Stand: Januar 2024

EU-Datenschutzgrundverordnung - Checkliste für Sachverständige

1. Gilt die EU-Datenschutzgrundverordnung auch für meine Sachverständigentätigkeit?
Ja. Jeder, der personenbezogene Daten verarbeitet, muss die Vorgaben der EU-DSGVO und darüber hinaus insbesondere die des Bundesdatenschutzgesetzes (BDSG) 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)
- Vertrag mit dem Auftraggeber für die (vor-)vertragliche Abwicklung (z. B. relevant für Privatgutachten – andernfalls könnten Sie den Auftrag nicht erfüllen)
- Wahrung berechtigter Interessen des Sachverständigen (hier müssen Sie eine Interessenabwägung vornehmen – schwierig zu begründen und daher nicht ohne vorherige Beratung durch einen Datenschutzbeauftragten zu empfehlen)
- zweckgebundene, persönliche Einwilligung des Betroffenen (kommt in Betracht, wenn keiner der vorstehenden Fälle vorliegt). Hier ist in der Regel eine sog. "informierte Einwilligung“ erforderlich. Das bedeutet, dass Sie den Dateninhaber über Art und Zweck der Datenverarbeitung sowie über die Widerrufsmöglicheit und deren Folgen vorher informieren müssen, z.B. beim Anfertigen von Fotos auf einer Vortragsveranstaltung, bei der einzelne Personen identifizierbar sind.

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. Ebenso wenig das PKW-Kennzeichen auf sorglos gemachten Fotos in Gutachten.
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, zum Beispiel die Speicherung von Gutachten auf Ihrem PC oder bei externen Dienstleistern (Achtung: dann auch Auftragsverarbeitung prüfen!) müssen Sie ein sog. Verarbeitungsverzeichnis anlegen, in dem Sie die Art der Tätigkeiten, den Zweck und die Rechtsgrundlage, die Art der Daten, die Empfänger, die Löschfristen sowie die technischen und organisatorischen Schutzmaßnahmen 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. Diese betragen in der Regel 10 Jahre und beginnen mit dem Schluss des Kalenderjahres, in dem die Aufzeichnungen zu machen oder die Unterlagen entstanden sind.

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 zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ist ein Datenschutzbeauftragter zu bestellen (§ 38 BDSG). Dies kann sowohl ein Externer als auch ein Mitarbeiter sein, sofern kein Interessenkonflikt zwischen Amt und Tätigkeit besteht (in der Regel darf dies niemand mit Personalverantwortung oder aus der IT sein).

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 welchen Daten zu welchem Zweck?
- Sind mindestens 20 Mitarbeiter in meinem Büro regelmäßig mit der automatisierten Datenverarbeitung befasst (PC-Arbeitsplatz reicht aus!)?
- 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 oder externen 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 Cookiehinweise 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 (z. B. Webdienstleister): Auftragsverarbeitung abschließen (z. B. https://www.lda.bayern.de/media/muster/formulierungshilfe_av.pdf)