Datenschutz geht alle in unserem Team an!

Diese Pflichtschulung zum Datenschutz in der Apotheke soll Sie, die Mitarbeiter der Apotheke, mit den Bestimmungen des Datenschutzrechts vertraut machen und Sie für den richtigen Umgang mit personenbezogenen Daten sensibilisieren. Einiges ist selbstverständlich. Gleichwohl ist es wichtig, sich die Grundlagen immer wieder vor Augen zu führen und auch die neuen Anforderungen, die der Gesetzgeber stellt, zu verinnerlichen.

Folgende Aspekte werden wir beleuchten:

- die **Grundlagen** des Datenschutzrechts, insbesondere dessen Ziele und die maßgeblichen Gesetzeswerke sowie den Anwendungsbereich der Datenschutz-Grundverordnung und die Rechtsgrundlagen für die Datenverarbeitung,
- die erforderlichen **Maßnahmen** zur Datensicherheit und wie Sie dazu beitragen können,
- die **Informationspflichten**, die gegenüber den Kunden bestehen,
- die **Rechte** der Kunden,
- die **Melde- und Benachrichtigungspflichten** im Fall von Datenpannen,
- die **Konsequenzen**, die **Verstöße** gegen die Vorschriften des Datenschutzrechts für die Apotheke, den Erlaubnisinhaber, aber auch für Sie als Mitarbeiter haben können.

Grundlagen des Datenschutzrechts
Personenbezogene Daten

Beispiele für personenbezogene Daten:

- Name, Adresse, Geburtsdatum
- IP-Adresse
- Telefonnummer
- Kontonummer, Personalausweisnummer
- Foto-/Videoaufnahmen (wenn die Person erkennbar ist)
- „Sprechende“ E-Mail-Adresse

Nicht personenbezogen sind reine Sachangaben und Unternehmensdaten.

Pflichtschulung Datenschutz | © Deutscher Apotheker Verlag

Folie 7

Grundlagen: Was sind personenbezogenen Daten?

- Daten, aus denen die **Identität** der betroffenen Person **unmittelbar** hervorgeht, sind beispielsweise der **Name**, die **Anschrift** und das **Geburtsdatum**.
- Personenbezogene Daten sind aber auch Daten, die erst durch die **Verknüpfung mit weiteren Informationen** eine Identifikation der Person zulassen, wie beispielsweise **IP-Adressen**, die über die Website der Apotheke erhoben werden. Allein über die IP-Adresse ist der Apotheke die Identifikation einer Person nicht möglich. Im Fall von Cyberattacken kann die Apotheke aber unter Hinzuziehung der zuständigen Behörden über den Internetdienstanbieter die IP-Adresse einer bestimmten Person zuordnen. Der Rechtsprechung reicht diese Möglichkeit aus, um IP-Adressen als personenbezogene Daten einzuordnen.
- Weitere Beispiele für personenbezogene Daten sind **Telefonnummern**, **Kontonummern**, **Personalausweisnummern**, **Rentenversicherungsnummern**, K**fz-Kennzeichen** usw.
- Auch **Foto- und Videoaufnahmen** gehören dazu, wenn die Personen darauf erkennbar sind.
- **E-Mail-Adressen** sind jedenfalls dann personenbezogen, wenn sie den **Namen ihres Inhabers** enthalten.
- Auch die Daten zu **Mitarbeitenden von Arztpraxen** (Namen und/oder Kontaktdaten der Sprechstundenhilfen) sind personenbezogene Daten!

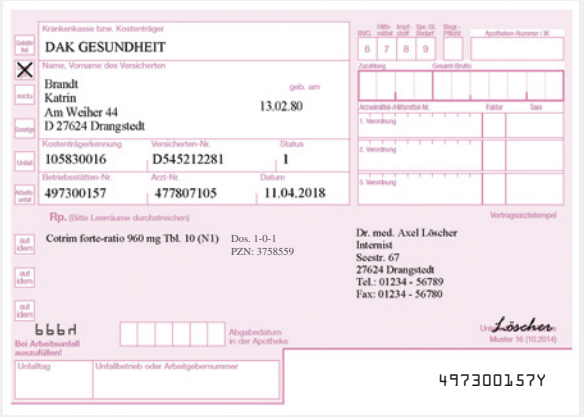
Nicht zu den **personenbezogenen Daten** gehören **Sachangaben ohne Bezug zu einer Person** (bspw. Ablaufdatum eines Medikaments). Ebenfalls nicht personenbezogen sind reine **Unternehmensdaten** (bspw. Name einer GmbH oder Aktiengesellschaft, wenn diese **nicht sprechend** sind). Der Name einer Apotheke kann aber ebenso wie der Name einer Arztpraxis personenbezogen sein, wenn er den Inhaber erkennen lässt (Max Mustermann Apotheke). Wenn **Unternehmensdaten mit Personen ergänzt werden**, zum Beispiel dem Namen des Pharmareferenten, dann ist dieser Name als **personenbezogen** zu werten.

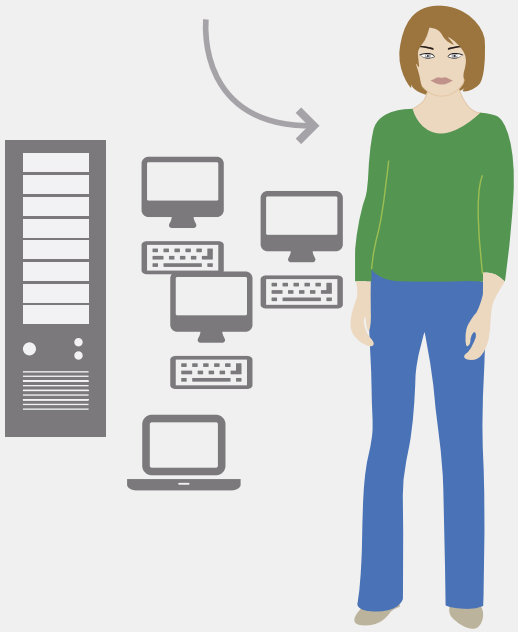
Grundlagen des Datenschutzrechts
Personenbezogene Daten

Beispiele für **personenbezogene Daten**:

- Name, Adresse, Geburtsdatum
- IP-Adresse
- Telefonnummer
- Kontonummer, Personalausweisnummer
- Foto-/Videoaufnahmen (wenn die Person erkennbar ist)
- „Sprechende“ E-Mail-Adresse

Nicht personenbezogen sind reine Sachangaben und Unternehmensdaten.





Maßnahmen: Umgang mit Computern

Beim Umgang mit dem Computer müssen Sie darauf achten, dass **keine unberechtigten Dritten Zugang** zu den Daten erhalten können und **Daten nicht verloren** gehen.

Passwörter

- Wählen Sie daher **sichere Passwörter**, die möglichst zehn Stellen haben und aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Das Passwort ist geheim zu halten und darf niemandem – auch nicht Ihren Kollegen – mitgeteilt werden. Passwörter sind möglichst nicht zu notieren. Falls eine Notiz notwendig ist, ist diese sicher aufzubewahren, also nicht am Monitor, auf dem Schreibtisch oder in der Schreibtischschublade.
- **Passwörter** sollten **nicht doppelt verwendet** werden. Früher wurde empfohlen, Passwörter in regelmäßigen Abständen zu ändern. Diese Empfehlung gilt heute als überholt, da sie zur Wahl einfacher Passwörter und zur doppelten Verwendung von Passwörtern verleitet. Wählen Sie daher besser ein sicheres Passwort und ändern Sie dieses nur, wenn es Anzeichen gibt, dass dieses in fremde Hände gelangt ist.

Sonstige Maßnahmen

- Bei **Nichtbenutzung des Computers melden Sie sich ab**; natürlich erst Recht, wenn Sie die Offizin länger verlassen. Außerdem ist der Computer so einzustellen, dass sich bei mehrminütiger Nichtbenutzung ein **Sperrbildschirm** öffnet, damit nicht Lieferanten, Reinigungspersonal oder sonstige Dritte in der Apotheke auf den Computer zugreifen können.
- E-Mail-Anhänge und Links in E-Mails **unbekannter Absender** dürfen wegen der **Gefahr von Computerviren** nicht geöffnet werden. Verwenden Sie keine USB-Sticks, die Sie nicht neu und leer im qualifizierten Fachhandel gekauft haben.
- Regelmäßige **Updates** schließen Sicherheitslücken und schützen den Computer vor Schadsoftware.
- Außerdem sind regelmäßige **Datensicherungen** zum Schutz der Daten vor Verlust durchzuführen.
  → *Die spezifische Vorgehensweise der Apotheke ist hier gegebenenfalls zu erläutern.*

Private Nutzung / private Endgeräte

- Beachten Sie die Vorgaben der Apotheke zur privaten Nutzung von Computern und Telefonen.
  → *Spezifische Vorgaben der Apotheke sind hier gegebenenfalls zu ergänzen.*
- **Private Endgeräte** (insbesondere Smartphones) sind **nicht für die Kommunikation mit Kunden** zu verwenden; insbesondere dürfen Sie dort keine Kundendaten speichern!

Maßnahmen zur Datensicherheit
Umgang mit dem Computer

- Sichere Passwörter wählen
- Bei Nichtbenutzung ausloggen
- Keine E-Mail-Anhänge unbekannter Absender öffnen
- Keine fremden USB-Sticks nutzen
- Regelmäßig Updates durchführen
- Regelmäßige Datensicherungen
- Private Nutzung beschränken
- Keine Benutzung privater Endgeräte für Kundenkommunikation