La Kanzlei

Datenschutz in Frankreich nach der DSGVO

Datenschutz / IT

Übersicht

[1] Welche Unternehmen sind von der DSGVO betroffen?

Die Datenschutzgrundverordnung (Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016, DSGVO) ist am 25. Mai 2018 in Kraft getreten. Diese Verordnung reformiert das Datenschutzrecht, und ist in der gesamten EU direkt anwendbar.

Die DSGVO findet zum einen Anwendung, wenn die Datenverarbeitung mit einer in der Europäischen Union ausgeübten Geschäftstätigkeit verbunden ist. Zum anderen gilt sie für jedes Unternehmen, das personenbezogene Daten von EU-Bürgern verarbeitet, auch wenn dieses Unternehmen nicht in einem EU-Mitgliedsstaat ansässig ist. Damit sind sowohl internationale Unternehmen, sondern etwa auch kleine und mittelständische Unternehmen sowie Handwerker mit einer Kundenkartei betroffen. Im Ergebnis ist die weit überwiegende Mehrzahl aller in Europa tätigen Unternehmen von der Verordnung betroffen.

[2] Was sind die Ziele der DSGVO?

Mit der DSGVO werden in erster Linie folgende Ziele verfolgt:

- Europäische Vereinheitlichung der Datenschutzvorschriften. Bei der DSGVO handelt es sich um eine Verordnung, d.h. die neuen Bestimmungen sind unmittelbar anwendbar, ohne dass es hierfür einer Umsetzung durch den nationalen Gesetzgeber bedarf;
- Stärkung der Rechte der betroffenen Personen;
- Stärkere Verantwortung der Unternehmen durch Mechanismen zur Selbstkontrolle.

[3] Welche Pflichten haben die Unternehmen?

Gemäß den neuen Vorschriften müssen die betroffenen Unternehmen:

- Maßnahmen ergreifen, welche den Datenschutz durch Technikgestaltung (Art. 25.1, auch „privacy by design“ genannt) und durch datenschutzfreundliche Voreinstellungen (Art. 25.2, „privacy by default“) sicherstellen. Dies bedeutet, dass der für die Datenverarbeitung Verantwortliche den Datenschutz bereits bei der Konzeption seines Produkts oder seiner Dienstleistung gewährleisten, und datenschutzfreundliche Voreinstellungen treffen muss. Konkret bedeutet dies beispielsweise, dass er von Anfang an dafür Sorge tragen muss, dass die Menge der gesammelten/verarbeiteten Daten von Anfang an minimiert wird;
- die für eine Einhaltung der Vorschriften ergriffenen Maßnahmen dokumentieren (Art. 24);
- den Schutz personenbezogener Daten durch Umsetzung geeigneter Maßnahmen wie der Pseudonymisierung und Verschlüsselung der Daten oder der regelmäßigen Überprüfung auf technische Schwachstellen zu sichern (Art. 32);
- der Aufsichtsbehörde (in Frankreich: CNIL, in Deutschland: DSK) jede Verletzung des Schutzes personenbezogener Daten binnen einer Frist von 72 Stunden melden (Art.33) und in bestimmten Fällen sogar die hiervon betroffene Person benachrichtigen (Art. 34);
- einen Datenschutzbeauftragten benennen (nur in den nachstehend aufgelisteten Fällen obligatorisch).
- überprüfen, dass ihre Auftragsdatenverarbeiter hinreichende Garantien im Bereich des Datenschutzes bieten (vgl. Art. 28 DSGVO). Auftragsdatenverarbeitungsverträge (ADV-Verträge) müssen vor dem Stichtag an das neue Recht angepasst werden.

[4] Welche Rechte haben die betroffenen Personen?

- **Datenübertragbarkeit:** Das Recht auf Datenübertragbarkeit ermöglicht es einer Person, die sie betreffenden Daten zu erhalten oder ihre personenbezogenen Daten von einem Unternehmen an ein anderes übermitteln zu lassen (Art. 20).

- **Einwilligung:** Der für die Verarbeitung Verantwortliche muss nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Darüber hinaus ist vorgesehen, dass die betroffene Person das Recht hat, ihre Einwilligung jederzeit zu widerrufen (Art. 7 Abs. 3).

- **Recht auf „Vergessenwerden“:** Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass die sie betreffenden personenbezogenen Daten unverzüglich gelöscht werden (Art. 17). Darüber hinaus muss der Verantwortliche die Daten unaufgefordert löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind.

- **Recht auf Information**: Der Verantwortliche muss die von der Datenverarbeitung betroffenen Personen in klarer und präziser Sprache über die Verwendung ihrer Daten informieren. Die Verordnung enthält detaillierte Regelungen zu den Angaben, die hierbei zu machen sind (Art. 12).

- **Besondere Bedingungen für die Verarbeitung der Daten von Kindern**: Die Verarbeitung personenbezogener Daten von Personen unter 16 Jahren bedarf der vorherigen Zustimmung der Eltern (Art. 8).

- **Sammelklage:** Betroffene Personen haben das Recht, eine Einrichtung, Organisation oder Vereinigung zu beauftragen, in ihrem Namen eine Beschwerde bei der Aufsichtsbehörde einzureichen und Schadensersatz zu verlangen (Art. 80).

- **Einschränkung des Profiling**: Abgesehen von wenigen Ausnahmen ist das „Profiling“ ohne die Einwilligung der betreffenden Person verboten (Art. 22).

5 Welche Vorkehrungen sieht die DSGVO vor?

Die DSGVO sieht weiter einige Vorkehrungen vor, die den Unternehmen bei der Einhaltung Ihrer Pflichten helfen sollen.

- Das Führen eines Verzeichnisses aller vorgenommenen Verarbeitungstätigkeiten (Art. 30; in den meisten Fällen obligatorisch);
- Zertifizierungsverfahren (Art. 42 und 43);
- Ausarbeitung und Einhaltung von Verhaltensregeln, sog. „best practices“ (Art. 40 und 41);
- Einsetzung eines Datenschutzbeauftragten (Art. 37 bis 39; nur in bestimmten Fällen obligatorisch);
- Durchführung einer Datenschutz-Folgenabschätzung für Datenverarbeitungsvorgänge mit hohem Risiko (Art. 35 und 36, obligatorisch).

6 Benötige ich einen Datenschutzbeauftragten und was sind seine Aufgaben?

Dem Datenschutzbeauftragten (engl. Data Protection Officer, frz. Délégué à la protection des données) kommt nach der DSGVO bei der eine strategische Funktion zu. Im Vergleich zu dem Datenschutzbeauftragten nach bisherigem Recht hat er weitergehende Rechte und Pflichten.

In welchen Fällen muss ein Datenschutzbeauftragter eingesetzt werden?

Gemäß Artikel 37 DSGVO ist die Ernennung eines Datenschutzbeauftragten (DPO) in den drei folgenden Fällen verpflichtend:

- Die Verarbeitung wird von einer Behörde oder öffentlichen Stelle durchgeführt.
- Die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters macht (aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke) eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich.
- Die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters besteht in der umfangreichen Verarbeitung von besonderen Kategorien von Daten (sog. „sensible Daten“). Als „sensible Daten“ gelten insbesondere genetische und biometrische Daten, Gesundheitsdaten, Daten zur Religionszugehörigkeit, zur politischen Meinung, zur Gewerkschaftszugehörigkeit, zur sexuellen Orientierung und zu strafrechtlichen Verurteilungen und Straftaten.

Zu diesem Punkt bestehen Öffnungsklauseln. Damit haben die Mitgliedsstaaten die Möglichkeit, zusätzliche Fälle festzulegen, in denen ein DPO ernannt werden muss. In Deutschland sind privatwirtschaftliche Unternehmen in folgenden Fällen ebenfalls zur Ernennung eines Datenschutzbeauftragten verpflichtet (§ 38 Abs. 1 BDSG-neu):

- Wenn mehr als 9 Beschäftigte mit der automatisierten Verarbeitung personenbezogener Daten betraut sind;
- wenn mehr als 20 Beschäftigte mithilfe anderer Mittel personenbezogene Daten verarbeiten;
- wenn die Verarbeitung Gegenstand einer vorherigen Kontrolle ist oder
- wenn die Verarbeitung zwecks Übermittlung der Daten an Dritte oder im Rahmen von Meinungsumfragen erfolgt.

Darüber hinaus ist es stets möglich (und häufig auch ratsam) freiwillig einen Datenschutzbeauftragten zu ernennen.

Was sind die Aufgaben des Datenschutzbeauftragten?

Die Hauptaufgabe des Datenschutzbeauftragten besteht darin, dem Unternehmen dabei zu helfen, die Vorschriften der DSGVO einzuhalten.

Zu seinen wesentlichen Aufgaben gehören:

- Die Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und ihrer Mitarbeiter;
- die Überwachung der Einhaltung der anwendbaren Datenschutzvorschriften;
- die Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter;
- die Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und die Überwachung ihrer Durchführung;
- die Zusammenarbeit mit den zuständigen Aufsichtsbehörden;
- die Durchführung von Datenschutz-Audits.

Wie wird der Datenschutzbeauftragte ernannt?

Der Datenschutzbeauftragte wird von den Unternehmen intern bestimmt und eingesetzt. Dabei sollte ihm ein klar umrissener Aufgabenbereich zugeordnet werden, insbesondere falls mehrere Datenschutzbeauftragte eingesetzt werden sollen.

Die Artikel 37 und 38 der DSGVO stellen folgende Anforderungen an die Ernennung des Datenschutzbeauftragten:

- Der DPO muss „auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens […], das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung [seiner] Aufgaben“ ausgewählt werden.
- Er muss seine Aufgaben und Pflichten in völliger Unabhängigkeit erfüllen können und darf sich nicht aufgrund anderer Pflichten in einem Interessenkonflikt befinden: Das bedeutet, dass er innerhalb der Einrichtung keinen Posten besetzen darf, im Rahmen dessen er die Zwecke und Mittel der Datenverarbeitung bestimmt.
- Bei dem Datenschutzbeauftragten kann es sich sowohl um eine unternehmensinterne Person als auch um einen Dritten handeln. Daher können beispielsweise auch externe Rechtsanwälte oder Kanzleien mit dieser Aufgabe betraut werden.

Nach seiner Ernennung muss der DPO der zuständigen Behörde angezeigt werden.

Ein Konzern kann einen gemeinsamen Datenschutzbeauftragten ernennen, sofern dieser für alle Tochterunternehmen und Betriebe leicht zu erreichen ist. Es obliegt dem für die Verarbeitung Verantwortlichen, sich zu vergewissern, dass der gemeinsame Datenschutzbeauftragte in der Lage ist, die ihm zufallenden Aufgaben tatsächlich zu erfüllen. Es kann daher ratsam sein, einen Datenschutzbeauftragten pro Land zu ernennen, insbesondere um die Zusammenarbeit mit den unterschiedlichen nationalen Aufsichtsbehörde zu erleichtern.

7 Wie kann ich die DSGVO konkret umsetzen?

Die französische Datenschutzbehörde CNIL hat sechs Schritte definiert, die Unternehmen helfen müssen, die DSGVO umzusetzen.

Schritt 1: Benennung eines „Lotsen“ (Datenschutzbeauftragter oder Angestellte / externe Berater, die mit dem Datenschutz betraut werden), der die organisatorische Leitung für die Anpassung an die Vorschriften der DSGVO übernimmt.

Schritt 2: Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten (VVT), d.h. Erfassung und detaillierte Auflistung aller bestehenden Datenverarbeitungsvorgänge im Unternehmen

Schritt 3: Identifizierung und Priorisierung der Handlungen, die für eine Einhaltung der DSGVO vorzunehmen sind: Sobald Sie die Verarbeitungsprozesse für personenbezogene Daten in Ihrem Unternehmen identifiziert haben (vgl. Schritt 2), müssen Sie für jeden von ihnen die Maßnahmen identifizieren, die zur Erfüllung der gegenwärtigen und künftigen Verpflichtungen zu ergreifen sind. Diese Priorisierung kann im Lichte der Risiken erfolgen, die Ihre Verarbeitungsprozesse für die Freiheiten der betroffenen Personen bergen. Einige Aufgaben sind einfach zu implementieren und ermöglichen Ihnen schnelle Fortschritte.

Schritt 4: Beherrschung der Risiken durch Vornahme einer gegebenenfalls erforderlichen Datenschutz-Folgenabschätzung.

Schritt 5: Einführung interner Verfahren, die „eine jederzeitige Berücksichtigung des Datenschutzes gewährleisten, indem sie allen Ereignissen Rechnung tragen, die im Verlaufe einer Verarbeitung auftreten können“ (z.B. Interne Verfahren zur Aufdeckung und Behebung von Sicherheitslücken, zur Verwaltung von Anfragen der Nutzer auf Berichtigung oder und Änderung der Daten oder über den Zugang zu den personenbezogenen Daten, Verfahren im Falle des Wechsels des Diensteanbieters).

Schritt 6: Dokumentierung der zur Einhaltung der Vorschriften ergriffenen Maßnahmen.

In Deutschland hat die DSK einen Maßnahmenplan "DS-GVO" für Unternehmen veröffentlicht. Dieses Kurzpapier der DSK soll als erste Orientierung dienen, wie die DSGVO im praktischen Vollzug angewendet werden sollte.

8 Welche Strafen drohen bei Verstößen gegen die DSGVO?

- **Schadensersatzanspruch der betroffenen Personen:** Jede Person, der wegen eines Verstoßes gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

- **Verwaltungsrechtliche Sanktionen:** Bei Verstoß gegen die DSGVO können die Datenschutzbehörden insbesondere Folgendes tun:
  - Eine Verwarnung aussprechen;
  - das Unternehmen abmahnen;
  - die Datenverarbeitung vorübergehend oder endgültig einschränken;
  - die Übermittlung der Daten aussetzen;
  - den Verantwortlichen oder den Auftragsverarbeiter anweisen, den Anträgen der Personen auf Ausübung der ihr zustehenden Rechte zu entsprechen;
  - die Berichtigung oder Löschung der Daten oder die Einschränkung der Verarbeitung anordnen.

- **Geldbußen** verhängen, deren Höhe sich nach Art und Schwere des Verstoßes richtet:
  - bei leichteren Verstößen, insbesondere im Falle eines Verstoßes gegen die von den Artikeln 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43 vorgesehenen Pflichten: Geldbußen von bis zu 10 Millionen Euro oder von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher der Beträge höher ist
  - bei schweren Verstößen, insbesondere im Falle eines Verstoßes gegen die von den Artikeln 5, 6, 7, 9, 12 bis 22, 44 bis 49, 58 und Kapitel IX vorgesehenen Pflichten: Geldbußen in Höhe von bis zu 20 Millionen Euro oder von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher der Beträge höher ist.

La Kanzlei

2020-01-01

Qivive
Rechtsanwalts GmbH

qivive.com

Köln[D]

Konrad-Adenauer-Ufer 71
D – 50668 Köln
T + 49 (0) 221 139 96 96 - 0
F + 49 (0) 221 139 96 96 - 69
koeln@qivive.com

Paris[F]

50 avenue Marceau
F – 75008 Paris
T + 33 (0) 1 81 51 65 58
F + 33 (0) 1 81 51 65 59
paris@qivive.com

Lyon[F]

10 –12 boulevard Vivier Merle
F – 69003 Lyon
T + 33 (0) 4 27 46 51 50
F + 33 (0) 4 27 46 51 51
lyon@qivive.com