igs
psychiatrie. sozial.

Datenschutzkonzept Interessengemeinschaft Sozialpsychiatrie Bern

1. Inhaltsverzeichnis

2. Zweck und Umfang

Das vorliegende Datenschutzkonzept der Interessengemeinschaft Sozialpsychiatrie Bern (nachfolgend «igs Bern» genannt) trägt der Bedeutung und dem Stellenwert des Datenschutzes im Sinne der Achtung der Privatsphäre und der Persönlichkeitsrechte unserer Nutzenden, Mitarbeitenden und allenfalls auch unserer Geschäftspartner:innen Rechnung. Es bildet die verbindliche Grundlage für alle datenschutzrelevanten Massnahmen und Aktivitäten innerhalb der igs Bern, namentlich für das Bearbeiten von

- Personendaten der Nutzenden;
- Personendaten der Mitarbeitenden, inklusive Daten über Stellenbewerber:innen und ehemalige Mitarbeitenden;
- Informationen über Geschäftspartner:innen und weitere Dritte, soweit Personendaten betroffen sind.

3. Gesetzliche Grundlagen

Grundlage für dieses Datenschutzkonzept ist das Bundesgesetz über den Datenschutz vom 25. September 2020 (Eidg. Datenschutzgesetz DSG; SR 235.1), die Verordnung über den Datenschutz vom 31. August 2022 (Eidg. Datenschutzverordnung DSV; SR 235.11) sowie das Datenschutzrecht des Kantons Bern vom 19. Februar 1986 (Kantonales Datenschutzgesetz KDSG; BSG 152.04).

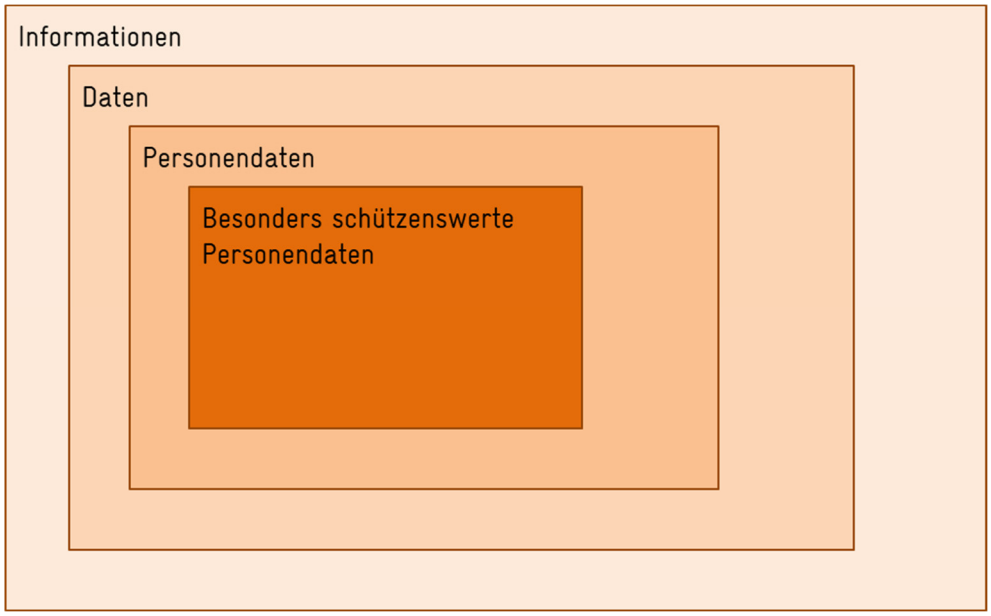
4. Geltungsbereich

Das vorliegende Datenschutzkonzept gilt für alle Organe und Mitarbeiter:innen der igs Bern, die im Rahmen der Erfüllung ihrer Funktionen und Aufgaben Personendaten bearbeiten. Es gilt ebenfalls für externe Personen und Unternehmen, sofern sie sich durch entsprechende schriftliche Vereinbarung zu dessen Einhaltung verpflichten.

5. Zielsetzung

Das Hauptziel dieses Konzepts ist die Gewährleistung des Schutzes der Persönlichkeit natürlicher Personen vor widerrechtlicher oder unverhältnismässiger Bearbeitung der Daten von Personen gemäss Ziffer 2. Dieses Konzept soll als verbindliche Richtlinie alle für die igs Bern tätigen Personen darin unterstützen, in Eigenverantwortung datenschutzrechtlich einwandfrei zu handeln. Mit der Umsetzung dieser Zielsetzung vermeidet die igs Bern auch materielle Nachteile und Imageschäden, welche ihr aufgrund von datenschutzwidrigen Handlungen erwachsen könnten.

6. Unterscheidung Informationen, Daten und Personendaten



6.1. Informationen

Zweckbezogenes Wissen, das man bei der täglichen Arbeit benötigt, um die Aufgaben anforderungsgemäss zu erfüllen. Dabei können Informationen in unterschiedlichster Form vor-handen sein oder zwischen Personen übertragen werden (mündlich, schriftlich auf Papier, elektronisch auf Informatikmittel).

6.2. Daten

In der Informatik und Datenverarbeitung versteht man Daten gemeinhin als (maschinen-)lesbare und -bearbeitbare, in der Regel digitale Repräsentation von Information. Daten werden also elektronisch auf Informatikmittel zur weiteren Bearbeitung gespeichert. Durch das Lesen der gespeicherten Daten und das Zusammenfügen von in den Daten enthaltenen Informationsteilen erhält man wiederum Informationen.

6.3. Personendaten

Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Das Bundesgesetz über den Datenschutz (Eidg. Datenschutzgesetz DSG; SR 235.1) bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden. Entsprechend geht es in diesem Datenschutzkonzept um Personendaten.

6.4. Besonders schützenswerte Personendaten

a) Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten;

b) Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer ethnischen Gruppe oder Herkunft;
c) genetische Daten;
d) biometrische Daten, die eine natürliche Person eindeutig identifizieren;
e) Daten über verwaltungs- und strafrechtliche Verfolgung oder Sanktionen;
f) Daten über Massnahmen der sozialen Hilfe.

6.5. Daten Mitarbeiter:innen

Unter Daten Mitarbeiter:innen werden alle Daten verstanden, die einer angestellten Person oder einer auszubildenden Person direkt zugeordnet werden können. Zu den Daten Mitarbeiter:innen gehören insbesondere die Personaldossiers und die Lohnbuchhaltung.

6.6. Bearbeiten von Personendaten

Unter das Bearbeiten fällt jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren (manuell, automatisiert oder gemischt), insbesondere das Beschaffen, Speichern, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten. Personendaten werden nach den Grundsätzen der Rechtmässigkeit, Verhältnismässigkeit, Zweckbindung, Transparenz, Datenqualität sowie Treu und Glauben bearbeitet. Dabei gilt Folgendes:

- Es sind angemessene technische und organisatorische Schutzmassnahmen vorzukehren
- Personendaten müssen rechtmässig bearbeitet werden. Rechtmässig ist die Datenbearbeitung, wenn sie durch die Einwilligung der betroffenen Person, eine gesetzliche Ermächtigung oder ein überwiegendes öffentliches oder privates Interesse gerechtfertigt ist
- Es muss ein Rechtfertigungsgrund vorliegen (gesetzliche Grundlage oder Einwilligung der betroffenen Person oder überwiegendes Interesse)
- Die Bearbeitung von Personendaten hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein, das heisst, die Datenerhebung muss erforderlich sein, zudem soll ein überwiegendes Interesse an der Erhebung bestehen. Datenerhebungen auf Vorrat sind widerrechtlich, nicht mehr benötigte Daten sind zu vernichten
- Personendaten dürfen nur zu einem bestimmten und für die betroffene Person klar erkennbaren Zweck beschafft werden. Bei grundsätzlich jeder beabsichtigten Beschaffung von Personendaten muss die betroffene Person vorgängig angemessen informiert werden, selbst wenn die Daten nicht direkt bei ihr beschafft werden
- Die Daten dürfen nur zum Zweck bearbeitet werden, der bei der Erhebung der Daten genannt wurde. Ihre Daten dürfen zu keinem für die betroffene Person nicht erkennbaren Zweck bearbeitet werden (Zweckbindung)
- Personendaten dürfen nur so bearbeitet werden, dass dies mit dem Zweck zu vereinbaren ist
- Es muss überprüft sein, ob die Daten richtig sind

- Es muss sichergestellt sein, dass die bearbeiteten Daten richtig, vollständig und aktuell sind. Unrichtige und unvollständige Daten sind zu korrigieren, zu ergänzen oder zu vernichten (Datenqualität).
- Unrichtige oder unvollständige Personendaten, die für die Bearbeitung erforderlich sind, müssen korrigiert oder ergänzt werden
- Ist für die Bearbeitung die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig und eindeutig erfolgt. Für die Bearbeitung von besonders schützenswerten Personendaten muss die Einwilligung zudem ausdrücklich erfolgen
- Personendaten müssen so lange wie gefordert aufbewahrt werden
- Die Verantwortlichen sowie die Auftragsbearbeiter müssen je ein Verzeichnis sämtlicher Datenbearbeitungen führen. Die entsprechenden Mindestangaben gibt das DSG nach Art. 12 vor
- Die Datenerhebung und -bearbeitung muss klar erkennbar sein. Die notwendigen Informationen sollen direkt bei der betroffenen Person beschafft werden (Transparenz)
- Wenn eine beabsichtigte Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann, müssen auch private Verantwortliche vorgängig eine Datenschutzfolgenabschätzung erstellen
- Widersprüchliches und rechtmissbräuchliches Verhalten ist unzulässig (Treu und Glauben).

7. Rechte der betroffenen Personen

7.1. Aufklärung und Orientierung

Nutzende sowie Mitarbeitende werden beim Eintritt über ihre datenschutzrechtlichen Rechte und Pflichten informiert. Der/Die Datenschutzverantwortliche orientiert sie danach angemessen über die Beschaffung sie betreffender Personendaten.

7.2. Auskunfts- und Einsichtsrecht

Die von der Bearbeitung ihrer Daten betroffene Person darf über Erhebung, Herkunft, Inhalt, Zweck, Kategorie und Rechtsgrundlage Auskunft verlangen und in die Datensammlung Einsicht nehmen. Sie hat auch das Recht auf die Bekanntgabe der an der Sammlung Beteiligten und Datenempfänger. Die Auskunft beziehungsweise Einsicht verlangende Person muss sich über ihre Identität ausweisen. Die Auskunft ist innert 30 Tagen in allgemeinverständlicher Weise, schriftlich und kostenlos zu erteilen. Die Erteilung von Auskünften und die Einsichtsrechte dürfen ausnahmsweise beschränkt oder verweigert werden, wenn wichtige und überwiegende öffentliche Interessen oder besonders schützenswerte Interessen von Dritten entgegenstehen.

Angestellte und auszubildende Mitarbeitende haben das Recht,

a) die Berichtigung falscher Daten Mitarbeiter:innen zu verlangen
b) den Daten Mitarbeiter:innen eine Gegendarstellung beizufügen, wenn eine Berichtigung im Sinne von Buchstabe a) nicht möglich ist
c) die Löschung der Daten Mitarbeiter:innen zu verlangen, die nicht mehr gebraucht werden und die keiner gesetzlichen Aufbewahrungspflicht unterliegen

Besteht das Risiko, dass die betroffene Person (vor allem Minderjährige) mit der Auskunftserteilung oder Einsichtnahme einer zu hohen Belastung ausgesetzt werden könnte, kann sie eine andere Person bestimmen, der an ihrer Stelle Auskunft erteilt beziehungsweise Einsicht gewährt wird.

7.3. Recht auf Berichtigung

Widerrechtlich oder unrichtig bearbeitete sowie unrichtige Daten müssen berichtigt oder vernichtet werden.

7.4. Sperrung und Verweigerung der Datenbekanntgabe

Jede betroffene Person kann die Bekanntgabe ihrer Daten sperren lassen, wenn sie ein schutzwürdiges Interesse nachweist. Dies gilt dann nicht, wenn die Datenbekanntgabe eine gesetzliche Verpflichtung darstellt, aufgrund überwiegender Interessen Dritter erforderlich ist oder zur Aufklärung von mutmasslich rechtsmissbräuchlichen Handlungen der betroffenen Person erforderlich ist.

7.5. Einsichtnahme in eigene Personaldaten

Angestellte und auszubildende Personen haben jederzeit das Recht, in sämtliche Personaldaten Einsicht zu nehmen, die sie betreffen (beispielsweise Personaldossiers, Verlaufsprotokolle, Berichte an externe Stellen und dergleichen sowie für Akten, die der Einsicht verlangenden Person bereits bekannt sind).

Die Einsichtnahme kann verweigert werden, wenn wichtige und überwiegende öffentliche Interessen oder besonders schützenswerte Interessen Dritter (Personendatenschutz von Dritten, die in den Akten erwähnt werden) entgegenstehen.

8. Massnahmen der Datensicherheit

Mit organisatorischen und technischen Massnahmen soll der Datenschutz gewährleistet und Personendaten insbesondere vor dem Zugang Unbefugter, Missbrauch, Vernichtung, Verlust, technischen Fehlern, Fälschung, Diebstahl und dergleichen geschützt werden.

8.1. Mögliche Risikosituationen

- Dokumente/Fotos, die in falsche Hände geraten
- Verlorene Dokumente (intern oder extern)

- Verlorene Datenträger (intern oder extern)
- Kein Zugriff auf Bewohnerdaten aufgrund Informatik-Störung
- Fremde Personen in Arbeitsräumen
- Verlust medizinischer Daten durch Schadsoftware
- Nichteinhalten von Vorgaben durch Mitarbeitende
- Gespräch mit vertraulichen Inhalten in öffentlichen Zonen, z.B. in der Cafeteria, im Gang
- Unverschlüsselter Mailversand an falsche Empfänger
- Speichern vertraulicher Daten auf Datenträger wie Stick, etc.
- Zugriff auf Personaldaten ohne Berechtigung
- und weitere

8.2. Organisatorische Massnahmen

Zugang zu Personendaten besteht bei der igs Bern nach dem Grundsatz «So viel wie nötig, so wenig wie möglich».

Die/Der Datenschutzverantwortliche regelt deshalb in Zusammenarbeit mit den jeweils zuständigen Führungspersonen für jede Datensammlung, wer unter welchen Bedingungen Zugang zu Personendaten hat und wie dies überwacht wird.

Sie/Er führt ein Verzeichnis der Bearbeitungstätigkeiten gemäss den gesetzlichen Anforderungen und hält dieses aktuell. Sie/Er regelt zudem, wem Zugang zu archivierten Daten gewährt wird.

8.3. Technische Massnahmen

Der Schutz elektronisch bearbeiteter Daten wird insbesondere durch die Verwendung und regelmässige umfassende Verschlüsselung, den Einsatz von Firewalls, Virenschutzprogrammen und dergleichen und die Protokollierung von Zugriffen gewährleistet.

Durch Zugangs- und Personendatenträgerkontrollen wird verhindert, dass unbefugte Personen Zugang zu Datenbeständen haben oder diese verändern, zerstören, entwenden oder Ähnliches.

8.4. Archivierung

Personendaten, die für die Bearbeitung nicht mehr benötigt werden, werden gemäss den Richtlinien der/des Datenschutzverantwortlichen aufbereitet und während der definierten Dauer archiviert.

8.5. Vernichtung

Daten von untergeordneter Bedeutung werden unmittelbar nach Erreichen des Bearbeitungszwecks vernichtet (physisch zerstört oder elektronisch unwiederbringlich gelöscht). Die/Der Datenschutzverantwortliche bestimmt die Einzelheiten.

9. Handlungsanleitungen

Dem Ziel, dass im Alltag regelmässig eintretende Situationen datenschutzrechtlich korrekt gehandhabt werden, dienen die folgenden Handlungsanleitungen:

9.1. Auskunftserteilung

Beim Anstellungsverhältnis, beim Aufenthalt einer/eines Mieter:in oder Bewohner:in handelt es sich um Personendaten im Sinne des DSG, jedoch nicht um besonders schützenswerte Personendaten. Die Auskunftserteilung stellt eine Datenbearbeitung dar. Die reine Auskunftserteilung über die Tatsache, dass eine Person in einem Betrieb arbeitet oder wohnt, ist gestützt zulässig.

Mitarbeiter:innen, Mieter:innen oder Bewohner:innen können jedoch anordnen, dass keine Auskunft erteilt wird beziehungsweise eine Datensperre verlangen. In diesem Fall darf keine Auskunft erteilt werden.

Das voranstellend Ausgeführte gilt auch für die Auskunft, dass eine Person verstorben ist. Dabei ist jedoch zu beachten, dass über die genauen Umstände des Todes, allfällige Krankheiten und dergleichen keine Auskunft gegeben werden darf, denn dabei handelt es sich um besonders schützenswerte Personendaten, auch über den Tod hinaus.

9.2. Verhalten bei telefonischen und schriftlichen Anfragen

Ohne ausdrückliche Einwilligung der betroffenen Person oder ohne entsprechende gesetzliche Erlaubnis dürfen Personendaten nicht an Aussenstehende weitergegeben werden. Bei telefonischen Anfragen ist die eindeutige Identifizierung der anfragenden Person sicherzustellen. Werden Telefongespräche aufgezeichnet, muss darauf hingewiesen und die Zustimmung des/der Gesprächspartner:in eingeholt werden.

9.3. Grundsätze der E-Mail-Nutzung

E-Mails können durch Dritte mitgelesen oder verändert werden. Grundsätzlich sollen deshalb möglichst wenig Personendaten per E-Mail übermittelt werden und sie sollen keine sensiblen Informationen oder Angaben über Passwörter und andere Zugangsdaten enthalten.

Per E-Mail dürfen besonders schützenswerte Daten grundsätzlich nur verschlüsselt übermittelt werden, sofern die betroffene Person keine gegenteilige, schriftliche Erklärung abgegeben hat.

Zu beruflichen Zwecken bearbeitete Personendaten dürfen nicht auf privaten Geräten gespeichert werden. Im Übrigen sind auch die Vorschriften im Informatik-Konzept der igs Bern zu beachten.

9.4. Verwendung von Bild- und Tonaufnahmen

Auf Bild-, Film- und/oder Tonaufnahmen erkennbar dürfen nur Personen festgehalten werden, welche dazu ihre Einwilligung gegeben haben. Die Einwilligung der betroffenen Person muss freiwillig, ausdrücklich und nach vorgängiger Aufklärung über den Zweck und die Verwendung der Aufnahmen erfolgen. Die Zustimmung kann schriftlich oder – bei Anwesenheit mehrerer Personen – mündlich oder nonverbal erfolgen und ist zu dokumentieren.

10. Verantwortlichkeiten

10.1. Eidg. Datenschutz- und Öffentlichkeitsbeauftragte:r (EDÖP)

Die/der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) beaufsichtigt die Anwendung der bundesrechtlichen Datenschutzvorschriften.

10.2. Vorstand

Der Vorstand ist auf strategischer Ebene für die Gewährleistung des Datenschutzes bei der igs Bern verantwortlich.

Er nimmt den Datenschutz als relevantes Thema in sein Risikomanagement-System auf und beurteilt die entsprechenden Risiken in strategisch stufengerechter Weise.

Er erlässt das vorliegende Datenschutzkonzept und überprüft dieses regelmässig.

Er bestimmt die/den Datenschutzverantwortliche:n, regelt ihre/seine Aufgaben, Verantwortlichkeiten und Kompetenzen unter Berücksichtigung der Vorschriften der Gesetzgebung in einem Pflichtenheft und nimmt ihre/seine regelmässige Berichterstattung entgegen.

10.3. Geschäftsleitung

Die Geschäftsleitung ist in Zusammenarbeit mit der/dem Datenschutzverantwortlichen zuständig für die Umsetzung dieses Konzepts und für die Einhaltung der datenschutzrechtlichen Vorgaben im Rahmen aller Datenbearbeitungen auf operativer Ebene.

Sie sorgt in geeigneter Weise dafür, dass alle Mitarbeiter:innen regelmässig für die Belange des Datenschutzes sensibilisiert und über die Vorgaben dieses Konzepts und deren Anwendung im beruflichen Alltag informiert werden.

10.4. Datenschutzverantwortliche:r

Die/Der Datenschutzverantwortliche nimmt betriebsintern die Aufgaben gemäss der Gesetzgebung und dem Pflichtenheft wahr.

Sie/Er ist nach innen und aussen die Ansprechperson für alle Fragen bezüglich des Datenschutzes.

Sie/Er prüft die Rechtmässigkeit der Datenbearbeitung bei der igs Bern.

Sie/Er verfügt über ein Weisungsrecht, soweit dies für die Einhaltung der Gesetzgebung und die Umsetzung dieses Konzepts erforderlich ist.

Sie/Er erstattet gegebenenfalls Meldungen an die Datenschutzbeauftragten des Bundes und/oder des Kantons.

Sie/Er berichtet dem Vorstand und der Geschäftsleitung regelmässig über die Datenbearbeitung bei der igs Bern, weist dabei auf erkannte Risiken hin und gibt Empfehlungen für mögliche Verbesserungen ab. Über besondere Vorkommnisse von grösserer Tragweite orientiert sie/er unverzüglich.

Sie/Er führt regelmässige Datenschutz-Audits durch und zieht hierfür bei Bedarf externe Unterstützung bei.

Sie/Er steht dem Vorstand, der Geschäftsleitung, der Leitung HR, den Mitarbeiter:innen sowie den Klientinnen und Klienten bei datenschutzrechtlichen Fragen beratend zur Verfügung.

10.5. Leitung HR

Die Leitung HR ist für die sorgfältige und datenschutzkonforme Bearbeitung der Personendaten der Mitarbeitenden im Rahmen der Personalarbeit verantwortlich.

10.6. Führungspersonen

Die Vorgesetzten aller Stufen nehmen eine Vorbildfunktion wahr und fördern die Motivation der Mitarbeitenden, dem Datenschutz bei ihrem Handeln am Arbeitsplatz Rechnung zu tragen.

Sie sind in ihren Verantwortungsbereichen für die Durchsetzung und Einhaltung des Datenschutzes verantwortlich, insbesondere im Rahmen dieses Konzepts und der Geschäftsprozesse.

Sie sorgen in Zusammenarbeit mit der/dem Datenschutzverantwortlichen für die datenschutzmässige Sensibilisierung und handlungsorientierte Anleitung der Mitarbeitenden.

10.7. Mitarbeiter:innen

Alle Mitarbeiter:innen der igs Bern, welche Personendaten bearbeiten, tragen dem Datenschutz eigenverantwortlich Rechnung und handeln dabei insbesondere gemäss dem vorliegenden Konzept und den Weisungen der/des Datenschutzverantwortlichen.

Sie wenden sich bei Fragen und Unsicherheiten an ihre Vorgesetzten oder an die/den Datenschutzverantwortliche:n.

11. Schlussbestimmungen

Dieses Konzept gilt ab dem 1. September 2023.

Bern, 31. März 2024
Interessengemeinschaft Sozialpsychiatrie Bern

Luca Lo-Faso	Manuel Moser
Co-Präsident	Co-Präsident

12. Anhang 1: Begriffe

Informationen	Zweckbezogenes Wissen, das man bei der täglichen Arbeit benötigt, um die Aufgaben anforderungsgemäss zu erfüllen. Dabei können Informationen in unterschiedlichster Form vorhanden sein oder zwischen Personen übertragen werden (mündlich, schriftlich auf Papier, elektronisch auf Informatikmittel).
Personendaten	Angaben über eine bestimmte oder bestimmbare natürliche Person.
Besonders schützenswerte Personendaten	a) Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; b) Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer ethnischen Gruppe oder Herkunft; c) genetische Daten; d) biometrische Daten, die eine natürliche Person eindeutig identifizieren; e) Daten über verwaltungs- und strafrechtliche Verfolgung oder Sanktionen; f) Daten über Massnahmen der sozialen Hilfe.
Bearbeiten von Personendaten	Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, wie das Beschaffen, Speichern, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.
Bekanntgabe von Personendaten	Jedes Übermitteln oder Zugänglichmachen von Personendaten.
Datensammlung	Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach bestimmten Personen erschliessbar sind.
Datenschutzverantwortliche/r	Person, welche betriebsintern die Einhaltung der Datenschutzvorschriften überwacht und u.a. ein Verzeichnis der Datensammlungen führt.
Inhaber/in der Datensammlung	Verantwortliche/r für eine Datenbearbeitung. Sie/Er entscheidet allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung.
Persönlichkeitsprofil	Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.
Profiling	Bewertung bestimmter Merkmale einer Person aufgrund von automatisiert bearbeiteten Personendaten (um z.B. die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, bestimmte Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen).

Klassifizierungskriterien	Klassifizierungskriterien sind Instrumente, welche den Objekt-Eigner unterstützen, die dem Schutzbedarf seines Schutzobjektes entsprechende Klassifizierungsstufe zu wählen. Wer schutzwürdige Informationen (beispielsweise personenbezogene Dokumente) verfasst oder herausgibt, weist sie entsprechend dem Grad ihrer Schutzwürdigkeit einer der folgenden Klassifizierungsstufen zu: ▪ **Öffentliche Daten** sind für jedermann, auch ausserhalb der Unternehmung, zugänglich. Dabei handelt es sich zum Beispiel um Informationen, die auf der öffentlichen Webseite im Internet dargeboten werden. Die Anschrift, das Leitbild oder die Werbebroschüren fallen in diese Kategorie ▪ **Interne Daten** werden lediglich den eigenen Mitarbeiter:innen und den betriebsinternen Gremien zugänglich gemacht. Also nur die eigenen Angestellten eines Unternehmens (und vielleicht ausgewählte Partnerbetriebe) sollten Zugriff auf diese haben. Dies können zum Beispiel Telefonverzeichnisse, Weisungen oder allgemeine Strategiedokumente sein. ▪ **Vertraulich definierten Daten** sind lediglich einer begrenzten Anzahl an Mitarbeiter:innen zugänglich. Hierbei handelt es sich in der Regel um Informationen, die massgeblich für den Erfolg eines Unternehmens von Wichtigkeit sind. Zum Beispiel sind Gehaltslisten und Mitarbeiterdossiers ausschliesslich der Personalabteilung und den zuständigen Linien-vorgesetzten zugänglich. Die Herausgabe dieser ist gesetzlich geregelt und ein Verstoss der Vorschriften würde juristische Folgen nach sich ziehen. ▪ **Geheim** ist die höchste Sicherheitsstufe für Daten. Diese sind punktuell und ausschliesslich bestimmten definierten Personen zugänglich. Derlei Informationen sind unmittelbar für den Erfolg des Unternehmens verantwortlich. Dies können beispielsweise Dokumente zur Integration/Übernahme einer Unternehmung sein. Die Weitergabe diese Information kann das Geschäftsverhältnis unmittelbar und nachhaltig schädigen.