**Verzeichnis von Verarbeitungstätigkeiten[[1]](#footnote-1)**

**Auftragsverarbeiter:innen**

1. **Allgemeine Angaben zum Ziviltechniker:innenbüro, welches im Auftrag eines Verantwortlichen[[2]](#footnote-2) Daten verarbeitet[[3]](#footnote-3)**
   1. **Name und Kontaktdaten des/der Auftragsverarbeiters/Auftragsverarbeiter/in[[4]](#footnote-4) (= Auftragnehmer/in):**
   2. **Name/n und Kontaktdaten der/des ZT bzw. ZT GmbH:**

DI Max Mustermann *oder* Max Mustermann ZT GmbH, FN xxxx

Musterweg 1

0000 Musterdorf

Tel Nr. des Ziviltechnikerbüros: 0000….

Emailadresse: [office@xxxx.at](mailto:office@xxxx.at)

* 1. **Name und Kontaktdaten des/der Vertreters/Vertreterin der Ziviltechniker:innengesellschaft:**

DI Maria Musterfrau als Geschäftsführerin/Prokuristin

Tel Nr. von DI Musterfrau: 0000….

Emailadresse: [maria.musterfrau@xxxx.at](mailto:maria.musterfrau@xxxx.at)

* 1. **Name und Kontaktdaten des/der verpflichtend oder freiwillig bestellten Datenschutzbeauftragten[[5]](#footnote-5) des/der Auftragsverarbeiters/Auftragsverarbeiter/in[[6]](#footnote-6) (= Auftragnehmer/in):**

1. **Allgemeine Angaben zum/zur Verantwortlichen[[7]](#footnote-7), in dessen/deren Namen Daten verarbeitet werden[[8]](#footnote-8)** 
   1. **Name und Kontaktdaten des/der für die Verarbeitung (gemeinsam) Verantwortlichen (=Auftraggebers/in) bzw. dessen/deren Vertreters:**

*[zB. Behörde XY, für die der/die ZT als EDV-Betreuer:in tätig ist, inklusive Name des leitenden Organs bzw. weiterer Kontaktpersonen]*

* 1. **Name und Kontaktdaten des/der Datenschutzbeauftragten[[9]](#footnote-9) des/der Verantwortlichen (= des/der Auftraggebers/in)**

1. **Kategorien von Datenverarbeitungen[[10]](#footnote-10), die im Rahmen der Auftragserfüllung erfolgen:[[11]](#footnote-11)**

*[Hinweis: Die untenstehenden Ausführungen sind unter Berücksichtigung des konkreten Auftrags zu ergänzen, zu ändern bzw. ist Nichtzutreffendes zu streichen.]*

* 1. **Gegenstand des Auftrags**

Meine/Unsere Tätigkeit zum Projekt *XY* umfasst folgende Leistungen:

*[…]*

* 1. **Aus dem Auftragsgegenstand ergibt sich die Notwendigkeit für folgende Datenverarbeitungen:**

Es werden automationsunterstützt (Email, Textverarbeitung im Word, etc) sowie in Form von archivierten Textdokumenten (zB. Korrespondenz, etc.) Kontaktdaten, Angebote, Vertragsdaten, Verrechnungsdaten, *[usw…]* verarbeitet.

* 1. **Folgende Personen sind betroffen:**

Auftraggeber/in, deren Kontaktpersonen, deren Mitarbeiter/innen *[usw…]*

* 1. **Abhängig von der Auftragsabwicklung sind diese gegenüber folgenden Empfängern/Empfängerinnen[[12]](#footnote-12) in *Drittländern[[13]](#footnote-13)* offengelegt worden oder werden noch offengelegt[[14]](#footnote-14):**
* *Empfänger:innenkategorien in Drittstaaten oder internationalen Organisationen* ***und***
* *Angabe des Drittstaats* ***und***
* *Dokumentation der getroffenen geeigneten Garantien im Falle der Übermittlung in Drittstaaten, zB. Angemessenheitsbeschluss, Standarddatenschutzklauseln, usw.*

1. **Allgemeine Beschreibung der technisch und organisatorischen Maßnahmen**

*[Hinweis: Überdies treffen Sie auch als Auftragsverarbeiter/in Datensicherheitspflichten****[[15]](#footnote-15)****: Sie haben die im Rahmen des Auftrags verarbeiteten Daten vor dem Zugriff durch Unberechtigte zu schützen* ***(Vertraulichkeit)****. Sie haben Maßnahmen zur Verhinderung von Datenverlust zu treffen* ***(Verfügbarkeit)****. Überdies müssen Daten vor einer Veränderung/Verfälschung gesichert sein* ***(Integrität)****.*

*Abhängig von der Auftragstätigkeit können die risikoangemessenen Sicherheitsmaßnahmen unterschiedlich gestaltet sein. Es ist eine Einschätzung der Notwendigkeit der Sicherheitsmaßnahmen unter Berücksichtigung des Stands der Technik, der Durchführungskosten, der Art, des Umfangs und des Zwecks der Datenverarbeitung sowie der Wahrscheinlichkeit und Schwere des Datensicherheitsrisikos vorzunehmen. Wir haben im Folgenden beispielhaft Sicherheitsmaßnahmen angeführt, die in Frage kommen könnten, wobei die in Ihrem Unternehmen vorliegenden anzukreuzen sind:]*

|  |  |  |
| --- | --- | --- |
| **Vertraulichkeit[[16]](#footnote-16)** |  |  |
| Zutrittskontrolle zum Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen | Schlüssel |  |
| Magnet- oder Chipkarte |  |
| Elektrische Türöffner |  |
| Alarmanlage |  |
| Videoanlage |  |
| Sicherheitspersonal |  |
| Anmeldung beim Empfang mit Personenkontrolle |  |
| Einbruchshemmende Fenster und/oder Sicherheitstüren |  |
| Begleitung von Besuchern im Unternehmensgebäude |  |
| Sonstiges: |  |
| Zugangskontrolle zum Schutz vor unbefugter Systembenutzung | Benutzernamen und Kennwörter |  |
| Automatische Sperrmechanismen |  |
| Verschlüsselung von Datenträgern |  |
| Zwei-Faktor-Authentifizierung[[17]](#footnote-17) |  |
| Sonstiges: |  |
| Zugriffskontrolle, dh. kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, durch: | Protokollierung von Zugriffen |  |
| Standard-Berechtigungsprofile auf „need to know-Basis“[[18]](#footnote-18) |  |
| Zugriff nur für Unternehmensinhaber:innen |  |
| Zugriff nur für bestimmte Mitarbeiter:innen |  |
| Periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten |  |
| Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger |  |
| Standardprozess für Berechtigungsvergabe |  |
| Sichere Aufbewahrung von Speichermedien | Sic |
| Datenschutzgerechte Wiederverwendung von Datenträgern |  |
| Pseudonymisierung: | Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt. |  |
| Klassifikationsschema für Daten vorhanden: | Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich). |  |
| **Integrität** |  |  |
| Weitergabekontrolle zum Schutz vor unbefugtem Lesen, Kopieren, Verändern, Entfernen bei elektronischer Übertragung | Verschlüsselung von Datenträgern |  |
| Verschlüsselung von Dateien |  |
| Virtual Private Networks (VPN)[[19]](#footnote-19) |  |
| Elektronische Signatur |  |
| Sonstiges: |  |
| Eingabekontrolle zur Nachvollziehbarkeit, ob und von wem Daten eingegeben, verändert, entfernt wurden | Protokollierung |  |
| Dokumentenmanagement |  |
| **Verfügbarkeit und Belastbarkeit:**  Verfügbarkeitskontrolle zum Schutz gegen zufällige und mutwillige Zerstörung/Verlust | Security Checks auf Infrastruktur- und Applikationsebene |  |
| Virenschutz |  |
| Backup-Strategie |  |
| Firewall |  |
| Standardprozesse bei Wechsel/Ausscheiden von Mitarbeiter:innen |  |
| Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum |  |
| Rasche Wiederherstellbarkeit von Daten |  |
| **Evaluierungsmaßnahmen** |  |  |
| Datenschutz-Management | Risikoanalyse |  |
| Regelmäßige Mitarbeiter:innenschulung |  |
| Incident-Response-Management[[20]](#footnote-20): |  |
| Datenschutzfreundliche Voreinstellungen[[21]](#footnote-21): |  |
| Auftragskontrolle, dh. keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers bzw. der Auftraggeberin durch: | Eindeutige Vertragsgestaltung |  |
| Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS) |  |
| Nachkontrollen |  |
| Formalisiertes Auftragsmanagement |  |
| Vorabüberzeugungspflicht |  |
| Sonstiges: |  |

[Ort], am [Datum zur Erstellung des Verarbeitungsverzeichnisses]

1. Bitte passen Sie das Muster an die tatsächlichen Begebenheiten in ihrem Unternehmen an und löschen Sie bei Verwendung des Musters die rot gekennzeichneten HInweise!

   Dieses Muster 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 des Musters.

   Das Muster soll lediglich bei der Abdeckung der Mindestanforderungen unterstützen. Aus Gründen der Vereinfachung haben wir Spezialkonstellationen außer Betracht gelassen. Wenn Sie mit dem vorliegenden Muster nicht das Auslangen finden oder zusätzliche Fragen haben, empfehlen wir Ihnen, eine/n Ziviltechniker:in für Informationstechnologie zu kontaktieren. [↑](#footnote-ref-1)
2. „Verantwortliche/r“ ist die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Nähere Informationen zu diesem Begriff finden Sie auf der [Homepage der Europäischen Kommission](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_de). [↑](#footnote-ref-2)
3. Als „Verarbeiten“ gilt jedes „Hantieren“ mit Daten am Computer und auch in Papierform z.B. das Verwenden, Erheben, Erfassen, Ordnen, Speichern, Übermitteln, Anpassen, Verändern, Auslesen, Abfragen, Löschen, Vernichten, Ablegen usw. [↑](#footnote-ref-3)
4. „Auftragsverarbeiter:in“ ist jede natürliche oder juristische Person, die personenbezogene Daten im Auftrag und auf Weisung eines „Verantwortlichen“ verarbeitet. Nähere Informationen zu diesem Begriff finden Sie auf der [Homepage der Europäischen Kommission](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_de). [↑](#footnote-ref-4)
5. Eine Verpflichtung zur Bestellung einer Datenschutzbeauftragten/eines Datenschutzbeauftragten besteht, wenn die Kerntätigkeit (= Haupttätigkeit) in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (wie z.B. Banken, Versicherungen, Kreditauskunfteien und Berufsdetektive) *oder* die Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung [sensibler Daten](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Wichtige-Begriffsbestimmu.html#sensible_Daten) oder von Daten über strafrechtliche Verurteilungen oder Straftaten besteht (z.B. Krankenanstalten). Eine Verpflichtung zur Bestellung einer Datenschutzbeauftragten/eines Datenschutzbeauftragten wird für Ziviltechniker:innen daher in aller Regel nicht gegeben sein. [↑](#footnote-ref-5)
6. „Auftragsverarbeiter:in“ ist jede natürliche oder juristische Person, die personenbezogene Daten im Auftrag und auf Weisung eines „Verantwortlichen“ verarbeitet. Nähere Informationen zu diesem Begriff finden Sie auf der [Homepage der Europäischen Kommission](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_de). [↑](#footnote-ref-6)
7. vgl. FN 2 [↑](#footnote-ref-7)
8. vgl. FN 3 [↑](#footnote-ref-8)
9. vgl. FN 5 [↑](#footnote-ref-9)
10. Datenverarbeitung ist jeder Umgang mit personenbezogenen Daten. Dies kann sowohl mit als auch ohne Hilfe automatisierter Verfahren erfolgen. Als Verarbeiten gilt demnach jedes „Hantieren“ mit Daten am Computer und auch in Papierform z.B. das Verwenden, Erheben, Erfassen, Ordnen, Speichern, Übermitteln, Anpassen, Verändern, Auslesen, Abfragen, Löschen, Vernichten, Ablegen usw. [↑](#footnote-ref-10)
11. Ein/e Aufragnehmer/in darf personenbezogenen Daten nur verarbeiten, soweit und solange dies zur Ausführung des Auftrags notwendig ist. Die Datenschutzbehörde muss daher einen Überblick über den Auftragsinhalt und die in diesem Zusammenhang verarbeiteten personenbezogenen Daten erhalten. Personenbezogene Daten sind im Grunde alle Angaben, anhand derer auf eine bestimmte Person geschlossen werden kann (wie z.B. Name, Adresse, …). Es ist daher eine allgemeine, kurze Beschreibung des Auftragsinhalts und der damit im Zusammenhang stehenden Datenverarbeitungen notwendig. [↑](#footnote-ref-11)
12. Vgl. FN 6 [↑](#footnote-ref-12)
13. Drittland = Land außerhalb der EU bzw. des Geltungsbereichs der DSGVO [↑](#footnote-ref-13)
14. Werden Daten an Empfänger:innen in ein Drittland (= Nicht-EU Land) übermittelt, sind dazu Angaben ins Verarbeitungsverzeichnis aufzunehmen! Erläuterungen zu den Vorschriften, welche gelten, wenn Daten an in Drittländern (= Nicht-EU Ländern) ansässige Empfänger:innen geschickt werden, finden Sie auf der [Homepage der Europäischen Kommission](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_de) oder der [Datenschutzbehörde](https://www.dsb.gv.at/aufgaben-taetigkeiten/internationaler-datenverkehr.html). [↑](#footnote-ref-14)
15. vgl. Art 30 Abs 2 lit d iVm Art 32 DSGVO [↑](#footnote-ref-15)
16. Vertraulichkeit bedeutet: Schutz vor unbefugter Preisgabe von Informationen. Diese dürfen ausschließlich den Befugten zugänglich sein. [↑](#footnote-ref-16)
17. Die Zwei-Faktor-Authentisierung bezeichnet den Identitätsnachweis eines Nutzers mittels einer Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren), z.B. die Notwendigkeit zur Eingabe eines Passworts und eines PIN-Codes. [↑](#footnote-ref-17)
18. 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-18)
19. VPN= eine [Netzwerkverbindung](https://de.wikipedia.org/wiki/Netzwerk), die von Unbeteiligten nicht einsehbar ist. [↑](#footnote-ref-19)
20. = Vorfallreaktionsmanagement = eine systematische Strategie, welche Unternehmen, Organisationen und Einzelpersonen in die Lage versetzt, Cyberangriffe und IT-Sicherheitslücken abzuwehren oder zu schließen. [↑](#footnote-ref-20)
21. = „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-21)