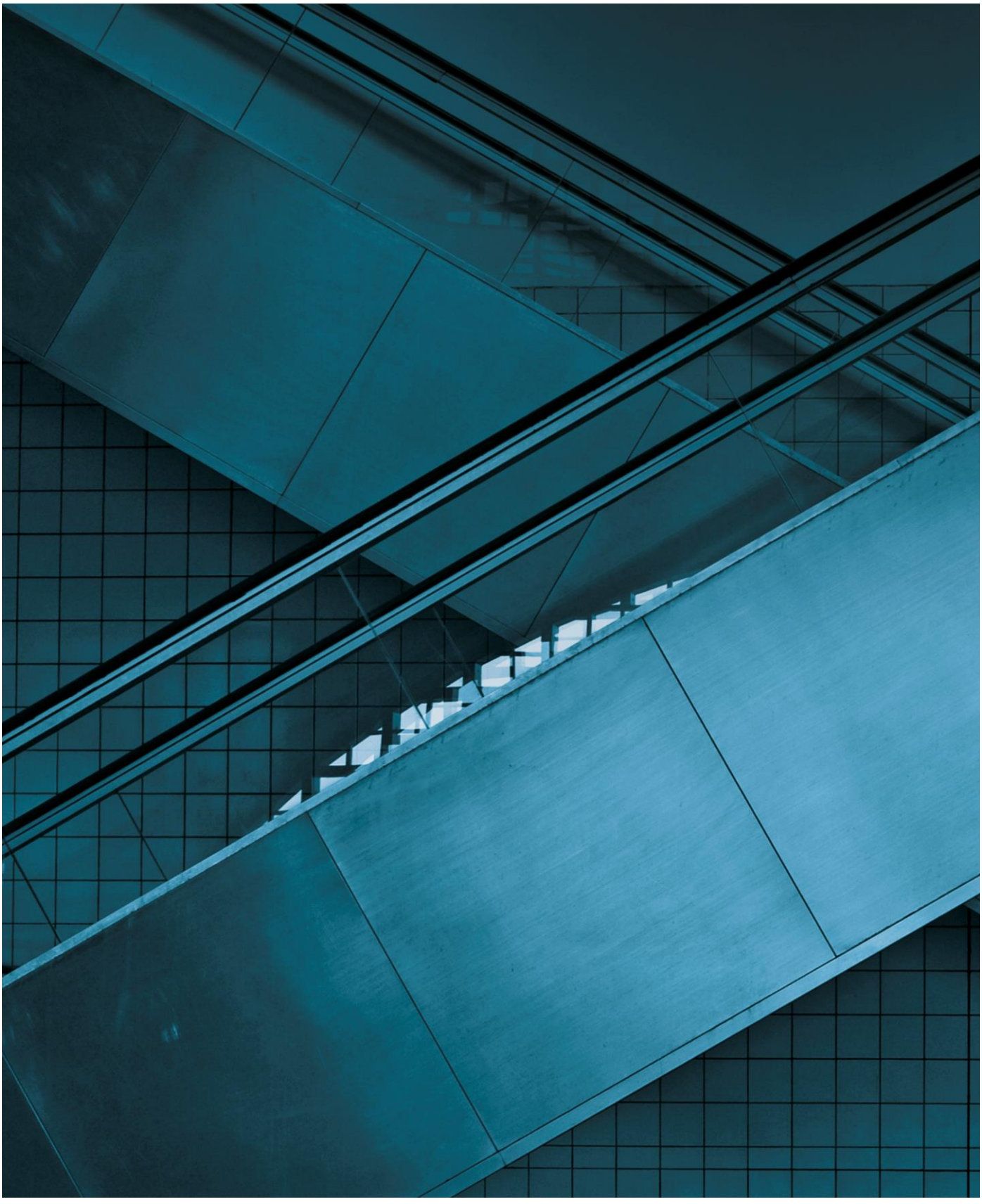
Preparing your business for data protection regulation reform

September 2017

CharlesRussell Speechlys



Introduction

Finally, after three years of discussions and negotiations, the EU General Data Protection Regulation (GDPR) has been agreed.

The GDPR will replace the current Data Protection Directive 95/46/EC (Directive) and will take direct effect in all Member States without the need for local implementing legislation. The GDPR will apply from 25 May 2018.

This document sets out the main changes under the GDPR that will have most impact on businesses as well as "top tips" on what to do and think about in order to comply.

On 23 June 2016, the UK population voted to leave the EU in a national referendum. The formal Article 50 notice to leave the UK was given by the UK Government to the European Council on 29 March 2017, meaning that the official exit will not take place until at *least* March 2019. Therefore, the GDPR will already have taken effect by the time the UK leaves the EU. However, regardless of the political future of the UK, one thing is certain: if the UK wishes to continue benefiting from the EU Digital Single Market, it will have to enact the GDPR, in some form or other.

On 7 August 2017 the UK Government published a statement of intent on its planned Data Protection Bill, due to be published in Autumn 2017, which confirms the intention for the future UK legislation to reflect the provisions of the GDPR. We are therefore recommending all UK companies to continue with their GDPR compliance programmes.

Please contact us if you have any questions in relation to the GDPR and how it applies to your business.

Jonathan McDonald
Senior Associate
T: +44 (0)20 7427 6725
jonathan.mcdonald@crsblaw.com

The main changes under the GDPR

Extra-territorial applicability

Current law

Currently, a business is required to comply with the requirements of the Directive where data are processed "*in the context*" of an "*establishment*" or where it uses "*equipment*" in a Member State for the purpose of processing the data (otherwise than for the purposes of transit). The ambiguity of the drafting of this definition means that it is not always clear when, or, if, the Directive is applicable; for example, does a one-person office constitute an establishment? Does a UK server used by US business to store the data of its US employees constitute equipment and trigger the Directive? Does a user's device constitute equipment through which their personal data are being processed in the EU by a business located in the US?

Applicability of the Directive has also arisen in a number of high profile court cases, most notably in *Google Spain v AEPD and Mario Costeja González* (2014). In this case, Google argued that search engine activities did not take place within the EU and that the Spanish establishment simply promoted and sold advertising space, thereby meaning that the Directive was not applicable. The court took the opposite view and concluded that the activities of the search engine and the establishment in Spain were "*inextricably linked*"; without the advertising activities, the search engine would not be economically viable. The processing was considered to take place within the "*context of*" an establishment and thus triggered the requirements of the Directive. Perhaps if the GDPR had been in force at the time of dispute, the question of applicability would not have been in dispute...

The GDPR

The GDPR makes its applicability very clear. The GDPR will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to:

- offering of goods or services to EU citizens, irrespective of whether a payment of data subjects is required, or
- monitoring of behaviour that takes place within the EU, i.e. tracking EU citizens on the internet to create profiles or to analyse / predict their behaviour / preferences.

In short, this means that the GDPR will have extra-territorial applicability; if a non-EU business wants to process the data of EU citizens, it will have to play by EU rules. It will also have to appoint a representative in the EU.

Top tip
If your organisation does not wish to offer goods / services to certain EU data subjects, ensure that this is reflected on your website; otherwise your organisation may find that it is inadvertently caught by the requirements of the GDPR in relation to that specific processing. For example, a US company that does not wish to offer its goods to EU customers, should not accept local currencies or allow for orders to be delivered to the EU.

Breach Notification

Current law

Whilst some local EU data protection authorities (DPAs) encourage voluntary notification of serious data breaches, the majority of EU countries have not introduced mandatory data breach notification requirements as part of their implementation of the Directive.

The GDPR

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "*result in a risk for the rights and freedoms of individuals*". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "*without undue delay*" after first becoming aware of a data breach.

Whilst it is expected that further guidance will be produced by the European Data Protection Board (EDPB) on the circumstances in which controllers will need to make a notification, the GDPR suggests that this may include "*loss of control over personal data, limitation of rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to reputation, loss of confidentiality*".

There will also be an obligation to notify the affected individuals of data breaches "*as soon as reasonably feasible*" and "*in close co-operation*" with the relevant DPA.

Top tip
Review your organisation's incident response policy against the requirements of the GDPR particularly since the GDPR requires controllers to document data breaches for regulatory audit purposes. Co-operation with the DPA is also a mitigating factor in relation to the imposition of fines and your organisation should be prepared to inform and work with the DPA as much as possible in the event of a breach.

Data Protection Officer (DPO)

Current law

Currently, controllers are required to register their data processing activities with local DPAs. For multinationals this can be a bureaucratic nightmare, with

Member States having different registration requirements and differing levels of complexities as to what must be registered, how and when!

However, in some Member States, a DPO may be appointed in lieu of submitting registrations (Sweden and Poland, for example), whilst in Germany the appointment of a DPO is mandatory for most organisations.

The GDPR

Multinationals will be delighted to hear that, under the new regime, it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

Importantly, the DPO:

- must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- may be a staff member or an external service provider
- contact details must be provided to the relevant DPA
- must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- must report directly to the highest level of management
- must not carry out any other tasks that could results in a conflict of interest.

Top tip

If you decide to opt for an internal DPO, make sure you invest in the training and development of the responsible person. Data protection professionals are in high demand and short supply!

Data transfers

Current law

Personal data may not be transferred outside of the European Economic Area (EEA) unless appropriate safeguards are in place; for example, where binding corporate rules (BCRs) have been approved, MCCs (see above) executed or where the European Commission has deemed a third country as offering adequate protection for personal data. Until recently, Safe Harbor was also a very useful mechanism to enable transfers of data to US companies which had self-certified compliance with the Safe Harbor data privacy principles.

However, these data transfer mechanisms are far from ideal; Safe Harbor was declared to be invalid last year by the Court of Justice, MCCs are a bureaucratic process and as for BCRs, not all Member States, currently, accept them and they normally take between 12 and 18 months to be approved by relevant DPAs. In addition, not all DPAs accept the adequacy findings of the European Commission.

The GDPR

Whilst under the GDPR, the fundamental principle regarding transfers of personal data outside of the EEA remains unchanged, the GDPR does provide for an increased number of safeguarding data transfer mechanisms, including approved codes of conduct and certifications, as well as a seemingly simplified procedure for BCRs which will be accepted in all Member States.

The exact details and procedure of how to adhere to a code of conduct or obtain a certification are yet to be determined, but the following will generally apply:

Codes of Conduct

- Associations or bodies representing certain sectors of controllers or processors may prepare data protection codes of conduct and submit the same to the relevant DPA for approval.
- Once approved, the DPA will register and publish the code. Adherence to an approved code will not only act as a data transfer mechanism but may also act as a mitigating factor in the event of enforcement action and will also demonstrate compliance with the GDPR generally.

Certifications

- Certifications will be issued by accredited certification bodies and will take into account "*the specific needs of micro, small and medium-sized enterprises*". The idea seems to be that a common certification, a "*European Data Protection Seal*" will be developed.
- Organisations wishing to become certified will need to provide the certification provider or, where applicable, the DPA with all information and access to its processing activities to enable the certification procedure to be conducted
- Certifications will be issued to a maximum three-year period and then will need to be renewed.
- As with codes of conducts, certifications will not only act as a data transfer mechanism but may also act as a mitigating factor in the event of enforcement action and will also demonstrate compliance with the GDPR generally.

Whilst procedures relating to codes of conduct and certifications will take time to develop, the procedure for approving BCRs is already established and has the key advantage that under the GDPR it will be accepted in all Member States. This will be very appealing for multinationals wishing to future proof their internal data transfers, meaning that the queue for BCR approvals may get longer and longer over the coming years.

Top tip

If you want to go down the BCR route, start working on the application now in order to beat the queue.

If the certification / code of conduct route is more appealing, keep a close eye on the UK Information Commissioner Office (ICO) Privacy Seals scheme which is leading the way in this space and is expected to be up and running in 2016.

Notifications / Record keeping

Current law

As mentioned above, most organisations have to submit notifications to their local DPAs of their data processing activities. This can be a huge burden for multinationals, especially anyone registering their MCCs in Spain right now following the Safe Harbor decision!

The GDPR

Under the GDPR, notifications will be abolished but there will be internal record keeping requirements. Controllers and processors will be required to maintain a record of their data processing activities, which must be available upon request to the relevant DPA. This requirement will not, however, apply to SMEs with fewer than 250 employees, unless the processing they carry out is high risk or they process sensitive or criminal data.

Top tip

Do not let your existing registrations go to waste! Use these documents to help compile your internal data processing records.

Agreements with data processors

Current law

Currently, each Member States' data protection laws contain different requirements as to what "*mandatory*" data protection clauses must be contained in agreements with data processors (i.e. outsourcers). This can be a challenge for multinationals when negotiating global master services agreements with outsourcers.

The GDPR

Fortunately, the GDPR streamlines these requirements, meaning that the "*mandatory clauses*" will be the same in all Member States. However, they are much more extensive than what the majority of current local laws require and, in fact, seem rather akin to the obligations in the MCCs. For example, data processors will be required to agree that they will:

- assist data controllers with the controller's breach notification obligations
- delete or return all personal data to the controller at the end of the provision of services
- allow for and contribute to audits by the controller
- not engage sub-processors without the consent of the controller and, where consent is obtained, processors will ensure that a sub-processing agreement is in place imposing back-to-back data protection obligations on the sub-processor and the processor will have full liability to the controller for the performance of these obligations by the sub-processor.

Top tip
Create a standard data processing template, which reflects these obligations and make sure that data processing contracts you enter in to going forwards contain these standard provisions.

The "one-stop-shop"

Current law
Different DPAs have different attitudes and priorities; this can be a particular challenge for multinationals where processing operations span more than one Member State and it is necessary to consult with, notify, and be answerable to, multiple DPAs.

The GDPR
Under the GDPR, where processing takes place in more than one Member State, the DPA of the controller's or processor's "*main establishment*" will act as the "*lead supervisory authority*" in relation to that processing. This change will be welcomed by multinationals as in the majority of circumstances it will only be necessary to deal with one DPA rather than, potentially, up to 28.

The "*main establishment*" is defined as the "*central place of administration*" unless the decisions about the data processing activities are taken in another establishment, in which case that establishment will be the "*main establishment*".

Top tip
Start considering which DPA will be your lead authority and monitor guidance notes published by that DPA in relation to the implementation of the GDPR.

Sanctions for non-compliance

Current law
The level of fines that DPAs are able to impose differs between Member States. In the UK, the ICO may impose fines of up to £500,000 for serious breaches and the Spanish Agency up to EUR 600,000. In other member states, the level of fines is much lower with the maximum amount in Estonia being approximately EUR 67,000 and EUR 30,000 in Cyprus.

The GDPR
Fines under the GDPR will be streamlined with all Member States having the power to impose massive fines on non-compliant controllers and processors. The level of fines will be tiered

- for breaches regarding general obligations, such as record keeping, data processor relationships, data protection impact assessments or DPOs, the relevant DPA may impose fines of up to the greater of EUR 10 million or 2% of the total worldwide annual turnover / revenue of the preceding financial year

- for breaches regarding the fundamental data protection principles (including conditions for consent), data subjects' rights and international data transfers, the relevant DPA may impose fines of up to the greater of EUR 20 million or 4% of the total worldwide annual turnover / revenue of the preceding financial year.

Helpfully, the GDPR sets out factors that DPAs or the relevant court will consider before determining whether to impose a fine and the amount, including:

- the number of data subjects affected and the level of damage suffered by them
- any actions taken by the controller or processor to mitigate the damage to data subjects and to remedy the breach
- previous breaches
- the degree of co-operation with the relevant DPA
- whether the relevant DPA found out about the breach from another DPA or whether they found out in another manner
- adherence to approved codes of conduct or certifications.

Top tip

Make sure that you document your compliance with the GDPR, for example, by putting in place policies, procedures and carrying out data protection impact assessments. These documents will be important to produce to the relevant DPA in the event of an investigation and may result in a lesser fine.

.

Contact
If you have any queries please contact

Jonathan McDonald
Senior Associate
T: +44 (0)20 7427 6725
jonathan.mcdonald@crsblaw.com

CharlesRussell Speechlys

charlesrussellspeechlys.com