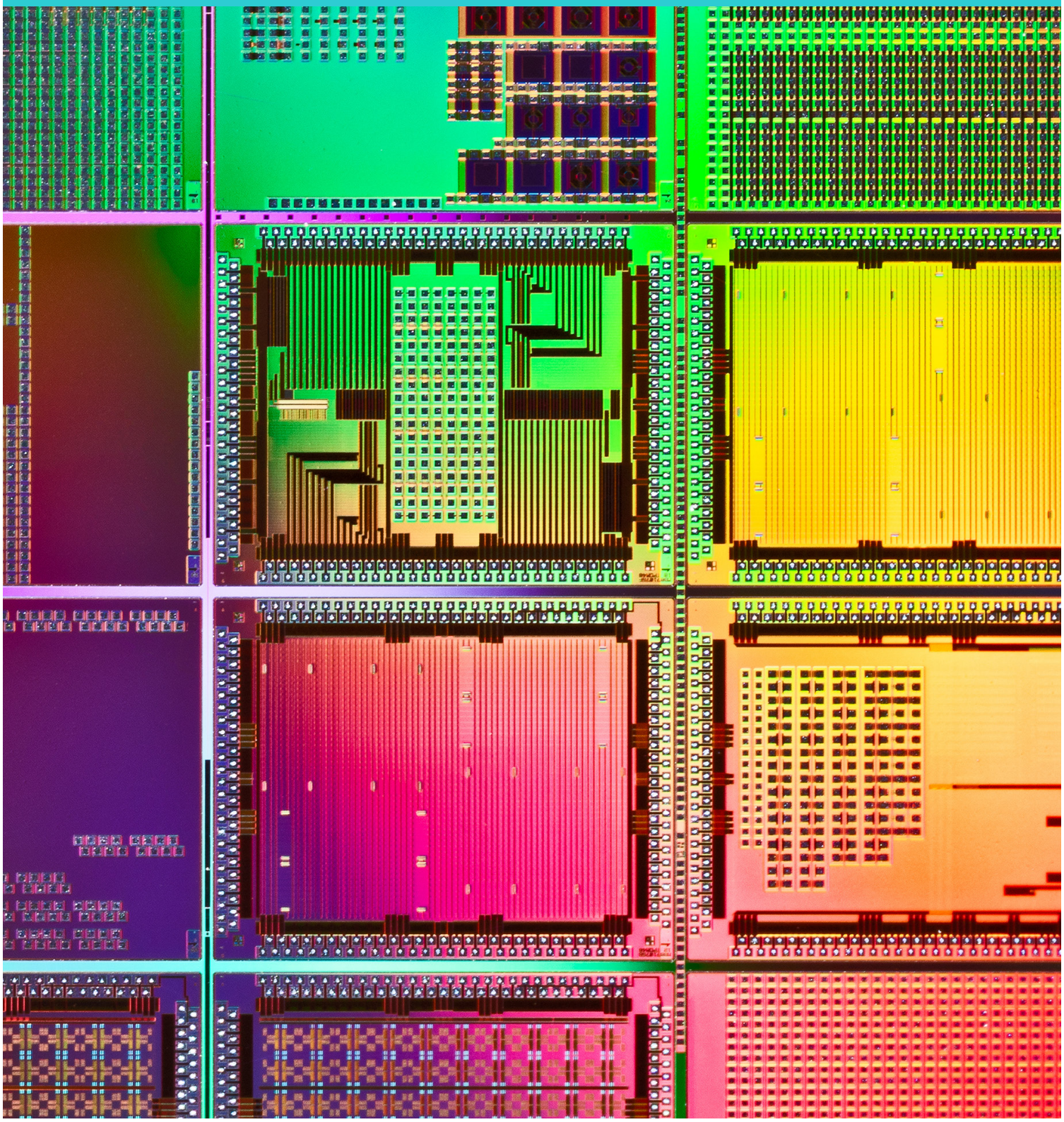
TaylorWessing

Implementierung der EU-Datenschutz-Grundverordnung



Seit ihrem Inkrafttreten im Mai 2018 gilt die EU-Datenschutz-Grundverordnung (DSGVO) für alle Unternehmen im Europäischen Wirtschaftsraum (EWR) und – aufgrund des erweiterten räumlichen Anwendungsbereiches – auch für viele Unternehmen außerhalb des EWR. Die DSGVO hat zu deutlich erhöhten Compliance-Anforderungen geführt. Im Falle von Verstößen müssen Unternehmen mit Bußgeldern von bis zu 20 Mio. EUR bzw. 4% des gesamten weltweit erzielten Jahresumsatzes der Unternehmensgruppe rechnen. Die Aufsichtsbehörden scheuen sich nicht davor, diesen Bußgeldrahmen auszuschöpfen. Im Jahr 2019 haben die europäischen Aufsichtsbehörden rekordverdächtige Bußgelder in Höhe von 183 Millionen Pfund (Großbritannien) und 50 Millionen Euro (Frankreich) angekündigt und verhangen. Selbst Compliance-Verstöße kleinerer und weniger wichtiger Niederlassungen eines Konzerns können nun schwerwiegende Konsequenzen haben. Da die Vorbereitung auf die DSGVO eine Restrukturierung zahlreicher interner Prozesse erfordert und damit zeitaufwendig werden kann, ist es anzuraten, das Umsetzungsprojekt strukturiert durchzuführen.

Haben Sie die DSGVO bereits umgesetzt, sollten Sie ihre rechtliche Pflicht zur regelmäßigen Überprüfung und Aktualisierung der internen Prozesse nicht aus den Augen verlieren. Dabei kann Ihnen unser Leitfaden zur Durchführung von DSGVO-Audits als Hilfestellung dienen.

Schritte zur Implementierung von DSGVO-Standards:

1 Schritt 1
Gap analysis

2 Schritt 2
Risikoanalyse

3 Schritt 3
Projektsteuerung und Ressourcen-/ Budgetplanung

4 Schritt 4
Umsetzung einer rechtskonformen Datenschutz-Struktur

5 Schritt 5
Zusätzliche landesspezifische Voraussetzungen

6 Schritt 6
Coping with the Brexit

---

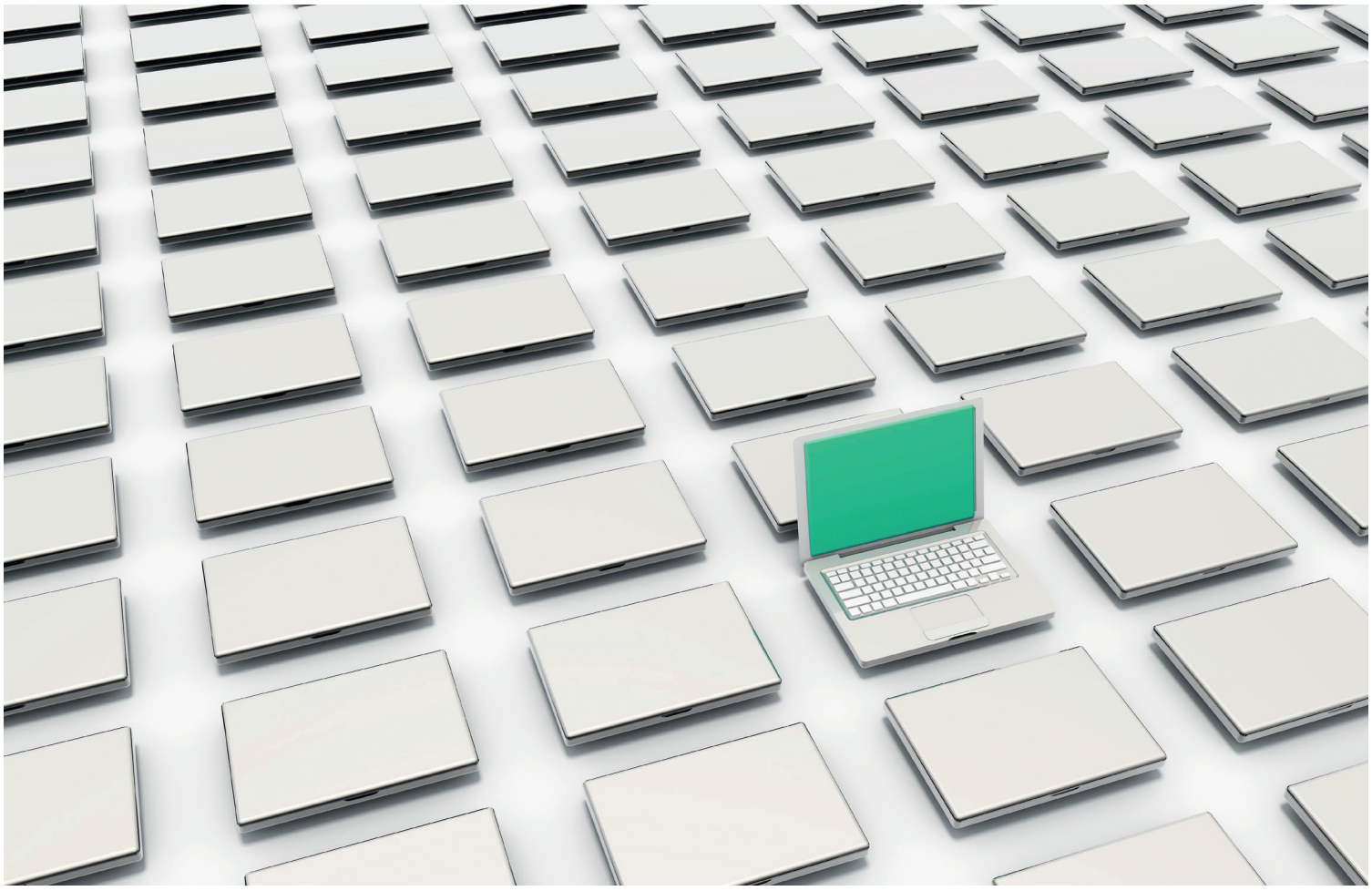
1 Die DSGVO gilt gem. Art. 3 für alle Unternehmen, die personenbezogene Daten verarbeiten,
- soweit dies im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet
- von betroffenen Personen, die sich in der Union befinden (unabhängig vom Sitz des Unternehmens), wenn die Datenverarbeitung im Zusammenhang damit steht:
  - betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten (auch bei Entgeltlosigkeit);
  - das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

1 Schritt 1
Gap analysis

- Zur Feststellung des datenschutzrechtlichen Handlungsbedarfs eines Unternehmens sollte zuerst eine „Lückenanalyse" durchgeführt werden, bei der die gegenwärtige Datenschutz-Compliance mit den Anforderungen der DSGVO verglichen wird.
  - In einem ersten Schritt sollten Unternehmen Informationen über ihre aktuelle Datenschutzpraxis sammeln (z.B. (i) welche Abteilungen welche Arten von Daten für welchen Zweck verarbeiten, (ii) wie die internen Verantwortlichkeiten verteilt sind, (iii) wie die Rechte betroffener Personen geschützt werden, (iv) ob Datenschutzbeauftragte eingesetzt worden sind, (v) welche IT-Sicherheitsmaßnahmen vorhanden sind etc.).
  - In einem zweiten Schritt muss das Unternehmen bestimmen, welche Anforderungen der DSGVO konkret gelten.

2 Schritt 2
Risikoanalyse

- Die vielfältigen Anforderungen der DSGVO können nicht zeitgleich vollständig erfüllt werden. Das Unternehmen muss daher abschätzen, welche Datenverarbeitungstätigkeiten das größte Risiko für (i) den Geschäftsbetrieb des Unternehmens und/oder (ii) die Rechte der betroffenen Personen darstellen sowie (iii) welche Risiken am wahrscheinlichsten zu hohen Geldbußen führen (z.B. durch die Auswertung von Fällen, für die von den Aufsichtsbehörden bereits Bußgelder verhängt wurden). Im Anschluss an diese Einschätzung sind die Ressourcen entsprechend zu verteilen. Der Datenschutz-Compliance für risikoreiche Verarbeitungstätigkeiten sollte dabei größere Aufmerksamkeit geschenkt werden als der für weniger riskante Bereiche.



3 Schritt 3
Projektsteuerung und Ressourcen-/Budgetplanung

- Die Umsetzung der DSGVO erfordert zum einen die Zusammenarbeit der europäischen Niederlassungen des Unternehmens, zum anderen die Kenntnis der noch ausstehenden Aufgaben auf Management-Ebene. Das Unternehmen sollte Verantwortlichkeiten für das Projekt an Schlüsselpersonen in den Niederlassungen übertragen und einen leitenden Projektmanager ernennen. Dieser kann auch ein externer Berater sein.
- Das Unternehmen muss die notwendigen Ressourcen zur Verfügung stellen. Die Budgetplanung sollte insbesondere (i) interne Ressourcen, wie für die Umsetzung benötigtes internes Personal, (ii) rechtliche Kosten sowie (iii) IT-Kosten (z.B. für unterstützende Software; IT-Überprüfungen etc.) berücksichtigen.

4 Schritt 4
Umsetzung einer rechtskonformen Datenschutz-Struktur

Die DSGVO enthält eine Reihe strenger Datenschutzanforderungen, wie zum Beispiel

- Umfassende Rechte der betroffenen Personen (z.B. auf Information, Auskunft und Berichtigung/Löschung; das Recht auf Datenübertragbarkeit; das Recht auf Widerspruch gegen bestimmte Datenverarbeitungstätigkeiten; das „Recht auf Vergessenwerden" – die Verpflichtung, Auskunfts- oder Löschanträge an dritte Datenempfänger weiterzuleiten; strenge Anforderungen an Einwilligungserklärungen etc.),
- Organisatorische Anforderungen (z.B. die Verpflichtung zum Führen eines internen Verzeichnisses von Verarbeitungstätigkeiten; die Notwendigkeit, in verschiedenen Fällen eine Datenschutz-Folgeabschätzung durchzuführen und einen Datenschutzbeauftragten zu ernennen; Datenschutz durch Technik („privacy by design") und Datenschutz durch datenschutzrechtliche Voreinstellungen („privacy by default"); die Verpflichtung zur Verknüpfung personenbezogener Daten mit dem Zweck ihrer Erhebung und der Ermächtigungsgrundlage für ihre Verarbeitung; die Dokumentation von Datenübermittlungen; ein Entwurf für Löschkonzepte etc.),
- Meldepflichten (z.B. die Verpflichtung, im Falle einer Verletzung des Schutzes personenbezogener Daten binnen 72 Stunden die Aufsichtsbehörden sowie ggf. die betroffenen Personen zu informieren),
- IT/Cyber-Sicherheitsanforderungen,
- Vertragliche Anforderungen (mit externen Service-Providern und unter Umständen auch innerhalb der Unternehmensgruppe müssen Datenverarbeitungsverträge geschlossen werden).

Für weitere Details zu den wichtigsten Anforderungen der DSGVO wird auf den Annex verwiesen. Um allen Verpflichtungen nachzukommen, muss das Unternehmen eine robuste Datenschutzstruktur einführen:

4.1 Datenschutz-Management-System

Die DSGVO sieht eine Reihe von Anforderungen vor, die ohne ein umfassendes Datenschutz-Management-System schwierig zu bewältigen sind. Ein solches System sollte konzernweit eingeführt werden, da datenschutzrechtliche Verstöße selbst in kleineren Niederlassungen zu hohen Geldbußen für die gesamte Unternehmensgruppe führen können.

(a) Festlegung von Rollen und Verantwortlichkeiten

Das Unternehmen sollte Datenschutzstrukturen in allen EU-Niederlassungen schaffen und einen verantwortlichen Leiter in der Muttergesellschaft bestimmen. Die entsprechende Struktur sollte (i) eine einfache Erteilung datenschutzbezogener Anweisungen und/oder Empfehlungen an die beteiligten Stellen ermöglichen („top-down-Ansatz") sowie (ii) die Mitteilung datenschutzbezogener Angelegenheiten an den Leiter gewährleisten („bottom-up-Kommunikation").

(b) Verfahren und Konzepte

Viele der Verpflichtungen aus der DSGVO können in der Praxis nur implementiert werden, wenn entsprechende Konzepte, Richtlinien und Standardvorgehensweisen (kumulativ sog. „Standard Operating Procedures", „SOP") eingeführt werden. Dies betrifft insbesondere die Rechte betroffener Personen, die Meldepflichten bei der Verletzung des Schutzes personenbezogener Daten, die Datenschutz-Folgeabschätzungen etc.

(c) Training

Mitarbeiter sollten in Bezug auf ihre sich aus der DSGVO ergebenden Verpflichtungen und Verantwortlichkeiten geschult werden. Das Unternehmen sollte die Schulung an den Aufgabenbereich des Mitarbeiters anpassen. Insofern ist es sinnvoll, den Schulungsbedarf in einem Schulungskonzept abzubilden.

Dieses Konzept sollte auch den Schulungszyklus festlegen (regelmäßige Schulung, Schulung bei gesetzlichen Änderungen (z.B. aufgrund neuer Vorschriften, abweichender Rechtsprechung, aktueller Richtlinien der Aufsichtsbehörden)).

(d) Dokumentation

Das Unternehmen muss angemessene Maßnahmen ergreifen, um die Einhaltung der Anforderungen der DSGVO nachweisen zu können. Wenn die kontinuierliche Einhaltung datenschutzrechtlicher Vorschriften auf Verlangen der Aufsichtsbehörden nicht nachgewiesen werden kann, ist mit der Verhängung von Bußgeldern zu rechnen. Diese Maßnahmen sollten regelmäßig überprüft und aktualisiert werden. Zu diesem Zweck sollte das Unternehmen regelmäßig interne DSGVO-Audits durchführen

4.2 Datenverarbeitungsverträge

Aufgrund der hohen Anzahl von Vereinbarungen, die konzernintern sowie mit Dritten geschlossen werden müssen, ist eine durchdachte Strategie für das Management von Datenverarbeitungsverträgen erforderlich.

- Der Einsatz von Auftragsverarbeitern (Stellen, die personenbezogene Daten im Auftrag des Unternehmens entsprechend dessen Anweisungen verarbeiten) erfordert zwingend den Abschluss von umfassenden Datenverarbeitungsverträgen. Bestehende Verträge müssen überprüft werden, um festzustellen, ob sie den Voraussetzungen der DSGVO entsprechen oder ob Änderungsbedarf besteht. Dies kann auch für den unternehmensinternen Datenaustausch gelten (z.B. Daten-Hosting einer Gruppengesellschaft für andere Gruppengesellschaften).
- In einigen Fällen können verschiedene Unternehmensteile als gemeinsam für die Verarbeitung Verantwortliche qualifiziert werden, wenn sie zusammen den Zweck und die Mittel der Datenverarbeitung festlegen. Grundsätzlich müssen auch in diesen Fällen zwischen den involvierten Stellen Datenverarbeitungsverträge geschlossen werden.

5 Schritt 5
Zusätzliche landesspezifische Voraussetzungen

Das Unternehmen sollte des Weiteren prüfen, ob neben den EU-weit einheitlichen Voraussetzungen der DSGVO darüber hinausgehende nationale Vorschriften anzuwenden sind.

- Die Mitgliedsstaaten der EU verfügen über einen weiten Ermessensspielraum für den Erlass zusätzlicher nationaler Vorschriften, welche die DSGVO ergänzen und/oder präzisieren.
- In den meisten EWR-Ländern kann es zusätzliche arbeitsrechtliche Vorschriften für die Verarbeitung von Daten im Personalbereich geben (etwa die Einbeziehung eines Betriebsrates in Deutschland und Frankreich oder behördlicher Stellen in Italien).

6 Schritt 6
Der Umgang mit dem Brexit

- Viele internationale Unternehmensgruppen haben Niederlassungen im Vereinigten Königreich („UK"), welches kein Teil der Europäischen Union mehr ist. Aufgrund britischer Gesetzgebung dürften – auch nach Ablaufen einer Übergangsfrist, in der die DSGVO direkt weitergilt – die Anforderungen der DSGVO weiterhin auf dortige Niederlassungen entsprechend anwendbar sein.. Allerdings werden für Datenübermittlungen aus anderen europäischen Unternehmensteilen nach UK zusätzliche Datenschutzgarantien erforderlich werden. Betroffene Unternehmen werden daher für den Brexit Datenschutzvorkehrungen treffen müssen.

Annex

Die wichtigsten Verpflichtungen aus der DSGVO

Nachfolgend werden die wichtigsten Verpflichtungen aus der DSGVO kurz dargestellt:

1. Organisatorische Maßnahmen

1.1 Rechenschaftspflicht, Art. 5 Abs. 2

Unternehmen müssen nachweisen können, dass sie ihren Verpflichtungen aus der DSGVO in vollem Umfang nachkommen. Um die Rechtmäßigkeit ihrer Verarbeitungstätigkeiten zu dokumentieren, müssen Unternehmen geeignete Maßnahmen implementieren. Die Datenschutzdokumentation muss stets auf dem aktuellen Stand gehalten werden.

1.2 Verzeichnis von Datenverarbeitungstätigkeiten, Art. 30

In den meisten Fällen muss ein Verzeichnis der in die Unternehmenszuständigkeit fallenden Datenverarbeitungstätigkeiten geführt werden. Dieses soll insbesondere die folgenden Informationen enthalten:

- Den Namen und die Kontaktdaten des Unternehmens und dessen Datenschutzbeauftragten;
- Die Zwecke der Verarbeitung;
- Eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- Die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittstaaten oder in internationalen Organisationen;
- Die Übermittlung von personenbezogenen Daten an Drittstaaten und die Dokumentierung geeigneter Garantien;
- Vorgesehene Fristen für die Löschung verschiedener Datenkategorien;
- Eine allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen.

1.3 Datenschutz-Folgeabschätzung (DSFA), Art. 35, 36

Birgt eine Datenverarbeitungstätigkeit voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen in sich, muss das Unternehmen vor der Datenverarbeitung eine Einschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge durchführen. Unternehmen sollten auf die von den Datenschutzaufsichtsbehörden veröffentlichten Listen zurückgreifen, in denen Verarbeitungstätigkeiten aufgeführt sind, die stets eine DSFA erfordern. Ergibt die DSFA ein hohes Risiko, wenn keine Maßnahmen zur Risikominimierung seitens des Unternehmens getroffen werden, ist die Aufsichtsbehörde zu konsultieren.

1.4 Auftragsverarbeiter, Art. 28

Unternehmen können interne oder externe Dienstleister mit der Verarbeitung personenbezogener Daten beauftragen. Diese Auftragsverarbeiter verarbeiten personenbezogene Daten im Auftrag und auf Grundlage der Weisungen des Unternehmens. Beide Parteien unterliegen eigenen Verpflichtungen aus der DSGVO. Als zusätzliche Compliance-Anforderung müssen die Parteien einen Auftragsdatenverarbeitungsvertrag schließen, in dem ihre datenschutzrechtlichen Pflichten festgelegt und die Verantwortlichkeiten für die vertraglich vereinbarte Verarbeitungstätigkeit zugewiesen werden.

1.5 Data Protection Officer, Art. 37-39

Bestehen die Kerntätigkeiten des Unternehmens aus folgenden Verarbeitungsvorgängen, ist grundsätzlich ein Datenschutzbeauftragter zu ernennen:

- Verarbeitungsvorgänge, welche eine regelmäßige und systematische Überwachung von betroffenen Personen in großem Umfang erforderlich machen; oder
- Die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten (z.B. Gesundheit, Religion, Rasse, sexuelle Orientierung etc.) und von Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten.
- Der Datenschutzbeauftragte muss unabhängig, zuverlässig und sachkundig sein. Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern dieser von jeder Niederlassung aus leicht erreicht werden kann. Nationale Gesetze können die Ernennung eines Datenschutzbeauftragten in weiteren Fällen erforderlich machen. Dies ist z.B. in Deutschland der Fall, wobei die nach alter Rechtslage geltenden Voraussetzungen gelockert wurden. Ein betrieblicher Datenschutzbeauftragter ist statt bei zehn oder mehr Arbeitnehmern nun grds. erst ab 20 Arbeitnehmern zu benennen (§ 38 Abs. 1 S. 1 BDSG).

1.6 Einführung von technischen und organisatorischen Sicherheitsmaßnahmen, Art. 32

Zum Schutz der verarbeiteten personenbezogenen Daten sind geeignete und dem Stand der Technik entsprechende technische und organisatorische Maßnahmen zu ergreifen.

1.7 Meldung von Verletzungen des Schutzes personenbezogener Daten, Art. 33, 34

Im Falle einer Verletzung des Schutzes personenbezogener Daten mit der Folge von Risiken für die Rechte und Freiheiten der betroffenen Person muss die Aufsichtsbehörde innerhalb von 72 Stunden nachdem das Unternehmen Kenntnis von der Verletzung erlangt hat, informiert werden; im Falle von hohen Risiken für die betroffene Person muss auch diese unverzüglich über die Verletzung informiert werden. Die Einhaltung der Meldepflicht innerhalb der gesetzlichen Frist lässt sich nur mit Hilfe eines vernünftigen internen Eskaltationsverfahrens bewerkstelligen.

1.8 Privacy by design und Privacy by default, Art. 25

Die Verarbeitungstätigkeiten jedes Unternehmens müssen so konzipiert sein, dass

- Datenschutzgrundsätze, wie etwa zur Datenminimierung, wirksam umgesetzt werden (z.B. durch Pseudonymisierung);
- Voreinstellungen vorhanden sind, die sicherstellen, dass nur solche personenbezogenen Daten verarbeitet werden, die für den jeweilig bestimmten Verarbeitungszweck erforderlich sind.

1.9 Vertreter in der EU, Art. 27

Unternehmen, die dem Anwendungsbereich der DSGVO unterfallen, aber über keine Niederlassung in der EU verfügen, müssen für behördliche Angelegenheiten einen Vertreter in der EU benennen. Der Vorteil eines solchen Vertreters: Es wird ein „one-stop-shop" für Unternehmen aus Drittländern für die Meldung von Datenschutzverstößen an die Datenschutzaufsichtsbehörde geschaffen.

Ihre Ansprechpartner

Dr. Axel Frhr. von dem Bussche, LL.M. (L.S.E.)

Tel +49 (0)40 3 68 03 347
a.bussche@taylorwessing.com

Dr. Paul Voigt, Lic. en Derecho, CIPP/E

Tel +49 (0)30 88 56 36 408
p.voigt@taylorwessing.com

2. Materielle Anforderungen an die Datenverarbeitung

2.1 Jede Verarbeitung personenbezogener Daten setzt wie bisher entweder eine wirksame Einwilligung der betroffenen Person oder eine gesetzliche Grundlage voraus.

2.2 Grenzüberschreitende Datenübermittlungen an Länder außerhalb des Europäischen Wirtschaftsraums setzen nach wie vor zusätzliche Schritte (s.o. Abschnitt 2.1) voraus, z.B. eine Zertifizierung des Empfängers nach den „EU-U.S. Privacy Shield"-Prinzipien, den Abschluss von EU-Standardvertragsklauseln, die Implementierung von „Binding Corporate Rules" oder (in eingeschränkten Fällen) eine Einwilligung.

3. Rechte der betroffenen Personen, Art. 12-23

Die Rechte der betroffenen Personen sind weitreichend. Insbesondere haben Sie die folgenden Rechte:

3.1 Informationsrechte, Art. 12-14

Den betroffenen Personen müssen transparente und weiterreichende Informationen über die Verarbeitung zur Verfügung gestellt werden.

3.2 Auskunfts-, Löschungs-, Berichtigungs- und Beschränkungsrechte, Art. 16-19

Betroffene Personen haben weitreichende Auskunftsrechte bezüglich ihrer Daten; in einigen Fällen werden sie auch das Recht haben, ihre Daten löschen oder berichtigen zu lassen oder die Beschränkung der Verarbeitungstätigkeiten zu verlangen.

3.3 Widerspruchsrecht, Art. 21-22

In einigen Fällen haben die betroffenen Personen das Recht, der Datenverarbeitung aus Gründen zu widersprechen, die sich aus ihrer besonderen Situation ergeben.

3.4 Datenübertragbarkeit, Art. 20

In begrenzten Fällen haben betroffene Personen das Recht, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu verlangen, zu erhalten und diese Daten an ein anderes Unternehmen zu übermitteln.

TaylorWessing

16 Jurisdiktionen
28 Büros
300+ Partner
1000+ Anwälte

Belgien	Brüssel
China	Peking* I Hongkong I Shanghai*
Deutschland	Berlin I Düsseldorf I Frankfurt I Hamburg I München
Frankreich	Paris
Großbritannien	Cambridge I Liverpool I London | London Tech City
Niederlande	Amsterdam I Eindhoven
Österreich	Wien I Klagenfurt*
Polen	Warschau
Slowakei	Bratislava
Südkorea	Seoul**
Tschechien	Prag I Brno*
Ukraine	Kiew
Ungarn	Budapest
USA	Silicon Valley* I New York*
VAE	Dubai

* Repräsentanzen
** Assoziierte Büros