 

  DFN-CERT Services GmbH Logo

Handreichung zur   
AV-Vertragsprüfung

Version 2.0, 11. Juni 2019

Die Nutzung dieses Dokuments ist zulässig unter der Lizenz CC BY-SA 3.0   
<https://creativecommons.org/licenses/by-sa/3.0/de/legalcode>   
Autor: NRW Projektgruppe „Umsetzung der EU-Datenschutz-Grundverordnung (DS-GVODS-GVO) −  
Datenschutzmanagementsysteme“ 2018

gefördert vom 

Prüfprotokoll zu der geplanten Auftragsverarbeitung mit …

(Prüfer, Datum)

# Checkliste zur Auswahl eines Auftragsverarbeiters

(Die datenschutzkonforme Auswahl des Auftragsverarbeiters muss vor Abschluss eines Vertrags (Hauptvertrags) oder einer Beauftragung von der Bedarfsstelle, ggf. unter Beratung des Datenschutzbeauftragten geprüft werden.)

|  |  |  |
| --- | --- | --- |
| **Bedingung** |  | **Begründung und  Anmerkungen** |
| **Fachliche Eignung des Auftragsverarbeiters** | | |
| Bietet der Auftragsverarbeiter hinreichend Garantien dafür, dass die Verarbeitung durch geeignete Maßnahmen in Einklang mit der EU-DSGVO erfolgt und die Rechte der Betroffenen gewahrt bleiben? | ja  nein  (ja bei mind.  einem „ja“ unter 1.-4.) |  |
| 1. Hinreichende Dokumentation eines ausreichend hohen Sicherheitsniveaus bei der Datenverarbeitung liegt vor (gibt es ein Sicherheitskonzept / einen hinreichenden Maßnahmenkatalog). **Eine Begründung dieser Einschätzung ist erforderlich und im Anhang beizufügen.** | ja  nein |  |
| 1. Liegen anerkannte Zertifizierungen bzw. Nachweise über jüngst stattgefundene Audits vor, aus denen sich die sichere und datenschutzkonforme Verarbeitung ergeben (die Zertifikate und der Prüfbereich des/der Audits müssen die gesamte Verarbeitung umfassen, nicht nur Teile der Infrastruktur) | ja  nein |  |
| 1. Der Auftragsverarbeiter hat sich zur Umsetzung von genehmigten Verhaltensregeln gemäß Artikel 40 DSGVO verpflichtet. | ja  nein |  |
| 1. Der Auftragsverarbeiter wurde vom Verantwortlichen oder einem beauftragten, qualifizierten Dritten auf seine Tauglichkeit für diese Auftragsverarbeitung hin überprüft. | ja  nein |  |
| Wurden einschlägige Quellen zur öffentlichen Begutachtung des Auftragsverarbeiters konsultiert? (z. B. Suchmaschinen-Suche) | ja  nein |  |
| Liegen keine Hinweise auf Datenschutzverstöße beim Auftragsverarbeiter vor? | ja  nein |  |
| Lassen die Leistungsbeschreibungen, Dokumentationen und mündlichen Antworten des Auftragsverarbeiters eine fachgerechte und professionelle Verarbeitung der Daten erwarten? | ja  nein |  |
| Besteht der Eindruck, dass die Schutzmaßnahmen des Auftragsverarbeiters den Risiken bei der Verarbeitung gerecht werden? | ja  nein |  |
| **Ort der Verarbeitung und Sitz des Auftragnehmers** | | |
| Findet die Verarbeitung der Daten ausschließlich innerhalb der EU / EWR statt?  (Zu beachten: Auch Fernzugriff zur Wartung o.Ä. von außerhalb EU/EWR bedeutet eine Verarbeitung außerhalb EU/EWR.) | ja  nein |  |
| Liegt der Sitz des Auftragsverarbeiters innerhalb EU/EWR? | ja  nein |  |
| Falls nein, gibt es einen in der EU ansässigen Vertreter gemäß Art. 27 und Art. 4 Nr. 17 DSGVO? | ja  nein |  |
| Verarbeiten alle Unterauftragnehmer die personenbezogenen Daten ausschließlich innerhalb EU/EWR (Ansässigkeit innerhalb EU/EWR und/oder ausdrückliche Garantie der Verarbeitung innerhalb EU/EWR)? | ja  nein |  |
| Werden im Falle einer Verarbeitung außerhalb EU/EWR Angaben zur rechtlichen Zulässigkeit gemacht? Wenn ja, welche? | ja  nein |  |
| Hat der Auftragsverarbeiter eine Mutter- oder Tochtergesellschaft mit US-amerikanischer Registrierung? (Wenn ja besteht prinzipiell ein Zugriff auf personenbezogene Daten durch (US-) Behörden beim Auftragsverarbeiter unter dem CLOUD Act von 2018) | ja  nein |  |

**Aufzählung der Referenzen zur Erfahrung als Auftragsverarbeiter:**

**Bei nein-Antworten, Begründung warum der Auftragsverarbeiter dennoch in Frage kommt:**

# Checkliste zur AV-Vertragsprüfung

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Werden die folgenden Punkte  im AV-Vertrag hinreichend  beschrieben? | Fundstelle | Erläuterung |  | Anmerkungen |
| Kontaktdaten und Vertrag | | | | |
| Angaben zu den Vertragspartnern gemacht:  Verantwortlicher, Auftragsverarbeiter, ggf. Subunternehmer, Vertreter (Angabe „Vertreter“ erforderlich: nur wenn keine Niederlassung in der EU besteht) | Art. 28 Abs. 3 S. 1  Vertreter: Art. 27 | Erforderliche Angaben:  Name, Anschrift, Handelsregisternummer etc.  Zumindest muss der Verweis auf einen Hauptvertrag erfolgen, in dem diese Angaben enthalten sind. | ja  nein |  |
| Bezug zu einem Hauptvertrag, falls vorhanden | Art. 28 Abs. 3 S. 1 |  | ja  nein |  |
| Bestehen Regelungen zur Weisungsgebundenheit der Verarbeitung? | Art. 28 Abs. 3 S. 2 lit. a | Dürfen personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen (Auftraggebers) verarbeitet werden? | ja  nein |  |
| Weisungsbefugte Personen beim Auftraggeber  Weisungsempfänger beim Auftragnehmer | Keine Pflicht aber sinnvoll | Sind weisungsbefugte Personen und Weisungsempfänger genannt? | ja  nein |  |
| Nur relevant, wenn aus besonderen Gründen eine rechtliche Verpflichtung des Auftragnehmers besteht. Diese rechtliche Verpflichtung beeinträchtigt das Weisungsrecht des Auftraggebers, weshalb der den Pflichten unterliegende Auftragnehmer dies dem Auftraggeber mitteilen muss. | Art. 28 Abs. 3 S. 1 | Mitteilungspflicht enthalten, wenn der Auftragsverarbeiter gesetzlich zur Verarbeitung der Daten verpflichtet ist? | ja  nein |  |
| Regelung zur Pflicht des Auftragnehmers zur Information des Auftraggebers, wenn er eine Weisung für rechtswidrig hält | Art. 28 Abs. 3 UAbs. 2 |  | ja  nein |  |
| Datenschutzbeauftragte des Auftragsverarbeiters genannt | Keine Pflicht aber sinnvoll | Kontaktdaten | ja  nein |  |
| **Verarbeitung** | | | | |
| Gegenstand der Verarbeitung benannt?  (Z. B. Fernwartung, Betrieb von Software (SaaS), mit der personenbezogene Daten verarbeitet wird, Zurverfügungstellung von externem Speicherplatz) | Art. 28 Abs. 3 S. 1 | Beschreibung im Vertrag: Was wird mit den Daten getan? Was ist der Kern der Verarbeitungstätigkeit?  Falls Fehlanzeige: Es reicht ein Verweis auf den Hauptvertrag, in dem die Tätigkeit beschrieben ist. | ja  nein |  |
| Enthält der Vertrag Angaben über Art und Zweck der Verarbeitung? | Art. 28 Abs. 3 S. 1 | Die Art ist das „Wie“ der Verarbeitung.  Der Zweck ist das „Ziel“ oder „Warum“ der Verarbeitung.  Auch durch Verweis auf Hauptvertrag, wenn dort entsprechende Angaben vorhanden sind | ja  nein |  |
| Enthält der Vertrag die Auflistung der personenbezogenen Daten, zumindest nach ihrer Art (z. B. Personendaten, Prüfungsergebnisse, Hochschulzugangsberechtigungen, etc.)? | Art. 28 Abs. 3 S. 1 | Welche Daten?  Auch durch Verweis auf den Hauptvertrag erfüllbar, sofern sich die Informationen aus diesen ergeben. | ja  nein |  |
| Sind die Kategorien (z. B. Studierende, Beschäftigte, Praktikanten, etc.) betroffener Personen aufgelistet? | Art. 28 Abs. 3 S. 1 | Betroffene Personengruppen  Auch durch Verweis auf den Hauptvertrag erfüllbar, sofern sich die Informationen aus diesen ergeben. | ja  nein |  |
| Dauer der Verarbeitung | Art. 28 Abs. 3 S. 1 | Z. B. auch durch Verweis auf Vertragslaufzeit des Hauptvertrags möglich | ja  nein |  |
| Datenrückgabe bzw. Löschung nach Vertragsende geregelt? | Art. 28 Abs. 3 S. 2 lit. g | Grundsätzlich müssen personenbezogene Daten nach Beendigung der Verarbeitung gelöscht oder zurückgegeben werden. | ja  nein |  |
| Sicherheit der Verarbeitung | | | | |
| Verpflichtung, dass der Auftragsverarbeiter nur Mitarbeiter einsetzt, die sich zur Einhaltung der Vertraulichkeit verpflichtet haben | Art. 28 Abs. 3 S. 2 lit. b  Art. 29 | Sind die mit der Datenverarbeitung beim Auftragsverarbeiters betrauten Personen zur Vertraulichkeit verpflichtet oder unterliegen sie einer gesetzlichen Verschwiegenheitspflicht? | ja  nein |  |
| Verpflichtung zur Implementierung von technischen und organisatorischen Maßnahmen um die Sicherheit der Verarbeitung zu gewährleisten | Art. 28 Abs. 3 S. 2 lit. c | Sind hinreichende Angaben zur Gewährleistung der Sicherheit der Daten (gem. Art. 32 i.V.m. Art 5 (2) DSGVO) vorhanden und hat der Auftragsverarbeiter sich zu deren Einhaltung verpflichtet? | ja  nein |  |
| Berechtigung des Auftraggebers, die Verarbeitung beim Auftragnehmer selbst oder durch einen beauftragten Dritten zu überprüfen. | Art. 28 Abs. 3 S. 2 lit. h | Ist eine für den Auftragsverarbeiter verpflichtende (regelmäßige) Überprüfung der Verarbeitung durch den Verantwortlichen (oder ein von ihm beauftragten Dritten) einschließlich Inspektion vor Ort vorgesehen? | ja  nein |  |
| Schriftliche Dokumentation der Weisungen |  | Ist der Auftragnehmer berechtigt, eine schriftliche/elektronische Bestätigung von mündlichen Weisungen zu Dokumentations- und Beweiszwecken anzufordern? | ja  nein |  |
| Sonderkündigungsrecht, wenn ein US-Amerikanisches Unternehmen Anteile am Auftragsverarbeiter erwirbt und der Auftragsverarbeiter damit dem CLOUD Act unterliegt? |  |  | ja  nein |  |
| **Unterauftragsverhältnisse** | | | | |
| Sind Unterauftragsverhältnisse geregelt? Damit ist die weitere Auslagerung der Verarbeitung durch den Auftragnehmer an einen Unterauftragnehmer gemeint. | Art. 28 Abs. 3 S. 2 lit. d | Enthält der Vertrag eine Regelung zur generellen Zulässigkeit der Unterbeauftragung? | ja  nein |  |
| **Falls die Unterbeauftragung erlaubt ist:**  Ist die Weiterreichung der datenschutzrechtlichen Rechte und Pflichten an Unterauftragnehmer geregelt | Art. 28 Abs. 4 S. 1 | Wird der Auftragnehmer verpflichtet, alle datenschutzrechtlichen Verpflichtungen aus dieser Auftragsverarbeitung an alle Unterauftragnehmer weiterzureichen? | ja  nein |  |
| **Falls die Unterbeauftragung erlaubt ist:**  Pflicht zur Information mit Widerspruchsmöglichkeit oder Zustimmung des Verantwortlichen bei Unterauftragsverhältnissen | Art. 28 Abs. 2 S. 1, 2 | Wenn eine Unterbeauftragung erlaubt ist: Enthält der Vertrag Regelungen zur Information/Zustimmung des Auftraggebers in die Unterbeauftragung bzw. beim Austausch eines Unterauftragnehmers? | ja  nein |  |
| Unterstützung bei Betroffenenrechten, Datenpannen und DSFA | | | | |
| Unterstützung des Auftraggebers bei Gewährleistung der Betroffenenrechte | Art. 28 Abs. 3 S. 2 lit. e | Ist im Vertrag festgelegt, dass der Auftragnehmer den Auftraggeber bei Erfüllung von Betroffenenrechten unterstützen muss, insbesondere durch:  Weiterleitung von Anfragen von Betroffenen an den Auftraggeber  Zurverfügungstellung von erforderlichen Informationen und Vornahme von Handlungen um Betroffenenrechte umzusetzen | ja  nein |  |
| Unterstützung des Auftraggebers bei den Pflichten zur Sicherheit der Verarbeitung, Datenpannen und Datenschutzfolgeabschätzung | Art. 28 Abs. 3  S. 2 lit. f | Ist eine Unterstützung bei der Meldung von Datenpannen, bei Sicherheitsmaßnahmen und der Durchführung von Datenschutzfolgenabschätzungen vorgesehen? | ja  nein |  |
| Pflicht des Auftragnehmers zur unverzüglichen Meldung von Datenpannen | Art. 33 Abs. 2 | Ist die Pflicht zur möglichst sofortigen Meldung von (möglichen) Datenpannen an den Auftraggeber geregelt? | ja  nein |  |
| Pflicht zur Unterstützung des Auftraggebers beim Nachweis der Einhaltung der datenschutzrechtlichen Pflichten | Art. 28 Abs. 3 S. 2 lit. h |  | ja  nein |  |
| **Wichtige weitere Regelungen für den Auftraggeber, die nicht als Pflichtangaben in Art. 28 genannt sind** | | | | |
| Besteht eine ausdrückliche Regelung für den Fall der Haftung im Rahmen der gesamtschuldnerischen Haftung? (Problem: Prinzipiell haften Auftraggeber und Auftragnehmer erst einmal beide in vollem Umfang für Schäden gegenüber dem Betroffenen, egal wer den Schaden verursacht hat. Der Betroffene kann sich somit aussuchen, von wem er sich seinen Schaden ersetzen lässt) |  | Besteht eine Regelung, dass jeder Vertragspartner die Haftung im Umfang seiner Verantwortlichkeit übernimmt und den anderen Teil insoweit von der Haftung und den erforderlichen Kosten für die Rechtsverfolgung freistellt? | ja  nein |  |
| Ausschluss des Zurückbehaltungsrechts an personenbezogenen Daten (Problem: Wenn ein Vertragspartner meint noch einen Anspruch gegen den anderen Partner zu haben, so kann dieser grundsätzlich seinerseits die Erfüllung von Pflichten verweigern. Ohne eine diesbezügliche Regelung im Vertrag könnte somit der Auftragnehmer einer Auftragsverarbeitung die Herausgabe von personenbezogenen Daten nach Beendigung an den Auftraggeber verweigern, wenn er meint, dass seinerseits noch Ansprüche gegen den Auftraggeber bestehen. Betroffen von dieser Zurückbehaltung der Daten ist aber dann nicht nur der Auftraggeber, sondern auch die Personen, deren Daten bei dem Auftragnehmer verarbeitet wurden. Daher gilt es, das Zurückbehaltungsrecht an den personenbezogenen Daten vertraglich auszuschließen.) |  | Besteht eine Regelung, nach der das Zurückbehaltungsrecht (§ 273 BGB) an den personenbezogenen Daten ausgeschlossen ist? | ja  nein |  |
| Klare Regelungen zu Kosten bei Zusatzaufwänden des Auftragnehmers im Rahmen der Erfüllung der Pflichten aus dem Vertrag zur Auftragsdatenverarbeitung |  | Ist entweder geregelt, dass die Aufwände mit der Vergütung für den Hauptvertrag abgegolten sind bzw. ist anderenfalls klar geregelt für welche zusätzlichen Tätigkeiten Vergütungen fällig werden und wie diese ermittelt werden (z. B. nach Aufwand zum Stundensatz aus dem Hauptvertrag)? | ja  nein |  |
| Recht zur außerordentlichen Kündigung des Auftraggebers bei einem erheblichen oder trotz Abmahnung wiederholten Verstoß gegen die Vereinbarung zur Auftragsverarbeitung? |  |  | ja  nein |  |

**Bei nein-Antworten (mit Ausnahme der grau hinterlegten Felder), Begründung warum der Vertrag dennoch geschlossen werden soll/kann:**

(Bedarfsstelle / Justiziariat)