IHK München und Oberbayern

MERKBLATT

Checkliste Sachverständige Datenschutz

EU-Datenschutzgrundverordnung – Checkliste für Sachverständige

Checkliste

1. Gilt die EU-Datenschutzgrundverordnung auch für meine Sachverständigentätigkeit?

Ja. Jeder, der personenbezogene Daten verarbeitet, muss die Vorgaben der EU-DSGVO und die ergänzenden bundes- und landesdatenschutzrechtlichen Regelungen beachten. Personenbezogen sind alle Informationen über eine identifizierte oder identifizierbare Person. Verarbeiten bedeutet erheben, erfassen, organisieren, ordnen, speichern, anpassen, verändern, abfragen, verwenden, offenlegen, übermitteln, verbreiten, bereitstellen, abgleichen, verknüpfen, löschen, vernichten.

2. Wann darf ich welche Daten verarbeiten?

Für jede Datenverarbeitung muss eine Rechtsgrundlage gegeben sein. Es gibt gem. Art. 6 DSGVO folgende Rechtsgründe:

- rechtliche Verpflichtung (z.B.: aufgrund eines Gesetzes oder der Sachverständigenordnung)
- für die (vor-)vertragliche Abwicklung erforderlich (z.B. relevant für Privatgutachten)
- Wahrung berechtigter Interessen des Sachverständigen (hier müssen Sie eine Interessenabwägung vornehmen)
- zweckgebundene, persönliche Einwilligung des Betroffenen (kommt in Betracht, wenn keiner der vorstehenden Fälle vorliegt).

Es dürfen immer nur zweckgerichtete Informationen verarbeitet werden – so viele Daten wie nötig, so wenige wie möglich. Beispiel: Für die Erfüllung eines privaten Sachverständigenvertrages dürfte das Geburtsdatum des Auftraggebers nicht relevant sein.

Schalten Sie bei der Datenverarbeitung externe Dienstleister ein und liegen die Voraussetzungen einer sog. Auftragsverarbeitung vor, müssen Sie mit dem Dienstleister einen Vertrag über die Auftragsverarbeitung abschließen. Dieser muss die in Art. 28 DSGVO genannten Bestandteile enthalten. Für Ihre regelmäßig auftretenden Verarbeitungsvorgänge müssen Sie ein Verarbeitungsverzeichnis anlegen, in dem Sie die Art der Tätigkeiten, der Zweck und die Rechtsgrundlage, die Art der Daten, die Empfänger, die Löschfristen sowie die technischen und organisatorischen Schutzmaßnehmen beschreiben.

3. Wie lange darf/muss ich die Daten aufbewahren?

Je nach Zweck und Rechtsgrundlage unterschiedlich, spätestens aber, sobald der Zweck der Speicherung weggefallen ist. Bei Verträgen ist dies z. B. die Verjährungsfrist von Ansprüchen, bei der Einwilligung insbesondere der Widerruf. Zu beachten sind Aufbewahrungspflichten aus dem Steuerrecht oder den Sachverständigenordnungen.

4. Welche Rechte haben Betroffene?

- Transparente Information über Verarbeitung (Ausnahme: der Betroffene verfügt bereits über die Information oder sie stellt einen unverhältnismäßigen Aufwand dar)
- Recht auf Datenauskunft
- Recht auf Datenberichtigung
- Recht auf Datenlöschung
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit

5. Brauche ich einen Datenschutzbeauftragten?

Das kommt insbesondere auf die Zahl der mit der Datenverarbeitung befassten Mitarbeiter im Sachverständigenbüro an. Wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ist ein Datenschutzbeauftragter zu bestellen (§ 38 BDSG). Weitere Gründe ergeben sich aus Art 37 DSGVO (s. hierzu Informationsblatt unter www.lda.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf).

6. Was passiert, wenn ich die Vorgaben der DSGVO nicht einhalte?

Dann drohen Bußgelder von bis zu € 20.000.000, bzw. bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs und ggf. wettbewerbsrechtliche Abmahnungen. Bei Kleinunternehmen und geringen Verstößen könnte die Datenschutzbehörde das Prinzip „Beratung vor Bestrafung“ anwenden. Im Übrigen muss das Bußgeld zwar abschreckend, aber auch verhältnismäßig sein und berücksichtigt z.B. die Schwere des Verstoßes (Art. 83 DSGVO).

To-Do-Liste

1. Bestandsaufnahme

- Wer verarbeitet wie welche Daten zu welchem Zweck?
- Sind mindestens 10 Mitarbeiter in meinem Büro regelmäßig mit der automatisierten Datenverarbeitung befasst?
- Gibt es für jeden Datenverarbeitungsvorgang eine Rechtsgrundlage gem. Art. 6 DSGVO (z. B. Einwilligung, Vertragserfüllung, Rechtliche Verpflichtung)?
- Habe ich alle Datenverarbeitungsprozesse in einem Verfahrensverzeichnis erfasst?
- Verfüge ich über eine ausreichende Dokumentation meiner Datenverarbeitungsprozesse inkl. Löschmanagement und Umgang mit Datenschutzverletzungen?

- Erfülle ich die erforderlichen technischen und organisatorischen Maßnahmen (TOM), um einen sicheren Datenschutz zu gewährleisten?
- Habe ich auf meiner Webseite einen ausreichenden Datenschutzhinweis?
- Ist meine IT ausreichend gesichert und werden die erforderlichen praktischen Sicherungsmaßnahmen im Büro eingehalten (Verschluss von Personaldaten, passwortgeschützter Zugang zu den Arbeitsrechnern, Bildschirmschoner, Firewall, etc.)?
- Gebe ich Daten an Dritte weiter, die diese verarbeiten (z. B. IT-Dienstleister, Versender)?

2. Umsetzungsmaßnahmen

- Bestimmung eines internen Datenschutzkoordinators und/oder ggf. eines Datenschutzbeauftragten
- Erstellung eines Verarbeitungsverzeichnisses (Muster unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf) inkl. Darstellung der Rechtsgrundlagen und ergänzenden Dokumentationen, Löschkonzepten und Umgang mit Datenschutzverletzungen (s. hierzu die Hinweise unter www.lda.bayern.de/media/dsk_hinweise_vov.pdf)
- Sicherheitsstandards checken (IT) und ggf. anpassen
- Datenschutzhinweise erstellen und ggf. auf Webseite einstellen (auch an Cookie-Hinweise denken)
- IT-Sicherheit sicherstellen (z. B. https, etc.)
- Zugangsberechtigungen prüfen (z. B. Personalunterlagen verschließen, passwortgeschützter Zugang zu den Arbeitsrechnern, Bildschirmschoner, etc.)
- Bei Weitergabe der verarbeiteten Daten an Dritte: Auftragsdatenverarbeitung (ADV-Verträge) abschließen (z. B. Webdienstleister); Muster unter www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf

Hilfreich ist auch die Checkliste unter www.lda.bayern.de/media/dsgvo_fragebogen.pdf. Weitere Auskünfte erteilen Fachverbände und -organisationen.

Hinweis:
Dieses Merkblatt dient als erste Orientierungshilfe und erhebt keinen Anspruch auf Vollständigkeit. Obwohl es mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden. Die Veröffentlichung von Merkblättern ist ein Service der Industrie- und Handelskammer und kann eine Rechtsberatung im Einzelfall nicht ersetzen.

IHK für München und Oberbayern
Ihr Kontakt: Johann Petras, Stefanie Seidl, Mirjami Wirth
Stand: August 2023