SKW
Schwarz
Rechtsanwälte

# Representing non-EU companies under the EU General Data Protection Regulation

## A new era of data protection will start on May 25, 2018. And it does not stop at the EU borders.

As of May 25, 2018, the landscape of data protection rules for handling personal data of EU citizens will dramatically change. Companies from all sectors will have to adjust to the new legal regulations at an early stage. The regulations apply not only to companies in the EU, but also to companies that offer services within the EU, irrespective of what country they come from. Even suppliers from the USA, China, or India will have to comply with the requirements of the GDPR.

Who ever is targeting its products or services to EU citizens or (not only occasionally) handles personal data of EU citizens (e.g. by way of online tracking or profiling) will be subject to the new legal regime.

And this involves for companies with no establishment within the EU to appoint and work with a representative established in the EU who will act as legal point of contact for them with regard to EU authorities, individuals/customers and courts.

## We will represent and guide non-EU companies through this.

## What will change specifically?

- Companies must actively prove compliance with the GDPR in the future ("**accountability obligation**").
- All agreements on **contracted data processing** must be adapted to the new legal requirements.
- Companies must meet comprehensive **information duties** to customers, interested parties, employees, and other data subjects.
- In the future, data protection will occur according to a **risk-based approach**; considerations must be documented.
- The **requirements on technical data protection** are increasing; protection must correspond to the state of the art.
- **Privacy by Design**: Services and products must be designed with a minimum of data.
- When processing sensitive data, a **privacy impact assessment (PIA)** must be conducted and documented.
- Data subjects have a right to a digital **copy of all stored data**.
- Data protection incidents must be reported within 72 hours (**Data Breach Notification**).
- Data controller will have to appoint a **data protection officer (DPO)** and an **EU representative**.
- The **level of fines** increased considerably, now up to EUR 20 million or **4% of annual global revenue**; the higher value is applicable.

### The new law

As an EU regulation, the GDPR is applicable national law in all member states of the EU (including the UK) without another act of transposition. There are quite a number of escape clauses (on the data protection officer or on employee data protection); they have no influence, however, on the basic requirements of the GDPR and cannot reverse them. Companies must begin to implement the new requirements expeditiously.

### Will non-EU companies have to care for GDPR?

Are you offering free or paid services or products online or offline to EU citizens? At least as part of your offerings? Are you collecting or handling personal data of EU citizens, for example as part of your online tracking and advertising activities? If the answer to either or all of these questions is "yes" you are subject to the GDPR. Basically, you will have to appoint a Data Protection Officer, update your privacy policy, comply to the 72 hour data breach notification requirement, document your compliance to data privacy laws and ensure appropriate data processing agreements with vendors.

### New fine levels

Under the GDPR, the level of fines will generally increase up to EUR 20 million or 4% of global annual revenue. The infringement of the requirement to assign an EU representative will lead to administrative fines up to EUR 10 million or 2% of your annual turnover, whichever is higher.

### Data privacy is a relevant business factor

Not only supervisory authorities in all EU member states and press or media will be looking into the data privacy compliance of those who do business within the EU. Data privacy is a relevant factor for business relationships to EU partners, customers or vendors. As they will be subject to the increased accountability standards to document their own compliance, EU companies will be keen on stable and compliant relationships with their foreign and EU partners. Don't be the data compliance risk they would like to avoid!

# The EU representative for non-EU data controller

## 1) Can I avoid it?

Any data controller subject to the GDPR with no establishment in the EU will have to appoint a representative who is actually established in one of the EU Member States. Exception: e.g. when EU personal data is only “occasionally” processed. Because data processing or website monitoring is usually done automatically, and not on an individual basis confined to only a few individuals, this exception is though unlikely to apply in most instances.

## 2) What is the task?

The EU representative acts on behalf of the controller, is the direct contact for authorities, individuals and courts regarding data processing compliance and can be subject to enforcement proceedings in case of legal non-compliance. It also is an authorized agent to receive legal and court documents. The representative shall maintain a record of data processing activities and will have to present it to the authorities upon their request.

## 3) How to assign?

The EU representative’s appointment needs to be in written form. It should describe the representative’s tasks and the way to fulfill them, including the chain of communication e.g. in case of data breach notifications or information requests from authorities or individuals. It must not be communicated to the authorities but the contact details are to be included in the data privacy information (privacy policy) and records of processing.

## 4) Who do I need?

There is no formal requirement as to the EU representative’s personal qualification. It may either be an employee of the controller or external service provider. It needs to be established within the EU. Controllers will have to rely on its judgement in reacting or reply to the requests of authorities and individuals, maybe will ask for advice regarding legal compliance under GDPR. Thus, a good knowledge of the applicable rules would be advisable.

## 5) What is the effort?

As a set up, the EU representative will have to learn all about the controller’s data processing activities and the flow of data. It will require a copy of the controller’s record of data processing activities or the necessary information to draft it. The chain of and rules for communication will have to be implemented. All this needs to be updated on a regular basis. The representative will have to ask for the information to fulfill its tasks.

Source of the image: © sdecoret – fotolia.com

---

## Advice and support by SKW Schwarz

SKW Schwarz is an independent German law firm with more than 120 lawyers, more than 30 of whom are practicing in IT & Digital Business. All are fluent in German and English, many are skilled in other languages spoken by our clients (e.g. Spanish or French).

We have already assisted many customers, ranging from the classic German medium-sized company up to multinational large companies, to implement the GDPR. We can draw on an experienced, trans-regional team of data protection specialists and use a common set of checklists and best-practice documents, which we can adjust to the client’s individual needs.

Now we are extending our service to guide and represent our non-EU clients as well. We are aware that these client do require not only a legal letterbox but practical advice and legal proof guidance. Through our external partner we offer the services of EU representatives to all sorts of clients from all over the globe. As a leading data privacy law firm we provide the respective legal support and guidance.

Where necessary or requested we can rely on our stable network of longstanding relationships to the finest expert independent law firms in all EU legislations and outside the EU.

SKW
Schwarz
Rechtsanwälte

## Your Contacts

**Dr. Matthias Orthwein, LL.M. (Boston)**
Attorney at law / Rechtsanwalt, Partner

E m.orthwein@skwschwarz.de
T +49 89 28640 102

## The SKW Schwarz GDPR Team

**Nikolaus Bertermann**
Rechtsanwalt, Certified Expert in IT Law
Cert. Data Protection Auditor (TÜV, GDDcert.)

**Dr. Oliver Hornung**
Rechtsanwalt, Partner

**Dr. Volker Wodianka, LL.M. (Strathclyde)**
Rechtsanwalt, Partner
Certified Information Privacy Professional
(CIPP/E, CIPM, GDDcert.)












Ivan Brankov
Dr. Oliver M. Bühr
Insa Janßen, LL.M.
Dr. Wulf Kamlah
Franziska Ladiges, LL.B.
Dr. Matthias Nordmann, M.A.
Dr. Stefan Peintinger, LL.M.
Yvonne Schäfer
Stefan C. Schicker, LL.M.
Jan Schneider
Martin Schweinoch
Benjamin Spies

**SKW Schwarz Rechtsanwälte Wirtschaftsprüfer Steuerberater mbB**

10719 Berlin
Kurfürstendamm 21

T +49 30 889 26 50 0
F +49 30 889 26 50 10

40212 Düsseldorf
Steinstr. 1

T +49 211 82 89 59 0
F +49 211 82 89 59 60

60598 Frankfurt/Main
Mörfelder Landstr. 117

T +49 69 63 00 01 0
F +49 69 63 55 22

20095 Hamburg
Ferdinandstr. 3

T +49 40 334 01 0
F +49 40 334 01 530

80333 Munich
Wittelsbacherplatz 1

T +49 89 286 40 0
F +49 89 280 94 32

**www.skwschwarz.de**

JUVE AWARDS 2016 Kanzlei des Jahres für Medien und Technologie

JUVE AWARDS 2011 Kanzlei des Jahres für Informationstechnologie