www.inblf.com

Privacy Matters: an overview of the European Union's General Data Protection Regulation

Introduction

In recent years, technological advances such as mobile and cloud computing and the ubiquity of the internet have made it ever easier for organisations to handle vast amounts of data about their customers, suppliers and staff, to move the information around and to share it domestically and internationally. With greater volumes, sharing, and outsourced processing comes increasing threats to that data, some external (such as theft by hackers) and others internal (such as corruption or accidental loss by employees).

Understandably, particular concerns arise in relation to data relating to people lives, namely personal data. Those concerns have been exacerbated by the publicity surrounding incidents such as the mass surveillance of EU citizens by the US National Security Agency (which led to the revelation of this activity by Edward Snowden in 2013), the hacking attack on a Sony data centre in 2015 and, more recently, the hacking attacks on British Airways, on Marriott International, the hotel group, and on Capital One, the credit card company, resulting in the theft of personal data relating to millions of people.

In short, organisations handling personal data are rightly concerned about what they can or cannot do with it, and people want to feel that their privacy will be respected.

Last year, the EU General Data Protection Regulation 2016/679 ("GDPR") came into effect. It concerns itself with personal data and replaces the old regime which was based on a Directive dating back to 1995 (EU Directive 95/46/EC). It has been a long time coming.

The regulation has many similarities with the old regime, not least of all in respect of the core principles which underpin it. However, it is more prescriptive to make changes in a number of

aspects, introduces some new concepts, and is underpinned by much tougher sanctions. As such, it can be seen as somewhere between evolution and revolution.

The purpose of this paper is to introduce the main concepts and themes of the GDPR with more detailed analysis of sub-topics to follow in later papers. In this regard, it should be noted that there are many other laws which concern themselves with data, such as confidentiality laws and regulations which are specific to the sector in which a business operates (e.g. financial services regulations). These are outside of the scope of this paper.

Before exploring GDPR's details, as a preliminary observation, GDPR came into effect from 25 May of 2018 without the need for member states to introduce enabling legislation. This is known as "direct effect" which is in contrast to EU directives, which required each member state to introduce enabling legislation and all that entails with some member states taking a lighter touch. The use of a regulation is, therefore, intended to ensure greater consistency across the EU member states, albeit allowing member states to introduce specific rules in discrete areas (known as "derogations"). That said, it remains to be seen whether the regulators across the member states will adopt consistent attitudes to enforcement and sanctions.

The seven core principles

Before looking at the seven core principles of the regulation, it is worth looking at some key definitions.

As mentioned above, the regulation concerns itself with the "processing" of "personal data." The term "personal data" refers to any information relating to an identifiable or identified living individual ("the data subject"). A typical example is someone's name and address. Another common expression for personal data, especially in the U.S., is "personally identifiable information" (PII).

"Processing" is very widely defined to include activities such as collecting, retrieving, organising, storing, transmitting and disseminating of personal data. In short, just about any handling of personal data, including merely viewing it, is a form of processing which is covered by the regulation.

The regulation makes a distinction between a "controller" and a "processor." A controller means the organisation that determines the purpose and means of processing of personal data. A good example of a controller is a retailer that handles personal data, such as contact and payment information, relating to its customers.

A "processor" means an organisation that processes personal data on behalf of the controller. By way of example, if a retailer (as a controller) looks to put some or all of the personal data it is handling into the cloud, the cloud service provider would be considered a processor. In the retail example, the consumer is the data subject.

All organisations, including businesses providing products and services only to other businesses, will be handling personal data in some shape or form, if nothing else the personal data the business collects from its own employees.

Whilst most of the obligations under the regulation fall on the shoulders of controllers, the regulation imposes some statutory obligations on processors. Moreover, the regulation requires that controllers include certain contractual obligations on processors in agreements these controllers enter into with their processors.

The regulation affords additional protection to special categories of data (which are akin to sensitive personal data under the directive). Examples include data by which a person's racial or ethnic origin or religious beliefs can be ascertained. It also extends to health data and to biometric data (such as thumbprints).

Organizations share personal data from time to time. In some cases, a controller shares personal data with a processor (such as in the retail example mentioned above). In other cases, a controller shares personal data with another controllers. In some business contexts, two businesses collecting personal data from the same data subjects for a common purpose are joint controllers. In other situations, different combinations of all of these situations may apply. We will pick this up in later papers.

The seven principles are set out in Article 5 of the regulation.

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subjects ("lawfulness, fairness and transparency");
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, subject to limited caveats in relation to purposes such as scientific research ("purpose limitation");
3. adequate, relevant and limited to what is necessary in relation to the purpose in which they are processed ("data minimisation");
4. accurate and, where necessary kept up to date, with every reasonable step to be taken to assure that inaccurate data is erased or rectified without delay ("accuracy");
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed, subject to caveats in relation to purposes such as scientific research ("storage limitation");
6. processed in manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality");

The regulation goes on to stipulate that the:

7. the controller shall be responsible for, and be able to demonstrate compliance with, the six principles mentioned above ("accountability").

The lawful bases

In relation to the first principle ("lawfulness, fairness and transparency"), Article 6 states that the processing shall be lawful only if and to the extent that at least one of the following applies:

1. that the data subject has given consent to the processing of his or her personal data for one or more specified purposes;
2. the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. the processing is necessary for compliance with a legal obligation to which the controller is subject;
4. the processing is necessary in order to protect the vital interests of the data subject or another person;
5. the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden in the interests or fundamental rights and freedoms of the data subjects which require protection of personal data, in particular where the data subject is a child.

The sixth subsection of this article ("legitimate interests") does not, however, apply to processing carried out by public authorities in the performance of their tasks.

The regulation places additional restrictions in relation to the processing of special categories of personal data. For example, if the controller wishes to rely on consent, the consent must be explicit (i.e. in writing) and "legitimate interests" lawful basis cannot be relied on.

Businesses which collect personal data from consumers typically rely on consent and/or performance of the contract to collect personal data, transact, and communicate with data subjects in their routine activities. In the business to business context, the "legitimate interests" basis is more commonly used.

Transparency and accountability

The first six of the seven core principles are very similar to the principles under the directive save that first principle now includes the concept of transparency, namely that people need to be kept informed. The concept of transparency appears in the first (and arguably, the most important) of the core principles that serve to emphasise the importance which the legislators have attached to it. The regulation goes on to spell out some detail, the sorts of things that need to be done to comply with the transparency requirement (such as privacy notices), which will be discussed further below.

The seventh principle ("accountability") is, however, a completely brand new concept, namely the requirement that controllers must not only comply with the six principles mentioned above, they must also be able to demonstrate compliance (i.e. comply and be seen to comply). This requirement is so important in the eyes of the legislation that it is expressed as a principle in its own right. In broad terms, it points to the need for controllers to have robust governance in place and to be able to evidence this, e.g. by way of policies and procedures). As with transparency, the regulation spells out the sorts of things which controllers need to do to satisfy this requirement (such as undertaking impact assessments) which will be considered later in this article.

Consent

As mentioned above, one of the lawful bases for processing personal data is consent and to be able to evidence this.

Whilst this basis was also available under the directive, the regulation (and, in particular, Article 7) has raised the bar. First and foremost, if processing is based on consent, the controller must be able to demonstrate that the data subject has consented to the processing of his or her personal data. The ability to evidence consent promotes compliance with the "accountability" principle mentioned above.

Whilst consent can be applied, the regulation makes it clear that the consent must be freely given, specific, informed and unambiguous. When consent is being sought, it is also incumbent on the controller to let the person know that he or she can withdraw his or her consent at any time.

The consent must be by way of an express statement or implied by way of clear affirmative action by the data subject. For example, implied consent would likely exist where a trade show attendee hands her business card to a representative of an exhibitor saying she is interested in the products of the exhibitor. By contrast, silence or pre-ticked boxes or inactivity on an online form are insufficient.

If consent is given in the context of a written declaration which concerns other matters, the request for consent must be readily distinguishable from the other matters, and readily accessible using clear and plain language. If the declaration does not meet these standards, the consent will not be binding. One example is a situation where a data subject is confronted with a form seeking to secure consent for a range of matters including consent to the processing of his or her data in, say, a single tick box. This will not work.

Importantly, paragraph 4 of Article 7 makes it clear that if the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract, consent will not be considered to have been freely given. In other words, a controller should not use consent as a basis for gathering personal data which it does not need and/or to go on a fishing expedition.

If consent is sought in relation to the processing of the special categories of data, Article 9 makes it clear that the consent must be explicit. In other words, consent cannot be implied from the circumstances and must, of course, comply with the requirements of Article 7 (for example it must be freely given, specific, informed and unambiguous).

Technical and organisational measures

A common theme in the regulation is the need for controllers to have, in place, technical and organisational measures to comply with the regulation including the six principles and, in particular, the sixth principle (which relates to security of persona data).

Taking the security example, and to paraphrase, the controller must keep the data secure and be on guard against external threats (for example, from hackers), and insider threats (namely from its own employees and consultants). Technical measures should, for example, include ensuring that vulnerabilities in IT systems are patched promptly. Organisational measures relate to the people side of things such as making sure that it has appropriate policies and procedures in place for its employees to comply with its security practices and procedures. Whilst the more high-profile hack attacks in the media exploit vulnerabilities in IT, most breaches of the regulation (for example, data leakage) are down to accidental loss by employees.

In the meantime, by way of context, I set out below a specific example of where technical and organisational measures come together. A sloppy practice seen time and time again (and which

has been the subject of cautionary tales posted by the UK regulator, the ICO) is where an employees, wanting to work on documentation over, say a weekend, downloads the documentation onto a portable devide (e.g a flash drive) which is not password protected and then loses it on the way home. Organisational measure could include making sure that the employee understands (through awareness raising and training) that this activity is not acceptable, particularly if personal data and/or confidential information is involved and that he/she needs to follow a particular procedure (i.e ask the IT department). On the technical measures side, the organisation could/should, for example, set up the systems so that it is impossible for data to be extracted s onto portable devices) so that the employee in question has no choice but to ask someone in the IT department to facilitate copying the data in the first place (and, in so doing, ensure the device is protected).

The requirement in Article 32 of the regulation is to use "reasonable" care to protect personal data. What is "reasonable" will depend on the context of the organization, its capabilities, and the sensitivity of the personal data being protected.

Transparency and Rights of Individuals

As mentioned above, one of the most important aspects of the regulation is the emphasis it places on the rights of data subject, namely the idea to put people back in control of their personal data. In order to give people informed choices, the regulation requires keeping people informed ("transparency")

Underpinned by the first principle ("lawfulness, fairness and underlying transparency"), the regulation goes on to spell out what controllers need to do to comply with this requirement.

If the controller collected the personal information from the data subject, it is required to provide certain information to the data subject in question including its identity and contact details,

contact details of the data protection officer (where applicable), the purpose of the processing for which the personal data are intended as well as the legal basis for the processing (and if the lawful basis is the legitimate interests, what those legitimate interest are), the categories of the recipients of the personal data, (such as cloud service providers), and if the controller intends to transfer the personal data outside of the European Economic Area, how it will be complying with the regulation's rules surrounding the export of personal data.

The controller is also required to let the data subject know, amongst other things: the period for which the personal data will be stored or if that is not possible the criteria used to determine that period; the rights of the data subject such as the right to object (which are considered below), if processing is based on consent, that the data subject's right to withdraw that consent and its right to lodge a complaint with the supervisory authority.

The regulation imposes similar requirements in relation to situations where the controller obtained the information from other sources (such as in a controller-to-controller transfers) as opposed to collecting it from the data subject. In particular, it is required to reveal the source of the personal data including publicly available resources.

The regulation does not prescribe how the information is communicated, but it is typically done by way of privacy notices, privacy statements or communications to the data subjects that point them to a privacy statement it has published on its website.

As the regulation is much more prescriptive about what needs to be communicated to data subjects, than under the directive, privacy notices/statements are typically much longer than the ones which were issued under the old regime.

CONCLUSION

As indicated above, the purpose of this paper is to introduce the main themes and concepts of the GDPR.

As is demonstrated by the fines which the Information Commissioner's Office (the UK data protection authority) intends to levy on British Airways (just over £180 million and on Marriott International (just under £180 million), data security, which is a key component of technical and organisational measures, remains a key issue.

That said, cases such as the fine which the CNIL (the French data protection authority) has recently imposed on Google (50 million Euros) puts the concepts of "lawful bases" and "transparency" in the spotlight. (In short, the CNIL considered that the consent for ad personalisation was invalid because it was ambiguous and unspecific and that essential information, such as processing purposes, was excessively disseminated across several documents.