

sovt-Datenschutzberatung

Datenschutz als ein Qualitätsmerkmal
in Unternehmen und Krankenhäusern

Lothar Bräutigam, sovt
(Dipl. Inform.)



Fritz-Glenz-Str. 3
64297 Darmstadt
Tel. (06151) 62 60 2
Fax (06151) 62 60 6
Mail info@sovt.de

Datenschutz & IT-Sicherheit

- Beratung zum betrieblichen Datenschutz mit den Schwerpunkten
 - Arbeitnehmerdatenschutz
 - Datenschutz im Gesundheitswesen
- Tätigkeit als externer Datenschutzbeauftragter
- Datenschutzkonzepte und Vorabkontrollen
- Durchführung von Datenschutzaudits
- Coaching von internen Datenschutzbeauftragten
- Seminare zum betrieblichen Datenschutz
- Unterstützung beim Abschluss von Betriebsvereinbarungen



Fritz-Glenz-Str. 3
64297 Darmstadt

Tel. (06151) 62 60 2

Fax (06151) 62 60 6

eMail: info@sovt.de

Internet: www.sovt.de

Allgemeines
Datenschutzrecht
(BDSG, LDSG)

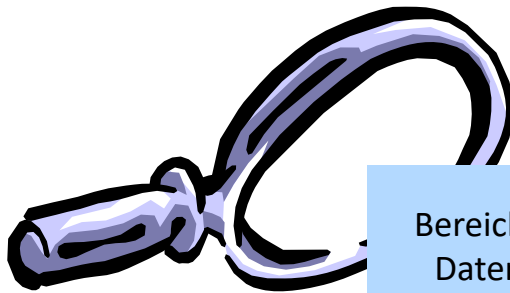
Bereichsspezifisches
Datenschutzrecht



**Datenschutz
im Betrieb**

Diverse bereichsspezifische Datenschutzregelungen, z.B.

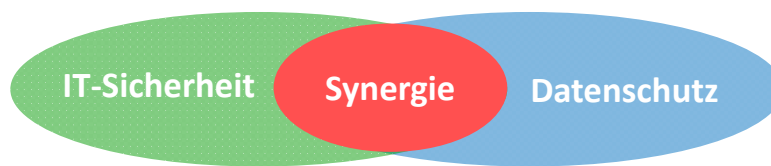
- Telekommunikationsgesetz, Telemediengesetz, Sozialgesetzbuch
- Berufsgeheimnisse (§ 203 StGB)
- Betriebsvereinbarungen zum Beschäftigtendatenschutz



Bereichsspezifisches
Datenschutzrecht

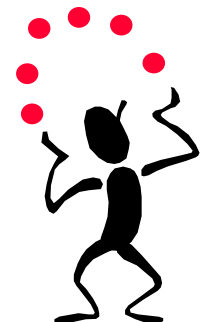
Viele bereichsspezifische Datenschutzregelungen, z.B.

- Telekommunikationsgesetz, Telemediengesetz, DEÜV
- Sozialgesetzbuch
- Landeskrankenhausgesetz
- RöV, StrahlenSchV, TransfusionsG, ...
- Betriebsvereinbarungen zum Beschäftigtendatenschutz
- Personalaktegeheimnis u.v.m.



- Höhere IT-Sicherheit durch mehr Datenschutz
- Vertrauen von Kunden (in den sicheren Umgang mit ihren Daten)
- Vertrauen der Mitarbeiter, höhere Motivation
- Sicherheit geschäftskritischer Daten und Prozesse
- Vermeidung von Bußgeldern, Haftungs- bzw. Schadensersatzrisiken

- **Zulässigkeit der Verarbeitung**
 - Erforderlichkeit
 - Zweckbindung
- **Rechte des Betroffenen**
 - Auskunft, Benachrichtigung
 - Löschung, Sperrung, Berichtigung
- **Durchführungspflichten der verantwortlichen Stelle**
 - Datengeheimnis
 - Technische und organisatorische Maßnahmen
 - Verzeichnis
- **Kontrolle des Umgangs mit personenbezogenen Daten**
 - Betrieblicher Datenschutzbeauftragter
 - Aufsichtsbehörde
- **Regelungen zu Gesetzesverletzungen**
 - Strafvorschriften
 - Bußgeldvorschriften
 - Schadensersatz



Aufgaben nach §§ 4f, 4g BDSG:

- „auf Einhaltung des Datenschutzes ... hinwirken“
- ordnungsgemäße Anwendung von DV-Anlagen überwachen (→ Datenschutz-Audits)
- Unterrichtung, Qualifizierung der Beschäftigten
- zuständig für Vorabkontrolle
- führt das Verzeichnis (nach § 4e BDSG) und macht es auf Antrag jedermann verfügbar
- Ansprechpartner für Betroffene

externer DSB

Komplette Übernahme der Aufgabe durch sovt

interner DSB

- Datenschutzberatung zu einzelnen Aufgaben
- Coaching des internen DSB

Vor- und Nachteile beider Lösungen?

- Wie läuft die Zusammenarbeit ab?
- Wie hoch sind Aufwand bzw. Kosten?
- Wie sieht die Vertragsgestaltung aus?

Mein Ansatz:

1. Datenschutzaudit / Bestandsaufnahme als Einstieg

- Eruierung des Status quo und der Defizite
- Aufwand für spätere Tätigkeit als DSB lässt sich besser abschätzen
- Chance zum Kennenlernen

2. Laufende Tätigkeit als externer DSB

- Üblicherweise mit einer 3jährigen Laufzeit

I. Aufbau des Datenschutzes

1. Bestandsaufnahme zum Datenschutz

über Interviews (z.B. mit GF, IT-Abt., Pers.-Abt. BR) und Prüfung ausgewählter Bereiche vor Ort

- Welche Rechtsvorschriften und internen Regelwerke?
(Datenschutzrichtlinien, Betriebsvereinbarungen, IT-Sicherheitskonzept)
- Welche personenbezogenen Daten in welchen IT-Verfahren?
- Welche technischen und org. Sicherheitsmaßnahmen?

2. Präsentation der Ergebnisse des Datenschutzaudit

- Risiken bzgl. Datenschutz und IT-Sicherheit, Handlungsvorschlag (sovt)
- Diskussion der erforderlichen Maßnahmen, Aktionsplan beschließen (Gf)

3. ggf. Mitwirkung beim Aufbau des betrieblichen Datenschutzes, z.B.

- Entwurf und Diskussion von Datenschutzrichtlinien
- Schulung der Mitarbeiter, Datenschutz-Handbuch, Verfahrensverzeichnisse, ...



II. Laufende Tätigkeit als DSB

1. Hinwirkung auf die Umsetzung des Datenschutzes

- Beratung der Geschäftsführung zu Datenschutzfragen
- Unterweisung der Beschäftigten zum Datenschutz
- Ansprechpartner für Alle zum Datenschutz
- Jahresbericht an GF: Status quo und Verbesserungsvorschläge

2. Regelmäßige Kontrollen

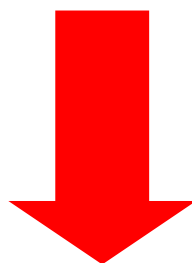
- Gespräche mit den Beschäftigten in den verschiedenen Bereichen (Begehungen)
- Prüfung der Einhaltung der Datenschutzmaßnahmen (Stichprobenkontrollen bzgl. Benutzer- und Administrationsaktivitäten)

3. Mitwirkung bei der Einführung neuer IT-Verfahren

- Prüfung der Zulässigkeit der Verarbeitung personenbezogener Daten
- Beratung bzgl. den erforderlichen technischen und organisatorischen Maßnahmen
- Verzeichnisse, Vorabkontrolle, Vertrag zur Datenverarbeitung im Auftrag



- Datenschutz: Vielfältige, zeitintensive und anspruchsvolle Tätigkeit
- Der Datenschutzbeauftragte allein ist oft überfordert (zumindest zeitlich)



Angebot:

**Unterstützung durch externes
Datenschutz-Know-how**

- **Tätigkeit als externer Datenschutzbeauftragter**
- **Beratung zur Umsetzung von Datenschutz und IT-Sicherheit, z.B.**
 - Beratung bei Einführung eines speziellen IT-Systems
 - Erstellung eines betrieblichen Datenschutz-/Berechtigungskonzepts
 - Durchführung von Vorabkontrollen
- **Durchführung von Datenschutz-Audits**
 - Überprüfung des Datenschutzkonzepts, ggf. nur in Teilen für best. IT-Systeme
- **Aufbau bzw. Optimierung des betrieblichen Datenschutzmanagements**
 - Aufgaben und Zuständigkeiten für den betrieblichen Datenschutz entwickeln
 - Umsetzung in Form einer Dienst-/Organisationsanweisungen, Datenschutzhandbuch
- **Coaching des betrieblichen Datenschutzbeauftragten**
- **Seminare zu Datenschutz und IT-Sicherheit**
 - Passgenaue Inhouse-Seminare (in Absprache mit dem Kunden)

Der betriebliche Datenschutzbeauftragte allein kann den Datenschutz nicht umsetzen !!!

Datenschutz als Gewährleistung der Persönlichkeitsrechte des Einzelnen kann nur wirksam funktionieren, wenn er

- integraler Bestandteil der Organisation des Unternehmens ist,
- zur Aufgabe jeden Vorgesetzten wird (Führungsaufgabe),
- auf viele Schultern verteilt wird (Dezentralisierung),
- im Bewusstsein jedes Mitarbeiters verankert ist
(zur täglichen Routine wird).

Datenschutz ist auch Organisationsentwicklung !

- Pflichten und Verantwortlichkeiten zum Datenschutz in Form von **Dienstanweisungen bzw. internen Richtlinien** beschreiben, z.B.
 - Verfahrensrichtlinie für Vergabe / Änderung von Zugriffsberechtigungen
 - Freigabeverfahren für neue und geänderte IT-Verfahren
 - Richtlinien zum Umgang mit PCs, Internet-Diensten, Datenträgern etc.und den zuständigen Mitarbeitern (Stellen) zuweisen
 - für IT-Benutzer, IT-Abteilung, Personalabteilung, Vorgesetzte, ...
- **Datenschutz als Führungsaufgabe** ausgestalten
 - Datenschutzrichtlinie für Führungskräfte
- **Schulungen, Seminare, Gespräche, Unterweisungen** zum Datenschutz
 - die wichtigste Datenschutzmaßnahme !! (→ „Awareness“)

Technische und organisatorische Maßnahmen (§ 9 BDSG)

- Verantwortliche Stelle muss die *erforderlichen* Maßnahmen zur Umsetzung des BDSG treffen
- je nach Art der zu schützenden personenbezogenen Daten
- Aufwand muss in angemessenem Verhältnis zum angestrebten Schutzzweck stehen
- **Anforderungen für automatisierte Verarbeitung und Nutzung** (Anlage zu § 9):
 - Zentral: datenschutzkonforme Gestaltung der innerbetrieblichen Organisation

- | | |
|-----------------------|---------------------------|
| ■ Zutrittskontrolle | ■ Eingabekontrolle |
| ■ Zugangskontrolle | ■ Auftragskontrolle |
| ■ Zugriffskontrolle | ■ Verfügbarkeitskontrolle |
| ■ Weitergabekontrolle | ■ Trennungsgebot |

- Rechtlich und technisch kompetente Beratung zum betrieblichen Datenschutz durch langjährige Erfahrung
- Schnelle Reaktionszeit und kurzfristig durchführbare Gespräche vor Ort bei aktuell auftretenden Problemen
- Sicherheit bzgl. der Einhaltung gesetzlicher Vorgaben zum Datenschutz
- Erforderliches Know-how muss nicht mühsam und teuer aufgebaut werden (Einsparung von Qualifizierungs- und Einarbeitungskosten)
- Kundenindividuell anpassbar: Kontinuierliche Beratung, punktuelle Einsätze oder Aufbau der internen Ressourcen

- Langjährige Tätigkeit als externer Datenschutzbeauftragter und Datenschutzberater (in Unternehmen und Krankenhäusern)
- Erstellung betrieblicher Datenschutz- und Berechtigungskonzepte (z.B. KMU, Krankenhäuser, Non-Profit-Organisationen)
- Aufbau der Datenschutzorganisation im Unternehmen
- Coaching interner Datenschutzbeauftragter
- Erarbeitung von Datenschutz-Leitfäden für betriebliche Standardsoftware (KIS und elektronische Patientenakte, im Auftrag von Siemens Medical Solutions)
- Langjährige Beratungs-, Gutachter- und Prüftätigkeit zur datenschutzkonformen Personaldatenverarbeitung
- Langjährige Sachverständigentätigkeit zum Beschäftigtendatenschutz (Betriebsvereinbarungen zu SAP HR/HCM, Internet & E-Mail, Data Warehouse Systeme u.v.m.)
- Langjährige Weiterbildungstätigkeit: Planung und Durchführung von Seminaren für betriebliche Datenschutzbeauftragte)
- Referententätigkeit für Siemens Medical Solutions, Integrata AG und den BvD

Vielen Dank !

ENDE