BVfB-Newsletter
Bundesverband freier Berufsbetreuer e.V.

Nr. 3/ 2018 vom 22.05.2018

Datenschutz im Betreuerbüro – Aktuelle Informationen

Sehr geehrte Kolleginnen und Kollegen,

im Folgenden erhalten Sie weitere Informationen aus unserer Reihe "Datenschutz", die Sie auch auf unserer Online-Zeitschrift vollständig nachlesen können https://btdirekt.de/thema/datenschutz.html:

III. Technische und organisatorische Maßnahmen (Datensicherheit)

Das Verzeichnis über die Tätigkeit der Datenverarbeitung beinhaltet - wenn möglich - auch eine **allgemeine** Beschreibung der technischen und organisatorischen Maßnahmen (**TOM`s**), die der Betreuer oder die Betreuerin getroffen hat, um die Sicherheit der personenbezogenen Datenverarbeitung zu gewährleisten.

Dem BVfB ist es besonders wichtig, im diesem Zusammenhang darauf hinzuweisen, dass der Gesetzgeber den Umfang dieser Maßnahmen u.a. vom **Zweck der Datenverarbeitung** und den **Kosten** abhängig macht. Berufsbetreuer werden von den Gerichten verpflichtet, bestimmte Aufgaben für den Betreuten zu erledigen. Der Zweck der Datenverarbeitung erfolgt also zum einen **im Interesse des Betreuten** und zum anderen, **um einer** von den Betreuungsgerichten übertragenen **Pflicht zu entsprechen, deren Verletzung Schadensersatzansprüche des Betreuten zur Folge haben kann**. Hinzu kommt, dass zahlreiche - nicht alle - Berufsbetreuer als Einzelunternehmer nicht über die finanziellen Möglichkeiten verfügen dürften, um kostspielige technische Maßnahmen zur Verbesserung der Datensicherheit zu ergreifen. Es liegt daher auf der Hand, dass die Anforderungen an die Datensicherheit in großen Unternehmen, die häufig Daten **im eigenen Interesse** verarbeiten, deutlich höher sind als in einem Betreuungsbüro.

Dieser Ausgangspunkt ändert aber nichts daran, dass Berufsbetreuer verpflichtet sind, sich grundsätzlich Gedanken über die Datensicherheit in ihrem Betreuungsbüro zu machen und die ergriffenen technischen und organisatorischen Maßnahmen in dem Verzeichnis über die Tätigkeit der Datenverarbeitung niederzulegen.

Dem BVfB ist außerdem der Hinweis wichtig, dass der **Gesetzgeber** die im Einzelfall zu treffenden **TOM`s nicht beschrieben hat** und eine eigenverantwortliche Abwägung des Betreuers verlangt, bei der die Schwere der Risiken für die Rechte der Betreuten, die Eintrittswahrscheinlichkeit (Verlust, Veränderung, Vernichtung oder unbefugte Offenlegung personenbezogener Daten) und der Stand der Technik zu berücksichtigen sind.

Der BVfB empfiehlt anhand folgender **Checkliste** zu prüfen, welche TOM`s zur Datensicherheit ergriffen worden sind und ob diese als ausreichend angesehen werden. Anschließend sollten die TOM's im Verzeichnis über die Tätigkeit der Datenverarbeitung - geordnet nach der Checkliste -beschrieben werden. Die Checkliste ist so umfangreich, damit zumindest jeder Problembereich **gedanklich überprüft** und abgehakt wird. **Das bedeutet nicht, dass sämtlich in Frage kommenden TOM's im Verzeichnis über die Tätigkeit der Datenverarbeitung erwähnt werden müssen**. Der BVfB berät nicht zu technischen Fragen der IT-Sicherheit. Insoweit wird empfohlen - soweit erforderlich - sich bei IT-Fachleuten sachkundig zu machen.

Checkliste

I. Zugangskontrolle
Die Zugangskontrolle soll verhindern, dass Unbefugte Zugang zu Verarbeitungsanlagen (Bsp.: Server / eigener PC) erhalten, mit denen die Verarbeitung durchgeführt wird

1. Passwortgeschützter Zugang
2. Alarmanlage
3. Sicherheitsschlösser
4. Sorgfältige Auswahl des Reinigungspersonals
5. Abschließbare Serverschränke

II. Datenträgerkontrolle
Die Datenträgerkontrolle soll verhindern, dass Unbefugte Datenträger (CD-Rom / USB-Stick / Aktenordner) lesen, kopieren, verändern oder löschen können

1. Sichere Aufbewahrung von Datenträgern
2. Kennzeichnung der Aktendeckel lediglich mit den Initialen des Betreuten
3. Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
4. Ordnungsgemäße Vernichtung von Datenträgern
5. Einsatz von Aktenvernichtern
6. Vernichtung von größeren Aktenmengen durch Dienstleister mit Datenschutz-Gütesiegel
7. Einrichtung von Standleitungen bzw. VPN-Tunneln
8. Verschlüsselung von mobilen Datenträgern

III. Benutzerkontrolle
Die Benutzerkontrolle soll verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Datenübertragung nutzen können

1. Festlegung zugangsberechtigter Mitarbeiter
2. Passwortvergabe
3. Regelmäßige Kontrolle von Berechtigungen
4. Sperrung von Berechtigungen ausscheidender Mitarbeiter
5. Einsatz von Anti-Viren-Software (aktualisieren)

IV. Speicherkontrolle
Speicherkontrolle soll verhindern, dass Unbefugte von gespeicherten personenbezogenen Daten Kenntnis nehmen sowie diese eingeben, löschen oder verändern können

1. Vergabe von persönlichen Passwörtern
2. Festlegung von Berechtigungen zum Zugang zum IT-System
3. Festlegung von Passwortrichtlinien (Anzahl der Zeichen / Buchstaben / Zahlen / Sonderzeichen)

V. Zuverlässigkeit
Die Zuverlässigkeit soll gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden

1. Anti-Viren-Schutz (aktualisieren)
2. Automatisierte Meldung von Fehlfunktionen
3. Unabhängig voneinander funktionierende Systeme

VI. Wiederherstellbarkeit und Datenintegrität
Die Wiederherstellbarkeit soll gewährleisten, dass eingesetzte Systeme im Störfall wiederhergestellt werden können. Die Datenintegrität soll gewährleisten, dass gespeicherte, personenbezogene Daten nicht durch Fehlfunktionen beschädigt werden können.

1. Erstellen eines Backup- & Recoverykonzepts
2. Regelmäßige externe Speicherung der Daten (externe Festplatte / USB-Stick)
3. Erstellen eines Notfallplans

VII. Verfügbarkeitskontrolle
Die Verfügbarkeitskontrolle soll gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind

1. Feuer- und Rauchmeldeanlagen
2. Feuerlöschgeräte in Servernähe
3. Geräte zur Überwachung von Temperatur, Feuchtigkeit und / oder beim Betreten von Räumlichkeiten durch Unbefugte
4. Erstellen eines Notfallplans

VIII. Transportkontrolle
Die Transportkontrolle soll gewährleisten, dass bei der Übermittlung von personenbezogenen Daten sowie beim Transport von Datenträgern die Vertraulichkeit geschützt wird

1. Passwortgeschützter Zugang zu Datenträgern
2. Einsatz von Verschlüsselungstechnologien

IX. Übertragungskontrolle
Die Übertragungskontrolle soll gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung (Beispiel: Email / Telefax) übermittelt oder zur Verfügung gestellt wurden

1. Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
2. Dokumentation der Empfänger von Daten (nach Ansicht des BVfB kann sich diese Dokumentation bereits aus einer gründlichen Aktenführung ergeben, wenn dort die Übertragung der Datenübermittlung dokumentiert wird)

In größeren Betreuungsbüros mit mehreren Mitarbeitern, die nur zu einem Teil der personenbezogenen Daten Zugang haben dürfen, sind ggf. Maßnahmen zur Zugriffskontrolle erforderlich (Bsp.: Mehrere Betreuer / Betreuerinnen arbeiten in Bürogemeinschaft zusammen und jeder beschäftigt Mitarbeiter, die ausschließlich für ihn / sie tätig sind).

IMPRESSUM

Herausgeber

Bundesverband freier Berufsbetreuer e.V.

Bundesgeschäftsstelle
Richard-Wagner Str. 52
10585 Berlin

eingetragen:

Registergericht Berlin Charlottenburg
VR 26684B

HINWEIS

Alle Angaben des BVfB-Newsletter werden sorgfältig geprüft.

Wir können jedoch keine Gewähr für die Richtigkeit übernehmen.

Postanschrift:
Bundesverband freier Berufsbetreuer e.V.
Servicegeschäftsstelle
Sachsendorfer Str. 7
03051 Cottbus

info@bvfbev.de

www.bvfbev.de

HOTLINE

Mo – Do: 09.00 – 16.30 Uhr
Fr: 09.00 – 14.00 Uhr

0180 2001896

0800 1901009