IITR Cert GmbH
Frequently Asked Questions regarding
Art. 27 GDPR Representatives

We, IITR Cert GmbH, Marienplatz 2, 80331 Munich, Germany, provide education, certifications and various services relating to data protection law compliance. We have prepared this FAQ to help answer frequently asked questions from our clients and help our clients' legal counsel quickly understand the basic facts regarding our services. This FAQ does not contain or constitute a substitute for legal advice.

Question 1: Who has to designate a representative under Art. 27 GDPR?

Most companies outside the European Union (EU) have to designate a representative in the EU if they process personal data of EU residents and do not maintain an establishment in the EU (*e.g.*, a branch office).

Such companies are subject to the GDPR with respect to personal data of data subjects who are in the Union that they process relating to the monitoring of such data subjects' behavior or to the offering of goods or services directly to data subjects in the EU. It does not matter whether the company charges for such goods or services. Controllers and processors are covered.

Companies can claim an exception if their processing is occasional, does not include, on a large scale, processing of special categories of data (such as personal data relating to health, religion, etc.) and is unlikely to result in privacy intrusions.

For example, a U.S. company without an establishment in the EU that sells products online to consumers in the EU has to comply, because it regularly collects personal data relating to sales of goods; if such a U.S. company uses a service provider to process payments or provide shopping cart functionality, such company can also be covered as a "processor." On the other hand, a U.S. company that provides a software-as-a-service solution to EU-based manufacturers would likely not be covered, because the U.S. company does not offer goods or services to data subjects (only to companies), even if it will likely receive and process some personal data (e.g., contact information of the EU corporate customers' employees). U.S. companies that maintain subsidiaries in the EU may be covered to the extent they offer services directly to employees of their EU subsidiaries, unless the processing of personal data from the EU remains occasional.

Question 2: Does the representative have to be a person or can companies appoint other companies?

Companies can appoint individuals or other companies.

Question 3: Where must or should the representative be established or reside?

Companies must designate a representative anywhere in the Union where relevant data subjects reside (i.e., all over the EU for most websites, mobile apps and other online services). Art. 27(3) GDPR does not prescribe a particular member state.

Question 4: What role does the representative have under Art. 27 GDPR?

The designated representative

- represents the non-EU based company with respect to obligations under the GDPR, pursuant to Art. 4(17) GDPR;
- shall be identified in privacy notices of the non-EU based company pursuant to Art. 13(1)(a) and 14(1)(a) GDPR;
- be addressed in addition to or instead of the non-EU based company, in particular, with respect to communications with supervisory authorities and data subjects, on all issues related to data processing, for the purposes of ensuring compliance with the GDPR, pursuant to Art. 27(4) GDPR
- maintains records of processing activities for the non-EU based company pursuant to Art. 30 GDPR (which shall prepare and provide such records to the representative, and
- cooperate with the supervisory authority pursuant to Art. 31 GDPR on request.

Question 5: Is the representative role under Art. 27 GDPR similar to the role of a data protection officer under Art. 37-39 GDPR?

No, the roles, tasks, functions and requirements are quite different.

The data protection officer functions as a long arm of a data protection authority within a company to foster a compliance culture. The designated representative acts more like a local mailbox.

Companies without an establishment in the EU are required under Art. 27 GDPR to designate a representative in the EU so data protection authorities can reach and sanction them easier and with less jurisdictional complications. The representative keeps records of processing activities and is available to receive inquiries and complaints; it has no other duties.

Companies are required to appoint a data protection officer under Art. 37(1) GDPR if the nature of data processing creates particular risks (e.g., processing by a public authority; core activities require regular and systematic monitoring of data subjects on a large scale; core activities consist of processing on a large scale of special categories of data). Companies within and outside the EU have to appoint data protection officers (but only non-EU based companies have to appoint representatives). Like a representative under Art. 27 GDPR, the data protection officer also acts as a contact point under Art. 39(1)(e) GDPR. But, the data protection officer becomes more involved in consultations with data protection authorities (whereas the representative can merely forward inquiries to the foreign controller or processor) and the data protection officer also advises, informs and monitors compliance. Per Art. 38(3) GDPR, a data protection officer acts independently and not subject to instructions from the company. A representative, on the other hand, is subject to a mandate and instructions from the company, per Art. 27(4) GDPR.

Question 6: Can the same person or company serve as representative under Art. 27 GDPR and data protection officer under Art. 37-39 GDPR?

Yes.

Question 7: Can the representative be held responsible for violations of the GDPR?

The GDPR does not expressly define responsibilities or liabilities for an authorized representative in its legally binding, operative articles. But, the explanatory, non-binding recital 81 of the GDPR notes that the "designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor."

Question 8: Do companies that are based in the EU have to appoint a representative under Art. 27 GDPR?

No.

Question 9: Can non-EU based companies appoint their corporate subsidiaries or affiliates in the EU as representative under Art. 27 GDPR?

Yes.

Question 10: Can a company appoint their law firm, accounting firm, consultants, external data protection officer, or other service providers in the EU as a representative under Art. 27 GDPR?

Yes.

The GDPR does not expressly favor or disqualify any particular businesses or professional organizations. Most law firms would probably not accept such a designation, as it does not constitute "practice of law" and could create ethical problems for law firms and their clients, such as implied waivers of attorney-client privilege and conflicts of interest. The representative can be subjected to enforcement actions, which would not be covered by law firm malpractice insurance and create diverging interests between the attorney and its client. A law firm cannot as easily or quickly resign from representation of a client as may be necessary in the context of acting as a representative. The representative acts in a non-advisory role, which can destroy attorney-client privilege. If a law firm accepts an inquiry, this could constitute a waiver of objections to jurisdiction in the EU. Also, any professional services firm, including law firms and consulting firms, have incentives to provide additional advice and services to clients. This motivation could create conflicts of interest in the case of inquiries from authorities about compliance with data protection laws.

Another option would be to appoint an individual or firm that acts as external data protection officer. The fact that the legal representative is subject to a mandate and instructions whereas the data protection officer has to act independently could create conflicts and put an individual into a difficult position in the context of inquiries or enforcement actions from data protection authorities. But, if a company hires another specialized service provider company to provide an external data protection officer, then such a service provider company could assign different individuals to act as data protection officer and discharge representative obligations. Of course, not all companies that have to appoint a representative under Art. 27 GDPR are also subject to the requirement of appointment a data protection officer under Art. 37 GDPR. Also, the roles of a representative under Art. 27 GDPR and a data protection officer under Art. 37 GDPR are quite different, as noted above.

Dr. Sebastian Kraska
External Data Protection Officer
IAPP Country Leader Germany

Email: email@iitr.de

Tel: +49-89-18917360

Munich, May 30 2018