



Jul 30, 2018

Categories:

[Blogs](#)

[Podcast](#)

[Publications](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

Data Privacy Detective Podcast – Episode 25 – Europe’s GDPR – Representatives and Data Protection Officers

The European Union’s General Data Protection Regulation (GDPR), effective as of May 25, 2018, requires businesses outside the EU that are subject to GDPR to appoint a “representative” in a member state. It further stipulates that many EU businesses, as well as certain non-EU businesses, must appoint a Data Protection Officer in the EU to consult on and monitor data privacy matters.

According to the GDPR, a “representative” is just what the word implies – a natural person or a legal entity that represents a business within the EU. Importantly, Article 27 requires the representative to be “established in one of the Member States.” So, for example, a U.S. law firm with no presence in the EU cannot be a U.S. business “representative” for the formal EU purpose, though it can provide advice to its clients about GDPR and other matters. By contrast, a designated representative’s role is largely to communicate with data protection authorities, data subjects, and others in the EU when there is a question or issue about the manner in which personal data are collected and processed, as directed by the appointing business. A person or entity appointed as a GDPR representative should, of course, be expert, knowledgeable and responsive. Article 27(5) says that when a controller or processor designates a representative for GDPR purposes, this is “without prejudice to legal actions which could be initiated against the controller or the processor themselves.” With a registered representative in place in a member state, a non-EU business will have a point of contact for EU authorities. A representative for a business that operates throughout the EU can form a network with other persons or firms throughout the EU, so that local language and contact can be available immediately or as needed.

A Data Protection Officer (DPO), by contrast, must be an individual, not an entity. A DPO in the EU has a highly defined and quasi-independent role compared with a business “representative.” A DPO for a data controller is a person who should be involved in the entire range of data privacy issues. This includes consultation with data protection authorities, direction of joint controllers and processors of personal data, and communications with data subjects about their rights and the processing and handling of their data, while also monitoring compliance with GDPR and member state rules and cooperating with supervisory authorities. To carry out their responsibilities, DPOs must have sufficient independence from the business that appoints them, requiring the right balance, at once, between their responsibilities to the business’ board of directors, to local data protection authorities, and to data subjects. Because this can be an area of conflicting interests, DPOs are protected against retaliation by the business for performing their tasks.

DPOs can, however, face personal civil or even criminal liability, though as a practical matter only in very limited circumstances. A DPO’s advice is not binding on the appointing business, but if there is disagreement over what a DPO advises a business to do, the business should justify in writing the reasons for not following its DPO’s advice, according to the Guidelines of the Article 29 Working Party (an advisory group within the EU that was replaced by the European Data Protection Board under GDPR).

Both the representative and DPO role may be outsourced by a company or staffed by an internal person. There are numerous companies currently advertising their services as GDPR representatives or for staffing DPO positions on an outsourced basis. Other firms offer DPO clouds, checklists, work aids, and training.

For more information, please contact [Joe Dehner](#) or any attorney in Frost Brown Todd’s [Privacy and Information Security Law industry Group](#).

To share your thoughts or questions about this or other Data Privacy Detective podcasts, send a message to info@thedataprivacydetective.com. And remember – protecting

your personal information begins with you.

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