FOCUSON – MMF GmbH, Messendorfgrund 30, A-8042 Graz

Datenschutzrichtlinien für Mitarbeiter

Dieses Dokument dient als Datenschutz-Grundschulung für die Mitarbeiter, die die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vornehmen.

1. Datenschutz-Grundverordnung (DSGVO)

- DSGVO gilt seit dem 25.05.2018;
- Datenschutzrecht wird EU-weit vereinheitlicht;
- Die DSGVO gilt für natürliche und juristische Personen, Körperschaften und sonstige Organisationen jeglicher Größe, die personenbezogene Daten verarbeiten (somit auch für NPO, Behörden und öffentliche Stellen);
- Sanktionen: Geldbußen bis zu EUR 20 Mio. bzw. 4 % des weltweiten Vorjahresumsatzes (je nachdem welcher Betrag höher ist).

2. Was ist Datenschutz?

Der Datenschutz gilt nicht für juristische Personen, betrifft also keine Daten über Firmen oder Gesellschaften.

Es geht um Daten, die sich aus dem persönlichen Lebensbereich einer bestimmten oder bestimmbaren Person zusammentragen lassen.

Datenschutz ist nicht (primär) der „Schutz der Daten“, sondern der Schutz von Personen vor dem Umgang mit ihren Daten

- vor unberechtigter Speicherung,
- vor fremder (unberechtigter) Kenntnisnahme und Verwendung,
- vor unsauberem Umgang mit ihren Daten (Computer, Internet!)

3. Was sind personenbezogene Daten?

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Beispiele:

- **persönliche Verhältnisse betreffend:** Name, Anschrift, Geburtsdatum, Foto, Ausbildung, Beruf, Familienstand, Staatsangehörigkeit, religiöse oder politische Einstellung, Gesundheitsdaten, Urlaubsplanung, Beurteilungen, Vorstrafen
- **sachliche Verhältnisse betreffend:** Einkommen, Kapitalvermögen, Schulden, Eigentum (Haus, Wohnung, Auto etc.)
- **bestimmbare Daten** (erst mit weiteren Informationen kann man auf eine Person rückschließen), zB: Personalnummer, Kfz-Kennzeichen, Kontonummer

4. Was sind sensible personenbezogene Daten?

Rassische und ethnische Herkunft, politische Meinungen, Religion, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, Gesundheitsdaten, sexuelle Orientierung.

Beispiele: Krankengeschichte, Sozialversicherungsnummer, Bestätigung für Religionszugehörigkeit.

Sensible personenbezogene Daten dürfen nur nach schriftlicher Einwilligungserklärung des Betroffenen erhoben und verarbeitet werden.

5. Wann dürfen Daten erhoben, verarbeitet und genutzt werden?

Personenbezogene Daten **dürfen nicht** erhoben, verarbeitet oder genutzt werden.

Ausnahmen:

- bei Erfüllung eines Vertrages
- bei Erfüllung einer rechtlichen Verpflichtung
- wenn eine Einwilligung / Zustimmung erteilt wurde
- wenn es um lebenswichtiges Interesse geht
- wenn es um öffentliches Interesse geht

6. Was sind die Grundregeln des Datenschutzes?

Rechtsgrundlage: Immer, wenn personenbezogene Daten „angefasst“ werden, muss es dafür eine Gesetzesgrundlage oder eine Einwilligung des Betroffenen geben.

Datenerhebung beim Betroffenen: Sofern möglich, sind die Daten direkt beim Betroffenen zu erheben. Andernfalls ist er in der Regel darüber zu informieren („informationelle Selbstbestimmung“).

Auskunftsrechte: Der Betroffene muss jederzeit Kenntnis darüber haben, dass Daten über ihn gespeichert sind (Transparenzgebot), aus diesem Grund darf er Auskunft verlangen.

Zweckbestimmung: Erhobene Daten dürfen ausschließlich für den Zweck verwendet werden, zu dem sie ursprünglich erhoben wurden.

Datensparsamkeit: Beim Beschaffen und beim Umgang mit personenbezogenen Daten sollte das Moto immer lauten: so viel wie nötig und so wenig wie möglich.

Berichtigung: Personenbezogene Daten, die falsch sind, müssen berichtigt werden.

Schutz durch technische und organisatorische Maßnahmen: Daten sind vor Missbrauch zu schützen.

7. Praktizierter Datenschutz im Büroalltag

Büro und Schreibtisch

- Aufgeräumter Schreibtisch
- Alle vertraulichen Unterlagen verschließen
- Keine Passwörter liegen lassen oder irgendwo hinschreiben
- Vertrauliche Ausdrucke sofort am Drucker abholen
- Vermeiden Sie, dass vertrauliche Unterlagen über den Müll oder anderweitig in falsche Hände geraten (Shredder sollte genutzt werden)
- Jeden Abend die Kästen im Büro versperren

PC / Laptop:

- Nur sichere Passwörter auswählen (z.B. mindestens 8 Stellen, mit Sonderzeichen, keine Namen)
- Passwörter regelmäßig wechseln (mindestens alle 90 Tage)
- Bildschirme und PCs sind bei Abwesenheit vom Arbeitsplatz zu sperren (auch bei nur kurzzeitiger Abwesenheit, sofern kein Blickkontakt besteht)
- Laptops auf Reisen sorgfältig sichern
- Daten verschlüsseln (wenn nötig)
- Das Senden von Daten des Unternehmens an eine private E-Mail-Adresse oder die Mitnahme von Daten auf mobilen Datenträgern oder Cloud-Diensten für den privaten Gebrauch ist verboten!

Bei Datenverlust – Was ist zu beachten?

Wird ein mobiles Gerät (Notebook, Smartphone, Datenstick,..) oder Ordner mit personenbezogenen Daten verloren oder gestohlen, oder eine E-Mail an den falschen Empfänger geschickt, ist dies unverzüglich der Geschäftsführung an industrial@focuson.eu zu melden, da eine mögliche Datenpanne innerhalb von 72 Stunden an die Datenschutz Behörde gemeldet werden muss.

8. Datenschutz bei Bewerbungsverfahren

Bewerbungsunterlagen dürfen im Unternehmen nur den Personen zugänglich gemacht werden, die mit der Besetzung der freien Stelle direkt befasst sind. Dabei sind jedoch alle Betroffenen zur Verschwiegenheit verpflichtet. Die Weitergabe muss streng begrenzt sein.

Sollte ein Bewerber zu keiner Stelle im Unternehmen passen, müssen die Bewerbungsunterlagen sofort sowohl aus dem Posteingangsordner als auch aus dem Papierkorb gelöscht werden (wenn auf Papier - mit Shredder vernichten).

Nachdem das Bewerbungsverfahren zu Ende ist müssen die Bewerbungsunterlagen:

- Mit Einwilligungserklärung - bis auf Widerruf (schriftlich per E-Mail oder per Post) aufbewahrt werden (siehe Anhang 1)
- Ohne Einwilligungserklärung - spätestens sechs Monate nach Zugang der Ablehnung gelöscht (aus E-Mail und in Papierform) werden. Falls der Bewerber möchte, dass seine Daten sofort gelöscht werden, muss dies sofort geschehen.

Wenn die Bewerbungsunterlagen an Dritte übermittelt werden müssen, ist eine Einwilligungserklärung des Bewerbers entweder per E-Mail oder schriftlich erforderlich (siehe Anhang 2).

9. Datenschutz bei bestehenden Dienstverhältnissen

Zulässige Verarbeitung von personenbezogenen Daten im Arbeitsverhältnis:

- zur Erfüllung einer gesetzlichen Verpflichtung – zB alle Daten zur Sozialversicherungsmeldung
- nach Einwilligung des Betroffenen – zB Gewerkschaftszugehörigkeit, Religionszugehörigkeit

Was ist zu beachten?

Bei der Einstellung müssen die Arbeitnehmer informiert werden, für welche Zwecke ihre personenbezogenen Daten erhoben werden, wer Datenschutzbeauftragter ist, an welche Empfänger die Daten gehen und welche Rechte die Arbeitnehmer nach der DSGVO haben (siehe Anhang 3).

Dokumente, die personenbezogene Daten enthalten (Krankmeldungen, Urlaubsanträge, Zeiterfassungsbögen, Meldezettel, Bankverbindungen, Kontaktdaten von Leihmitarbeiter), und die per E-Mail geschickt werden, sind sofort aus dem betreffenden Mail-Ordner als auch aus dem Papierkorb zu löschen, nachdem sie zur Weiterverarbeitung an den jeweiligen Mitarbeiter weitergeleitet wurden.

E-Mails, die an die E-Mail-Adresse industrial@focuson.eu übermittelt werden, werden automatisch nach 6 Monaten nach dem Erhalt aus der Gruppe gelöscht. Stellen Sie sicher, dass alle notwendigen, für Ihre Arbeit wichtigen Informationen aus der Gruppe auf dem Firmencomputer gespeichert werden.

Wenn die personenbezogenen Daten von einem bestehenden Mitarbeiter an Dritten übermittelt werden müssen, ist eine Einwilligungserklärung des Mitarbeiters erforderlich (siehe Anhang 4).

Bei Datenanfragen von Dritten (Lohnbescheinigungen für Banken) sowohl persönlich als auch telefonisch, darf die gewünschte Information nur an die betroffene Person übermittelt werden.

10. Datenschutz bei Austritten von Mitarbeitern

Da die Zwecke, für die die personenbezogenen Daten erhoben und verarbeitet wurden, nach dem Austritt nicht mehr aufrecht sind, müssen die bestimmten Daten von den ehemaligen Dienstnehmern sowohl aus dem System als auch in Papierform gelöscht / vernichtet werden.

Zu den Daten, die gelöscht werden müssen, gehören: Kontaktdaten (Telefonnummer, E-Mail-Adresse), Bewerbung und Bewerbungsbogen, Teste, Führerschein, Meldezettel.

Der verantwortliche Mitarbeiter ist dafür zuständig, die obenstehenden Daten aus dem System zu löschen.

Mitarbeiter, die für die Ablage von Personalakten der ausgetretenen Mitarbeiter zuständig sind, sollen die obenstehenden Daten aus dem Papierakt schreddern / schwärzen.

Falls die Kontaktdaten von den ausgetretenen Mitarbeitern für weitere Stellenangebote benötigt werden, muss eine Einwilligungserklärung für die Kontaktaufnahme nach dem Austritt (siehe Anhang 5) vorhanden sein.

Fazit

Alle Mitarbeiter, die mit personenbezogenen Daten zu tun haben, sind letztlich für die Einhaltung der Regeln zum Datenschutz und der Datensicherheit verantwortlich.

Seien Sie sensibel hinsichtlich der Privatsphäre Ihrer Bewerber und Mitarbeiter und beachten Sie die Grundsätze der Datensicherheit.

Für die Rückfragen steht Ihnen _____ gerne zur Verfügung.

Beilagen:

Anhang 1: Einwilligungserklärung zur Datenverarbeitung
Anhang 2: Einwilligung zur persönlichen Datenweitergabe
Anhang 3: Datenschutzerklärung für Mitarbeiter
Anhang 4: Datenschutzrechtliche Einwilligungserklärung zur Kontaktaufnahme nach Austritt des Mitarbeiters

Anhang 5: Erklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen