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 (juristische Person)

1.1 Wer sind die gesetzlichen Vertreter (Geschäftsführer)?

Berufsbetreuer

1.2 Wer ist der Datenschutzbeauftragte?

(bei Betreuungsbüros mit weniger als 10 Mitarbeitern, die ständig mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, nicht erforderlich)

2. Zu welchen Zwecken verarbeitet das Betreuungsbüro personenbezogene Daten? *(Art. 30 Abs. 1 S. 2, lit. b DSGVO)*

2.1 Der Verantwortliche verarbeitet im Rahmen seiner beruflichen Tätigkeit

- als Berufsbetreuer gemäß § 1896 BGB,
- als Nachlasspfleger gemäß §1960 BGB,
- als Verfahrenspfleger gemäß § 276 FamFG,
- als Betreuungsverein nach § 1900 BGB

personenbezogene Daten in folgenden Systemen:

- Fachsoftware zur Verwaltung von elektronischen Akten (Name)
- Aktenordner/Handakten
- Onlinebanking-Software (Name)
- E-Mail-Programm (Name)
- Telefon-/Faxsoftware (Name)
- Office-Programme
- Elektronische Ordner oder Festplatten

(Diese könnten auch als eigene Verarbeitungsvorgänge verstanden werden, siehe Vorschlag des DAV.)

2.2 Der Verantwortliche beschäftigt Mitarbeiter und verarbeitet Beschäftigtendaten

- auf der Grundlage des § 26 BDSG neu.

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

3.1 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.

3.1.1 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)

3.1.2 Welche Datenarten und -kategorien werden erhoben (für Beschäftigte)

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

4. Welchen Kategorien von Empfängern werden Daten offengelegt?

4.1 Dem Gericht die erforderlichen Daten zur Erfüllung der rechtlichen Aufgaben, Vermögensverzeichnis, Jahresbericht; Anträge auf Grund eines Einwilligungsvorbehaltes;

4.2 den Sozialleistungsträgern die erforderlichen Daten zur Erlangung der Sozialleistung, Institutionen die erforderlichen Daten zur Erfüllung des Rechtsgeschäftes, Gesundheitseinrichtungen, -diensten die erforderlichen Daten für Behandlung

4.3 Empfängern von Daten zur Durchführung des Beschäftigungsverhältnisses, d.h. Steuerberater, Berufsgenossenschaft, Krankenversicherung, Rentenversicherung, Finanzamt.

5. Gibt es Empfänger in einem Drittland oder eine internationale Organisation?

– keine –

6. Gibt es für verschiedene Datenkategorien Fristen zur Löschung (wenn möglich), bzw. Fristen zur Aufbewahrung?

6.1 Daten der Betreuten

Zur Wahrung der Betroffenenrechte und der 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.

6.2 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.

7. Beschreiben Sie allgemein die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO:

7.1 Wie wird die Vertraulichkeit, die Integrität, die Belastbarkeit sichergestellt?

siehe Anlage/Checkliste technische und organisatorische Maßnahmen

7.2 Wie oft werden die o.g. Sicherheitsmaßnahmen überprüft?

Einmal jährlich.

7.3 Beschreiben Sie das Risiko, das den Schutz der Person gefährdet (ggfs. erforderlich für die Verarbeitung der Kundendaten im Rechenzentrum, da diese besonders sensible Informationen enthalten, sowie auch für Personaldaten)

Eine Risikofolgeabschätzung ist nicht erforderlich. Es werden zwar Gesundheitsdaten erhoben, aber nicht ausschließlich und nicht überwiegend.

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

Aufklärung jeden Mitarbeiters bei Einstellung,
Abschluss einer Datenschutzerklärung jeden Mitarbeiters, verwaltet in der Personalakte.
regelmäßige Datenschutzschulung mindestens einmal pro Jahr.

2. Anlage: Checkliste technische und organisatorische Maßnahmen/ Maßnahmen der prosozial GmbH

2.1 Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, oder Aktenordnern, in denen personenbezogene Daten verarbeitet (gesammelt, geordnet oder genutzt) werden, verwehrt wird:

Checkliste

z.B.:

- Alarmanlage
- Chipkarten-/Transponder-Schließsystem
- Abschließbare Serverschränke, Serverräume
- Sorgfältige Auswahl Reinigungspersonal
- Sicherheitsschlösser

Maßnahmen im Rechenzentrum Koblenz für butler 21 Services

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. 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.

2.2 Zugangskontrolle

Maßnahmen, um die Nutzung von Datenverarbeitungssystemen durch Unbefugte zu verhindern:

Checkliste

- Festlegung von Berechtigungen in den IT-Systemen
- Differenzierte Berechtigungen für Lesen, Löschen und Ändern
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem

- Verwaltung der Rechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen

Maßnahmen im Rechenzentrum Koblenz für butler 21 Services

- ✓ 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 Firewall-Systeme geschützt.
- ✓ Die Passwörter der Kundendatenbanken werden in einem eigenem Passwortverfahren mit Passwortrichtlinie erstellt und aufbewahrt. Die Kundenbetreuer erhalten keine Klarsicht auf die Passwörter.

2.3 Zugriffskontrolle

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.

Maßnahmen im Rechenzentrum Koblenz für butler 21 Services

Der Zugriff auf die Kundensysteme ist zweistufig durch eine Anmeldung am Rechenzentrum (1) und eine Anmeldung in der Anwendung (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.
- ✓ Der Zugriff auf das Rechenzentrum unterliegt ausschließlich autorisierten Mitarbeitern.
- ✓ Zugriff auf die **Datenbank** des Auftraggebers haben ausschließlich: Autorisierte Mitarbeiter der IT-Abteilung zum Zwecke der Wartung und Fehlerbehebung.
- ✓ Zugriff auf die **Anwendung:** Die Kundenberater haben mit personalisierten Zugangsdaten Zugriff für vom Auftraggeber autorisierte Dienstleistungen (z.B. Second Level Support, Postservice, Fehlerbehebungen, Konfiguration).

2.4 Weitergabekontrolle/Transportkontrolle

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:

Checkliste

- Einrichtung von Standleitungen beziehungsweise Verschlüsselungs-Technologien
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung beziehungsweise vereinbarter Löschfristen

Maßnahmen im Rechenzentrum Koblenz für butler 21 Services

- ✓ Die Transportwege sind grundsätzlich verschlüsselt (https, RDP).
- ✓ Die Zutritte und Zugänge an den Anwendungen/Applikationen auf dem Rechenzentrum werden nachvollziehbar mitgeloggt.
- ✓ Zu Testzwecken bei Fehlerbehebungsaufträgen werden die Daten ausschließlich in den EDV-Systemen von prosozial zurückgesichert, die wiederum dem oben beschriebenen Zutrittskontroll-, Zugangskontroll- und Zugriffskontrollsystem unterliegen.
- ✓ Eine Weitergabe auf andere Datenträger wie 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.

2.5 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

Checkliste

- Festlegung von Berechtigungen in den IT-Systemen
- Differenzierte Berechtigungen für Lesen, Löschen und Ändern
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem
- Verwaltung der Rechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

- Protokollierung von Zugriffen auf Anwendungen

Maßnahmen im Rechenzentrum Koblenz für butler 21 Services

- ✓ Änderungen an Daten bzw. Zugriffe auf Daten werden mitgeloggt (Transparenzprinzip, Änderungslogs, Dokumenten-Versionierung)
- ✓ Die Logdateien sind gesichert und nicht durch den Anwender löschbar.

2.6 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

Maßnahmen im Rechenzentrum Koblenz für butler 21 Services

- ✓ Der Gegenstand des Auftrages wird in einer Vereinbarung 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.
- ✓ Insbesondere das Löschen der Daten erfolgt ausschließlich auf Weisung des Auftraggebers. Und soweit es technisch möglich ist bzw. der Aufwand im Verhältnis zum angestrebten Schutzzweck steht.
- ✓ Die Löschung der Daten nach Herausgabe an den Kunden erfolgt entsprechend der im Vertrag vereinbarten Löschfrist.

2.7 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Checkliste

- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Notfallplans

Maßnahmen im Rechenzentrum Koblenz für butler 21 Services

- ✓ Daten werden systemisch in der Anwendung gesichert.
- ✓ Ein Ausfall der Techniksysteme wird durch ein zentrales USV geschützt.
- ✓ Es liegt ein Disaster Recovery-Plan vor.

- ✓ Der Eintritt eines Brandes, der Ausfall der Raumklimatisierung, der Ausfall von Strom werden durch entsprechende Systeme überwacht.
- ✓ Die Verfügbarkeit der Daten wird durch Maßnahmen entsprechend der aktuell vorhandenen technischen Möglichkeiten sichergestellt (siehe Systembeschreibung).

2.8 Trennungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten nur Ihrem Zweck entsprechend von autorisierten Nutzern verarbeitet werden

Maßnahmen im Rechenzentrum Koblenz für butler 21 Services

- ✓ Die Kundendatenbanken im Rechenzentrum sind physikalisch voneinander getrennte Datenbanken.
- ✓ Die Vergabe von Rechten kann sehr detailliert innerhalb der Anwendung geregelt werden.
- ✓ Veränderungen werden mit Datum und Nutzerangaben mitprotokolliert.

2.9 Allgemeine Schutzmaßnahmen: Wiederherstellbarkeit, Zuverlässigkeit Datenintegrität

Checkliste

- Unabhängig voneinander funktionierende Systeme
- Automatisierte Meldung von Fehlfunktionen
- Anti-Viren-Schutz

Allgemeine Schutzmaßnahmen im Rechenzentrum Koblenz für butler 21 Services

- ✓ Eingehende E-Mails werden durch Spamfilter beim Provider gefiltert, es werden nur E-Mails aus dem Posteingang des Providers abgeholt. (Anm: Die prosozial GmbH empfiehlt die Verwendung von Office 365, da Microsoft einen Vereinbarung zur Auftragsverarbeitung mittels von der EU anerkannten Standardklauseln anbietet.)
- ✓ Beim Abholen der Mails über eine verschlüsselte Verbindung werden die E-Mails in Textfiles umgewandelt und auf Viren geprüft.
- ✓ Es gibt einen Virenschutzverantwortlichen. Viren werden eliminiert.
- ✓ Verlust durch Löschen ist technisch nicht möglich.
- ✓ Verlust durch Ausfall wird durch ein Sicherheitskonzept bzw. Disaster Recovery-Konzept verhindert. Es gibt einen Stand der Daten, der außerhalb des Rechenzentrums sicher aufbewahrt wird.

Quellen:

www.anwaltverein.de
www.dsgvo-gesetz.de