**Verzeichnis der Verarbeitungstätigen**

**nach Art 30 Abs. 1 EU-Datenschutz-Grundverordnung (DSGVO)**

**Inhalt**

1. Stammdaten
2. Datenverarbeitungen/Datenverarbeitungszwecke
3. Detailangaben zu den einzelnen Datenverarbeitungszwecken
4. Beschreibung organisatorisch-technischer Datensicherheits-Maßnahmen
5. **Stammdaten**

Name und Kontaktdaten der/des für die Verarbeitung verantwortlichen Person/en:

Max Mustermann GmbH

Neuer Weg 1

ZZZZ Musterdorf

Karl Datenschützer

karl.datenschuetzer@mustermann.at

Tel. Nr.

Fax Nr.

Vertreter: KEINER

1. **Datenverarbeitungen / Datenverarbeitungszwecke**

*Im ersten Schritt müssen Sie die einzelnen Verarbeitungstätigkeiten inkl. der dabei verarbeiteten Daten identifizieren und auflisten.*

1. **Zwecke und Beschreibung der Datenverarbeitungen (Übersicht):**

|  |  |  |
| --- | --- | --- |
| 1 | Auftragsverwaltung  Auftragsverwaltung in Fremdsystemen  (Trafik-Plus, Ö-Ticket,  Asfinag, Lotto)  Handelskette | Kunden-, Lieferanten und Artikeldatenverwaltung;  Erstellung von Angeboten, Aufträgen, Lieferscheinen und Rechnungen;  Verwaltung der Bestellungen bei Lieferanten und Durchführung von Lieferungen an Kunden;  Katalog- und Bestellsystem über Website inkl. Benutzerkontenverwaltung; Schnittstellen zu Buchhaltung (Datenexport) und Payment-Provider für Zahlungsabwicklung. |
| 2 | Buchhaltung / EAR | Durchführung der Buchhaltung gem. der gesetzlichen Vorgaben |
| 3 | Kontaktdatenbank | Verwaltung der Kontakte für Korrespondenz mit mobilen Geräten, E-Mail, Brief etc.; Speicherung und Datenabgleich erfolgt über Cloudsystem.  Sammlung Visitenkarten. |
| 4 | Marketingdatenbank | Verwaltung Interessentendaten für Marketing-Aktivitäten, Katalogzusendung, Newsletter und sonst. Werbeaktionen (postalische personalisierte Werbung). |
| 5 | Personalverwaltung  & Bewerbungskartei | Mitarbeiterdaten für Lohn und Gehaltsverrechnung der Mitarbeiter; Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, auf Grund von Gesetzen, Kollektivverträgen oder vertraglicher Verpflichtungen.  Archivierung bzw. Evidenzhaltung von Stellenausschreibungen, Bewerbungen, Korrespondenz, Dienstzeugnisse. |
| 6) | Alarm- oder Überwachungssysteme | Aufzeichnung von Bild- oder Videomaterial zur Überwachung der Geschäftsräumlichkeiten zum Zwecke der Dokumentation bei Diebstahl, Fehlgeld-/Waren-Transaktionen oder Alarmsicherung außerhalb der Geschäftszeiten. |
|  |  | Weitere ergänzen bzw. nichtzutreffendes löschen |

\*) *Weitere ergänzen bzw. nichtzutreffendes löschen*

1. **Kategorien personenbezogener Daten / Datenarten:**

*Im nächsten Schritt müssen die einzelnen Datenkategorien erhoben werden.*

|  |
| --- |
| Firmendaten   * Kundenname / Firmenname * Rechtsform * Anschrift * Telefon Nr. * Fax Nr. * E-Mail-Adresse * Website * Firmenbuch Nr. * UID Nr. * Bankverbindung * IP-Adresse |
| Kontaktdaten Ansprechpartner   * Name, Vorname, Titel * E-Mail-Adresse * Telefon Nr. * Mobil Nr. * Funktion * Sonstige Daten |
| Mitarbeiter- & Bewerbungsdaten   * Allg. Kategorie (Personal Nr., Name, Adresse, Geburtsdatum, Konto Nr., KFZ-Kennzeichen) * Besondere Kategorien (SV-Nummer, Gewerkschaft, Religionsbekenntnis, Arbeitszeugnisse) \*) * Strafrechtsrelevanten Daten (Strafregisterauszug, Waffenverbot) \*)   \*) *prüfen ob sensible, schützenswerte Daten gespeichert werden!* |
| Bild-/Videodaten   * Bilddaten der Alarm- / Überwachungssysteme des Geschäftslokales \**\*)* |
| *Weitere ergänzen bzw. nichtzutreffendes löschen* |

*\*\*) falls Mitarbeiter darauf zu erkennen sind, ist deren schriftliches Einverständnis erforderlich  
 + Info-Aufkleber im Geschäft „Achtung Videoüberwachung“*

1. **Kategorien Datenempfänger:**

*Im nächsten Schritt müssen die einzelnen Empfängerkategorien erhoben werden an die personenbezogene Daten weitergegeben werden.*

|  |  |  |
| --- | --- | --- |
| **Empfängerkategorien** | **Weitergabe an Drittstaat**  \*\*\*\*) | **EU-Angemessenheits-Beschluss**  \*\*\*\*) |
| Lieferanten |  |  |
| Partnerfirmen oder -Shop |  |  |
| Distributoren (mit eigenem Buchungssystem \*) |  |  |
| Generalvertretungen |  |  |
| Hosting-Provider für Website/Online-Shop |  |  |
| Cloudanbieter (Apple, Dropbox, Google) \*\*) | USA ? | ja |
| IT-Dienstleister |  |  |
| Sicherheitsfirmen \*\*\*) |  |  |
| Banken |  |  |
| Transportunternehmen |  |  |
| Steuerberater & Wirtschaftstreuhänder |  |  |
| Inkassounternehmen |  |  |
| Rechtsvertreter |  |  |
| Behörden, Gerichte | - | - |
| Finanzamt | - | - |
| Sozialversicherung | - | - |
| Betriebsrat | - | - |
| Mitarbeiter-Vorsorge- & Pensionskassen | - | - |
| Intern | - | - |
| *Weitere ergänzen bzw. nichtzutreffendes löschen* |  |  |

*\*) z.B. Trafik-Plus, Ö-Ticket, Asfinag, Lotto etc.*

*\*\*) Div. US-Firmen speichern Daten in EU (z.B. Microsoft)*

*\*\*\*) Im Alarmfall werden Bilddaten weitergeleitet bzw. Sicherheitsfirma hat Zugriff auf die Bilddaten*

*\*\*\*\*) bei Datenspeicherung* ***außerhalb*** *der EU*

1. **Rechtsgrundlagen:**

* Vertragserfüllung (Bestellformular, Online-Shop)
* Zustimmungserklärung (schriftlich oder online)
* Gesetzliche Verpflichtung gem. BAO, UGB, etc.
* überwiegend berechtigtes Interesse des Verantwortlichen oder eines Dritten

Es sollen nur die **notwendigen Daten erhoben und gespeichert werden**, die zum Zwecke der Verarbeitung benötigt werden. **Entfällt** die **Rechtsgrundlage**, so sind die **Daten** ausnahmslos unter Berücksichtigung der Aufbewahrungsfristenzu **löschen**.

1. **Aufbewahrungs- & Löschfristen:**

Eine gesammelte Auflistung der Speicher und Aufbewahrungsfristen finden Sie im Dokument „Speicher\_und\_Aufbewahrungsfristen.pdf“, sowie unter folg. Link:

<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html>.

Darüber hinaus gehend können Daten

* bis zur Beendigung eines allfälligen Rechtsstreits
* für laufende Gewährleistungs- oder Garantiefristen
* Produkthaftung oder Schadenersatz-Abwicklung
* zur Wahrung von Rechtsansprüchen

gespeichert bzw. aufbewahrt werden.

1. **Datenschutz-Folgenabschätzung:**

* Eine Datenschutz-Folgenabschätzung wurde nicht durchgeführt, da sie nach aktueller gesetzlicher Lage nicht erforderlich ist (Datenschutz-Deregulierungs-Gesetz 2018).

1. **Detailangaben zu den einzelnen Datenverarbeitungen**

*Die Felder sind entsprechend der im Punkt B.1. erhobenen Verarbeitungstätigkeiten zu auszufüllen.*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr.** | **Datenverarbeitung & Zweck** | **Datenkategorien / Datenarten** | **Rechtsgrundlage** | **ADV**  \*) | **Empfänger** | **3.Staat**  \*\*) | **Speicherdauer** | **Lösch-methode** |
| 1 | Auftragsverwaltung  Distributoren  Partner-Shop  Fremdsysteme | Kundenname/ Firmenname  Rechtsform  Anschrift  Telefon Nr.  Fax Nr.  E-Mail-Adresse  UID-Nr.  Firmenbuch Nr.  Bankverbindung  Kontaktdaten Ansprechpartner (E-Mail, Telefon Nr., Mobil, Funktion)  IP-Adresse | Vertragserfüllung | ja /  nein | Kunden  Steuerberater  Provider  Cloud | ?? | 7 J. | manuell |
| 2 | Buchhaltung / EAR | Rechnungsdaten Einnahmen + Ausgaben, Lieferantendaten, Bankdaten | Gesetzliche Verpflichtung | ja /  nein | Steuerberater  FA | - | 7 J | Manuell |
| 3 | Kontaktdatenbank | Firmenname Rechtsform  Anschrift  Telefon Nr.  Fax Nr.  E-Mail-Adresse  UID-Nr.  Firmenbuch Nr.  Bankverbindung  Kontaktdaten Ansprechpartner (E-Mail, Telefon Nr., Mobil Nr., Funktion) | Einwilligung,  Vertragserfüllung | ja /  nein | Provider  Cloud | ?? | bis Widerruf bzw. 7 J. nach der letzten Bestellung | manuell |
| 4 | Marketingdatenbank | Kundenname  Anschrift  Telefon Nr.  E-Mail-Adresse  Kontaktdaten Ansprechpartner (E-Mail, Telefon Nr., Mobil, Funktion) | Einwilligung | ja /  nein | Provider  Cloud  Druckereien | ?? | bis zum Widerruf | manuell |
| 5 | Personalverwaltung  & Bewerbungskartei | Mitarbeiter- & Bewerbungsdaten   * Allg. Kategorie (Name, Adresse, Geburtsdatum, Konto Nr., KFZ-Kennzeichen) * Besondere Kategorien (SV-Nr. Gewerkschaft; Religion, Arbeitszeugnisse) * Strafrechtsrelevante Daten (Strafregisterauszug, Waffenverbot) | Vertragserfüllung  Gesetzliche Verpflichtung | ja /  nein | Steuerberater,  Sozialversicherung  Finanzamt  BMVK  Banken  Betriebsrat | nein | 7 bis 30 J.  Bewerbungsunterlagen 1 J. ab Ablehnung | manuell |
| 6 | Alarm- oder Überwachungs-systeme | Bild-/Videodaten | Berechtigtes Interesse | Ja/nein  \*\*\*) | Sicherheitsfirma | ?? | max. 72 Stunden | automatisch |
|  | Weitere ergänzen bzw. nichtzutreffendes löschen |  |  |  |  |  |  |  |

*\*) ADV = Auftragsverarbeiter-Vertrag (Vertrag mit einem Dienstleister, der im Auftrag des Unternehmens personenbezogene Daten verarbeitet);   
 Mustervorlage siehe Kap. 3 DSGVO-Ordner*

*\*\*) bei Datenspeicherung* ***außerhalb*** *der EU*

*\*\*\*) Vertrag mit Sicherheitsfirma notwendig wenn diese Daten übertragen bekommen (ständig oder im Alarmfall)*

1. **Beschreibung technische & organisatorische Datensicherheits-Maßnahmen**

Im Zuge der Umsetzung der DSGVO-Vorgaben gem. Art. 32 hat die für Datenschutz verantwortliche Person dafür zu sorgen, dass geeignete **technische und organisatorische Maßnahmen** festgelegt werden die sicherstellen, dass die Datensicherheit bei der Verarbeitung von personenbezogenen Daten gewährleistet ist.

Zum Schutz von personenbezogenen Daten haben die Verantwortlichen und Auftragsverarbeiter die Grundsätze des Datenschutzes schon in Ihre Anwendungen zu integrieren (privacy by design) und datenschutzfreundliche Voreinstellungen zu verwenden (privacy by default).

Für die Umsetzung technisch/organisatorischer Maßnahmen gelten folgende **Grundsätze**:

* **Sicherheit**: Daten müssen gegen unbefugten Zugriff durch technische und organisatorische Maßnahmen geschützt sein.
* **Vertraulichkeit**: personenbezogene Daten dürfen niemand anderem, als im eigentlichen Zweck vorgesehen, zur Verfügung gestellt werden, bzw. muss verhindert werden, dass jemand anderer darauf Zugriff erhält.
* **Integrität**: Datensätze dürfen nicht fälschlicherweise verändert werden. Es muss die Korrektheit gewährleistet werden.
* **Verfügbarkeit**: Die Systeme und Dienste müssen verfügbar bleiben. Sie dürfen nicht unwiederbringlich verloren gehen durch Systemabsturz oder Verlust eines Ordners.

Folgende Maßnahmen dienen zur Umsetzung der **organisatorischen Sicherheit**:

* absperrbare Büros & Schränke
* Mitarbeiter bezüglich IT-Sicherheit schulen
* Richtlinien zur sicheren Nutzung von sozialen Medien
* IT-Sicherheitsbeauftragte/n (eventuell externer Dienstleister)
* Zugangskontrollen zu sensibler Hardware (Server, Router)
* Notfallpläne für IT-Sicherheitsvorfälle
* Richtlinie zur sicheren Nutzung von IT und Internet
* Weiter Maßnahmen ergänzen bzw. nichtzutreffendes streichen

Folgende Maßnahmen dienen zur Umsetzung der **technischen Sicherheit**:

* Virenschutz
* Firewall
* Passwortregelungen
* Passwörter sicher verwahren
* Berechtigungskonzept
* Regelmäßige Datensicherung
* Verschlüsselung von E-Mails, Daten und Festplatten
* Verwendung von VPNs
* Protokollierung von Zugriffen
* Bild- und Videoaufzeichnung Geschäftslokal
* Alarmsicherung von Geschäftslokal / Lager
* Blocken von Funktionen (z.B. USB-Ports)
* Pseudonymisierung und Verschlüsselung von personenbezogenen und sensiblen Daten
* Datenlöschungs-Konzept erstellen
* Weiter Maßnahmen ergänzen bzw. nichtzutreffendes streichen

Zusätzliche sollen Unternehmen Verfahren zur **laufenden Überprüfung** und **Evaluierung der Wirksamkei**t der festgelegten Maßnahmen fixieren (z.B. jährliche Überprüfung bzw. Audit).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Datum Unterschrift Verantwortlicher