

# Merkblatt

## DATENSCHUTZ

Lieber Mitarbeiter, liebe Mitarbeiterinnen,

mit der „Verpflichtung zur Einhaltung von datenschutzrechtlichen Anforderungen und der Vertraulichkeit“ erhalten Sie dieses Merkblatt. In diesem möchten wir Sie kurz über wichtige Punkte beim Datenschutz informieren. In unserem Unternehmen legen wir besonderen Wert auf die Vertraulichkeit im Umgang mit schutzbedürftigen Informationen. Hierunter fallen insbesondere personenbezogene Daten, also die zu einem Menschen gehören und unter den Datenschutz fallen.

### **Welche Daten fallen unter den Datenschutz?**

Alle Daten und Angaben, die einer Person zugeordnet werden können, egal ob dies gleich direkt oder erst indirekt möglich ist.

#### Ein Beispiel für direkte Zuordnung

Sie bekommen zur Erfüllung irgendeiner Aufgabe eine Liste von der Personalverwaltung. Auf dieser stehen die Namen und Gehälter der Mitarbeiter. Somit wissen Sie direkt welcher Mitarbeiter welches Gehalt hat.

#### Ein Beispiel für indirekte Zuordnung

Gleiches Beispiel, jedoch möchte die Personalverwaltung diesmal nicht, dass Sie die Gehälter der anderen Mitarbeiter wissen. Deshalb macht sich die Personalverwaltung die Arbeit und vergibt jedem Namen eine Nummer. Im Datenschutz spricht man hier von pseudonymisieren. Sie bekommen jetzt die Liste nur mit den Nummern und den Gehältern. Sie wissen jetzt also nicht mehr welcher Mitarbeiter was verdient. Und trotzdem fällt auch diese Liste in den Datenschutz, da mithilfe der Personalverwaltung der Personenbezogen indirekt da ist und die Pseudonymisierung leicht rückgängig gemacht werden kann.

#### Einige Beispiele für personenbezogene Daten

Adresse, Telefonnummer, Geburtsdatum, Familienstand, Staatsangehörigkeit, Konfession, Beruf, Foto, Arbeitgeber, Einkommen, Vermögen, Urlaubsplanung, Arbeitsverhalten, Arbeitsergebnisse, Zeugnisnoten, Beurteilungen, Krankheiten, Vorstrafen, Steuern, Versicherungen, Personalnummer, Kundennummer, persönliche geschäftliche E-Mail-Adresse, private Anschrift.

### **Welche Daten betreffen nicht den Datenschutz?**

Nicht alles was im Unternehmen unter die Vertraulichkeit oder Geheimhaltung fällt betrifft gleich den Datenschutz. Dies ist zum Beispiel der Fall, wenn Unterlagen oder Zeichnungen keinen Personenbezug haben. Wenn Sie sich nicht sicher sind, gehen Sie im Zweifelsfall davon aus das ein Personenbezug besteht oder Fragen Sie ihren Vorgesetzten.

# Merkblatt

## DATENSCHUTZ

### **Warum müssen Sie die „Verpflichtung zur Einhaltung von datenschutzrechtlichen Anforderungen und der Vertraulichkeit“ unterschreiben und was bedeutet das?**

Unternehmen müssen nachweisen das Mitarbeiter, welche mit personenbezogenen Daten in Berührung kommen, auf die Vertraulichkeit verpflichtet sind. Sie haben vorher vermutlich schon einmal eine ähnliche Erklärung mit der Bezeichnung „Verpflichtung auf das Datengeheimnis nach §5 BDSG“ unterschrieben. Jedoch ändert sich mit der Datenschutz-Grundverordnung auch das Bundesdatenschutzgesetz und der §5 fällt damit weg. Deshalb verpflichten wir alle Mitarbeiter neu. Mit Ihrer Unterschrift bestätigen Sie, dass Sie auf die Einhaltung der datenschutzrechtlichen Anforderungen achten.

### **Das ist jetzt der Rechtstext, aber was können Sie in der Praxis tun um das zu gewährleisten?**

#### Ändern und schwächen Sie keine eingerichteten technischen Schutzmaßnahmen

Diese Maßnahmen werden in der Regel von der IT oder dem Gebäudemanagement eingerichtet.

Beispiele für Änderungen bzw. Schwächung der Schutzmaßnahmen:

- Sie ändern die Sperrzeit des Bildschirmschoners von 5 Minuten auf 30 Minuten, damit Sie das Kennwort nicht so häufig eingeben müssen.
- Sie deaktivieren die PIN in Ihrem Smartphone, damit Sie dieses nicht immer eingeben müssen, wenn sich der Bildschirm sperrt.
- Sie blockieren mit einem Gegenstand eine automatisch schließende Tür mit Knauf, damit diese offen bleibt und Sie nicht immer den Schlüssel verwenden müssen.

#### Missachten Sie keine getroffenen organisatorischen Maßnahmen

Diese Maßnahmen werden in Richtlinien und Arbeitsanweisungen zum Datenschutz- und der IT-Sicherheit definiert und beschrieben.

Beispiele für die Missachtung getroffener Regelungen:

- Das Anschließen von privaten Geräten an USB-Anschlüssen von PCs ist untersagt. Sie laden aber Ihr Smartphone darüber auf oder stecken eine privaten USB-Stick an.
- Alle Papiere mit personenbezogenen Daten sind immer datenschutzgerecht zu vernichten. Sie zerreißen das Papier jedoch nur, anstatt den Aktenvernichter zu nehmen.

#### Führen Sie keine neuen Arbeitsprozesse ein,

ohne der vorherigen Abstimmung und Freigabe des *Datenschutz- und IT-Sicherheitsteams (DIST)*. Wenden Sie sich bitte im ersten Schritt an Ihren Vorgesetzten, wenn Sie einen Arbeitsprozess erstellen beziehungsweise einführen möchten.

Beispiele:

- Sie stellen fest, dass es noch keine Lieferantenbewertung gibt und möchten diesen Arbeitsprozess einführen und dafür eine Excel-Tabelle kreieren.
- Sie möchten in Ihrer Abteilung einen Wandkalender aufhängen und hier die Geburts- und Urlaubstage der Mitarbeiter eintragen.

# Merkblatt

## DATENSCHUTZ

### Änderung Sie keine bestehenden Arbeitsprozesse,

ohne der vorherigen Abstimmung und Freigabe des *Datenschutz- und IT-Sicherheitsteams (DIST)*. Wenden Sie sich bitte im ersten Schritt an Ihren Vorgesetzten, wenn Sie einen Arbeitsprozess ändern möchten.

### Beispiele:

- Sie haben Termineinladungen für Besprechungen bis jetzt immer per E-Mails koordiniert. Jetzt haben Sie aber eine bessere Lösung bei einem Onlinedienst oder in einer App gefunden und möchten nun diese nutzen.
- Es gibt eine organisatorische Anweisung zu einem Arbeitsprozess, den Sie gerade durchführen. Hier stellen Sie fest, dass die Anweisung nicht passt. Deshalb möchten Sie hier eine Änderung.

### Und...

- Achten Sie die Vertraulichkeit bei erhaltenen personenbezogenen Informationen.
- Verarbeiten Sie nur so wenige Daten, wie für den Arbeitsprozess notwendig sind.
- Wenn Sie unsicher bei etwas sind, fragen Sie uns. Der Datenschutzbeauftragte oder das Datenschutz- und IT-Sicherheitsteams (DIST) steht Ihnen gerne zur Verfügung. Wir möchten in unserem Unternehmen Datenschutz leben und auch verbessern.

### **Was ist das Datenschutz- und IT-Sicherheitsteams (DIST) und wie kann ich es erreichen?**

Dies ist ein Zusammenschluss mehrerer Personen. Diese betrachten im Unternehmen diverse Arbeitsprozesse in Bezug auf den Datenschutz und die IT-Sicherheit. Die Struktur ist gerade im Aufbau und Kontaktdaten werden wir nachreichen bzw. veröffentlichen.

### **Wer ist unser Datenschutzbeauftragter und was ist der Unterschied zum DIST?**

Unser externer Datenschutzbeauftragter ist Herr Kevin Ehl. Dieser ist auch ein Teil des DIST. Sollten Sie eine Frage zu Arbeitsprozessen haben, können Sie sich an das DIST wenden. Wenn Sie eine persönliche oder vertrauliche Frage zum Datenschutz haben, wenden Sie sich bitte an Herr Ehl direkt. Dieser ist gegenüber Ihrer Identität zur Verschwiegenheit verpflichtet. Sie erreichen diesen unter der Rufnummer 0821 – 54 37 827 oder per E-Mail unter [ehl.kevin@dsb-augsburg.de](mailto:ehl.kevin@dsb-augsburg.de)

### **Fragen und Anliegen zu diesem Merkblatt oder Verpflichtung**

Falls Sie noch Fragen haben, können Sie sich am einfachsten direkt an die folgende Emailadresse [info@pele.de](mailto:info@pele.de) wenden.