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

**Verantwortlicher/Verantwortliche**

1. **Allgemeine Angaben zum Ziviltechniker:innenbüro** 
   1. **Name und Kontaktdaten des/der für die Verarbeitung (gemeinsam) Verantwortlichen[[2]](#footnote-2):**
   2. **Name/n und Kontaktdaten der/des ZT bzw. ZT GmbH:**

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

Musterweg 1

0000 Musterdorf

Tel Nr. des Ziviltechniker:innenbüros: 0000….

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

* 1. **Name und Kontaktdaten des Vertreters/ der 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[[3]](#footnote-3) oder freiwillig bestellten Datenschutzbeauftragte/n**

1. **Zweck und Beschreibung der Datenverarbeitung[[4]](#footnote-4)**

*[Hinweis: Im Folgenden werden die in einem Ziviltechniker:innenbüro üblicherweise getätigten Datenverarbeitungen vereinheitlicht beschrieben und nach den Vorgaben der DSGVO kategorisiert.[[5]](#footnote-5) Die beispielhaften Ausführungen sind daher unter Berücksichtigung Ihrer konkreten Geschäftstätigkeit zu ergänzen, zu ändern bzw. ist Nichtzutreffendes zu streichen.]*

* 1. **Geschäftstätigkeit des Ziviltechniker:innenbüros**

*[Hinweis: Allgemeine, kurze Beschreibung der Unternehmenstätigkeit, d.h. im Falle eines Architekturbüros z.B.:]*   
Die gestaltende, technische, wirtschaftliche Planung von Bauwerken, die Überwachung der Bauausführung, Vertretung vor Verwaltungsgerichten oder Behörden usw.….

* 1. **Aus dieser Tätigkeit ergibt sich die Notwendigkeit für folgende Datenverarbeitungen:**

**2.2.1. Kunden- und Kundinnendatenverwaltung:**

Im Zuge der o.g. Geschäftstätigkeit werden im Rahmen der Geschäftsbeziehung mit Kunden und Kundinnen sowie des unternehmensinternen Rechnungswesens automationsunterstützt (z.B. E-Mailverkehr, Zeichenprogramme) als auch in Form von archivierten Textdokumenten (z.B. Korrespondenz, Verträge, Pläne, Bescheide, Handakte, personalisierte Rechnungen) personenbezogene Daten verarbeitet.

**Davon sind folgende Personen betroffen:**

Kunden/Kundinnen, inklusive Kontaktpersonen beim Kunden/bei der Kundin

**Von den betroffenen Personen werden abhängig vom Auftrag folgende personenbezogene Daten verwendet:**

Namen; Firma oder sonstige Geschäftsbezeichnung; Funktion; Angaben zur Vertretungsbefugnis; Anschrift; Kontaktdaten (Tel., Mail, Fax); Firmenbuchdaten; Bankverbindungen; UID-Nummer; Sozialversicherungsnummer; Bonitätsdaten; *[…]*

**Abhängig von der Auftragsabwicklung sind diese gegenüber folgenden Empfängern/Empfängerinnen[[6]](#footnote-6) offengelegt worden oder werden noch offengelegt:**

Gerichte; Verwaltungsbehörden; mitwirkende Vertrags- und Geschäftspartner:innen (inklusive Subunternehmer:innen); Wirtschaftstreuhänder:innen/Steuerberater:innen; Rechtsvertreter:innen; EDV-Betreuer:innen; Versicherungen, *[…]*

**Abhängig von der Auftragsabwicklung sind diese gegenüber folgenden Empfängern/Empfängerinnen[[7]](#footnote-7) in *Drittländern[[8]](#footnote-8)* offengelegt worden oder werden noch offengelegt[[9]](#footnote-9):**

* *Empfänger:innenkategorien in Drittstaaten oder internationalen Organisationen, zB. in Drittstaaten ansässige Geschäftspartner:innen* ***und***
* *Angabe des Drittstaats* ***und***
* *Dokumentation der getroffenen geeigneten Garantien im Falle der Übermittlung in Drittstaaten, zB. Angemessenheitsbeschluss, Standarddatenschutzklauseln usw.*

**Rechtsgrundlage:[[10]](#footnote-10)** Die Kundendatenverarbeitung und Kundinnendatenverarbeitung ist zur Erfüllung des Vertrages mit den betroffenen Kunden und Kundinnen bzw. zur Durchführung vorvertraglicher Maßnahmen notwendig.[[11]](#footnote-11) Darüber hinaus zur Erfüllung gesetzlicher Verpflichtungen (wie z.B. 7-jährige, buchhalterische Aufbewahrungspflicht gemäß BAO). Die Datenverarbeitung zu Marketing- und Werbezwecken[[12]](#footnote-12) liegt im berechtigten Interesse des Ziviltechniker:innenbüros bzw. erfolgt bei Vorliegen einer Einwilligung.[[13]](#footnote-13)

**Aufbewahrungs- und Löschfristen:[[14]](#footnote-14)**

Die zur Erfüllung der Rechnungslegungspflichten[[15]](#footnote-15) und steuerrechtlicher Vorgaben[[16]](#footnote-16) notwendigen Daten werden jedenfalls 7 Jahre aufbewahrt.[[17]](#footnote-17) Darüber hinaus erfolgt im Einzelfall eine längere Aufbewahrung bis zur Beendigung der Geschäftsbeziehung bzw. eines Rechtsstreits bzw. bis zum Ablauf der Gewährleistungs- und Garantiefristen sowie der Verjährungsfristen für den Fall der Geltendmachung von Schadenersatzansprüchen bzw. soweit dies zur Geltendmachung urheberrechtlicher Ansprüche erforderlich ist.[[18]](#footnote-18) Für alle im elektronischen Urkundenarchiv gespeicherten Daten gilt überdies eine Aufbewahrungsfrist von mindestens 30 Jahren.[[19]](#footnote-19)

**2.2.2. Personaldatenverwaltung:**

Im o.g. Ziviltechniker:innenbüro sind Mitarbeiter:innen beschäftigt, deren personenbezogene Daten automationsunterstützt (z.B. E-Mailverkehr, Buchhaltungsprogramm) sowie in Form archivierter Textdokumente (z.B. Korrespondenz, Personalhandakt) verarbeitet werden. Insbesondere werden Daten zur Begründung des Dienstverhältnisses (z.B. Bewerbungen, Einstellungstests*),* Daten betreffend das laufende Dienstverhältnis (z.B. Zeiterfassung, Lohnbuchhaltung, Urlaubserfassung) und Daten betreffend die Beendigung des Dienstverhältnisses (z.B. Dienstzeugnisse) verarbeitet.

**Davon sind folgende Personen betroffen:**

Bewerber:innen; Mitarbeiter:innen des Ziviltechniker:innenbüros und deren Angehörige, soweit diese mitversichert sind bzw. sich aus der Angehörigeneigenschaft Ansprüche der Mitarbeiter:innen (z.B. Pflegeurlaub) ergeben.

**Von den betroffenen Personen werden abhängig vom Anstellungsverhältnis (Werkvertrag, [freier] Dienstvertrag) folgende personenbezogene Daten erfasst:**

Namen; Anschrift; Kontaktdaten (Tel., Mail, Fax); Sozialversicherungsnummer; Staatsbürgerschaft, Familienstand, Bankverbindungen; Zugriffsberechtigungen, *[…]*

Daten über die Religionszugehörigkeit werden nur insoweit erfasst, als sie die Mitarbeiter:innen von sich aus bekanntgegeben haben und diese zur Wahrnehmung des gesetzlichen Urlaubsanspruchs an religiösen Feiertagen dienen.[[20]](#footnote-20)

**Diese sind aufgrund der sich aus dem Arbeitsvertrag bzw. sonstigen gesetzlichen Bestimmungen ergebenden Verpflichtungen gegenüber folgenden Empfänger:innen[[21]](#footnote-21) offengelegt worden oder werden noch offengelegt:**

Hauptverband der Sozialversicherungsträger, Finanzamt, Steuerberater:innen-/Wirtschaftstreuhänder:innen, EDV-Betreuer:innen; Banken; im Falle von sich aus dem Arbeitsverhältnis ergebenden Rechtsstreitigkeiten auch an Gerichte und Rechtsvertreter:innen, *[…]*

**Diese sind aufgrund der sich aus dem Arbeitsvertrag bzw. sonstigen gesetzlichen Bestimmungen ergebenden Verpflichtungen gegenüber folgenden Empfänger:innen[[22]](#footnote-22) in *Drittländern[[23]](#footnote-23)* offengelegt worden oder werden noch offengelegt[[24]](#footnote-24):**

* *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.*

**Rechtsgrundlagen:[[25]](#footnote-25)** Die Aufbewahrung von Bewerbungsunterlagen erfolgt zur Anbahnung eines Arbeitsverhältnisses als vorvertragliche Maßnahme. Die Verarbeitung der o.g. Personaldaten von Mitarbeiter:innen bzw. deren Angehörigen ist zur Erfüllung der Arbeitsverträge bzw. der sich aus dem Arbeitsverhältnis ergebenden Rechtspflichten (z.B. § 132 BAO, § 464 ASVG) erforderlich.[[26]](#footnote-26)

**Aufbewahrungs- und Löschfristen:[[27]](#footnote-27)** Bewerbungsunterlagen abgelehnter Bewerber:innen werden aufgrund der Möglichkeit der Geltendmachung von Gleichbehandlungsansprüchen mindestens 6 Monate aufbewahrt (§§ 15 Abs 1 und 29 Abs 1 GlbG, § 7k Abs 1 iVm Abs 2 Z 1 BEeinstG) bzw. 3 Jahre soweit ein Anspruch auf Ersatz von Vorstellungskosten geltend gemacht werden könnte (§ 1486 Z 5 ABGB). Darüber hinaus erfolgt eine Aufbewahrung nur soweit der/die abgelehnte Bewerber:in einer Evidenzhaltung zugestimmt hat.[[28]](#footnote-28)

Die zur Erfüllung der Rechnungslegungspflichten[[29]](#footnote-29) und steuerrechtlicher Vorgaben[[30]](#footnote-30) notwendigen personenbezogenen Daten von Mitarbeiter:innen werden jedenfalls 7 Jahre aufbewahrt. Unterlagen zur sozialversicherungsrechtlichen Beurteilung von Dienstverhältnissen werden 3 bzw. 5 Jahre aufbewahrt.[[31]](#footnote-31) Personenbezogene Daten, die im Zusammenhang mit der Ausstellung eines Dienstzeugnisses (insbesondere Art und Dauer der Tätigkeit) erforderlich sind, werden 30 Jahre aufbewahrt. Darüber hinaus werden personenbezogene Daten im Einzelfall bis zur Beendigung eines Rechtsstreits bzw. bis zum Ablauf von Verjährungsvorschriften zur Geltendmachung von arbeitsrechtlichen Ansprüchen aufbewahrt.[[32]](#footnote-32)

* + 1. **Geschäftspartner:innendatenbank:**

Zur Geschäftsabwicklung müssen im Anlassfall externe Dienstleister:innen beigezogen werden (z.B. Subunternehmer:innen, EDV-Betreuer:innen), deren Daten im Rahmen der Vertragsabwicklung und des Rechnungswesens automationsunterstützt (z.B. E-Mailverkehr, Buchhaltungsprogramm) sowie in Form archivierter Textdokumente (z.B. Korrespondenz, Verträge, Pläne, Handakte, personalisierte Rechnungen) verarbeitet werden.

**Davon sind folgende Personen betroffen:**

Geschäftspartner:innen, inklusive Kontaktpersonen der Geschäftspartner:innen

**Von den betroffenen Personen werden abhängig vom Auftrag folgende personenbezogene Daten verwendet:**

Namen; Firma oder sonstige Geschäftsbezeichnung; Funktion; Angaben zur Vertretungsbefugnis; Anschrift; Kontaktdaten (Tel., Mail, Fax); Firmenbuchdaten; Bankverbindungen; UID-Nummer; Sozialversicherungsnummer; Bonitätsdaten; *[…]*

**Abhängig vom Auftrag sind diese gegenüber folgenden Empfänger:innen[[33]](#footnote-33) offengelegt worden oder werden noch offengelegt:**

Gerichte; Verwaltungsbehörden; KundInnen; Wirtschaftstreuhänder:innen/Steuerberater:innen; Rechtsvertreter:innen; EDV-Betreuer:innen; Versicherungen; Banken; *[…]*

**Abhängig von der Auftragsabwicklung sind diese gegenüber folgenden Empfängern/Empfängerinnen[[34]](#footnote-34) in *Drittländern[[35]](#footnote-35)* offengelegt worden oder werden noch offengelegt[[36]](#footnote-36):**

* *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*

**Rechtsgrundlage:** Die Verarbeitung der Daten von Geschäftspartner:innen ist aufgrund des bestehenden Auftragsverhältnisses bzw. zur Durchführung vorvertraglicher Maßnahmen notwendig.[[37]](#footnote-37) Die Datenverarbeitung zu Marketing- und Werbezwecken[[38]](#footnote-38) liegt im berechtigten Interesse des Ziviltechniker:innenbüros bzw. erfolgt bei Vorliegen einer Einwilligung.[[39]](#footnote-39)

**Aufbewahrungs- und Löschfristen:[[40]](#footnote-40)**

Die zur Erfüllung der Rechnungslegungspflichten[[41]](#footnote-41) und steuerrechtlicher Vorgaben[[42]](#footnote-42) notwendigen Daten werden jedenfalls 7 Jahre aufbewahrt. [[43]](#footnote-43) Darüber hinaus erfolgt im Einzelfall eine längere Aufbewahrung bis zur Beendigung der Geschäftsbeziehung bzw. eines Rechtsstreits bzw. bis zum Ablauf der Gewährleistungs- und Garantiefristen sowie der Verjährungsfristen für den Fall der Geltendmachung von Schadenersatzansprüchen bzw. soweit dies zur Geltendmachung urheberechtlicher Ansprüche erforderlich ist[[44]](#footnote-44) Für alle im elektronischen Urkundenarchiv gespeicherten Daten gilt überdies eine Aufbewahrungsfrist von mindestens 30 Jahren.[[45]](#footnote-45)

* + 1. **Webseiten-Besucher:innen:**

*[Hinweis: Diesen Punkt nur im Falle des Vorhandenseins einer Unternehmenswebsite anführen und entsprechend den tatsächlichen Funktionen der Website anpassen! Bitte beachten Sie dazu auch die Informationspflichten und das dazugehörige Muster „Datenschutzerklärung für Websites“, welches unter den DSGVO Hilfestellungen auf arching.at zu finden ist.]*

Zur Präsentation des Unternehmens wird eine Unternehmenswebsite betrieben. Die Website ist mit einem Website-Analyse-Tool ausgestattet. Dieses ermöglicht die Auswertung der Webseitenutzung, Reportzusammenstellung, Sicherstellung der IT- und Netzwerksicherheit. Weiters verwendet die Website Cookies, insbesondere zur Ausspielung von Banner-Werbung und sonstiger Werbung auf Webseiten.

**Davon sind folgende Personen betroffen:**

Besucher:innen der Webseite

**Von den betroffenen Personen werden abhängig von deren Nutzung der Unternehmenswebseite folgende personenbezogene Daten verwendet:** *[Hinweis: Passen Sie diese Informationen – gegeben falls nach Rücksprache mit Ihrem/ihrer Webdesigner:in – unbedingt den tatsächlich technischen Funktionen Ihrer Website an!*

IP-Adresse (anonymisiert), Art des Browsers, Plug-ins, Gerätetyp und -ID, Land des Zugriffs, landing-page, besuchte Seiten, angesehene und gesuchte Produkte, Verlauf, Dauer des Besuches, Aktivitäten auf der Website

**Abhängig vom Auftrag sind diese gegenüber folgenden Empfänger:innen[[46]](#footnote-46) offengelegt worden oder werden noch offengelegt:**

IT- Dienstleister:innen; ggf das Unternehmen, dass das Webanalyse-/Cookie Tool zur Verfügung stellt

**Abhängig von der Auftragsabwicklung sind diese gegenüber folgenden Empfängern/Empfängerinnen[[47]](#footnote-47) in *Drittländern[[48]](#footnote-48)* offengelegt worden oder werden noch offengelegt[[49]](#footnote-49):**

* *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*

**Rechtsgrundlagen:**

Die Verarbeitung erfolgt aufgrund einer Einwilligung[[50]](#footnote-50) nach Art 6 Abs 1 lit a DSGVO; sowie falls keine Einwilligung vorliegt, aufgrund des berechtigten Interesses des Verantwortlichen nach Art 6 Abs lit f DSGVO.[[51]](#footnote-51)

**Aufbewahrungs- und Löschfristen:[[52]](#footnote-52)**

*Die Aufbewahrungsdauer der Daten[[53]](#footnote-53) richtet sich nach dem Zweck der Datenverarbeitung. Es wird empfohlen, die Daten nicht länger als 6 Monate bis zu 1 Jahr aufzubewahren.* *Bitte um Ergänzung der Speicherdauer je nach individueller Einstellung!*

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

*[Hinweis: Überdies treffen Sie Datensicherheitspflichten****[[54]](#footnote-54)****: Sie haben die 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 Unternehmenstätigkeit 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 und nicht vorhandene gegebenenfalls aus der Liste zu entfernen sind:]*

|  |  |  |
| --- | --- | --- |
| **Vertraulichkeit[[55]](#footnote-55)** |  |  |
| 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[[56]](#footnote-56) |  |
| Sonstiges: |  |
| Zugriffskontrolle, dh. kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, durch: | Protokollierung von Zugriffen |  |
| Standard-Berechtigungsprofile auf „need to know-Basis“[[57]](#footnote-57) |  |
| 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)[[58]](#footnote-58) |  |
| 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[[59]](#footnote-59): |  |
| Datenschutzfreundliche Voreinstellungen[[60]](#footnote-60): |  |
| 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 den vorliegenden Mustern 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 Europäische 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. 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-3)
4. Ein Unternehmer/eine Unternehmerin darf im Rahmen seiner/ihrer Unternehmenstätigkeit personenbezogenen Daten nur verarbeiten, soweit und solange dies zur Ausführung seiner/ihrer Geschäftstätigkeit notwendig ist. Die Datenschutzbehörde muss daher einen Überblick über Ihre Geschäftstätigkeit 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, …). 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-4)
5. vgl. Art 30 Abs 1 DSGVO [↑](#footnote-ref-5)
6. Als „**Empfänger:in“** gilt jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, gegenüber der personenbezogene Daten offengelegt werden (vgl. Art 4 Z 9 DSGVO). [↑](#footnote-ref-6)
7. Vgl. FN 6 [↑](#footnote-ref-7)
8. Drittland = Land außerhalb der EU bzw. des Geltungsbereichs der DSGVO [↑](#footnote-ref-8)
9. Werden Daten an Empfänger:innen in ein Drittland (= Nicht-EU Land) übermittelt, sind darüber zusätzliche Angaben ins Verarbeitungsverzeichnis aufzunehmen. Bitte prüfen Sie insbesondere, in welchem Land der/die Bertreiber:in des Unternehmensservers ansässig ist sowie jene Unternehmen, die die Tools für Ihre Unternehmenswebseite zur Verfügung stellen! 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-9)
10. Art 6 DSGVO normiert, dass die Verarbeitung von Daten nur bei Vorliegen bestimmter [Rechtfertigungsgründe](https://www.usp.gv.at/it-geistiges-eigentum/datenschutz/rechtmaessigkeit-und-grundsaetze.html) durchgeführt werden darf. Dazu gehört insbesondere die Erfüllung einer rechtlichen Verpflichtung; die Erfüllung eines Vertrages; die Einwilligung oder das berechtigte Interesse der/des Verantwortlichen oder eines Dritten. [↑](#footnote-ref-10)
11. Erfolgt die Datenverarbeitung im Zuge der Vertragsabwicklung, ist die zusätzliche Einholung einer Einwilligungserklärung vom Kunden/von der Kundin nicht erforderlich (vgl. Art 6 Abs 1 DSGVO). [↑](#footnote-ref-11)
12. Werbung kann jede Art der Verkaufsförderung für Dienstleistungen sein, die den Kunden/die Kundin überreden oder die Allgemeinheit informieren und gleichzeitig einen Kaufanreiz schaffen soll, z.B. auch Newsletter mit Informationen über neue Projekte und Dienstleistungen. [↑](#footnote-ref-12)
13. Gemäß Art 6 Abs 1 lit f DSGVO ist eine Datenverarbeitung im Einzelfall auch bei Vorliegen berechtigter Interessen des Verarbeiters/der Verarbeiterin rechtmäßig. Die Zusendung von **Werbung per Post** kann als berechtigtes Interesse eines Unternehmers/einer Unternehmerin gewertet werden (vgl. Erw. 47 DSGVO). Für die Zusendung von **Massen- und** **Werbe-E-Mails** gelten Sondervorschriften und ist in der Regel eine Einwilligung erforderlich. Welche E-Mails Sie mit oder ohne Einwilligung versenden dürfen, entnehmen Sie bitte den Ausführungen auf der [Homepage der WKO.](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/E-Mails_versenden_-_aber_richtig.html) [↑](#footnote-ref-13)
14. Zur Frage, wie lange Daten aufbewahrt werden dürfen, finden Sie Erläuterungen auf der [Homepage der Europäischen Kommission](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_de). [↑](#footnote-ref-14)
15. vgl. §§ 190, 212 UGB [↑](#footnote-ref-15)
16. vgl. § 132 BAO [↑](#footnote-ref-16)
17. Eine Auflistung weitere möglicher Speicher-, Verjährungs- und Aufbewahrungsfristen finden Sie auf der [Homepage der WKÖ](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/E-Mails_versenden_-_aber_richtig.html) [↑](#footnote-ref-17)
18. vgl. Art 17 Abs. 3 lit e DSGVO [↑](#footnote-ref-18)
19. § 13 Urkundenarchiv-Verordnung – 228. VO der BKZT [↑](#footnote-ref-19)
20. **Achtung:** Daten über die Religionszugehörigkeit sind [personenbezogene Daten der besonderen Kategorie („sensible Daten“)](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Wichtige-Begriffsbestimmu.html) und dürfen nur in den gesetzlich vorgesehen Fällen, sehr eingeschränkt verarbeitet werden, z.B. zur Ausübung von sich aus dem Arbeits- oder Sozialrecht ergebenden Rechtsansprüchen (vgl. Art 9 DSGVO). [↑](#footnote-ref-20)
21. Als „**Empfänger:in“** gilt jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden (vgl. Art 4 Z 9 DSGVO). [↑](#footnote-ref-21)
22. Vgl. FN 21 [↑](#footnote-ref-22)
23. Drittland = Land außerhalb der EU bzw. des Geltungsbereichs der DSGVO [↑](#footnote-ref-23)
24. Werden Daten in ein Drittland (= Nicht-EU Land) übermittelt, sind darüber zusätzliche Angaben ins Verarbeitungsverzeichnis aufzunehmen. Bitte prüfen Sie insbesondere, in welchem Land der/die Bertreiber:in des Unternehmensservers ansässig ist sowie jene Unternehmen, die die Tools für Ihre Unternehmenswebseite zur Verfügung stellen! 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-24)
25. Art 6 DSGVO normiert, dass die Verarbeitung von Daten nur bei Vorliegen [bestimmter Rechtfertigungsgründe](https://www.usp.gv.at/it-geistiges-eigentum/datenschutz/rechtmaessigkeit-und-grundsaetze.html) durchgeführt werden darf. Dazu gehören insbesondere die Erfüllung einer rechtlichen Verpflichtung, die Erfüllung eines Vertrages, die Einwilligung oder das berechtigte Interesse des Verantwortlichen oder eines Dritten. [↑](#footnote-ref-25)
26. Erfolgt die Datenverarbeitung im Zuge der Vertragsabwicklung oder aufgrund gesetzlicher Verpflichtungen ist die zusätzliche Einholung einer Einwilligungserklärung von Mitarbeiter:innen bzw. deren Angehörigen nicht erforderlich (vgl. Art 6 Abs 1 DSGVO). [↑](#footnote-ref-26)
27. Zur Frage, wie lange Daten aufbewahrt werden dürfen, finden Sie Erläuterungen auf der [Homepage der Europäischen Kommission](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_de). [↑](#footnote-ref-27)
28. Zu den Voraussetzungen für eine gültige Einwilligungserklärung finden Sie Informationen im [Unternehmensserviceportal](https://www.usp.gv.at/it-geistiges-eigentum/datenschutz/einwilligung.html). [↑](#footnote-ref-28)
29. vgl. §§ 190, 212 UGB [↑](#footnote-ref-29)
30. vgl. § 132 BAO [↑](#footnote-ref-30)
31. vgl. § 68 ASVG [↑](#footnote-ref-31)
32. vgl. Art 17 Abs 3 lit e DSGVO; Näheres zu den möglichen Aufbewahrungsfristen im Zusammenhang mit dem Arbeitsverhältnis finden Sie auf der [Homepage der WKÖ](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html) [↑](#footnote-ref-32)
33. Als „**Empfänger:in“** gilt jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden (vgl. Art 4 Z 9 DSGVO). [↑](#footnote-ref-33)
34. Als „**Empfänger:in“** gilt jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden (vgl. Art 4 Z 9 DSGVO). [↑](#footnote-ref-34)
35. Drittland = Land außerhalb der EU bzw. des Geltungsbereichs der DSGVO [↑](#footnote-ref-35)
36. Werden Daten an Empfänger:innen in ein Drittland (= Nicht-EU Land) übermittelt, sind darüber zusätzliche Angaben ins Verarbeitungsverzeichnis aufzunehmen. Bitte prüfen Sie insbesondere, in welchem Land der/die Bertreiber:in des Unternehmensservers ansässig ist sowie jene Unternehmen, die die Tools für Ihre Unternehmenswebseite zur Verfügung stellen! 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-36)
37. Erfolgt die Datenverarbeitung im Zuge der Vertragsabwicklung ist die zusätzliche Einholung einer Einwilligungserklärung vom Kunden in der Regel nicht erforderlich (vgl. Art 6 Abs 1 DSGVO). [↑](#footnote-ref-37)
38. Werbung kann jede Art der [Verkaufsförderung](http://www.onpulson.de/lexikon/verkaufsfoerderung/) für Dienstleistungen sein, die den Kunden/der Kundin überreden oder die Allgemeinheit informieren und gleichzeitig einen Kaufanreiz schaffen soll, zB. auch Newsletter mit Informationen über neue Projekte und Dienstleistungen. [↑](#footnote-ref-38)
39. Gemäß Art 6 Abs 1 lit f DSGVO ist eine Datenverarbeitung nicht nur im Zuge der Vertragserfüllung oder nach Einholung einer Einwilligung rechtmäßig, sondern im Einzelfall auch bei Vorliegen berechtigter Interessen des Verarbeiters /der Verarbeiterin. Die Zusendung von **Werbung per Post** kann als berechtigtes Interesse eines Unternehmers /einer /Unternehmerin gewertet werden (vgl. Erw. 47 DSGVO). Für die Zusendung von **Massen- und Werbe-E-Mails** gelten Sondervorschriften und ist in der Regel eine Einwilligung erforderlich. Welche Emails Sie mit oder ohne Einwilligung versenden dürfen, entnehmen Sie bitte den Ausführungen auf der [Homepage der WKÖ.](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/E-Mails_versenden_-_aber_richtig.html) [↑](#footnote-ref-39)
40. Zur Frage, wie lange Daten aufbewahrt werden dürfen, finden Sie Erläuterungen auf der [Homepage](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_de)

    [der Europäischen Kommission](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_de). [↑](#footnote-ref-40)
41. vgl. §§ 190, 212 UGB [↑](#footnote-ref-41)
42. vgl. § 132 BAO [↑](#footnote-ref-42)
43. Eine Auflistung weitere möglicher Speicher-, Verjährungs- und Aufbewahrungsfristen finden Sie auf der [Homepage der WKÖ](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html) [↑](#footnote-ref-43)
44. vgl. Art 17 Abs 3 lit e DSGVO [↑](#footnote-ref-44)
45. vgl. § 13 Urkundenarchiv-Verordnung – 220. VO der bAIK, Zl 20/17 [↑](#footnote-ref-45)
46. Als „**Empfänger:in“** gilt jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden (vgl. Art 4 Z 9 DSGVO). [↑](#footnote-ref-46)
47. Als **„Empfänger:in“** gilt jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden (vgl. Art 4 Z 9 DSGVO). [↑](#footnote-ref-47)
48. Drittland = Land außerhalb der EU bzw. des Geltungsbereichs der DSGVO [↑](#footnote-ref-48)
49. Werden Daten an Empfänger:innen in ein Drittland (= Nicht-EU Land) übermittelt, sind darüber zusätzliche Angaben ins Verarbeitungsverzeichnis aufzunehmen. Bitte prüfen Sie insbesondere, in welchem Land der/die Bertreiber:in des Unternehmensservers ansässig ist sowie jene Unternehmen, die die Tools für Ihre Unternehmenswebseite zur Verfügung stellen! 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-49)
50. Einwilligungen von Websitebesucher:innen werden üblicherweise über einen Cookie Banner eingeholt. Der Cookie Banner muss in diesem Fall den Erfordernissen einer [DSGVO-konformen Einwilligung](https://www.usp.gv.at/it-geistiges-eigentum/datenschutz/einwilligung.html) entsprechen. Von der Einholung einer Einwilligung kann nur dann abgesehen werden, wenn die verwendeten Tools ausschließlich der Funktionalität der Webseite dienen! [↑](#footnote-ref-50)
51. Die Rechtsgrundlage des berechtigten Interesses kann nur sehr eingeschränkt herangezogen werden, insbesondere wenn Web-Tracking angewandt wird, ist dies nicht zulässig! [↑](#footnote-ref-51)
52. Zur Frage, wie lange Daten aufbewahrt werden dürfen, finden Sie Erläuterungen auf der [Homepage](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_de)

    [der Europäischen Kommission](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_de). [↑](#footnote-ref-52)
53. Eine Auflistung weitere möglicher Speicher-, Verjährungs- und Aufbewahrungsfristen finden Sie auf der [Homepage der WKÖ](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html). [↑](#footnote-ref-53)
54. vgl. Art 32 DSGVO [↑](#footnote-ref-54)
55. Vertraulichkeit bedeutet: Schutz vor unbefugter Preisgabe von Informationen. Diese dürfen ausschließlich den Befugten zugänglich sein. [↑](#footnote-ref-55)
56. 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-56)
57. 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-57)
58. VPN= eine [Netzwerkverbindung](https://de.wikipedia.org/wiki/Netzwerk), die von Unbeteiligten nicht einsehbar ist. [↑](#footnote-ref-58)
59. = Vorfallreaktionsmanagement = eine systematische Strategie, welche Unternehmen, Organisationen und Einzelpersonen in die Lage versetzt, Cyberangriffe und IT-Sicherheitslücken abzuwehren oder zu schließen. [↑](#footnote-ref-59)
60. = „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-60)