**VEREINBARUNG über eine AUFTRAGSVERARBEITUNG[[1]](#footnote-1)**

**VEREINBARUNG**

Der/Die Verantwortliche: Auftragsverarbeiter:in:[[2]](#footnote-2)

DI Max Mustermann *oder* *[xxx]*

Max Mustermann ZT GmbH *[Adresse]*

Musterweg 1

0000 Musterdorf

(im Folgenden Auftraggeber:in) (im Folgenden Auftragnehmer:in)

# Gegenstand der Vereinbarung

1. Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: [*möglichst detaillierte Beschreibung der Aufgaben des Auftragnehmers/der Auftragnehmerin, einschließlich Art und Zweck der vorgesehenen Verarbeitung].*

*[Falls es einen bereits bestehenden Rahmenvertrag, Werkvertrag, Leistungsvereinbarung, udgl gibt]* Diese Vereinbarung ist als Ergänzung zu [z.B. *Vertrag, samt Datum ergänzen*] zu verstehen.

1. Folgende Datenkategorien werden verarbeitet: [*Datenkategorien aufzählen, z.B. Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltdaten, usw*].
2. Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: [*Betroffenenkategorien ergänzen, z.B. Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte usw.*]

# Dauer der Vereinbarung *[alternativ]:*

* Die Vereinbarung endet mit einmaliger Durchführung der Arbeiten.
* Die Vereinbarung endet automatisch mit Beendigung des [*Titel des der Auftragsverarbeitung zugrundeliegenden Hauptvertrages, wie z.B: Auftrags- oder Werkvertrages, samt Datum ergänzen*].
* Die Vereinbarung ist befristet abgeschlossen und endet mit *[Fristende eintragen]*
* Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von *[Kündigungsfrist eintragen, z.B. ein Monat]* zum [*Kündigungstermin eintragen, z.B. Kalenderviertaljahr*] gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

# Pflichten des Auftragnehmers

1. Der/die Auftragnehmer:in verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers/der Auftraggeberin zu verarbeiten. Erhält der/die Auftragnehmer:in einen behördlichen Auftrag, Daten des Auftraggebers/der Auftraggeberin herauszugeben, so hat er/sie - sofern gesetzlich zulässig - den Auftraggeber/die Auftraggeberin unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers/der Auftraggeberin eines schriftlichen Auftrages.
2. Der Auftragnehmer/die Auftragnehmerin erklärt rechtsverbindlich, dass er/sie alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer/der der Auftragnehmerinaufrecht.
3. Der Auftragnehmer/die Auftragnehmerin erklärt rechtsverbindlich, dass er/sie alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1 zu entnehmen).
4. Der Auftragnehmer/die Auftragnehmerin ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber/die Auftraggeberin die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber/der Auftraggberin alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer/die Auftragnehmerin gerichtet und lässt dieser/dieser erkennen, dass der Antragsteller/die Antragstellerin ihn/sie irrtümlich für den Auftraggeber/die Auftraggeberin der von ihm/ihr betriebenen Datenverarbeitung hält, hat der Auftragnehmer/die Auftragnehmerin den Antrag unverzüglich an den Auftraggeber/die Auftraggeberin weiterzuleiten und dies dem Antragsteller/der Antragstellerin mitzuteilen.
5. Der Auftragnehmer/die Auftragnehmerin unterstützt den Auftraggeber/die Auftraggeberin bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).
6. Der Auftragnehmer/die Auftragnehmerin wird darauf hingewiesen, dass er/sie für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.
7. Dem Auftraggeber/der Auftraggeberin wird hinsichtlich der Verarbeitung der von ihm/ihr überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch von ihm/ihr beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer/die Auftragnehmerin verpflichtet sich, dem Auftraggeber/der Auftraggberin jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.
8. Der Auftragnehmer/die Auftragnehmerin ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber/der Auftraggeberin zu übergeben *[bzw. alternativ]* in dessen Auftrag zu vernichten. Wenn der Auftragnehmer/die Auftragnehmerin die Daten in einem speziellen technischen Format verarbeitet, ist er/sie verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers/der Auftraggeberin in dem Format, in dem er die Daten vom Auftraggeber/der Auftraggeberin erhalten hat oder in einem anderen, gängigen Format herauszugeben.
9. Der Auftragnehmer/die Auftragnehmerin hat den Auftraggeber/die Auftraggeberin unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

# Ort der Durchführung der Datenverarbeitung *[alternativ]:*

* Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.
* Datenverarbeitungstätigkeiten werden zumindest zum Teil auch außerhalb der EU bzw des EWR durchgeführt, und zwar in *[Staaten aufzählen].* Das angemessene Datenschutzniveau[[3]](#footnote-3) ergibt sich aus *[alternativ]:*
* einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
* einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO.
* verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO.
* Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.
* genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
* einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO.
* von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO.
* einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

# Sub-Auftragsverarbeiter:IN *[alternativ]:*

* Der Auftragnehmer/die Auftragnehmerin ist nicht berechtigt, einen Sub-Auftragsverarbeiter/eine Sub-Auftragsverarbeiterin heranzuziehen.
* Der Auftragnehmer/die Auftragnehmerin darf folgendes Unternehmen als Sub-Auftragsverarbeiter:in hinzuziehen: *[Firmenname und Sitz ergänzen, Art der Tätigkeiten].*

Beabsichtigte Änderungen des Sub-Auftragsverarbeiters/der Sub-Auftragsverarbeiterin sind dem Auftraggeber/der Auftraggeberin so rechtzeitig schriftlich bekannt zu geben, dass er/sie dies allenfalls untersagen kann. Der Auftragnehmer/die Auftragnehmerin schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter/der Sub-Auftragsverarbeiterin ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter/die Sub-Auftragsverarbeiterin dieselben Verpflichtungen eingeht, die dem Auftragnehmer/der Auftragnehmerin auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter/die Sub-Auftragsverarbeiterin seinen/ihren Datenschutzpflichten nicht nach, so haftet der Auftragnehmer/die Auftragnehmerin gegenüber dem Auftraggeber/der Auftraggeberin für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters/der Sub-Auftragsverarbeiterin.

* Der Auftragnehmer/die Auftragnehmerin kann Sub-Auftragsverarbeiter:innen [*Tätigkeiten*] hinzuziehen.

Er/sie hat den Auftraggeber/die Auftraggberin von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters/einer Sub-Auftragsverarbeiterin so rechtzeitig zu verständigen, dass er/sie dies allenfalls untersagen kann. Der Auftragnehmer/die Auftragnehmerin schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter/der Sub-Auftragsverarbeiterin ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter/die Sub-Auftragsverarbeiterin dieselben Verpflichtungen eingeht, die dem Auftragnehmer/der Auftragnehmerin auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter/die Sub-Auftragsverarbeiterin seinen/ihren Datenschutzpflichten nicht nach, so haftet der Auftragnehmer/die Auftragnehmerin gegenüber dem Auftraggeber/der Auftraggeberin für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters/der Sub-Auftragsverarbeiterin.

|  |  |  |
| --- | --- | --- |
| [*Ort*], am [*Datum*] |  | [*Ort*], am [*Datum*] |
| *Für den Auftraggeber/der Auftraggeberin:* |  | *Für den Auftragnehmer/der Auftragnehmerin:* |
| ....................................................  [*Name samt Funktion*] |  | ....................................................  [*Name samt Funktion*] |

# Anlage ./1 – Technisch-organisatorische MaSSnahmen[[4]](#footnote-4)

## **A. Vertraulichkeit[[5]](#footnote-5)**

**Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

|  |  |
| --- | --- |
| Schlüssel | Magnet- oder Chipkarten |
| Elektrische Türöffner | Portier |
| Sicherheitspersonal | Alarmanlagen |
| Videoanlage | Einbruchshemmende Fenster und/oder Sicherheitstüren |
| Anmeldung beim Empfang mit Personenkontrolle | Begleitung von Besuchern im Unternehmensgebäude |
| Tragen von Firmen-/Besucherausweisen | Sonstiges: |

**Zugangskontrolle**: Schutz vor Systembenutzung durch Unbefugte durch:

|  |  |
| --- | --- |
| Kennwörter (einschließlich entsprechender Policy) | Verschlüsselung von Datenträgern |
| Automatische Sperrmechanismen | Sonstiges: |
| Zwei-Faktor-Authentifizierung |  |

**Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

|  |  |
| --- | --- |
| Standard-Berechtigungsprofile auf „need to know-Basis“[[6]](#footnote-6) | Standardprozess für Berechtigungsvergabe |
| Protokollierung von Zugriffen | Sichere Aufbewahrung von Speichermedien |
| Periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten | Datenschutzgerechte Wiederverwendung von Datenträgern |
| Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger | Clear-Desk/Clear-Screen Policy |
| Sonstiges: |  |

**Pseudonymisierung[[7]](#footnote-7)**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

|  |  |
| --- | --- |
| Ja | Nein |

**Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

|  |  |
| --- | --- |
| Ja | Nein |

## **B. DatenIntegrität[[8]](#footnote-8)**

**Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

|  |  |
| --- | --- |
| Verschlüsselung von Datenträgern | Verschlüsselung von Dateien |
| Virtual Private Networks (VPN) | Elektronische Signatur |
| Sonstiges: |  |

**Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

|  |  |
| --- | --- |
| Protokollierung | Dokumentenmanagement |
| Sonstiges: |  |

## **C. Verfügbarkeit[[9]](#footnote-9) und Belastbarkeit[[10]](#footnote-10)**

**Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

|  |  |
| --- | --- |
| Backup-Strategie (online/offline; on-site/off-site) | Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat) |
| Virenschutz | Firewall |
| Meldewege und Notfallpläne | Security Checks auf Infrastruktur- und Applikationsebene |
| Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum | Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern |
| Sonstiges: |  |

Rasche **Wiederherstellbarkeit:**

|  |  |
| --- | --- |
| Ja | Nein |

## **D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

**Datenschutz-Management**, einschließlich regelmäßiger Mitarbeiter-Schulungen:

|  |  |
| --- | --- |
| Ja | Nein |

**Incident-Response-Management[[11]](#footnote-11)**:

|  |  |  |
| --- | --- | --- |
| Ja |  | Nein |

**Datenschutzfreundliche Voreinstellungen[[12]](#footnote-12)**:

|  |  |
| --- | --- |
| Ja | Nein |

**Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch:

|  |  |
| --- | --- |
| Eindeutige Vertragsgestaltung | Formalisiertes Auftragsmanagement |
| Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS) | Vorabüberzeugungspflicht |
| Nachkontrollen | Sonstiges: |

1. Dieser Mustervertrag ist auf eine Auftragsverarbeitung in Österreich, innerhalb des EWR oder in [Staaten mit angemessenem Datenschutzniveau](https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_de) zugeschnitten und soll lediglich bei der Abdeckung der Mindestanforderungen unterstützen. Für die Auftragsverarbeitung in Drittstaaten ist die Verwendung von [Standardvertragsklauseln](https://ec.europa.eu/info/law/law-topic/data-protection_de) zu empfehlen (Bewilligungsfreiheit nach Art 46 Abs 2 lit c DSGVO).

   Dieser Mustervertrag wurde mit größter Sorgfalt erstellt und kann laufend aktualisiert werden. Für die Richtigkeit, Vollständigkeit, Aktualität oder Qualität des bereitgestellten Musters sowie auch für weiterführende Links können wir jedoch keine Gewähr übernehmen. Haftungsansprüche gegen Personen, welche dieses Muster bereitgestellt haben, sind daher ausgeschlossen.

   Wir behalten uns ausdrücklich vor, das Muster ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen und übernehmen daher keine Gewähr und Haftung für die dauerhafte Verfügbarkeit der des Musters.

   Wenn Sie mit den vorliegenden Mustern nicht das Auslangen finden oder zusätzliche Fragen haben, empfehlen wir Ihnen, eine/n ZT für Informationstechnologie zu kontaktieren. [↑](#footnote-ref-1)
2. Zum Begriff des/der Auftragsverarbeiters/Auftragsverarbeiterin siehe [Überblick der WKÖ](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Verantwortlicher-und-Aufr.html) [↑](#footnote-ref-2)
3. Zum Internationalen Datenverkehr siehe die Information der [Europäischen Kommission zum internationalen Datenverkehr](https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_de) [↑](#footnote-ref-3)
4. Bitte passen Sie die folgende Liste den tatsächlichen Begebenheiten im Unternehmen des/der Auftragnehmers/in an! [↑](#footnote-ref-4)
5. Vertraulichkeit bedeutet: Schutz vor unbefugter Preisgabe von Informationen. Diese dürfen ausschließlich den Befugten zugänglich sein. [↑](#footnote-ref-5)
6. Das „Need-to-know-Prinzip“ („Kenntnis nur, wenn nötig“), bedeutet, dass auch grundsätzlich zugriffsberechtigte Personen nur Zugang zu Daten oder Informationen haben sollen, wenn diese Daten/Informationen zur Erfüllung einer konkreten Aufgabe von dieser Person unmittelbar benötigt werden. [↑](#footnote-ref-6)
7. Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym (zumeist ein Code, bestehend aus einer Buchstaben- oder Zahlenkombination) ersetzt, um die Feststellung der Identität des Betroffenen auszuschließen oder wesentlich zu erschweren [↑](#footnote-ref-7)
8. Datenintegrität bedeutet: Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten. [↑](#footnote-ref-8)
9. Verfügbarkeit bedeutet: Das im Unternehmen im Einsatz befindliche IT-System muss zeitgerecht betriebsbereit sein und die Verarbeitung muss auch korrekt erfolgen. [↑](#footnote-ref-9)
10. Belastbarkeit bedeutet: Die Fähigkeit eines Systems, trotz massiver externer oder interner Störungen wieder in den ursprünglichen Ausgangszustand zurückkehren zu können. Ein IT-System muss dazu gezielten Angriffen oder anderen Vorfällen widerstehen und trotz dieser Störungen seinen Betrieb aufrechterhalten können. [↑](#footnote-ref-10)
11. = Vorfallreaktionsmanagement = eine systematische Strategie, welche Unternehmen, Organisationen und Einzelpersonen in die Lage versetzt, Cyberangriffe und IT-Sicherheitslücken abzuwehren oder zu schließen. [↑](#footnote-ref-11)
12. = „Privacy by Default“: Dieser Grundsatz besagt, dass Datenschutzeinstellungen so zu setzen sind, dass von vornherein möglichst wenig Daten erhoben, gespeichert und geteilt werden. [↑](#footnote-ref-12)