***Checkliste zur Prüfung der Verarbeitung von Daten im Auftrag durch***

Stand: 02.05.2023

Name und Anschrift des Unternehmens, mit dem der AVV geschlossen wird

1. Auftragsverarbeitungsvertrag vom:
2. Geprüft am:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Regelungsgegenstände** | **Rechtsgrundlage** | **Fundstelle im AVV** | **erfüllt** | **nicht erfüllt** | **Anmerkungen** |
|  | **Vorabfrage** |  |  |  |  |  |
| 1. | Handelt es sich um eine Auftragsverarbeitung?  **Hinweis:** Ein Auftragsverarbeitungsvertrag (AVV) ist immer dann erforderlich, wenn bei Einsatz einer Anwendung oder eines Dienstes die Verarbeitung personenbezogener Daten nicht lokal, sondern bei einem Dienstleister (Programmanbieter, Hostingdienstleister) erfolgt. | Art. 28 Abs. 1 DSGVO | - |  |  |  |
|  | **Gegenstand, Dauer und Form des Vertrages** |  |  |  |  |  |
| 2. | Wird der Auftrag schriftlich oder elektronisch geschlossen?  **Hinweis:** Anlagen müssen vorliegen und in den Vertrag eingebunden sein; Verweis allein genügt nicht. Neben der handschriftlichen Unterschrift genügt es, wenn der Anbieter den Vertrag (mit Anlagen) per Mail schickt, zum Download anbietet oder das unterschriebene Papier eingescannt wird. | Art. 28 Abs. 9 DSGVO |  |  |  |  |
| 3. | Gibt es eine Regelung zum Gegenstand des Vertrages? | Art. 28 Abs. 3 DSGVO |  |  |  |  |
| 4. | Sind Beginn und Ende des Auftrages im Vertrag geregelt?  **Hinweis:** Der Vertrag muss gelten, solange personenbezogene Daten für den Auftraggeber verarbeitet werden. Das gilt auch nach Beendigung bis zur Löschung der Daten. | Art. 28 Abs. 3 DSGVO |  |  |  |  |
|  | **Umfang, Art und Zweck der Datenverarbeitung** |  |  |  |  |  |
| 5. | Gibt es konkrete Weisungen, welche Verarbeitungen vom Auftragnehmer vorzunehmen sind? | Art. 28 Abs. 3 a DSGVO |  |  |  |  |
| 6. | Ist der Verwendungszweck im Vertrag geregelt? | Art. 28 Abs. 3 DSGVO |  |  |  |  |
| 7. | Sind die Datenarten vertraglich festgehalten oder bestimmt bzw. bestimmbar? | Art. 28 Abs. 3 DSGVO |  |  |  |  |
| 8. | Sind die Kategorien der Betroffenen dem Vertrag zu entnehmen? | Art. 28 Abs. 3 DSGVO |  |  |  |  |
|  | **Technisch-organisatorische Maßnahmen (TOM) (s. Anlage 1)** |  |  |  |  |  |
| 9. | Gibt es Regelungen zur Gewährleistung der Vertraulichkeit? | Art. 32 Abs. 1 b DSGVO |  |  |  |  |
| 10. | Gibt es Regelungen zur Gewährleistung der Integrität? | Art. 32 Abs. 1 b DSGVO |  |  |  |  |
| 11. | Gibt es Regelungen zur Gewährleistung der Datenverfügbarkeit? | Art. 32 Abs. 1 b DSGVO |  |  |  |  |
| 12. | Gibt es Regelungen zur Gewährleistung der Belastbarkeit der Systeme mit der Verarbeitung auf Dauer? | Art. 32 Abs. 1 b DSGVO |  |  |  |  |
| 13. | 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? | Art. 32 Abs. 1 c DSGVO |  |  |  |  |
| 14. | 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? | Art. 32 Abs. 1 c DSGVO |  |  |  |  |
|  | **Weisungsrecht** |  |  |  |  |  |
| 15. | Ist der Umfang des Weisungsrechts des Auftraggebers geregelt? | Art. 28 Abs. 3 a DSGVO |  |  |  |  |
|  | **Vertraulichkeitspflichten** |  |  |  |  |  |
| 16. | Gibt es Regelungen zu den Vertraulichkeitspflichten von Beschäftigten des Auftragnehmers? | Art. 28 Abs. 3 b DSGVO |  |  |  |  |
|  | **Unterauftragsverhältnisse** |  |  |  |  |  |
| 17. | Ist die Zulässigkeit von Unterauftragsverhältnissen geregelt? | Art. 28 Abs. 3 d i.V.m. Abs. 2 DSGVO |  |  |  |  |
| 18. | Falls ja, gibt es eine Regelung dazu, wie der Unterauftragnehmer zu beauftragen ist? | Art. 28 Abs. 3 d i.V.m. Abs. 4 DSGVO |  |  |  |  |
| 19. | Falls ja, gibt es eine Regelung dazu, wie neue Unterauftragnehmer vom Auftragnehmer zu genehmigen sind bzw. im Falle einer allgemeinen Genehmigung, dass neue Unterauftragnehmer dem Auftraggeber im Voraus benannt werden und dem Auftraggeber ein Widerspruchsrecht zusteht? | Art. 28 Abs. 3 d i.V.m. Abs. 2 DSGVO |  |  |  |  |
|  | **Unterstützung des Auftraggebers** |  |  |  |  |  |
| 20. | Ist geregelt, dass der Auftragnehmer den Auftraggeber bei der Geltendmachung von Rechten von betroffenen Personen unterstützt? | Art. 28 Abs. 3 e DSGVO |  |  |  |  |
| 21. | Ist geregelt, dass der Auftragnehmer den Auftraggeber bei der Einhaltung seiner Pflichten aus den Art. 32 bis 36 DSGVO unterstützt?  **Hinweis:** Bei diesen Pflichten handelt es sich um die technisch-organisatorischen Maßnahmen, Meldepflichten im Fall eines Datenschutzvorfalls, Information der von einem Datenschutzvorfall Betroffenen und die Erstellung einer Datenschutz-Folgeabschätzung in Abstimmung mit der Aufsichtsbehörde. | Art. 28 Abs. 3 f DSGVO |  |  |  |  |
| 22. | Gibt es Regelungen zu Kontrollrechten des Auftraggebers und entsprechende Duldungspflichten des Auftragnehmers?  **Hinweis:** z.B. Kontrollrechte vor Ort, Herausgabe von Informationen | Art. 28 Abs. 3 h DSGVO |  |  |  |  |
| 23. | Gibt es eine Regelung zu Kontrollrechten des Auftraggebers gegenüber etwaigen Unterauftragnehmern)  **Hinweis:** z.B. Kontrollrechte vor Ort, Herausgabe von Informationen | Art. 28 Abs. 3 d i.V.m. Abs. 4 DSGVO |  |  |  |  |
|  | **Informationspflichten des Auftragnehmers** |  |  |  |  |  |
| 24. | Gibt es eine Verpflichtung des Auftragnehmers, Verstöße gegen Datenschutzvorschriften (sog. Datenschutzvorfall) oder gegen die vom Auftraggeber erteilten Weisungen zu melden? | Art. 28 Abs. 3 a und f DSGVO |  |  |  |  |
| 25. | Ist im Vertrag eine Frist geregelt, binnen derer der Auftragnehmer nach Kenntnis eines Datenschutzvorfalles dies dem Auftraggeber zu melden hat.  **Hinweis:** Der Auftraggeber ist verpflichtet, einen Datenschutzvorfall innerhalb von 72 Stunden nach Bekanntwerden an die Aufsichtsbehörde zu melden. Dementsprechend muss die vereinbarte Frist so bemessen sein, dass der Auftraggeber nach Vorliegen der Informationen seinen Verpflichtungen nachkommen kann. | Art. 28 Abs. 3 f i.V.m. Art. 33 DSGVO |  |  |  |  |
|  | **Regelungen zur Rückgabe und Löschung der Daten** |  |  |  |  |  |
| 26. | Gibt es eine Regelung, die den Auftragnehmer verpflichtet, überlassene Daten nach Beendigung des Auftrags zurückzugeben bzw. für den Auftraggeber gespeicherte Daten zu löschen?  **Hinweis:** Es genügt nicht, wenn nur auf Verlangen des Auftraggebers gelöscht wird, der Auftraggeber keine Wahl zwischen Löschen und Rückgabe hat, die Löschfrist erst nach Vertragsschluss und nicht schon nach Ende der Verarbeitungsleistung besteht. | Art. 28 Abs. 3 g DSGVO |  |  |  |  |