# Verantwortlich

Name

Adresse

Telefonnummer

Mailadresse

# Grundsätzliches

Wir legen großen Wert auf den Schutz der Daten unserer Kunden und Geschäftspartner und speichern nur für den jeweiligen Zweck absolut notwendige Daten.

Die Daten werden nur in notwendigen Fällen an Dritte weitergegeben und werden NICHT zu Profilingzwecken o.ä. eingesetzt.

In unserem Unternehmen werden keine sensiblen Daten (lt. Definition der DSGVO) verarbeitet, es werden keine Angebote an Kinder gemacht und keine Videoüberwachung eingesetzt.

Zudem legen wir größten Wert auf die technische Sicherheit unserer Daten.

Es ist daher im Falle eines datenschutzrechtlich problematischen Zwischenfalls nur von einem sehr geringen Risiko für die Rechte und Freiheiten unserer Kunden und Geschäftspartner auszugehen.

# Datenschutzfolgenabschätzung

Es wurde keine Datenschutzfolgenabschätzung durchgeführt, da voraussichtlich kein hohes Risiko für die Betroffenen besteht.

# Betroffenen-Kategorien

|  |  |
| --- | --- |
| **KAT.** | **BETROFFENE** |
| **A** | Kunden inkl. Daten zu Kontaktperson(en) |
| **B** | Interessenten |
| **C** | Auftragsverarbeiter inkl. Daten zu Kontaktperson(en) |
| **D** | Lieferanten inkl. Daten zu Kontaktperson(en) |

# Daten-Kategorien

|  |  |  |
| --- | --- | --- |
| **KAT.** | **Name der Datenkategorie** | **Enthält folgende Daten** |
| **a** | Rechnungsdaten | Firmenwortlaut  Adresse  UID-Nummer |
| **b** | Kontaktdaten | Name  Adresse  Telefon  Mail  Kontaktpersonen & Position |
| **c** | Vertragsdaten | Verträge |
| **d** | Projektbezogene Daten | Baupläne, Fertigstellungsmeldungen, Inbetriebnahmen, technische Anforderungen, |
| **e** | Bestelldaten | Art und Anzahl der bestellten Produkte oder Dienstleistungen |
| **f** | Verrechnungsdaten | Bankverbindung  Zahlungsinformationen |
| **g** | Login-Daten | Benutzernamen, Passwörter je Anwendung |
| **h** | Kommunikationsdaten | Korrespondenzen zum Projekt (Mailverkehr, Schriftverkehr) |
| **i** | Dokumentation & Ablage | Datensicherung & Ablage & Archiv  Projektdokumentation |

*Mit \* markierte Daten sind „sensible Daten“ iSd. Art. 9 DSGVO*

# Übermittlungs-Empfänger

|  |  |
| --- | --- |
| **KAT.** | **EMPFÄNGER** |
| **1** | Banken |
| **2** | Rechtsvertreter |
| **3** | Wirtschaftstreuhänder/prüfer |
| **4** | Gerichte |
| **5** | Zuständige Verwaltungsbehörden (Finanzamt, AMS, BH, etc.) |
| **6** | Inkassounternehmen |
| **7** | Fremdfinanzierer / Leasingunternehmen |
| **8** | Vertrags/Geschäftspartner |
| **9** | (private) Versicherungen |
| **10** | Statistik Austria |
| **11** | Inspektorate |
| **12** | Betriebliche und außerbetriebliche Interessenvertretungen (AK, WKO, etc.) |
| **13** | Vorsorgekassen, Abfertigungskassen, Sozialversicherungen, Pensionskassen |
| **14** | Transportunternehmen (Post, etc.) |

# Datenverarbeitungen & Zwecke

1. Rechnungswesen

Zweck:

Verarbeitung und Übermittlung von Daten im Rahmen einer Geschäftsbeziehung zum Zweck der Angebotserstellung (Vorvertragliche Maßnahme), der Rechnungslegung und des Mahnwesens, der Erfüllung der steuerlichen Gesetze inkl. Finanzbuchhaltung.

Fügen Sie bei jeder Verarbeitung eigene/weitere Erklärungen hinzu!

Beauftragte Auftragsverarbeiter:

Steuerberater

Besondere technisch-organisatorische Maßnahmen:

Der Zugriff auf die Buchhaltung ist nur von einem Computer aus möglich

Von welchen Betroffenen werden personenbezogene Daten gespeichert?

|  |  |  |
| --- | --- | --- |
| **KAT.** | **Rechtliche Basis** | **Aufbewahrungsfrist** |
| **A**  **C**  **D** | Vertragserfüllung  Gesetzliche Grundlage | Steuerrechtliche Aufbewahrungsfrist: 7 Jahre |

Welche personenbezogenen Daten werden wo gespeichert und an wen weitergegeben?

|  |  |  |  |
| --- | --- | --- | --- |
| **Betroffene** | **Datenkat.** | **Wo werden sie gespeichert** | **Empfängerkategorie** |
| **A** | a, b, e | Lokal am PC/am Server  Buchhaltungsprogramm  In Papierform  Cloudspeicher | 1,3,5,6,8,9 |
| **C/ D** | a, b, e, f | Lokal am PC/am Server  Buchhaltungsprogramm  In Papierform | 1,3,5 |

1. Kommunikation & Korrespondenz

Zweck:

Die Kommunikation & Korrespondenz mit Geschäftspartnern wird im allgemeinen via E-Mail und Telefon abgewickelt.

Zur Kommunikation via E-Mail wird die bei \_\_\_\_\_\_\_ gehostete Mailadresse verwendet.   
Die Kontaktdaten werden in \_\_\_\_\_\_\_\_ gespeichert.

In vereinzelten Fällen und auf ausdrücklichen Wunsch des Kunden kann die Kommunikation via WhatsApp oder Facebook stattfinden.

In allen Fällen werden keinerlei besonders schutzwürdige Daten über diese Kommunikationswege übermittelt.

Beauftragte Auftragsverarbeiter:

Besondere technisch-organisatorische Maßnahmen:

Es wird darauf geachtet, keinerlei schutzwürdige und vertrauliche Daten (wie z.B. Passwörter) via Mail zu übertragen oder personenbezogene Daten via Mail zu verarbeiten.   
Die Kontaktdaten in der Mailsignatur werden nicht als besonders schutzwürdig gewertet und bergen daher kein hohes Risiko

Von welchen Betroffenen werden personenbezogene Daten gespeichert?

|  |  |  |
| --- | --- | --- |
| **KAT.** | **Rechtliche Basis** | **Aufbewahrungsfrist** |
| **A** | Vertragserfüllung | Nach Ablauf der Geschäftsbeziehung 7 Jahre |
| **B** | Vorvertragliche Maßnahme  Eigenes Interesse | Maximal 12 Monate |
| **C** | Vertragserfüllung  Auftragsverarbeiter-Vertrag | Nach Ablauf der Geschäftsbeziehung 7 Jahre |
| **D** | Vertragserfüllung | Nach Ablauf der Geschäftsbeziehung 7 Jahre |

Welche personenbezogenen Daten werden wo gespeichert und an wen weitergegeben?

|  |  |  |  |
| --- | --- | --- | --- |
| **Betroffene** | **Datenkat.** | **Wo werden sie gespeichert** | **Empfängerkategorie** |
| **A** | b, c, d, e, h | Outlook | 2, 4 im Anlassfall |
| **B** |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Marketing

Zweck:

Marketingaktivitäten mit personenbezogenen Daten finden derzeit auf folgenden Wegen statt:

- Newsletterversand via Newsletter

- eigene Homepage / Kontaktformular

- in Einzelfällen werden bestehende Kunden über neue Angebote informiert (via Email)

Beauftragte Auftragsverarbeiter:

Besondere technisch-organisatorische Maßnahmen:

Von welchen Betroffenen werden personenbezogene Daten gespeichert?

|  |  |  |
| --- | --- | --- |
| **KAT.** | **Rechtliche Basis** | **Aufbewahrungsfrist** |
| **A** | Berechtigtes Interesse | Nach Ablauf der Geschäftsbeziehung 7 Jahre |
| **B** | Einwilligungserklärung via Newsletter (Double Opt-In) | Bis Einwilligung entzogen wird |
| **B** | Vorvertragliche Maßnahme  Eigenes Interesse | Maximal 12 Monate |

Welche personenbezogenen Daten werden wo gespeichert und an wen weitergegeben?

|  |  |  |  |
| --- | --- | --- | --- |
| **Betroffene** | **Datenkat.** | **Wo werden sie gespeichert** | **Empfängerkategorie** |
| **A** |  |  | 14 |
| **B** |  |  |  |

1. Webseite

Zweck:

Auf unserer eigenen Webseite werden grundsätzlich keine personenbezogenen Daten gespeichert, außer jenen, die Interessenten von sich aus eingeben.

Es besteht die Möglichkeit, über ein Kontaktformular und ein Newsletter-Anmeldeformular Kontakt aufzunehmen.

Das Kontaktformular wurde um die Angabe der Kenntnisnahme unserer Datenschutzerklärungen erweitert (Checkbox).

Die Newsletter-Anmeldung erfolgt via Double-Opt-In. Der Interessent kann sich jederzeit wieder abmelden.

Zudem wird der Webanalyse-Dienst Google Analytics verwendet. Allerdings können durch diese Daten keinerlei Rückschlüsse auf einzelne Personen gezogen werden, da die Daten pseudonymisiert werden.

Sämtliche automatisch gespeicherte Daten (die z.B. vom Hoster erfasst werden), werden von uns in keinster Weise verarbeitet oder ausgewertet.

Beauftragte Auftragsverarbeiter:

Besondere technisch-organisatorische Maßnahmen:

Von welchen Betroffenen werden personenbezogene Daten gespeichert?

|  |  |  |
| --- | --- | --- |
| **KAT.** | **Rechtliche Basis** | **Aufbewahrungsfrist** |
| **B** |  | Maximal 12 Monate |
| **C** |  |  |
| **D** |  |  |

Welche personenbezogenen Daten werden wo gespeichert und an wen weitergegeben?

|  |  |  |  |
| --- | --- | --- | --- |
| **Betroffene** | **Datenkat.** | **Wo werden sie gespeichert** | **Empfängerkategorie** |
| **A/B** | b, h | Outlook |  |

1. Kundenaufträge & Logistik

Zweck:

Zur Abwicklung von Kundenprojekten werden primär nur jene personenbezogenen Daten benötigt, die auch schon in den Datenverarbeitungen 1-7 gespeichert werden.

Hinzukommen lediglich noch Daten, die das jeweilige spezifische Projekt betreffen.

Die Daten werden vereinzelt nach Kunden sortiert zusätzlich in Papierform abgelegt.

Ebenso beinhaltet diese Datenverarbeitung auch die logistische Abwicklung unserer Aufträge.

Zu diesem Zweck werden Auftragsverarbeiter herangezogen.

Beauftragte Auftragsverarbeiter:

Besondere technisch-organisatorische Maßnahmen:

Von welchen Betroffenen werden personenbezogene Daten gespeichert?

|  |  |  |
| --- | --- | --- |
| **KAT.** | **Rechtliche Basis** | **Aufbewahrungsfrist** |
| **A** | Vertragserfüllung | Bis zur Beendigung der Geschäftsbeziehung oder bis zum Ablauf der für den Auftraggeber geltenden Garantie-, Gewährleistungs-, Verjährungs- und gesetzlichen Aufbewahrungsfristen; darüber hinaus bis zur Beendigung von allfälligen Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden. |
| **C** | Vertragserfüllung  Auftragsverarbeiter-Vertrag | Nach Ablauf der Geschäftsbeziehung 7 Jahre |
| **D** | Vertragserfüllung | Nach Ablauf der Geschäftsbeziehung 7 Jahre |

Welche personenbezogenen Daten werden wo gespeichert und an wen weitergegeben?

|  |  |  |  |
| --- | --- | --- | --- |
| **Betroffene** | **Datenkat.** | **Wo werden sie gespeichert** | **Empfängerkategorie** |
| **A** | a, b, c ,d, e | Server, Outlook | 8, 14 |
| **C/D** | a, b, c, d | Server, Outlook | 8, 14 |

1. Dokumentenablage & Archiv

Zweck:

Diese Verarbeitung umfasst die Ablage & Archivierung von Dokumenten aller Art (Verträge, Korrespondenzen, Projektdokumentationen, etc.), sowie die Inventarisierung.

Beauftragte Auftragsverarbeiter:

Besondere technisch-organisatorische Maßnahmen:

Von welchen Betroffenen werden personenbezogene Daten gespeichert?

|  |  |  |
| --- | --- | --- |
| **KAT.** | **Rechtliche Basis** | **Aufbewahrungsfrist** |
| **A-E** | Gesetzliche Grundlage  Eigenes Interesse | Bis zur Beendigung der Geschäftsbeziehung oder bis zum Ablauf der für den Auftraggeber geltenden Garantie-, Gewährleistungs-, Verjährungs- und gesetzlichen Aufbewahrungsfristen; darüber hinaus bis zur Beendigung von allfälligen Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden. |

Welche personenbezogenen Daten werden wo gespeichert und an wen weitergegeben?

|  |  |  |  |
| --- | --- | --- | --- |
| **Betroffene** | **Datenkat.** | **Wo werden sie gespeichert** | **Empfängerkategorie** |
| **A -E** | a - i | Versperrte Archivräume, Server | 5 im Anlassfall |

# Auftragsverarbeiter VERZEICHNIS

Die folgende Liste enthält all jene Dienstleister bzw. webbasierte Services, die uns als Auftragsverarbeiter bei der Abwicklung unserer Geschäfte unterstützen.

Dabei wurde bei allen eine umfassende Prüfung im Hinblick auf Vertrauenswürdigkeit und Unbescholtenheit durchgeführt.

Ein eigener Auftragsverarbeitervertrag wurde nur mit ausgewählten Partnern abgeschlossen.

Bei allen anderen wurden die veröffentlichten Datenschutzrichtlinien/Nutzungsvereinbarungen auf DSGVO-Konformität überprüft und abgespeichert.

Es kann bei allen Partnern von einem angemessenen Datenschutzniveau ausgegangen werden.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Zweck / Erklärung | Eigener Vertrag vorhanden? | Weitergabe in ein Drittland? |
| Homepage-Hosting-Provider | Hosting der Homepage und Mailadresse |  |  |
| Newslettertool | Name & Mailadresse zum Zweck des Versands von Newslettern & Informationen  Die Newsletter-Einstellungen wurden auf das maximal mögliche Datenschutzniveau gemacht. |  |  |
| EDV-Dienstleister |  |  |  |
| Reinigungsunternehmen |  |  |  |
| Entsorgungsunternehmen |  |  |  |
| Buchhaltungssoftware |  |  |  |
| Steuerberater | Jahresabschluss | Nicht nötig, weil selbst Verantwortlicher |  |
| Logistikdienstleister |  |  |  |
| Microsoft Office365 |  | Nein  <https://privacy.microsoft.com/de-de/privacystatement> |  |
| Google |  | Nein  <https://privacy.google.com/businesses/> | Ja |
| Google Analytics | Anonymisierte Datenerhebung der Homepagebesucher | Ja | Ja |
| WhatsApp | Im Einzelfall zur Kommunikation mit Kunden | Nein, wird nur in Ausnahmefällen genutzt |  |

# Wo werden die DSGVO Dokumente aufbewahrt?

|  |  |
| --- | --- |
| dieses Dokument (= Verarbeitungsverzeichnis) | **konkreten Speicherpfad angeben** |
| die Auftragsverarbeiter-Verträge | **konkreten Speicherpfad angeben** |
| die Einwilligungserklärungen Newsletterversand | Direkt im Newslettertool |

# Technisch-organisatorische Massnahmen zur Datensicherheit

1. Infrastruktur

Die **Vertraulichkeit & Integrität** der Daten ist durch folgende Maßnahmen gegeben:

Bauliche Maßnahmen:

Der **Zutritt** zur Betriebsstätte ist durch Schlüssel gesichert.

Der Verantwortliche stellt sicher, dass der **Zutritt zu den Räumlichkeiten** und der Infrastruktur nur berechtigten Personen möglich ist. Mitarbeiter, welche Schlüssel oder Zutrittsberechtigungen zu den Räumlichkeiten erhalten haben, sind entsprechend geschult und darüber infomiert, dass diese den Verantwortlichen umgehend informieren müssen, sollte der Schlüssel abhandenkommen (Verlust, Diebstahl oder ähnliches).

Videoüberwachung? Zutrittssysteme?

IT-Infrastruktur (Server & Clients)

Der Verantwortliche stellt sicher, dass **Server** vor unberechtigtem Zugriff geschützt (etwa versperrt) sind und eine Verfügbarkeit des Servers in ausreichendem Ausmaß sichergestellt ist. Ferner hat der Verantwortliche Maßnahmen ergriffen, die IT-Infrastruktur vor Zerstörung (etwa durch Feuer) zu schützen. Server und andere Komponenten sind mit einer unterbrechungsfreien Stromversorgung gesichert.

Der Verantwortliche stellt sicher, dass **Computer** vor unbefugtem Zugriff und unbefugter Nutzung geschützt sind. Darüber hinaus sind sämtliche Arbeitsplatzrechner so konfiguriert, dass sich Updates und Softwarekorrekturen, die Sicherheitslücken schließen, automatisch installieren. Er stellt darüber hinaus sicher, dass regelmäßig geprüft wird, ob das Einspielen ordnungsgemäß funktioniert hat.

Bei Arbeitsplatzrechnern, auf denen besondere Kategorien von Daten gespeichert sind, sind die genutzten Speichermedien verschlüsselt.

Der Verantwortliche stellt sicher, dass sämtliche Arbeitsplatzrechner so gesichert sind, dass Rechnermikrofone und Kameras gegen unberechtigten Zugriff gesperrt sind. Sämtliche Arbeitsplatzrechner werden regelmäßig auf Viren untersucht. Die Grundkonfiguration der Rechner sieht vor, dass die Rechner vor unberechtigtem Zugang geschützt sind (die Nutzung des Rechners ist nur nach Eingabe eines Passworts möglich).

Folgende technische Maßnahmen werden je Arbeitsplatzrechner ergriffen:

**[bitte ergänzen]**

Der Verantwortliche stellt sicher, dass der Zugriff auf Systeme nur nach Eingabe eines Passworts möglich ist, wobei Passwörter folgende Kriterien erfüllen müssen (Passwortrichtlinie):

Es werden nur Passwörter verwendet, die mindestens 8 Zeichen lang sind und sowohl Zahlen/Groß-Kleinbuchstaben/Sonderzeichen enthalten. Die Passwörter müssen alle 2 Monate geändert werden.

Der Verantwortliche stellt sicher, dass Benutzer gelöscht oder gesperrt werden, sobald diese keinen Zugriff mehr auf das System benötigen (etwa: Löschen von Benutzerkonten von ehemaligen Mitarbeitern).

Der Verantwortliche stellt sicher, dass sämtliche Systeme durch eine Firewall geschützt werden, um einen unberechtigten externen Zugriff zu verhindern. Der Verantwortliche stellt sicher, dass ein aktueller Viren- und Spamfilter installiert ist und gewartet wird.

Der Verantwortliche stellt sicher, dass sämtliche Telekommunikationseinrichtungen (etwa Telefonanlage, Fax, VPN, W-LAN, E-Mailserver, Firewalls) vor unberechtigtem Zugriff geschützt sind.

Sofern der Verantwortliche öffentlich zugängliche Netzwerke („WLAN“) betreibt, wird er diese so sichern, dass ein Zugriff auf nicht öffentlich zugängliche Systeme des Verantwortlichen nicht möglich ist.

Der Verantwortliche stellt ferner sicher, dass öffentlich zugängliche Netzwerkanschlüsse (etwa Netzwerkdosen) nicht genutzt werden können.

Der Verantwortliche stellt sicher, dass sämtliche Rechner, welche nicht mehr genutzt werden sollen, ordnungsgemäß entsorgt werden und personenbezogene Daten auf den Rechnern vor unberechtigtem Zugriff geschützt werden

Sicherungen/Backup:

Die betrieblichen Daten werden (mit Ausnahme jener Daten, die in webbasierten Anwendungen gespeichert werden) folgendermaßen **gesichert**:

Der Verantwortliche stellt sicher, dass Backups der Datenbestände in folgenden Abständen erstellt werden:

**[bitte ergänzen]**

Der Verantwortliche stellt sicher, dass sämtliche lokal auf den Arbeitsplatzrechnern gespeicherten Daten regelmäßig gesichert werden.

Die Sicherungen reichen 14 Tage zurück, danach werden sie überschrieben.

Pseudonymisierung und Verschlüsselung

Sofern für die jeweilige Datenverarbeitung möglich, werden die Daten pseudonymisiert und verschlüsselt weitergegeben.

Sämtliche Cloud-basierte Dienste sind ausschließlich via SSL-Verschlüsselung (https) erreichbar.

Mobile Geräte

Sämtliche Notebooks wurden verschlüsselt (Festplattenverschlüsselung mit Bitlocker), um im Fall eines Verlustes des mobilen Gerätes die Datensicherheit zu gewährleisten.

USB Sticks werden niemals für den Transport von personenbezogenen Daten verwendet

Mobiltelefone sind mit SIM-Code gesichert / Fernwartung aktiviert / Backup lokal

# Umsetzung der Betroffenenrechte & Informationspflichten

Die **Informationspflichten** werden über die auf unserer Homepage veröffentlichten Datenschutzbestimmungen erfüllt.

Die **Betroffenenrechte** auf Auskunft, Löschung, Richtigstellung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch werden von wahrgenommen.

Es würde für unser Einzelunternehmen einen unzumutbaren organisatorischen Aufwand bedeuten, einzelne Datenkategorien zu unterschiedlichen Zeitpunkten zu löschen, daher wurde im Allgemeinen die gesetzliche Aufbewahrungsfrist von 7 Jahren gewählt.

Falls in Einzelfällen eine Löschung zu einem anderen Zeitpunkt nötig, gesetzlich erlaubt und möglich ist, wird dies natürlich durchgeführt.

# Evaluierungsmassnahmen

Dieses Dokument wird jährlich auditiert und um den Status Quo ergänzt.

# DATA BREACH NOTIFICATION

Für die Benachrichtigung der Datenschutzbehörde (und ggf. der Betroffenen) im Falle eines Datenmissbrauchs ist ebenfalls der oben genannte Verantwortliche zuständig.

Stand \_\_\_\_\_\_\_\_\_ / verfasst von \_\_\_\_\_\_\_\_\_