Proskauer

An Overview of the New General Data Protection Regulation

Privacy Law Blog on **August 3, 2016**

The European Parliament has approved the reformed General Data Protection Regulation (the "GDPR"). Because this is a Regulation (rather than a Directive), this legislation will apply automatically in every Member State (without need for additional domestic legislation) when it comes into force on **May 25, 2018.**

Many of the requirements are similar to those set out in Directive 95/46/EC (the "EU Directive"); however, there are certain key differences. The table below summarizes the key changes.

Topic	The current position	The new GDPR position	Comment
Transparency in data processing	Data must be fairly and lawfully processed.	Data will need to be processed fairly, lawfully and transparently. This requires a business to provide information in clear, intelligible and plain language in an easily accessible form. In line with this, privacy policies will need to be clear, understandable and easily accessible.	These changes place the onus on businesses to provide clarity and transparency to ensure individuals can understand clearly how and why their data is being processed and removing the scope for businesses to hide behind technical jargon.

Topic	The current position	The new GDPR position	Comment
Consent	Consent is a valid basis for transferring data; however, the consent needs to be "*freely given and unambiguous.*" Many companies include consent wording in employment contracts to cover data gathering and transfers. There has been debate as to whether such consent is valid or not.	Regulators have generally disapproved of using consent to enable data processing. Now there are more detailed conditions for using consent; namely consent must be "*freely given, specific, informed, and unambiguous.*" In cases of sensitive personal data it must also be "*explicit*." The GDPR goes on to say that "…*in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters*…"	The new requirements will make consent even more difficult to rely upon as a valid basis for transferring data, including where consent is given in the context of agreeing to terms of employment.
Data subjects rights	Data subjects have explicit rights to rectification and erasure. The right to be forgotten was introduced through case law.	Individuals' rights have been extended to explicitly include the right to be forgotten, the right to switch personal data between service providers (known as data portability), and the right to know if their data has been hacked.	These expanded rights strengthen the controls that individuals have on the use of their data. However, the rights will significantly impact businesses, particular those that rely on the gathering, analysis and transfer to third parties of personal data.

Topic	The current position	The new GDPR position	Comment
Subject Access Requests	To make a subject access request, individuals must go through a number of steps. In the UK, this includes writing to the business specifying the information sought and paying a fee of up to £10. The business must respond to the request promptly and certainly within 40 days of receipt.	In most cases a fee will no longer be payable, and business will only have a month to comply with a request. However, a business can refuse to act on the request if it is "*manifestly unfounded or excessive.*" Additional information will need to be provided to the person making the request e.g., data retention periods.	The time to respond to a request is shortened, which will create an additional burden on the business, but the ability for a business to refuse to act on a request that is "*manifestly unfounded or excessive*" will be welcomed.
Data Protection Officers ("DPO")	Although there is no requirement to have DPO, some business have appointed one internally, or appointed an independent third-party to carry out this role (this enables certain businesses to exempt themselves from certain notification requirements).	All public authorities must appoint a DPO. Certain other businesses whose activities involve "*regular and systematic monitoring of data subject on a large scale*" or the large-scale processing of "*special categories of personal data*" will need to appoint a DPO to oversee compliance.	It may be difficult for businesses to ascertain if they are required to appoint a DPO and will increase the administrative burden on those required to do so.
Multi-jurisdictional businesses	Non-EU companies who targeted EU citizens do not necessarily have to comply with the EU Directive.	Businesses that target the EU, i.e., offering goods or services to EU citizens or monitor the behaviors of EU citizens, even if the business itself is not based in the EU, will be subject to the GDPR.	This change will significantly increase the extraterritorial reach of European data privacy legislation.

Topic	The current position	The new GDPR position	Comment
“One-stop shop”	Businesses have to deal with the requirements of each of the different data protection authorities of every jurisdiction in which they operate. As the EU Directive was implemented differently in different jurisdictions this means that currently, different jurisdictions have different requirements.	Businesses targeting the EU and/or operating in the EU and processing data in multiple EU jurisdictions will have to establish the location of their “*main establishment*” to determine which Member State’s data protection authority’s control the business comes under.	This is the so-called “one-stop shop” so that it is easier to do business in the EU, as a business will no longer need to deal with different data protection authorities in different jurisdictions.
Enforcement	Currently, each local data protection authority is responsible for determining the level of any fines imposed. For example, fines in the UK are currently set at £500,000 maximum, though most fines that the UK data protection authority has imposed are substantially lower. This is similar to other EU Member States.	The ability to impose harsher penalties will be introduced. The maximum penalty for non-compliance will become the higher of EUR20 million and 4% of an undertaking’s worldwide turnover.	Given the disparate fines across the EU, as well as the concept of the “one-stop shop,” how data protection authorities in each Members State enforce the GDPR remains to be determined. However, the GDPR gives the scope to impose fines that are substantially larger than those commonly imposed at the moment.

Next steps

After much waiting, we now have the final version of the new legislation which means businesses are now able to start preparing for its implementation. Practical steps to help get prepared include appointing a person or team (either internally or externally) that can audit current data protection policies and procedures and identify the changes needed to ensure compliance with the GDPR. The review should cover a broad range of areas including:

- the structures in place for processing employee data, client and customer data;
- any data protection policies and/or notices;
- agreements in relation to the transfer of data, including international transfers of data;

- default data retention periods;
- the processes for handling data breaches;
- IT changes needed to implement changes identified; and
- whether there is a need to appoint a DPO.

View Original.

Related Professionals

- **Kelly M. McMullon**
  Special International Labor, Employment & Data Protection Counsel