Out with the old, in with the new: 6 upcoming changes to EU data protection law under the GDPR

| Tuesday, September 26, 2017

This is the second in a 3-part series examining the Global Data Protection Regulation. Click here for the first article, which gave a high-level overview of the GDPR and stay tuned for future insight on what GDPR enforcement you can expect.

The much-anticipated General Data Protection Regulation (GDPR) will soon replace the current European Data Protection Directive 95/46/EC (the Directive), representing one of the most significant changes to EU data protection law in over two decades. Although the GDPR is similar in many respects to the Directive, there are several important changes to come under this new law that will undoubtedly have a significant impact on companies operating across the globe.

I. Rules Directly Applicable Across the EU: Directive vs. Regulation

The GDPR is different not only in substance to its predecessor but also in form. A regulation applies directly to EU member states and, as a formal matter, allows them little discretion in implementation. On the other hand, a directive sets forth desired results and policies but depends upon member state implementation into national law. Consequently, the Directive required transposition into the national laws of each member state, resulting in 28 different interpretations of EU data protection law and, as such, a fragmented legal landscape in Europe.

As the GDPR is a regulation, and not a directive, it has immediate binding legal force and will create a

unified data protection law that is directly applicable in all EU member states (as well as in Iceland, Liechtenstein and Norway, which are part of the European Economic Area), without the need for national implementing legislation. When the GDPR takes effect on May 25, 2018, it will automatically become part of each member state's legal framework and should reduce—though probably not eliminate—the current patchwork of data protection laws across the EU.

II. Expanded Territorial Scope

Arguably, the biggest change to the regulatory landscape of data protection law comes with the extra-territorial reach of the GDPR.

Presently, the Directive only applies to businesses that either collect and/or use personal data and are established within the EU (such as by way of having an office, branch or agency located in a member state), or if they are established outside the EU but use equipment within the EU to process personal data. EU jurisprudence deems "equipment" to include servers and employees, and even in some cases only one representative, as well as more traditional forms of equipment. Thus, there would generally be no jurisdiction with respect to a non-EU established entity that did not utilize any means within the EU for processing personal data.

As compared to the Directive, the GDPR has a significantly broader territorial scope that applies not only to organizations established within the EU (regardless of whether such processing takes place in the EU), but also to organizations based outside the EU that process the personal data of EU data subjects in connection with either:

- The "offering of goods or services" to data subjects in the EU (irrespective of whether payment is required), or
- The "monitoring" of their behavior within the EU.

Under the first prong, determining whether a non-EU established business offers goods or services to EU data subjects is based on the business's intent (i.e., whether it "envisages" offering goods or services to a data subject). The GDPR explains that having a commerce-oriented website that is accessible to EU residents does not by itself constitute offering goods or services. However, the existence of certain factors could indicate a non-EU company's intention to attract EU residents as customers and, as a result, become subject to the GDPR. Such factors include:

- Marketing goods or services in the same language generally used in an EU member state.
- Listing prices in EU member state's currencies (e.g., the euro, British pound and Swiss franc) and enabling EU residents to place orders using such currency.
- Referencing EU users or customers in its publications or online.

Even if a business cannot adequately demonstrate that its activities sufficiently satisfy the first prong of this analysis, it still must consider whether it engages in the "monitoring of behavior," the practice of tracking individuals online to create profiles and analyze/predict personal preferences, behaviors and attitudes. Moreover, all websites that use tracking cookies and applications that track online usage will be subject to the GDPR to the extent that the information collected, in the aggregate, renders an individual identifiable. In practice, this means that a company located outside the EU which is targeting or profiling consumers in the EU, such as ad tech or social media companies, for example, will likely be subject to the GDPR. This demonstrates a huge shift from the existing Directive.

Obligation to appoint a representative

Non-EU-established organizations that are caught by the GDPR's long-arm jurisdictional reach based on its processing activities with regard to residents of an EU member state will be obligated to appoint a representative to act on their behalf in that member state, unless the processing:

- Is occasional.
- Does not include large scale processing of sensitive personal data (such as racial origin, health/genetic data, religious beliefs, etc.).
- Is unlikely to result in a risk to the rights and freedoms of data subjects. The primary role of this representative is to liaise with the relevant supervising authorities.

III. Direct Liability Imposed on Data Processors

As discussed in the first alert in this series, EU privacy law differentiates between data controllers and data processors.

Under the existing Directive, a data controller would often impose data protection responsibilities and obligations onto the data processor within the parties' service contract to protect itself against unnecessary data protection compliance risk. In doing so, the data processor would be contractually liable to the data controller but would not be subject to direct enforcement or penalties from a data protection regulator.

In contrast, the GDPR imposes direct statutory obligations on data processors. These obligations mean that data processors may be subject to direct enforcement by supervisory authorities, serious fines for non-compliance and compensation claims by data subjects for any damage caused by breaching specific provisions of the GDPR. Some of the main obligations imposed on data processors by the GDPR include the following:

- Appointing a representative in the EU if not established in the EU.
- Ensuring certain minimum clauses in contracts with data controllers and complying with the mandatory requirements with regard to the content of the Processing Agreement entered into with each data controller.
- Keeping a written record of processing activities carried out on behalf of each controller.
- Cooperating, on request, with the supervisory authority in the performance of its tasks.
- Notifying the data controller without undue delay after becoming aware of a data breach.
- Designating a data protection officer (DPO) in specified circumstances.
- Obtaining prior written authorization from the data controller before subcontracting out any data processing.

IV. Data Breach Notifications

At present, the Directive does not require member states to impose data breach notification obligations. When the GDPR comes into force, however, it will drastically change the current status quo of data breach reporting in the EU. Notably, the GDPR will impose a widespread mandatory breach notification obligation on all organizations subject to its provisions with respect to providing notice of a personal data breach to the relevant supervisory authority and, in some cases to the individuals affected, within a very short timeframe following discovery of the breach.

Under the GDPR, a personal data breach is broadly defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." The breach notification requirements take different forms depending on whether the company is acting as a "data controller" or a "data processor." These scenarios and related obligations are discussed more fully below.

Obligation for data processors to notify data controllers

In the event that a processor becomes aware of a data breach, it must notify the controller of such breach without undue delay. Beyond this, the processor has no other notification or reporting obligation with respect to a personal data breach under the GDPR.

Obligation for data controllers to notify supervisory authorities

Data controllers must notify the relevant supervisory authority of a personal data breach without undue delay and, where feasible, not later than 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk for the rights and freedoms of individuals.

Although the risk of harm exception affords some discretion to controllers for assessing whether or not a breach must be reported, it should be interpreted narrowly. In order to use the exception, a controller must demonstrate – in accordance with the accountability principle – that the breach is unlikely to result in a risk to the rights and freedoms of individuals. For example, breaches that may cause damage to reputation or result in identity theft or fraud, discrimination, financial loss or exposure of personal data protected by professional privilege will likely need to be reported.

To the extent such an exception does not apply, the notification to the regulator must, at a minimum, describe:

1. The nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned.
2. The name and contact information of the organization's DPO or other point of contact.
3. The likely consequences of the breach.
4. The measures taken or proposed to be taken to address the breach and mitigate its effects

Controllers that notify after 72 hours of discovering a breach will be required to demonstrate a reasoned justification. Where it is not possible to provide all relevant information about a breach at once, information may be provided in phases without undue further delay. Controllers are also required to keep a record of – and document – any data breaches (whether or not it is notified to the supervisory authority) and permit audits by the supervisory authority.

Obligation for data controllers to notify affected data subjects (individuals)

If a breach is likely to result in a high risk to the rights and freedoms of data subjects, the data controller will also have the obligation to notify those affected data subjects of the breach without undue delay. Notification to individuals must have the same content of the notification submitted to the relevant supervisory authorities and needs to be provided in clear and plain language.

The GDPR provides exceptions to this additional requirement to notify data subjects in situations where:

1. The controller has implemented appropriate technical and organizational measures that render the data unintelligible to any person who is not authorized to access it, such as encryption.
2. The controller has taken subsequent actions that ensure the high risk for the rights and freedoms of data subjects is unlikely to occur.
3. When notification would involve a disproportionate effort. (In this instance other notification methods, such as a public announcement, should be used.)

Even if the controller determines that a breach does not pose a high risk to individuals' rights and freedoms, a supervisory authority may still override that decision and require them to notify the affected

data subjects of the breach.

V. Reinforcement of Data Subjects' Rights

The GDPR enhances and clarifies the existing rights of data subjects set forth by the Directive, in addition to introducing a number of new rights for data subjects, some of which are detailed below.

Fair processing notices (the right to be informed)

The principle of fair and transparent processing means that the data controller must provide information to data subjects about its processing of their data, unless the data subject already has this information. Under the Directive, a controller already must provide the data subject with the identity of the controller, the purpose of the processing and the recipients of the data. However, under the GDPR, the list of data to be provided is expanded to include the following:

- Details of any relevant DPO.
- The legal basis for the processing of the data.
- Details of data transfers outside the EU, including how the data will be protected (e.g., the recipient is in an "adequate" country; Binding Corporate Rules are in place, etc.).
- The retention period for the data or, if that is not possible, the criteria used to determine this.
- The existence of rights of the data subject in relation to their personal data.
- The individual's right to complain to a supervisory authority.
- Whether there is a statutory or contractual requirement to provide the data and the consequence of not providing the data.

This information must be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language (in particular where the data subject is a child). In addition, where a controller wishes to process existing personal data for a new purpose, they must inform data subjects of that further processing, providing the above information.

The right of access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Although this right existed in the Directive, it is expanded in the GDPR to require controllers to provide more detailed information similar to what is required in the Fair Processing Notices.

If a request is made in electronic form, the information should be provided in a commonly used electronic form (unless the data subject requests otherwise). This could impose costs on controllers who use special formats, or who hold paper records. In addition, controllers no longer have the right to charge a fee for providing this information to data subjects, subject to some narrow exceptions. Controllers also must respond to these requests for information within one month of receipt, with a possibility to extend this period for particularly complex requests.

The right to object

Although the right to object to processing already exists in the Directive, the GDPR clarifies and further expands upon this right granted to data subjects. As is currently the case, any individual has the right to object to direct marketing at any time, and in that event, the controller must stop using the information for marketing purposes. This is an absolute right; once the individual objects, the data must not be processed

for direct marketing any further under any condition.

In addition, data subjects have the right to object to processing which is legitimized on the grounds of either the legitimate interests of the data controller or the public interest, in which case the controller must then cease processing of the personal data unless it can demonstrate either:

- Compelling legitimate grounds which override the interests of the data subject.
- That the processing is for the establishment, exercise or defense of legal claims.

Unlike the Directive, which placed the burden on the data subject to demonstrate "compelling legal grounds" when objecting to data processing, the GDPR places the burden directly on the controller to establish why it should, despite the data subject's objection, be able to process personal data.

The right to data portability

The GDPR introduced the right to data portability as a means of further empowering data subjects in giving them greater control over their personal data. To the extent data subjects have provided their personal data to a controller, and the controller processes that data by automated means and on the basis of consent or a contract, data subjects may require the controller to provide them with their personal data in a structured, commonly used and machine-readable format, and, where technically feasible, transmit that data directly to another controller.

In essence, data subjects have the right obtain and reuse their data for their own purposes and across different services. The reasoning behind this point is that user data should be protected from 'siloed' or closed systems that facilitate customer "lock-in," and where the controller of the data does not permit the user to change providers. To that end, the GDPR expresses the wish that controllers are stimulated to develop interoperable formats that enable data portability. In practice, this means that data controllers need to provide functionality that enables the data subject to move, copy or transfer personal data easily from one IT environment to another, without hindrance (even if honoring this right could result in handing over valuable personal data to a competitor).

Notably, the right to portability is limited, as it applies only where the data is processed:

1. By automated means (therefore excluding paper files), and
2. On the basis of consent or as necessary for the performance of a contract to which the data subject is a party (but not where the data was obtained on other grounds – e.g., compliance with a legal obligation)

VI. Consent and Children

Recognizing that children deserve specific protection of their personal data, the GDPR (unlike the Directive) make express reference for consents provided by children and place limits on their ability to consent to data processing without parental authorization. In essence, it prescribes that, in an online context, the age for consent is 16 by default; however, member states are granted the option to set this threshold age to as low as 13 years old. Below the specified age, verifiable parental or guardian consent will be required where information society services (which will cover the vast majority of online services, including any chargeable online offerings) are offered to a child.

For example, where online services are offered to children, the processing of personal data of a child below the age of 16, or if provided for by member state law a lower age which shall not be below 13, requires

consent to be given or authorized by the person with parental responsibility for the child. The controller will be required to make reasonable efforts (taking into account available technology) to verify the parental consent.

Consequently, the national variation in threshold ages will certainly pose a challenge for the operators of websites and mobile apps operating across several member states and will inevitably result in a lack of harmonization, as it would not be surprising to see numerous member states opt for a lower age of consent.

Interestingly, the GDPR's consent requirements for children apply only to certain online data – it has no impact on offline data and, as such, that data will continue to remain subject to the usual member state rules on capacity to consent. Moreover, the protection afforded to children under the GDPR does not affect the general contract laws of member states regarding the validity, formation or effect of a contract with a child, nor does it change the age of legal consent under those laws for purposes of entering into a contract with a child.