19. März 2025

KI und Datenschutz

KANTON solothurn

KI und Datenschutz

01

Grundlagen zu Personendaten

02

Pseudonymisieren vs. Anonymisieren

03

Wann braucht es eine Schutzbedarfsanalyse? Wie wird diese erstellt? Wann braucht es ein Informationssicherheits- und Datenschutzkonzept – ISDS?

04

Awareness Kampagne ABMH "KI sicher nutzen"

SO!GPT – KI für den Kanton Solothurn

Grundlagen zu Personendaten

Wann wurde das erste Datenschutzgesetzt weltweit erlassen?

1970 verabschiedete Hessen das weltweit erste Datenschutzgesetz

Informations- und Datenschutzgesetz – InfoDG

Personendaten §6 abs.2

Personendaten (Daten) sind Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person (betroffene Person) beziehen.

Besonders schützenswerte Personendaten

§6 abs. 3

Besonders schützenswerte Personendaten sind Angaben über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, über die Gesundheit, die Intimsphäre, die rassische und ethnische Herkunft, über Massnahmen der sozialen Hilfe sowie über administrative oder strafrechtliche Verfolgungen und Sanktionen.

Grundlagen zu Personendaten

Bundesgesetz über den Datenschutz – DSG

Personendaten Art.5 abs. a und b

a. alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen;

b. betroffene Person: natürliche Person, über die Personendaten bearbeitet werden

Besonders schützenswerte Personendaten Art. 5 abs. c 1-6

1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,

2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,

3. genetische Daten,

4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,

5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,

6. Daten über Massnahmen der sozialen Hilfe;

Grundlagen zu Personendaten

Definition von wichtigen Begriffen

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;

Bekanntgeben: das Übermitteln oder Zugänglichmachen von Personendaten;

Grundlagen zu Personendaten

Definition von wichtigen Begriffen

Profiling: jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

Profiling mit hohem Risiko: Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;

Anonymisierung vs. Pseudonymisierung

Der Unterschied zwischen **Anonymisieren** und **Pseudonymisieren** liegt hauptsächlich im Grad der Schutzmassnahmen und der Möglichkeit, die ursprünglichen Daten wiederherzustellen:

1.Pseudonymisierung

1. **Definition**: Bei der Pseudonymisierung werden personenbezogene Daten so verändert, dass sie ohne zusätzliche Informationen nicht mehr direkt einer Person zugeordnet werden können. Diese zusätzlichen Informationen werden separat gespeichert.
2. **Rückführbarkeit**: Die Identität der Person kann wiederhergestellt werden, wenn man Zugriff auf die zusätzlichen Informationen (z. B. eine Zuordnungstabelle) hat.
3. **Beispiel**: Ein Patientendatensatz wird mit einer zufälligen Nummer statt mit dem echten Namen versehen. Die Zuordnungstabelle, die Name und Nummer verknüpft, wird separat und sicher aufbewahrt.

Anonymisierung vs. Pseudonymisierung

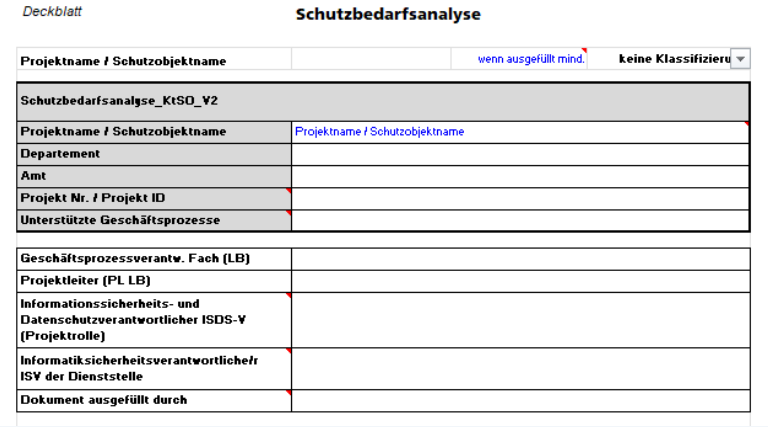
Der Unterschied zwischen **Anonymisieren** und **Pseudonymisieren** liegt hauptsächlich im Grad der Schutzmassnahmen und der Möglichkeit, die ursprünglichen Daten wiederherzustellen:

1.Anonymisierung

1. **Definition**: Bei der Anonymisierung werden personenbezogene Daten so verändert, dass sie nicht mehr einer bestimmten Person zugeordnet werden können – weder direkt noch indirekt.
2. **Rückführbarkeit**: Eine Rückverfolgung auf die ursprüngliche Person ist nicht mehr möglich.
3. **Beispiel**: Eine Kundenliste wird so verändert, dass Namen, Adressen und andere Identifikationsmerkmale vollständig entfernt oder unkenntlich gemacht werden.

Merkmal	Anonymisierung	Pseudonymisierung
Identifizierbarkeit	Nicht möglich	Möglich mit Zusatzinfos
Datenschutzlevel	Höher	Geringer
Rückführbarkeit	Unmöglich	Möglich (unter Bedingungen)

Schutzbedarfsanalyse - SchubAn



Deckblatt **Schutzbedarfsanalyse**

Projektname / Schutzobjektname		wenn ausgefüllt mind.	keine Klassifizieru

Schutzbedarfsanalyse_KtSO_V2	
Projektname / Schutzobjektname	Projektname / Schutzobjektname
Departement	
Amt	
Projekt Nr. / Projekt ID	
Unterstützte Geschäftsprozesse	

Geschäftsprozessverantw. Fach (LB)	
Projektleiter (PL LB)	
Informationssicherheits- und Datenschutzverantwortlicher ISDS-V (Projektrolle)	
Informatiksicherheitsverantwortliche/r ISV der Dienststelle	
Dokument ausgefüllt durch	

Was ist eine Schutzbedarfsanalyse?

- Die **Schutzbedarfsanalyse** ist ein zentraler Bestandteil des **IT-Sicherheits- und Datenschutzmanagements**. Sie dient dazu, die Sensibilität von Daten, Systemen und Prozessen zu bewerten und darauf basierend geeignete Sicherheitsmassnahmen zu definieren.
- Die Schutzbedarfsanalyse bewertet, wie stark ein bestimmtes **System**, eine **Anwendung** oder ein **Prozess** geschützt werden muss.

Wann braucht es ein ISDS-Konzept?

Wann braucht es ein ISDS?

1. **Hoher Schutzbedarf für Vertraulichkeit, Integrität oder Verfügbarkeit**

   Beispiel: In einer Schule: Schülerakten mit Noten und Gesundheitsdaten müssen besonders geschützt werden.

2. **Gesetzliche oder regulatorische Vorgaben**

   In einer Schule: Die Schule verarbeitet Gesundheitsdaten von Schülern, die nach Datenschutzgesetzen besonders geschützt werden müssen.

3. **Erhöhtes Risiko durch Cyberangriffe oder Datenmissbrauch**

   In einer Schule: Schüler und Lehrpersonen nutzen Cloud-Dienste → Es braucht klare Regeln für den Datenschutz.

4. **Externe Anforderungen durch Partner, Kunden oder Zertifizierungen**
   1. Falls Geschäftspartner oder Kunden ein hohes Sicherheitsniveau verlangen.
   2. Falls eine Zertifizierung (z. B. ISO 27001) angestrebt wird.

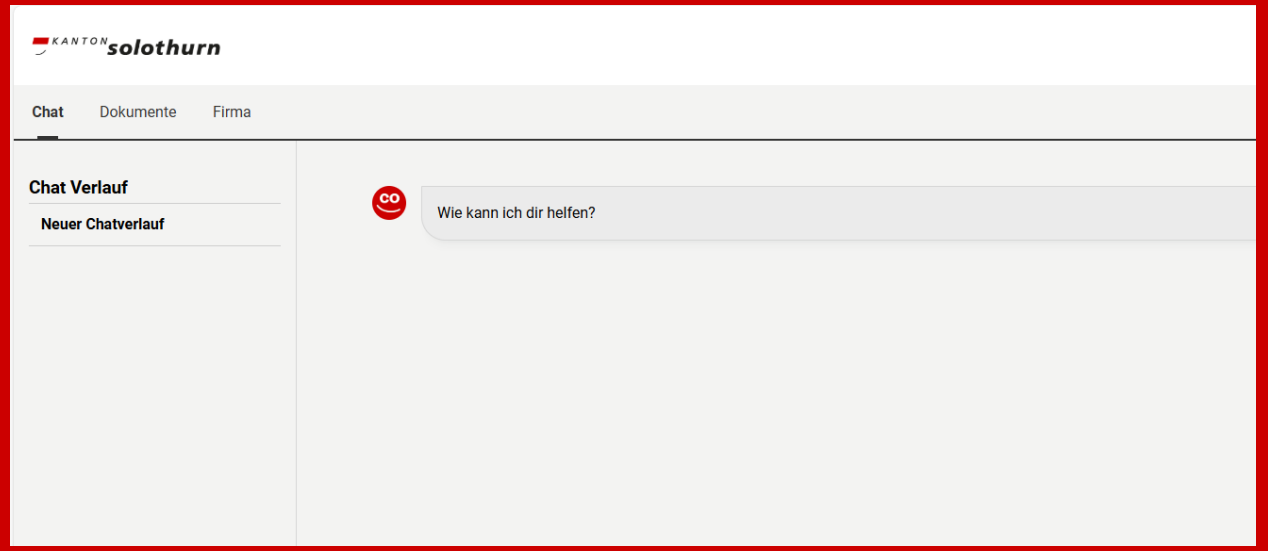
5. **Notwendigkeit der Risikominimierung und Krisenvorsorge**

   In einer Schule: Prüfungsdaten oder Online-Lernplattformen müssen verfügbar bleiben.

Berufsbildungszentren
und Kantonsschulen

KI sicher nutzen

KI für den Kanton – SO!GPT



Amt für Berufsbildung, Mittel- und Hochschulen

KI und Datenschutz

KI bringt Fortschritt – doch was ist mit unseren Daten?
Datenschutz muss mitziehen, sonst zahlen wir den Preis.
Die Zukunft gehört denen, die beides im Griff haben!

Christof Kramer
ABMH – IT Kompetenzzentrum
christof.kramer@dbk.so.ch