

Datenschutz

u^b

^b
UNIVERSITÄT
BERN



Guido Suter 19.08.2019

Datenschutz am Institut für Pathologie

- > **Ziel**
- > Zuständigkeiten
- > Schulung und Dokumentation
- > Allgemeine Grundsätze Datenschutz
- > Herausgabe von Daten
- > Grenzüberschreitender Datenverkehr
- > Organisatorische Massnahmen
- > Technische Massnahmen
- > Diskussion

Schutzziele

Schutz der Patientendaten

Schutz der Mitarbeiterdaten

Schutz von vertraulichen Geschäftsdaten

Technisch



Organisatorisch



Datenschutz am Institut für Pathologie

- > Ziel
- > **Zuständigkeiten**
- > Schulung und Dokumentation
- > Allgemeine Grundsätze Datenschutz
- > Herausgabe von Daten
- > Grenzüberschreitender Datenverkehr
- > Organisatorische und technische Massnahmen
- > Diskussion

Zuständigkeiten



- > Allgemeiner Datenschutz - Guido Suter
— Klinikmanager



- > Datenschutz Forschung - Prof. Inti Zlobec
— Leiterin Translational Research Unit

Datenschutz Behörde

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (Edöp)

<https://www.edoeb.admin.ch/edoeb/de/home.html>

Überblick	Technologien	Gesundheit	Wohnen und Verkehr
Datenschutz	Personentracking	Krankengeschichte und Auskunftsrecht	Mietrecht
Auskunftsrecht	Digitale Stromzähler	Schweigepflicht	Anmeldeformulare für Mietwohnungen
Aufgaben des EDÖB	WLAN	Arzt- und Prämienrechnungen	Eigentümerrechte
Glossar	RFID	Erhebung medizinischer Daten	Abfall
Internet und Computer	Biometrie	Genetik	Öffentlicher Verkehr
Onlinedienste	Digitales Fernsehen	Kranken- und Unfallversicherungen	Pay as you drive
Recht auf Vergessen	Videoüberwachung	Case Management	Digitale Stromzähler
Analysetools für Webseiten	Geolokalisierung	Swiss DRG	WLAN
Webtracking	Handel und Wirtschaft	Versicherung	Videoüberwachung

Datenschutz am Institut für Pathologie

- > Ziel
- > Zuständigkeiten
- > **Schulung und Dokumentation**
- > Allgemeine Grundsätze Datenschutz
- > Herausgabe von Daten
- > Grenzüberschreitender Datenverkehr
- > Organisatorische und technische Massnahmen
- > Diskussion

Schulung und Dokumentation

Link

https://ilias.unibe.ch/goto_ilias3_unibe_cat_1258954.html#il_mhead_t_focus

The screenshot shows the Ilias LMS interface for a course titled "Datenschutz / data protection". The header includes a navigation bar with "Inhalt", "Info", "Einstellungen", "Export", and "Rechte". Below this is a sub-header with "Zeigen", "Verwalten", "Sortierung", and "Seite gestalten". A red button "Neues Objekt hinzufügen" is visible. The main content area is divided into two sections: "KATEGORIEN" and "WEBLINKS". Under "KATEGORIEN", there are three items: "Kurse / Training", "Schulungsunterlagen / Training materials" (highlighted), and "Gesetzessammlung". Under "WEBLINKS", there is one item: "Eidgenössischer Datenschutz und Öffentlichkeitsbeauftragter".

Datenschutz / data protection Aktionen ▾

Im Kurs werden die Datenschutzrichtlinien für die Dienstleistung und die Forschung geschult.

Inhalt Info Einstellungen Export Rechte

[Zeigen](#) [Verwalten](#) [Sortierung](#) [Seite gestalten](#)

Neues Objekt hinzufügen ▾

KATEGORIEN

- Kurse / Training ▾
- Schulungsunterlagen / Training materials ▾
- Gesetzessammlung ▾

WEBLINKS

- Eidgenössischer Datenschutz und Öffentlichkeitsbeauftragter ▾

Datenschutz am Institut für Pathologie

- > Ziel
- > Zuständigkeiten
- > Schulung und Dokumentation
- > **Allgemeine Grundsätze Datenschutz**
- > Herausgabe von Daten
- > Grenzüberschreitender Datenverkehr
- > Organisatorische Massnahmen
- > Technische Massnahmen
- > Diskussion

Geltende Gesetzte Institut für Pathologie

Datenschutz

- Schweizerische Verfassung, Verordnung DS
- Bundesdatenschutzgesetz (DSG)
- **Kantonales Datenschutzgesetz**
- **Gesundheitsgesetz**
- **Kantonales Datenschutzgesetz (KDSG)**
- **Humanforschungsgesetz (HFG)**
- Zivilgesetzbuch (ZGB) und das Schw. Strafbuch
- Verordnung (EU) 2016/679, gültig ab 18.05.2018

Betriebs- und Geschäftsgeheimnisse

- Geistiges Eigentum, Know How, OR 321 a Abs. 4

Berufsgeheimnis

- Ärztliche Schweigepflicht: GesG, Art. 27, Abs. 1
- Die Schweigepflicht entfällt: GesG, Art. 27, Abs. 2, Art. 28

Bundesverfassung, Art. 13: Schutz der Privatsphäre

Schutz der Privatsphäre

Jede Person hat Anspruch auf Achtung ihres Privat- und Familien-lebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.



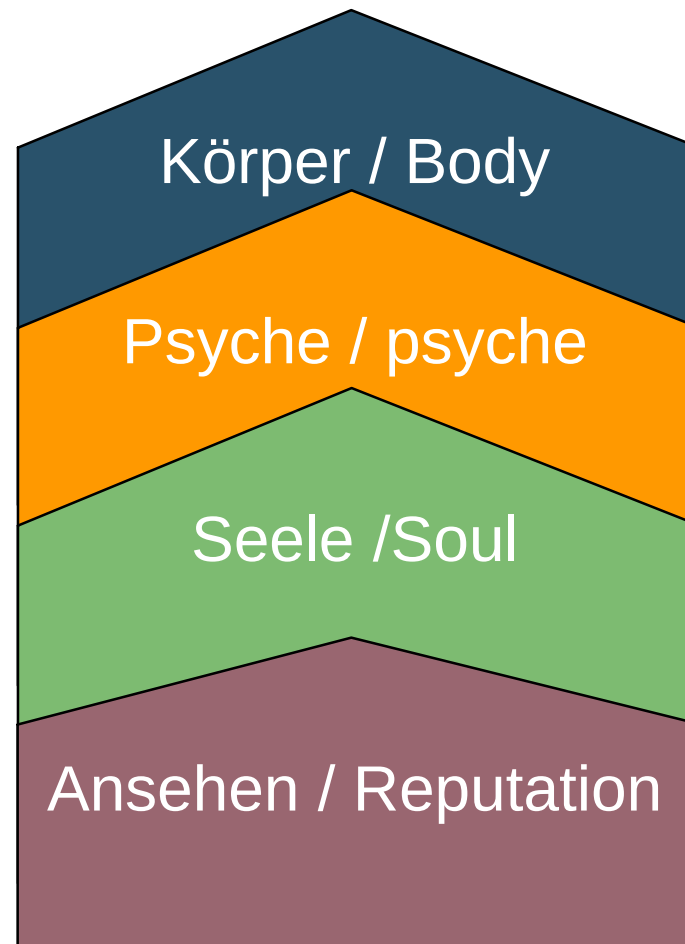
Der Schutz der Persönlichkeit nach ZGB Art. 28

Der Schutz der Persönlichkeit

Wer in seiner Persönlichkeit widerrechtlich verletzt wird, kann zu seinem Schutz gegen jeden, der an der Verletzung mitwirkt, das Gericht anrufen.

Eine Verletzung ist widerrechtlich, wenn sie nicht

- durch Einwilligung des Verletzten
by consent of the injured person
- durch das öffentliche Interesse, oder
public interest
- durch das Gesetz gerechtfertigt ist
justified by the law



Rechtliche Folgen von Persönlichkeitsverletzungen im Datenbereich

- **Zivilrechtliche Forderungen:**
 - u.a. Genugtuung, Schadenersatz, Gewinnherausgabe, Unterlassung, Beseitigung, Feststellung, Mitteilung
 - Vertragsverletzungen, Verwertungsverbote
- **Untersuchung/Empfehlung des EDÖB**
- **Publikation, Vollstreckung über Bundesverwaltungsgericht**
- **Strafrechtliche Sanktion:**
 - nur bei Verletzung von Informations-, Melde-, Auskunfts- und Registrierungspflichten (Busse bis CHF 10'000)
 - schärfer bei Erfüllung von Straftatbeständen des StGB

Allgemeine Grundsätze Datenschutz

Besonders Schützenswerte Daten sind:

- > die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten betreffend,
- > Die **Gesundheit**, Intimsphäre oder die Rassenzugehörigkeit betreffend.
- > Massnahmen der sozialen Hilfe,
- > Administrative oder strafrechtliche Verfolgungen und Sanktionen

Allgemeine Grundsätze Datenschutz

Personendaten

- > Sind alle Angaben über eine bestimmte oder bestimmbare natürliche oder juristische Person.
 - Patientendaten, Personaldaten, Lieferanten

Bearbeitung

- > Umfasst jeden Umgang mit Personendaten, wie das Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntmachen oder Vernichten.
 - Diagnostik, Forschung

Bekanntgeben

- > Umfasst jedes Zugänglichmachen von Personendaten, wie das Einsicht gewähren, Auskunft geben, Weitergeben oder Veröffentlichen.
 - Übermittlung Befund, Forschungsdaten

Allgemeine Grundsätze Datenschutz

Unverschlüsselt

- > Datenverarbeitungsprogramme
 - Patientendaten im Pathowin+, Krebsregister
 - Personaldossier

Pseudonymisierte Verschlüsselte Daten

- > Ist das Verändern personenbezogener Daten, die Identifikation wird durch einen Code ersetzt. Die Code-Liste wird bei einer unabhängigen Stelle gelagert.
 - Diese Daten unterliegen dem Datenschutz.
 - Z.b. Verschlüsselte Patientendaten für ein Forschungsprojekt.

Anonymisierte Daten:

- > Ist das Verändern personenbezogener Daten derart, dass diese Daten nicht mehr einer Person zugeordnet werden können.
 - Diese Daten unterliegen nicht dem Datenschutz.

Allgemeine Grundsätze Datenschutz

Zweckbindung:

- > Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde oder aus den Umständen ersichtlich ist.
 - Z. B. Patientendaten PathoWin+

Verhältnismässigkeit:

- > Die Bearbeitung der Daten muss für die Erreichung des Zwecks geeignet und notwendig sein.
 - Nur soviel Daten wie nötig.

Datenzugriff:

- > Der Datenzugang ist auf Personen zu beschränken, welche diese Daten zwingend für ihre Aufgabenerfüllung benötigen.
 - Zutritt-, und Zugangsberechtigung für Software, Archive etc.

Begriffe

Was ist ein Persönlichkeitsprofil:

- Alle Daten müssen durch angemessene technische und organisatorische Massnahmen gegen Verlust und unbefugtes Bearbeiten geschützt werden.

Datensicherung:

- > Alle Daten müssen durch angemessene technische und organisatorische Massnahmen gegen Verlust und unbefugtes Bearbeiten geschützt werden.

Datensammlungen

- > Datensammlung am Institut
- > - Pathowin+
- > - Tumorbank
- > - Personalinformationssystem
- > - Personalakten
- > - Auftragsformulare
- > - Lieferantendaten
- > - **Jede Excelliste mit persönlichen Daten**

Datenschutz am Institut für Pathologie

- > Ziel
- > Zuständigkeiten
- > Schulung und Dokumentation
- > Allgemeine Grundsätze Datenschutz
- > **Herausgabe von Daten**
- > Grenzüberschreitender Datenverkehr
- > Organisatorische und technische Massnahmen
- > Diskussion

Bekanntgabe von Patientendaten

ZULÄSSIG

INNERHALB des Behandlungs- /
Administrativteams

Umfasst alle Personen, die am
Behandlungs- und Administrativprozess
beteiligt sind.

Es gilt das Prinzip der Verhältnis-
mässigkeit und Zweckbindung

UNZULÄSSIG

an alle **DRITTPERSONEN**

Als Drittperson gelten alle Personen,
welche NICHT am Behandlungs- oder
Administrativprozess beteiligt sind.

Bspw. Angehörige, MA anderer Kliniken
oder Institute, Arbeitgeber, Polizei,
Versicherungen etc.



Die Bekanntgabe von Patientendaten **an Dritte ist zulässig** bei
Vorliegen eines **Rechtfertigungsgrundes**

Bekanntgabe von Patientendaten

Rechtfertigungsgründe für Weitergabe von Patientendaten an Dritte:

- **Einwilligung des Patienten, Formlos mündlich oder schriftlich**
 - Angehörige nur mit Einwilligung des Patienten
 - Berichtsversandt an Mit- oder Nachbehandelnde Gesundheitsperson, stillschweigende Einwilligung wird angenommen.
 - Forschung
- **An der Behandlung beteiligte Dritte**
- **Gesetzliche Grundlage**
 - Meldepflicht Polizei, KESB, - Verbrechen, aussergewöhnliche Todesfälle

Bekanntgabe von Patientendaten

Rechtfertigungsgründe für Weitergabe von Patientendaten an Dritte:

- Krankenversicherer und Unfallversicherer: Der Leistungserbringer muss dem Versicherer alle Angaben machen, die er zur Abklärung der Leistungsansprüche benötigt (Art. 54a UVG, Art. 42 Abs. 3 und 5 KVG).
 - Weitergabe von Befunden immer die Institutsleitung informieren.
- Kantonsarzt
- Akute Notstandssituation

Einsichtrecht / Datenherausgabe an den Patienten

- Jeder Patient hat auf Verlangen das Recht auf Einsicht sowie Erläuterung der ihn betreffenden Personendaten.
- Mitarbeiter/in Einsicht ins Personaldossiers.
 - In der Regel bei Patienten auf schriftlichen Antrag.
 - Identifikation des Antragstellers prüfen.
 - Daten vor Zugriff unberechtigter schützen.
 - Ausdruck, Fotokopie aller Daten des Betroffenen
 - Einsicht vor Ort, wenn Betroffener einverstanden
 - Kann auch elektronisch erfolgen

Datenschutz am Institut für Pathologie

- > Ziel
- > Zuständigkeiten
- > Schulung und Dokumentation
- > Allgemeine Grundsätze Datenschutz
- > Herausgabe von Daten
- > **Grenzüberschreitender Datenverkehr**
- > Organisatorische und technische Massnahmen
- > Diskussion

Umgang mit nicht anonymisierten Daten

Grenzüberschreitender Versandt

- Art. 6 DSG: Die grenzüberschreitende Bekanntgabe von Personendaten unterliegt besonders strengen Vorschriften. Dabei spielt das Vorhandensein einer Gesetzgebung im Zielland, die einen angemessenen Datenschutz garantiert, eine entscheidende Rolle.
- Insgesamt ist dies nur bei wenigen Staaten der Fall. Der EDÖB führt eine Länderliste der «sicheren» Staaten. Dies sind aktuell: **die Länder der EU, Kanada, Argentinien, Uruguay, Israel, Neuseeland, Australien (bedingt)**
- Drittstaaten nur mit Vertrag, Vorlage Edöp

Grenzüberschreitender Versandt



Datenschutz am Institut für Pathologie

- > Ziel
- > Zuständigkeiten
- > Schulung und Dokumentation
- > Allgemeine Grundsätze Datenschutz
- > Herausgabe von Daten
- > Grenzüberschreitender Datenverkehr
- > **Organisatorische und technische Massnahmen**
- > Diskussion

Umgang mit nicht anonymisierten Daten

Papier

- **Alle Patientendaten** (Pathologieberichte, Arztberichte, usw.) sind vor zugriff Dritter zu schützen.
- Beim verlassen des Arbeitsplatzes Computer zur weiteren Nutzung sperren.
- Die Dokumente müssen nach dem Verlassen des Arbeitsplatzes weggesperrt werden.
- **Die Weitergabe** von Dokumenten in Papierform muss in einem Blickdichten Couvert erfolgen.
- **Aktenvernichter** erfüllt mindestens die Norm DIN 4 (2x15) oder Einsatz Datarec.

Umgang mit nicht anonymisierten Daten

Vernichtung

- > **Datenträger** müssen zur Entsorgung der Informatikabteilung abgegeben werden.
- > **Weitergabe** von Datenträgern mit Patientendaten: Diese müssen vor einer Weitergabe durch die IT gelöscht werden
- > **Aktenvernichtung** erfüllt mindestens die Norm DIN 4 (2x15) oder Datarec.
- > **Gewebe**: wird über die Autopsie entsorgt
- > **Objektträger und Blöcke**: Via TD, begleiteter Transport ins KVA

Umgang mit nicht anonymisierten Daten

Elektronischer Versand nur Verschlüsselt:

- HIN-E-Mail-Adressen an HIN-E-Mail
- Andere Möglichkeiten sind elektronische Datenträger (wie beispielsweise USB-Stick, CD oder DVD) oder der FTP-Server. Diese müssen passwortgeschützt sein, zudem müssen die Daten verschlüsselt darauf gespeichert werden.
- Faxübermittlung, wenn möglich Vermeiden, Empfänger müssen

Archivierung Löschen von Daten

Archivierung

- > Solange wie es für die Gesundheit des Patienten notwendig jedoch mindestens **am IFP 20 Jahre**.
- > Forschungsrelevante Daten können länger aufbewahrt werden nach Ablauf der Frist müssen diese gelöscht werden, **am IFP 10 Jahre**.
- > Archive Zutritts geregelt und dokumentiert
- > Elektronische Daten Zugriff geregelt und Verschlüsselt.
- > Auf privaten Geräten dürfen keine Schützenswerten Daten verarbeitet werden.

Archivierungszeiten

	Gewebe (nativ)	Schnitte (KPath)	Schnitte (PMD)	Blöcke (Kpath)	Blöcke (PMD)	Ausstrich Zytologie	DNA MolPath	Epoxydharz- Blöcke und Ultradünnschnitte (EM)	FISH- Präparate	Biobank Bern, Kryomaterial
Dauer	4 Wochen	20 Jahre	20 Jahre	30 Jahre	30 Jahre	20 Jahre	20 Jahre	30 Jahre	3 Monate	mindestens 10 Jahre

	Auftragsformulare / Befund	Finanzdokumente / Verträge	Ringversuche / Laborvergleiche	Personalaufzeichnungen	Technische Aufzeichnungen	QM-Dokumente	Sitzungsprotokolle	Labordokumente	Dokumente Arbeits- und Umweltschutz
Dauer	10 Jahre	gemäss Richtlinie der Universität Bern	10 Jahre	10 Jahre	10 Jahre	10 Jahre	10 Jahre	10 Jahre	gemäss Sicherheitskonzept