EU GDPR & EU-US Privacy Shield

A Pocket Guide

Alan Calder

itgp™

EU GDPR
&
EU-US Privacy Shield

A Pocket Guide

ALAN CALDER

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom

www.itgovernance.co.uk

First published in the United Kingdom in 2016
by IT Governance Publishing.

ISBN 978-1-84928-872-9

ABOUT THE AUTHOR

Alan Calder is the founder and executive chairman of IT Governance Ltd (*www.itgovernance.co.uk*), an information, advice and consultancy firm that helps company boards tackle IT governance, risk management, compliance and information security issues. He has many years of senior management experience in the private and public sectors.

The company operates websites around the world that distribute a range of books, tools and other publications on IT governance, risk management, compliance and information security.

CONTENTS

INTRODUCTION

Over the last decade, cyber security has become an increasingly important issue for organisations across the EU. While cyber threats cover a wide spectrum of targets, from critical national infrastructure to intellectual property, from trade secrets to financial information, a key area of interest for cyber criminals continues to be personally identifiable information, or PII.

PII – names, addresses, social security or tax identifiers, payment card information – is valuable because it can open routes to a wide range of crimes, including economic theft and identity crime.

The migration of business to the Cloud magnifies the risk; PII held somewhere beyond a clearly-defined physical and logical security perimeter is open to a wide array of attacks, and it is often not in fact clear where PII is held, or by which organizations, or under what security arrangements.

The concern of the individual – what data protection legislation usually calls the data subject – extends way beyond cyber crime. Nation states and large organisations are now able to gather substantial volumes of personal information, which enables them to track individual activity in cyberspace. Digital marketing companies evolve new and ever more effective methods of tracking consumers. Social media companies thrive on

publishing personal data. While there are social benefits to all this activity, it can also potentially undermine individual privacy.

The EU has long been at the forefront of the movement to protect the rights of individuals in respect of their personal data. The General Data Protection Regulation (GDPR) – which is now law and comes into force from May 2018 – is probably the world's most significant forward step in the move by elected authorities to ensure that the privacy and personal data of their citizens is appropriately protected.

The GDPR creates a level playing field for data protection across all the EU member states. This means that citizens of EU member states can expect to be treated the same way, wherever they are in the EU, and that organisations complying with the GDPR requirements in one jurisdiction can be assured that they will be compliant across all member states.

American organisations outside the EU – and supplying services into the EU – are also within the scope of the GDPR. Existing arrangements for data export from the EU to other countries is covered specifically and, most importantly, breaches of the GDPR are penalised with fines that are intended to be 'proportionate and dissuasive', with a maximum penalty of €20 million or 4% of global revenue, whichever is the larger.

The transition period for bringing data handling practices into compliance with the GDPR ends in

May 2018. From that point on, organisations that breach the legislation run the risk of substantial fines for breaches.

This pocket guide aims to help you thrive under these new conditions by providing you with an understanding of the Regulation, the broader principles of data protection, and what the Regulation means for businesses – and doing business – in Europe and beyond.

There are key terms throughout this book that need to be properly understood to really get to grips with the new Regulation, which are defined in Chapter 2 – Terms and definitions.

CHAPTER 1: A BRIEF HISTORY OF DATA PROTECTION

The common conception of data protection is a very modern notion. We think of digitally stored databases and records, and we understand the importance of protecting them. It's obvious: digital records have no physical weight, and can be mislaid or stolen without removing the original, and it's easy to comprehend that such a loss could represent an enormous amount of information. This isn't the way it's always been, though, and even today information in other formats needs to be protected.

Possibly the earliest forms of data and privacy protection come from the professions rather than legislation itself. Lawyer-client confidentiality (or legal professional privilege, as it's called in the UK), for instance, is believed to have begun as a sort of contract between a lawyer and their client many decades (and possibly centuries) before it entered into law itself. It was introduced as a way of ensuring that a lawyer could adequately represent their clients' interests without the client fearing legal repercussions.

Equally, the keeping of medical records and a doctor's confidentiality were established decades ago, and, while a court could force those records to be handed over, the medical profession otherwise kept them relatively safe. Once again, this was

something that the profession handled long before the law moved to codify the practice.

Under these practices, specific silos of personal information were protected according to the interests of the business: if a profession could see the business value in protecting information, it was protected. This has had to change, however, as record keeping shifted from paper to electronics, and as the methods for manipulating even small elements of personal information have become more powerful, which puts all this information at risk because it now has a distinct value. Political campaigns, as a *reasonably* ethical example, have used increasing volumes of data to better target key demographics, define policy, manage candidates' image and so on. On the other end of the scale, identity theft has become a significant problem that has only become a greater threat with the greater volume of information that is available.

With regard to the situation in Europe, one of the first legal protections for personal information was codified in Article 8 of the European Convention on Human Rights (ECHR) in 1953. This wasn't in the form that we might expect to see privacy legislation today, but it provides the foundation for modern European privacy laws. Article 8 reads:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except

> such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

There is some criticism that this is an unnecessarily open-ended provision, as unscrupulous people could interpret it in order to restrict the rights of the people (through the application of laws to circumvent some of the protections, which are permitted), to place undue regulatory burden on third parties (through the application of laws that use equally broad language) and to limit the power of the state to pursue justice (because the European Court of Human Rights will almost always find against any laws that could violate the right to privacy[1]). Obviously, these are conflicting opinions, so it has remained generally balanced in the interests of all parties.

Regardless of its interpretation, the ECHR's legacy with regard to the right to privacy has carried down

[1] Especially if those laws seem to contravene or impinge on other articles in the ECHR, such as Article 10 – the right to freedom of expression and information.

through the decades into our modern legal landscape.

In 1981, the Council of Europe established standards to ensure the free flow of information throughout EU member countries without infringing personal privacy. The convention that enacted these standards – the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – was developed in response to the burgeoning use of computers to store and process personal data. The minimum standards it set then became the basis of the first round of privacy laws across Europe.

As we know, however, the power and availability of computers exploded during the 80s and 90s, and by 1995 more than a million people in the UK were regularly using the Internet. Furthermore, over the years since the Convention was applied, EU Member States' data protection laws had diverged, which began impeding the flow of data through the European Union – and thus impeding business. It was quite clear that existing data protection regimes across Europe were inadequate to support Articles 8 and 10 of the ECHR, and so the Data Protection Directive (DPD) was enacted in 1995.

The DPD required EU member states to respond by developing laws of their own to meet new, more rigorous minimum standards, and taking into account the significantly more powerful, readily available and affordable computers and electronic devices. It was functionally a 'reset' for data protection, obliging all member states to align with

it and thereby improve protections for personal data, while simultaneously reducing the burdens impeding the free flow of data through the Union.

The DPD also established rules for the transport of personal data outside of the EU. This was most famously reflected in the US-EU Safe Harbor framework, which asserted that US data protection laws were sufficient for the protection of personal data originating in the EU, as long as the recipient in the US observed a set of self-policed data protection principles. While this framework was found to be in breach of the DPD in 2015, it did support considerable business activity for 15 years.

The UK's Data Protection Act of 1998 was the British law that enacted the requirements of the DPD and was founded on eight principles. These principles clearly laid out the general aims of the Act, which made it reasonably simple to determine whether an organisation was meeting its obligations. There was some complexity in the broader Act, however, and repeated amendments and updates meant that it continued to grow and become more unwieldy as time went on.

In Germany, meanwhile, data protection was primarily regulated through the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), supported by a number of sector-specific regulations at varying levels of federal and state government. Because it also sought to meet the requirements of the DPD, this law was broadly comparable to the UK's DPA, but with considerable differences in the detail.

France's Data Protection Act (Loi informatique et libertés, LIL) dates back to 1978, predating many other national data protection laws and covering the lifespan of both the EU convention and the DPD. Rather than developing new laws in response to those pressures from the European Union, the French legislature instead opted to amend its existing law. Despite this, the LIL we see today is surprisingly concise.

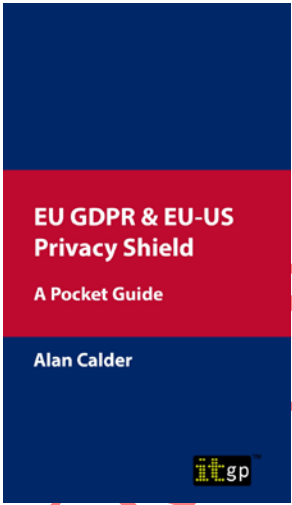
Across the EU, other, similar legislation was enacted, but through a combination of time and varying national interests, no two national laws were sufficiently similar for an organisation to simultaneously be compliant in its home country and across all the other EU member states. That is, the free flow of information was effectively inhibited because the different regulatory environments clashed on matters of detail, requiring businesses and governments alike to arrange processes specific to an increasing array of scenarios. It is this, in conjunction with the steady march of technological progress that created the environment into which the General Data Protection Regulation was born.

That the solution is a regulation rather than a directive (as the DPD was) is worthy of discussion. Within EU law, a directive sets out minimum conditions or requirements but does not pass any specific measures in itself. That is, an individual or organisation is not required to be in compliance with a directive. Rather, each Member State is obliged to pass its own laws in order to meet the

minimum requirements of the directive, and this is what organisations and individuals have to comply with.

A regulation, meanwhile, is functionally a law and enters into force across the Union simultaneously. No Member State needs to pass additional laws in order to bring it into force, and it is not dependent on the interpretation of the local government, courts or authorities. Because of the legal weight of a regulation, they typically take much longer to pass through the legislative process, but they also ensure greater consistency across the Union.

The GDPR had a particularly long and arduous journey on its way to approval by the European Parliament and Council, and it was not without controversy. Over the several years it spent in committee stages, being written and rewritten – it had thousands of amendments proposed, pushing for more or less data privacy – the more contentious points were gradually eradicated, however.



Buy your copy today!

www.itgovernanceusa.com/shop/Product/eu-gdpr-eu-us-privacy-shield-a-pocket-guide