Is it a good idea to appoint your Contracted Research Organization as your Data Protection Representative ?

There is sometimes confusion between the role of the Data Protection Representative and the Legal Representative of the Sponsor in the Union. It may be worth recalling that there is a distinction between these two functions encountered in the context of clinical studies. The designation of a Data Protection Representative is an obligation that comes from the General Data Protection Regulation[1] while that of a Legal Representative is an obligation imposed by the Clinical Trials Regulation[2].

Non-EU-based controllers or processors can be subject to the European General Data Protection Regulation (GDPR) because they offer products or services to data subjects in an EU country or monitor the behavior of natural persons located in the EU (as long as their behavior takes place in the EU). Some of them can have the obligation to designate a Data Protection Representative in the Union[3], failure to comply with this obligation would be a breach of the Regulation.

The Data Protection Representative (DPR) appointed must be a natural or legal person established in one of the EU Member States, the DPR represents the controller or processor with regard to their respective obligations under the GDPR[4].

As clarified by Recital 80, the Data Protection Representative should be explicitly designated by a written mandate of the controller or of the processor to act on his behalf with regard to its obligations under the Regulation. The Data Protection Representative should perform its tasks according to the mandate received from the controller or processor. Therefore, the written agreement should state the obligations of the Data Protection Representative and the controller or processor. An oral appointment of the representative is excluded.

The fact that the Data Protection Representative represents the controller or the processor with regard to their GDPR obligations involves different tasks for the DPR.

First, the Data Protection Representative must be a point of contact for the data subjects. That is why the controller must inform the data subjects about the identity and contact details of the Data Protection Representative. The DPR is not himself responsible for complying with the data subjects' rights, but he has to facilitate the communication between the data subjects and the controller or processor he represents. The purpose is to ensure the effective exercise of the data subjects' rights.

Second, the obligation imposed by the GDPR to maintain a record of processing activities is shared between the controller or the processor and its Data Protection Representative. A non-EU-based controller or processor must make all accurate and updated information available to its Data Protection Representative in order for the DPR to keep the record up to date and make it available.

Third, the Data Protection Representative has to act as point of contact for the supervisory authorities. He must cooperate with regard to any action taken to ensure compliance with the GDPR. For any matter concerning the

[1] *Article 27 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).*

[2] *Article 74 of the Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.*

[3] *This obligation does not apply to processing which is occasional, does not include, on a large scale, processing of sensitive data or data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons.*

[4] *Article 4 (17) of the GDPR.*

compliance obligations of a non-EU-based controller or processor, the authority will contact the Data Protection Representative. The DPR's role is to facilitate any informational or procedural exchange with the non-EU-based controller or processor and the supervisory authority.

In addition, we can imagine that the mandate confers more tasks on the DPR.

Various entities can act as your Data Protection Representative, but it is important to choose a premium specialized service provider and not simply an additional regulatory service supplier. Your Data Protection Representative must have an expert knowledge of the GDPR because he must know what the Regulation implies with regard to the rights of the data subjects and the powers of the supervisory authorities, to name just a few. Moreover, your DPR must be specialized and have knowledge of the data protection laws of the Member States if the mandate he is given is to take other actions concerning the controller or processor's compliance. Above all, having a DPR who only provides services related to GDPR ensures his availability which is essential in order to enable data subjects and supervisory authorities to establish contact easily with the non-EU-based controller or processor.

As the DPR is the point of contact for EU data protection authorities and, in order to facilitate the exchange of information with the authorities, the DPR may hold copies of the data controller/processor's documents demonstrating their compliance with the GDPR (i.e. training, gap analysis, memorandums for the board, data transfers clauses, contracts with the sub-contractors, assessment of the services providers or any document related the internal implementation of the GDPR) and shall make these available to the EU data protection authorities if requested. Such information is confidential, and it is not recommended to mix these responsibilities with other additional operational activities. Most importantly, appointing a Data Protection Representative that also has operational responsibilities in some processing activities, like a CRO or any other processor may result in disclosure of information that it is not supposed to receive, such the contracts you have with other services providers.

Recital 80 also clarifies that the Data Protection Representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor. Actually, behind the notion of "Data Protection Representative", the idea is to ensure enforcement of the GDPR against non-EU-based controllers or processors. Then, it is possible for enforcers to initiate enforcement action against a Data Protection Representative essentially identical to those against controllers or processors. Similarly, the DPR could be fined administratively, be subject to penalties or be held liable.

Given the possible conflict of obligation and interests in cases of enforcement proceedings, the European Data Protection Board (EDPB) does not consider the function of a data controller representative in the Union as compatible with the role of data processor for that same data controller[5].

[5] *European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018, page 21.*

Let's illustrate this with an example:

If a supervisory authority determines that the security measures implemented by one of your data processors are not sufficient, the authority will inform this data processor that it is required to adapt its security measures; the data processor will have to implement appropriate security measures. As a data controller, you are obliged to work with compliant data processors. The DPR of the controller has the obligation to ensure that its controller complies with the GDPR. A Data Protection Representative can be held liable if its controller does not comply with the GDPR, this will be the case if the controller uses a non-compliant processor. Given the risk of fines, the DPR will never say that the appropriate security measures are not in place at the processor's premises.

IN CONCLUSION, the role of Data Protection Representative is critical for all non-EU organizations that conduct data processing activities in the EU. The Data Protection Representative is the single point of contact for authorities in case of inspection. In this occasion, it needs to address the questions adequately to avoid any risks of fines and penalties. Its personnel must be trained to face the authorities questions and requests.

Since the Data Protection Representative may become aware of your internal documents and due to the fact that there is a risk of conflict of obligation and interests in cases of enforcement proceedings; we do not advise you to appoint one of your data processor, including your CRO, as your Data Protection Representative.

Sources:

- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).*
- *Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.*
- *European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018.*

AUTHORS

Xavier GOBERT,
Data Protection Manager, CEO at MyData-TRUST

Benjamine BOMBECK,
Data Protection Lawyer at MyData-TRUST