Source: IAPP.org - 12-06-2018 - All your art. 27 questions answered

According to Art. 27 of the European Union's General Data Protection Regulation, most companies outside the 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 (such as a branch, representative office or other unincorporated presence — which most companies try to avoid for tax reasons). With this requirement, the EU wants to increase the chances for data protection authorities to reach and sanction foreign companies that could otherwise be difficult to get ahold of. Companies frequently ask a number of questions regarding if and why this requirement applies to them and how they should comply. We'll try to answer them here:

What's new?

Some companies outside the EU were supposed to be subject to a similar requirement already before May 25, 2018. Yet, little is known or publicized to date about compliance by companies or standardized processes or enforcement attempts by data protection authorities. It seems that very few foreign companies have appointed representatives in the EU under Article 4 of Directive 95/46/EC, which has provided since 1995 that a "controller must designate a representative established in the territory of [a] Member State" where such controller "makes use of equipment, automated or otherwise, situated on the territory of the said Member State ..." Art. 3(2) and 27 of the GDPR expand the requirements to processors and discontinue the limiting condition of local equipment.

Who has to comply?

Most companies are covered if they are subject to the GDPR but do not maintain an establishment in the EU. Companies have to comply with the GDPR with respect to personal data that pertains to persons who are in the EU if they process such data relating to the monitoring of such persons' behavior or relating 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.

The term "establishment" is not defined, but Recital 22 notes: "Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect." In the context of international tax treaties, the term "permanent establishment" is defined to mean a fixed place of business, such as an office, branch or factory. Most companies try to avoid maintaining a permanent establishment in another country, because it can subject them to double taxation and accounting complexities. Instead, they incorporate a subsidiary, which is responsible for its own local tax filings and its own compliance under data protection laws.

For example, if a U.S. company incorporates a subsidiary company in the EU, such subsidiary company is fully subject to the GDPR and does not have to designate a representative under Art. 27 GDPR. Also, the U.S. company does not become subject to the designation requirement merely by incorporating a subsidiary in the EU. If the U.S. company conducts business with its subsidiary at arm's length — e.g., subject to a services or distribution agreement — then the EU subsidiary should not be considered as the U.S. company's own establishment. In that case, which is common in practice, the U.S. company would become subject to the requirement of designating a local representative under Art. 27 GDPR if the U.S. company collects personal data directly from persons in the EU relating to the offering of services, e.g., via a consumer-facing website.

Companies can claim an exception from Art. 27 if their processing is occasional, does not include, on a large scale, processing of special categories of data (such as personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, 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, the service provider can also be covered as a "processor."

On the other hand, a U.S. company that provides a cloud storage or software-as-a-service solution to EU-based manufacturers of industrial goods 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, e.g., in the context of equity grants or global training programs, unless the processing of personal data from the EU remains occasional.

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

The designated representative has a largely passive role: It shall be identified in privacy notices of the non-EU based company pursuant to Art. 13(1)(a) and 14(1)(a) and can 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). It represents the non-EU based company with respect to obligations under the GDPR, pursuant to Art. 4(17).

In terms of active duties, the representative shall maintain records of processing activities for the non-EU based company (which is the one that has to prepare and provide such records, pursuant to Art. 30). And, the local representative shall "cooperate" with the supervisory authority pursuant to Art. 31 on request.

How do the roles of a representative and data protection officer compare?

A representative under Art. 27 and a data protection officer under Art. 37 have quite different roles, tasks, functions and duties: A data protection officer functions as the long arm of a data protection authority within a company and is intended 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 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 active duties.

Also, companies are subject to designation requirements on different grounds regarding data protection officers and representatives: Companies are required to appoint a data protection officer under Art. 37(1) 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, the data protection officer also acts as a contact point under Art. 39(1)(e). 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), a data protection officer acts independently and is 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).

Can the representative be fined for violations of the GDPR?

Yes, but only for the representative's own violations of its own obligations.

The GDPR does not expressly define liabilities for an authorized representative in its legally binding, operative articles. Art. 27(5) merely clarifies that the foreign company remains subject to "legal actions" even if it designates a representative in the EU. 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."

In general, the purpose of fines is to punish wrongdoing. Therefore, the representative could not be fined under the GDPR unless the representative itself violates the GDPR. A representative is subject to only two

active obligations: cooperate with data protection authorities and maintain records of processing activities, which the company that appoints the representative has to prepare and provide to the representative. Even if a representative were to violate its own active duties (e.g., ignores inquiries from data protection authorities or fails to maintain records of processing activities), the GDPR does not specify administrative fines for violations committed by representatives. Art. 83(4)(a), for example, provides for an administrative fine if a controller or processor fails to designate a representative in violation of Art. 27 GDPR, but does not contemplate fines for representatives as such.

If the foreign company commits violations of the GDPR, the data protection authorities in the EU have to impose enforcement proceedings and fines against the foreign company. For administrative convenience, the EU authorities can address summons, orders and fines to the local representative, provided that it is the foreign company that is subject to the sanction. Courts and government agencies outside the EU do not typically cooperate with authorities in the EU regarding the enforcement of orders, injunctions, fines or other sanctions. Therefore, fines imposed under the GDPR against companies outside the EU will be difficult if not impossible to enforce outside the EU, contrary to commonly-made assumptions (see, for example, Tim Bell, "Is Article 27 the GDPR's 'hidden obligation'?", in The Privacy Advisor, May 3, 2018). As a consequence, data protection authorities in the EU can be expected to continue to apply pressure indirectly, e.g., on EU-based subsidiaries and customers of foreign companies, and, going forward, on local representatives of foreign companies.

A representative in the EU would be in a difficult position if data subjects, data protection authorities or others subject the representative to enforcement proceedings and the foreign company that designated the representative stops cooperating or accepting responsibility. In such situations, the representative would presumably have to resign effective immediately and end its involvement, which will add another violation to the tab of the foreign company (failure to designate a local representative, Art. 83(4)(a)). To prevent this, the foreign company should implement processes to respond to inquiries quickly, proactively and directly to data protection authorities, data subjects and others, to minimize stress on the local representative, which will, in most cases, not be able to contribute much to the resolution of a dispute in any event.

Whom can companies designate as representative?

Companies can appoint individuals or other companies. The representative can reside or be established anywhere in the EU where relevant data subjects reside; Art. 27(3) does not prescribe a particular member state. The same person or company could serve as representative under Art. 27 and as a data protection officer under Art. 37-39, but companies could also select different persons or entities, in the same or different EU member states.

Whom should companies designate?

Companies that own subsidiaries or have corporate affiliates in the EU can appoint these as representatives under Art. 27. This is cheap and easy and does not present any significant downsides for most companies so long as they are confident that the subsidiary is capable to forward inquiries to the legal department or global privacy office. Based on prior experience, data protection authorities in the EU will usually try to entangle local subsidiaries anyhow if they face difficulties getting a hold of foreign affiliates. The designation as representative will not expose the local subsidiary to a significant amount of additional liability of its own and could be revoked at any time if the foreign company wants to take an adversarial approach to a conflict with a data protection authority.

Also, companies that have appointed an external data protection officer could designate the same person as representative under Art. 27. The data protection officer will usually be involved in inquiries from data protection authorities anyhow and knows how to handle them. But, companies usually appoint individuals, not companies, as data protection officer, and such individuals may become concerned about personal liability as a representative under Art. 27. Also, not all companies that have to appoint a representative under Art. 27 are also subject to the requirement of appointment a data protection officer under Art. 37. Foreign companies will typically appoint a data protection officer in their home jurisdiction, outside the EU, whereas the Art. 27 representative must be in the EU. Moreover, the roles of a representative under Art. 27 and a data protection officer under Art. 37 are quite different, as noted above. 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 (see, Thomas Shaw, “How do the DPO and EU representative interplay?”, IAPP Advisor, Jan 23, 2018).

Alternatively, a company could appoint an unaffiliated person or entity. A number of professional services firms are already offering themselves up as representatives (see some listed in the IAPP Vendor List). Companies are wary of costs and potential conflicts of interests. Law firms face the issue that such a designation does not constitute "practice of law" for purposes of insurance, VAT/GST and attorney-client privilege. This could create risk management, tax and 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. Also, joint actions against law firms and their clients create diverging or outright conflicting interests. 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 or responds to an inquiry from a data protection authority to its client, this could constitute a waiver of objections on jurisdictional grounds. Attorneys or auditors face limitations under professional rules and responsibilities regarding what they can communicate on behalf of their clients to an authority whereas Art. 27(4) subjects the representative to a mandate without express limitations or discretion. 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.

In light of these considerations, many companies may gravitate towards appointing a subsidiary that they control and which is exposed to inquiries and challenges in any event. Companies that maintain several subsidiaries may select the one that is in the EU member state where it has "EU headquarters" or its largest presence or the presence most involved with the processing of personal data, because that is where it may find its "lead authority" under Art. 56 and possibly apply for binding corporate rules according to Art. 47.

How designate?

Companies can effectuate the designation with an informal letter that does not have to contain more than one sentence. Art. 27(1) requires the designation to be “in writing” and does not expressly permit electronic form, unlike Art. 28(9) or verbal appointments, unlike Art. 37. If a company designates an individual or unaffiliated entity, it should also put in place a separate services agreement to clarify responsibilities, compensation, termination rights and other commercial terms.

Author
Lothar Determann