processors”, who are organisations/individuals engaged by a data controller to process personal data on the data controller’s behalf.

**Imprima’s clients can rest assured we are a 100% European owned organisation, with servers based in the EU. We are not reliant on any indirect adequacy provisions and will directly adhere to the GDPR, providing our clients with the ongoing protection that makes us the most trusted and secure data room provider in the industry.**

Coming soon >>

In our next piece, Imprima will focus on the benefits of the GDPR, what companies can do to ensure compliance and, clearly outline what steps Imprima have taken to help them comply with the new regulation.

## Contact us

---

To find out more about how GDPR will impact your business, please visit our website or contact your local Imprima office:

[www.imprima.com](http://www.imprima.com)



### Imprima global offices

---

#### London

Imprima iRooms Limited  
30 Crown Place  
London EC2A 4EB  
Tel: +44 20 7965 4700  
E: [londonsales@imprima.com](mailto:londonsales@imprima.com)

#### Frankfurt

Imprima (Deutschland) GmbH  
Barckhausstraße 10  
60325 Frankfurt am Main  
Tel: +49 69 915 0980  
E: [frankfurt@imprima.com](mailto:frankfurt@imprima.com)

#### Paris

Imprima (France) SARL  
32 Avenue de l'Opéra  
75002 Paris  
Tel: +33 1 76 75 32 91  
E: [paris@imprima.com](mailto:paris@imprima.com)

#### Amsterdam

Imprima (Nederland) B.V.  
De Boelelaan 7  
1083 hj Amsterdam  
Tel: +31 207 155 600  
E: [amsterdam@imprima.com](mailto:amsterdam@imprima.com)

#### New York

Imprima (USA) Inc.  
135 East 57th Street  
New York  
NY 10022  
Tel: +1 646 844 2993  
E: [newyork@imprima.com](mailto:newyork@imprima.com)

#### Sydney

Imprima Australia  
Level 12, Plaza Building  
95 Pitt Street  
Sydney, NSW 2000  
Tel: +61 283 110 266  
E: [sydney.sales@imprima.com](mailto:sydney.sales@imprima.com)