WIRTSCHAFTSKAMMER VORARLBERG

DATENSCHUTZ GRUNDVERORDNUNG (DSGVO)

MUSTERFORMULAR

der Wirtschaftskammer Vorarlberg

Datenschutz Grundverordnung (DSGVO)
Erforderliche Dokumente mit Mustern

Ausfüll-Anleitung

Diese Sammlung enthält eine Anleitung mit Ausfüllvorschlägen speziell für kleinere Unternehmen, um in wenigen Schritten die Verpflichtungen gemäß DSGVO umzusetzen. Je nach Komplexität des Unternehmens sind teilweise weit umfangreichere Dokumentationen erforderlich; Betreiber von Webshops z.B. sollten sich unbedingt mit dem Hersteller der Applikation sowie ihrem Provider abstimmen.

Im Folgenden sind Kommentare und Vorschläge zum korrekten Ausfüllen der Mustervorlage, die Sie weiter individualisieren können, rot markiert. Bitte ergänzen Sie das Dokument um Ihre spezifischen Angaben und löschen Sie nicht benötigte Passagen, bzw. stellen Sie die Schrift der verwendeten Passagen in Ihrem fertigen Dokument auf schwarz um!

Ein Vertrag für Auftragsverarbeiter ist in dieser Dokumentation bewusst nicht enthalten - Ihr jeweiliger Auftragsverarbeiter, z.B. Steuerberater, sollte einen individuell angepassten Vertrag für Sie haben.

Sofern Sie höhere Anforderungen erfüllen müssen (z.B. Datenschutzbeauftragter, Folgeabschätzung, etc.), finden Sie alle verfügbaren Informationen auf unserer Homepage www.wko.at

Datenverarbeitungsverzeichnis nach Art 30 Abs 1 EU-Datenschutz-Grundverordnung (DSGVO) (Verantwortlicher)

INHALT

A. Stammdatenblatt

Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen

Das kann der Firmeninhaber sein; bei kleineren Unternehmen ist das meist sinnvoll.

a. Name(n) und Anschrift(en):

b. E-Mail-Adresse(n): (allenfalls weitere Kontaktdaten wie zB Tel.Nr.):

Wenn die Kerntätigkeit in einer regelmäßigen und systematischen Überwachung der Person, deren Daten verarbeitet werden besteht, ist die Bestellung eines Datenschutzbeauftragten verpflichtend. → **In der Regel wird ein kleineres Unternehmen daher keinen Datenschutzbeauftragten brauchen.**

c. Name und Kontaktdaten des Datenschutzbeauftragten:

Wenn der Verantwortliche nicht in der EU niedergelassen ist, ist ein Vertreter zu bestellen.

d. Name und Kontaktdaten des Vertreters des (der) Verantwortlichen:

Die Punkte c und d können daher in den meisten Fällen entfallen. Von der Bestellung eines Datenschutzbeauftragten ohne rechtliche Verpflichtung oder sachlichem Grund raten wir ab.

B. Datenverarbeitungen/Datenverarbeitungszwecke

- Beschreibung und Zweck der Datenverarbeitung

  - Geschäftsführung und Rechnungswesen:
    Buchhaltung bzw. Einnahmen Ausgaben Rechnung, Kostenrechnung, Verwaltung von Bankdaten, Registrierkassenpflicht, Steuerpflicht, Ein-/Ausgangsrechnungen, Lagerverwaltung, Offerte, Aufträge und Bestellungen, Reklamationen bzw. Gewährleistung, Garantie, Versicherungen, Leasing- und Mietverträge (Versicherungsagenten: Schadensabwicklung, KFZ An-/Abmeldung, …)

  - Personalverwaltung:
    Verwaltung aufrechter Dienstverhältnisse, Dienstverträge, Stellenausschreibungen, Bewerbungen, Personalverrechnung inkl. Pfändungen, Gehaltszahlungen, Gehaltsmeldung an das Finanzamt, Zeiterfassung, Zutrittssysteme (Gebäude, EDV), Krankmeldungen, An-/Abmeldung bei der GKK, AMS, …

  - Marketing:
    Werbung, Newsletter, Kundenbindungsprogramme, Veranstaltungen …

  - Videoüberwachung:
    Schutz des Eigentums und der Mitarbeiter

- Wurde eine Datenschutz-Folgenabschätzung durchgeführt?

Wenn Sie keine sensiblen personenbezogenen Daten (Gesundheitsdaten, genetische Daten, sexuelle Orientierung, politische, weltanschauliche oder religiöse Weltanschauungen, Gewerkschaftszugehörigkeit, …) umfangreich verarbeiten und die Datenverarbeitung nicht zum Zweck von Profiling erfolgt, ist eine Folgeabschätzung in aller Regel nicht erforderlich.

Ja ☐ Wann? _____

Nein ☐ Es besteht voraussichtlich kein hohes Risiko für die Rechte der Betroffenen.

C. Detailangaben zur Datenverarbeitung

1. Kategorien der betroffenen Personen

   - Mitarbeiter und Bewerber
   - Geschäftspartner
   - Kunden und Interessenten

2. Rechtsgrundlagen

   - Mitarbeiter: Vertragserfüllung, rechtliche Verpflichtung
   - Bewerber: berechtigtes Interesse, Vertragserfüllung
   - Geschäftspartner: Vertragserfüllung, rechtliche Verpflichtung, berechtigtes Interesse
   - Kundendaten: Vertragserfüllung, berechtigtes Interesse
   - Interessenten: Vertragserfüllung, berechtigtes Interesse
   - Videoüberwachung: berechtigtes Interesse (Schutz)

3. Verträge , Zustimmungserklärungen oder sonstige Unterlagen (empfohlen)

   - Einverständniserklärungen
   - Datenschutzerklärung nach § 13 u. § 14 DSGVO
   - Datenschutzerklärung Homepage
   - Verträge mit Auftragsverarbeitern (Steuerberater, Buchhalter, Cloud, …)

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen

   a. Kategorien der verarbeiteten Daten und ankreuzen, ob sie an Empfänger übermittelt werden sowie Aufbewahrungs- und Löschungsfristen

Erklärung zur folgenden Tabelle:

- Detaillierte Angaben zu den einzelnen Kategorien der betroffenen Personen finden Sie in den Fußnoten zum Verzeichnis.

- Den Ausfüllvorschlag bitte prüfen und allenfalls ergänzen bzw. nicht Zutreffendes streichen (z.B. die Markierungen unter der Empfängerkategorie Cloud, wenn Sie keine Cloud Lösung verwenden, etc.)

Kategorien der betroffenen Personen-gruppe aus Punkt 1 des C-Blattes	Datenkategorien	Verwaltungs- und Finanzbehörden	Gerichte	Vorsorge- und Krankenkassen	AMS	Wirtschaftsprüfer und Steuerberater, Buchhalter	Rechtsvertreter	Banken/Leasing	Inkassounternehmen	Versicherungen	Cloud	Geschäftspartner in der Auftragsausführung	Konzern	Löschungs- und Aufbewahrungs-fristen (wenn möglich) Jahre
Mitarbeiter	Kommunikationsdaten[1]	X	X	X	X	X	X	X		X	X		X	7
	Personaldaten[2,7]	X	X	X	X	X	X	X		X	X		X	7
	Zahlungs-/Bankdaten[4]	X	X	X		X	X	X		X	X		X	*7*
	Bewerberdaten[3]				X		X				X		X	*3*
Geschäftspartner	Kommunikationsdaten[1]	X	**X**			X	X	X	X	X	X	X	X	7
	Vertragsdaten[5]	X	X			X	X	X	X	X	X	X	X	7/30
	Zahlungs-/Bankdaten[4]	X	X			X	X	X	X	X	X	X	X	7
	Korrespondenz[6]	X	X			X	X			X	X	X	X	7/30
	Registerauszüge		X				X			X	X	X	X	7/30
Kunden	Kommunikationsdaten[1]	X	X			X	X	X	X	X	X	X	X	7
	Sensible Daten[7]		X	X			X			X	X	X	X	7/30
	Vertragsdaten[5]	X	X	X		X	X	X	X	X	X	X	X	7/30
	Zahlungs-/Bankdaten[4]	X	X	X		X	X	X	X	X	X	X	X	7
	Korrespondenz[6]	X	X			X	X			X	X	X	X	7/30
	Nutzerdaten für Onlinedienste[8]		X				X				X		X	7

[1]Kommunikationsdaten:

Wohnanschrift, Telefon, Fax, Mobiltelefon, E-Mail-Adresse, Notfallkontakt (Mitarbeiter);
Stellvertretung bzw. Ansprechpartner im Geschäftsfall (Geschäftspartner);
andere Ansprechpersonen (Kunden);
andere Lieferanschrift (Geschäftspartner, Kunden)

[2]Personaldaten:

Personenbezogene Daten

Personalnummer; Name u. frühere Namen; Geburtsdatum; Geburtsort; Geschlecht; Personenstand; Kinder und sonstige Familienangehörige, im Zusammenhang mit Leistungen, die in Verbindung mit dem Arbeitsverhältnis des Betroffenen erbracht werden (insb. Namen, Geb. Datum, SV Nummer); Gesetzlicher Vertreter; Staatsbürgerschaft; Bankverbindung;

SV / Organisatorisches

Organisatorische Zuordnung im Betrieb, einschließlich Beginn und Ende; SV Nummer; SV Träger; Krankenscheindaten; Dienstnehmer-SV Daten (Versichertenmeldung: Beitragsgruppe An-Abmeldedatum Zugehörigkeit[Arbeiter, Angestellter], Geringfügigkeit;
Verwandtschaftsverhältnis zum Dienstgeber; Beteiligung am Unternehmen des Dienstgebers, Lehrzeit [1. bis Ende], Nacht-Schwerarbeit[Anfang/Ende],

Entlohnung

Beitragsgrundlage für Malusberechnung Fondsschlüssel für Nebenbeiträge [z.B. Kammerumlage, Wohnbauförderungsbeitrag], Abmeldegrund Kündigungsentschädigung/Ersatzleistung für Urlaubsentgelt [von, bis]; Beitragsgrundlagenmeldung: Beitragszeitraum [von-bis, Monat, Jahr, Verrechnungsart], Allgemeine Beitragsgrundlage, Beitragsgrundlage Sonderzahlung, Anzahl der Tage mit Teilentgelt, Beitragspflichtiges Teilentgelt, Zugehörigkeit [Arbeiter, Angestellter, ..], Anspruch auf Sonderzahlung[ja/nein]; Kennzeichen für Krankheit/Unglücksfall/Arbeitsunfall/Berufskrankheit,, Anspruch in Wochen, Vorbezugstage [Summe, Angabe in Arbeits- oder Kalendertagen], Erstattungszeitraum [Beginn, Ende], Fortgezahltes Bruttoentgelt, Art der Beschäftigung [Arbeiter, Lehrling, Heimarbeiter, Sonstige], Tagesturnus [Anzahl der Tage], Berechnung der Ansprüche nach Kalenderjahr/Arbeitsjahr, Ende des Entgeltsanspruches, Vordienstzeiten [von, bis], Arbeitsfreie Tage; Arbeits- und Entgeltsbestätigung für Krankengeld: Grund der Arbeitseinstellung, Beschäftigungsverhältnis [gelöst bzw. nicht gelöst], Bruttoentgelt im letzten Beitragszeitraum ohne Sonderzahlungen, Bezug [Betrag von bis], Betragssumme, Sonderzahlungsanspruch [ja/nein], Sachbezug [Anzahl der Tage, Text], Entgelt wird bezahlt bis …, EFZ-Anspruch in Wochen, Berechnung der Ansprüche nach Arbeits- bzw. Kalenderjahr, Arbeits- Kalendertage Teilentgelt - %Anteil des Gesamtentgelts [% von-bis], Provision während der Arbeitsunfähigkeit [ja/nein],Anrechnung Vorerkrankungen [von, bis]; Arbeits- und Entgeltsbestätigung für Wochengeld: Grund der Arbeitseinstellung, Beschäftigungsverhältnis [gelöst, nicht gelöst], Urlaub vor Eintritt der Mutterschaft [von, bis], Arbeitsverdienst der letzten drei Kalendermonate [ohne SZ, minus gesetzliche Abzüge], Arbeitsverdienstzeitraum [von, bis], Unterbrechung des Bezuges während der letzten drei Monate [von, bis], Ausmaß der Sonderzahlung [Anzahl Monate, Anzahl Wochen], Anspruch auf Fortbezug des Entgelts [gesetzlich, vertraglich, kein Anspruch], Anspruch auf das halbe Entgelt [bis], Anspruch auf mehr als das halbe Entgelt [bis]; Gesetzliche, kollektivvertragliche, betriebsvereinbarungsmäßige und einzelvertragliche Grundlagen der Entgeltberechnung (Einstufung); Brutto- und Nettogehalt (Daten des Gehaltszettels); Daten der Entgeltsfortzahlung; Abzüge vom Nettogehalt aufgrund Gesetzes oder betrieblicher Vereinbarungen; Sachbezüge; Aufwandsentschädigungen(wie Reisegebühren); Sozialleistungen im Zusammenhang mit dem Arbeitsverhältnis; Höhe des Gewerkschaftsbeitrages und Bezeichnung und Adresse des Empfängers (nach Bekanntgabe des Betroffenen); Versicherungsprämien als Leistung des Arbeitgebers; Verwaltung von Vorschüssen und Darlehen; Lohnpfändungsdaten; Daten des Lohnzettels (L-16 Formular); Alleinverdiener- oder Alleinerzieher-Absetzbetrag (ja, nein); Wohnsitzfinanzamt; Daten zur Pensionskasse (insbesondere Ein- und Austritt, Beitragsdaten und Versicherungszeiten in der gesetzlichen Sozialversicherung im Zeitraum der Beschäftigung); Daten zur Verwendung von Dienstfahrzeugen (insbesondere Führerschein, Abrechnungen, Schadensfälle, Versicherungen); Besondere Qualifikationen (z.B. Gewerbeschein, Ausbildung, ..); Nebenbeschäftigungen; Daten nach dem Berufsausbildungsgesetz, BGBl. Nr. 142/1969 idgF., und einschlägigen kollektivvertraglichen Regelungen bei Lehrlingen, insbesondere Lehrvertragsdaten und sonstige Daten aus dem Ausbildungsverhältnis und Berufsschulbesuch; Schwerarbeiterzeiten.

Mitarbeitervorsorge
Mitarbeitervorsorge gem. BMSVG: MVK-Leitzahl, MV-Beitragsgrundlage [inkl. Sonderzahlungen], Beitragshöhe gem. BMSVG [Gruppensumme], Beginn und Ende der MV-Beitragszahlung [Stichtag], Eingezahlter Betrag an MV, MV-Beitragszeiten [Beitragsmonat von bis], Vordienstzeiten [bei Übertritt ins neue Abfertigungsmodell], Übertragungsbetrag an die MVK und Zahlungsmodus, Zuordnung zu Dienstgeberkontonummer, Abmeldegründe [z.B. Unterbrechung der Beitragszahlung durch Karenz]); Eintrittsdatum; Vordienstzeiten; Austrittsdatum, Kündigungsfrist; Art der Beendigung des Dienstverhältnisses;

Gesetzliche Beschäftigungsvoraussetzungen
Daten der Beschäftigungsbewilligung; Bezeichnung der Tätigkeit; Gruppenzugehörigkeit (Arbeiter, Angestellter); Kammerzugehörigkeit; Sicherheitsstufe/Zugangs- u. Zugriffsrechte; Lichtbild (für Ausweiskarte);

Arbeitszeiterfassung
Sonstige Daten zur Arbeitszeit (insbes. Geringfügigkeit, Arbeitsstunden, Überstunden, Gleitzeit, Nacht- u. Teilzeitarbeit); Daten zur Urlaubsverwaltung; Religionsbekenntnis nach Angaben des Betroffenen (zur Abwesenheitsverwaltung);

Arbeitsverhinderung
Krankenstand, einschließlich Arbeitsunfall und Berufskrankheit (Beginn, Ende u. Dauer); Zeitpunkt des Arbeitsunfalls; Kuraufenthalte; Mutterschutz (Beginn und Ende); Karenz gem. MSchG und VKG (Beginn und Ende); Präsenzdienst, Ausbildungsdienst oder Zivildienst (Beginn und Ende); Art und Dauer der sonstigen Abwesenheit wegen Dienstverhinderung oder Dienstfreistellung (einschließlich vereinbarte Karenzierung); Daten zur Entgeltfortzahlung; Beschäftigungsrelevante Daten gem. ArbeitnehmerInnenschutzgesetz, BGBl Nr. 450/1994 idgF., Tuberkulosegesetz BGBl. Nr. 127/1968 idgF. und ähnlichen Rechtsvorschriften; Grad der Behinderung gem. Behinderteneinstellungsgesetz (nach Bekanntgabe des Betroffenen);

[3]Bewerberdaten (vom Betroffenen angegeben bzw. zur Verfügung gestellt):
Name; Geburtsdatum; Staatsbürgerschaft; Geschlecht; Anschrift; Telefonnummer; E-Mail Adresse; Lichtbild; Ausbildungsdaten; Lebenslauf und Berufserfahrung; Angestrebte Beschäftigung; Beginn der angestrebten Beschäftigung; Ausbildungen; Sprachkenntnisse; Spezielle Berufserfordernisse, Testergebnisse; Dienstzeugnisse;

[4]Zahlungs- und Bankdaten:
Name, Anschrift, Bankinstitut, IBAN, BIC, UID Nummer, Rechnungsnummer, Verwendungszweck, Zahlungsreferenz

[5]Vertragsdaten:
Personendaten Auftraggeber; Angebot zur Offertlegung; Offerte; Angebote; Bestellungen; Reservierungen; Auftragserteilung bzw. -annahme; Zahlungsmodalitäten (Anzahlung, Akontozahlungen auf Teilleistung, Zahlungen auf Treuhandkonto, Abschlusszahlung, Ratenzahlung, Terminverlust); Rechnungen; Ausschreibungen; Leistungsbeschreibungen; Garantiezusagen; Terminplanung; Pläne zur Ausführung; Produktkonfiguration; Gutachten; Vertragliche Vorleistungen; Dokumentation der (vor)vertraglichen Aufklärungs- und Sorgfaltspflichten; Behördenbescheide; Vereinbarung zu Erfüllungsort und Erfüllungszeit; Austausch von notwendigen Kundendaten zwischen Vertragspartner und Subunternehmer; Gutscheine; Gutschriften; Daten zu Gewährleistung, Garantie bzw. Wandlung, Schadenersatzforderungen; Rücktritt vom Vertrag nach KSchG.; Rücktrittserklärungen; Auftrag Subunternehmer; Vertrag über Liefermengen und Konditionen; Treuhandvereinbarungen; Vereinbarungen zugunsten Dritter; Vertragskündigung; Vertragsauflösung aus anderen Gründen; Allgemeine Vertrags-bedingungen; Zusatzvereinbarungen und Vertragsänderungen; Konventionalstrafen und Pönalen; Folgen des Verzuges; Ursachen für Verzug; Urheberrecht; Muster und Patente; Daten zu Schäden; Dokumentation zur Schadensabwicklung; Zertifikate; Dokumente über die Einhaltung gesetzlicher Verpflichtungen; Daten zur durchgeführten Qualitätskontrolle; Schadensmeldungen, Dokumentation Schadensbehebung, Reparaturauftrag, Reparaturprotokoll; Leistungsausweis; Übernahmebestätigung; Transportdokumentation, Kontaktdaten des Bewohners, Mieters bzw. dessen Angehörigen

[6]Korrespondenz (schriftlich und per E-Mail):

Fragen zu Produkten oder Leistungen bzw. Anfragebeantwortung; Versandbestätigungen; Reklamationen; Terminvereinbarungen; Verständigung zum Liefertermin; Änderung vom Lieferort; Beratung zur Produktauswahl; Zusendung von angefragtem Prospektmaterial; ..

[7]Sensible Kundendaten:

Arztbefunde; Krankengeschichte; Behandlungsdaten; Daten zur sexuellen Orientierung; Verschreibungen (z.B. medizintechnische Geräte);

[8]Nutzerdaten Onlinedienste:

Einverständniserklärungen für Newsletter zu div. Angeboten; Kundenlogin; Bestellübersicht für Kunden; Übersicht über Rücksendungen; Kunden Bonifikationssysteme; Transportverfolgung für Waren im Versand; ..

5. Kategorien von Empfängern in Drittstaaten oder Internationale Organisationen, an die personenbezogene Daten offengelegt werden (Auftragsverarbeiter und Dritte).

Empfängerkategorien (aus 4.a.)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU des EWR)	Internationale Organisation (Angabe der intern. Organisation)
Öffentliche Einrichtungen		
Auftragsverarbeiter		
Geschäftspartner		

Eine Angemessenheit ist derzeit nur anerkannt für folgende
→ EWR Staaten: Liechtenstein, Norwegen, Island
→ Drittstaaten: Andorra, Argentinien, Färöer Inseln, Guernsey, Insles Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay sowie, unter der Bedingung des Privacy Shield, für die USA.

D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

a) Vertraulichkeit

Zutrittskontrolle:
Schutz vor unbefugtem Zutritt zu Räumen mit Anlagen der Datenverarbeitung, z.B. abgesperrte Tür mit Schlüssel, Magnetkarte, Zutrittscode, zum Öffnen, Alarmanlagen, Videoüberwachung, etc.

Zugangskontrolle:
Schutz vor unbefugter Systembenutzung (z.B. Kennwörter, Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Datenverschlüsselung, etc.

Zugriffskontrolle:
Schutz vor unbefugtem Lesen, Kopieren, Ändern oder Entfernen von Daten, USB-Block, Zugriffsprotokoll, Berechtigungsstufen für Datenzugriff, etc.

b) Integrität

Weitergabe von Daten:
kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei Datenübertragung und -transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), Digitale Signatur, etc.

Dateneingabe:
Dokumentation, ob und von wem personenbezogene Daten in das Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind, z.B. über ein Datenprotokoll

c) Verfügbarkeit und Belastbarkeit

Schutz gegen zufällige oder mutwillige Zerstörung bzw. gegen Verlust von Daten; Backups, Virenschutz, Firewall, etc.

d) Pseudonymisierung und Verschlüsselung

Bei sensiblen Daten, soweit für die jeweilige Datenverarbeitung möglich, Trennung der primären Identifikationsmerkmale von den restlichen Daten und getrennte Speicherung

Es werden folgende Verschlüsselungstechnologien eingesetzt: [AUFZÄHLUNG]

e) Evaluierungsmaßnahmen

Datenschutz-Management, z.B. durch beauftragtes IT-Unternehmen, regelmäßige Mitarbeiterschulungen, Policy

Bildaufnahmen (Videoüberwachung)

Teil 1	JA	NEIN
Schütze ich Personen oder Sachen auf meiner privaten Liegenschaft?	X	
Schütze ich Personen oder Sachen an öffentlichen zugänglichen Orten, die unter meinem Hausrecht liegen? (zB Geschäftslokal)	X	
Habe ich ein privates Dokumentationsinteresse, und erfasse Personen so, dass sie nicht identifizierbar sind, bzw. Objekte keiner Person zugeordnet werden können?		X

Teil 2		
Die Bildaufnahme dient für:	JA	NEIN
Die Überwachung des höchstpersönlichen Lebensbereichs einer betroffenen Person (z.B. Garderobe), ohne deren Einwilligung (unzulässig!)		X
Die Überwachung der Mitarbeiter (unzulässig!)		X
Den automatischen Abgleich der gewonnenen mit anderen Daten (unzulässig!)		X
Zur Auswertung, um die Personen in Kategorien einteilen zu können (unzulässig!)		X

Kann in Teil 1 mindestens eine Frage mit JA beantwortet werden, **UND** lauten in Teil 2 alle Antworten NEIN, ist eine Bildaufnahme im privaten Raum zulässig.

Auf Grund der oben angeführten Antworten ist eine Bildaufnahme zulässig.

Maßnahmen, die für eine zulässige Bildaufnahme getroffen werden müssen (§ 13 DSG):

- Der Verantwortliche muss die Bildaufnahmen vor einer Änderung schützen!
- Jeder Bildverarbeitungsvorgang – außer bei Echtzeitüberwachungen – muss protokolliert werden.
- Gibt es keinen Zweck mehr die Bildaufnahmen aufzubewahren, sind sie zu löschen. Eine länger als 72 Stunden andauernde Aufbewahrung muss verhältnismäßig sein und ist gesondert zu protokollieren und zu begründen. (§ 13 Abs 3 DSG) →
  Empfehlung: automatisches Überschreiben der Daten spätestens nach 72 Stunden!
- **Aushang**, dass der Bereich videoüberwacht wird und Grund (z.B.: „Dieses Geschäft ist durch Videoüberwachung gegen Übergriffe geschützt.“)
- Name u. Kontakt des Verantwortlichen (u. allenfalls des Datenschutzbeauftragten)

Wichtig: wenn Arbeitnehmer von der Videoüberwachung mit betroffen sind, ist eine Dienstvereinbarung darüber erforderlich!
Weitere Infos finde Sie hier: Servicedokument Videoüberwachung

Datenschutzerklärung nach Art. 13 und 14 DSGVO

Firmennamen
Kontaktdaten des Verantwortlichen

- Wir verarbeiten Ihre personenbezogenen Daten, die unter folgende Datenkategorien fallen:

Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltdaten, …

☐ **Einwilligung:** Sie haben uns Daten über sich freiwillig zur Verfügung gestellt und wir verarbeiten diese Daten auf Grundlage Ihrer Einwilligung zu folgenden Zwecken:

Information über unsere Produkte, Werbung, Newsletter, Veranstaltungen, Firmenbeiträge auf Social Media, …

Sie können diese Einwilligung jederzeit widerrufen. Ein Widerruf hat zur Folge, dass wir Ihre Daten ab diesem Zeitpunkt zu oben genannten Zwecken nicht mehr verarbeiten.

☐ **Vertrag:** Die von Ihnen bereitgestellten Daten sind zur Vertragserfüllung bzw. zur Durchführung vorvertraglicher Maßnahmen erforderlich.

Das sind: Die Erstellung von Offerten, die Abwicklung von Aufträgen und Bestellungen, die Zustellung der Waren, die Bearbeitung von Reklamationen, Abwicklung von Gewährleistung oder Garantie, Schadensabwicklung, KFZ An- und Abmeldung, Kennzeichen-hinterlegung, Wahrung Ihrer rechtlichen Interessen gegenüber Dritten.

Ohne diese Daten können wir den Vertrag mit Ihnen nicht erfüllen.

☐ **Gesetzliche Verpflichtung:** Wir müssen Daten, die wir von Ihnen erhalten haben, aufgrund einer gesetzlichen Verpflichtung verarbeiten.

Das sind Steuer- und Abgaberechtliche Vorschriften, Arbeits- und Sozialrechtliche Vorschriften, Zollvorschriften (U34), etc., um die gesetzlich erforderlichen Nachweise zu erbringen.

☐ **Berechtigtes Interesse:** Wir verarbeiten Daten über Sie aufgrund unserer berechtigten Interessen oder denen eines Dritten.

Dieses besteht in der Anbahnung von Geschäftsabschlüssen, in der Durchführung Dokumentation der Geschäftsfälle, der Information über von uns angebotene Produkte und Dienstleistungen, Veranstaltungen, Aktionen etc. Zu diesem Zweck können auch Daten auch an Dritte übermittelt werden, falls dies für die Durchführung der erwähnten oder anderer Marketingmaßnahmen, statistische Auswertungen etc. erforderlich ist bzw. für die interne Verwaltung im Konzern.

- Wir speichern Ihre Daten für die Dauer der Geschäftsbeziehung und darüber hinaus im Rahmen der jeweils zur Anwendung gelangenden gesetzlichen Aufbewahrungs- und Dokumentationspflichten.

- Für die Datenverarbeitung ziehen wir fallweise Auftragsverarbeiter heran. Wir geben Ihre Daten auch an folgende Empfänger bzw. Empfängerkategorien weiter:

  Steuerberater, Banken, Subunternehmer, Lieferanten, Konzern, ..

- Da wir Daten in unseren berechtigten Interessen verarbeiten, haben Sie für diese grundsätzlich ein Widerspruchsrecht, wenn Gründe vorliegen, die sich aus Ihrer besonderen Situation ergeben und die gegen diese Verarbeitung sprechen.

- Da wir die Daten (auch) für Direktwerbung verarbeiten, können Sie gegen diese Verarbeitung für Zwecke der Direktwerbung jederzeit Widerspruch erheben

- Ihnen stehen grundsätzlich die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch zu. Dafür wenden Sie sich an unseren Verantwortlichen.

- Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, wenden Sie sich bitte an unseren Verantwortlichen. Sofern eine Klärung nicht möglich sein sollte, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist die Datenschutzbehörde zuständig.

Achtung: Die Datenschutzerklärung nach Art. 13 u. 14 DSGVO ersetzt nicht die Datenschutzerklärung für eine Homepage!

Einwilligungserklärung

Name: _____

Adresse: _____

Telefonnummer: _____

E-Mail-Adresse: _____

Ich stimme zu, dass meine folgenden persönlichen Daten von

Firmenname samt Adresse und eMail

zu folgendem Zweck gespeichert und verarbeitet werden:

☐ Kontaktaufnahme und Vereinbarung von Terminen

☐ Zusendung von Werbung (Aktionen, Produktneuigkeiten, Newsletter, …)

☐ Veröffentlichung von Bildern, die bei Firmenveranstaltungen aufgenommen wurden, z.B. auf social media

Diese Einwilligungserklärung kann jederzeit von mir widerrufen werden.
Informationen zum Datenschutz finden Sie auf der Website www.muster.at.

Bei Kindern unter 14 Jahren ist eine Zustimmung des Erziehungsberechtigten notwendig.

_____ _____

Datum Unterschrift

Eine Einwilligungserklärung ist nicht erforderlich:

- wenn sich die Verarbeitung auf personenbezogene Daten (auch sensible) bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.
- bei nicht sensiblen Daten, die aufgrund eines (Vor-)Vertrages oder einer rechtlichen Verpflichtung (z.B. Arbeitsrecht) verarbeitet werden.
- bei „sensiblen Daten“, wenn die Verarbeitung aus Gründen des Arbeitsrechts oder des Sozialrechts, einschließlich der Kollektivverträge und Betriebsvereinbarungen erforderlich ist.

Allgemeine Datenschutzrichtlinie im Unternehmen (für Mitarbeiter)

Unser Unternehmen benötigt Informationen über Kunden, Lieferanten und Mitarbeiter. Aufgrund der DSGVO dürfen nur noch notwendige Daten erfasst und verarbeitet werden (Datenminimierung). Diese Richtlinie legt unsere Mindeststandards für die Verarbeitung von personenbezogenen und vertraulichen Daten fest.

Personenbezogenen Daten sind all jene Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Das ist der Fall, sobald eine Person direkt oder indirekt, durch Zuordnung von speziellen Merkmalen (Name, Kennnummer, Bankdaten, Geburtsdatum, Adresse, etc.), identifiziert werden kann.

Eine besondere Kategorie von personenbezogenen Daten sind die sensiblen Daten. Das sind all jene Informationen, aus denen die rassische und ethnische Herkunft, die politische Meinung, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, Gesundheitsdaten oder sexuelle Orientierung hervorgehen.

Es ist, bei einem angemessenen Verhältnis zwischen Aufwand und Schutzzweck, zu gewährleisten, dass

- ausschließlich befugte Mitarbeiter/innen Zugriff auf diese Daten erlangen
- Daten jederzeit ihrem Ursprung zuordenbar sind
- Festgehalten wird, wer wann welche Daten verwendet und verarbeitet hat
- Daten vollständig und aktuell gehalten werden

Folgende Punkte müssen ausnahmslos eingehalten werden:

- Alle Arbeitsplätze sind so zu sichern, dass Unbefugte keinerlei Einblick in oder Zugriff auf personenbezogene Daten erlangen können.
- Monitore und Drucker sind so aufzustellen, das Dritte keine Einsicht nehmen können.
- Ausdrucke mit sensiblen Daten sind dem Drucker sofort zu entnehmen.
- Werden schriftliche Unterlagen nicht mehr benötigt, sind diese so zu vernichten, dass ihr Inhalt nicht mehr lesbar ist (z.B. durch einen Aktenvernichter).
- Mobile Datenträger sind vor dem Zugriff von Dritten zu sichern.
- Datenträger die nicht mehr benötigt werden sind unwiderruflich zu löschen.
- Sensible Daten dürfen unter keinen Umständen Unbefugten weitergegeben werden.
- Alle Mitarbeiter mit Zugang zu sensiblen Daten sind zur Verschwiegenheit verpflichtet.
- Auskunftsersuchen/Datenschutzanfragen sind ausnahmslos schriftlich abzuwickeln.
- Sensible Daten dürfen nur vertraulich übermittelt werden (Verschlüsselung, VPN).
- Zu sensiblen Daten haben ausschließlich befugte Personen Zugang.

Diese Richtlinie gilt für alle IT-Systeme und Anwendungen (analog u. digital). Sie wurde mir erläutert und in Kopie überlassen.

_____ _____

Datum Unterschrift

Dienstanweisung zur Verarbeitung von Daten besonderer Kategorien
(z.B. für Mitarbeiter in der Personalverwaltung)

Im Rahmen Ihrer Tätigkeit im Unternehmen xxx sind Sie mit der Verarbeitung besonderer Kategorien von Daten (sensibler Daten) nach der Datenschutzgrundverordnung (Art. 9) betraut.

Im Detail sind dies folgende Daten:

Beispiel: Krankenstandsdaten von MitarbeiterInnen
Beispiel: Gesundheitsdaten von Kunden
Beispiel: Religionsbekenntnis von Kunden

Zusätzlich zur Einhaltung der allgemeinen Datenschutzrichtlinie im Unternehmen haben Sie bei der Verarbeitung dieser Daten folgende vom Unternehmen definierte Vorschriften einzuhalten:

Beispiel: beim Verlassen des Büros die Türe zu versperren
Beispiel: jeden Abend die Kästen im Büro zu versperrern
Beispiel: keine Unterlagen in den Müll, alles ist zu schreddern

Diese Richtlinie wurde mir erläutert und ich habe sie in Kopie erhalten.

_____ _____

Datum Unterschrift

Richtlinie für den Umgang mit mobilen Datenträgern / Privatgeräten
(für Mitarbeiter)

Notebooks

- Sperre mit Kennwort (nicht offen einsehbar ablegen, alle drei Monate ändern).
- Verschlüsselung der Festplatte, wenn sensible Daten darauf gespeichert werden.
- Das Gerät niemals entsperrt an Dritte weitergeben.
- Das Gerät stets sicher verwahren (z.B. nicht unbeaufsichtigt im geparkten Auto).
- Unternehmensfremde Datenträger oder Geräte dürfen nicht angeschlossen werden.
- Das Betriebssystem muss regelmäßig aktualisiert werden.
- Fremde Software darf nur nach Zustimmung installiert werden.
- Bei Verdacht auf Virenbefall, Datenspionage oder andere sicherheitsgefährdende Umstände ist unverzüglich eine Meldung zu erstatten.

Smartphones

- Sperre mit PIN oder Kennwort (nicht offen einsehbar ablegen, alle drei Monate das Passwort ändern).
- Das Gerät niemals entsperrt an Dritte weitergeben.
- Das Gerät stets sicher verwahren (z.B. nicht im geparkten Auto).
- Nicht benötigte Funktionen deaktivieren (z.B. Bluetooth, WIFI, etc.).
- Das Gerät nicht über USB-Anschluss an unbekannte Quellen anschließen.
- Das System regelmäßig aktualisieren.
- Überprüfung der Berechtigung, die eine App bei Installation verlangt.
- Die Verwendung eines Jailbreak oder Rooting ist verboten.
- Keinerlei Daten in Cloud-Diensten speichern.
- Keine fremde Apps installieren.
- Bei Verdacht auf Virenbefall, Datenspionage etc. unverzüglich Meldung erstatten.

Das Senden von Daten des Unternehmens an eine private E-Mail-Adresse oder die Mitnahme Daten auf mobilen Datenträgern oder Cloud-Diensten für den privaten Gebrauch ist verboten!

Wird das mobile Gerät (Notebook, Smartphone, Datenstick,..) verloren oder gestohlen, ist dies unverzüglich der Geschäftsführung/dem Datenschutzmanager zu melden, da ein möglicher Data-Breach innerhalb von 72 Stunden an die Datenschutz Behörde gemeldet werden muss.

Hiermit bestätige ich, die Richtlinien zum Thema Umgang mit Datenträgern/Privatgeräten gelesen zu haben und einzuhalten. Eine Kopie der Richtlinie wurde mir ausgehändigt.

_____ _____

Datum vollständiger Name + Unterschrift

Datenschutzanfragen

Personen deren Daten verarbeitet werden, haben im Zuge der DSGVO sieben Betroffenenrechte:

1. Widerspruchsrecht (Sie können eine Zustimmung zur Verarbeitung widerrufen)
2. Recht auf Datenübertragbarkeit (es müssen aber ausschließlich jene Daten an einen Dritten übertragen werden, die vom Kunden zur Verfügung gestellt wurden)
3. Recht auf Einschränkung der Verarbeitung
4. Recht auf Löschung („Recht auf Vergessenwerden“)
5. Recht auf Berichtigung
6. Auskunftsrecht
7. Informationspflicht bei Erhebung von sensiblen Daten

Vorgehensweise bei einer Anfrage:

- Anfragen müssen aus Dokumentationszwecken schriftlich gestellt werden
- Prüfung der Identität des Betroffenen
- Erhebung, ob und welche Daten verarbeitet werden (analog u. digital)
- Prüfung, ob das Recht auf die Anfrage/Löschung/… besteht
- Prüfung, ob die Anfrage erfüllt werden kann und darf (Aufbewahrungspflichten haben Vorrang, Datenauskünfte dürfen nicht die Rechte Dritter beeinträchtigen)
- Beantwortung der Anfrage ev. unter Beilegung der gespeicherten Daten in Dateiform innerhalb von 1 Monat (2 bei sehr komplexen Anfragen)
- Dokumentation der Anfrage und der Beantwortung (Logbuch)

Wenn eine Person persönlich Auskünfte zum Thema Datenschutz oder die Löschung seiner Daten verlangt, weisen Sie höflich darauf hin, dass nur schriftliche oder per eMail übermittelte Anfragen, jeweils mit beigelegter Ausweiskopie, beantwortet werden können!

Der Datenschutzmanager hat anfragenden Personen alle Informationen und Mitteilungen präzise, transparent, verständlich und in leicht zugänglicher Form sowie in einfacher Sprache mitzuteilen.

Die erteilte Auskunft und alle Mitteilungen und Maßnahmen sind unentgeltlich zur Verfügung zu stellen. Sollte eine Person exzessive und wiederholte Anfragen stellen, darf ein angemessenes Entgelt verlangt werden, beziehungswiese kann auch verweigert werden, tätig zu werden.

Vorgehen bei Datenschutzverletzung
Data Breach Notification
(Art 33 DSGVO)

Meldung an die Aufsichtsbehörde:
Österreichische Datenschutzbehörde,
Wickenburggasse 8-10, 1080 Wien
E-Mail: dsb@dsb.gv.at

1. Name und Kontaktdaten des **Verantwortlichen:**

   e. Name und Anschrift:

   f. E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.):

2. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des **Datenschutzbeauftragten:**

   a. Name und Anschrift:

   b. E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.):

3. Beschreibung der **Art der Verletzung** des Schutzes personenbezogener Daten:

soweit möglich Kategorien und ungefähre Zahl der **betroffenen Personen**:

   a. soweit möglich betroffene Kategorien und ungefähre Zahl der **personenbezogenen Datensätze**:

4. Beschreibung der **wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten:

5. Beschreibung der **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung:

a. ggf **Maßnahmen zur Abmilderung** der Auswirkungen der Verletzung:

6. **Datum und Uhrzeit** des Vorfalls:

Begründung, falls die Meldung länger als 72 h nachdem der Vorfall dem Verantwortlichen bekannt wurde, erfolgte:

Logbuch Datenschutz

Für eine genaue Darstellung aller Änderungen in den Verarbeitungstätigkeiten oder anderen Bereichen sowie der anfallenden Datenschutzanfragen, soll der Verantwortliche für Datenschutz im Unternehmen alle Vorgänge chronologisch aufzeichnen, d.h. ein sog. Logbuch führen. Das elektronische Logbuch dient zur Dokumentation aller Vorfälle, Anfragen und Veränderungen.

Das Logbuch kann formfrei geführt werden und dient zur Organisation und Strukturierung der Maßnahmen zum Datenschutz sowie im Anlassfall zum Nachweis von durchgeführten Maßnahmen gegenüber der Datenschutzbehörde.
Folgende Angaben sollten jedenfalls im Logbuch enthalten sein:

- Datum
- Kategorie (Betroffenen Anfrage, Data Breach, Änderungen in Verarbeitungstätigkeiten, technische organisatorische Maßnahmen, Sonstiges)
- Die getroffenen Maßnahmen bzw. Beschreibung deren
- Datum der Erledigung

Datum	Kategorie	Beschreibung	erledigt
10.9.18	*Anfrage*	*Muster: Anfrage von Herrn X beteffend Auskunft, Anfrage nach Vorgehensmodell bearbeitet, Auskunft erteilt, Dokumentation abgelegt unter …*	15.9.18
25.10.18	*TOMs*	*Muster: Fertigstellung Einführung neues Berechtigungskonzept für RW-Applikation, Dokumentation abgelegt unter …*	25.10.18
28.10.18	*Data-Breach*	*Muster: Handyverlust Geschäftsführer, Evaluierung welche Daten darauf waren, keine Geschäftsdaten, Ergebnis: Kein Risiko, Dokumentation abgelegt unter*	29.10.18

Erstellt: Mag. Julius Moosbrugger, Wirtschaftskammer Vorarlberg