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.

Inhalt

1. Gesetzliche Rahmenbedingungen

Nahezu alle Kunden der Diartis speichern und verarbeiten besonders schützenswerte Personendaten im Sinne von Art. 5 lit. c. DSG. Im Rahmen von Projekten und Supporttätigkeiten kommt Diartis mit diesen Daten bzw. Datensammlungen in Berührung. In dieser Funktion ist Diartis (zeitweise) **Auftragsbearbeiter** im Sinne von Art. 5 lit. k. DSG / 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. 5 lit. j. DSG / 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.** Im Falle von Kunden, die der DSGVO unterstehen, wird die DSGVO auch auf die Diartis angewendet.

2. Übersicht

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

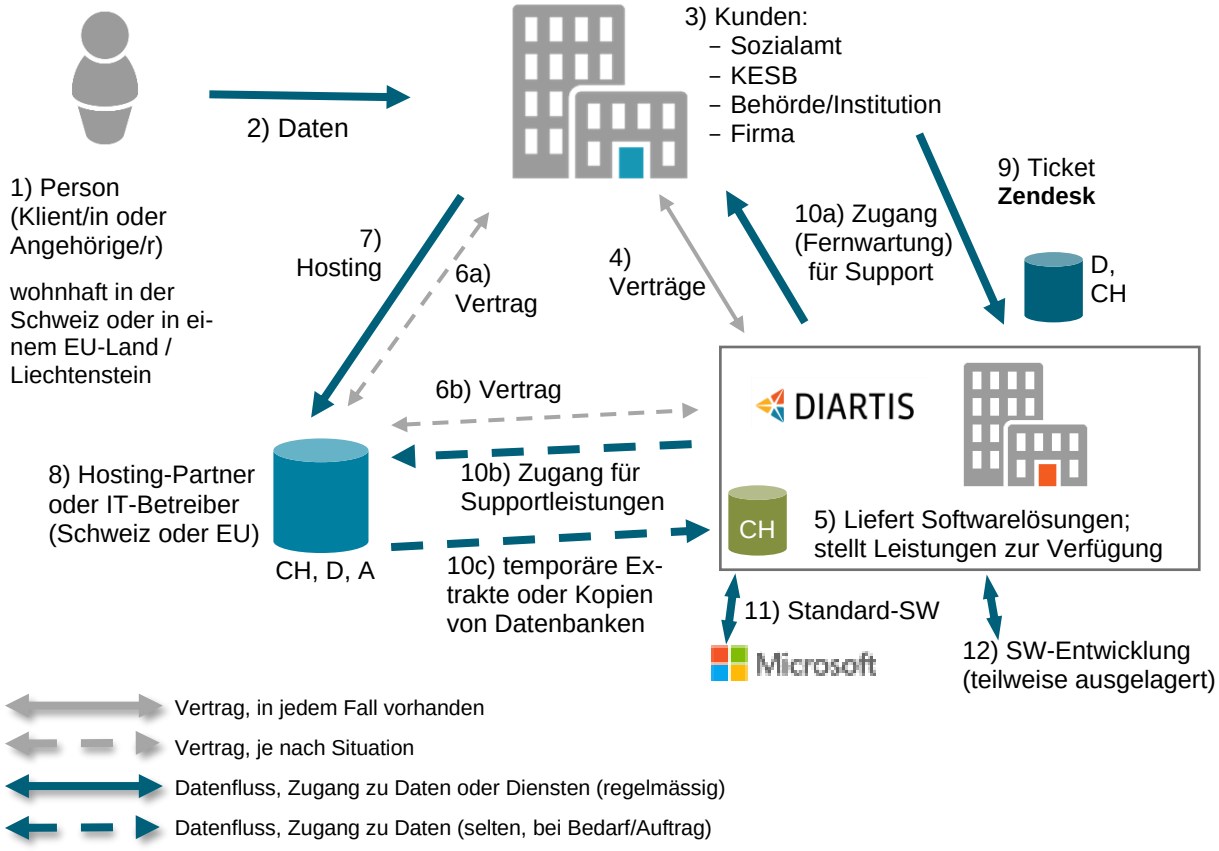

Abbildung 1: Übersicht der Verträge und Datenflüsse

Legende / Erklärungen:

1) Betroffene Personen sind in der Regel Klientinnen und Klienten sowie deren Angehörige in Bezug auf die spezifische Behörde. Mitarbeitende des Kunden sind ebenfalls betroffene Personen, woeit ihre Daten mit derselben Softwarelösung verwaltet werden oder sie Anwender/innen der Software sind.
2) Der Kunde (die Behörde oder Institution) sammelt und verarbeitet Daten über die betroffenen Personen für einen bestimmten Zweck, oft im Rahmen eines gesetzlichen Auftrages.

3) Der Kunde ist in der Regel ein Sozialamt, eine KESB oder eine andere Behörde oder Institution im sozialen Umfeld.
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) an Diartis. Dieses Ticket (bzw. dessen Anhänge) können unter Umständen Fragmente von Daten betroffener Personen enthalten (Screenshots). Die Zendesk-Datenbank ist in Deutschland gespeichert, der Hersteller von Zendesk ist eine US-amerikanische Firma mit Sitz in Irland. Der Kunde ist dafür verantwortlich sicherzustellen, dass er nur so viele Daten preisgibt, wie notwendig.
10) a) Diartis erhält im Auftrag eines Kunden für Supportzwecke über Fernwartung Zugang zu einem Arbeitsplatz des Kunden und kann dabei unter Umständen Einblick in Daten betroffener Personen erhalten.
    b) Nach Genehmigung durch den Kunden greift Diartis über Fernwartung direkt auf die Datensammlung zu, oder der Kunde überträgt eine Kopie der Datenbank über eine verschlüsselte Verbindung an den Kundenbetreuer von 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 von Diartis auf einem dedizierten Server mit Zeitbeschränkungen gespeichert. Der Server wird von Backups ausgeschlossen und es sind nur Mitarbeitende der Diartis zugriffsberechtigt, welche aufgrund ihrer Tätigkeit einen Zugang benötigen. Zusätzlich sind regelmäßige Löschprozesse eingerichtet, um sicherzustellen, dass Datenbanken gelöscht werden, sobald sie nicht mehr für den Auftrag des Kunden benötigt werden.
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 mit Kloon GmbH, Schweiz und Kloon Ltd., Vietnam zusammen. Bei der Software-Entwicklung sind keine Personendaten involviert.

3. Bearbeitungsreglement

3.1. Gesetzliche Grundlage

Gemäss Art. 6 DSG gelten für die Bearbeitung von Personendaten folgende Grundsätze:
[1] Personendaten müssen rechtmässig bearbeitet werden.

[2] Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein.

[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.

[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.

[4] Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.

[5] Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Massnahmen hängt namentlich ab von der Art und dem Umfang der Bearbeitung sowie vom Risiko, das die Bearbeitung für die Persönlichkeit oder Grundrechte der betroffenen Personen mit sich bringt.

[6] Ist die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.

[7] Die Einwilligung muss ausdrücklich erfolgen für:
a. die Bearbeitung von besonders schützenswerten Personendaten;
b. ein Profiling mit hohem Risiko durch eine private Person; oder
c. ein Profiling durch ein Bundesorgan.

In der Zusammenarbeit mit Kunden in der EU / Liechtenstein sind die Verarbeitungsgrundsätze personenbezogener Daten nach Art. 5 DSGVO anwendbar.

3.2. Art der Bearbeitung und Inhalt der Datensammlungen

Diartis bearbeitet Datensammlungen von Kunden mit Daten über betroffene Personen ausschliesslich im Rahmen eines Auftrags und nur für eine begrenzte Zeit:

- Im Rahmen eines Supportauftrags, der mündlich, telefonisch, per E-Mail oder über ein Ticket erteilt wurde, wird in der Regel per Fernwartung auf die Arbeitsplätze der Kunden zugegriffen. Je nach Situation kann auch die Datenbank untersucht werden, wenn dies für die Problembehebung erforderlich ist.
- Wenn eine ausführliche Problemanalyse erforderlich ist, kann der Kunde gebeten werden, Diartis eine Kopie oder einen Auszug der Datenbank für einen begrenzten Zeitraum (in der Regel einige Tage) zur Verfügung zu stellen, damit sie von Diartis untersucht werden kann. Dieser Vorgang wird in geeigneter Weise dokumentiert. Wenn der Kunde nicht selbst Zugang zu diesen Datenbanken hat, wird der IT-Betreiber oder Hosting-Partner des Kunden kontaktiert.
- 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.

In der Regel enthalten diese Datensammlungen 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 immer 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 ohne Einwilligung des Kunden an Dritte weiter und verkauft keine Daten oder Auswertungen von Daten.

3.3. Verantwortlichkeiten

Der Kunde entscheidet allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung der Daten seiner Klienten und Mitarbeitenden. Dadurch ist er in der Rolle des Verantwortlichen. Diartis und andere Leistungserbringer sind Auftragsbearbeiter.
Diartis hat eine Datenschutz-Beauftragte: Frau Ursula Sury, Die Advokatur Sury AG, CH-6005 Luzern.
Interne Ansprechstelle für Datenschutzfragen ist Herr Markus Widmer, Leiter HFC, Diartis AG.
Operative Mitarbeiterin Datenschutz ist Frau Nathalie Dubois, HFC, Diartis AG.
Alle Mitarbeitenden der Diartis haben vor Antritt ihrer Stelle eine Geheimhaltungsverpflichtung 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, erfolgt dies auf einem dedizierten Server, auf welchem die Datensammlungen regelmässig automatisch gelöscht werden. Die Zugriffsberechtigungen werden nach Produkt- und Fachbereich vergeben.

3.4.2. Rollen

Die Rollen sind pro Produktbereich vergeben. Folgende Rollen können in der Ausübung ihrer Tätigkeit Zugriff auf Daten von Kunden haben:

- Services Support
- Services Operations Application
- Services Operations ICT Technik
- Services Operations Data Engineering
- Entwicklung
- Business Analysten

3.4.3. Prozess Zugriffsberechtigung

Beim Eintritt erhalten neue Mitarbeitende spezifische Berechtigungen aufgrund der zugewiesenen Rolle (z.B. Supporter/in) 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 durch Checklisten der Personaladministration und der internen IT-Administration unterstützt.
Die erteilten Berechtigungen werden durch die Applikationsverantwortlichen überprüft.

3.5. Bearbeitung der Personendaten

3.5.1. Geschäftsprozesse

Personendaten von Kunden können in den Geschäftsprozessen Service Desk, Change-Management, Entwicklung sowie Dienstleistungen und Schulungen bearbeitet werden. Die 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 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.

Teilweise erstellen Kunden eine Kopie eines Bildschirmbereichs und hängen diese an ein Zendeskticket an. Bei Zendesk erfolgt die Speicherung der Tickets in der Cloud, die physische Speicherung ist in Deutschland. Die Kunden der Diartis werden angehalten, Stellen mit Klientendaten auf den Bildschirmfotos (Screenshots) 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 verbleiben, 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 Bearbeitungszweck. 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.

3.6.2. Archivierung

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

3.6.3. Löschung

Wenn der Bearbeitungszweck erfüllt ist, werden die Datensammlungen gelöscht. Zudem gibt es einen automatisierten Backup-Löschprozess, der sicherstellt, dass die Löschung nicht vergessen werden kann.

3.7. Technische und organisatorische Massnahmen

Diartis schützt die technische Server- und Netzwerkinfrastruktur durch geeignete Massnahmen, die kontinuierlich aktuell gehalten werden. Dabei greift das Unternehmen sowohl auf qualifiziertes internes Personal als auch auf die Ressourcen eines erfahrenen IT-Anbieters zurück.
Die Rollen, Aufgaben, Kompetenzen und Stellvertretungen sind in einem Dokument beschrieben, das allen Mitarbeitenden bekannt ist.
Die Einhaltung der Massnahmen wird durch ein jährlich stattfindendes Datenschutzaudit überprüft, das von der Datenschutzbeauftragten (vgl. Kap. 3.3) durchgeführt wird.

3.8. Privacy by Design und Privacy by Default

Diartis unterstützt ihre Kunden in der Umsetzung von Privacy by Design und by Default im Rahmen von Softwareentwicklungen und individualisierten Projekten.

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 25. September 2020 über den Datenschutz (DSG)
Verordnungen	Verordnung vom 31. August 2022 über den Datenschutz (DSV)
EU-Verordnung	Datenschutz-Grundverordnung der Europäischen Union (DSGVO)
Website-Infos und weitere relevante Diartis-Weisungen und Reglemente	https://www.diartis.ch/diartis/datenschutz

4.2. Abkürzungen

Abkürzung	Bedeutung
Art.	Artikel
DSG	Bundesgesetz über den Datenschutz (SR 235.1)
DSGVO	Datenschutz-Grundverordnung
Diartis	Diartis AG – Mit «Diartis» ist in diesem Dokument ausschliesslich die Diartis AG gemeint. Das Dokument gilt nicht für weitere Diartis Gesellschaften.
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
IT	Information Technology, Informationstechnologie
KESB	Kindes- und Erwachsenenschutzbehörde
QMS	Qualitätsmanagementsystem
SW	Software

4.3. Begriffe

Begriff	Bedeutung
Bearbeiten	Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten (siehe Art. 5 lit. d. DSG).
Bekanntgeben	Das Übermitteln oder Zugänglichmachen von Personendaten (Art. 5 lit. e. DSG).
Besonders schützenswerte Personendaten	Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, genetische Daten, biometrische Daten, die eine natürliche Person eindeutig identifizieren, Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen und Daten über Massnahmen der sozialen Hilfe (Art. 5 lit. c. DSG).
Hosting-Partner	Eine privatwirtschaftliche Firma, welche gegen Bezahlung Server, Speicherplatz, Netzwerke, Datenbanksysteme, Applikationen und Dienstleistungen zur Verfügung stellt.

Verantwortlicher	Private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet (Art. 5 lit. j. 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 natürliche Person beziehen (Art. 5 lit. a. DSG)