Datenschutzrechtliche Bedingungen für die Beauftragung von Dienstleistern

Diese Bedingungen sollen die ordnungsgemäße Verarbeitung personenbezogener Daten sicherstellen und berücksichtigen die gesetzlichen Vorgaben des Artikel 28 der EU-Datenschutzgrundverordnung (DS-GVO).

1. Geltungsbereich, Gegenstand, Dauer

Diese Bedingungen finden Anwendung auf alle Aufträge, die der Auftraggeber im eigenen Namen dem Auftragnehmer erteilt. Mit Annahme des Auftrags verpflichtet sich der Auftragnehmer zur Einhaltung dieser Bedingungen.

2. Art und Zweck

2.1. Der Auftragnehmer bearbeitet die zur Verfügung gestellten Daten lediglich im Rahmen der vom Auftraggeber genannten Aufgaben. Bei Unklarheit darüber, ob die Verarbeitung dem Zweck der Beauftragung entspricht, muss sich der Auftragnehmer mit dem Auftraggeber abstimmen.

2.2. Die Art der Verarbeitung hat dem Zweck der Beauftragung zu entsprechen. Der Auftragnehmer kann die Mittel der Verarbeitung auswählen, diese müssen jedoch in einem datenschutzkonformen Verhältnis zum Zweck der Verarbeitung und Sensibilität der personenbezogenen Daten stehen und immer im Einklang mit den geltenden datenschutzrechtlichen Regelungen sein.

3. Art der Daten und Kategorien betroffener Personen

3.1. Die Art der zu verarbeitenden Daten wird durch die Art der konkreten Beauftragung bestimmt. Grundsätzlich kommen alle in Artikel 4 Nr. 1 DSGVO genannten personenbezogenen Daten in Betracht. Welche Daten der konkreten Verarbeitung zugrunde liegen, ergibt sich aus dem Gegenstand der Beauftragung.

3.2. Dem Auftragnehmer werden im Rahmen seiner Tätigkeit Daten vom Arbeitgeber, der zugleich auch Auftraggeber ist, zur Verfügung gestellt. Diese Daten betreffen aktuelle und ausgeschiedene Mitarbeiter des Auftraggebers sowie alle Versorgungsberechtigten, die sich aus dem Versorgungsversprechen des Arbeitgebers ergeben.

4. Rechte und Pflichten des Verantwortlichen

4.1. Der Auftraggeber hat das Recht, jederzeit dokumentierte Einzelweisungen über das Auftragsverhältnis zu erteilen. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt oder einer ordnungsgemäßen Begutachtung zuwiderläuft.

4.2. Der Auftragnehmer sichert zu, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind und verpflichtet sich zu ihrer Einhaltung. Er verpflichtet sich zur Verschwiegenheit hinsichtlich der ihm zur Kenntnis gelangten mündlichen oder schriftlichen Informationen, personenbezogenen Daten und überlassenen Unterlagen. Die zur Datenverarbeitung befugten Personen verpflichtet er zur Vertraulichkeit. Diese Verpflichtung gilt auch nach Beendigung des Vertrags fort.

4.3. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Anträge und Ansprüche betroffener Personen gemäß Kapitel III der DSGVO sowie bei Einhaltung der in Artikel 32 - 36 DSGVO genannten Pflichten.

4.4. Der Auftraggeber ist dazu berechtigt, jederzeit die Erhebung und Verwendung der Daten des Auftraggebers durch den Auftragnehmer einschließlich der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen des Auftragnehmers zu prüfen. Zur Durchführung von Kontrollen ist der Auftragnehmer entsprechend Artikel 28 Abs. 3 lit h DSGVO zur Mitwirkung verpflichtet.

4.5. Der Auftragnehmer ist verpflichtet, die ihm zur Verfügung gestellten Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden und strikt von sonstigen, bei ihm gespeicherten Datenbeständen zu trennen.

4.6. Der Auftragnehmer ist verpflichtet, die Daten nach Abschluss der Erbringung der Verarbeitungsleistungen – nach Wahl des Auftraggebers – vollständig datenschutzgerecht zu löschen (einschließlich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) und/oder an dem Auftraggeber zurück zugeben, sofern nicht nach dem Recht der Europäischen Union oder nationalem Recht eine Verpflichtung zur Speicherung besteht

4.7. Der Auftragnehmer ist berechtigt, zur Vertragsdurchführung Subunternehmen einzusetzen. Subunternehmen sind dabei keine Dienstleister, die reine Unterstützungsleistungen wie Telekommunikation usw. sind. Bei Abschluss dieser Vereinbarung setzt der Auftragnehmer die in der Anlage „Liste der wesentlichen Dienstleister“ bezeichneten Subunternehmen ein, zu dessen Einbeziehung der Auftragnehmer mit Auftragserteilung seine Zustimmung erteilt. Die jeweils aktuelle Liste der Subunternehmen ist über https://pm.hdi.de einsehbar.

4.8. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mit-

gliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

4.9. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

4.10. Der Auftragnehmer ist zur Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 28 Abs. 3 S. 2 lit. c, 32 DSGVO verpflichtet. Wegen weiterer Details wird auf die Übersicht und Erläuterungen am Ende der Bedingungen verwiesen.

5. Sonstiges

Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

Übersicht und Erläuterungen zu den technischen und organisatorischen Maßnahmen i. S. d. Artikel 32 DSGVO unter Einbeziehung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz

A. Vertraulichkeit (Artikel 32 Abs. 1 lit. b DSGVO)

1. Zutrittskontrolle

Kein unbefugter Zutritt zu Räumlichkeiten in denen Datenverarbeitungsanlagen stehen oder Dokumente gelagert werden

2. Zugangskontrolle

Keine unbefugte Systembenutzung, z.B. (sichere) Kennwörter, automatische Sperrmechanismen, Verschlüsselung von Datenträgern

3. Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B. Berechtigungskonzepte oder bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen

4. Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantentrennung

B. Pseudonymisierung (Artikel 32 Abs. 1 lit. a DSGVO; Artikel 25 Abs. 1 DSGVO)

Soweit erforderlich und sinnvoll ist zu erwägen, ob die Verarbeitung personenbezogener Daten in einer Weise erfolgt, bei der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen

C. Integrität (Artikel 32 Abs. 1 lit. b DSGVO)

1. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B. Verschlüsselung, Virtual Private Networks (VPN)

2. Eingabekontrolle

Sicherstellung, dass bei Eingabe, Veränderung oder Löschung von personenbezogenen Daten in Datenverarbeitungssystemen dieses auf protokollierter Art und Weise erfolgt (z.B. Versionierungen, Dokumentenmanagement)

D. Verfügbarkeit und Belastbarkeit (Artikel 32 Abs. 1 lit. b DSGVO)

1. Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall

E. Rasche Wiederherstellbarkeit (Artikel 32 Abs. 1 lit. c DSGVO)

Sofern notwendig, Sicherstellung von alternativen Datenverarbeitungen, wenn die eigentliche Datenverarbeitung ausfällt wie z.B. Ausweichhardware mit Zugriff auf Backup Daten.