EU Data Protection Reform moving forward

Losdyck, Bénédicte; Vandendriessche, Johan

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

EU Data Protection Reform moving forward: which changes will the General Data Protection Regulation (GDPR) bring?

par Johan Vandendriessche
7 janvier 2016
Privacy

The data protection reform package has finally been adopted. What are the main changes and how do they affect the business in practice ?

In January 2012, the European Commission proposed a full reform of the current EU data protection rules. On 15 December 2015, after a lengthy legislative process and many months of negotiations, the European Commission, the European Parliament and the European Council finally found an agreement on the data protection reform package during the so-called trilogue meetings.

The data protection reform package consists of two legal instruments, a general regulation applicable to the processing of personal data (the so-called GDPR) and a directive applicable to the processing of personal data in the police and criminal justice sector (the Data Protection Directive). This article will focus solely on the GDPR.

The final texts are expected during the first semester of this year. As far as the GDPR is concerned, a transition period of two years applies, which means that the new data protection rules will in all likelihood need to be complied with by the second semester of 2018.

The key purposes of the data protection reform are (i) the creation of a single set of rules, (ii) the affirmation and strengthening of the data subjects' rights, (iii) increased responsibility and accountability of data controllers and data processors, (iv) the removal of unnecessary administrative burdens and (v) a strengthened enforcement framework.

The creation of a single set of rules

The choice for a regulation as a legal instrument implies that data protection will be governed by a single legal instrument with direct effect in each EU member state's law. The existence of a single legal framework for the European Union should make it easier for multinational

companies to comply with data protection rules, as it enables a more centralized approach to the management of data processing activities.

Together with this new approach, the GDPR also substantially changes the rules in relation to the territorial scope of the data protection rules. If personal data are being processed in the context of activities of an establishment of a data controller or a data processor in the European Union, the GDPR applies. Moreover, the GDPR also applies to the processing of personal data by a data controller or a data processor not located in the European Union, if the processing relates to data subjects who are in the European Union and where the processing activities are related to the offering of goods or services or the monitoring of their behaviour within the European Union.

The changes in the territorial scope should also be read in conjunction with the "one stop shop" mechanism, whereby data controllers and data processors with more than one establishment in the European Union are normally only subject to the supervision of a single supervisory authority. The possibility for a company group to appoint a single data protection officer will in all likelihood lead to a further centralization of the management of data processing activities.

The confirmation and strengthening of the data subjects' rights

The European Commission has affirmed on multiple occasions its desire to confirm and strengthen the data subject's rights. Without going too much into the details of the changes, it can indeed be said that the data subject's rights are reinforced.

A clear example is the fine-tuning of the requirements in relation to the data subject's consent. The definition of consent is clarified with the requirement of affirmative action. This requirement, together with the requirement of a distinguishable consent in case of a written declaration, clearly attacks the practice of implied consent (e.g. consent resulting from silence or inactivity). Last but not least, it should be noted that consent may be withdrawn by the data subject at all times. To that effect, the data subject must be informed of the right to withdraw his consent. This right must be offered in a manner which makes withdrawing consent for the data subject as easy as giving consent.

In addition to the reinforcement of the data subject's rights, there are also some novelties in the GDPR. The GDPR introduces two new privacy concepts, *privacy by design* and *privacy by default*, it confirms the right to be forgotten in a more general manner and it includes a restricted data portability principle.

Increased responsibility and accountability of data controllers and data processors

The aim of increased responsibility and accountability is achieved through various mechanisms, notably obligations in relation to the management of data processing activities, the limited requirement of the designation of a data protection officer and the implementation of a personal data breach notification obligation.

In terms of data protection management, the data protection impact assessment obligation should be highlighted. For any data processing activity which is likely to result in a high risk for the rights and freedoms of individuals, the data controller must carry out a prior impact

assessment (together with the data protection officer, where one is designated and, if appropriate, in consultation with the data subjects or their representatives).

The GDPR does not impose a general obligation to designate a data protection officer. The obligation to designate a data protection officer is mandatory only for (i) public authorities or bodies and (ii) data controllers and data processors that have core activities which require systematic monitoring of data subjects on a large scale or which consist of the processing on a large scale of special categories of data and data relating to criminal convictions and offences.

However, the GDPR does still allow member states to require the designation of a data protection officer in other cases. This option reflects the currently diverging policy of the different member states in relation to the designation of data protection officers.

The importance of the data protection officer is confirmed, amongst others, by the protection and independence that is granted to him, as well as the obligation to provide a direct reporting link with the highest management level.

The GDPR implements a mandatory data breach notification obligation. Except if a personal data breach event is unlikely to result in a risk for the rights and freedoms of individuals, a data controller must notify each personal data breach to the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach event.

In addition to the notification to the competent supervisory authority, the data controller also has to communicate, without undue delay, the incident to the data subjects, if the personal data breach is likely to result in a high risk to the rights and freedoms of individuals. The communication shall however not be required under certain circumstance, e.g. if the data controller has encrypted the relevant personal data.

As a corollary to the data controller's data breach notification obligation, a data processor has to notify the data controller without undue delay after becoming aware of a personal data breach. This legal obligation confirms a well-established contractual practice, whereby data controllers already imposed a contractual data breach notification obligation on data processors processing personal data on their behalf.

The removal of unnecessary burden

One noteworthy change is removal of the notification obligation. Under the current data protection rules, a data controller must notify any data processing activity with its supervisory authority. Although it may not seem a particularly onerous obligation, it must be taken into account that local member states have widely varying requirements in relation to this notification obligation. Consequently, multinational groups wishing to comply with this obligation have to review their obligations in each relevant member state. Given the general lack of consultation of the public registers containing these notifications by the data subjects, it is clear that the compliance effort is disproportionate to the intended protective effect. Given the important record keeping duties under the GDPR, the impact of the removal of the requirement of prior notification should not be exaggerated.

The "one stop shop" mechanism may also result in cost savings for multinational groups, as they will normally only be subject to a single supervisory authority. It remains however to be seen in practice to which extent this mechanism will lead to actual cost savings.

A strengthened enforcement framework

Another topic that will undoubtedly continue to be much debated is the strengthening of the enforcement measures.

Current data protection rules already provide for civil and criminal enforcement measures, but the rules differ widely from member state to member state. It is clear that these divergences may induce data controllers to establish themselves in countries with a more flexible approach to enforcement, particularly in view of the existing country of origin principle. Given the fact that the data protection rules shall form part of a single legal instrument, this situation will disappear in the future. As a result, enforcement should be more efficient.

The enforcement of the data protection rules is also reinforced by means of a system of administrative fines. Many countries, including the UK, France and Holland, already have implemented a system of administrative fines. In these countries, the administrative fines appear to be an excellent mechanism for the supervising authorities to enforce the data protection rules. The GDPR takes the height of administrative fines to an entirely new level. For undertakings, administrative fines may be applied up to the higher of (i) 10.000.000 EUR or 2% of the total worldwide annual turnover of the preceding financial year in case of infringement of data processing management related obligations of the data controller and the data processor or (ii) 20.000.000 EUR or 4% of the total worldwide annual turnover of the preceding financial year in case of infringement of the fundamental provisions of the GDPR, the data subject's rights or non-compliance with certain orders from a supervisory authority.

Johan Vandendriessche
Partner Crosslaw
Visiting Professor UGent

Bénédicte Losdyck
Lawyer Crosslaw
Researcher CRIDS (University of Namur)

Bibliography:

- Data Protection reform package (EU Commission website)