



Betrieblicher Datenschutz

Verstöße gegen die Schweigepflicht und den Datenschutz sind keine Kavaliersdelikte. Das bedeutet: Bei schweren Verstößen drohen neben arbeitsrechtlichen auch strafrechtliche Konsequenzen!

Anregungen zur Optimierung des betrieblichen Datenschutzes

Sollten Sie Anregungen zur Verbesserung des Datenschutzes in Ihrem Arbeitsbereich haben, können Sie sich an die hier genannten Ansprechpartner wenden.

Verantwortlicher für die Verarbeitung:

- Evangelisches Krankenhaus Wesel GmbH
- Altenpflege Wesel GmbH
- Visalis Therapiezentrum Niederrhein GmbH
- MVZ am Evangelischen Krankenhaus Wesel GmbH
- Altenheim am Willibrordiplatz GmbH
- MVZ Gynäkologie Wesel GmbH

vertreten durch Geschäftsführer Heino ten Brink
Schermebecker Landstraße 88 · 46485 Wesel
eMail info@evkwesel.de
Telefon (02 81) 106 – 1
Telefax (02 81) 106 – 29 99
Internet www.evkwesel.de

Ihre Ansprechpartner für:

- Evangelisches Krankenhaus Wesel GmbH
- Altenpflege Wesel GmbH
- Altenheim am Willibrordiplatz GmbH

Örtlich Beauftragter für Datenschutz

Marcus Rosenkranz
eMail dsb@evkwesel.de
Telefon (02 81) 106 – 29 20
Telefax (02 81) 106 – 29 95

Zuständige Aufsichtsbehörde

Der Beauftragte für den Datenschutz der EKD
Böttcherstraße · 730419 Hannover
eMail info@datenschutz.ekd.de
Telefon (05 11) 76 81 28 – 0
Telefax (05 11) 76 81 28 – 20

Ihre Ansprechpartner für:

- MVZ am Evangelischen Krankenhaus Wesel GmbH
- Visalis Therapiezentrum Niederrhein GmbH
- MVZ Gynäkologie Wesel GmbH

Datenschutzbeauftragter

Ulrich Brandt
Arnswalder Straße 34c · 22147 Hamburg
eMail info@brandtu.eu
Telefon (040) 41 48 91 16
Telefax (040) 64 89 08 10

Zuständige Aufsichtsbehörde

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Postfach 20 04 44 · 40102 Düsseldorf
eMail poststelle@ldi.nrw.de
Telefon (0211) 38424 – 0
Telefax (0211) 38424 – 10



Datenschutz



Betrieblicher Datenschutz

**Sehr geehrte Mitarbeiterin,
sehr geehrter Mitarbeiter,**

im Rahmen Ihrer Tätigkeit erhalten Sie Kenntnis von vertraulichen Patienten- oder Bewohnerdaten. Die Schweigepflicht dient unmittelbar dem Schutz der Privatsphäre der uns anvertrauten Menschen. Unsere Mitarbeiterinnen und Mitarbeiter unterliegen nach §203 Strafgesetzbuch (StGB) der Schweigepflicht.

Patienten-/Bewohnerdaten umfassen nach der Datenschutzdurchführungsverordnung (DSVO) „Einzelangaben über persönliche oder sachliche Verhältnisse von Personen“, die sich in unserer Obhut befinden. Hierzu gehören alle Angaben über den Gesundheitszustand wie beispielsweise die Leidensgeschichte, Befunde, Diagnosen, Therapien oder pflegerische Maßnahmen, aber auch erforderliche Informationen zur Leistungsabrechnung und Kostenerstattung. Schon allein die Tatsache, wer sich in unseren Einrichtungen aufhält, unterliegt dem Datenschutz.

Der Gesetzgeber geht von einem grundsätzlichen Nutzungsverbot von Patienten-/Bewohnerdaten aus. Deshalb erfolgt eine legale Datenverwendung nur, wenn eine ausdrückliche Einwilligung des Patienten oder Bewohners vorliegt. Und auch dann ist die Datenverwendung auf die „betrieblichen Zwecke“ der Erhebung beschränkt.

12 nützliche Tipps, die Ihnen bei der Umsetzung des betrieblichen Datenschutzes helfen:

- Unterlagen und Räume mit Patienten-/Bewohnerdaten nicht unbeaufsichtigt lassen oder abschließen.
- Behandlungsakten oder andere personenbezogene Unterlagen niemals aus den Einrichtungen mitnehmen, um z.B. Arztbriefe zu diktieren.
- Auskünfte nur an die ausdrücklich vom Patienten/ Bewohner benannten Personen geben. Im Zweifelsfall für telefonisch erbetene Auskünfte Rückruf vereinbaren, um sich zu vergewissern, dass der Anrufer für die Auskunft ermächtigt wurde.
- Darauf achten, dass Unbefugte keine Gespräche mithören (im Wartebereich, in der Aufnahme, auf der Station, am Telefon).
- Die Nutzung von Patienten-/Bewohnerdaten immer auf den minimal möglichen Umfang reduzieren (Sparsamkeitsgebot).
- EDV-System vor Zugriff schützen – auch beim kurzzeitigen Verlassen des Büros den PC sichern (Bildschirmschoner aktivieren), Tür(en) zum Büro stets verschließen.
- Sensible Daten in eMails verschlüsseln.
- Vorsicht beim Öffnen von eMail-Anhängen!
- eMail-Rundschreiben nur mit BCC-Funktion („Blindkopie“) versenden.
- Passworte regelmäßig wechseln, nicht an andere weitergeben und nicht in der Nähe des Systems aufbewahren; immer die eigene Benutzerkennung verwenden. Sichere Passwörter verwenden!
- Datenträger niemals unbeaufsichtigt lassen oder aus dem Krankenhaus mitnehmen.
- Gespeicherte Patienten-/Bewohnerdaten dürfen das speziell gesicherte Netzwerk unserer Einrichtungen nicht verlassen, deshalb ist der ungesicherte Datenaustausch per
 - USB-Stick,
 - eMail,
 - Laptop,
 - Internet,
 - Faxnicht gestattet!