# DSGVO Sicherheitseinweisung
für Mitarbeiter

## 1. Einführung

Der Umgang mit personenbezogenen Daten ist rechtlich besonders geschützt. Mit der am 25. Mai 2018 in Kraft getretenen DSGVO (Datenschutz-Grundverordnung) der Europäischen Union wird dieser Schutz nun nochmals verstärkt und stellt diese zusätzliche Regelungen auf, welche uns in unserem Arbeitsalltag betreffen. Als Ihr Arbeitgeber sind wir daher angehalten Sie zum Thema Datenschutz zu unterweisen. Die Verarbeitung personenbezogener Daten ist insbesondere dann zulässig, wenn die betroffene Person in die Datenverwendung eingewilligt hat (zB „ja, ich möchte einen Newsletter bekommen") oder die Datenverwendung zur Erfüllung eines Vertrages notwendig ist (zB Weitergabe von Kontaktdaten des Kunden an den Montagepartner). Weiters ist Datenverwendung zulässig, wenn sie zur Erfüllung gesetzlicher Pflichten erforderlich ist (zB Weitergabe von Mitarbeiterdaten an die Sozialversicherung zur Anmeldung).

## 2. Was sind personenbezogene Daten und was darf ich damit machen?

Unter personenbezogenen Daten versteht man alle Informationen, die sich auf eine identifizierte/identifizierbare natürliche Person beziehen (z.B. Name, Adresse, Telefonnummer, E-Mail-Adresse, Geschlecht, Bankdaten, etc.). Wir verarbeiten dabei personenbezogene Daten von Mitarbeitern, Kunden, Lieferanten und Partnern – dies passiert in den unterschiedlichen Abteilungen und Bereichen.

**Beim Umgang mit solchen Daten sind insbesondere folgende Grundregeln stets zu beachten:**

- Personenbezogene Daten, die Ihnen aufgrund Ihrer beruflichen Tätigkeit anvertraut werden, sind geheim zu halten.
- Datensätze dürfen nicht fälschlicherweise verändert werden – es muss die Korrektheit gewährleistet sein (sog. Integrität).
- Nach dem Ausscheiden aus dem Beschäftigungsverhältnis dürfen Sie personenbezogene Daten, die Ihnen beruflich zugänglich gemacht wurden, nicht weitergeben oder anderweitig nutzen.

Verstöße gegen den Datenschutz können hohe Geldstrafen für das Unternehmen nach sich ziehen und unter Umständen auch zu arbeitsrechtlichen Konsequenzen führen! Die Einhaltung der Vorschriften des Datenschutzes wird durch die zuständige Behörde durch sog. Datenschutzaudits überprüft!

## 3. Clear-Desk-Policy

Als weitere Grundregel gilt die sog. Clear-Desk-Policy. Dies bedeutet, dass die Mitarbeiter alle vertraulichen Unterlagen bei Abwesenheit sicher zu verwahren bzw. zu verschließen haben, sodass unberechtigte Personen (Besucher, Reinigungspersonal, unbefugte Kollegen, etc.) keinen Zugriff darauf haben.

**Zur Sicherung der Einhaltung der DSGVO sind nachstehende Dienstanweisungen zu befolgen:**

- Computerausdrucke und Kopien mit sensiblen Informationen dürfen nicht für Unbefugte frei zugänglich herumliegen. Diese Dokumente sind sicher zu verwahren bzw. zuverlässig zu vernichten. Achten Sie daher vor allem darauf, dass nach dem Kopieren/Drucken sämtliche Dokumente mitgenommen werden.
- Versperren Sie Schriftstücke oder Datenträger mit vertraulichen Inhalten an einem sicheren Ort (Schreibtisch, versperrbare Kästen, etc.).

- Falls möglich, sperren Sie Ihr Büro bei Nichtanwesenheit ab.
- Falls sich Ihr Arbeitsplatz z.B. in einem einsehbaren Empfangsbereich etc. befindet, so achten Sie stets darauf, dass unbefugte Dritte keine Kenntnis von personenbezogenen Daten erhalten (z.B. Briefe nicht offen herumliegen lassen).
- Achten Sie darauf, dass bei Verlassen von Besprechungsräumen sämtliche sensiblen Informationen (z.B. auf Flipcharts) entfernt oder mitgenommen werden.
- Keine Passwortnotizen am Arbeitsplatz aufbewahren (z.B. Post-it am Bildschirm).
- Sperren Sie den Computer, wenn Sie Ihren Arbeitsplatz für längere Zeit verlassen.
- Richten Sie Ihr Smartphone oder Tablet so ein, dass es nur nach Eingabe einer PIN oder eines Passworts verwendet werden kann.
- Halten Sie Termine mit Lieferanten, Kunden etc. – falls möglich – nicht in Ihrem Büro, sondern in einem Besprechungsraum ab, sodass keine Gefahr besteht, dass unbefugte Dritte Kenntnis personenbezogener Daten erlangen.

Weiterführende Informationen zu diesen Themen finden Sie zudem in den Dokumenten „Verpflichtungserklärung betreffend die Benutzung von Informationstechnologie-Komponenten“ und „Kennwortrichtlinie“, abrufbar jeweils in ELO.

## 4. Richtige Entsorgung von Daten

Computer, Datenträger und Papierdokumente mit vertraulichen oder personenbezogenen Inhalten, die defekt geworden sind oder nicht mehr benötigt werden, müssen auf sichere Art entsorgt werden.

**Befolgen Sie hiezu nachstehende Anweisung:**

- Übergeben Sie nicht mehr benötigte Datenträger (Festplatten, USB-Sticks, Speicherkarten, etc.) den Verantwortlichen Ihrer EDV-Abteilung bzw. Ihrem Vorgesetzten. Diese kümmern sich um eine sichere Entsorgung. Werfen Sie solche Datenträger auf keinen Fall in den Papierkorb!
- Datenträger wie CDs und DVDs können nur „gelöscht“ werden, indem man sie physisch zerstört.
- Entsorgen Sie Papierdokumente mit sensiblen Informationen nicht mit dem Altpapier. Kleinere Mengen können Sie mit einem handelsüblichen Aktenvernichter, größere Mengen über ein Entsorgungsunternehmen vernichten.

## 5. Sicherer Umgang mit Laptops, Handys und Tablets

Beachten Sie hierzu die Dokumente „Verpflichtungserklärung betreffend die Benutzung von Informationstechnologie-Komponenten“ und „Kennwortrichtlinie“, abrufbar jeweils in ELO.

**An dieser Stelle noch 2 wichtige Hinweise:**

- Verlust oder Diebstahl unverzüglich der IT-Abteilung bzw. dem Vorgesetzten melden! Sollten sich auf dem abhanden gekommenen Gerät personenbezogene Daten befinden, so muss dies innerhalb von 72 Stunden der Datenschutzbehörde gemeldet werden! Ansonsten droht dem Unternehmen eine Geldstrafe!

- Kein eigenmächtiges installieren von Apps etc.!

## 6. Wechselmedien richtig verwenden

**Bei der Verwendung von USB-Sticks, externen Festplatten, Speicherkarten, CDs etc. sollten folgende Grundregeln stets beachtet werden:**

- Lassen Sie Wechseldatenträger nie unbeaufsichtigt liegen!
- Setzen Sie Verschlüsselungs- oder Sperrfunktionen ein.
- Jeder Verlust muss sofort gemeldet werden!

## 7. Passwörter richtig auswählen und verwalten

Beachten Sie stets die Vorgaben im Dokument „Kennwortrichtlinie“, abrufbar in ELO.

## 8. Virenverdacht

Im Falle eines etwaigen Virenbefalls unverzüglich die IT-Abteilung bzw. den Vorgesetzten kontaktieren und jegliche weitere Tätigkeiten am befallenen Gerät unterlassen!

## 9. Was passiert bei Datenschutzvorfällen?

Jeder Mitarbeiter muss Fälle von (auch nur möglichen) Verstößen (z.B. unrechtmäßige Übermittlung von personenbezogenen Daten an Dritte, Verlust Handy, …) gegen die internen Datenschutzrichtlinien bzw. die gesetzlichen Vorgaben unverzüglich unter datenschutz@josko.at melden. Dies ist vor allem deshalb wichtig, weil Unternehmen nur 72 Stunden nach Kenntnis eines Vorfalles Zeit haben, um ihrer Meldepflicht bei der Datenschutzbehörde nachzukommen. Wird diese Frist versäumt, so droht bereits deshalb eine Geldstrafe. Bei Verlust oder Diebstahl von IT-Komponenten ist zusätzlich die IT-Abteilung unverzüglich zu verständigen!

## 10. Was mache ich bei Anfragen/Aufforderungen zum Thema Datenschutz?

Wenn Sie eine Anfrage zum Thema Datenschutz erhalten, so dürfen Sie persönlich keine Auskunft geben! Werden Sie z.B. aufgefordert Daten zu löschen, dann weisen Sie darauf hin, dass sie das nicht dürfen. Notieren Sie vielmehr das Anliegen des Betroffenen und leiten Sie die Anfrage per Mail an datenschutz@josko.at.

Die hierfür intern zuständige Person hat Zugriff auf diese E-Mail-Adresse und wird sich um das Anliegen kümmern.

## 11. Wer ist intern mein Ansprechpartner für datenschutzrechtliche Fragen?

Für sämtliche Fragen zum Thema Datenschutz formulieren Sie bitte Ihr Anliegen per E-Mail an datenschutz@josko.at.

### Datengeheimnis nach § 6 DSG

(1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).
(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.
(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.
(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.
(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

### Sicherheit der Verarbeitung nach Art. 32 Abs 4 DSGVO

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

### Verletzung von Geschäfts- oder Betriebsgeheimnissen und Missbrauch anvertrauter Vorlagen nach § 11 UWG

(1) Wer als Bediensteter eines Unternehmens Geschäfts- oder Betriebsgeheimnisse, die ihm vermöge des Dienstverhältnisses anvertraut oder sonst zugänglich geworden sind, während der Geltungsdauer des Dienstverhältnisses unbefugt anderen zu Zwecken des Wettbewerbes mitteilt, ist vom Gericht mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen. (BGBl. Nr. 120/1980, Art. I Z 6)
(2) Die gleiche Strafe trifft den, der Geschäfts- oder Betriebsgeheimnisse, deren Kenntnis er durch eine der im Abs. 1 bezeichneten Mitteilungen oder durch eine gegen das Gesetz oder die guten Sitten verstoßende eigene Handlung erlangt hat, zu Zwecken des Wettbewerbes unbefugt verwertet oder an andere mitteilt.
(3) Die Verfolgung findet nur auf Verlangen des Verletzten statt.