Konzept Datensicherheit und Datenschutz

HPD Graubünden
Geschäftsstelle
Aquasanastrasse 12
7000 Chur

www.hpd-gr.ch
info@hpd-gr.ch

Grundlage	Mastervorlage Verband der Heilpädagogischen Dienste der Schweiz VHDS, erarbeitet von der Firma: OTB Applications GmbH / Herbert Knutti
Projektleitung Mastervorlage	Angela Hepting, Elke Bernhardt
Erarbeitung	Dezember 2022 – März 2023
Adaption für HPD GR	Angela Hepting
Schreibweise	Es werden nach Möglichkeit geschlechterneutrale Begriffe verwendet (Lernende) und wo nicht möglich die Genderschreibweise mit einem Doppelpunkt gewählt (Betreuer:in) Ausnahmen sind alle Begrifflichkeiten, die aus Gesetzes- und Verordnungstexten stammen. Um Missverständnisse zu vermeiden, werden diese wie in den gesetzlichen Vorlagen verwendet. Der Begriff «Erziehungsberechtigte» wird stellvertretend für alle Personen eingesetzt, die im rechtlichen Sinne das Sorgerecht inne haben und die Rechte der Kinder juristisch vertreten.
Version	Januar 2024

VHDS Verband Heilpädagogischer Dienste Schweiz

OTB OUTSIDE THE BOX Applications

Datensicherheit und Datenschutz

Datenschutzkonzept HPD GR

INHALT

DATENSCHUTZKONZEPT

1 Zweck und Umfang

Das vorliegende Datenschutzkonzept des Heilpädagogischen Dienstes Graubünden beschreibt den Auftrag und die Massnahmen zum Schutz der Privatsphäre und der Persönlichkeitsrechte der Kinder/Jugendlichen, der Erziehungsberechtigten, der Mitarbeitenden und allfällig anderen Personen, die mit dem Dienst zusammenarbeiten.

Die Aussagen des Konzepts betreffen folglich:

- Personendaten der Kinder/Jugendlichen sowie der Erziehungsberechtigten;
- Personendaten der Mitarbeitenden, inklusive Daten von Stellenbewerber:innen und ehemaligen Mitarbeitenden;
- Informationen über Geschäfts- und Kooperationspartner:innen, soweit Personendaten betroffen sind.

Dieses Konzept soll alle im Heilpädagogischen Dienst Graubünden tätigen Personen darin unterstützen, datenschutzrechtlich einwandfrei zu handeln. Das Konzept gilt als verbindliche Richtlinie und wurde daher vom Stiftungsrat genehmigt. Das Konzept wirkt in diesem Sinne präventiv in Bezug auf die Verletzung des Datenschutzrechtes. Zudem wird mit dem Konzept der Informationspflicht Rechnung getragen, die gegenüber betroffenen Personen in Bezug auf die Datensicherheit besteht.

2 Gesetzliche Grundlagen

Grundlage für dieses Konzept sind das Bundesgesetz 235.1 über den Datenschutz (rev. Datenschutzgesetz, rev. DSG) und die Verordnung 235.11 über den Datenschutz (rev. Datenschutzverordnung, rev. DSV) vom 31. August 2022 (Stand am 1. September 2023).

Der Heilpädagogische Dienst Graubünden untersteht auf Grundlage des Leistungsauftrags mit dem Kanton/Amt für Volksschule und Sport, dem kantonalen Datenschutzgesetz.

3 Geltungsbereich

Das vorliegende Datenschutzkonzept gilt für alle Organe und Mitarbeitenden des Heilpädagogischen Dienstes Graubünden, die Personendaten bearbeiten.

Es gilt ebenfalls für externe Dienstleister:innen, welche im Auftrag des Heilpädagogischen Dienstes Graubünden Personendaten bearbeiten.[1] Derartige Dienstleistungen werden in jedem Fall vertraglich geregelt.

[1] Unter Bearbeiten wird insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten verstanden.

4 Verantwortliche Personen

Bereichsleitung Finanzen/Dienste

5 Grundsätze

Der Heilpädagogische Dienst Graubünden ist folgenden Grundsätzen des Datenschutzes verpflichtet:

5.1 Rechtmässigkeit

Die Art und Weise der Datenbearbeitung wird gegenüber den betroffenen Personen kommuniziert. Sie ist dann rechtmässig, wenn eine Einwilligung der betroffenen Person vorliegt. Ausnahmen sind im Rahmen eines Strafverfahrens oder im Zusammenhang mit Abklärungen durch die Kindes- und Erwachsenenschutzbehörde (KESB) aufgrund der Mitwirkungspflicht möglich.

5.2 Verhältnismässigkeit

Der Zweck der Bearbeitung ist durch den Auftrag des Heilpädagogischen Dienst Graubünden legitimiert, welcher im Leistungsauftrag mit dem Kanton GR und den Rahmenverträgen mit den Schulträgerschaften definiert ist. Die Bearbeitung muss verhältnismässig zu diesem Zweck erfolgen. Personendaten (Personalangaben und sämtlich Unterlagen im Kinderdossier) werden nach der festgelegten Frist vernichtet resp. professionell gelöscht. Es werden keine Daten erhoben, die für die Erfüllung des Zwecks nicht notwendig sind.

5.3 Datenqualität

Es wird sichergestellt, dass die bearbeiteten Daten richtig, vollständig und aktuell sind. Unrichtige und unvollständige Daten sind zu korrigieren oder zu vernichten. Fehlende Daten werden ergänzt.

5.4 Transparenz

Daten werden, wo immer möglich, direkt bei den betroffenen Personen erhoben. Diese werden über die Erhebung der notwendigen Daten und die Art der Bearbeitung informiert. Diese Informationen erfolgen präzise und in verständlicher Form.

5.5 Sicherheit und Verfügbarkeit

Daten werden vor Verlust, Diebstahl und missbräuchlicher Bearbeitung geschützt. Digitale Daten können bei einem Systemabsturz wiederhergestellt werden.

5.6 Vertraulichkeit

Nur berechtigte Personen haben auf jene Daten Zugriff, die sie zur Erfüllung ihres Auftrages benötigen. Es ist nachvollziehbar, wer welche Daten bearbeiten kann und bearbeitet hat.

6 Datensicherheit: Massnahmen

Zugang zu Personendaten besteht beim Heilpädagogischen Dienst Graubünden nach dem Grundsatz «so viel wie nötig, so wenig wie möglich».

Mit personellen, organisatorischen und Massnahmen zur IT-Sicherheit wird der Datenschutz gewährleistet. Personendaten sind geschützt vor Missbrauch, Vernichtung, Verlust, Fälschung, Diebstahl und vor dem Zugang Unbefugter.

6.1 Personen und Funktionen

6.1.1 Stiftungsrat

Der Stiftungsrat ist auf strategischer Ebene für die Gewährleistung des Datenschutzes verantwortlich. Er hat die Geschäftsleitung beauftragt ein Konzept zum Datenschutz und zur Datensicherheit zu erstellen und eine:n Datenschutzverantwortliche:n zur Wahl vorzuschlagen.

Das vorliegende Konzept wurde vom Stiftungsrat genehmigt und am 09.02.2024 in Kraft gesetzt. Datenschutzverantwortliche/r ist die Bereichsleitung Finanzen/Dienste. Der Stiftungsrat sorgt für die notwendigen Ressourcen.

6.1.2 Datenschutzverantwortliche:r

Ins Aufgabengebiet der für die Datensicherheit verantwortlichen Person gehören insbesondere:

- die (jährliche) Rechenschaftspflicht zum Datenschutz und zur Datensicherheit gegenüber der Geschäftsleitung und gegenüber dem Stiftungsrat
- die Auskunftspflicht gegenüber den betroffenen Personen
- die Aufsicht über die Einhaltung der Massnahmen zur Datensicherheit
- die (Mit-)Verantwortung für die Umsetzung der im Konzept oder anderen Quellen beschlossenen Massnahmen zur Steigerung der Datensicherheit
- die Aktualisierung der Dokumentation über alle Formen der Datenbearbeitung und der umgesetzten Massnahmen
- die Festlegung – gemeinsam mit den Führungspersonen – von Berechtigungen im Umgang mit Personendaten
- die Erstellung von internen Weisungen und Merkblättern zur Datensicherheit
- die Schulung der Mitarbeitenden im Bereich der Datensicherheit
- die interne Beratung
- die Prüfung der Risiken bei einer geplanten Umstellung der (digitalen) Prozesse rund um die Datenbearbeitung
- das Einholen von Informationen bei der kantonalen Datenschutzstelle bei ungeklärten Fragen
- die (Mit)-Unterzeichnung von Aufträgen an Dritte bezüglich der Bearbeitung von Personendaten
- die (Mit)-Unterzeichnung von Verträgen zur Datensicherheit, insbesondere mit Versicherungen
- die Erarbeitung von Richtlinien bezüglich Archivierung, Anonymisierung und/oder Löschung von Daten
- die umgehende Informationspflicht gegenüber der Geschäftsleitung und dem Stiftungsrat bei Ereignissen (Angriffen), welche von grosser finanzieller, technischer und personeller Tragweite sind oder das Potential dazu haben

- die Meldepflicht gegenüber den Behörden bei der Verletzung der Datenschutzrichtlinien oder bei Angriffen von aussen

6.1.3 Bereichsleitungen

Die Bereichsleitungen der Fachbereiche sowie die Leitung Sekretariat sind zusammen mit der/dem Datenschutzverantwortlichen (Bereichsleitung Finanzen/Dienste) für die Umsetzung des vorliegenden Konzepts verantwortlich. Die Bereichsleitungen sowie die Leitung Sekretariat haben insbesondere folgende Aufgaben:

- Auskunftspflicht gemässe Raster «Zuständigkeiten Datenschutz» gegenüber den betroffenen Personen
- Festlegung – gemeinsam mit der/dem Datenschutzverantwortlichen - von Berechtigungen im Umgang mit Personendaten
- Mitarbeit beim Erstellen von internen Weisungen und Merkblättern zur Datensicherheit
- Organisation der Schulung der Mitarbeitenden im Bereich der Datensicherheit
- Mitarbeit bei der Prüfung der Risiken bei einer geplanten Umstellung der (digitalen) Prozesse zur Bearbeitung von Personendaten
- Erarbeitung von Richtlinien bezüglich Archivierung, Anonymisierung und/oder Löschung von Daten
- Förderung von Mitarbeitenden im Bereich Datenschutz und Datensicherheit
- Meldepflicht gegenüber dem/der Datenschutzverantwortlichen bei der Verletzung der Datenschutzrichtlinien oder bei Angriffen von aussen

Die Bereichsleitung Finanzen/Dienste ist für die Bearbeitung der Personendaten der Mitarbeitenden im Rahmen der Personalarbeit verantwortlich. Sie arbeitet in Bezug auf den Datenschutz eng mit dem:r Datenschutzverantwortlichen zusammen.

6.1.4 Mitarbeitende

Alle Mitarbeitenden des Heilpädagogischen Dienstes Graubünden, welche Personendaten bearbeiten, tragen dem Datenschutz eigenverantwortlich Rechnung und handeln dabei gemäss unterzeichnetem Kodex, dem vorliegenden Konzept und den Weisungen der/des Datenschutzverantwortlichen.

Sie wenden sich bei Fragen und Unsicherheiten an ihre:n Vorgesetzten oder an die:den Datenschutzverantwortliche:n. Insbesondere haben sie folgende Aufgaben:

- Befolgen des Grundsatzes der absoluten Sorgfaltspflicht gegenüber Personendaten
- Teilnahme an internen Schulungen zur Datensicherheit
- Befolgen der Weisungen des Heilpädagogischen Dienstes Graubünden bezüglich des Datenschutzes und der Datensicherheit und Unterzeichnung des entsprechenden Verhaltenskodex

- Klärung offener Fragen zum Datenschutz und zur Datensicherheit mit den Vorgesetzten und der dafür verantwortlichen Person
- Beitrag durch Beobachtungen, Beispielen und Fragestellungen aus der Praxis zur Weiterentwicklung der Datensicherheit
- Klärung der Datenweitergabe mit Erziehungsberechtigten/Jugendlichen

Weisungen

Grundsätzlich werden keine Daten Dritter (z.B. Arztberichte etc.) weitergegeben. In begründeten Fällen ist mit der Einwilligung der Erziehungsberechtigten eine Ausnahme möglich.

Die «Vollmacht Datenweitergabe/Besuche» hat Gültigkeit während der Dauer der laufenden Verfügung für Daten, welche im Rahmen des Leistungsauftrags im HPD erhoben werden.

Für die Weitergabe von Daten nach Ablauf der Verfügung müssen die Erziehungsberechtigten angefragt werden. Mündliche Zustimmung werden sicherheitshalber durch den/die MA HPD/SEK HPD mit einer Notiz festgehalten.

Kinder mit Doppelmassnahmen

Finden zeitgleich Doppelmassnahmen statt, soll dies intern den zuständigen MA bekannt sein. Die Erziehungsberechtigten sind informiert, dass man von der Doppelmassnahme Kenntnis hat.

Für die Weitergabe von Daten zwischen den Fachdisziplinen ist die reguläre Zustimmung der Erziehungsberechtigten notwendig.

Besuche im Therapiezimmer

Mitglieder von Behörden, Aufsichtsinstanzen und Fachstellen sowie Praktikantinnen und Praktikanten können Therapiesitzungen besuchen, sofern eine Rechtsgrundlage besteht oder wenn die ausdrückliche Einwilligung der betroffenen Kinder und Jugendlichen, bzw. deren gesetzlichen Vertretung vorliegt. Hierfür dient die «Vollmacht Datenweitergabe/Besuche».

Antragstellung und Berichterstattung für sonderpädagogische Massnahmen

Die Datenweitergabe und der Informationsfluss müssen gegenüber dem Amt für Volksschule und Sport (AVS) bzw. der Entscheidungsinstanz umfassend sein. Für das Ausweisen des Bedarfs für die Massnahme nicht relevante Daten dürfen nicht erfasst werden.

Auskünfte an einen geschiedenen oder getrenntlebenden Elternteil

Der Elternteil, welcher nicht die elterliche Sorge ausübt, hat in gleicher Weise das Recht, Auskünfte über den Entwicklungsstand und die Förderung des Kindes oder Jugendlichen zu erhalten, wie jener Elternteil, welcher die elterliche Sorge ausübt (Art. 275a ZGB).

Auskünfte an die KESB, die Berufsbeistandschaft

Bei Vorliegen einer Entbindungserklärung dürfen sowohl die Kinder- und Erwachsenenschutzbehörde (KESB) als auch der Berufsbeistandschaft Informationen weitergegeben werden.

Der Beiständin/dem Beistand dürfen gemäss ihren Kompetenzen in der Ernennungsurkunde ebenfalls Informationen weitergegeben werden. Die Ernennungskurkunde muss dem HPD vorliegen.

Bei Unklarheiten ist die Geschäftsführung HPD oder die zuständige KESB zu kontaktieren.

Austausch von Informationen zwischen medizinischen Fachpersonen, Fachstellen, Lehrpersonen, Schulbehörden und sonstigen Dritten

Die Weitergabe von Personendaten sowie das Einholen von Berichten und Informationen bedürfen einer Rechtsgrundlage oder der ausdrücklichen Einwilligung der betroffenen Kinder und Jugendlichen, bzw. deren gesetzlichen Vertretung. Hierfür dient die «Vollmacht Datenweitergabe/Besuche».

Lehrpersonen werden keine Berichte ausgehändigt. Die Lehrpersonen erhalten über die Schulleitung Einsicht.

6.2 Datensammlung, Zugriffsregelung, Risikobeurteilung und Massnahmen zur Sicherheit

Im Folgenden werden die bestehenden Datensammlungen mit den festgelegten Zugriffsregelung aufgeführt und mögliche Risiken mit Massnahmen zu deren Minimierung definiert. Daten werden physisch und digital gespeichert.

a) <u>Kinder/Jugendliche und Erziehungsberechtigte</u>

- **Kinderakte:** Von jedem Kind/Jugendlichen wird eine Kinderakte geführt. Diese kann physisch oder digital abgelegt sein. Neben den Stammdaten sind dort sämtliche Vereinbarungen mit den Erziehungsberechtigten, Berichte von externen und internen Stellen, Gesprächsprotokolle, Förderpläne sowie Gesprächs- und Aktennotizen abgelegt. Dabei werden auch die Kontaktdaten von wichtigen Bezugspersonen erfasst (Erziehungsberechtigte, Beistand/Beiständin etc. erfasst).

  Erfassungen von Grenzverletzungen mittels Erfassungsformular Bündner Standard werden bei der Geschäftsführung physisch und/oder digital abgeschlossenen resp. passwortgeschützt abgelegt und während 50 Jahren aufbewahrt.

  Zugriff und Sicherheit <u>physische</u> Kinderakte: Die physischen Kinderakten werden im Sekretariat (Erdgeschoss) abgeschlossen aufbewahrt. Zugriff haben die zuständigen Mitarbeitenden, die Geschäftsleitung, die Mitarbeitenden des Sekretariats sowie die Fachleitungen zu den Dossiers ihres Fachbereichs. 10 Jahre nach Abschluss der Massnahme wird die Kinderakte sicher und vollständig vernichtet. Die Erziehungsberechtigten/volljährigen Jugendlichen sind jederzeit dazu berechtigt, Einsicht in die Kinderakte nehmen und diese zu erhalten.

  Handakte: Während der Massnahme können die Mitarbeitenden eine physische Kinderakte (Handakte) führen. Während der laufenden Massnahme ist sie sicher und vor dem Zugriff von Dritten geschützt mitzuführen resp. aufzubewahren. Die Handakte wird nach Beendigung der Massnahme sicher und vollständig vernichtet. Sie kann zur Vernichtung im SEK HPD abgegeben werden.

- **Risiko physische Kinderakte:** Es gibt kein Backup der Papierdaten. Bei einem Feuer oder Wasserschaden könnten die Daten nicht oder nur teilweise wieder hergestellt werden. Die Aktualität der Daten ist nicht gewährleistet, wenn Mitarbeitende neue Dokumente nicht tagesaktuell dem Sekretariat zur Einordnung abgeben.

- **Massnahmen physisch Kinderakte:** Abschliessbare Räumlichkeiten und Aufbewahrungsmöbel, Schlüsselmanagement, baulicher Schutz vor Wasser und Feuer

  Zugriff und Sicherheit digitale Kinderakte: Die digitalen Kinderakten sind passwortgeschützt auf einer SharePoint-Plattform gespeichert.

  Zugriff haben die zuständigen Mitarbeitenden, die Geschäftsführung, die Mitarbeitenden des Sekretariats sowie die Fachleitungen zu den Dossiers ihres Fachbereichs.

  10 Jahre nach Abschluss der Massnahme wird die Kinderakte sicher und vollständig vernichtet. Die Erziehungsberechtigten/volljährigen Jugendlichen sind jederzeit dazu berechtigt, Einsicht in die Kinderakte nehmen und diese zu erhalten.

  Das Login auf die SharePoint-Plattform erfolgt über eine Authentifizierung mittels User-Name (Mailadresse) und Passwort. Die Server erstellen automatisch einmal pro 24h (Nacht) ein Backup und zusätzlich einmal pro Woche ein Wochenbackup.

  Speichern auf privaten Geräten: Es ist den Mitarbeitenden erlaubt, Berichte und Protokolle auf privaten Geräten zu verfassen, wenn sie kein Gerät des Heilpädagogischen Dienstes nützen können oder wollen. Der Download auf einen passwortgeschützten Stick (des HPD GR) oder ein Gerät ist im Prinzip möglich und damit der Kontrolle durch den Dienst enthoben.

  Die Mitarbeitenden versichern mit der Unterzeichnung des Kodex zur Datensicherheit, dass sie Daten auf privaten Geräten nicht an Dritte weiterreichen resp. für niemanden anderes zugänglich sind und die privaten Geräte vor dem Zugriff Dritter geschützt sind.

  Spätestens nach Beendigung der Massnahme werden sämtliche Dateien (Dokumente, Video-Audioaufnahmen, Fotos), die das Kind betreffen, auf den privaten Geräten gelöscht.

  Austretende Mitarbeiterinnen verlieren mit dem Austritt ihren Zugriff auf die Daten (SharePoint, Lobos, OneDrive). Bei Problemen oder einem allfälligen Systemabsturz stehen der/dem Datenschutzverantwortlichen und der Geschäftsleitung der Support der Firma 2sic zur Verfügung.

  Den Mitarbeitenden steht der Support durch den Leiter Rechnungswesen/Dienste zur Verfügung. Diese:r kann bei Bedarf professionellen Support beiziehen.

  Praktikant:innen verfügen über keine Rechte. Die zuständige Praktikumsleitung gewährt den unter Schweigepflicht stehenden Praktikant:innen den notwendigen Einblick in die Kinderakte. Informationen daraus dürfen nur anonymisiert weiterverwendet werden.

- **Risiko digitale Kinderakte:** Versagen Backup, Passwortmissbrauch, widerrechtlicher Zugang auf private Geräte; ungenügend geschützte private Geräte

- **Massnahmen digitale Kinderakte:** Mehrfachbackup auf Server intern, extern, datenschutzkonforme Cloud-Lösung, Ablage auf Server in der Schweiz

b) Mitarbeitende

- **Personalakte/Kontaktdaten:** Von sämtlichen Mitarbeitenden wird eine Personalakte geführt. Diese kann digital und/oder physisch abgelegt sein.

  Die Personalakte beinhaltet Bewerbungsunterlagen, Personalienblatt, Arbeitsverträge inkl. Zusatzdokumente wie Strafregisterauszug und Sonderprivatauszug, Stellenbeschrieb, Protokolle der Mitarbeitergespräche, Protokolle Praxisbesuche, Angaben zu Absenzen/Arztzeugnisse, Schadenmeldungen, Versicherungsunterlagen, Aktennotizen, Vereinbarungen, bewilligte Weiterbildungsgesuche.

  Personaldaten: Von Mitarbeitenden werden Adresse, Geburtsdatum, Telefonnummer sowie Bankkontakte elektronisch auf dem eigenen Server sowie im Buchhaltungsprogramm Lobos gespeichert.

  Passwörter: Für alle Mitarbeitenden werden Passwörter generiert für den Zugang zu Office 365/OneDrive, SharePoint und Lobos (Stundenerfassung).

- **Zugriff zu Passwörtern und Sicherheit**

  Zugriff Geschäftsführung:

  Sämtliche Unterlagen physisch

  Passwort lobos Lohn der Bereichsleitung Finanzen und Dienste

  Zugriff Leitung Rechnungswesen/Dienste, Personaladministration auf:

  Bewerbungsunterlagen, Personalienblatt, Arbeitsverträge inkl. Zusatzdokumente wie Strafregisterauszug und Sonderprivatauszug, Stellenbeschrieb, Angaben zu Absenzen/Arztzeugnisse, Schadenmeldungen, Versicherungsunterlagen, Vereinbarungen die Personaladministration betreffend, bewilligte Weiterbildungsgesuche, Verwaltung sämtlicher Passwörter exkl. Lobos-Passwort (dieses ist nur den einzelnen Mitarbeitenden bekannt).

  Die digitalen und physisch abgelegten Dokumente sind abgeschlossen resp. passwortgeschützt aufbewahrt.

  Zugriff Bereichsleitungen auf Anfrage bei der Geschäftsführung:

  Bewerbungsunterlagen, Personalienblatt, Arbeitsverträge inkl. Zusatzdokumente wie Strafregisterauszug und Sonderprivatauszug, Stellenbeschrieb, Angaben zu Absenzen/Arztzeugnisse, Schadenmeldungen, Vereinbarungen, bewilligte Weiterbildungsgesuche

  Sekretariat:

  Informationen aus Personalienblättern

  Zugriff IT-Supporter für technischen Support:

  Die IT-Supporter stehen unter Schweigepflicht.

  Firma 2sic: Passwörter Office 365/SharePoint

  Lobos: Zugriff auf Surver, Berechtigung Passwörter zu generieren (lobos lohn, lobos web, lobos admin).

  Risiko physische Personalakte/Kontaktdaten: Es gibt kein Backup der Papierdaten. Bei einem Feuer oder Wasserschaden könnten die Daten nicht oder nur teilweise wieder

hergestellt werden. Die Aktualität der Daten ist nicht gewährleistet, wenn Mitarbeitende neue Dokumente nicht tagesaktuell dem Sekretariat zur Einordnung abgeben.

Massnahmen physisch Kinderakte/Kontaktdaten: Abschliessbare Räumlichkeiten und Aufbewahrungsmöbel, Schlüsselmanagement, baulicher Schutz vor Wasser und Feuer

Risiko digitale Personalakte/Kontaktdaten: Versagen Backup, Passwortmissbrauch

Massnahmen digitale Personalakte/Kontaktdaten: Mehrfachbackup auf Server intern, extern, datenschutzkonforme Cloud-Lösung, Ablage auf Server in der Schweiz

Mittelfristig: Umstellung für alle Mitarbeitenden auf organisationseigene Geräte (Laptop/Surface und Telefonie). Die Personalakten von ehemaligen Mitarbeitenden werden auf Verlangen vernichtet.

c) Digitale Ablagen und Kommunikationskanäle im Heilpädagogischen Dienst GR

Office 365/OneDrive

Mitarbeitende arbeiten passwortgeschützt mit Office 365. Die beruflichen digitalen Unterlagen sind auf OneDrive datenschutzkonform gespeichert.

Share Point

Mitarbeitende haben einen passwortgeschützten Zugang zur Plattform Share Point des Heilpädagogischen Dienstes Graubünden. Share Point dient der Berichtadministration und als Ablagesystem. Die Sicherung der Daten ist professionell durch die Firma 2sic in der Schweiz gewährleistet. Systembedingt sind in einer Einstellung alle im Heilpädagogischen Dienst erfassten Kindernamen (ohne weitere Angaben) einsehbar. Die Mitarbeitenden unterstehen der Schweigepflicht und dürfen diese Kenntnis ausserhalb ihres Auftrags nicht verwenden.

Lobos

Über Lobos werden webbasiert die Stundenerfassung der Mitarbeitenden erhoben und die gesamte Betriebs- und Lohnbuchhaltung abgewickelt. Die Sicherung ist über die Firma Lobos in der Schweiz gewährleistet.

Website

Auf der Website des HPD werden keine Personaldaten gespeichert.

Über die Website des Heilpädagogischen Dienstes Graubünden werden keine Cookies[2] erhoben. Daher ist keine entsprechende Zustimmung notwendig beim Aufruf der Website.

Die Kinderanmeldung kann digital über die Website des Heilpädagogischen Dienstes erfolgen. Die Übermittlung dieser Daten ans Sekretariat erfolgt geschützt.

E-Mail

Der Heilpädagogischen Dienst verfügt über eine geschützte HIN-Mail-Adresse. (Bedingung für diesen Schutz: Die Mail-Adresse des Gegenübers muss auch eine HIN-Adresse sein).

Der Mailverkehr mit allen anderen Mail-Adressen im Heilpädagogischen Dienst ist nicht geschützt. Entsprechend dürfen keine schützenswerten Personaldaten per Mail verschickt werden. Kinder/Jugendliche werden mit Initialen und Geburtsdatum bezeichnet.

Telefonie

Die Telefonie gilt als sicherer Kanal.

WhatsApp

Mitarbeitende des Heilpädagogischen Dienstes erstellen beruflich keine WhatsApp-Chats mit Familien und/oder Fachpersonen.

Werden sie von extern dazu eingeladen können sie mitlesen und nicht schützenswerte Daten austauschen. Dazu gehören z.B. Terminvereinbarungen.

Wenn immer möglich wird auf SMS, Threema oder Alternativen ausgewichen, welche die Daten geschützt in der Schweiz speichern. Auch über diese Kanäle dürfen keine schützenswerten Informationen fliessen.

Entwicklung

Langfristig wird die vollständige Umstellung auf die digitale, passwortgeschützte und nach den gängigen Sicherheitsvorschriften geschützten Ablagesysteme angestrebt.

- **Risiko digitale Ablage/Kommunikationskanäle:** Versagen Backup, Passwortmissbrauch
- **Massnahmen digitale Ablage/Kommunikationskanäle:** Mehrfachbackup auf Server intern, extern, datenschutzkonforme Cloud-Lösung, Ablage auf Server in der Schweiz.
- **Massnahmen in Planung:**

  Umstellung für alle Mitarbeitenden auf organisationseigene Geräte (Laptop/Surface und Telefonie).

[2] Cookies sind Datenpakete, die zwischen Computerprogrammen ausgetauscht werden. Allgemein werden mit dem Begriff meist HTTP-Cookies bezeichnet, mit deren Hilfe Websites Nutzerdaten lokal und serverseitig speichern, um einzelne Funktionen und Webanwendungen wie Onlineshops, soziale Netzwerke und Foren nutzerfreundlicher gestalten zu können.

d) Verwendung von Daten für schulische, therapeutische, wissenschaftliche und statistische Zwecke

Die Verwendung von Personendaten für schulische, therapeutische, wissenschaftliche und statistische Zwecke ist dann zulässig, wenn diese anonymisiert sind. Personendaten sind dann anonymisiert, wenn die betroffenen Kinder und Jugendlichen sowie deren gesetzliche Vertretung nicht mehr bestimmbar sind. Zu beachten ist in diesem Zusammenhang das Bundesstatistikgesetz.

Ist eine Anonymisierung nicht möglich oder erschwert – wie beispielsweise bei Videoaufnahmen – ist eine zusätzliche Einwilligung der betroffenen Kinder und Jugendlichen bzw. deren gesetzlichen Vertretung notwendig. Hierfür dient die «Vollmacht Video/Fotos/Audio». Aufnahmen bzw. Fotos gegen den Willen der betroffenen Kinder und Jugendlichen sind nicht zulässig und können strafrechtliche Konsequenzen haben.

e) Daten von Dritten

- **Schnittstelle HPD – AVS:** Die Schnittstelle zwischen HPD und AVS erfolgt geschützt mit einer entsprechend gesicherten IT-Lösung.
- **Zugriff:** Geschäftsführung, Bereichsleitungen, Sekretariat
- **Risiko digitale Ablage/Kommunikationskanäle:** Versagen Backup, Passwortmissbrauch
- **Massnahmen digitale Ablage/Kommunikationskanäle:** Mehrfachbackup auf Server intern, extern, datenschutzkonforme Cloud-Lösung, Ablage auf Server in der Schweiz.

7 Rechte der betroffenen Personen

Der Heilpädagogische Dienst Graubünden gewährt allen Personen, deren Personendaten in irgendeiner Weise erfasst und bearbeitet werden, die von der Gesetzgebung vorgesehenen Rechte.

7.1 Aufklärung/Orientierung

Kinder/Jugendlichen, deren Erziehungsberechtigte, Mitarbeitende und Dritte werden beim Eintritt bzw. beim Beginn der Zusammenarbeit über die Bearbeitung ihrer Personendaten und über ihre Rechte bezüglich Datenschutz informiert.

7.2 Auskunfts-/Einsichtsrecht

Die von der Bearbeitung ihrer Daten betroffene Personen dürfen über Erhebung, Herkunft, Inhalt, Zweck, und Bearbeitung der Daten Auskunft verlangen. Dazu gehört auch, auf welche rechtlichen Grundlagen die Bearbeitung von Daten geschieht. Sie haben auch das Recht auf die Bekanntgabe der Firmen und Personen, die durch den Heilpädagogischen Dienst Graubünden mit der Bearbeitung oder Aufbewahrung der Daten beauftragt sind.

Die Auskunft bzw. Einsicht verlangende Person muss sich über ihre Identität ausweisen. Die Auskunft ist innert 30 Tagen in allgemeinverständlicher Weise, schriftlich und kostenlos zu erteilen. Jede

betroffene Person kann die Bekanntgabe ihrer Daten gegenüber Dritten entgegen einer ursprünglichen Vereinbarung sistieren lassen.[3]

Übergeordnet zu diesem Anliegen ist die Datenbekanntgabe gegenüber den Behörden, wenn diese Informationen zur Aufklärung von mutmasslich rechtsmissbräuchlichen Handlungen einfordern Verletzungen der Sorgerechts-Pflichten durch die betroffene Person abklären.

Die betroffenen Personen dürfen grundsätzlich in Datensätze Einsicht nehmen, die ihre Person oder die Person der Kinder betreffen, für die sie sorgeberechtigt sind. Die Erteilung von Auskünften und die Einsichtsrechte dürfen ausnahmsweise beschränkt oder verweigert werden, wenn wichtige juristische Gründe dagegensprechen.[4]

7.3 Recht auf Berichtigung

Widerrechtlich bearbeitete sowie unrichtige Daten müssen auf Verlangen der betroffenen Personen berichtigt oder vernichtet werden.

7.4 Verweigerung der Datenweitergabe

Betroffene Personen können jederzeit die Weitergabe jeglicher oder definierter Informationen zu ihrer Person oder zur Person ihrer Kinder verweigern.

7.4.1 Auftragserfüllung

Dem Heilpädagogischen Dienst Graubünden ist es vorbehalten, den therapeutischen Auftrag als nicht durchführbar zu deklarieren, wenn ein Minimum an notwendigen Daten und Berechtigungen seitens der Erziehungsberechtigten nicht zur Verfügung gestellt werden.

Dies sind insbesondere:

- Die Stammdaten der Kinder bzw. der Erziehungsberechtigten
- Daten zur medizinischen und therapeutischen Vorgeschichte
- Die Berechtigung, notwendige Informationen bei medizinischen und pädagogischen Fachstellen zu beschaffen, die mit dem Kind relevant zu tun haben oder zu tun hatten
- Die Berechtigung, mit medizinischen und pädagogischen Fachstellen in Austausch zu treten, die relevant mit dem Kind zu tun haben oder zu tun haben werden[5]

[3] Meist geschieht dies, wenn ein schutzwürdiges Interesse vorliegt, muss aber nicht weiter begründet werden.

[4] Im Zweifelsfall wendet sich der HPD GR die kantonale Datenschutzstelle.

[5] Im Rahmen eines definierten Auftrages durch den Kanton oder die Gemeinde, ist es möglich, Daten mit anderen oder abnehmenden Stellen auszutauschen, die wiederum einen Auftrag in Bezug auf die Förderung, Betreuung oder Bildung des Kindes haben. Beispielsweise können wichtige Angaben zur Gesundheit an Fachpersonen des Kindergartens weitergegeben werden, sofern diese Angaben zur Erfüllung deren Auftrages unabdingbar sind. Da in der Regel das Einverständnis der Erziehungsberechtigten vorliegt, können allfällige andersliegende Einzelfälle mit den kantonalen Datenschutzstellen besprochen werden.

8 Genehmigung und Unterschriften

Dieses Konzept gilt ab 01.01.2024

Nina Tinner

Chur, 09.02.2024

Stiftungsratspräsidentin

9 Anhänge zum Konzept Datenschutz

- 1.1.3.22 H-Hintergründe_rechtliche Grundlagen Datenschutz
- 1.1.3.23 H-Beispiele_Hilfestellung für die Praxis Datenschutz
- 1.3.2.9 H-Kodex_Datensicherheit und Datenschutz
- 2.1.6.2 F-Vollmacht Datenweitergabe/Besuche
- 2.1.6.3 F-Vollmacht digitale Datennutzung
- 2.3.1.8 H-Information Datenschutz Erziehungsberechtigte

10 Verwendete Quellen

In diesem Leitfaden sind folgende Quellen konsultiert worden:

- Bundesgesetz 235.1 über den Datenschutz (revDatenschutzgesetz, revDSG) und die Verordnung 235.11 über den Datenschutz (revDatenschutzverordnung, revDSV) vom 31. August 2022 (Stand am 1. September 2023).
- Das neue Datenschutzgesetz aus Sicht des EDÖB, Februar 2021
- Diverse kantonale Datenschutzstellen, insbesondere jene des Kantons Graubündens und des Kantons Basel-Landschaft zu Fragen der Folgeabschätzung.
- Koller Markus; Datenschutzkonzept der Blindenschule Zollikofen, genehmigt durch die Geschäftsleitung am 31.02.2023
- Koller Markus; Datenschutz-Leitfaden der Blindenschule Zollikofen, genehmigt durch die Geschäftsleitung am 28.04.2023
- ARTISET, curaviva, INSOS, YOUVITA, senesuisse; 19.06.2022; Datenschutzkonzept (eine Vorlage).
- Stiftung RgZ; Merkblatt für den Umgang mit Auskunftswünschen und der Herausgabe von Daten
- Stiftung RgZ; Interne Richtlinien zur Führung und Archivierung der Klientendossiers
- Adrian Bieri / Julian Powell, Die Totalrevision des Bundesgesetzes über den Datenschutz, in: Jusletter 16. November 2020
- Kibesuisse; Datenschutzerklärung; www.kibesuisse.ch/datenschutz/