Checkliste

AUFTRAGSVERGABE
Checkliste für Auftragsverarbeitung

Wozu dient die Checkliste?

- Sobald Sie vorhaben, ein Unternehmen mit Leistungen zu beauftragen oder mit diesem zusammenzuarbeiten, müssen Sie prüfen, wie die Zusammenarbeit in Bezug auf den Datenschutz einzustufen ist. Hier ist abzugrenzen in Sachen Datenschutz von einer Auftragsverarbeitung, einer gemeinsamen Verantwortlichkeit und der eigenverantwortlichen Verantwortlichkeit des Beauftragten.
- Liegt eine Auftragsverarbeitung vor, ist der Dienstleister sorgfältig auszuwählen.
- Sie müssen des Weiteren einen Vertrag über die Auftragsverarbeitung abschließen, um die datenschutzrechtlichen Vorgaben zu erfüllen.

Rechtliche Grundlage

- Art. 28 DSGVO – Auftragsverarbeiter
- Art. 29 DSGVO - Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters
- Erwägungsgrund 81 – Heranziehung eines Auftragsverarbeiters

CHECKLISTE Auftragsverarbeitung

☐ 1 Liegt eine Auftragsverarbeitung vor?

Sie beauftragen einen Dienstleister oder arbeiten mit einem anderen Unternehmen zusammen? Dann ist die datenschutzrechtliche Grundlage zu prüfen. Insbesondere hat dabei eine Abgrenzung zur gemeinsamen Verantwortlichkeit und der eigenen Verantwortlichkeit des Dienstleisters zu prüfen.

✓ **Auftragsverarbeitung liegt vor, wenn ...**

- Die Datenverarbeitung stellt einen Schwerpunkt der zu beauftragenden Dienstleistung dar.
- Es besteht eine hierarchische Struktur.
- Ihr Auftragnehmer bzw. Vertragspartner ist Ihren Weisungen zur Verarbeitung unterworfen.
- Sie bestimmen allein Zwecke und Mittel der Verarbeitung.

✕ **Gemeinsame Verantwortlichkeit liegt vor, wenn ...**

- Die Datenverarbeitung stellt einen Schwerpunkt der gemeinsamen Zusammenarbeit dar.
- Es besteht keine hierarchische Struktur.
- Jede Vertragspartei hat Einfluss auf die Zwecke und Mittel der Verarbeitung, d.h. entscheidet über das WARUM und WIE der gemeinsamen Datenverarbeitung und kann dies kontrollieren.
- Die Parteien können im Rahmen der Zusammenarbeit einen gemeinsamen Zweck oder auch jede für sich einen eigenen Zweck mit der Verarbeitung verfolgen.

✕ **Ansonsten liegt Eigenverantwortlichkeit des Vertragspartners vor**

- Liegt kein Fall der gemeinsamen Verantwortlichkeit oder Auftragsverarbeitung vor, so entscheidet der Vertragspartner i.d.R. eigenverantwortlich über seine Datenverarbeitung personenbezogener Daten. Es handelt sich insoweit meist um eine Inanspruchnahme fremder Fachleistungen bei eigenständig Verantwortlichen. Der Dienstleister unterliegt insoweit nicht Ihren Weisungen. Beispiele sind Dienste von Berufsgeheimnisträgern, wie Rechtsanwalt, Steuerberater, extern Betriebsarzt. Auch liegt kein Fall der Auftragsverarbeitung oder gemeinsamen Verantwortlichkeit vor, wenn die Verarbeitung der übermittelten Daten nur als ungewolltes Beiwerk der eigentlichen beauftragten Leistung anzusehen ist. Beispiele sind die Weitergabe der Anschrift eines Mieters durch den Vermieter an einen Handwerker im Rahmen von Reparaturleistungen,
- Es ist kein spezieller datenschutzrechtlicher Vertrag erforderlich, jedoch bieten sich Regelungen zum Datenschutz an.

Beispiele für Auftragsverarbeitung und Abgrenzung zu gemeinsamer Verantwortlichkeit und Funktionsübertragung

Auftragsverarbeitung liegt vor	**Gemeinsame Verantwortlichkeit liegt vor**	**Eigene Verantwortlichkeit des Dienstleisters liegt vor**
Daten- und Aktenvernichtung	Konzern: gemeinsame Verwaltung zum Beispiel von „Stammdaten“ für bestimmte gleichlaufende Geschäftszwecke	Inkassobüro mit Forderungsübertragung
Lohn- und Gehaltsabrechnungen über Dienstleister, die nicht Steuerberater sind	Joint-Venture	Rechtsanwaltsdienste
Werbeadressenverarbeitung in einem Lettershop	Entwickeln und Betreiben einer gemeinsamen Vertriebsplattform	Steuerberater
Verarbeitung von Kundendaten durch ein Callcenter ohne wesentliche eigene Entscheidungsspielräume	klinische Arzneimittelstudien, bei welchen den Mitwirkenden (Sponsor, Institut, Ärzte) Entscheidungskraft mindestens in Teilbereichen zukommt	Sachverständigentätigkeit
Auslagerung der Backup-Sicherheitsspeicherung und anderer Archivierungen	Facebook-Fanpage, und ggf. ähnliche Social-Media-Konstellationen, Siehe EuGH-Urteil	externe Betriebsärzte
Übermittlung von Daten zu Sicherungszwecken an einen IT-Dienstleister		Wirtschaftsprüfer
Übermittlung von Daten in eine Cloud (Sicherungszwecke oder Nutzung von cloudbasierter Software)		Bankleistungen für den Geldtransfer
Auslagerung der Systemadministration		Postdienstleistung für den Brieftransport
Nutzung von Analyse-Tools z.B. (Google-Analytics, Matomo)		Tätigkeit als WEG-Verwalter
Betreiben einer Webseite		Insolvenzverwalter
Wartung der Hard- und Software durch Hersteller oder IT-Dienstleister		Personalvermittlung nach Auftrag von Stellensuchenden oder Arbeitgebern

Daten- und Aktenvernichtung		Internet-Plattformbetreiber zur Vermittlung zwischen Anbietern und Nachfragern
Lohn- und Gehaltsabrechnungen über Dienstleister, die nicht Steuerberater sind		Detektive hinsichtlich Überwachung und Ausforschung
Werbeadressenverarbeitung in einem Lettershop		beauftragte Warenzusendung: Hersteller und Großhändler, die von Einzelhändlern die Endkundenadressen zur Direktlieferungen erhalten; Geschenksendungen, z.B. durch Blumen- oder Weinversender
Verarbeitung von Kundendaten durch ein Callcenter ohne wesentliche eigene Entscheidungsspielräume		Anfertigung individueller medizinischer Produkte, Hilfsmittel (Prothesen u.ä.) im Auftrag von Ärzten, Apotheken, Sanitätshäusern usw.
Auslagerung der Backup-Sicherheitsspeicherung und anderer Archivierungen		Schulungsdienstleistung hinsichtlich der Übersendung von Teilnehmer-Daten an externen Trainer, Schulungsveranstalter oder Tagungshotel
Übermittlung von Daten zu Sicherungszwecken an einen IT-Dienstleister		Handelsvertreter im Rahmen ihrer Beratungstätigkeit und Vertragsvermittlungen
Übermittlung von Daten in eine Cloud (Sicherungszwecke oder Nutzung von cloudbasierter Software)		Reisebüro: Übermittlung aufgrund Kundenvertrags von Daten an Leistungsanbieter, wie Hotels, Miet- wagenfirmen, Fluggesellschaften, Busunternehmen, Versicherungen usw.
Auslagerung der Systemadministration		
Nutzung von Analyse-Tools z.B. (Google-Analytics, Matomo)		
Betreiben einer Webseite		

Wartung der Hard- und Software durch Hersteller oder IT-Dienstleister		

✓ ANTWORT JA: Weiter in der Checkliste

✗ ANTWORT NEIN: Wenn eine gemeinsame Verantwortlichkeit vorliegt, ist eine entsprechende vertragliche Vereinbarung notwendig. Wenn eine eigene Verantwortlichkeit des Dienstleisters vorliegt, benötigen Sie keinen speziellen Vertrag nach DSGVO. (Es empfiehlt sich jedoch auch Regelungen zum Datenschutz in den Auftrag/Vertrag einfließen zu lassen.)

☐ 2 Ist der Dienstleister geeignet?

Prüfen sie ob der Dienstleister folgende Kriterien erfüllt:

- ☐ Fachwissen,
- ☐ Zuverlässigkeit und
- ☐ Ressourcen
- ☐ sachgerechte technische und organisatorische Maßnahmen

zur Datensicherheit hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen dieser Verordnung genügen.

Zu einer positiven Bewertung können geeignete Zertifizierungen des Anbieters (z.B. ISO 27001) hilfreich sein, als auch genehmigte Verhaltensregeln nach Art. 40 DSGVO, denen sich der Anbieter unterworfen hat.

✓ ANTWORT JA: Weiter in der Checkliste

✗ ANTWORT NEIN: Anderen Anbieter suchen

☐ 3 Erforderlicher Vertragsinhalt enthalten?

Die Auftragsverarbeitung muss auf Grundlage eines entsprechenden Vertrages erfolgen. Hierzu macht die DSGVO Vorgaben. Prüfen Sie, ob folgende Punkte im Vertrag abgedeckt und geregelt sind.

- ☐ **Gegenstand und Dauer der Verarbeitung**
  - In der Regel wird im AVV auf den Hauptvertrag verwiesen.
  - Gegenstand und Dauer ergeben sich dann aus dem Hauptvertrag, in welchem die detaillierten Leistungen des Dienstleisters abgebildet werden. So kann sich insb. bei Standardleistungen der Gegenstand durch eine Leistungsbeschreibung und die Dauer aus Allgemeinen Geschäftsbedingungen ergeben.

- Eine zeitliche Befristung oder ein Abschluss auf unbestimmte Zeit sind möglich, sofern bestimmt ist, wie der Vertrag beendet werden kann.

☐ **Art und Zweck der Verarbeitung**

- Entsprechend der beauftragten Leistung sind Art und Zweck der Verarbeitung von personenbezogenen Daten näher zu beschreiben und festzulegen.

☐ **Art der personenbezogenen Daten und Kategorien von betroffenen Personen**

- Oftmals wird Ihnen der Auftragnehmer, der ein Vertragsmuster zur Prüfung bereitstellt, es Ihnen selbst überlassen, diesen Punkt im Auftragsverarbeitungsvertrag auszufüllen.
- Beispiele von Kategorien von Personen: Kunden, Mitarbeiter, Interessenten, Abonnenten, Beschäftigte, Lieferanten, Ansprechpartner, Besucher, Antragsteller
- Beispiele der Art der personenbezogenen Daten: Personenstammdaten (Name, Anschrift, Kontaktdaten, Geburtsdatum), Vertragsstammdaten, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Bestelldaten, Kommunikationsdaten

☐ **Verarbeitung nach dokumentierter Weisung**

- Enthalten sein muss insbesondere, dass die Datenverarbeitung durch den Dienstleister ausschließlich nach Ihren Weisungen hin erfolgt, die zu dokumentieren sind (elektronisch, schriftlich, Textform).
- Der Auftragsverarbeiter ist verpflichtet, Sie als Verantwortlichen unverzüglich zu informieren, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Es sollte daher eine ergänzende Regelunge im Vertrag erfasst werden, die bestimmt wie mit rechtswidrigen Weisungen umzugehen ist.
    - *Beispielklausel: Sofern der Auftragsverarbeiter eine Weisung des Auftraggebers dahingehend bewertet, dass diese gegen den Vertrag oder das geltende Datenschutzrecht verstößt, hat er den Auftraggeber unverzüglich zu informieren. Er ist berechtigt, die weisungsgemäße Ausführung bis zur Prüfung und Bestätigung der Weisung durch den Auftraggeber einstweilen einzustellen. Die Durchführung einer offensichtlich rechtswidrigen Weisung darf abgelehnt werden.*

☐ **Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit**

- *Beispielklausel: Der Auftragsverarbeiter hat alle Mitarbeiter, die in die beauftragte Datenverarbeitung einbezogen werden, auf die Vertraulichkeit für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses schriftlich zu verpflichten und diese auf erstes Anfordern nachzuweisen. Die Mitarbeiter werden vor Aufnahme ihrer Tätigkeit hinsichtlich der einschlägigen Bestimmungen des Datenschutzes belehrt.*

☐ **Sicherstellung von technischen und organisatorischen Maßnahmen (TOM)**

- Im Vertrag sind die entsprechen Art. 32 DSGVO bestimmten TOM konkret anzugeben.
- Diese sind zu prüfen.

☐ **Hinzuziehung von Subunternehmern**

- Die Subunternehmer müssen konkret benannt (Name, Kontakt, beauftragte

Leistungen) werden.

- Es sind Regelung aufzunehmen, die Änderungen von Subunternehmern sowie die Sicherstellung, dass der Subdienstleister dasselbe Datenschutzniveau gewährleistet wie der Auftragsverarbeiter, bestimmen. Es ist möglich (i) den Einsatz von Subunternehmern gänzlich auszuschließe oder (ii) von der vorherigen Zustimmung abhängig zu machen oder (iii) es wird die Befugnis zur Beauftragung im Voraus erteilt, wobei Ihnen dann Einspruchsrecht bei Änderungen zusteht. In jedem Fall sind Sie bei Änderungen zu informieren.
- Der Vertrag mit dem Subunternehmer muss die gleichen vertraglichen Verpflichtungen aufweisen wie der Vertrag zwischen Ihnen und dem Auftragsverarbeiter.
- Die Beauftragung von in Drittstaaten ansässigen Subunternehmern darf nur unter Erfüllung der besonderen Voraussetzungen der Art. 44 ff. DSGVO erfolgen.

☐ **Vorliegen einer Datenübermittlung in Drittländer**

- Die Übermittlung in Drittländer ist nur unter besonderen Voraussetzungen der der Art. 44 ff. DSGVO zulässig. Sollte im Vertrag bestimmt sein, dass eine entsprechende Übermittlung erfolgt, muss geprüft werden ob die Voraussetzungen hierfür erfüllt werden.
- Ansonsten sollte im Vertrag bestimmt sein, dass keine Übermittlung in Drittländer erfolgt und eine spätere Änderung Ihrer Zustimmung bedarf.
- *Beispielklausel: Die Verarbeitung personenbezogener Daten erfolgt ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (sog. Drittländer). Sollten sich hierzu zukünftig Änderungen ergeben, bedarf dies der vorherigen Zustimmung des Auftraggebers. Eine Übermittlung in Drittländer darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).*

☐ **Unterstützung hinsichtlich der Erfüllung von datenschutzrechtlichen Verpflichtungen, insbesondere der Betroffenenrechte**

- Aufzunehmen ist die Unterstützung des Auftragsverarbeiters bei der Erfüllung seiner datenschutzrechtlichen Verpflichtungen, bei der Einhaltung der nach Kapitel III und Art. 32 bis 36 DSGVO bestehenden Verpflichtung zur Sicherstellung eines risikoadäquaten Schutzniveaus bei der Datensicherheit, bei der Durchführung von Risikobewertungen und etwaigen Datenschutz-Folgenabschätzungen, bei Datenpannen und bei der Erfüllung von Betroffenenrechten.
- *Beispielklausel: Der Auftragsverarbeiter leistet mit geeigneten technischen und organisatorischen Maßnahmen und Informationen Unterstützung bei der Erfüllung und Einhaltung der Pflichten des Auftraggebers nach Kapitel III (Art. 12 bis Art. 22) DSGVO sowie Art. 32 bis Art. 36 DSGVO.*
- Zu empfehlen sind darüber hinaus nähere Bestimmungen, insbesondere wie Anfragen betroffener Personen gehandhabt werden.

☐ **Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung**

- Es ist im Vertrag zu bestimmen, dass Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Ihrer Wahl entweder gelöscht oder zurückgegeben werden, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

☐ **Kontrollrechte des für die Verarbeitung Verantwortlichen und Duldungspflichten des Auftragsverarbeiters**

- Im Vertrag ist festzuhalten, dass der Auftragsverarbeiter alle erforderlichen Informationen zum Nachweis der Einhaltung der datenschutzrechtlichen Pflichten zur Verfügung stellt und Überprüfungen (z.B. Inspekitonen) die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht.
- Nachweise können auch spezifiziert werden, z.B. Vorlage von genehmigten Verhaltensregeln nach Art. 40 DSGVO oder Zertifikaten nach Art. 42 DSGVO.

☐ **Hat der Auftragsverarbeiter einen Datenschutzbeauftragten und wurde dieser im Vertrag bezeichnet?**

- Wenn ja, ist dieser mit Kontaktdaten zu erfassen.
- Falls kein Datenschutzbeauftragter bestellt ist, ist die Angabe eines Ansprechpartners zu empfehlen.

✓	ANTWORTEN: JA > Weiter in der Checkliste
✗	ANTWORTEN: NEIN > Haken Sie beim Anbieter nach und bitten um entsprechende Vertragsergänzungen. Wenn der Anbieter sich weigert erforderliche Änderungen vorzunehmen, wählen Sie einen anderen Anbieter.

☐ 4 Welche Form ist beim Vertragsabschluss zu beachten?

Es ist ausreichend den Vertrag in Textform (z.B. per Online-Formular) zu schließen.

Der sicherste Weg ist und bleibt jedoch die Schriftform.

☐ 5 Muster

Muster hat beispielsweise das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) bereitgestellt:

https://www.lda.bayern.de/de/thema_auftragsverarbeitung.html

Direktdownload:

https://www.lda.bayern.de/media/muster/formulierungshilfe_av.pdf