Quelle: Stephan Hansen-Oest, <https://www.datenschutz-guru.de/checkliste-zur-prufung-eines-auftragsverarbeitungsvertrages/>

**Checkliste zur Prüfung eines Auftragsverarbeitungsvertrages**

Checkliste zur Prüfung der Verarbeitung von Daten im Auftrag durch

**Mustermann GmbH
Musterstr. 123
12345 Musterstadt**

Nach Art. 28 der Datenschutz-Grundverordnung (DSGVO) ist der Auftragnehmer, der personenbezogene Daten im Auftrag des Auftraggebers verarbeitet, sorgfältig auszuwählen. Es dürfen nur Dienstleister („Auftragsverarbeiter“) ausgewählt werden, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt grundsätzlich. auf der Grundlage eines Vertrags. Dieser muss die folgenden Inhalte regeln:

1. Sind Gegenstand und Dauer des Auftrages geregelt?

*Der Auftrag der Verarbeitung muss verständlich bezeichnet werden. Auch wenn nicht einzelne Verarbeitungsschritte benannt werden müssen, so muss deutlich gemacht sein, welchen Umfang die Arbeiten haben, die vom Auftragnehmer zu erledigen sind.*

Gibt es eine Regelung zum Gegenstand des Vertrages?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

Sind Beginn und Ende des Auftrages im Vertrag geregelt?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

2. Sind Umfang, Art und Zweck der Datenverarbeitung geregelt?

*Im Auftragsverarbeitungsvertrag sind konkrete Weisungen im Hinblick auf die Verarbeitung im konkreten Fall zu treffen, die nach Möglichkeit auch die einzelnen Verarbeitungsschritte betreffen. Die Möglichkeiten, insbesondere aber auch die Grenzen der Datenverarbeitung durch den Auftragnehmer müssen den Regelungen entnommen werden können.*

*Der Zweck der Verarbeitung der Daten ist im Vertrag zu benennen. Auch die Datenarten sind zu benennen, im Falle der Verarbeitung besonderer Arten personenbezogener Daten ist ggf. eine namentliche Nennung der betreffenden Datenarten sinnvoll.*

*Der Kreis der Betroffenen ist so konkret wie möglich zu fassen.*

Gibt es konkrete Weisungen, welche Verarbeitungen vom Auftragnehmer vorzunehmen sind?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

Ist der Verwendungszweck im Vertrag geregelt?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

Sind die Datenarten vertraglich festgehalten oder bestimmt bzw. bestimmbar?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

Ist der Kreis der Betroffenen dem Vertrag zu entnehmen?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

3. Sind die nach Art. 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen geregelt?

*Der Auftragsverarbeitungsvertrag sollte konkrete Regelungen beinhalten, welche technischen und organisatorischen Maßnahmen vom Auftragnehmer bei der Durchführung des Auftrages eingehalten werden oder zumindest welche Mindestkriterien einzuhalten sind.*

Gibt es Regelungen zur Gewährleistung der Vertraulichkeit?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

Gibt es Regelungen zur Gewährleistung der Verfügbarkeit?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

Gibt es Regelungen zur Gewährleistung der Integrität?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

Gibt es Regelungen zur Gewährleistung der Belastbarkeit der Systeme auf Dauer?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

Gibt es Regelungen zur Fähigkeit des Auftragsverarbeiters, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

Gibt es Regelungen dazu, wie der Auftragsverarbeiter die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gewährleistet?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

4. Ist das Weisungsrecht (insbesondere das Recht zu ergänzenden Weisungen) im Vertrag geregelt?

*Aus dem Vertrag muss sich ergeben, ob die getroffenen Regelungen abschließenden Charakter haben, oder – was zwingend erforderlich sein kann, zumindest aber geboten ist – ergänzende Weisungen des Auftraggebers möglich sind. Auch das „Wie“ der ergänzenden Weisungen ist zu regeln (Wer kann weisen? Wie (z.B. Form) sind Weisungen zu erteilen?)*

Gibt es eine Regelung, aus der sich der Umfang des Weisungsrechts des Auftraggebers (ggf. auch hinsichtlich der Zulässigkeit ergänzender Weisungen („Weisungsvorbehalt“) ergibt?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

5. Sind Regelungen zu den Vertraulichkeitspflichten von Beschäftigten des Auftragnehmers im Vertrag enthalten?

*Unabhängig davon, dass für den Auftragnehmer schon regelmäßig selbst die Vorgaben der DSGVO gelten, sind im Vertrag noch einmal gesondert bestimmte Anforderungen zur Wahrung der Vertraulichkeit zu regeln. Dies ergibt sich zudem aus Art. 28 Abs. 3 lit. b) DSGVO.*

Gibt es eine Regelung zur Verpflichtung der Beschäftigten des Auftragnehmers zur Vertraulichkeit?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

6. Sind Regelungen zu Unterauftragsverhältnissen im Vertrag enthalten?

*Das Ob und Wie einer Beauftragung von Unterauftragnehmern durch den Auftragnehmer bei der Verarbeitung von Daten für den Auftraggeber ist vertraglich zu regeln.*

Gibt es eine Regelung zur Zulässigkeit von Unterauftragsverhältnissen („Ob“)?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

a) Falls ja, gibt es eine Regelung dazu, wie der Unterauftragnehmer zu beauftragen ist („Wie“)?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

b) Falls ja, gibt es eine Regelung dazu, wie neue Unterauftragnehmer vom Auftraggeber zu genehmigen sind bzw. im Falle einer allgemeinen Genehmigung, dass neue Unterauftragnehmer dem Auftraggeber im Voraus benannt werden und dem Auftraggeber ein Widerspruchsrecht zusteht.

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

7. Gibt es Regelungen zur Unterstützung des Auftraggebers bei der Geltendmachung von Rechten von betroffenen Personen?

*Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten zu unterstützen. Diese Pflichten sollten im Auftragsverarbeitungsvertrag geregelt sein.*

Gibt es eine Regelung zur Unterstützung des Auftraggebers durch den Auftragnehmer bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten)?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

8. Gibt es Regelungen zur Unterstützung des Auftraggebers bei der Einhaltung seiner Pflichten aus den Art. 32 – 36 DSGVO?

*Der Auftragnehmer ist verpflichtet, den Auftraggeber dabei zu unterstützen, dass dieser seinen Pflichten aus Art. 32 – 36 DSGVO nachkommen kann. Diese Pflichten sollten im Auftragsverarbeitungsvertrag geregelt oder benannt sein.*

Gibt es eine Regelung zur Unterstützung des Auftraggebers durch den Auftragnehmer bei der Einhaltung seiner Pflichten aus den Art. 32 – 36 DSGVO?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

9. Gibt es Regelungen zu Kontrollrechten des Auftraggebers und entsprechenden Duldungspflichten des Auftragnehmers?

*Um eine wirksame Kontrolle des Auftragnehmers vornehmen zu können, müssen Kontrollrechte vertraglich vereinbart werden. Damit einhergehen entsprechende Duldungspflichten des Auftragnehmers, die z.B. den Zugang zu Geschäftsräumen etc. beinhalten.*

Gibt es eine Regelung zu Kontrollrechten des Auftraggebers?

*(z.B. Kontrolle vor Ort, Herausgabe von Informationen etc.)*

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

Gibt es eine Regelung zu Kontrollrechten des Auftraggebers gegenüber etwaigen Unterauftragnehmern?

*(z.B. Kontrolle vor Ort, Herausgabe von Informationen etc.)*

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

10. Gibt es Regelungen zu Informationspflichten des Auftragnehmers bei Verstößen gegen Datenschutzvorschriften oder Pflichten gegenüber dem Auftraggeber?

*Insbesondere, damit der Auftraggeber seinen etwaigen Pflichten nach Art. 33, 34 DSGVO nachkommen kann, müssen entsprechende Informationspflichten des Auftragnehmers bei Unregelmäßigkeiten bzw. Verstößen gegen Rechtsvorschriften oder vertragliche Pflichten gegenüber dem Auftraggeber geregelt sein.*

Gibt es eine Regelung, aus der sich die Pflicht des Auftragnehmers ergibt, Verstöße gegen Datenschutzvorschriften (insbesondere der DSGVO) oder gegen die vom Auftraggeber erteilten Weisungen zu melden?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

Ist im Vertrag eine Frist geregelt, binnen derer der Auftragnehmer nach Kenntnis eines Datenschutzvorfalls eine Meldung gegenüber dem Auftraggeber zu machen hat?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter:

11. Gibt es Regelungen zur Rückgabe bzw. Löschung von Daten nach Auftragsbeendigung?

*Es muss gewährleistet sein, dass nach Beendigung des Auftrags keine personenbezogenen Daten mehr beim Auftragnehmer verbleiben, soweit keine gesetzlichen Aufbewahrungspflichten des Auftragnehmers bestehen. Hierzu bedarf es entsprechender Regelungen.*

Gibt es eine Regelung, aus der sich die Pflicht des Auftragnehmers ergibt, überlassene Datenträger zurückzugeben bzw. für den Auftraggeber gespeicherte Daten zu löschen?

* [ ] Nein
* [ ] Ja. Die Regelung ist im Vertrag zu finden unter: