The General Data Protection Regulation (GDPR)

Tim Kaye

Contents

Assigned Reading

Heather Burns and Dan Barker, *GDPR: A Guide for eCommerce* (included with your course materials). Note that this is written as a guide for e-commerce businesses in the United Kingdom, so some references are UK- rather than EU-specific.

The full text of the Regulation may be found online at https://gdpr-info.eu/. A PDF version is included with your course materials.

Introduction

The GDPR is arguably the most significant instrument of international law to have been enacted in the twenty-first century. It has certainly had more immediate impact than any other international law. Indeed, while it is an instrument of EU law, its impact has been felt around the world, as business after business has sent out emails asking individuals for consent to process their data.

As Art. 1(1) says, the GDPR "lays down rules relating to the protection of natural persons [in the EU] with regard to the processing of personal data and rules relating to the free movement of personal data." This means that any businesses and organizations that process data on a person within the EU are subject to the GDPR, irrespective of where they themselves are based.

While some commentators predicted that the GDPR would nevertheless be ignored by companies and organizations outside the EU because of a perceived difficulty in enforcement, the reality has been quite the reverse. Through previous successful prosecutions (under other laws) of some of the biggest companies in the world, including Microsoft and Google, the EU has established a reputation for following through on its laws, and Microsoft has already promised to comply with the GDPR even when any personal data it processes relates to persons outside the EU.

In addition, the GDPR will effectively be indirectly enforced, as many organizations will insert clauses in contracts that their contractual partners must comply with the GDPR. Yet, to judge from many of the emails sent out, the GDPR is poorly understood. Many of those emails were unnecessary and counter-productive.

With an emphasis on the implications for e-commerce — which includes the provision of services, such as legal services, over the web — this class will provide clarity on one of the most important international law topics of the moment.

Human Rights or Consumer Rights?

This is the fundamental philosophical question at the heart of the issue. In the GDPR, the EU has taken the former view. The Recitals to the GDPR assert, for example, that:

> The protection of natural persons in relation to the processing of personal data is a fundamental right. (Recital 1)
>
> The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. (Recital 2)
>
> The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. (Recital 4)

The US, by contrast, generally treats privacy and personal data as things to be traded as part of the price of receiving goods or services, except in specific instances where legislation — such as the Health Insurance Portability and Accountability Act (HIPAA) or the Family Educational Rights and Privacy Act (FERPA) — applies. This also suggests that the EU and US differ in their respective views as to what "personal" means in the context of data.

READING: Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy* (included with your course materials).

The GDPR is *not* about "fixing" or regulating Facebook

- For example, the GDPR is not — and is not intended to be — a panacea for online hate speech, or to prevent meddling by one nation in the affair of another.
- It is simply concerned with maintaining the privacy of personal information.

READING: Mark Zuckerberg, *The Internet needs new rules. Let's start in these four areas* (included with your course materials).

Six (Plus One) Privacy Principles in Article 5

Article 5(1) requires that personal data shall be:

Lawfulness, Fairness and Transparency

> (a) processed lawfully, fairly and in a transparent manner in relation to individuals.

Purpose Limitation

> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Data Minimisation

> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage Limitation

> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

Integrity and Confidentiality

> (f) processed in a 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”).

Accountability

Article 5(2) adds:

> The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).

Practical Implications

Summary

As Burns and Barker explain (at p. 22):

> The most fundamental step towards GDPR compliance is being constantly aware of *what* personal data your business holds, *why* you collect it, *where* it is stored, and *who* you share it with.

Fines

The GDPR takes a tiered approach to the levying of fines.

Art. 83(4) provides for administrative (i.e. civil, not criminal) fines of up to €10 million, or 2% of a business's total worldwide annual turnover (whichever is higher) for certain types of infractions of the GDPR.

Art. 83(5) deals with the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of a business's total worldwide annual turnover (whichever is higher).

Big Data

The principles of purpose limitation and data minimisation have major implications for the capture and processing of big data, unless the data is processed purely for "statistical purposes" (Recital 162).

Web Browsing

- Web pages must no longer contain code that has the effect of breaching the GDPR, which means that such pages will often be much faster to load.

READING: David Murphy, *To Make Websites Load Faster, Browse the Web Like a European* (included with your course materials).

Specific Provisions

Basic definitions and principles

- Chapters I (Arts. 1–4) and II (Arts. 5–11).
- "Personal data" means "any information relating to an identified or identifiable natural person" (Art. 4(1)).
- Note the circumstances in which processing of personal data is permitted without the consent of the data subject (Art. 6).

- Highly relevant to collection of data required for EU VAT in order to charge correct VAT rate.

- Note that this also means that many emails among the flood you probably received last year, asking you to consent explicitly to receipt of further emails from that organization, were unnecessary and almost certainly counter-productive.

Rights of data subjects

- Chapters III (Arts. 12–23).

- Note, in particular, the right to rectification (Art. 16), the right to be forgotten (Art. 17), and the prohibition on automated decision-making except in specific circumstances (Art. 22).

READING: Jeffrey Toobin, *The Solace of Oblivion* (included with your course materials).

Processing specific types of data

- Chapter IX (Arts. 85–91).

Obligations of data controllers and processors

- Chapter IV (Arts. 24–43).

Transfers of personal data to third countries or international organizations

- Chapter V (Arts 44–50).

- Note the basis of the arrangement with the USA, known as Privacy Shield (Art. 45(1)).

Enforcement and compliance mechanisms

- Chapters VI (Arts 51–59) and VII (Arts. 60–76).

Liabilities and sanctions

- Chapter VIII (Arts. 77–84).

- Private contractual provisions.

Housekeeping

Class Attendance

This course is 1 credit hour and will meet for approximately 3 hours per class with a break in the middle. The Stetson Study Abroad Attendance Policy will apply.

Course Assessment

This class will be assessed by a one-hour exam administered at the end of the course.

Availability

I will be available before and after each class. You can also contact me at tkaye@law.stetson.edu.