**DAS VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN**

**Ein Muster zur Orientierung für Betreuer/innen**

1. **Wer ist der Verantwortliche?** *(Art. 30 Abs. 1 S. 2 lit. a DSGVO)*

Name des Betreuungsbüros/Betreuer\*in *(juristische Person)*

## Wer ist/sind die gesetzlichen Vertreter ?

Berufsbetreuer: *Vorname Name; Postadresse, E-Mail Adresse*

## Wer ist der Datenschutzbeauftragte?

(bei Betreuungsbüros mit weniger als 20 Mitarbeiter\*innen, die ständig mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, nicht erforderlich)

1. **Zu welchen Zwecken verarbeitet das Betreuungsbüro/der/die Berufsbetreuer\*in  
   personenbezogene Daten?** *(Art. 30 Abs. 1 S. 2, lit. b DSGVO)*
   1. **Der Verantwortliche verarbeitet im Rahmen seiner beruflichen Tätigkeit**

* als Berufsbetreuer gemäß § 1821 BGB,
* als Nachlasspfleger gemäß §1961 BGB,
* als Verfahrenspfleger gemäß § 276 FamFG,
* nach §20 BtOG personenbezogene Daten

**personenbezogene Daten in folgenden Systemen**:

* Fachsoftware zur Verwaltung von elektronischen Akten; butler 21 Services
* Aktenordner/Handakten
* Onlinebanking-Software (z.B. Starmoney)
* E-Mail-Programm (z.B. Outlook office 365 professional)
* Telefon-/Faxsoftware (z.B. Fritzbox)
* Office-Programme (z.B. Word, Excel)
* Elektronische Ordner oder Festplatten (Festplatte Typ Name)
  1. **Der Verantwortliche beschäftigt Mitarbeiter und verarbeitet Beschäftigtendaten**
* auf der Grundlage des § 26 BDSG

1. **Kategorien von betroffenen Personen und Kategorien personenbezogener Daten** *(Art. 30 Abs. 1 S 2 lit. c DSGVO)*
   1. **Zu welchen Kategorien von betroffenen Personen werden Daten verarbeitet?**

Beziehungen zu anderen Personen: Verwandtschaft, Nachbarschaft, soziales Netzwerk, Ansprechpartner von Institutionen; Gerichte, Betreuungsbehörden, Sozialleistungs­träger, Sozial- und Gesundheitseinrichtungen Versicherungen, Inkassounternehmen, Ärzte, Wohnungsgesellschaften, Vermieter, Banken, etc.

* + 1. **Welche Datenarten und -kategorien werden erhoben?   
       (im Rahmen der Betreuungstätigkeit)**

Name, Vorname, Kontaktdaten, biografische Daten, Daten bezüglich Sozialleistungen nach den Sozialgesetzbüchern (SGB II, III, IV, V, VIII, IX, XII), Daten zu Privatversicherungen (Haftpflicht-, Hausrat-, Gebäude-, Unfall-, Lebensversicherungen etc.), Kontodaten, Daten zum Vermögen und Einkommen, Daten zu Beziehungen, Verwandtschaft, Nachbarn, Freunde, Ärzte, Daten zu Unterbringung in Heimen, Krankenhäuser, Einrichtungen, Gesundheitsdaten zu Erkrankungen, Dokumentation von Besuchen.

Die Datenarten und -kategorien sind abhängig von dem beauftragten Aufgabenkreis und der Erforderlichkeit, das Wohl und den Willen des Betreuten zu ermitteln und zu dokumentieren (§1901 Satz 1 BGB)

* + 1. **Welche Datenarten und -kategorien werden erhoben (für Beschäftigte)**

Name, Vorname, Kontaktdaten, Qualifikationsdaten, Daten zur Sozialversicherung, Steuer­nummer, Arbeitszeiten, Krank- und Urlaubstage, Lohndaten.

1. **Welchen Kategorien von Empfängern werden Daten offengelegt?**
   1. Dem Gericht die erforderlichen Daten zur Erfüllung der rechtlichen Aufgaben, Anfangsbericht, Vermögensverzeichnis, Jahresbericht; Anträge auf Grund von Einwilligungsvorbehalten;
   2. den Sozialleistungsträgern die erforderlichen Daten zur Erlangung der Sozialleistung,  
      Institutionen die erforderlichen Daten zur Erfüllung des Rechtsgeschäftes, Gesundheitseinrichtungen, -diensten die erforderlichen Daten im Rahmen von Behandlungen
   3. Empfängern von Daten zur Durchführung des Beschäftigungsverhältnisses, d.h.  
      Steuerberater, Berufsgenossenschaft, Krankenversicherung, Rentenversicherung, Finanzamt, die Daten die Arbeitgeber verpflichtend im Rahmen von Mitwirkungspflichten zu melden sind.
2. **Gibt es Empfänger in einem Drittland oder eine internationale Organisation?**

– keine –

(ggfs. erforderlich in Sozial-, Vermögensangelegenheiten bei Auslandsaufenthalten der Betreuten)

1. **Gibt es für verschiedene Datenkategorien Fristen zur Löschung (wenn möglich), bzw. Fristen zur Aufbewahrung?**
   1. **Daten der Betreuten**

Zur Wahrung der Betroffenenrechte und zum Wahren des eigenen Interesses im Rahmen der Haftung und der darin begründeten Nachweispflicht gilt allgemein eine Aufbewahrungsfrist solange die Bestellung zum Betreuer besteht, Die Originaldaten werden digitalisiert und an den Betreuten übergeben.

Es gelten unterschiedliche Aufbewahrungsfristen für unterschiedliche Dokumenten­arten.

Es gilt eine allgemeine Verjährungsfrist von drei Jahren.

Es gelten Aufbewahrungsfristen von 6 Jahren oder 10 Jahren für Unterlagen, die unter §147 AO und §257 HGB fallen.

In Haftungsfragen (Ziilrecht, z.B. Grundstücksgeschäfte) kann für einzelen Dokumente eine Aufbewahrungspflicht von 30 Jahren betsehen

* 1. **Daten der Beschäftigten**

Bis zum Verjährungseintritt aller absehbaren geltend zu machenden Ansprüche (§ 195 BGB), also drei Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Beschäftigungsverhältnis beendet wurde.

1. **Beschreiben Sie allgemein die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO:**
   1. **Wie wird die Vertraulichkeit, die Integrität, die Belastbarkeit sichergestellt?**

siehe Anlage/Checkliste technische und organisatorische Maßnahmen

* 1. **Wie oft werden die o.g. Sicherheitsmaßnahmen überprüft?**

Einmal jährlich.

* 1. **Beschreiben Sie das Risiko, das den Schutz der Person gefährdet**

Eine Risikofolgeabschätzung i. S. d. Artikel 35 DSGVO ist nicht erforderlich. Es werden zwar Gesundheitsdaten erhoben, aber nicht Massenhaft, nicht ausschließlich und nicht überwiegend.

* 1. **Beschreiben Sie die Maßnahmen/Schritte zur Aufklärung, Schulung, Sensibilisierung der natürlichen Personen, welche die personenbezogenen Daten verarbeiten**

Die Mitarbeiter werden mit der Einstellung auf den Datenschutz verpflichtet und entsprechend aufgeklärt

Der Abschluss einer Datenschutzerklärung jeden Mitarbeiters, befindet sich in der Personalakte.

Es findet eine regelmäßige Datenschutzsensibilisierung statt, mindestens einmal pro Jahr.

# Anlage: Checkliste technische und organisatorische Maßnahmen/ Maßnahmen der prosozial GmbH (muss an die aktuellen Toms angepasst werden)

## Maßnahmen im Rechenzentrum der prosozial GmbH

| **Nr.** | **Maßnahme** | **Umsetzung der Maßnahme** |
| --- | --- | --- |
| **1.** | **Zutrittskontrolle (Vertraulichkeit)**  Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird: | - Das Gebäude ist durch ein Schließsystem gesichert. Nur autorisierte Personen haben durch eine Chipkarte Zutritt. Besucher und Lieferanten müssen sich per Sprechanlage anmelden und werden persönlich empfangen und begleitet. Sie erhalten entsprechend Ihren Zutrittsberechtigungen gekennzeichnete Ausweise. Außerhalb der ordentlichen Geschäftszeiten ist der Zutritt zum Gebäude und dem Serverraum videoüberwacht.  - Der Zutritt zu den Technikräumen und dem Serverraum ist ebenfalls durch ein Chipsystem gesichert. Zutritt haben lediglich autorisierte Personen der IT Abteilung Intern. Die Schlüsselgewalt hat der IT Leiter inne. Die Zutritte zum Raum werden protokolliert. |
| **2.** | **Zugangskontrolle (Vertraulichkeit, Integrität)**  Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert werden: | - Die Daten der Kundendatenbanken sind technisch und logisch getrennt von den Daten der prosozial GmbH.  - Der Zugang zu den Datenbanksystemen ist technisch durch Einrichtung von Benutzernamen und Kennworten gewährleistet.  - Der Zugang zu den Systemen ist nur auf autorisierte Mitarbeiter begrenzt.  - Der Zugang von außen ist durch entsprechende Firewallsysteme geschützt.  -Die Passwörter der Kundendatenbanken werden in einem eigenem Passwortverfahren mit Passwortrichtlinie erstellt und aufbewahrt. Die Kundenbetreuer erhalten keine Klarsicht auf die Passwörter. |
| **3.** | **Zugriffskontrolle (Vertraulichkeit, Integrität, Verfügbarkeit)**  Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können. | - Der Zugriff auf die Kundendatenbanken ist zweistufig durch eine Anmeldung am Rechenzentrum (1) und Anmeldung auf der Kundendatenbank (2).  - Der Zugriff ist jeweils personalisiert  - Der Zugriff besteht aus Benutzername und Kennwort mit einer Passwortrichtlinie  - Alle Mitarbeiter der prosozial GmbH haben nur für Ihre Zwecke eingerichtete Benutzerberechtigungen, die von den verantwortlichen Abteilungsleitern oder Geschäftsführern festgelegt und freigegeben werden müssen.  - Zugriff auf das Rechenzentrum unterliegt ausschließlich autorisierten Mitarbeitern.  - Zugriff auf die Datenbank des Auftraggebers haben ausschließlich:  -- autorisierter Mitarbeiter der IT Abteilung zum Zwecke der Wartung und Fehlerbehebung;  Zugriff auf die Anwendung haben ausschließlich:  - die Kundenberater mit personalisierten Zugangsdaten, für vom Auftraggeber autorisierte Dienstleistungen (z.B. Second Level Support, Postservice, Fehlerbehebungen, Konfiguration)  -- das Löschen von Daten ist vertraglich geregelt, Daten werden gelöscht nach Beendigung des Auftragsverarbeitungsverhältnisses, standardmäßig 90 Tagen danach wenn nichts anderes schriftlich vereinbart ist. |
| **4.** | **Weitergabekontrolle (Vertraulichkeit, Integrität, Verfügbarkeit)**  Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft bzw. festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist: | - die Transportwege zum Rechenzentrum, zur Anwendung sind grundsätzlich verschlüsselt (https, RDP)  - Die Zutritte und Zugänge per Anmeldung auf dem Rechenzentrum werden nachvollziehbar mitgeloggt.  - bei Fehlerbehebungsaufträgen werden die Daten ausschließlich zu Testzwecken in den EDV Systemen der Prosozial zurückgesichert, die wiederum dem oben beschriebenen Zutrittskontroll-, Zugangskontroll- und Zugriffskontrollsystem unterliegen.  - Eine Weitergabe auf andere Datenträger wie z.B. USB Stick; CD Rom, etc. ist verboten, es sei denn der Auftraggeber verlangt die Ausgabe per Datenträger oder per verschlüsseltem Datentransport an eine von Ihm benannte autorisierte Person |
| **5.** | **Eingabekontrolle (Integrität)**  Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können: | - Änderungen an Daten, bzw. Zugriffe auf Daten werden mit geloggt (Transparenzprinzip, Änderungslogs, Dokumentenversionierung)  - Die Logdateien sind gesichert und können durch den Anwender nicht gelöscht werden. |
| **6.** | **Auftragskontrolle (Vertraulichkeit, Verfügbarkeit)**  Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können: | - Der Gegenstand des Auftrages wird in einer Vereinbarung schriftlich festgehalten  - Der Auftrag erstreckt sich auf das Verarbeiten der Daten und hier insbesondere auf das Speichern und das zur Verfügung stellen über eine verschlüsselte Verbindung (Dateihosting).  - Insbesondere das Löschen der Daten erfolgt ausschließlich auf Weisung des Auftraggebers. Soweit eine Löschung der Daten technisch nicht möglich ist, bzw. der Aufwand im Verhältnis zum angestrebten Schutzzweck steht zu hoch ist werden die Daten gesperrt.  - Die Löschung der Daten nach Herausgabe an den Kunden erfolgt entsprechend der in der Systembeschreibung definierten Sicherheitsintervallen. bzw. bei Virenbefall entsprechend den ins den Systembeschreibung definierten Ausnahmen |
| **7.** | **Verfügbarkeitskontrolle (Verfügbarkeit, Wiederherstellung der Verfügbarkeit)**  Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind | - Datenbanken werden gesichert  - Daten werden systemisch in der Anwendung gesichert  - ein Ausfall der Techniksysteme wird durch ein zentrales USV geschützt  - es liegt ein Desasterrecoveryplan vor  - der Eintritt eines Brandes, der Ausfall der Raumklimatisierung, der Ausfall von Strom werden durch entsprechende Systeme überwacht  - die technischen System im Gebäude sind risikoabhängig in verschieden Brandabschnitte aufgeteilt  - Die Verfügbarkeit der Daten wird durch Maßnahmen entsprechend der aktuell vorhandenen technischen Möglichkeiten sichergestellt (siehe Systembeschreibung |
| **8.** | **Trennungskontrolle (Vertraulichkeit, Integrität)**  Maßnahmen die sicherstellen, dass Daten entsprechend Ihrem Zweck und den zugeordneten Berechtigungen verarbeitet werden. | - die Kundendatenbanken im Rechenzentrum sind physikalisch von einander getrennte Datenbanken  - die Vergabe von Rechten kann sehr detailliert innerhalb der Software geregelt werden  - Veränderungen an den Daten werden auf Entitätsebene mit Datum und Nutzerangaben mitprotokolliert |

## Maßnahmen im Betreuungsbüro

| **Nr.** | **Maßnahme** | **Umsetzung der Maßnahme** |
| --- | --- | --- |
| **1.** | **Zutrittskontrolle (Vertraulichkeit)**  Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird: | * Alarmanlage * Chipkarten-/Transponder-Schließsystem * Abschließbare Serverschränke, Serverräume * Sorgfältige Auswahl Reinigungspersonal * Sicherheitsschlösser |
| **2.** | **Zugangskontrolle (Vertraulichkeit, Integrität)**  Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert werden: | * Festlegung von Berechtigungen in den IT-Systemen * Differenzierte Berechtigungen für Lesen, Löschen und Ändern * Verwaltung der Rechte durch Systemadministratoren * Passwortrichtlinie inkl. Passwortlänge, |
| **3.** | **Zugriffskontrolle (Vertraulichkeit, Integrität, Verfügbarkeit)**  Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können. | * Der Zugriff ist jeweils personalisiert. * Der Zugriff besteht aus Benutzername und Kennwort mit einer Passwortrichtlinie. |
| **4.** | **Weitergabekontrolle (Vertraulichkeit, Integrität, Verfügbarkeit)**  Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft bzw. festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist: | * Die Verbindung ist verschlüsselt * Zugriffe werden mitgeloggt * Empfänger sind in der Anwendung dokumentiert |
| **5.** | **Eingabekontrolle (Integrität)**  Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können: | * Änderungen an Daten, bzw. Zugriffe auf Daten werden mit geloggt (Transparenzprinzip, Änderungslogs, Dokumentenversionierung) * - Die Logdateien sind gesichert und können durch den Anwender nicht gelöscht werden. |
| **6.** | **Auftragskontrolle (Vertraulichkeit, Verfügbarkeit)**  Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können: | * s.o. Maßnahmen im Rechenzentrum * Der Gegenstand des Auftrages wird in einer Vereinbarung schriftlich festgehalten * Der Auftrag erstreckt sich auf das Verarbeiten der Daten und hier insbesondere auf das Speichern und das zur Verfügung stellen über eine verschlüsselte Verbindung (Dateihosting). * Insbesondere das Löschen der Daten erfolgt ausschließlich auf Weisung des Auftraggebers. Soweit eine Löschung der Daten technisch nicht möglich ist, bzw. der Aufwand im Verhältnis zum angestrebten Schutzzweck steht zu hoch ist werden die Daten gesperrt. * - Die Löschung der Daten nach Herausgabe an den Kunden erfolgt entsprechend der in der Systembeschreibung definierten Sicherheitsintervallen. bzw. bei Virenbefall entsprechend den ins den Systembeschreibung definierten Ausnahmen |
| **7.** | **Verfügbarkeitskontrolle (Verfügbarkeit, Wiederherstellung der Verfügbarkeit)**  Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind | * s.o. Maßnahmen im Rechenzentrum * Datenbanken werden gesichert * Daten werden systemisch in der Anwendung gesichert * ein Ausfall der Techniksysteme wird durch ein zentrales USV geschützt * es liegt ein Desasterrecoveryplan vor * der Eintritt eines Brandes, der Ausfall der Raumklimatisierung, der Ausfall von Strom werden durch entsprechende Systeme überwacht * die technischen System im Gebäude sind risikoabhängig in verschieden Brandabschnitte aufgeteilt * - Die Verfügbarkeit der Daten wird durch Maßnahmen entsprechend der aktuell vorhandenen technischen Möglichkeiten sichergestellt (siehe Systembeschreibung |
| **8.** | **Trennungskontrolle (Vertraulichkeit, Integrität)**  Maßnahmen die sicherstellen, dass Daten entsprechend Ihrem Zweck und den zugeordneten Berechtigungen verarbeitet werden. | * s.o. Maßnahmen im Rechenzentrum * die Kundendatenbanken im Rechenzentrum sind physikalisch von einander getrennte Datenbanken * die Vergabe von Rechten kann sehr detailliert innerhalb der Software geregelt werden * - Veränderungen an den Daten werden auf Entitätsebene mit Datum und Nutzerangaben mitprotokolliert |