4 Tips to Prepare for the European General Data Protection Regulation

Get ready for a wild ride…

According to *IAPP-EY Annual Privacy Governance Report 2016*, "For privacy and data protection professionals, 2017 may prove to be a watershed year. The leading change agent is the ramp up in preparations for the European Union's new General Data Protection Regulation [GDPR], which enters into force in May 2018 to replace the EU Data Protection Directive…Together with the challenges brought by the invalidation of the Safe Harbor framework and entry into force of the new Privacy Shield, all eyes will be on Europe."

Until recently, the protection and security of information on identifiable individuals had taken a relatively low profile. Most countries, regions and states have data protection legislation but they vary considerably in the level of protection decreed. Exposure of personal information or data breaches were relatively rare, and state surveillance of such information was generally covert and not acknowledged by governments.

All of this has changed quite dramatically in the last few years. The amount of personal data stored by companies and governments has soared, and the value of that data has multiplied as more and more personal business is transacted on the internet. Identity theft has become a major new crime. In addition to the disruption to business and the impact on customer loyalty that data breaches create, many jurisdictions are looking to bring their data protection legislation into line with the new, internet-based world – although unfortunately, not in line with each other.

A new set of European rules and standards related to privacy and data protection has set in motion a mad compliance scramble not for European companies, *but for any company doing business in Europe or with European customers*.

So what do you need to know to start thinking about the implications of these regulations especially if you are a company from outside Europe?

Here are 4 tips to get started.

> A reminder: This does NOT constitute legal advice! See point 1 in the recommendations below.

1 Understand that European data protection legislation is nothing new.

While Americans often tend to view privacy as a *consumer* right, tradeable for convenience, many Europeans view it as a fundamental human right, and not tradeable. This approach was reflected in the European legislation on data protection that has been in place since 1995.

Non-European companies utilized "Safe Harbor" provisions to comply with the original data protection legislation. Per Wikipedia,

According to the original Data Protection Directive, companies operating in the European Union were not permitted to send personal data to "third countries" outside the European Economic Area, unless they guaranteed adequate levels of protection, "the data subject himself agreed to the transfer" or "if Binding corporate rules or Standard Contractual Clauses had been authorized." The latter meant that privacy protection could be at an organizational level, where a multinational organization produces and documents its internal controls on personal data or they can be at the level of a country if its laws are considered to offer protection equal to the EU. Safe Harbor Privacy Principles were developed between 1998-2000 and in July 2000, the European Commission (EC) decided that US companies complying with the principles and registering their certification that they met the EU requirements, the so-called "safe harbor scheme," were allowed to transfer data from the EU to the US. This is referred to as the Safe Harbor Decision.

2 Understand that the new regulations truly are a new game.

After four years in the works, in April of 2016 the European Parliament approved new data protection rules establishing a uniform level of data protection and set of standards for data use for policing and judicial purposes, across the European Union: "The **General Data Protection Regulation** [GDPR] will enable people to better control their personal data. At the same time modernized and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market by cutting red tape and benefiting from reinforced consumer trust."

The regulation was adopted on 27 April 2016. It enters into application 25 May 2018 after a two-year transition period and, unlike a Directive *it does not require any enabling legislation to be passed by governments.*

The new regulation puts in place a series of new and expanded requirements tied to the following areas. It is important to note that "the Regulation also applies to organizations based outside the European Union if they process personal data of EU residents."

- Single set of rules
- Responsibility and accountability
- Consent
- Data Protection Officer
- Data breaches
- Sanctions
- Right to erasure
- Data portability

According to Wikipedia, the following significant sanctions can be imposed:

- a warning in writing in cases of first and non-intentional non-compliance
- regular periodic data protection audits
- a fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 4)
- a fine up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83, Paragraph 5 & 6)

3 Don't count on the old Safe Harbor provisions.

The international Safe Harbor Privacy Principles were overturned on October 24, 2015 by the European Court of Justice after a customer complained that his Facebook data was insufficiently protected. The Safe Harbor provisions

AIIM
1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910
+1 301.587.8202
www.aiim.org

AIIM Europe
Broomhall Business Centre, Broomhall Lane,
Worcester, WR5 2NT, UK
+44 (0)1905 727600
www.aiim.eu

were replaced by what is known as Privacy Shield provisions.

Per *IAPP-EY Annual Privacy Governance Report 2016,* "many companies remain wary of Privacy Shield and are still weighing other transfer compliance options. This is especially true of small companies for whom GDPR compliance presents a formidable challenge. While 50 percent of all companies that transferred personal data between the EU and U.S. in the past used Safe Harbor, just 34 percent say they intend to use Privacy Shield in the future. At the same time, more than 80 percent of companies rely on pre-approved standard contractual clauses, which are currently under legal attack in the Court of Justice of the European Union."

4 Start immediately to get your own house in order.

Here are some recommendations as you think through the implications of the GDPR:

1. Get legal and technical counsel immediately. May 2018 will be here before you know it.
2. You should have a clear audit of what personally identifiable information (PII) you hold on employees, customers or citizens, and whether it constitutes sensitive personal data. You also need to know in which countries those persons reside, as this will affect which legislation might apply.
3. Ensure that your Information Governance policies specifically deal with PII, and how it is to be secured against loss or exposure to those not authorized to see it. Pay particular regard to laptops, USB sticks and mobile devices.
4. Review the risks posed by this information should it be lost or exposed, and make senior management aware of the potential consequences of a breach, including those involving internal staff or caused by general negligence.
5. If your audit shows that PII is being stored or handled by a cloud services provider, or a document process outsourcer, review the terms of your contract with the provider to ensure that they are taking joint responsibility for its security.
6. Ensure that you are familiar with your obligations under local laws to protect PII, and any that might apply in the country of origin of the data subject. There may also be specific regulations that apply to your industry.
7. Adopt a privacy-by-design approach, and look to encrypt as much of your content as possible. At the very least, ensure that credit-card details and email addresses are encrypted.
8. If you hold information on European citizens, be aware of the need to ensure that European data protection standards apply wherever that information is stored, and the different ways that you achieve that. The same holds true for all countries and governments with regard to private information.

You might also be interested in…

6 Things You Need to Know About Emerging Markets and Information Management

Data Privacy – Living by the New Rules (an AIIM Industry Watch report)

AIIM
1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910
+1 301.587.8202
www.aiim.org

AIIM Europe
Broomhall Business Centre, Broomhall Lane,
Worcester, WR5 2NT, UK
+44 (0)1905 727600
www.aiim.eu