Wichtige Mandanteninformation zur Datenschutzgrundverordnung
-Inkrafttreten am 25.05.2018-

Allgemeines kurz dargestellt

Nach Ende der zweijährigen Übergangsfrist (Anpassung des nationalen Datenschutzrechts an die EU-Verordnung) verschärfen sich **ab dem 25. Mai 2018** (übrigens in sämtlichen EU-Mitgliedsstaaten) unmittelbar die Vorschriften (EU-Datenschutz-Grundverordnung; kurz: DSGVO) rund um den Datenschutz ohne Ausnahme **für alle Unternehmen**. Wichtige Hinweise, Aktuelles und Arbeitshilfen finden Sie auch unter www.gdd.de.

Datenschutz dient dem **Schutz personenbezogener Daten** bei deren automatisierter Verarbeitung. Unter personenbezogenen Daten versteht man Informationen über (lebende) natürliche Personen; Unternehmensgeheimnisse oder Daten juristischer Personen werden vom Datenschutz nicht erfasst. Personenbezogen ist **jede Information**, die sich auf einen lebenden Menschen beziehen lässt.

Schnittmengen bestehen zwischen dem Schutz personenbezogener Daten i. S. des Datenschutzgesetzes sowie unserer Berufspflicht zur Verschwiegenheit i. S. d. Steuerberatergesetzes und auch mit Themen der IT-Sicherheit; jedoch besteht keine Deckungsgleichheit.

Personenbezogene Daten dürfen grundsätzlich nur auf gesetzlicher Grundlage oder mit Einwilligung des Betroffenen verarbeitet werden (umfassendes Verbot mit Erlaubnisvorbehalt). Das Datenschutzrecht fordert damit materiell zwingend für jeden Vorgang der Verarbeitung personenbezogener Daten, ob EDV-gestützt oder in Dateiform, eine Rechtsgrundlage oder eine (den rechtlichen Anforderungen entsprechende) wirksame Einwilligung des Betroffenen.

Wird die Verarbeitung personenbezogener Daten Dritten übertragen (sog. Auftragsverarbeitung), bleibt der Auftraggeber datenschutzrechtlich verantwortlich (z. B. Sie beauftragen uns mit der Erstellung der Lohnabrechnung für Ihre Beschäftigten; ein Fachunternehmen wird von Ihnen mit der Aktenvernichtung beauftragt).

Konkrete Erfordernisse, notwendige Vorbereitungen im Überblick (keine Gewähr für Vollständigkeit)

1. Datenschutzbeauftragter (DSB)

   - zwingend zu bestellen, wenn mehr als 10 Personen Zugang zur EDV besitzen (auch bei Unterschreiten dieser Grenze zu empfehlen, externer DSB ist empfehlenswert)
   - muss beruflich und fachlich qualifiziert für diese Aufgabe sein
   - muss bei Bestellung der Aufsichtsbehörde gemeldet werden

2. Rechtsgrundlagen der Datenverarbeitung

   - nach Art. 6 Abs. 1 DSGVO ist die Verarbeitung personenbezogener Daten nur dann rechtmäßig, wenn
     a) der Betroffene in die Verarbeitung eingewilligt hat

b) die Verarbeitung für die Vertragserfüllung/Beantwortung von Anfragen des Betroffenen notwendig ist
c) Rechtspflicht zur Datenverarbeitung besteht
d) lebenswichtige Interessen des Betroffenen oder anderer Menschen durch die Datenverarbeitung geschützt werden müssen oder
e) berechtigte Interessen an der Verarbeitung bestehen, solange Interessen des Betroffenen nicht überwiegen

3. Technische und organisatorische Maßnahmen (TOM)

- Beeinträchtigungen und Risiken für die Betroffenen sind auf ein Mindestausmaß zu beschränken
- Prinzipien z. B. Pseudonimisierung und Datensparsamkeit
- Empfehlung: verbindliche Festlegung in einer Datenschutz-Anweisung oder im Organisationshandbuch treffen
- Maßnahmen treffen gegen z. B.
  a) unbefugten Zutritt Dritter
  b) unbefugten Datenzugriff (abschließbare Schränke/Rollcontainer; Passwortabfragen und Berechtigungskonzepte an EDV-Arbeitsplätzen)
  c) keine Vermischung privater und dienstlicher E-Mails
  d) Löschung nicht mehr benötigter Daten
  e) verschlüsselte E-Mail-Kommunikation
- keine Aussagekraft über die Erfüllung der Datenschutzanforderungen (i. S. d. DS-GVO) besitzen die gängigen Zertifizierungen nach DIN ISO
-

4. Verzeichnisse von Verarbeitungstätigkeiten

- Vorgeschrieben für sämtliche Verarbeitungstätigkeiten; Inhalt: Zweck der Datenverarbeitung im Unternehmen, die Personen- und Datenkategorien, Übermittlungsvorgänge und Löschfristen sowie eine Beschreibung der getroffenen TOM (Art. 30 DS-GVO)

⇨ **Alle dauerhaft anfallenden Arbeitsabläufe, die mit der Verarbeitung personenbezogener Daten verbunden sind, müssen entsprechend dokumentiert werden!** (damit greift die Erleichterung gem. Art. 30 Abs. 5 DS-GVO für Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, eher selten)

5. Folgenabschätzung

- Erforderlich, wenn sich aus Datenverarbeitungen ein hohes Risiko für Rechte und Freiheiten natürlicher Personen ergeben kann (z. B. Einsatz umfassender Personalverwaltungssoftware)
- Identifizierung und Prüfung der bestehenden Risiken und Möglichkeiten zur Reduzierung dieser
- Ergebnis ist die dokumentationspflichtige Entscheidung der Unternehmensleitung, ob die Verarbeitung durchgeführt wird und welche TOM zur Risikominimierung bzw. –beseitigung zu treffen sind

6. Auftragsverarbeitung

   - Beispiel: Archivierung, Datenträgervernichtung wir an einen Dienstleister outgesourct
   - Dokumentation der Prüfung des Dienstleisters vor Beauftragung sowie der getroffenen datenschutzrelevanten Vereinbarungen und der (gesetzlich vorgeschriebenen) laufenden Kontrollen des Auftragsverarbeiters

7. Schulungen und Dokumentation

   - gesetzlich vorgeschriebene feste Intervalle
   - Dokumentation der durchgeführten Schulungsmaßnahmen

8. Sicherstellung der Betroffenenrechte

   - Betroffene haben Anspruch auf Auskunft über die entsprechend verarbeiteten Daten, auf Information bei deren Erhebung und Übermittlung an Dritte sowie ggf. auf Korrektur/Löschung
   - Empfehlung: Einführung feststehender Abläufe, dokumentiert in einer allg. Datenschutz- bzw. Organisationsanweisung

9. Datenschutzaufsicht

   - künftig verstärkte Prüfung der Einhaltung der Datenschutzvorgaben in automatisierter Form (z. B. Einhaltung der rechtlichen Vorgaben bei der Gestaltung einer Internetseite)
   - formularmäßige Anfragen zum Stand der Umsetzung der Datenschutzgesetze
   - Meldepflicht bei Datenpannen innerhalb von 72 Stunden
   - Sanktionen können erfolgen in Form von Bußgeldern, Klagen auf Unterlassung und Schadenersatz

Die Vorschriften zum Datenschutz bei automatisierter Verarbeitung personenbezogener Daten sind im BDSG (Bundesdatenschutzgesetz) sowie in der DS-GVO geregelt.