Frost Brown Todd's Data Privacy Detective series delves into information security and safeguarding data privacy. **PrivacyRules** has cooperated with the Privacy and Information Security Law practice at **Frost Brown Todd** for this specific podcast.

The podcasts are accessible here:

https://www.frostbrowntodd.com/services-practices-Privacy-and-Information-Security-Law.html

GDPR and non-EU Businesses

DPO's and Representatives – Necessary? Which? Both?

Businesses not located in the European Union have tried to understand whether the General Data Protection Regulation (GDPR), which became law on May 25, 2018, applies to them. And if it does, or if it might, one of the puzzles has been whether a non-EU business needs to appoint a natural person or legal entity to be its "representative" or a natural person to be its "Data Protection Officer" for dealing with EU and its Member States' Data Protection Authorities (DPAs). This podcast focuses on that question.

Let's start with definitions. Article 4(17) says:

> 17. 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation."

Article 27 is about "**Representatives of controllers or processors not established in the Union.**" (As discussed in an earlier podcast episode of the Data Privacy Detective series, "controllers" are companies or individuals that collect, control and are directly responsible for keeping and using personal information in either digital or hardcopy form. "Processors," on the other hand, are individuals or companies that process data at a controller's direction.)

The rest of Article 27 makes clear that "representative" for this purpose relates to controllers or processors that exist outside the EU but are directly liable under the GDPR under Article 3(2). This Article applies on its face to "a controller or a processor not established in the Union" in two instances: when the "processing activities of personal data of data subjects who are in the Union" relate to either:

"a. 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

b. the monitoring of their behaviour as far as their behaviour takes place within the Union."

A little noticed provision in Article 3(3) adds that the GDPR also applies to "processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law." This is a potential gaping loophole to expand the extraterritorial application of GDPR beyond the two instances of 3(2).

The Role of the Representative

These Articles make clear that the word "representative" refers to a natural person or legal entity established in the Union that represents a business that is established outside the EU.

An EU representative has a series of tasks covered by different Articles and Recitals:

1. Art. 27 (4) and Recital 80 establish a duty to answer any DPA's query or data subject's request for the purpose of ensuring compliance.

2. Recital 80 mandates a representative to manage enforcement proceedings for non-compliance.

3. Article 30 (1) requires a representative to maintain a record of the processing activities and to make such records accessible under request.

In summary, a representative acts as a controller's or a processor's point of contact for the local authorities and the data subjects. The representative acts for and at the direction of the controller or processor.

Responsibilities of the Data Protection Officer

A "Data Protection Officer" (DPO) is not defined in the definitions list of Article 4. DPO has its own chapter – Articles 37-39. Article 37(1) lists three explicit instances establishing that controller and processor "shall designate" a DPO when:

> "a. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
>
> b. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
>
> c. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10."

Article 37(4) adds that EU or Member State law may require other controllers and processors to appoint a DPO, a section that awaits further action over time to expand those entities that must appoint a DPO.

For businesses outside the EU, they need only consider subsections b and c at this time. These subsections are more limited in scope than Article 3(2), because the "core activities" of a controller or processor must be those defined in article 37(1) or no appointment and registration of a DPO is required of a non-EU controller or processor.

If a DPO is appointed, the DPO's tasks are defined in Article 39(1) as follows:

> "a. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
>
> b. to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c. to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

d. to cooperate with the supervisory authority;

e. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter."

Unlike the representative, the DPO has certain powers that provide a certain level of independence from the controller or processor. Article 38.3 says that the DPO "shall not be dismissed or penalised by the controller or the processor for performing his tasks." This instructs businesses that they may not retaliate against a DPO they appoint if this DPO does what the GDPR requires, despite the wishes or direction of the business.

Determining the Requirements for Non-EU Businesses

What does this mean for non-EU businesses that possess and use personal data of EU persons? When must they appoint a representative or a DPO?

There would be little point under GDPR to define "representative" as discussed above if a DPO were also required in all instances under Article 3(2). A sensible reading of Article 37(1) is that unless a non-EU business has "core activities" that involve monitoring the behavior of EU persons or processing certain sensitive data on a large scale, it is not required to register and appoint a DPO. The vast majority of non-EU businesses that handle some level of EU persons' data are companies selling goods or services into the EU as their core activity. They should appoint a "representative" for this purpose, but not a DPO. The limited number of non-EU businesses that as a core activity process EU persons' data through "regular systematic monitoring" or deal in the special cases addressed by Article 9 (special categories of personal data such as racial or ethnic origin) or Article 10 (criminal convictions and offences) should appoint a DPO.

Potential Conflicts of Interest

Considering this, may a representative and a DPO be the same person?

One DPA that has offered an answer is the Irish Data Protection Commissioner. This DPA has noticed that even if there are no legal prohibitions for an organization to hire one person for both, this may lead to a conflict of interest:

- A conflict may arise when the DPO carries out tasks contrary to instructions given by the controller or processor in the representative role. In this case, while a representative must respect its mandate, the DPO must remain somewhat independent.

- The DPO is also the person appointed for receiving concerns from employees. His/her autonomy cannot be undermined by subjecting its activities to the business' sole discretion because that could lead to violations of the confidentiality principle.

- When a DPA carries out enforcement activities, it should dialogue with the DPO as an independent official, differently from representatives who can be "addressed in addition or instead of" the controller or processor.

Finally, it is a controller's or processor's responsibility to ensure that the DPO does not take on other tasks that may result in a conflict. This explains why the Irish DPA recommends avoiding overlap in the two roles.

For more information, please contact Joe Dehner (jdehner@fbtlaw.com) or any attorney in Frost Brown Todd's Privacy and Information Security Law Practice Group at: https://www.frostbrowntodd.com/services-practices-Privacy-and-Information-Security-Law.html