

1. Geltungsbereich

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die entsprechenden Verantwortlichkeiten bei der VP Verbund Pflegehilfe GmbH. Alle Mitarbeiter sind zur Einhaltung dieser Richtlinie verpflichtet.

Sie richtet sich insbesondere an:

- Mitarbeiter der VP Verbund Pflegehilfe GmbH
- Dienstleiter
- Geschäftspartner (Anbieter)

2. Grundsätze des Datenschutzes

- *Rechtmäßigkeit*

Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn eine Einwilligung des Betroffenen (Art. 6 Abs. 1 S. 1 lit. a) DSGVO) oder eine gesetzliche Erlaubnis (Art. 6 Abs. 1 S. 1 lit. b) bis f) DSGVO) vorliegt.

- *Transparenz*

Es muss für den Betroffenen immer ersichtlich sein, für welchen Zweck seine personenbezogenen Daten verarbeitet werden. Eine „heimliche“ Verarbeitung ist unzulässig.

- *Zweckbindung*

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

- *Datenminimierung/-sparsamkeit*

Unternehmen dürfen nur so viele Daten erheben und verarbeiten, wie sie tatsächlich benötigen. Die Daten müssen für den Zweck erheblich und relevant sein.

- *Richtigkeit*

Daten müssen inhaltlich und sachlich richtig und aktuell gehalten werden.

- *Speicherbegrenzung*

Daten dürfen nicht für die Ewigkeit gespeichert werden. Ist der Zweck nicht mehr gegeben, müssen die Daten gelöscht werden.

- *Integrität und Vertraulichkeit*

Die Daten müssen vor unrechtmäßiger Verarbeitung durch Unbefugte geschützt werden. Ebenso müssen die Daten vor versehentlicher Beschädigung oder Verlust geschützt werden.

- *Rechenschaftspflicht*

In der DSGVO gilt die Rechenschaftspflicht, d.h. die verantwortliche Stelle ist für die Einhaltung der oben genannten Grundsätze verantwortlich. Auf Verlangen muss sie die Einhaltung gegenüber den Betroffenen und den Behörden nachweisen können.

3. Begriffsdefinition

"Personenbezogene Daten"

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person.

"Automatisierte Verarbeitung"

Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

"Erhebung"

Erhebung ist das Beschaffen von Daten über den Betroffenen.

"Verarbeitung"

Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

"Speichern" das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung

"Verändern" das inhaltliche Umgestalten gespeicherter personenbezogener Daten.

"Übermitteln" das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einem Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abrufen.

"Sperren" das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.

"Löschen" das Unkenntlichmachen gespeicherter personenbezogener Daten.

"Nutzung"

Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

"Anonymisieren"

Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbarer natürlichen Person zugeordnet werden können.

„Pseudonymisieren"

Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

"Verantwortlicher"

Der Verantwortliche oder die Verantwortliche ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

"Empfänger"

Empfänger ist jede Person oder Stelle, die Daten erhält.

„Dritter“

Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle.

"Besondere Kategorien personenbezogener Daten"

Besondere Kategorien personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, biometrische Daten, Sexualeben oder auch Straftaten.

"Beschäftigte"

Beschäftigte sind Arbeitnehmerinnen und Arbeitnehmer, zu ihrer Berufsbildung Beschäftigte, Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung, in anerkannten Werkstätten für behinderte Menschen Beschäftigte, nach dem Jugendfreiwilligendienstgesetz Beschäftigte, Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten, Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

4. Verantwortlichkeiten

Die Gesamtverantwortung für die Sicherheit und die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten trägt die Geschäftsleitung des Unternehmens.

Die Maßnahmen zum Schutz von sensiblen Informationen, Daten, IT-Systemen und IT-Ressourcen entsprechen den jeweils gültigen gesetzlichen Auflagen und Verordnungen.

Zu diesem Zwecke wurde ein interner Datenschutzbeauftragte bestellt, um mit seinem Wissen, den Erfahrungen und unabhängigen Weisungen die Einhaltung von Gesetzen und Auflagen zu überwachen.

Der Datenschutzbeauftragte aktualisiert und entwickelt die Datenschutzorganisation weiter. Er unterrichtet die Geschäftsführung regelmäßig über den aktuellen Stand des Datenschutzes im Unternehmen. Auf dem Gebiet des Datenschutzes informiert er die Geschäftsführung und die Anwender über die geltenden Vorschriften sowie über die aktuellen Entwicklungen und Neuerungen.

5. Datenschutzbeauftragter

Die VP Verbund Pflegehilfe GmbH hat nach Maßgabe der §§ 4f und d BDSG einen betrieblichen Datenschutzbeauftragten (ebDSB) bestellt.

Externer Datenschutzbeauftragter:	Secjur GmbH
Interne Datenschutzkoordinatorin:	Ricarda Mainzer
Telefon:	06131 – 49 32 074
E-Mail:	datenschutz@pflegehilfe.de

6. Ziel und Zweck des Datenschutzkonzepts

Grundlage aller datenschutzbezogenen Regelungen ist das Recht auf informationelle Selbstbestimmung. Die informationelle Selbstbestimmung ist ein Grundrecht und bezeichnet das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

Eine Zielsetzung des Datenschutzkonzeptes ist es, dieses Grundrecht durch einen wirksamen Datenschutz zu gewährleisten. Dieses Ziel soll durch Transparenz, d. h. durch die Dokumentation der Forderungen und deren konkreter Umsetzung im Unternehmen, erreicht werden.

Ein weiteres Ziel dieses Dokumentes soll es sein, allen (internen und externen) Mitarbeiterinnen und Mitarbeitern einen Leitfaden in die Hand zu geben, damit die Datenverarbeitung einheitlich und nach verabschiedeten Standards durchgeführt wird. Die Verarbeitung personenbezogener Daten soll dabei unter Berücksichtigung der Integrität, Vertraulichkeit und der Verfügbarkeit zu jedem Zeitpunkt gewährleistet werden.

"Vertraulichkeit" bedeutet Schutz vor Offenlegung durch unautorisierte Personen.

"Integrität" beinhaltet die Sicherung gegen unautorisierte Veränderung.

"Verfügbarkeit" bedeutet, dass Informationen, Funktionen oder IT-Komponenten immer dann zugreifbar sein müssen, wenn ein autorisierter Benutzer sie benötigt.

7. Leitlinie zum Datenschutz

Wir als Geschäftsleitung verabschieden hiermit folgendes Datenschutzkonzept als Bestandteil unserer Firmenpolitik zur Einhaltung des Datenschutzes bei unserem Unternehmen. Die IT unterstützt unseren Geschäftszweck insbesondere bei Speicherung, Verarbeitung und Selektion von personenbezogenen Daten.

Unsere Daten, die Daten unserer Klienten und Anbieter sowie unsere IT-Systeme werden in ihrer Verfügbarkeit in allen Bereichen so gesichert, dass die zu erwartenden Stillstands-/Ausfallzeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität). An die Sicherstellung der Vertraulichkeit von Daten stellen wir die höchsten Ansprüche.

Wir tragen den Anforderungen der EU-Datenschutzgrundverordnung und des BDSG-neu (2018) Rechnung und streben ein dem Geschäftszweck und der Bedeutung der personenbezogenen Daten bzw. Datenverarbeitung angemessenes Datenschutzniveau an. Die organisatorischen Voraussetzungen sind auf die Sicherstellung der Ordnungsmäßigkeit der Datenschutzgesetze ausgerichtet. Die Wahrung der gesetzlichen Bestimmungen zum Datenschutz und die Einhaltung von Verpflichtungen (Verschwiegenheitspflicht, Vertraulichkeitspflicht, Pflicht zur Wahrung des Bankgeheimnisses etc.) sind für unser Unternehmen von wichtiger und großer Bedeutung.

Mitarbeiter, externe Dienstleister und Auftraggeber werden stets in Bezug auf den Datenschutz verpflichtet. Diese Verpflichtungen gelten zudem auch für die Zeit nach einem etwaigen Ausscheiden aus unserem Unternehmen.

Des Weiteren ist unser Unternehmen jederzeit bestrebt das Prinzip der Datensparsamkeit anzuwenden. Jegliche Daten werden zum frühestmöglichen Zeitpunkt bzw. nach Zweck-erfüllung so schnell wie möglich gesperrt und gelöscht.

8. Schutzziele und Sicherheitsziele

Die einzuhaltenden Schutz- und Sicherheitsziele sind:

1. Schutz vor Zugriff auf vertrauliche Informationen, sowohl von Klienten- und Anbieterdaten als auch Daten unseres Unternehmens
2. Hohe Verfügbarkeit und eine gegen Null gehende Ausfallquote der IT-Systeme
3. Dokumentation der IT-Systeme, Software
4. Dokumentation der wertschöpfenden und allgemeinen Prozesse im Unternehmen
5. Sicherstellung der Integrität der Daten im Unternehmen
6. Gewährleistung gesetzlicher Vorgaben im Rahmen der Datenhaltung und Datenverarbeitung
7. Einhaltung und Optimierung von Qualitätsstandards

9. Verzeichnis der Verarbeitungstätigkeiten

Durch unser Unternehmen wurde ein Verzeichnis der Verarbeitungstätigkeiten erstellt, und regelmäßig bei prozessualen Veränderungen aktualisiert. Dabei ist das Verzeichnis der Verarbeitungstätigkeiten in permanente, nicht permanente und Verarbeitungstätigkeiten als Auftragsverarbeiter unterteilt

10. Technische und organisatorische Maßnahmen

Da unser Unternehmen personenbezogene Daten verarbeitet, verwaltet und speichert, wurden geeignete technische und organisatorische Maßnahmen getroffen, um den Bestimmungen der EU-DSGVO und des BDSG-neu zu entsprechen. Dabei wurden die technischen und organisatorischen Maßnahmen den Anforderungen der Schutzbedarfsfeststellung und des Risikomanagements entsprechend aufgebaut.

[...]

11. Rechte Betroffener

Bei unserem Unternehmen werden folgende Rechte eines Betroffenen zu jedem Zeitpunkt gewährleistet:

- *Widerspruchsrecht:*
Das Recht, jederzeit gegen die Verarbeitung Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling.
- *Widerrufsrecht bei Einwilligungen:*
Das Recht, erteilte Einwilligungen jederzeit zu widerrufen.

- *Auskunftsrecht:*

Das Recht, eine Bestätigung darüber zu verlangen, ob betreffende Daten verarbeitet werden und auf Auskunft über diese Daten sowie auf weitere Informationen und Kopie der Daten entsprechend den gesetzlichen Vorgaben.

- *Recht auf Berichtigung:*

Entsprechend den gesetzlichen Vorgaben das Recht, die Vervollständigung oder die Berichtigung der unrichtigen Daten zu verlangen.

- *Recht auf Löschung und Einschränkung der Verarbeitung:*

Nach Maßgabe der gesetzlichen Vorgaben das Recht, zu verlangen, dass die personenbezogenen Daten unverzüglich gelöscht werden, bzw. alternativ nach Maßgabe der gesetzlichen Vorgaben eine Einschränkung der Verarbeitung der Daten zu verlangen.

- *Recht auf Datenübertragbarkeit:*

Das Recht personenbezogene Daten nach Maßgabe der gesetzlichen Vorgaben in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder deren Übermittlung an einen anderen Verantwortlichen zu fordern.

- *Beschwerde bei Aufsichtsbehörde:*

Das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat des gewöhnlichen Aufenthaltsorts, des Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes der betroffenen Person, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die Vorgaben der DSGVO verstößt.

12. Datenschutzverstöße

Bei unserem Unternehmen wurde eine Verfahrensanweisung zur Informationspflicht bei Datenpannen angefertigt und allen Mitarbeitern zugänglich gemacht. Alle Mitarbeiter sind darüber informiert, was zu beachten ist, wenn ein Datenschutzverstoß bzw. eine Datenpanne eintreten sollte.

Unabhängig davon, ob ein Datenschutzverstoß bzw. eine Datenpanne vorliegt oder aber auch nur ein entsprechender Verdacht besteht, ist unverzüglich die Geschäftsleitung bzw. der ggf. ein interner oder externer Datenschutzbeauftragte zu informieren. Denn nur er kann prüfen und entscheiden, ob eine Informationspflicht gegenüber Behörden oder gegenüber Betroffenen steht. Soweit eine Stellungnahme zum Datenschutzverstoß gegenüber Dritten notwendig ist, wird diese durch die Geschäftsleitung (oder falls bestellt durch den Datenschutzbeauftragten) abgegeben. Das Verfahren und die konkrete Prüfung sind der entsprechenden Verfahrensanweisung dokumentiert und zu beachten.

13. Kontinuierliche Verbesserungen

Der interne Datenschutzbeauftragte nimmt in regelmäßigen Abständen an Fortbildungen und Schulungen teil. Des Weiteren ist es seine Pflicht, sich auch selbstständig zum Thema Datenschutz mit den aktuellen Informationen auf dem Laufenden zu halten. Das Unternehmen stellt für diese Maßnahmen ein entsprechendes Budget zur Verfügung. In regelmäßigen Abständen erfolgt ein Erfahrungsaustausch und eine Weiterbildung der Geschäftsleitung bzw. der Mitarbeiter des Unternehmens.

Durch regelmäßige Prüfungen durch den Datenschutzbeauftragten mit entsprechender Ausarbeitung eines Prüfberichtes werden der Geschäftsleitung die Ergebnisse von Kontrollen, entdeckte Fehler oder Schwachstellen dargelegt.