

Vertrag über Auftragsverarbeitung

Firmenstempel

Auftraggeber

und

Dupp GmbH
Kühlhausstraße 1
35708 Haiger

Auftragnehmer

schließen nachfolgende Vereinbarung über die Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer:

1. Allgemeines

- a. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des Artikel 28 Abs 1 EU-DSGVO als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Datenverarbeitung im Auftrag ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich erteilt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsdatenverarbeitung gemäß Artikel 28 Abs. 3 EU-DSGVO und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.
- b. Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, meint dies die Verarbeitung im Sinne von Art. 4 Nr. 2 EU-DSGVO.

2. Gegenstand des Auftrags

- a) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag und nach Weisung. Gegenstand des Auftrages sind Tätigkeiten, die im Hauptvertrag und/oder in den Einzelverträgen und in der jeweiligen Produktbeschreibung konkretisiert sind. In den jeweiligen Verträgen ist auch die Laufzeit geregelt.
- b) Im Rahmen der Leistungserbringung kann der Auftragnehmer Zugang zu personenbezogenen Daten erhalten, um seine Verpflichtungen aus dem Vertrag zu erfüllen. Der Zugang erfolgt dabei ausschließlich zur Vertragserfüllung. Der Zugang zu den Daten ist dabei auf den Zeitraum der Beauftragung beschränkt.
- c) Der Auftraggeber hat den Auftragnehmer darüber in Kenntnis zu setzen, wenn besondere personenbezogene Daten im Sinne des Artikel 9 EU-DSGVO verarbeitet werden sollen.
- d) Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus dem zwischen den Vertragsparteien bestehenden Vertrag (Auftrag). Siehe hierzu Anlage: Spezifizierung der Auftragsverarbeitung gemäß Art. 28 DSGVO nach Produkten und Dienstleistungen

3. Kategorien von betroffenen Personen und Daten

Prüfen Sie, ob unten genannte Informationen der Kategorien oder Datenarten, durch Ihre Nutzung und Eingabe, bei uns oder eines unserer Dienste (Hosting, Cloud, etc.) verarbeitet werden. Wenn Sie auf einem Cloud-Dienst weitere Informationen Ihrer Kunden erfassen, sind die entsprechenden Auswahlfelder bei Kategorie und Datenarten festzulegen.

a. Kategorien von betroffenen Personen der Verarbeitung: (zutreffendes bitte ankreuzen oder ergänzen)

- | | |
|---|--|
| <input checked="" type="checkbox"/> Kunden | <input checked="" type="checkbox"/> Interessenten |
| <input checked="" type="checkbox"/> Nutzer | <input checked="" type="checkbox"/> Geschäftspartner |
| <input checked="" type="checkbox"/> Lieferanten | <input checked="" type="checkbox"/> Mitarbeiter |
| <input type="checkbox"/> Mitglieder | <input type="checkbox"/> Dienstleister |
| <input type="checkbox"/> Bewerber | <input type="checkbox"/> Praktikanten |
| <input type="checkbox"/> _____ | <input type="checkbox"/> _____ |

b. Betroffene Datenarten der Verarbeitung: (zutreffendes bitte ankreuzen oder ergänzen)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Adressdaten | <input checked="" type="checkbox"/> Ansprechpartner |
| <input checked="" type="checkbox"/> Mitarbeiterdaten | <input type="checkbox"/> Abrechnungsdaten |
| <input type="checkbox"/> Vertragsdaten | <input checked="" type="checkbox"/> Bankverbindung |
| <input checked="" type="checkbox"/> Stammdaten | <input checked="" type="checkbox"/> E-Mail Nachrichten |
| <input type="checkbox"/> Video und Bilder | <input type="checkbox"/> Nutzungsdaten |
| <input type="checkbox"/> _____ | <input type="checkbox"/> _____ |

4. Pflichten des Auftragnehmers

- Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat oder ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 S. 2 lit. a EU-DSGVO vorliegt.
- Der Auftragnehmer wird den Auftraggeber bei der Durchführung von Kontrollen durch den Auftraggeber unterstützen und an der vollständigen und zügigen Abwicklung der Kontrolle mitwirken.
- Der Auftragnehmer gewährleistet im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen und dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.
- Der Auftragnehmer ist nach Art 28 Abs. 3 Lit. c, 32 DSGVO i.V. mit Art 5 Abs 1, Abs. 2 verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

- e. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung(en) solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.
- f. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder gegen die erteilten Weisungen des Auftraggebers sowie Unregelmäßigkeiten bei der Verarbeitung unverzüglich mitzuteilen.
- g. Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb des Sitzes (Homeoffice), ist nur auf Datenendgeräten der Firma Dupp zulässig. Für den Nutzungsumgang mit Personen Daten wurde eine Zusatzvereinbarung mit dem jeweiligen Dupp Mitarbeiter getroffen und liegt vor.
- h. Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb des Sitzes eines Subunternehmers ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig.
- i. Erteilt der Auftraggeber Weisungen ohne datenschutzrechtlichen Bezug, die über die zur Durchführung der vereinbarten Auftragsverarbeitung erforderlichen Leistungen hinausgehen (z. B. zusätzliche Auswertungen, Sonderberichte oder individuelle Anpassungen), kann der Auftragnehmer hierfür ein angemessenes Entgelt verlangen. Der Auftragnehmer informiert den Auftraggeber vorab schriftlich über den geschätzten Aufwand.
- j. Der Auftragnehmer unterstützt den Auftraggeber gemäß Art. 28 Abs. 3 lit. f DSGVO bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
 - k. die Unterstützung des Auftraggebers bei dessen technischen und organisatorischen Maßnahmen
 - l. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
 - m. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
 - n. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung und
 - o. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde. Nach der Meldung einer Verletzung personenbezogener Daten durch den Auftragnehmer an den Auftraggeber entscheidet der Auftraggeber in alleiniger Verantwortung, ob die Voraussetzungen für eine Meldung an Behörden bzw. betroffene Personen vorliegen, und nimmt die Meldungen in alleiniger Verantwortung vor.

5. Rechte und Pflichten des Auftraggebers

- a. Der Auftraggeber ist für die Erfüllung der gesetzlichen Pflichten des Verantwortlichen verantwortlich. Der Auftragnehmer gewährleistet die Einhaltung aller ihn treffenden vertraglichen und gesetzlichen Pflichten in seiner Rolle als Auftragsverarbeiter.
- b. Der Auftraggeber kann während der Laufzeit dieses Vertrags jederzeit die Berichtigung, Sperrung, Löschung oder Herausgabe von personenbezogenen Daten verlangen. Der Auftragnehmer hat diese Anfragen unverzüglich, spätestens jedoch binnen 5 Werktagen, umzusetzen.
- c. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber ist verpflichtet, das Ergebnis in geeigneter Weise zu dokumentieren.

- d. Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind unverzüglich vom Auftraggeber schriftlich oder in Textform (z.B. E-Mail) zu bestätigen.
- e. Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern sensitive Daten vom Auftragnehmer für den Auftraggeber verarbeitet werden, wird der Auftraggeber weisungsberechtigte Personen konkret benennen:
- f. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich oder in Textform mitteilen.
- g. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

6. Kontrollbefugnisse

- a. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.
- b. Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes a erforderlich ist.
- c. Soweit erforderlich, kann der Auftraggeber nach vorheriger Ankündigung eines Termins die Kontrolle im Sinne des Absatzes a am Sitz des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber stellt sicher, dass die Kontrollen nur im notwendigen Umfang durchgeführt werden.
- d. Kosten im Zusammenhang mit Kontrollen gemäß Ziffer 6 dieses Vertrags trägt grundsätzlich der Auftragnehmer. Eine Kostenbeteiligung des Auftraggebers erfolgt nur dann, wenn es sich um zusätzliche, freiwillige Kontrollen handelt, die nicht durch einen Verstoß des Auftragnehmers gegen datenschutzrechtliche oder vertragliche Pflichten veranlasst sind.

7. Weisungsbefugnis

- a. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen bezüglich Zwecks, Art und Umfang der Verarbeitung von Daten an den Auftragnehmer zu erteilen. Die Weisungen müssen schriftlich erfolgen. Dem Auftragnehmer soll eine angemessene Frist zur Umsetzung der Weisungen gesetzt werden.
- b. Mehraufwände, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, werden dem Auftraggeber in Rechnung gestellt.

8. Unterauftragsverhältnisse

- a. Der Auftragnehmer darf Subunternehmen (weitere Auftragsverarbeiter) nur nach vorheriger Zustimmung des Auftraggebers unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4, 9 EU-DSGVO, welche sowohl schriftlich als auch in einem elektronischen Format erfolgen kann, beauftragen.
- b. Die Übersicht der beauftragten Subunternehmer befindet sich im Anhang zu diesem Vertrag (siehe Anlage „Verzeichnis der Subunternehmer gemäß Art. 28 Abs. 3 DSGVO“) und ist Bestandteil dieser Vereinbarung.

- c. Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach Artikel 32 EU-DSGVO geforderten Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf schriftliche Anfrage dem Auftraggeber zu übermitteln.
- d. Der Auftragnehmer verpflichtet sich, mit jedem eingesetzten Unterauftragsverarbeiter einen Vertrag gemäß Art. 28 Abs. 4 DSGVO zu schließen, die sämtlichen datenschutzrechtlichen Pflichten aus diesem Vertrag in gleichem Umfang weitergibt. Auf Verlangen hat der Auftragnehmer diese Verträge nachzuweisen.

9. Fernmelde- und Datengeheimnis

- a. Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des Artikel 28 Abs 3 S. 2 lit. b EU-DSGVO verpflichtet.
- b. Der Auftragnehmer gewährleistet, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer gewährleistet ferner, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis i.S.d. Artikel 28 Abs. S. 2 3 lit. b EU-DSGVO verpflichtet werden. Sofern der Auftragnehmer im Zusammenhang mit Leistungen für den Auftraggeber an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirkt, ist er verpflichtet, die hieran beteiligten Beschäftigten schriftlich auf das Fernmeldegeheimnis i.S.d. § 88 TKG zu verpflichten. Der Auftragnehmer sichert zu, seine Pflichten aus dem TKB einzuhalten.

10. Betroffenenrechte

- a. Der Auftragnehmer unterstützt den Auftraggeber aktiv bei der Wahrung der Betroffenenrechte gemäß Kapitel III der DSGVO. Eingehende Anfragen von Betroffenen leitet der Auftragnehmer unverzüglich an den Auftraggeber weiter und trifft auf dessen Anforderung hin geeignete technische und organisatorische Maßnahmen zur Unterstützung bei Auskunft, Berichtigung, Löschung oder Daten Portabilität. Etwaige Zusatzkosten werden nur in dem Umfang erstattet, wie sie über vertraglich vereinbarte Leistungen hinausgehen.

11. Vergütung

- a. Die Vergütung wird gesondert vereinbart.

12. Technische und organisatorische Maßnahmen

- a. Siehe Anlage

13. Laufzeit

- a. Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages und/oder Einzelauftrages.

14. Vertragsende

- a. Nach Beendigung des Vertrags hat der Auftragnehmer sämtliche personenbezogenen Daten, einschließlich etwaiger Sicherungskopien, zu löschen oder an den Auftraggeber zurückzugeben, soweit keine anderweitige Verpflichtung zur Aufbewahrung nach dem Recht der Union oder der Mitgliedstaaten besteht. Die Löschung ist vom Auftragnehmer in geeigneter Weise zu dokumentieren. Die Dokumentation ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

15. Schlussbestimmungen

- a. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.
- b. Für sämtliche Rechtsbeziehungen zwischen den Vertragspartnern gilt ausschließlich das für die Rechtsbeziehungen inländischer Parteien maßgebliche Recht der Bundesrepublik Deutschland unter Ausschluss der Bestimmungen des Internationalen Privatrechts.
- c. Gerichtsstand ist Dillenburg, sofern der Kunde Vollkaufmann ist und der Vertrag zum Betrieb seines Handelsgewerbes gehört oder keinen festen Wohnsitz in der Bundesrepublik Deutschland hat. Ein etwaiger ausschließlicher Gerichtsstand bleibt hiervon unberührt.
- d. Sämtliche Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- e. Im Falle eventueller Konflikte zwischen dieser Vereinbarung und ggfs. anderweitig zwischen den Parteien bereits getroffenen oder noch zu treffenden Vereinbarungen geht diese Vereinbarung vor, sofern und soweit nichts Anderweitiges zwischen den Parteien ausdrücklich schriftlich vereinbart worden ist. Satz 1 gilt auch dann, sofern und soweit eine ggfs. anderweitig zwischen den Parteien bereits geschlossene oder noch zu schließende Vereinbarung eine Regelung enthält, die einen Vorrang der anderweitigen Vereinbarung im Kollisionsfalle vorsieht.
- f. Sollte eine Datenschutzaufsichtsbehörde oder ein Gericht der Auffassung sein, dass
 - a. die im Auftrag vorgenommenen Datenerhebungen, -verarbeitungen und/oder -nutzungen,
 - b. Regelungen in dieser Vereinbarung oder das Fehlen bestimmter Regelungen, oder
 - c. die getroffenen technisch-organisatorischen Maßnahmen oder das Fehlen bestimmter technisch-organisatorischer Maßnahmen
- g. gegen europäisches oder deutsches Datenschutzrecht verstoßen, so handeln die Parteien eine Änderung/Ergänzung dieser Vereinbarung und/oder des Verfahrens nach den Grundsätzen von Treu und Glauben aus, um die aufgezeigten Defizite zu beseitigen.
- h. Sollten durch Gesetzesänderungen Änderungen oder Ergänzungen dieser Vereinbarung erforderlich oder offenbar werden, so handeln die Parteien eine Änderung/Ergänzung dieser Vereinbarung nach den Grundsätzen von Treu und Glauben aus. Dies gilt auch, soweit durch gesetzliche Vorschriften Änderungen des Verarbeitungsverfahrens selbst notwendig werden. Sätze 1 und 2 gelten nicht für Bestimmungen, die über die gesetzlichen Anforderungen hinausgehen, aber nicht gegen gesetzliche Bestimmungen verstoßen.
- i. Die Pflichten zur Aushandlung von Änderungen oder Ergänzungen dieser Vereinbarung und/oder des Verfahrens nach den Absätzen f und g gelten nicht, soweit die betroffenen Defizite bereits durch die Weisungsrechte des Auftraggebers beseitigt werden können.

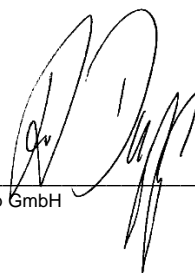
- j. Dieser Vertrag tritt in Kraft, sobald er vom Auftraggeber unterzeichnet wurde. Beide Parteien verpflichten sich, eine vollständige, gegengezeichnete Version aufzubewahren.

Ort, Datum

rechtsverbindliche Unterschrift Auftraggeber

Haiger

Dupp GmbH



Dupp GmbH
Kühlhausstr. 1
35708 Haiger
Tel.: 02773/92090 Fax 02773/920999
info@dupp.de

Anlage: Technische und organisatorische Maßnahmen (TOM)

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene *Daten verarbeitet oder genutzt werden, zu verwehren.*

- | | |
|---|--|
| <input checked="" type="checkbox"/> Alarmanlage im Serverraum | <input checked="" type="checkbox"/> Transponder-Schließsystem |
| <input type="checkbox"/> Automatisches Zugangskontrollsystem | <input checked="" type="checkbox"/> Manuelles Schließsystem |
| <input checked="" type="checkbox"/> Schließsystem mit Codesperre | <input type="checkbox"/> Videoüberwachung der Zugänge |
| <input type="checkbox"/> Biometrische Zugangssperren | <input checked="" type="checkbox"/> Sicherheitsschlösser |
| <input checked="" type="checkbox"/> Bewegungsmelder | <input checked="" type="checkbox"/> Personenkontrolle beim Empfang |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input type="checkbox"/> Protokollierung der Besucher | |
| <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen | |

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- | | |
|--|---|
| <input checked="" type="checkbox"/> Zuordnung von Benutzerrechten | <input checked="" type="checkbox"/> Erstellen von Benutzerprofilen |
| <input checked="" type="checkbox"/> Passwortvergabe | <input type="checkbox"/> Authentifikation mit biometrischen Verfahren |
| <input checked="" type="checkbox"/> Authentifikation mit Benutzername / Passwort | <input checked="" type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen |
| <input type="checkbox"/> PC-Gehäuseverriegelungen | <input checked="" type="checkbox"/> Einsatz von VPN-Technologie |
| <input type="checkbox"/> Sperren von externen Schnittstellen (USB etc.) | |
| <input type="checkbox"/> Einsatz von Intrusion-Detection-Systemen | <input checked="" type="checkbox"/> Verschlüsselung von mobilen Datenträgern |
| <input checked="" type="checkbox"/> Zugang Beschränkung von Smartphone-Inhalten | <input checked="" type="checkbox"/> Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) |
| <input checked="" type="checkbox"/> Einsatz von Anti-Viren-Software | <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern in Laptops / Notebooks |
| <input checked="" type="checkbox"/> Einsatz einer Hardware-Firewall gemäß dem Stand der aktuellen Technik. | <input type="checkbox"/> Einsatz einer Software-Firewall |

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- | | |
|---|--|
| <input type="checkbox"/> Erstellen eines Berechtigungskonzepts | <input checked="" type="checkbox"/> Verwaltung der Rechte durch Systemadministrator |
| <input checked="" type="checkbox"/> Anzahl der Administratoren auf das „Notwendigste“ reduziert | <input checked="" type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge und Passwort Komplexität, nach Vorgaben der Softwarehersteller, 2 faktor-Authentifizierung wenn möglich |
| <input type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | <input checked="" type="checkbox"/> Sichere Aufbewahrung von Datenträgern |
| <input type="checkbox"/> physische Löschung von Datenträgern vor Wiederverwendung | <input checked="" type="checkbox"/> ordnungsgemäße Vernichtung von Datenträgern (DIN 66399) |
| <input checked="" type="checkbox"/> Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) | <input checked="" type="checkbox"/> Protokollierung der Vernichtung von Datenträgern |
| <input type="checkbox"/> Verschlüsselung von Datenträgern | |

4. Weitergabe Kontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln | <input checked="" type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
| <input type="checkbox"/> E-Mail-Verschlüsselung | <input type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |
| <input checked="" type="checkbox"/> Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen | <input type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen |
| <input checked="" type="checkbox"/> Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen | <input checked="" type="checkbox"/> Gesicherter Datenverkehr über z.B. sFTP |

- Passwort geschützte Dateien wie z.B. Zip oder Rar Dateien
- TeamViewer verschlüsselte Datenübertragung

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung von Daten z.B. im TFS System oder Ticketsystem
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) Artikel 28 EU-DSGVO
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit
- Auftragnehmer hat Datenschutzbeauftragten bestellt und kann unter datenschutz@dupp.de kontaktiert werden
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags / Vertragsverhältnisses
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen

- Techniken zur Überwachung der Temperatur in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Separate Steckdosen im Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfallplans / Wiederanlaufplan
- Serverräume nicht unter sanitären Anlagen

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem

9. Datenschutz-Management

Maßnahmen, zur regelmäßigen Überprüfung, Bewertung und Evaluierung.

- Software-Lösung für Datenschutz Management im Einsatz
- Zentrale Dokumentation aller Verfahrensweisen und Regelung zum Datenschutz mit Zugriffsmöglichkeit der Mitarbeiter bei Bedarf
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen min. einmal pro Jahr
- Eine Datenschutz-Folgeabschätzung wird bei Bedarf durchgeführt
- Interner Datenschutzbeauftragter Kontakt unter datenschutz@dupp.de
- Regelmäßige Sensibilisierung der Mitarbeiter mindestens einmal pro Jahr
- Unterweisung von Mitarbeiter auf Vertraulichkeit und Datengeheimnis
- Die Organisation kommt den Informationspflichten nach Art. 13 /14 der DSGVO nach

10. Incident Response Management

Maßnahmen, zur Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Einsatz von Firewall und regelmäßige Aktualisierung | <input checked="" type="checkbox"/> Einsatz von Spamfilter und deren regelmäßige Aktualisierung |
| <input checked="" type="checkbox"/> Einsatz von Virens Scanner und deren regelmäßige Aktualisierung | <input checked="" type="checkbox"/> Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen |
| <input checked="" type="checkbox"/> Formaler Prozess und Verantwortlichkeiten zur Nacharbeitung von Sicherheitsvorfällen und Datenpannen | <input checked="" type="checkbox"/> Dokumentation von Sicherheitsvorfällen und Datenpannen im Datenschutz Management System. |

11. Datenschutzfreundliche Voreinstellungen

- | | |
|--|--|
| <input checked="" type="checkbox"/> Es werden nur die Daten erhoben, die für den jeweiligen Zweck erforderlich sind. | <input checked="" type="checkbox"/> Einfache Ausübung des Wiederrufrechts des Betroffenen durch technische Maßnahmen |
|--|--|

Die einzelnen Punkte der technischen und organisatorischen Maßnahmen (TOM) der Firma Dupp GmbH wurden vom Auftraggeber mit Unterschrift des Vertrags über Auftragsverarbeitung zur Kenntnis genommen und akzeptiert.

Letzte Aktualisierung: 05/2025

Anlage: Verzeichnis der Subunternehmer gemäß Art. 28 Abs. 3 DSGVO

Der Auftragnehmer setzt zur Erfüllung seiner vertraglichen Pflichten folgende Subunternehmer ein, die im Rahmen der Auftragsverarbeitung im Sinne von Art. 28 DSGVO tätig werden. Eine Datenverarbeitung durch diese Subunternehmer erfolgt ausschließlich im Umfang und zu den Zwecken, wie im jeweiligen Haupt- oder Einzelvertrag beschrieben.

Nr.	Subunternehmer	Anschrift	Leistung / Zweck	Ort der Datenverarbeitung	Drittlandübermittlung	Rechtsgrundlage
1	IONOS SE	Elgendorfer Str. 57, 56410 Montabaur	Hosting / Domains E-Mail-Dienste	Deutschland	Nein	–
2	Host Europe GmbH	Pilgrimstraße 6, 50674 Köln	Webhosting	Deutschland	Nein	–
3	shopware AG	Ebbinghoff 10, 48624 Schöppingen	Onlineshop- System	Deutschland	Nein	–
4	Gambio GmbH	Parallelweg 30, 28219 Bremen	Onlineshop- System	Deutschland	Nein	–
5	42 Software GmbH	Leißstraße 4, 83620 Feldkirchen-Westerham	Hersteller ERP System	Deutschland	Nein	–
6	Profihost GmbH	Hildesheimer Straße 25, 30880 Laatzen	Hosting- Dienstleistungen	Deutschland	Nein	–
7	Microsoft Corporation	One Microsoft Way, Redmond, WA 98052-6399, USA	Cloud-Dienste (Microsoft 365, MS Teams)	EU	Nein	EU- Standardvertragsklauseln (SCC)
8	TeamViewer Germany GmbH	Bahnstraße 16, 73037 Göppingen	Fernwartung	EU	Nein	–

Hinweise: Stand 05/2025

Der Auftragnehmer verpflichtet sich, alle vertraglichen Pflichten aus dem Auftragsverarbeitungsvertrag im Sinne von Art. 28 Abs. 4 DSGVO vollständig an die genannten Subunternehmer weiterzugeben.

Bei Drittlandübermittlungen werden geeignete Garantien im Sinne von Art. 46 DSGVO getroffen (z. B. Standardvertragsklauseln).

Die Liste wird bei Änderungen aktualisiert und dem Auftraggeber rechtzeitig zur Verfügung gestellt.

Anlage: Spezifizierung der Auftragsverarbeitung gemäß Art. 28 DSGVO nach Produkten und Dienstleistungen

Diese Anlage konkretisiert, welche der im Hauptvertrag vereinbarten Leistungen und im Rahmen der Nutzung der Produkte des Auftragnehmers eine Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers im Sinne des Art. 28 DSGVO darstellen.

Produkt sync4:

1. Installation und Konfiguration:
 - Installation und Konfiguration von Softwareprodukten auf Systemen des Auftraggebers, die personenbezogene Daten verarbeiten oder speichern, inklusive der dabei anfallenden Protokollierungs- oder Konfigurationsdaten, die Personenbezug aufweisen können.
2. Fernwartung:
 - Zugriff auf die IT-Systeme des Auftraggebers zum Zwecke der Installation, Konfiguration, Aktualisierung, Pflege, Fehleranalyse und Fehlerbeseitigung von Software- und/oder Hardwareprodukten, soweit diese Systeme personenbezogene Daten verarbeiten oder speichern.
3. Individualprogrammierung:
 - Entwicklung, Anpassung und Test von Software-Modulen, bei denen der Auftragnehmer Zugriff auf Testdaten oder (nach expliziter Freigabe und unter Aufsicht des Auftraggebers) auf Echtdaten erhält, die personenbezogene Daten enthalten können.
4. Aktualisierung und Pflege:
 - Einspielen von Updates, Patches und neuen Versionen für Softwareprodukte auf Systemen des Auftraggebers, die personenbezogene Daten verarbeiten oder speichern.
5. Fehleranalyse und Fehlerbeseitigung:
 - Analyse von Fehlermeldungen, Logfiles oder Systemzuständen auf den Systemen des Auftraggebers, die personenbezogene Daten enthalten können, zur Identifizierung und Behebung von Störungen.

Produkt desk4:

1. Hosting:
 - Bereitstellung der desk4-Software, als gehostete Dienstleistung (SaaS) gemäß Hauptvertrag.
2. Fernwartung:
 - Zugriff auf die IT-Systeme des Auftraggebers zum Zwecke der Installation, Konfiguration, Aktualisierung, Pflege, Fehleranalyse und Fehlerbeseitigung von Software- und/oder Hardwareprodukten, soweit diese Systeme personenbezogene Daten verarbeiten oder speichern.

3. Individualprogrammierung:
 - Entwicklung, Anpassung und Test von Software-Modulen, bei denen der Auftragnehmer Zugriff auf Testdaten oder (nach expliziter Freigabe und unter Aufsicht des Auftraggebers) auf Echtdateien erhält, die personenbezogene Daten enthalten können.
4. Aktualisierung und Pflege:
 - Einspielen von Updates, Patches und neuen Versionen für Softwareprodukte auf Systemen des Auftraggebers, die personenbezogene Daten verarbeiten oder speichern.
5. Fehleranalyse und Fehlerbeseitigung:
 - Analyse von Fehlermeldungen, Logfiles oder Systemzuständen auf den Systemen des Auftraggebers, die personenbezogene Daten enthalten können, zur Identifizierung und Behebung von Störungen.

Produkte von 42 Software:

1. Installation und Konfiguration:
 - Installation und Konfiguration von Softwareprodukten auf Systemen des Auftraggebers, die personenbezogene Daten verarbeiten oder speichern, inklusive der dabei anfallenden Protokollierungs- oder Konfigurationsdaten, die Personenbezug aufweisen können.
2. Fernwartung:
 - Zugriff auf die IT-Systeme des Auftraggebers zum Zwecke der Installation, Konfiguration, Aktualisierung, Pflege, Fehleranalyse und Fehlerbeseitigung von Software- und/oder Hardwareprodukten, soweit diese Systeme personenbezogene Daten verarbeiten oder speichern.
3. Individualprogrammierung:
 - Entwicklung, Anpassung und Test von Software-Modulen, bei denen der Auftragnehmer Zugriff auf Testdaten oder (nach expliziter Freigabe und unter Aufsicht des Auftraggebers) auf Echtdateien erhält, die personenbezogene Daten enthalten können.
4. Aktualisierung und Pflege:
 - Einspielen von Updates, Patches und neuen Versionen für Softwareprodukte auf Systemen des Auftraggebers, die personenbezogene Daten verarbeiten oder speichern.
5. Fehleranalyse und Fehlerbeseitigung:
 - Analyse von Fehlermeldungen, Logfiles oder Systemzuständen auf den Systemen des Auftraggebers, die personenbezogene Daten enthalten können, zur Identifizierung und Behebung von Störungen.