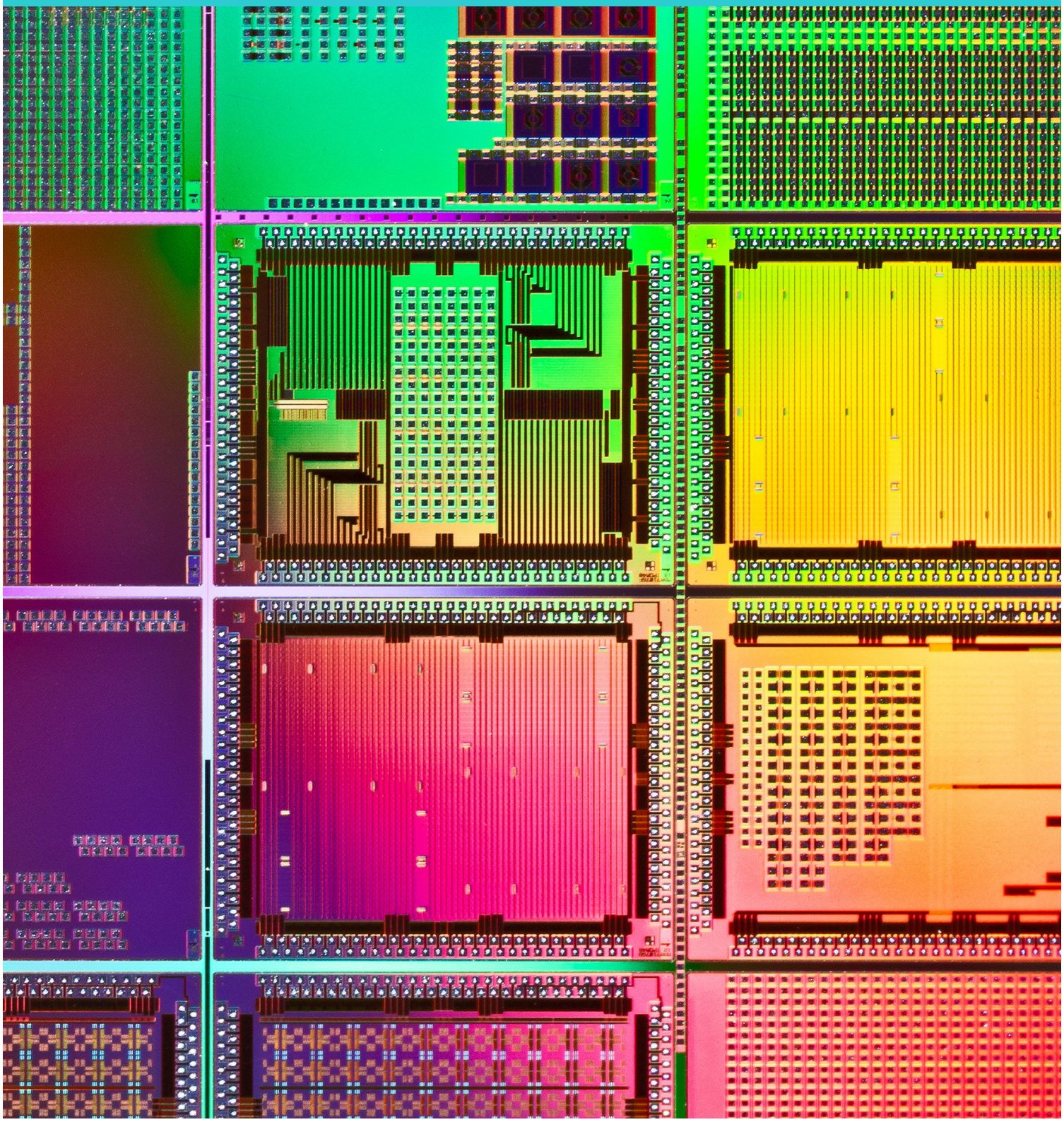
TaylorWessing

# Step Plan GDPR Implementation



Since entering into force in May 2018, the EU General Data Protection Regulation (GDPR) applies to all entities in the European Economic Area (EEA) and - due to the extended territorial scope - to a large extent also to entities outside of the EEA. The GDPR has led to a significant rise in data protection compliance duties. In case of violations, companies may face fines of up to 4% of the global annual turnover of the whole company group. Supervisory authorities do not seem to be afraid to push those limits. In 2019, European supervisory authorities have announced and issued record-breaking fines of £183 million (UK) and €50 million (France). Even data protection non-compliance in smaller and less important offices of a company group may now lead to significant ramifications. As the preparation for the GDPR requires reorganisation of various internal procedures, it is highly recommendable to follow a structured path when initiating a GDPR compliance project.

If you have already implemented compliance measures, please be aware of the duty to regularly audit and potentially update your internal processes. Please see our guidance on conducting GDPR audits in this regard.

## Steps to implement GDPR standards:

**1 Step 1**
Gap analysis

**2 Step 2**
Risk analysis

**3 Step 3**
Project steering and resource/ budget planning

**4 Step 4**
Implementation of a compliant data protection structure

**5 Step 5**
Local Add-on Requirements

**6 Step 6**
Coping with the Brexit

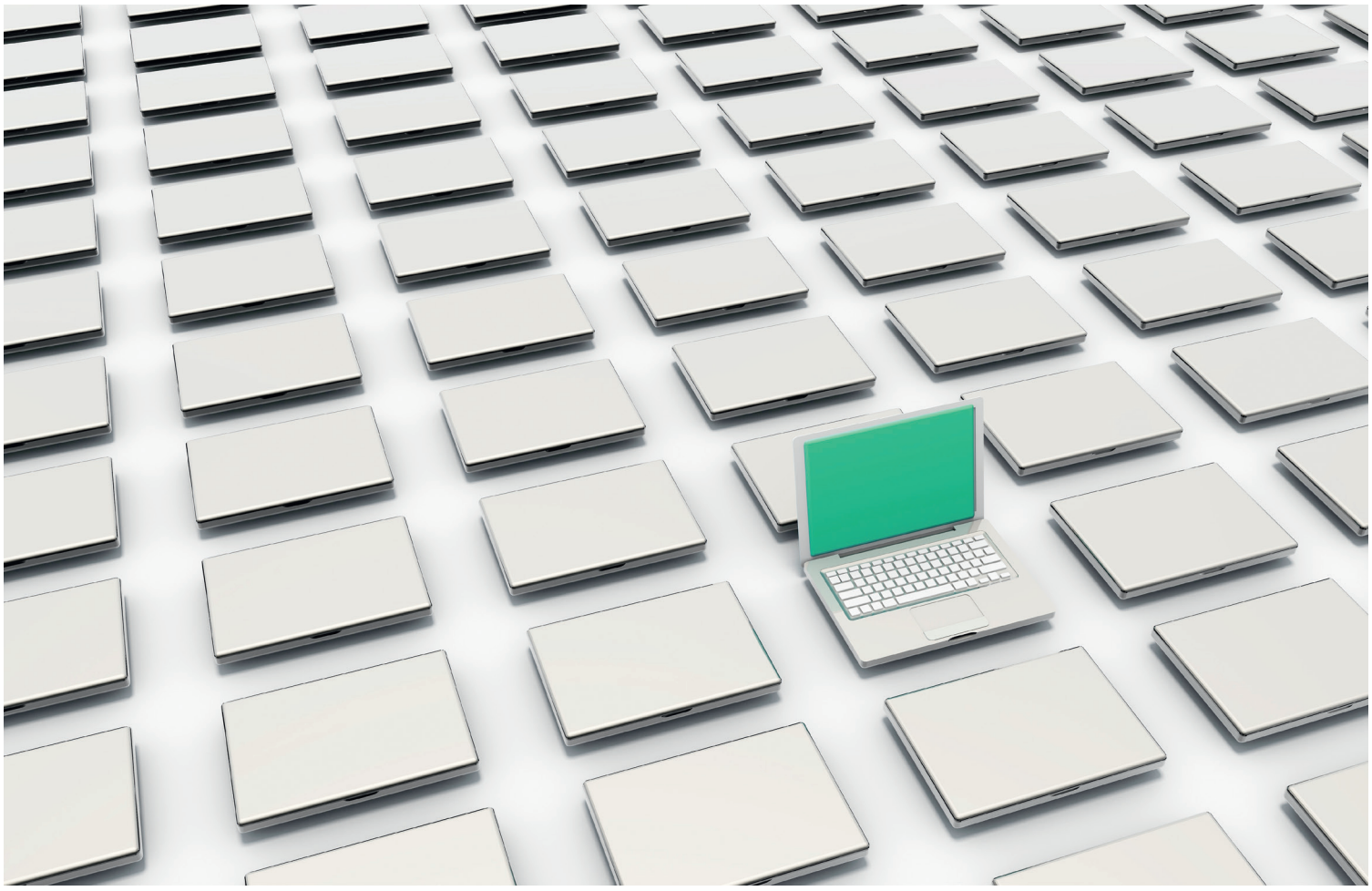
1 The GDPR applies to all companies processing personal data
- in the context of the activities of an establishment in the EU, regardless of whether the processing takes place in the EU or not;
- of data subjects who are in the EU (regardless of Company's seat), where the processing is related to:
  - the offering of goods/services (even if at "no-cost-basis") to such data subjects in the EU; or
  - the monitoring of their behaviour as far as their behaviour takes place within the EU.

## 1 Step 1
Gap analysis

- In order to assess a company's data protection To Do's, a "gap analysis" between the current status of data protection compliance and the obligations deriving from the GDPR should be carried out.
  - Thus, in a first step, the company should collect information about its current data protection activities (e.g. (i) which entities / departments process what kind of data for what purposes, (ii) internal responsibilities, (iii) how are data subjects' rights safeguarded, (iv) have data protection officers been appointed, (v) what IT security measures are in place etc.).
  - In a second step, the company has to assess which requirements deriving from the GDPR specifically apply.

## 2 Step 2
Risk analysis

- The efforts for implementing GDPR requirements are generally high; not all requirements can reasonably be fulfilled at once. The company will have to assess what kind of data processing activities are of biggest risk to (i) its business and/or (ii) rights of the data subjects as well as (iii) which risks most likely lead to high fines (e.g. by evaluating scenarios that authorities have sanctioned with fines in the past), and arrange its resources respectively. Efforts for data protection compliance should be higher for risky processing activities and lower for less risky processing activities.



## 3 Step 3
Project steering and resource/ budget planning

- The GDPR implementation process requires collaboration between the company's European entities, as well as awareness of the To Do's on the management level of the company. The company should assign project responsibilities to key personnel at the involved EU offices and designate one "head" project manager. This could also be an external advisor.
- The company must allocate the required resources. Planning should in particular cover (i) internal resources, such as personnel required for implementation, (ii) legal costs as well as (iii) IT costs (e.g. for supporting software; IT audits etc.)..

## 4 Step 4
Implementation of a compliant data protection structure

The GDPR includes a number of strict data protection requirements, such as

- Comprehensive data subjects' rights (e.g. regarding information, access and correction/deletion; right to data portability; right to object to data processing activities, "right to be forgotten"- obligation to forward access/deletion requests to third party data recipients; high requirements for consent declarations etc.),
- Organisational requirements (e.g. obligation to have records of processing activities summarizing internal data processing activities; necessity of conducting data protection impact assessments and to appoint data protection officers in various cases; obeying privacy by design and by default requirements to ensure that data processing systems are privacy-friendly; obligation to link personal data with the purposes for which they have been collected as well as with the legal basis for processing; documentation of data flows; having deletion concepts etc.),
- SNotification obligations (e.g. potential obligation to inform supervisory authorities within 72 hours of a data breach, as well as the concerned individuals),
- IT/Cyber Security requirements,
- Contractual requirements (conclusion of comprehensive data processing agreements with external service providers as well as potentially within the company group).

Please see the annex for more details regarding the major requirements deriving from the GDPR. In order to cope with these obligations, the company must implement an efficient data protection organisation:

### 4.1 Data Protection Management System

The GDPR stipulates a number of requirements that are difficult to handle unless a thorough data protection management system is implemented. Such system should work group-wide, as even data protection issues in smaller company offices may lead to high fines for the company group as a whole.

**(a) Defined roles and responsibilities in the involved Company entities**

Company should set up a structure of persons responsible for data protection in all of its EU offices as well as a responsible head officer at the Headquarters. Respective structure should allow for (i) easily giving data protection related orders and/or advice to the involved offices ("top-down approach") as well as (ii) communication of data protection related issues to the head officer ("bottom-up" communication).

**(b) Procedures and concepts**

Many of the GDPR obligations can only be effectively implemented if respective concepts, policies and standard operating procedures (cumulatively "SOPs") are in place, e.g. regarding data subjects' rights, data breach notification obligations, Data Protection Impact Assessments etc. Thus, respective SOPs should be prepared to ensure GDPR compliance.

**(c) Training**

Employees should be trained on their obligations and responsibilities deriving from the GDPR. The company should adapt the training to the employee's tasks. In this respect, it makes sense to map the training requirements in a training concept.

This concept should also reflect the cycle of training (regular training, training in the event of legal changes (e.g. due to new regulations, deviating case law, current guidelines of the supervisory authorities)).

**(d) Documentation of Compliance**

The company must implement appropriate measures to demonstrate compliance with GDPR requirements. Failure to prove continuous compliance upon request of supervisory authorities will likely result in fines. Internal data protection procedures should be reviewed and updated frequently. For this purpose, the company should carry out regular internal GDPR audits.

### 4.2 Data processing agreements

Due to the high number of agreements that the company must conclude with internal and external parties, companies should implement a sensible data processing contract management strategy:

- The use of data processors (entities processing personal data on behalf of the company in compliance with its instructions) will only be permissible if comprehensive data processing agreements are concluded. If pre-GDPR agreements exist, these will have to be checked to see whether they comply with GDPR requirements or must be updated. This may also apply for intra-company data sharing (e.g. data hosting of one group entity for other group entities).
- In some cases, various company entities may be regarded as joint data controllers if they jointly determine the purposes and means of data processing. In such cases, data processing agreements between the involved entities generally must be concluded as well.
- If personal data is transferred from the EEA to a country outside the EEA, additional data transfer agreements may be necessary.

## 5 Step 5
## Local Add-on Requirements

In addition to the EU-wide GDPR requirements, it must be assessed whether additional national requirements apply.

- The EU Member States have broad discretion to enact additional national regulations amending and/or refining the GDPR.
- In most EEA countries, additional employment-related requirements exist regarding the processing of HR data (such as e.g. requirements to involve works councils in Germany and France or a labour office in Italy).

## 6 Step 6
## Coping with the Brexit

- Many international company groups have their European Headquarters in the UK, which longer forms part of the European Union. Through UK legislation, GDPR requirements may continue to apply to company offices in the UK. However, data transfers from other company offices in the EEA to any UK office will require additional safeguards may lead to legal issues. Affected companies will have to take data protection precautions for Brexit.

# Annex

## Most important obligations of the GDPR

At a very high level, these are the most important GDPR requirements:

### 1. Organisational requirements

#### 1.1 Accountability, Art. 5 Sec. 2

Companies must be able to prove full compliance with their obligations under the GDPR. In order to document the lawfulness of their processing activities, companies must have appropriate measures and records in place. These must be constantly updated.

#### 1.2 Records of Data Processing Activities, Art. 30

Records of processing activities under the company's responsibility must be maintained in most cases. These records shall generally contain the following information:

- Name and contact details of the company and its data protection officer;
- The purposes of the processing;
- A description of the categories of data subjects and of the categories of personal data;
- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- Transfers of personal data to a third country and the documentation of suitable safeguards;
- Envisaged time limits for erasure of the different categories of data;
- A general description of the technical and organisational security measures

#### 1.3 Data Protection Impact Assessment (DPIA), Art. 35, 36

Where a data processing activity is likely to result in a high risk to the rights and freedoms of natural persons, the company shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations. Companies should consider the regulators' guidelines listing scenarios that always require DPIAs. If such assessment indicates a high risk that the company cannot mitigate, the supervisory authority shall be consulted.

#### 1.4 Data Processors, Art. 28

Companies may use internal or external service providers to process personal data. These data processors will process personal data on behalf and under the instructions of the company. Both parties are subject to their own data protection obligations under the GDPR. As an additional compliance requirement, the parties must conclude a Data Processing Agreement that specifies their obligations and allocates responsibilities for the contracted processing activity.

#### 1.5 Data Protection Officer, Art. 37-39

An independent, reliable and knowledgeable data protection officer must be appointed in case the company's core activities consist of

- Processing operations which require regular and systematic monitoring of data subjects on a large scale: or
- Processing on a large scale of special categories of personal data (e.g. health, religion, race, sexual orientation etc.) and personal data relating to criminal convictions and offences.
- A group of undertakings may appoint a single data protection officer provided that he/she is easily accessible from each establishment. Local laws may require the implementation of data protection officers in additional cases (e.g. in Germany). Thus, one global data protection officer steering data protection EU-wide may prove helpful in order to cope with differing EU-wide regulations.

#### 1.6 Implementation of Technical and Organisational Security Measures, Art. 32

Appropriate and reasonable state of the art technical and organisational measures (TOMs) must be implemented in order to protect the personal data.

#### 1.7 Data Breach Notifications, Art. 33, 34

In case of personal data breaches with risks to rights and freedoms of the data subjects, the supervisory authority shall generally be informed within 72 hours after the company became aware of the breach. In case of high risks for the data subjects, they generally also must be informed about the breach. Compliance with the notification obligation in the envisioned time period requires a proper internal data breach procedure.

### 1.8 Privacy by Design and by Default, Art. 25

Each company's processing activities shall

- be designed to implement data protection principles, such as data minimisation, and to integrate safeguards into the processing in order to protect data subject rights (e.g. pseudonymisation).
- Ensure that, by default, only personal data which are necessary for the specific processing purpose are processed.

### 1.9 Representative in the EU, Art. 27

Companies without establishment in the EU must appoint an EU representative for dealings with authorities etc. Upside of having a representative: this will establish a "one-stop-shop" for third country companies when it comes to notifying data breaches to the regulator.

## 2. Material requirements of data processing

**2.1**
Each processing of personal data will require either valid data subject consent or a legal justification.

**2.2**
Cross-border data transfers to countries outside the European Economic Area require additional justification (see above Section 2.1), e.g. use of Privacy Shield, EU Standard Contractual Clauses or Binding Corporate Rules (or, in limited cases, consent).

## 3. Rights of Data Subjects, Art. 12-23

The rights of the data subjects have been strengthened. In particular, data subjects have the following rights:

### 3.1 Information rights, Art. 12-14

Transparent and broad information about processing must be provided to data subjects.

### 3.2 Access, deletion, rectification, restriction rights, Art. 16-19

Data subjects generally have broad access rights with respect to their data; in some cases, they will also have the right to have their data deleted, rectified or the data processing activities restricted.

### 3.3 Right to Object, Art. 21-22

In some cases, data subjects have the right to object to the processing of their data on grounds relating to their particular situation.

### 3.4 Data Portability, Art. 20

In limited cases, data subjects may even have the right to request to receive the personal data concerning them in a structured, commonly used and machine-readable format and have the right to transmit those data to another company.

## Your Contacts

**Dr. Paul Voigt,**
**Lic. en Derecho, CIPP/E**
Tel +49 (0)30 88 56 36 408
p.voigt@taylorwessing.com

**Highlighted as Lawyer of the year 2020**
Data protection law,
Best Lawyers in Germany,
Handelsblatt

**Next Generation Lawyer – Germany**
Legal 500 Germany 2020

TOP Lawyer for
**Data Protection Law**
WirtschaftsWoche 2019

**Dr. Axel Frhr. von dem Bussche, LL.M. (L.S.E.)**
Tel +49 (0)40 3 68 03 347
a.bussche@taylorwessing.com

**Global Leader for Data Protection**
Who's Who Legal 2020

**Leading individual for IT and Digitalization – Germany**
Legal 500 Germany 2020

Leading individual for
TMT: **Data Protection**
Chambers Europe 2020

TaylorWessing

16 jurisdictions

28 offices

300+ partners

1000+ lawyers

| | |
|---|---|
| **Austria** | Vienna I Klagenfurt* |
| **Belgium** | Brussels |
| **China** | Beijing* I Hong Kong I Shanghai* |
| **Czech Republic** | Prague I Brno* |
| **France** | Paris |
| **Germany** | Berlin I Düsseldorf I Frankfurt I Hamburg I Munich |
| **Hungary** | Budapest |
| **Netherlands** | Amsterdam I Eindhoven |
| **Poland** | Warsaw |
| **Slovakia** | Bratislava |
| **South Korea** | Seoul** |
| **Ukraine** | Kyiv |
| **UAE** | Dubai |
| **United Kingdom** | Cambridge I Liverpool I London \| London Tech City |
| **USA** | Silicon Valley* I New York* |

* Representative offices
** Associated office