Bearbeitungsreglement der Diartis AG

Einleitung

Dieses Dokument beschreibt die Bearbeitungsvorgänge von Datensammlungen der Kunden der Diartis AG. Diartis AG in Lenzburg und Bern bietet Softwarelösungen für die soziale Arbeit und das Fallmanagement an. Die Kunden befinden sich zum grössten Teil in der Schweiz, einige Kunden haben ihren Sitz im nahen Ausland.

Änderungskontrolle

Version	Datum	Beschreibung, Bemerkung	Name
1.0	13.12.2018	Freigabe	Daniel Canonica
1.1	24.09.2020	Anpassung Grafik	Daniel Canonica
1.2	11.11.2020	Anpassung Kap. 2, 9) Datenstandort	Daniel Canonica

Inhalt

Einleitung 1
1. Gesetzliche Rahmenbedingungen 2
2. Übersicht 2
3. Bearbeitungsreglement 3
3.1. Gesetzliche Grundlage 3
3.2. Art der Bearbeitung und Inhalt der Datensammlungen 4
3.3. Verantwortlichkeiten 4
3.4. Benutzer und Datenzugriff 4
3.5. Bearbeitung der Personendaten 5
3.6. Aufbewahrungsdauer, Archivierung und Löschung 6
3.7. Technische und organisatorische Massnahmen 6
4. Anhang 6
4.1. Dokumentenverzeichnis 6
4.2. Abkürzungen 7
4.3. Begriffe 7

1. Gesetzliche Rahmenbedingungen

Nahezu alle Kunden der Diartis speichern und verarbeiten besonders schützenswerte Personendaten im Sinne von Art. 3 lit. c. DSG. Im Rahmen von Projekten und Supporttätigkeiten kommt Diartis mit diesen Daten bzw. Datensammlungen in Berührung. In dieser Funktion ist Diartis (zeitweise) **Auftragsverarbeiter** im Sinne von Art. 28 DSGVO und ist verpflichtet, die Interessen des Verantwortlichen und der betroffenen Personen wahrzunehmen.
Diartis ist gegenüber ihren Kunden und den betroffenen Personen nie in der Stellung des Verantwortlichen gemäss Art. 24 DSGVO. Diartis offeriert aber Hosting bei Drittanbietern im Rahmen von Gesamtangeboten für schweizerische und ausländische Kunden und hat in diesem Fall Zugriff auf die Datensammlungen. Für Diartis gilt **schweizerisches Recht**, Diartis berücksichtigt die DSGVO im Interesse ihrer Kunden.

2. Übersicht

Die folgende Grafik zeigt die Verträge und Bearbeitungsvorgänge in einer Übersicht:

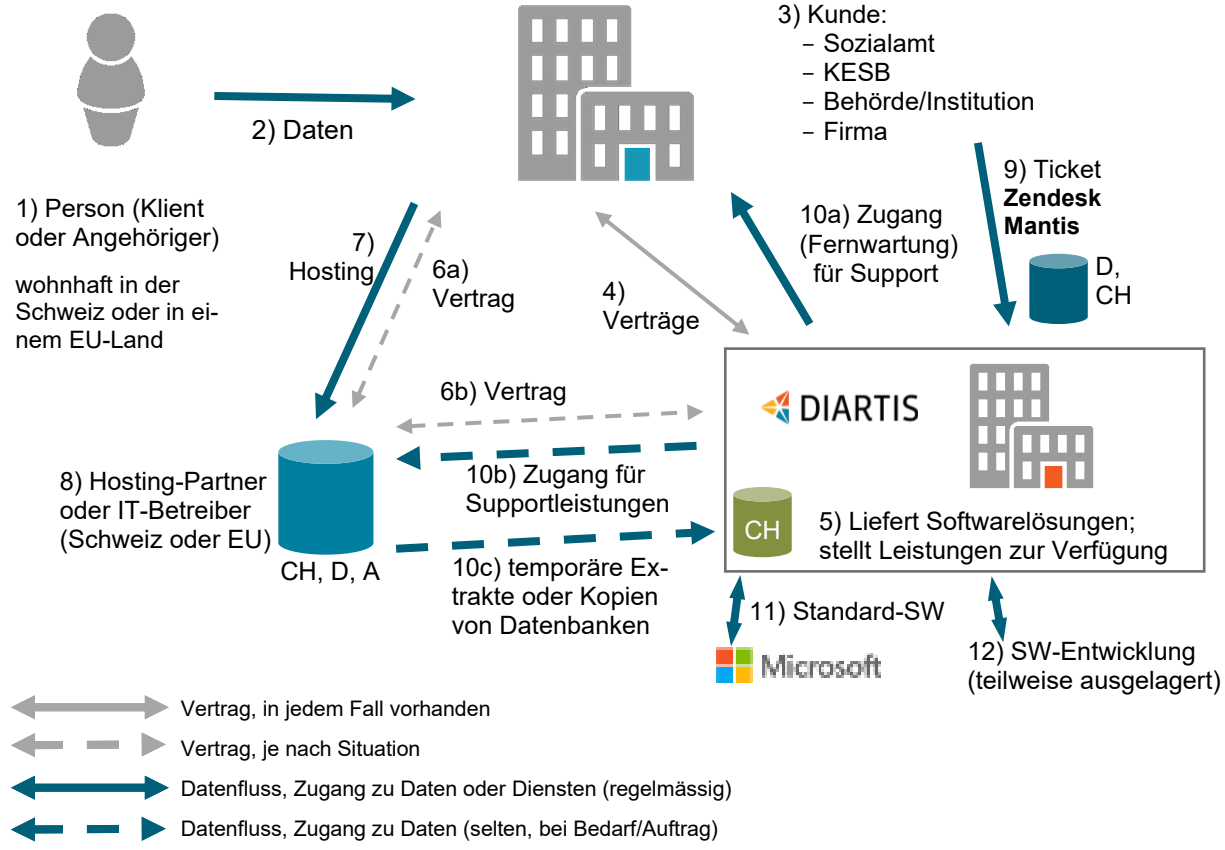

Abbildung 1: Übersicht der Verträge und Datenflüsse

Legende / Erklärungen:

1) Die betroffene Person ist in der Regel ein Klient oder Angehöriger eines Klienten der spezifischen Behörde. Wenn die betroffene Person temporär oder permanent in einem EU-Land wohnt, fällt sie unter die Anwendbarkeit der DSGVO. Betroffene Personen sind auch die Mitarbeitenden des Kunden, insoweit ihre Daten mit derselben Softwarelösung verwaltet werden.
2) Der Kunde (die Behörde oder Institution) sammelt und verarbeitet Daten über die betroffenen Personen für einen bestimmten Zweck.

3) Der Kunde ist im Falle der Produkte KLIBnet und KiSS in der Regel ein Sozialamt, eine KESB oder eine andere Behörde oder Institution im sozialen Umfeld. Bei den Produkten CASEnet und TEILHABEnet handelt es sich um öffentliche Behörden, Institutionen wie Heime, Krankenkassen, Versicherungen und privatwirtschaftliche Firmen, welche ein Case Management betreiben.
4) Der Kunde schliesst einen oder mehrere Verträge mit Diartis ab (Software-Lizenzen, Dienstleistungen, Wartung und Support).
5) Diartis liefert dem Kunden Softwarelösungen und Updates; sie stellt Projekt- und Supportleistungen sowie Schulungen zur Verfügung.
6) a) Der Kunde schliesst einen Hosting-Vertrag mit einem Anbieter ab[1], oder:
b) Diartis schliesst für den Kunden einen Hosting-Vertrag ab.
7) Die beim Kunden oder seinem IT-Betreiber installierte Softwarelösung verwaltet Datensammlungen, welche beim Hosting-Partner bzw. IT-Betreiber gespeichert sind.
8) Der Hosting-Partner stellt eine verschlüsselte Verbindung für den Datenzugriff zur Verfügung.
9) Der Kunde schreibt ein Support-Ticket (Zendesk oder Mantis) an Diartis. Dieses (bzw. dessen Anhänge) kann unter Umstände Fragmente der Daten von betroffenen Personen enthalten (Screenshots). Die Zendesk-Datenbank ist in Deutschland gespeichert, der Hersteller von Zendesk ist eine US-amerikanische Firma. Mantis ist eine Opensource-Lösung, die Diartis-Mantis-Datenbank ist in der Schweiz gespeichert.
10) a) Diartis erhält im Auftrag eines Kunden für Supportzwecke über Fernwartung Zugang zu einem Arbeitsplatz des Kunden und hat dabei unter Umständen auch Einsicht in Daten der betroffenen Personen.
b) Nach Genehmigung durch den Kunden greift Diartis über Fernwartung direkt auf die Datensammlung zu oder der Kunde schickt eine Kopie der Datenbank über eine verschlüsselte Verbindung an den Kundenbetreuer bei Diartis.
c) Insbesondere im Rahmen eines Projektes (Datenübernahme von Fremdsystem) hat Diartis über eine gewisse Zeit Zugriff auf die produktiven Datenbanken des Kunden. Kopien von Kundendatenbanken werden bei Diartis auf einem speziellen Server mit Zeitlimiten gespeichert.
11) Diartis nutzt Standard-Softwareprodukte von Microsoft und anderen Herstellern inklusive Office 365. In der Cloud werden keine Kundendaten oder Daten von betroffenen Personen gespeichert.
12) Diartis arbeitet für Software-Entwicklung und -Wartung mit Kloon GmbH, Schweiz und Kloon Ltd., Vietnam zusammen.

3. Bearbeitungsreglement

3.1. Gesetzliche Grundlage

Gemäss Art. 4 DSG dürfen

[1] Personendaten [..] nur rechtmässig bearbeitet werden.
[2] Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.
[3] Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.
[4] Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein

Gemäss DSGVO ist Diartis je nach Vertragsverhältnis in der Rolle des Auftragsbearbeiters. In der Zusammenarbeit mit Kunden in der EU sind Art. 28ff DSGVO anwendbar.

[1] In dem Fall, wo der Kunde einen verwaltungsinternen IT-Betreiber hat, wird unter Umständen dieser als Hosting-Partner agieren. In diesem Fall ist nicht immer ein formeller Vertrag vorhanden.

3.2. Art der Bearbeitung und Inhalt der Datensammlungen

Vorausschickend ist festzuhalten, dass das Sammeln und Verwalten von Daten nicht zum Geschäftsmodell der Diartis gehört. Diartis stellt ihren Kunden Softwarelösungen, Updates und Support zur Verfügung.
Diartis bearbeitet Datensammlungen von Kunden mit Daten über betroffene Personen nur aufgrund eines Auftrags und für eine begrenzte Zeit:

- im Rahmen eines Supportauftrags, welcher mündlich, telefonisch, per E-Mail oder Ticket erteilt wurde. In der Regel greift der Kundenbetreuer mittels Fernwartung auf den Arbeitsplatz des Kunden zu und untersucht dabei je nach Situation auch die Datenbank, wenn dies für die Problembehebung nötig ist.
- Wenn ein Problem gründlich analysiert werden muss, bittet der Diartis-Mitarbeiter den Kunden, ihm eine Kopie oder einen Auszug der Datenbank für eine bestimmte Zeit (in der Regel einige Tage) zu überlassen, damit sie bei Diartis untersucht werden kann. Dieser Vorgang wird protokolliert.
  Wenn der Kunde nicht selbst Zugang zu diesen Datenbanken hat, setzt sich der Diartis-Mitarbeitende mit dem IT-Betreiber oder Hosting-Partner des Kunden in Verbindung.
- Bei Projekten mit Neukunden werden in der Regel Daten von Datenbanken aus Fremdsystemen übernommen. Für Testzwecke und für die Durchführung der produktiven Datenübernahme erhält Diartis für eine bestimmte Zeit (einige Wochen) eine Kopie der produktiven Datenbank dieses Kunden.

Fast alle dieser Datensammlungen enthalten besonders schützenswerte Daten über die betroffenen Personen (nämlich die Klienten des Kunden). Sie können auch Personendaten über die Mitarbeitenden eines Kunden enthalten. Die Datensammlungen stammen immer von einem Kunden der Diartis bzw. dessen IT-Betreiber oder Hosting-Partner, wobei der Kunde die Autorisierung für den Datenbezug erteilt.
Diartis führt keine Aggregierungen von Datensammlungen durch und ändert die Struktur der Datensammlungen nicht. (Ausnahmen: bei Weiterentwicklungen der Software oder bei Datenübernahmen aus Fremdsystemen. Beides geschieht mit Wissen der Kunden und aufgrund von dokumentierten Vorgängen.)
Diartis gibt die Datensammlungen nie an Dritte weiter und verkauft keine Daten oder Auswertungen von Daten.

3.3. Verantwortlichkeiten

Der Kunde ist als juristische Person Inhaber der Datensammlungen über seine Klienten und Mitarbeitenden. Dadurch ist er in der Rolle des Verantwortlichen. Diartis und andere Leistungserbringer sind Auftragsverarbeiter.
Diartis hat eine Datenschutz-Beauftragte: Frau Ursula Sury, Die Advokatur Sury AG, CH-6005 Luzern.
Interne Ansprechstelle für Datenschutzfragen ist Herr Markus Widmer, Leiter Zentrale Dienste, Diartis AG.
Operativer Mitarbeiter Datenschutz ist Herr Daniel Canonica, Zentrale Dienste, Diartis AG.
Alle Mitarbeitenden der Diartis haben eine Geheimhaltungserklärung unterschrieben. Sie werden im Hinblick auf Datenschutzthemen regelmässig geschult und sensibilisiert. Die Einhaltung der Reglemente wird mit Journalen und internen und externen Audits überprüft.

3.4. Benutzer und Datenzugriff

3.4.1. Benutzerkreis und Zugriffsberechtigungen

Falls eine Datensammlung eines Kunden temporär bei Diartis gespeichert wird, geschieht dies auf einem dedizierten Server, welcher regelmässig automatisch gelöscht wird.
Zugriff auf diesen Server haben die Mitarbeitenden des entsprechenden Produktbereichs.
Das Speichern der Datenbank geschieht immer durch einen Support-Mitarbeiter der Diartis (Kundenbetreuer, manchmal auch Kundenmanager oder Projektleiter).

3.4.2. Rollen

Die Rollen sind pro Produktbereich vergeben. Im Bereich KLIBnet ist jeweils ein kleines Team für einen bestimmten Kundenkreis bzw. für eine geografische Region zuständig. In der Regel sind dann Mitarbeitende dieses Teams für die entsprechenden Kundendaten zuständig. Im Rahmen von Stellvertretungen oder Supportleistungen können aber auch andere Mitarbeitende Zugang zu solchen Kundendaten haben.

3.4.3. Prozess Zugriffsberechtigung

Beim Eintritt enthält ein neuer Mitarbeiter spezifische Berechtigungen aufgrund der zugewiesenen Rolle (z.B. Kundenbetreuer) und aufgrund der Zugehörigkeit einer Organisationseinheit.
Zugang zu Passwörtern und dergleichen werden in den Organisationseinheiten (Bereiche und Teams) reglementiert.

Für die Erteilung und den Entzug von Zugriffsberechtigungen ist der direkte Vorgesetzte verantwortlich. Er wird dabei mit Checklisten der Personaladministration und der internen IT-Administration unterstützt.
Die erteilten Berechtigungen werden durch die Applikationsverantwortlichen im Auftrag des Datenschutzverantwortlichen überprüft.

3.5. Bearbeitung der Personendaten

3.5.1. Geschäftsprozesse

Personendaten von Kunden können in den Geschäftsprozessen Service Desk, Auftragsabwicklung, Entwicklung sowie Dienstleistungen und Schulungen bearbeitet werden. Diese Prozesse sind im QMS der Diartis dokumentiert.

3.5.2. Datenbekanntgabe und Schnittstellen

Die detaillierten Schnittstellen sind in Abbildung 1 auf Seite 2 dargestellt.
Wenn ein Kunde eine Datenbank für Supportzwecke zur Verfügung stellt, speichert Diartis diese auf einem dedizierten internen Server ab. Der Transfer erfolgt nie per E-Mail, sondern über eine verschlüsselte Upload-/Download-Verbindung.

Es ist auch möglich, dass eine Datenbank für eine begrenzte Zeit auf einem lokalen Gerät (Notebook eines Diartis-Mitarbeitenden) gespeichert wird. Dieser Vorgang wird in einem Journal protokolliert.
Diartis gibt keine Kundendatenbanken an Dritte weiter.

Manchmal erstellen Kunden eine Kopie eines Bildschirmbereichs und hängen diese an ein Zendesk oder Mantis-Ticket an. Bei Zendesk erfolgt die Speicherung der Tickets in der Cloud, die physische Speicherung ist in Irland. Die Kunden der Diartis werden angehalten, Stellen mit Klientendaten auf den Bildschirmfotos unkenntlich zu machen.

Bei Neueinführungen von Diartis-Produkten wird oft eine Datenübernahme aus einem Fremdsystem gemacht. In diesem Fall erhält Diartis frühzeitig eine Kopie der Kundendatenbank(en) für Testzwecke. Die Verfahren sind vergleichbar mit dem Halten von Datenbanken für Supportleistungen, der Unterschied besteht vor allem darin, dass bei Datenübernahmen die Datenbanken länger bei Diartis bleiben, und dass es sich um Datenbankstrukturen von Herstellern von Konkurrenzprodukten handeln kann.

Derartige Datenbanken werden auf Diartis-eigenen Servern zwischengespeichert und nach Abschluss der Bearbeitung gelöscht.

3.6. Aufbewahrungsdauer, Archivierung und Löschung

3.6.1. Aufbewahrungsdauer

Wenn Diartis eine Datensammlung eines Kunden bei sich speichert, richtet sich die Aufbewahrungsdauer nach dem Bearbeitungsvorgang. In der Regel sind dies einige Tage bis wenige Wochen. Bei einem grösseren Projekt, welches eine Datenübernahme mit mehreren Testläufen einschliesst, kann die Zeitdauer auch länger sein. Diese wird mit dem Kunden vereinbart.
Je nach Abmachung mit dem Kunden können auch anonymisierte Datensammlungen verwendet werden.

3.6.2. Archivierung

Diartis archiviert keine Datensammlungen von Kunden. Es werden keine Backups des Servers erstellt, wo die Kundendatenbanken temporär gespeichert sind.

3.6.3. Löschung

Wenn der Bearbeitungszweck erfüllt ist, wird die Datensammlung gelöscht. Dieser Vorgang wird protokolliert.

3.7. Technische und organisatorische Massnahmen

Diartis schützt die technische Server- und Netzwerkinfrastruktur mit geeigneten Massnahmen, welche aktuell gehalten werden. Für diese Aufgaben stehen sowohl qualifiziertes internes Personal als auch Ressourcen eines erfahrenen IT-Anbieters zur Verfügung.
Die Rollen, Aufgaben, Kompetenzen und Stellvertretungen sind in einem Dokument beschrieben, welches allen Mitarbeitenden bekannt ist.
Die Einhaltung der Massnahmen wird in einem jährlich stattfindenden Datenschutzaudit überprüft, welches durch die Datenschutzverantwortliche (vgl. Kap. 3.3) durchgeführt wird.

4. Anhang

4.1. Dokumentenverzeichnis

Beinhaltet die Auflistung aller für die betreffenden Datensammlungen relevanten Gesetze, Verordnungen, Weisungen, Regelungen, technischen Spezifikationen, usw.

Dokumententyp	Titel
Gesetze	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)
Verordnungen	Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG)
EU-Verordnung	Datenschutz-Grundverordnung der Europäischen Union (DSGVO)
Diartis-Weisungen und Reglemente	• Datenschutz- und Geheimhaltungsvereinbarung • Datenschutzpolitik der Diartis AG • Reglement Datenschutzmanagement • Reglement Sicherheitskonzept
Website-Infos	https://www.diartis.ch/datenschutz.html

4.2. Abkürzungen

Abkürzung	Bedeutung
Art.	Artikel
DSG	Bundesgesetz über den Datenschutz (SR 235.1)
DSGVO	Datenschutz-Grundverordnung
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
IKT	Informations- und Kommunikationstechnik
IT	Information Technology, Informationstechnologie
KB	Kundenbetreuer/-in
KESB	Kindes- und Erwachsenenschutzbehörde
KM	Kundenmanager/-in
PL	Projektleiter/-in
QMS	Qualitätsmanagementsystem
SW	Software
VDSG	Verordnung zum Bundesgesetz über den Datenschutz (SR 235.11)

4.3. Begriffe

Begriff	Bedeutung
Bearbeiten	Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (siehe Art. 3 Bst. e DSG).
Bekanntgeben	Das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen (Art. 3 Bst. f DSG).
Besonders schützenswerte Personendaten	Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit; über Massnahmen der sozialen Hilfe; und über administrative oder strafrechtliche Verfolgungen und Sanktionen (Art. 3 Bst. c DSG).
Datensammlung	Im Sinne des Datenschutzgesetzes bedeutet Datensammlung „jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind“ (Art. 3 Bst. g DSG).
Hosting-Partner	Eine privatwirtschaftliche Firma, welche gegen Bezahlung Server, Speicherplatz, Netzwerke, Datenbanksysteme, Applikationen und Dienstleistungen zur Verfügung stellt.
Inhaber der Datensammlung	Inhaberin oder der Inhaber der Datensammlung sind private Personen oder Bundesorgane, die über den Zweck und den Inhalt der Datensammlung entscheiden (Art. 3 Bst. i DSG).
IT-Betreiber	Eine kommunale, regionale oder kantonale Organisation, welche Server, Speicherplatz, Netzwerke, Datenbanksysteme, Applikationen und Dienstleistungen für die Leistungsbezüger zur Verfügung stellt.
Personendaten	Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen; darunter fallen natürliche wie auch juristische Personen (Art. 3 Bst. a und b DSG).