EU-Datenschutz-Grundverordnung (DSGVO): Pflichten des Auftragsverarbeiters

Wofür ist der Auftragsverarbeiter haftbar?

Überblick

Mit der DSGVO wurde der Begriff des **datenschutzrechtlichen Dienstleisters** auf „**Auftragsverarbeiter**" geändert. Dieser wird definiert als eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Beispiele: Cloud-Dienste-Anbieter, Newsletter-Management-Anbieter und IT-Datenwartungsanbieter). Steuerberater sind nach einer neusten Entscheidung der Datenschutzbehörde keine Auftragsverarbeiter).

Ein datenschutzrechtliches Auftragsverarbeiterverhältnis ist nicht mit einem zivilrechtlichen Auftrag gleichzusetzen, z.B. erhält ein Handwerksbetrieb von der Hausverwaltung personenbezogene Daten wie Name und Adresse der Wohnungsmieter, um eine Reparatur in deren Wohnung durchführen zu können, liegt zwar zivilrechtlich ein Werkvertrag vor, datenschutzrechtlich ist das allerdings nicht als Auftragsverarbeitung zu werten. Die personenbezogenen Daten werden in diesem Fall nur weitergeben um den eigentlichen Auftrag (= Reparatur in der Wohnung) durchführen zu können. Die Datenverarbeitung ist hier nur als Nebenaspekt zu sehen. Der Handwerksbetrieb ist daher kein Auftragsverarbeiter.

Die Datenverarbeitung durch einen Auftragsverarbeiter muss im Interesse des Verantwortlichen erfolgen, dh der Auftragsverarbeiter ist als „verlängerter Arm" des „Herrn der Daten" (= Verantwortlicher) zu sehen.

> **Beispiel**:
> Der Verkauf einer Datenverarbeitungsanlage (z.B. Software) ist datenschutzrechtlich nicht als Auftragsverarbeitung zu qualifizieren.
>
> Wird aber eine Datenwartung bzw ein Support zum Verkauf der Software vereinbart, kann in diesem Fall eine Auftragsverarbeitung vorliegen, wenn der Support-Anbieter auf die Daten Zugriff nehmen kann.

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Pflichten

Allgemein:

- Er muss **Datensicherheitsmaßnahmen** implementieren. (Siehe dazu „Datensicherheit und privacy by design/privacy by default").
- Jeder Auftragsverarbeiter (und seine Vertreter) führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.
- Er ist verpflichtet mit der Aufsichtsbehörde auf Anfrage **zusammen zu arbeiten**.
- Der Auftragsverarbeiter hat **Risikoanalysen** der Datenanwendungen durchzuführen und den Verantwortlichen bei Erfüllung seiner Pflichten nach der DSGVO zu unterstützen.
- Es ist ein **Datenschutzbeauftragter** verpflichtend zu bestellen, wenn die Kerntätigkeit des Unternehmers eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht oder in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht.

Sub-Auftragsverarbeiter

Der Auftragsverarbeiter darf keinen weiteren Auftragsverarbeiter (Subunternehmer) ohne **vorherige schriftliche Genehmigung des Verantwortlichen** beauftragen. Liegt nur eine allgemeine schriftliche Genehmigung vor, muss der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte **Änderung** in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informieren. Der Verantwortliche hat die Möglichkeit, gegen derartige Änderungen **Einspruch** zu erheben.

Weiters hat er ebenso wie der Verantwortliche auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen zu arbeiten.

Vertragliche Bindung

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt **auf der Grundlage eines Vertrags**. Dieser kann auf Standardvertragsklauseln beruhen, welche entweder die Europäische Kommission oder die Aufsichtsbehörde festlegen kann. Der Vertrag ist schriftlich abzuschließen, wobei elektronisch auch als schriftlich gilt und hat Folgendes zu beinhalten:

- Bindung an den Verantwortlichen,
- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- die Art der personenbezogenen Daten,
- die Kategorien betroffener Personen und
- die Pflichten und Rechte des Verantwortlichen.

Dieser **Vertrag** sieht insbesondere vor, dass der Auftragsverarbeiter:

- die personenbezogenen Daten **nur auf dokumentierte Weisung** des Verantwortlichen verarbeitet (auch bei Übermittlung an ein Drittland oder eine internationale Organisation), sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet,
- gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur **Vertraulichkeit** verpflichtet haben oder einer angemessenen **gesetzlichenVerschwiegenheitspflicht** unterliegen,
- alle erforderlichen Sicherheitsmaßnahmen ergreift,
- **eine vorherige schriftliche Genehmigung des Verantwortlichen** für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters (Sub-Auftragsverarbeiter) einhält,
- den Verantwortlichen bei der Beantwortung **von Anträgen von betroffenen Personen** unterstützt (unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen),

  > **Hinweis**:
  > Der Auftragsverarbeiter ist gesetzlich nicht verpflichtet, selbst Anfragen von betroffenen Personen für den Verantwortlichen zu beantworten. Es empfiehlt sich aber, Anfragen von betroffenen Personen rasch an den Verantwortlichen weiterzuleiten, damit dieser diese Anfrage verordnungskonform erfüllen kann.

- den Verantwortlichen bei der Einhaltung der **Sicherheitsmaßnahmen und Meldeverpflichtungen** unterstützt (unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen),
- nach Vertragserfüllung alle personenbezogenen Daten nach Wahl des Verantwortlichen **entweder löscht oder zurückgibt und die vorhandenen Kopien löscht** (sofern keine anderweitige gesetzliche Verpflichtung besteht),
- dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Pflichtgemäßheit zur Verfügung stellt und **Überprüfungen** durch den Verantwortlichen ermöglicht und dazu beiträgt.

Nimmt der Auftragsverarbeiter einen Sub-Auftragsverarbeiters in Anspruch, werden auch diesem dieselben Datenschutzpflichten auferlegt.

> **Hinweis:**
> Ein Muster für eine Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter findet sich unter EU-Datenschutz-Grundverordnung (DSGVO): Mustervertrag.

Warnpflicht

Der Auftragsverarbeiter unterliegt einer besonderen **Warnpflicht**, dh er hat den Verantwortlichen unverzüglich zu informieren, falls er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt.

Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten nur auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie aufgrund einer gesetzlichen Vorschrift zur Verarbeitung verpflichtet sind.

Vertreter von nicht in der Union niedergelassenen Auftragsverarbeitern

Für Auftragsverarbeiter, deren Sitz sich außerhalb der Europäischen Union befindet, die sich aber dennoch im Geltungsbereich der DSGVO befinden benennt der Auftragsverarbeiter schriftlich einen **Vertreter**. Dieser Vertreter muss in einem der Mitgliedstaaten **niedergelassen** sein, in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, sich befinden. Der Vertreter fungiert zusätzlich oder an Stelle des Auftragsverarbeiters als **Anlaufstelle** insbesondere für Aufsichtsbehörden und betroffene Personen.

Ausnahmen von der Pflicht zur Benennung eines Vertreters bestehen nur bei:

- einer Verarbeitung, die **gelegentlich** erfolgt, **keine** umfangreiche Verarbeitung besonderer Datenkategorien („sensible Daten") oder umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten einschließt und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich **zu keinem** Risiko für die Rechte und Freiheiten natürlicher Personen führt, oder
- **Behörden** oder öffentlichen Stellen.

Der Auftragsverarbeiter haftet weiterhin selbst.

Haftung

Betroffene Personen haben neben verfügbaren **verwaltungsrechtlichen** oder **außergerichtlichen** Rechtsbehelfen auch das Recht auf einen wirksamen **gerichtlichen Rechtsbehelf** gegen Auftragsverarbeiter im Falle einer Rechtsverletzung durch den Auftragsverarbeiter.

Betroffene Personen können auf **materiellen oder immateriellen Schadenersatz** klagen. Jeder an einer Verarbeitung Beteiligte haftet für den Schaden, der durch eine unrechtmäßige Verarbeitung verursacht wurde. Die Haftung entfällt, wenn die fehlende Verantwortung für den Umstand, durch den der Schaden eingetreten ist, nachgewiesen werden kann.

Ist **mehr als ein Auftragsverarbeiter** (oder mehr als ein Verantwortlicher) oder sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie für einen Schaden verantwortlich, **haftet jeder** Auftragsverarbeiter (oder jeder Verantwortliche) **für den gesamten Schaden**. Es ist jedoch möglich, von den übrigen an derselben Verarbeitung Beteiligten den Teil des Schadenersatzes zurückzufordern, der ihrem Anteil an der Verantwortung für den Schaden entspricht, also Regress zu nehmen.

Relevante Artikel der DSGVO: Art 28, Art 30-31
Relevante Erwägungsgründe: 13, 22-24, 77, 95,146

Stand: 05.03.2021