Checkliste

EU-Datenschutz-Grundverordnung 2018

Überblick: Das müssen Sie bis zum 25. Mai 2018 erledigen.

Business Software Europe UG

cobra CRM

schneller erfolgreich

Checkliste

Datenschutzgrundverordnung (DSGVO)

Nach Inkrafttreten der DSGVO im Jahr 2016 ist diese ab dem **25.05.2018 wirksam** und europaweit unmittelbar anwendbar. Aufgrund der in Artikel 83 und 84 DSGVO geregelten und enorm angestiegenen **Geldbußen** ist eine rechtzeitige Anpassung an die neuen Vorschriften unbedingt zu empfehlen.

Diese Checkliste soll Ihnen und Ihrem Unternehmen helfen, nachzuvollziehen, ob Sie auf die wichtigsten Änderungen der DSGVO vorbereitet sind.

Prozesse dokumentieren

Nur wenn klar ist, bei welchen Prozessen und auf welche Art und Weise in einem Unternehmen personenbezogene Daten verarbeitet werden, können alle notwendigen Änderungen umgesetzt werden. Diese Dokumentation ist auch zur Erfüllung der Rechenschaftspflicht nach Artikel 5 Abs. 2 DSGVO notwendig

Da auf nationaler Ebene abweichende Regelungen existieren können, empfiehlt es sich, die Auflistung nach Ländern zu unterteilen (Deutschland, EU-Mitgliedsstaaten, Drittländer).

Sofern noch nicht vorhanden, muss im Anschluss nach Artikel 30 Abs. 1 DSGVO ein Verfahrensverzeichnis angelegt werden.

Dieses muss insbesondere die folgenden Angaben enthalten:

- ☐ den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen 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 Drittländern oder internationalen Organisationen
- ☐ gegenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
- ☐ wenn möglich, die vorgesehenen Fristen für die Löschung der technischen und organisatorischen Maßnahmen (TOMs)

Diese Checkliste soll einen ersten Überblick über die wichtigsten Anforderungen der DSGVO geben. Sie stellt keine Rechtsberatung dar und kann auch keine Rechtsberatung ersetzen.

Abweichungen feststellen

Nur nachdem alle datenschutzrechtlich relevanten Prozesse dokumentiert wurden, kann festgestellt werden, wo Abweichungen zwischen den aktuellen Prozessen und den neuen gesetzlichen Anforderungen liegen.

Auch hier empfiehlt es sich, wegen unterschiedlicher nationaler Regelungen, nach einzelnen Ländern zu unterscheiden.

- ☐ Deutschland (DSGVO, sonstige Verordnungen und Richtlinien, BDSG n.F., TMG TKG)
- ☐ EU-Mitgliedsstaaten (DSGVO, sonstige Verordnungen und Richtlinien, nationale Gesetze)
- ☐ Drittländer (Internationale Abkommen, DSGVO, sonstige Verördnungen und Richtlinien, nationale Gesetze)

Insbesondere müssen dabei die bei den folgenden Punkten entstandenen Neuerungen durch die DSGVO beachtet werden:

- ☐ Grundsätze und Rechtmäßigkeit der Verarbeitung (Artikel 5,6 DSGVO)
- ☐ Prozess der Einwilligung (Artikel 7,8 DSGVO)
- ☐ Betroffenenrechte, Informationspflichten, Datenschutzerklärung (Artikel 12 ff. DSGVO)
- ☐ Privacy as design, privacy by default (Artikel 25 DSGVO)
- ☐ TOMs (Artikel 32 DSGVO)
- ☐ Meldepflichten bei Datenpannen (Artikel 33,34 DSGVO)
- ☐ Datenschutz-Folgenabschätzung (Artikel 35, 36 DSGVO)

Datenschutzbeauftragter

Grundsätzlich muss in den Fällen des Artikel 37 Abs. 1 DSGVO ein Datenschutzbeauftragterbestellt werden. Artikel 37 Abs. 4 DSGVO enthält eine Öffnungsklausel, von der auf nationaler Ebene durch § 38 BDSG n.F. Gebrauch gemacht wurde. Hierdurch werden die Regelungen der DSGVO ergänzt.

Danach muss ein Datenschutzbeauftragter in Deutschland immer dann bestellt werden, wenn

- ☐ die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich nachen
- ☐ die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kateforien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht
- ☐ in einem Unternehmen in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind
- ☐ der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung unterliegen oder
- ☐ der Verantwortliche oder der Auftragsverarbeiter personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung verarbeiten

Alle anderen Unternehmen können freiwillig einen Datenschutzbeauftragten bestellen.

Nach Artikel 37 Abs. 2 DSGVO ist es mitunter möglich, für mehrere Niederlassungen eines Unternehmens nur einen Datenschutzbeauftragten zu bestellen.

Die Rechte und Pflichten eines Datenschutzbeauftragten folgen aus Artikel 38, 39 DSGVO. Er darf und muss insbesondere:

- ☐ frühzeitig in Verarbeitungsvorgänge eingebunden werden
- ☐ durch den Verantwortlichen und Auftragsverarbeiter unterstützt werden
- ☐ nicht an Weisungen gebunden sein
- ☐ für Fragen betroffener Personen zur Verfügung stehen und vertraulich arbeiten
- ☐ Schulungen durchführen
- ☐ die Einhaltung des Datenschutzrechts überwachen
- ☐ bei der Datenschutz-Folgenabschätzung beraten
- ☐ mit Aufsichtsbehörden zusammenarbeiten

Auftragsverarbeitung

Wenn personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet werden (Bsp.: Outsourcing, Cloud Computing, Hosting, IT-Support), liegt eine Auftragsverarbeitung vor. Deren Zulässigkeit richtet sich nach Artikel 27-30 DSGVO. Daraus folgt, dass bestehende „Auftragsdatenverarbeitungsverträge“ überarbeitet oder umbenannt und außerdem auch bei neuen Auftragsverarbeitungsverträgen vor allen Dingen folgende Änderungen berücksichtigt werden müssen:

- ☐ ggf. Bestellung eines Vertreters
- ☐ Garantie für geeignete TOMs und Einhaltung des Datenschutzrechts
- ☐ notwendige Angaben und Mindestanforderungen des Auftragsverarbeitungsvertrages
- ☐ Führen eines Verfahrensverzeichnisses durch den Auftragsverarbeiter

Übermittlung in Drittländer

Bei der Übermittlung personenbezogener Daten in Länder außerhalb der EU müssen neben den allgemeinen Vorschriften für die Datenverarbeitung zusätzlich die Artikel 44 ff. DSGVO beachtet werden. Typische Fälle sind insbesondere

- ☐ Outsourcing
- ☐ Kommunikation in internationalen Konzernen
- ☐ Cloud-Dienste

Die Übermittlung ist dabei nur zulässig, wenn

- ☐ die EU-Kommission ein angemessenes Schutzniveau im Drittland festgestellt hat (bspw. Aufgrund bestehender Abkommen, wie dem Privacy Shield mit den USA)
- ☐ sonstige Garantien vorliegen (rechtlich bindende Vereinbarungen oder Dokumente)
- ☐ Standardschutzklauseln verwendet werden oder
- ☐ Zertifizierungen nach Artikel 42 DSGVO vorliegen