Datenschutz in der Anwaltskanzlei: Plichten, Praxis und Fallstricke

Weiterbildung 2025
20. Mai 2025
Chur


Digital crime
Internet crime
Internet fraud
Trojan Horses
Internet addiction
Phishing
Kiddie porn
Internet scams
Malware
Identity theft
Internet sex
Email hoaxes
Stalking
Pornography
Email scams
Hacking
Child pornography
Viruses
Hackers
Spam
Credit card fraud
Internet gambling
Spyware
Email spoofing
Worms
Chat room predators

Agenda

1. Allgemeine Grundlagen
2. Datenschutzrechtliche Vorkehrungen
3. Ausblick
4. Zusammenfassung

Gesetzliche Gegebenheiten:

- Europ. Datenschutzverordnung (DSGVO)
- Eidg. Datenschutzgesetz (DSG)
- Eidg. Schengen-Datenschutzgesetz (SDG)
- Rev. Eidg. Datenschutzgesetz (rev.DSG)
- Kant. Datenschutzgesetz (KDSG)

Gesetzliche Gegebenheiten:

Bundesgesetz über den Datenschutz (1.7.1993/**1.9.2023**):

- Bundesorgane
- Private

Kantonales Datenschutzgesetz (1.1.2002/**1.1.2026**):

- Kantonsorgane
- Bezirksorgane
- Kreisorgane
- Gemeindeorgane

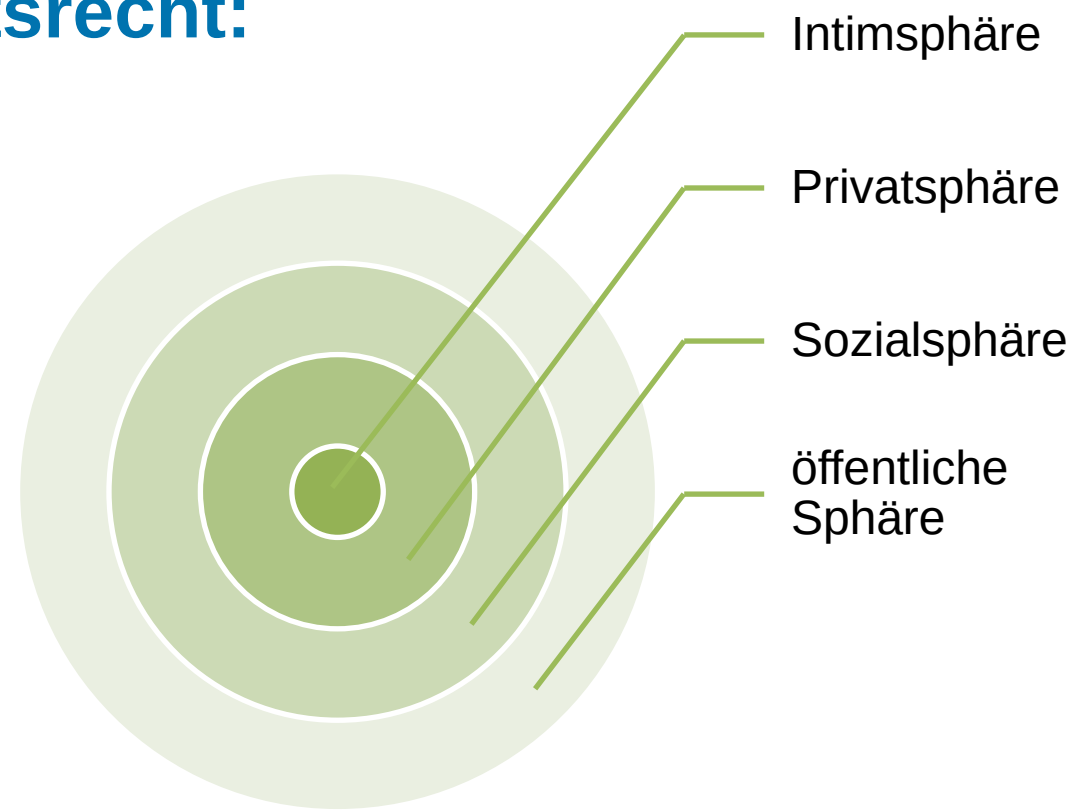
Neuerungen revDSG

- Anwaltskanzleien gelten als Verantwortliche (Art. 5 lit. j DSG)
- Erweiterte Informationspflicht (Art. 25 DSG)
- Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG)
- Technische und organisatorische Massnahmen (TOMs) (Art. 8 DSG)
- Meldung von Datenschutzverletzungen an EDOEB (Art. 24 DSG)

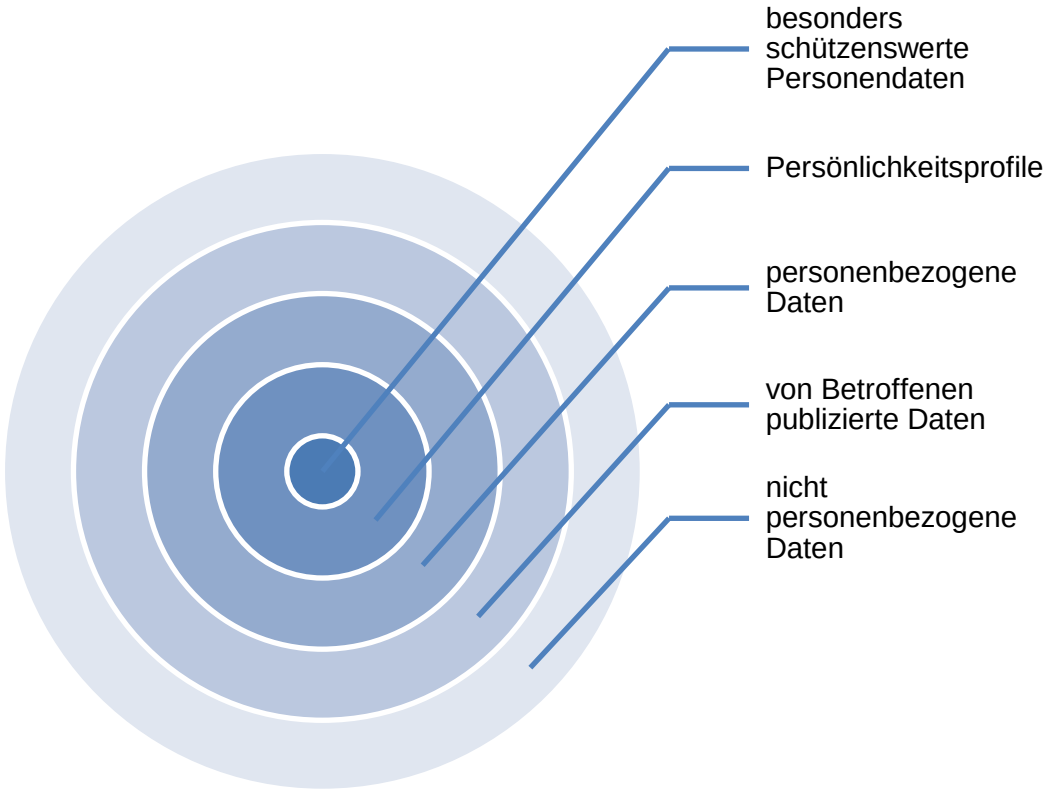
Typische Mängel

- Fehlende oder unvollständige Datenschutzerklärung
- Unzulässige Datenübermittlung
- Mangelhafte IT-Sicherheit
- Fehlender oder fehlerhafter Auftragsdatenbearbeitungsvertrag
- Unklare oder fehlende Einwilligung bei sensiblen Daten
- Unzureichende Mitarbeiterschulung
- Fehlerhafte oder verspätete Auskunftserteilung
- Probleme bei der mobilen Berufsausübung (Homeoffice, unterwegs)
- Fehlendes Verzeichnis der Bearbeitungstätigkeiten

Persönlichkeitsrecht:



Datenarten:


besonders schützenswerte Personendaten
Persönlichkeitsprofile
personenbezogene Daten
von Betroffenen publizierte Daten
nicht personenbezogene Daten

Besonders schützenswerte Personendaten

- Daten über religiöse, weltanschauliche, politische Ansichten
- Daten über Gesundheit, Intimsphäre oder Rassenzugehörigkeit
- Daten über Massnahmen der sozialen Hilfe
- Daten über administrative oder strafrechtliche Verfolgungen
- Genetische Daten
- Biometrische Daten

Grundsätze (Plichten):

- Prinzip der Rechtmässigkeit
- Prinzip der Verhältnismässigkeit, Datenminimierung
- Prinzip der Zweckgebundenheit
- Prinzip der Integrität, Richtigkeit der Daten, Vertraulichkeit
- Prinzip der Datensicherheit, Nachweisbarkeit
- Prinzip der Transparenz

Recht auf Auskunft

Jede Person – unabhängig von Alter, Wohnsitz und Nationalität – hat das Recht, Auskunft über die zu ihrer Person gespeicherten Daten zu verlangen.

Verweigerung/Einschränkung:

- gesetzl. Bestimmung gibt Möglichkeit (Berufsgeheimnis)
- überwiegende eigene Interessen
- überwiegende schützenswerte Interessen Dritter
- Daten werden nicht Dritten bekanntgegeben

Recht auf Auskunft

Personen können Auskunft verlangen:

- über alle zu ihrer Person in einer Datensammlung vorhandenen Daten, einschliesslich der Angabe, woher sie stammen
- über den Zweck der Bearbeitung
- über die Kategorien der bearbeiteten Daten
- über die Beteiligten an einer Datensammlung
- über Personen und Stellen, an die Daten übermittelt werden

- Auskunft **schriftlich;** elektronisch, mündlich oder vor Ort möglich

Akteneinsichtsrecht

Gesetzliche Grundlage:

Art. 29 Abs. 2 BV
Art. 25 DSG Auskunftsrecht
Art. 26 DSG Einschränkungen Auskunftsrecht

Rechte der Betroffenen:

Auskunft
Berichtigung
Sperrung
Beratung
Beschwerde

Technische und organisatorische Massnahmen

- Technische Massnahmen
  - Verschlüsselung (E-Mails und Daten, Transport und Speicherung)
  - Zwei-Faktoren-Authentifizierung (Stichwort Homeoffice)
  - Firewalls und Antivirussoftware
  - Regelmässige Softwareupdates
  - Backups

- Organisatorische Massnahmen
  - Zugriffsmanagement
  - Vertraulichkeitserklärungen für Mitarbeitende
  - Schulungen
  - Notfallkonzept bei Datenschutzverletzungen
  - Dokumentation der getroffenen Massnahmen

Persönlichkeitsverletzung

Art. 30 DSG

- Bearbeitung von Personendaten entgegen der Grundsätze
- Bearbeitung von Personendaten entgegen dem ausdrücklichen Willen des Betroffenen
- Bekanntgabe besonders schützenswerter Personendaten

aber

Art. 31 DSG

- Einwilligung der betroffenen Person liegt vor
- überwiegendes privates oder öffentliches Interesse ist gegeben
- Rechtfertigung durch Gesetz

Cloud-Dienste (1)[1)]

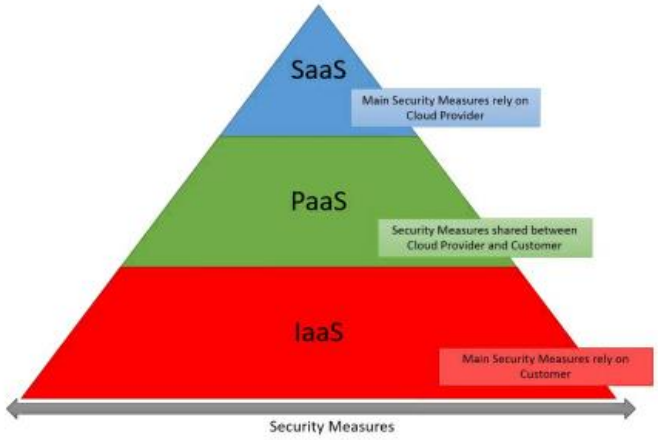
1) https://digital.sav-fsa.ch/documents/1060627/1169162/Gutachten_Thouvenin_Schwarzenegger_Schiller.pdf/0f612227-5274-943b-a82f-c1d6d99acef0?t=1614770740068

Allgemeines

- Dezentrales und verteiltes Speichersystem
- Verschlüsselung
- Ausprägung

Rechtliche Auswirkungen

- Strafrecht Art. 321 StGB
- Datenschutzrecht



intern

Haupt-Verantwortung bei Provider

Haupt-Verantwortung geteilt

Haupt-Verantwortung bei Kanzlei

Cloud-Dienste (2)[2]

Erkenntnisse

- Nutzung von Cloud-Diensten möglich
- Verschlüsselung in Kanzlei und Schlüssel in Kanzlei:
  - straf- und datenschutzrechtlich unbedenklich
- Verschlüsselung durch Provider
  - Cloud-Provider = Hilfsperson =) keine Verletzung Berufsgeheimnis
    jedoch, Gutachten Wohlers =) Cloud-Provider keine Hilfsperson[3]
  - Cloud-Provider = Auftragsdatenbearbeiter
    =) Vertrag:
    - ✓ Verantwortung
    - ✓ Schlüsselmanagement
    - ✓ Kontrollrechte
    - ✓ Geheimhaltungsvorschriften
    - ✓ Unterauftragsverhältnis
    - ✓ Speicherung in der Schweiz
    - ✓ Gerichtsstand und anwendbares Recht
    - ✓ Auflösung

2 https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess.pdf

3 Gutachten Wohlers vom 5. Dez. 2015 zuhanden DSB ZH

Cloud-Dienste (3)

- Hinweis auf Nutzung von Cloud-Diensten in der Anwaltsvollmacht

Nutzung von Cloud-Diensten

Die Anwaltskanzlei (Name der Kanzlei) setzt zur effizienten Bearbeitung des Mandats moderne IT-Infrastrukturen ein, insbesondere auch Cloud-Dienste von sorgfältig ausgewählten Anbietern mit Sitz oder Serverstandort in der Schweiz oder einem Land mit angemessenem Datenschutzniveau.

Ich nehme zur Kenntnis und erkläre mich damit einverstanden, dass meine Personendaten – einschliesslich besonders schützenswerter Daten gemäss Art. 5 lit. c DSG – im Rahmen der Mandatsführung in solchen Cloud-Systemen gespeichert und bearbeitet werden können. Die Kanzlei stellt sicher, dass die Anbieter geeignete technische und organisatorische Massnahmen zum Schutz dieser Daten treffen und die Vertraulichkeit gewahrt bleibt.

Diese Einwilligung erfolgt freiwillig und kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Ein Widerruf kann jedoch dazu führen, dass gewisse Dienstleistungen nur eingeschränkt oder gar nicht erbracht werden können.

E-Mail-Verkehr (1)

Probleme

- Fehlender Schutz bei unverschlüsselter Kommunikation
- Übermittlung besonders schützenswerter Personendaten grundsätzlich unzulässig
- Fehleradressierung
- Unzureichende Zugriffskontrollen
- Speicherung in ausländischen Clouds

Empfehlungen

- Verschlüsselung
- Einwilligung einholen
- Vermeidung heikler Daten
- Schulung Personal
- Kanzlei-E-Mail-Richtlinien

E-Mail-Verkehr (2)

Einbindung in Anwaltsvollmacht

Beispiel:

Ich bin damit einverstanden, dass die Anwaltskanzlei (Name der Kanzlei) mit mir via unverschlüsselter E-Mail kommuniziert und mir auf diesem Weg auch Personendaten übermittelt.

Ich nehme zur Kenntnis, dass damit gewisse Risiken verbunden sind (z. B. fehlender Schutz der Vertraulichkeit, unbefugter Zugriff durch Dritte) und entbinde die Kanzlei im gesetzlich zulässigen Rahmen von der Verantwortung für allfällige Datenschutzverletzungen, die aus der unverschlüsselten E-Mail-Kommunikation entstehen.

Datenschutzerklärung

Das DSG (Art. 19 und 20) verpflichtet die Verantwortlichen, betroffene Personen über die Bearbeitung ihrer Personendaten zu informieren.

Checkliste

1. Zweck
2. Umfang (Kategorien)
3. Speicherung
4. Zugriffsberechtigung
5. Datenweitergabe (Ausland)
6. Aufbewahrungsdauer
7. Rechte der Betroffenen
8. Datensicherheit
9. Soziale Medien
10. Externe Dienste
11. Änderungen
12. Datenschutzverantwortlicher

Cyberrisiken bei Ransomattacken (1)

- Angriff
  - Infizierung Netzwerk, Sperrung und Zugriff auf Daten
  - Lösegeldforderung
  - Alle werden angegriffen
  - Täterschaft spezialisiert und industriell organisiert

- Reaktion auf Angriff
  - Taskforce
  - Externe Experten beiziehen
  - Kommunikation
  - Meldepflicht an EDOEB
  - Beweissicherung
  - Dokumentation

Cyberrisiken bei Ransomattacken (2)

- Sicherungsmassnahmen
  - Passwörter
  - Zwei-Faktor-Authentifizierung
  - Back-up
  - Sicherheitstechnologien (z.B. Firewalls)
  - Penetrationstests
  - Schulung
  - Notfallblatt (in Papier)
  - Versicherungsschutz

Aktenvernichtung

- Mandats-, Personalakten, Verträge von Dienstleistern
- Vernichtung sobald der Zweck es erlaubt (Art. 6 Abs. 4 DSG), aber gesetzliche Aufbewahrungsfristen beachten (in der Regel 10 Jahre)
- Achtung Originalakten
- Vernichtung von Papierakten
  - kanzleiinterner Schredder (Sicherheitsstufe P 4 oder höher)
  - zertifizierter Aktenvernichtungsdienstleister
  - GEVAG (persönliche Entsorgung)
- Löschung digitaler Akten
  - Speicherort lokalisieren (PC, Cloud, Mailserver, Handy etc.)
  - lokale Datenträger mit Löschsoftware überschreiben
  - physische Vernichtung Festplatte
  - Server, Cloud, E-Mail (inkl. Backups) endgültig löschen
- Regelmässigkeit sicherstellen
- Verantwortlicher bestimmen

Justitia 4.0 Digitalisierung der Justiz

- Elektronische Justizakte (eJustizakte)
- Plattform justitia.swiss (öffentlich-rechtliche Körperschaft)
- Transformation und Schulung

- BG über die Plattformen für elektronische Kommunikation in der Justiz (BEKJ)
  - Akteure werden zur Nutzung der Plattform verpflichtet
- Pilotprojekte in den Kantonen (StA FR, GE, BL)
- Vereinbarung unter den Kantonen unterzeichnet
- 2027 Einführung geplant

Zurückhaltung ist ein guter Ratgeber