Data Privacy Detective Podcast – Episode 21 – GDPR is here

Jun 01, 2018

Categories:

Blogs
Podcast
Publications
Technology Blog

Authors:

Joseph J. Dehner

I did Y2K audits as the 21st century approached. There were warnings that planes could fall from the skies, elevators could stop or drop a second after midnight of the new millennium, that whole systems could crash. Would carbon paper and the abacus return? But it was not the apocalypse. 1999 saw a binge of business buying of hardware and software, and the year 2000 began without a computing disaster.

GDPR has been more like a wake-up call, augmented by headline news about Cambridge Analytica and massive database hacking leaks.

Multinational data businesses like Google and Facebook poured resources into GDPR compliance. They had no choice, except to consider whether they should treat Europeans differently from Americans and others about their personal data. Nonetheless, at 12:48 a.m. on May 26, these two tech giants were sued in Brussels by the nonprofit organization of Max Schrems, claiming they violate GDPR by not offering EU customers a real choice for how their personal data are used.

Most coverage about GDPR is about titanic battles of tech giants whose business models are based on monetizing customer data. My spyglass turns to a different subject: How did SMEs in the United States deal with GDPR? The clear majority of them do not sell personal data of Europeans, but instead collect and use it for ordinary business purposes, such as marketing goods and services, employing personnel, collecting payment and other processing that has nothing to do with surreptitious use of such personal information beyond the obvious.

Leading up to May 25

Many SMEs selling goods and services into Europe or with European affiliates explored many for the first time what EU personal data

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

they hold in the U.S. They found that HR held personal data about Europeans seeking employment, expats working a few years in the States, and expense reimbursement data. Business units had business cards gathered at trade shows, personal contact details for customers and suppliers. Some found data from focus groups or customer outreach that include information as simple as email or postal addresses or as sensitive as health and bank account details. What then?

A next step was to ask if they had to register with the EU because they hold and process such information about "persons in the Union," as GDPR phrases it. They read conflicting commentary about whether a business that does not purposely sell goods and services in the EU (companies that sell from a U.S.-centric website that only take orders in U.S. dollars and do not advertise in multiple languages) has to appoint a Data Privacy Officer and register with Data Protection Authorities in one or more EU countries. Most concluded they did not have to do so, but some commentators warned how access to, or use of, personal data of "persons in the Union" could subject them to liability if they do nothing.

Some U.S. SMEs with affiliates or outlets in the EU appointed the EU entity as the "controller" of the enterprise's EU personal data and created controller/processor agreements with the U.S. entity designated as the "processor." Joint controller and joint processor agreements were fashioned to fit differing circumstances, and enterprises decided where in the EU an affiliate would register. Multi-entity companies allocated risk and responsibility among their affiliates.

Many U.S. SMEs upgraded their privacy notices and policies posted on websites to embrace basic aspects of GDPR, while maintaining an opt-out approach for use of personal data. The opt-out approach is used by most U.S. businesses beyond fintech and medtech – "Please notify us if you don't want us to use your data as we describe – otherwise we can use it for purposes we have told you about." Some elected to adopt the standard commercial clauses of the GDPR that promise equivalent protection of EU personal data to what is required of European businesses. Others decided that promising basic GDPR protections without adopting

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

the full range of commitments contained in the standard commercial clauses is adequate.

Taking action

While no definitive survey has been made since May 25, 2018, it is the Data Privacy Detective's anecdotal conclusion that U.S. SMEs reacted to GDPR in various ways, in the following order of magnitude:

- Most that lack a focused effort on EU sales of goods and services (those that do not use multiple languages or have sales offices in the EU) have generally ignored GDPR and assume it does not affect them.
- Many revised their web-based privacy policies to embrace the essential elements of GDPR – fair notice of how personal data will be kept and used, ability of persons to correct and request deletion of data, heightened cybersecurity around sensitive data, etc. Some with affiliates in the EU have used inter-entity agreements to deal with EU registration and "Controller/Processor" allocation of responsibility and risk.

A large number of companies in this category decided to send emails to databases, such as "We would hate to lose you" or "If you want to continue to receive our newsletter, please click yes in reply." A blizzard of such emails hit in late May. The irony is that if we, as many of us did, simply moved on without clicking anything, those that sent the emails are now forced to delete the contacts or face the risk of keeping persons in their database who did not grant express consent. In many cases, express consent was not required under GDPR because the businesses had a legitimate interest in having the contact information and using it for limited legitimate purposes.

- A lesser number joined the U.S./EU Privacy Shield, which means upgrading policies and systems to the requirements of that program and subjecting themselves to U.S. agencies for enforcement if they declare they are treating personal data of EU persons in a compliant way, but fail to do so in practice.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

- A very few decided to stop selling to EU customers. Some U.S. local newspaper publishers, for example, halted paid subscriptions from EU residents. The Washington Post took a different approach – offering a "premium E.U. subscription" that costs a third more than a regular U.S. subscription and is ad- and tracking-free.
- The final type of response from U.S. SMEs came from those that asked why they should balkanize personal data. These companies began to think of a global personal data protection policy that embraces basic principles expressed not only in GDPR, and the reasons a business should be concerned about personal data privacy in the first place.

The U.S. – EU special relation

The U.S. and EU have the world's largest trading relationship. This is often ignored because the EU is not a country and trade figures are based on country statistics. If U.S.-EU trade were reported the way U.S./China or U.S./Canada trade are reported, the trade figures would reveal the U.S./EU relationship as by far the single largest market in the world. The U.S. and EU recognized the importance of this relationship by creating the U.S./EU Privacy Shield, which allows a U.S. business to receive from EU sources personal data without requiring the U.S. business to register in the EU, while agreeing to comply with basic requirements for the protection of personal data of EU persons. As of May 25, 2018, 3,063 U.S. business had joined the Privacy Shield, a trickle of usage.

Global standards – or – self-regulation on the horizon?

Businesses with an increasingly global nature began to consider that carving up the world simply to meet differing individual country rules would result in a hodgepodge of policies treating different human beings differently. What if a person is a dual citizen? What if a U.S. citizen travels or lives in Europe? From a business standpoint it is a bit ridiculous to treat the personal data of EU persons differently from Swiss, U.S., Canadian or Chinese persons. And if a

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

business tried to do this, how it would work as a practical matter? How can data be segregated by national origin?

Data are not like goods. Goods require a customs form and payment of applicable duty before being allowed entry across borders. Data are like fish. Fish don't declare citizenship or where their personal information arose. Neither do data. China's May 1, 2018, effort to declare tight standards on when certain personal data may leave China's borders is unlikely to work, just as the EU's effort since 1995 to restrict transfers of data outside of the EU failed. The GDPR changed the EU approach to recognize that the cloud is here to stay. GDPR shifted the focus to how EU persons' data will be processed rather than where the data exist or are stored and processed.

The Data Privacy Detective sees and foresees no serious effort by the governments of the world to forge an international agreement or global standards on how personal information of the world's people should be collected and used, and more importantly – not misused. Instead, it is more likely that businesses will – aside from what law requires – find ways to protect the personal data of the individuals they encounter and on whom they depend for services and revenue. Those businesses that surprise their customers by using data in unexpected ways or misuse the data will face lawsuits and penalties – and more fundamentally will need to reassess their revenue models or suffer severe reputational damage when a data breach occurs or their secret misuses of data are revealed.

It is unlikely that personal data will become part of the "trade war" brewing, though this is not impossible. If businesses follow the model of certain U.S. newspaper publishers – abandoning whole markets because of territorial personal data laws – this could herald a distressing era of data balkanization. This would play into the hands of protectionist and tribal forces that aim to erect walls around data flows. This would interfere with human freedom. It would stifle human creativity and the spread of knowledge.

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

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons