Data Privacy Detective Podcast – Episode 18 – How businesses outside the EU can comply with the GDPR

Apr 19, 2018

Categories:

Blogs
Podcast
Publications
Technology Blog

Authors:

Joseph J. Dehner

In prior podcasts we explored fundamentals of the General Data Protection Regulation of the European Union, including

- The GDPR's background and basic purposes
- How organizations outside the EU are affected by it
- The difference between controllers and processors of personal data
- The broad scope of personal data
- When processing of personal data is lawful
- Consent of data subjects and how to obtain it

Businesses inside the EU are actively working to bring their policies and procedures in line with the GDPR, with the benefit of many years of practice under the 1995 EU Directive that required EU countries to adopt laws based on a common background and similar principles to what becomes a directly binding regulation on May 25, 2018. For businesses beyond EU borders, how do they determine if GDPR's extraterritorial reach affects them and what should they do about it?

There's a flood of advice about this. You'll find guidance on the "5 steps to GDPR compliance," the 6 steps, the 7 steps, the 12 steps, etc. Much of comes from technology providers marketing solutions – to upgrade cybersecurity, to digitize, restrict and manage data use, flow and storage. These offerings can be helpful or even essential but can be costly and partial.

The first action is to do a data inventory. Does the business hold or have access to personal data that constitutes information that the GDPR protects? Article 3.2 limits the GDPR's extraterritorial application by saying that it applies to "the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union" in two instances: when the

processing is related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- the monitoring of their behavior as far as their behavior takes place within the Union.

This greatly restricts the outside reach of this part of the GDPR to non-EU businesses. Note that the wording does not limit application to EU "citizens" or EU "residents," but to any personal data of people (data subjects) "who are in the Union." Thus, personal data about people while they are present in the EU are potentially subject to GDPR's requirements.

Many businesses outside the EU collect and gather personal data about persons "in the Union." The data come in a variety of forms from a range of individuals, including customers, business chain personnel, employees, contractors and website browsers. If the data are processed for either of the two purposes stated in Article 3.2, the business is plainly subject to GDPR's express reach. If not, the business may still be subject to GDPR's reach for two reasons. First, controllers of personal data within the EU or non-EU controllers and processors subject to Article 3.2 must control how they transmit that data to third parties that become processors of the data. Second, Chapter V addresses transfers of personal data to third countries or international organizations. Articles 44-50 address this regardless of the purpose of the transfer and without any stated *de minimis* threshold.

Let's take an example. A U.S. headquarters of a multinational company has an EU-based subsidiary and receives information about potential hires from Europe. This is personal data about persons "in the Union." The U.S. parent will process that data in the U.S. when considering potential employees. Transfer of data from the EU subsidiary to the U.S. is captured by Article 44. It says that the transfer can occur only if the conditions of Chapter V are "complied with by the controller and processor, including for onward transfers" from the non-EU country. There are specific listed ways by which the transfer can be proper under the GDPR.

The first is if the EU makes an "adequacy decision" about the third country. The EU can determine that a non-EU country protects personal data adequately, meaning in a comparable manner to the GDPR. As of mid-April 2018, twelve jurisdictions have received this status – Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay – and the USA to the extent provided in the EU/U.S. Privacy Shield. The U.S. does not qualify without the Privacy Shield in light of the absence of a U.S. federal overarching personal data privacy protection law akin to the GDPR.

A U.S. business must look to one of the ways to comply with the GDPR to process EU personal data: binding corporate rules, standard clauses, an approved code of conduct or an approve certification mechanism – or joining the Privacy Shield.

Article 47 lists what **binding corporate rules** must provide. A U.S. business can adopt these for handling EU personal data and agree with its affiliated EU controller (or on its own) in basic compliance with the rules of the GDPR, including providing effective legal remedies for EU data subjects, as required by Article 46.1.

The EU has issued **standard data protection clauses** in multiple languages, including English, which give a non-EU business a second alternative – namely to adopt them formally as binding on the business. The exact language of these clauses must be adopted in full.

If neither of these choices is made, a non-EU business can look to a **Code of Conduct** or **Certification mechanism** under Articles 40 or 42. These provisions allow an industry sector association to develop group procedures about GDPR principles and procedures. This concept is new. It will take time for such codes and certifications to become available generally for businesses to use.

Absent one of these four approaches, a U.S. business can instead join the Privacy Shield. This is a governmental agreement that allows transfers of EU personal data to the U.S. for participants. Although it has been challenged in EU courts (and the prior Safe Harbor was rejected by the European Court of Justice), thousands of U.S. businesses have signed up for this before the GDPR comes into

effect, using this approach to be able to process EU personal data in conformance with GDPR. This Privacy Shield (which also addresses Swiss requirements) is the subject of the next podcast.

For more information, please contact Joe Dehner or any attorney in Frost Brown Todd's Privacy and Information Security Law Practice Group.

View the original article as a Frost Brown Todd Legal Update: Data Privacy Detective Podcast – Episode 18 – How businesses outside the EU can comply with the GDPR.

FBT Gibbons