GDPR: EU General Data Protection Regulation

EU data protection legislation is some of the best in the world, but the past year has seen a number of upheavals in how things are done.

Changes to the law are being made in substantive ways, and also in procedural ways for how the law will be implemented in the EU region and affect the rest of the world.

Particularly in relation to the EU and US data protection relationship, changes from the EU Data Protection Directive to the new EU General Data Protection Regulation (GDPR) will affect not just EU citizens, but other countries around the world, with the US in particular bearing a large number of these changes detrimentally.

In tandem, the striking down of the EU-US Safe Harbor provision made large changes to how the EU deals with the transfer of data to the US, and the new EU-US Privacy Shield is still to be tested."

Let's take a look at what the new EU General Data Protection Regulation (GDPR) is, what it will change, and how businesses can comply going forward.

What is EU Data Protection Regulation

The **EU Data Protection Regulation** (shorten as GDPR) is a new piece of legislation that was unveiled in 2012.

It's proposed to come into force in late 2015 or early 2016 and it's intended to replace the EU Data Protection Directive which has been in place since 1995.

Like the EU Data Protection Directive, the GDPR will apply to all EU member states, but it will also apply to many more countries around the world.

Let's take a look at some of those changes now, and what it may mean for your business.

One of the primary changes that the new GDPR regulation will make is that data collectors (website/mobile apps that are collecting personal data from users) will be required to reveal more information to users than previously.

The GDPR regulation sets out that:

- The personal data must be processed in a fair way. It should be collected for specific purposes only.
- The personal data must be sufficient for those stated purposes and no more
- All collected personal data must be accurate and kept up to date

- The data subject (the user) must be identified only for as long as necessary unless its collected data is kept for historical, statistical or scientific research purposes
- The data controller (the business that collects the data) must ensure its compliance with the GDPR regulation
- The identity and the contact details of the data controller and of the Data Protection Officer (a new requirement set by the GDPR) must be disclosed to users
- Users must be told why their personal data is being collected
- Users must be told how long their data will be kept for
- Users must be notified of their right to request access to the data
- Users have a right to request update or removal of their personal data
- Users' complaints can be lodged with the supervisory authority
- The contact details of the supervisory authority must be provided
- Users must be told who will receive their collected personal data
- The data controller must specify if they intend to transfer the user's data out of the EU
- If user's data is going to be transferred out of the EU, the data controller must specify where the data is going and the level of data protection that country has
- All other information necessary to guarantee fair processing of user's data must be provided

These changes in the regulation are not significantly different to what's now required by the current Directive but focus more on small details like disclosing to users the period for which the personal data will be stored and the existence of the right to request access to and update or removal of the collected data.

GDPR also increases the responsibility of the controller of the data, which no longer just includes the original collector. This means that third parties such as cloud providers are now also responsible in the case of a breach.

Now let's take a look at how this regulation will be implemented and what's different between the Directive and the GDPR regulation.

Data Protection Officers

The new regulation puts a new requirement in place for some businesses to have a Data Protection Officer (DPO).

A DPO is a staff member whose role is to ensure that the regulation is complied with in their business or organization.

The DPO's role is an independent one and they must keep a register that can be accessed by any interested person.

The EU Data Protection Officer's Network has released a paper setting out professional standards for Data Protection Officers. This paper notes that:

the DPO shall be selected on the basis of his or her personal and professional qualities, in particular, his or her expert knowledge of data protection.

Once a DPO has been selected for a business, their appointment must be registered with the European Data Protection Supervisor. The DPO can be appointed between 2 and 5 years and is eligible for reappointment up to a maximum of 10 years.

Some of the ways in which the DPO can ensure the regulation is complied with are:

- Hold regular training sessions with the data controllers and their staff
- Develop data protection guidelines and policies
- Attend meetings of senior and middle management to provide updates on compliance within the organization
- Publish short articles in company newsletters or publications
- Prepare information booklets or guides for staff

GDPR vs. Data Protection Directive

Previously, the EU Data Protection Directive was required to be implemented in local laws by individual EU member countries and each country had up to 3 years of the Directive being issued to do this. For example, the UK has been using the UK Data Protection Act 1998 to implement the Directive.

The new GDPR regulation will change that. Instead, the regulation will automatically apply to all EU countries. EU countries won't have to implement their own local laws to comply with this regulation.

However, without the 3 year lead-in period, some businesses may be caught out if they don't get up to speed before the law comes into force.

Businesses who want to be in compliance early, a draft of the Regulation has already been issued. This means that EU member states and businesses can use this draft to get started on complying with GDPR.

Another major step away from the Data Protection Directive is that GDPR will cast a wider net in terms of catching online service providers around the world. Rather than simply applying to businesses operating within the EU, the law also applies to anyone dealing with personal data of EU citizens.

If you think your business might be captured by this regulation, such as having users from the EU, you need to set up compliance measures sooner rather than later.

We'll cover compliance measures at the end of this guide. The GDPR regulation includes stronger rules on the transfer of personal data outside of the EU which you should know about.

For the personal data of citizen from the EU to be transferred out of the EU, the third country (the country the personal data is transferred to) must be one that "*ensures an adequate level of protection*" for that personal data.

When considering whether a third country ensures "an adequate level of protection", these factors are looked at:

- Relevant privacy legislation and the legal rights of data subjects (of users) in that third country
- One or more independent supervisory authorities responsible for data protection in that third country
- Any international commitments that the third country has entered into

The European Commission has deemed several countries to have met these criteria. Currently, these are:

- Andorra
- Argentina
- Canada
- Faroe Islands
- Guernsey
- Isle of Man
- Israel
- Jersey
- New Zealand
- Switzerland
- Uruguay

If your business isn't one of these countries listed above, a legal international agreement can be put in place between the EU and the country to agree that data can be transferred there.

The most well-known of this kind of agreement is the US-EU Safe Harbor agreement. However, major changes have just occurred in the European Court of Justice that mean that the Safe Harbor agreement may no longer be enforceable.

Safe Harbor

GDPR initially proposed to remove the Safe Harbor provisions which governed the transfer of data between the US and EU. However, this issue never came to light in the context of the regulation, as the Safe Harbor provisions were recently been struck down by the European Court of Justice before the regulation could come into force.

Previously, the European Commission considered the US to provide "adequate protection" only under the Safe Harbor provisions. This meant that without the provisions of the Safe Harbor agreement, the US could no longer be considered to provide "adequate protection" for the purpose of storing the personal data of EU citizens.

The new General Data Protection Regulation was assumed to change this, but the European Court of justice stepped in and made changes before the regulation could do so.

The European Court of Justice's decision in October 2015 in "Maximillian Schrems v Data Protection Commissioner" examined the Data Protection Directive's provisions that the transfer of personal data to a third country may take place **only if that third country ensures an adequate level of protection of the data**.

The Data Protection Directive also set out that the Commission could find that a third country ensured the "*adequate level of protection*" by reason of its domestic law or its international commitments. The Commission had taken advantage of this provision, by deeming that the Safe Harbor agreement ensured an "*adequate level of protection*" for the data of EU citizens.

However, the Court of Justice noted that despite the Commission's power to make a decision that the transfer of a person's data to a third country complies with the requirements laid down by the Data Protection Directive, there was nothing in that directive that prevented oversight by the national supervisory authorities of transfers of personal data.

As a result, the Court of Justice felt that despite the Commission's decision that the US-EU Safe Harbor provisions were adequate, the Court of Justice could still decide whether or not that Commission decision was valid.

The Court noted that:

legislation [i.e. US legislation that allows NSA spying] permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.

As a result, the Court found that Safe Harbor decision was not compatible "*with the protection of the privacy and of the fundamental rights and freedoms of individuals.*"

To that end, the Court declared the Commission's Safe Harbor decision **invalid**.

The EU Data Protection Authorities set a deadline of January 31 for the European Commission to agree on replacement Safe Harbor provisions, and the new EU-US Privacy Shield was approved by the EU Commission on 2 February 2016.

However, the Privacy Shield is still being slammed with criticism from privacy advocates, lawyers, and companies, who have all noted that it is not clear enough. With regard to consumers, the Privacy Shield has been critiqued for not providing them with enough protection.

This means that it is likely that changes to the Privacy Shield may still be yet to come.