

1 Grundlegende Bestimmungen

1.1 Zweck und Geltungsbereich

Im Gesundheitswesen herrschen im Umgang mit medizinischen Daten verschärfte Datenschutzbestimmungen. Als Anbieterin von datenbezogenen Dienstleistungen im Gesundheitswesen (Verschlüsselung, Transport, Zugriffskontrolle) anerkennt HIN (Health Info Net AG, Winterthur) die besondere Relevanz des Schutzes personenbezogener Daten im medizinischen Bereich.

Für Personendaten, die für Aufbau und Erhalt der Beziehungen zu den Kundinnen und Kunden des Unternehmens angelegt werden, gilt die für Unternehmen in Ausführung ihrer Tätigkeit übliche Praxis, hingegen gibt es keine branchenspezifischen Einschränkungen.

Die vorliegende Richtlinie zum Datenschutz regelt den Umgang von HIN mit Personendaten. Sie soll transparent machen, welche Daten zu welchem Zweck gespeichert werden, und wer darüber verfügt oder Einsicht hat.

1.2 Rechtliche Grundlagen

Rechtliche Grundlage bildet das Schweizer Recht, insbesondere die Bestimmungen über Datenschutz (DSG, VDSG). Darüber hinaus gelten spezielle Bestimmungen für Internet-Service-Provider. Für abgeschlossene Verträge gilt das Schweizer Obligationenrecht. Neben dem jeweiligen Vertragsinhalt sind die Allgemeinen Geschäftsbedingungen, die Rahmenbestimmungen für die elektronische Datenkommunikation von HIN und die Leistungsbeschreibungen der jeweiligen Produkte als Vertragsbestandteil ebenfalls bindend.

1.3 Grundsätze der Datenbearbeitung

Personendaten sind „alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen“¹. Für die Bearbeitung solcher Daten (beschaffen, aufbewahren, verwenden, umarbeiten, bekanntgeben, archivieren oder vernichten) formuliert HIN folgende Grundsätze:

- § HIN legt nur Datensammlungen an, die für den angegebenen Zweck notwendig sind.
- § HIN sorgt für den sicheren Transport von Daten und E-Mails. Dazu werden die Hülldaten einer Transaktion gespeichert. Inhalte von Transaktionen werden nur im Rahmen automatischer Server-Backups gespeichert.
- § HIN verkauft keine Daten an Dritte.
- § HIN kauft keine widerrechtlich angelegte Sammlung von Personendaten.
- § HIN gibt keine Personendaten an Dritte weiter, ausser wenn dies für die Erbringung einer vertraglichen Dienstleistung am Kunden nötig ist.
- § Dieser Fall ist in der Leistungsbeschreibung des jeweiligen Produktes geregelt.
- § Jede Person, deren Daten HIN bearbeitet, kann vom Auskunftsrecht Gebrauch machen.
- § HIN muss begründen, wenn dieses Auskunftsrecht im Einzelfall eingeschränkt wird.

¹ Art. 3 lit. a DSG

Richtlinie zur Datenbearbeitung

Umgang mit Personendaten bei Health Info Net AG (HIN)



2 Datenhaltung bei HIN

2.1 Datensammlungen

Nachfolgend sind die für den Betrieb, Administration, Kommunikation mit den Kundinnen/Kunden und gesetzlich notwendigen Datensammlungen aufgeführt, die von HIN angelegt werden. Für jede Datensammlung ist festgelegt, zu welchem Zweck sie angelegt wurde, wer auf die Daten zugreifen und diese bearbeiten kann und ob diese unter strengen Bedingungen (siehe Kapitel 4.2) an HIN Vertragspartner weitergegeben werden.

<p>Kundenstammdaten (Administration & Kundendienst)</p>	<p>§ Zweck der Datensammlung: Pflege der Kundenbeziehung</p> <p>§ Bearbeitung und Zugriff durch HIN Mitarbeitende</p> <p>§ Weitergabe nur an Vertragspartner zur Erbringung einer bestimmen vertraglich vereinbarten Leistung</p>
<p>Kontaktinformationen für die HIN Identität als Teilbereich der Kundenstammdaten (HIN Identität, HIN Teilnehmerverzeichnis)</p>	<p>§ Zweck der Datensammlung:</p> <ul style="list-style-type: none"> ○ Anbieten von Verzeichnisdiensten für HIN Teilnehmende, opt out durch Kunde möglich z.B. Testabo ○ Notwendige Grundfunktion einer PKI-basierenden Identitäts- und Rechtemanagement-Plattform <p>§ Bearbeitung und Zugriff durch HIN Mitarbeitende</p> <p>§ Weitergabe nur an Vertragspartner zur Erbringung einer bestimmen vertraglich vereinbarten Leistung</p>
<p>HIN E-Mail-Adresse (wichtiges Element der Kontaktinformationen)</p>	<p>§ Zweck der Datensammlung:</p> <ul style="list-style-type: none"> ○ Pflege der Kundenbeziehung ○ Anbieten von Verzeichnisdiensten für HIN Teilnehmende; opt out durch Kunde möglich <p>§ Bearbeitung durch HIN Mitarbeitende</p> <p>§ Einsicht für alle HIN Teilnehmende über den geschützten Bereich des HIN Teilnehmerverzeichnis</p>
<p>Produktbezogene Daten, Verträge, Rechnungsdaten (Administration & Kundendienst)</p>	<p>§ Zweck der Datensammlung: Erfüllung von vertraglichen Leistungen</p> <p>§ Bearbeitung und Zugriff nur durch HIN Mitarbeitende</p> <p>§ Weitergabe nur an Vertragspartner zur Erbringung einer vertraglich vereinbarten Leistung</p>
<p>Daten über erfolgte Kundenkontakte und Korrespondenz (Administration & Kundendienst)</p>	<p>§ Zweck der Datensammlung: Pflege der Kundenbeziehung z.B. technische Supportfälle oder administrative Anliegen</p> <p>§ Bearbeitung und Zugriff nur durch HIN Mitarbeitende</p> <p>§ Weitergabe: keine</p>

Richtlinie zur Datenbearbeitung

Umgang mit Personendaten bei Health Info Net AG (HIN)



Datensammlungen mit unveränderbaren Daten

Konnektionsdaten	<ul style="list-style-type: none">§ Zweck der Datensammlung: Betrieb der Applikationen und Erfüllung gesetzlicher Pflichten für Internet Service Provider§ Bearbeitung: keine, keine Veränderung möglich§ Zugriff nur durch speziell berechnigte HIN Mitarbeitende§ Weitergabe: keine
HIN Audit Trail-Daten	<ul style="list-style-type: none">§ Zweck der Datensammlung:<ul style="list-style-type: none">○ Sicherstellung der Nachvollziehbarkeit aller Transaktionen auf der HIN Plattform○ Zentrales Hilfsmittel zur Beurteilung der Einhaltung der HIN Security Policies○ Wichtiges Element zur Verhinderung von Missbrauch der HIN Plattform§ Nur Personen mit einer der folgenden Rollen haben Einsichtsrecht:<ul style="list-style-type: none">○ HIN Security Officer○ HIN Support und HIN Betrieb○ HIN Kunde, ausschliesslich Einsichtsrechte in den eigenen Audit Trail○ Dritte auf gerichtliche Anordnung hin§ Bearbeitung: keine, keine Veränderung möglich§ Weitergabe: keine

2.2 Technischer Schutz von Daten

HIN trifft organisatorische und technische Vorkehrungen zum Schutz der angelegten Datensammlungen. Der Schutz umfasst folgende Risiken:

- § unbefugte oder zufällige Vernichtung;
- § zufälliger Verlust;
- § technische Fehler;
- § Fälschung, Diebstahl oder widerrechtliche Verwendung;
- § unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen.

Die getroffenen Massnahmen werden laufend dem neuen Stand der Technik angepasst.



3 Umgang mit Personendaten bei HIN

3.1 Wer arbeitet mit Personendaten?

Die in Kapitel 2.1 beschriebenen Datensammlungen werden aufgrund der Angaben bei der Anmeldung der HIN Teilnehmenden resp. bei der Nutzung der HIN Dienste angelegt. Die bei der Anmeldung gemachten Angaben werden von HIN im Rahmen der Qualitätssicherung vor der Freischaltung des HIN Abo auf Korrektheit überprüft. Für das Gesundheitswesen relevante und wichtige Daten werden in den zentralen Registern und Listen überprüft.

Verschiedene Aktivitäten des operativen Betriebs wie das Pflegen der Kundenbeziehung, der technische Betrieb, die Verrechnung der Dienstleistung und der Korrespondenz erfordern die Nutzung dieser Daten. Die Nutzung findet in unterschiedlichen Organisationseinheiten statt: HIN Calldesk, HIN Backoffice, HIN Support, HIN Management, HIN Rechenzentrum.

Die beschriebenen Aktivitäten werden durch das Personal von HIN ausgeführt. Dieses untersteht der Schweigepflicht, welche arbeitsvertraglich geregelt ist.

3.2 Wer darf Personendaten mutieren?

Eine Person darf nur die Daten mutieren, die sie selber betreffen. Jede Person, die in den in Kapitel 2.1 beschriebenen, veränderbaren Datensammlungen geführt wird, hat folgende Rechte:

Recht auf Auskunft

Jede Person, deren Daten HIN bearbeitet, kann vom Auskunftsrecht Gebrauch machen. Es gelten auch die im Gesetz genannten Einschränkungen des Auskunftsrecht², insbesondere gewährt HIN keinen Einblick in Schriftverkehr zwischen / mit Drittpersonen oder Mitarbeitenden.

Recht auf Korrektur

Falsche oder unkorrekte Angaben dürfen von einer Person oder dem Rechtsvertreter dieser Person jederzeit beanstandet und deren Änderung verlangt werden.

Speziell für Firmen

Mitarbeiter von Firmen können ebenfalls HIN Teilnehmende sein. Sofern es klar ist, dass diese Personen nur als Organ einer Firma eine Kundenbeziehung zu HIN haben, kann die Firma über die betroffenen Verträge und Daten verfügen.

Sofern nicht klar festzustellen ist, dass ein Vertrag nicht ausschliesslich im Namen der Firma abgeschlossen wurde, dürfen Mutationen nur mit Zustimmung der Inhaber des betreffenden Vertrags durchgeführt werden.

3.3 Vorgehensweise für die Mutation von Personendaten

Die Änderungen von Angaben, die eine Person betreffen, sind bei HIN schriftlich einzureichen. Dies gilt sowohl für Vertragsänderungen oder –kündigungen als auch für Adressänderungen. Diese Regelung gilt zum Schutz der HIN Teilnehmenden vor unerlaubten Eingriffen Dritter.

² Art. 8 DSGVO und Art. 9 DSGVO



4 Weitergabe von Personendaten

4.1 Grundsätze zur Weitergabe von Personendaten

Grundsätzlich gibt HIN keine personenbezogenen Daten weiter. Personenbezogene Daten werden weder verkauft noch Partnerorganisationen zugänglich gemacht. Dennoch ist eine Weitergabe von Personendaten an Vertragspartner von HIN in speziellen Fällen möglich. Diese Fälle sind mit Datenschutzverträgen verbindlich geregelt.

4.2 Bedingungen für Ausnahmen

Für eine Weitergabe von Personendaten an Vertragspartner von HIN müssen folgende Voraussetzungen kumulativ erfüllt sind:

- § Die Weitergabe von Personendaten ist nur dann zulässig, wenn der Empfänger mit HIN ein Abkommen unterzeichnet haben, das den Schutz der übermittelten Daten sicherstellt.
- § Die Weitergabe von Personendaten ist nur dann zulässig, wenn sie zweckgebunden erfolgt, d.h. in besagtem Vertrag ist abschliessend geregelt, zu welchem Zweck die Daten weitergegeben werden und für welchen Zweck sie verwendet werden dürfen.
- § Die Weitergabe von Personendaten ist nur dann zulässig, wenn der Umfang der weitergegebenen Daten den für den definierten Zweck benötigten Umfang nicht übersteigt.

Ausgenommen von diesen Bedingungen sind Anfragen zur Weitergaben von Daten, die aufgrund einer gesetzlichen Grundlage erfolgen.