

Gefördert durch das



Bundesministerium  
für Wirtschaft  
und Technologie



Netzwerk Elektronischer Geschäftsverkehr

Leipzig, 25. November 2008

# Datenschutz in Kleinunternehmen

Dipl.-Ing. (FH) Jörg Jarick  
INTRAKONZEPT – Beratung für Managementsysteme

[www.mdc-ecomm.de](http://www.mdc-ecomm.de)



Mitteldeutsches Kompetenzzentrum für  
den elektronischen Geschäftsverkehr

**INTRa**  
KONZEPT  
Beratung für Managementsysteme

# Datenschutz in Kleinunternehmen

## Die Themen:

- Rechtliche Aspekte des Datenschutzes
- Organisatorische Aspekte des Datenschutzes
- Datenschutz und IT-Sicherheit
- Umsetzung im Kleinunternehmen

# Datenschutz in Kleinunternehmen – Das Eisbergphänomen



§ BDSG



20%

Weitere Gesetze

Prozesse

Verträge

IT-Betrieb

IT-Sicherheit

Archivierung

...

80%

# Datenschutz in Kleinunternehmen

## Was ist Datenschutz?

Datenschutz ist ein Grundrecht

### **Art. 2 Abs. 1 GG**

Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

### **Art. 33 der Sächsischen Verfassung**

Jeder Mensch hat das Recht, über die Erhebung, Verwendung und Weitergabe seiner personenbezogenen Daten selbst zu bestimmen. Sie dürfen ohne freiwillige und ausdrückliche Zustimmung der berechtigten Person nicht erhoben, gespeichert, verwendet oder weitergegeben werden. In dieses Recht darf nur durch Gesetz oder auf Grund eines Gesetzes eingegriffen werden.

## Datenschutz in Kleinunternehmen

### **Gesetze mit Bezug zum Datenschutz**

- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetz(e)
- Meldegesetz(e)
- Passgesetz (PaßG)
- Sozialgesetzbuch (SGB I bis X)
- ...

# Datenschutz in Kleinunternehmen

## Sinn und Zweck des Datenschutzes

### § 1 BDSG

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

- Geschützt wird der Einzelne, also die Person an sich.
- Der Schutz der Daten ist „lediglich“ Mittel zum Zweck.
- Betroffen sind nur Daten, die einer bestimmten oder bestimmbaren natürlichen Person gehören.
- Datensicherheit und/oder IT-Sicherheit dienen dem Datenschutz

# Aufbau des BDSG

## I. Abschnitt: Allgemeine Bestimmungen (§§ 1-11)

### II. Abschnitt (§§ 12-26): Öffentliche Stellen

- Rechtsgrundlagen der DV
- Rechte des Betroffenen
- Bundesbeauftragter für den Datenschutz

### III. Abschnitt (§§ 27-38a): Nicht-öffentliche Stellen

- Rechtsgrundlagen der DV
- Rechte des Betroffenen
- Aufsichtsbehörde

## IV. Abschnitt: Sondervorschriften (§§ 39-42)

## V. Abschnitt: Schlussvorschriften (§§ 43, 44)

## VI. Abschnitt: Übergangsvorschriften (§§ 45, 46)

# Aufbau des BDSG



# Grundsatz: Verbot mit Erlaubnisvorbehalt

## Zulässigkeit

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist nur zulässig, soweit

1. das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder
2. der Betroffene eingewilligt hat.

# Datenschutz in Kleinunternehmen

## Auch in Kleinunternehmen sind zu beachten (I)

- Rechtsgrundlage oder Einwilligung
- Beachtung der Zweckbindung
- Besondere personenbezogene Daten (§3 Abs. 9 BDSG)
- Beachtung von Datenvermeidung und Datensparsamkeit
- Beachtung der Rechte der Betroffenen:  
Information, Auskunft, Berichtigung, Sperrung, Löschung etc.  
...

# Datenschutz in Kleinunternehmen

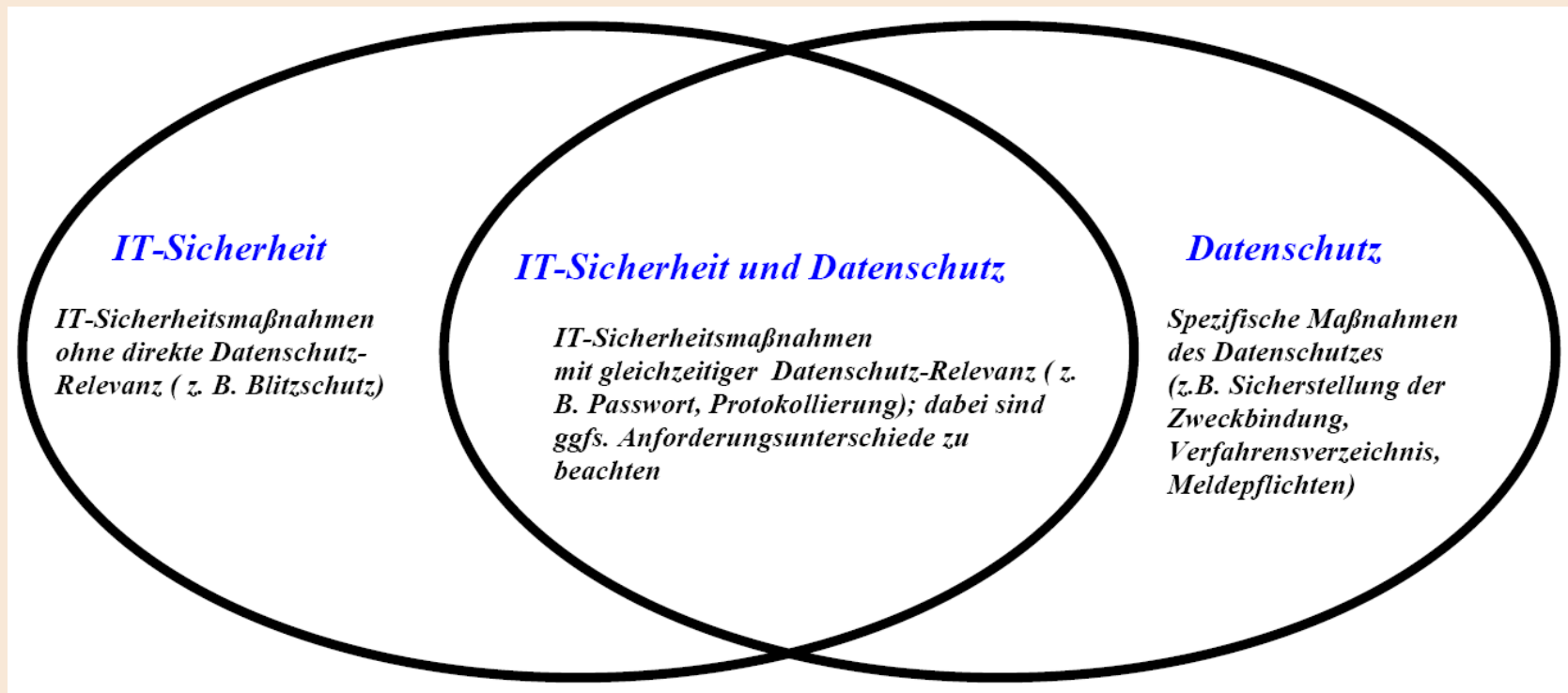
## Auch in Kleinunternehmen sind zu beachten (II)

- Auftragsdatenverarbeitung
- Übermittlung von Daten an öffentliche Stellen
- Übermittlung von Daten an nichtöffentliche Stellen
- Übermittlung von Daten an Drittstaaten

...

# Datenschutz in Kleinunternehmen

## Datenschutz und IT-Sicherheit



Quelle: BSI-IT-Grundschutzkataloge Baustein 1.5

# Datenschutz in Kleinunternehmen

## Risikobereiche bei der Verarbeitung von Daten

- Vertraulichkeit:** *Die Gefahr, dass Unberechtigte die Daten zur Kenntnis nehmen.*
- Integrität:** *Die Gefahr, dass die Daten verfälscht werden.*
- Authentizität:** *Die Gefahr, dass die Daten nicht vom angegebenen Urheber oder Absender stammen.*
- Verbindlichkeit:** *Die Gefahr, dass der Versand oder der Empfang der Daten bestritten wird.*
- Verfügbarkeit:** *Die Gefahr, dass auf die Daten nicht (mehr), nicht vollständig oder nicht rechtzeitig zugegriffen werden kann.*
- Annex:** *Die Gefahr, für indirekte Angriffe genutzt zu werden (sog. hopping station).*

# Datenschutz in Kleinunternehmen

## IT-Sicherheit – technische und organisatorische Maßnahmen

- Vorgaben in der Anlage zum §9 BDSG
- Hilfsmittel Grundschutzkataloge des BSI ([www.bsi.de](http://www.bsi.de))
- Grundsätzliche Empfehlungen zur IT-Sicherheit (Firewall, Virenschutz) dienen immer auch dem Datenschutz

...

# Datenschutz in Kleinunternehmen

## Datenschutz- und Informationssicherheitsmanagementprozess

### Verbesserung

- Aufrechterhaltung der ITK-Sicherheit
- Vorbeuge- und Korrekturmaßnahmen

### Planung

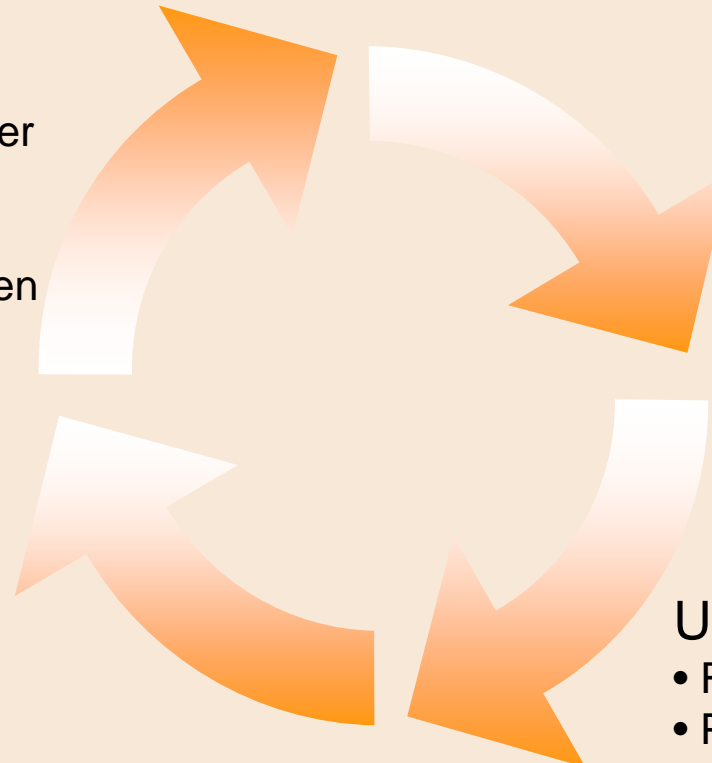
- ITK-Sicherheitsleitlinie
- ITK-Sicherheitskonzepte
- Strukturanalyse
- Schutzbedarfsfeststellung

### Kontrolle

- Soll-/Ist-Vergleich
- Audits

### Umsetzung

- Realisierung der Maßnahmen
- Priorisierung, Verantwortlichkeiten
- Schulung und Sensibilisierung



# Datenschutz in Kleinunternehmen

## Datenschutz – Wie umsetzen?

- Datenschutzverantwortlichen (-beauftragten) bestimmen (bestellen),
- Internes Verzeichnis erstellen,
- Maßnahmen der IT-Sicherheit umsetzen,
- Organisatorische Regelungen zur Sicherung der Betroffenenrechte,
- Schulung der Mitarbeiter,
- Vertragskontrolle bei Dienstleistern,
- Audits bei Dienstleistern,
- ...

# Datenschutz in Kleinunternehmen

Das Jedermann-Verfahrensverzeichnis muss enthalten:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten

# Datenschutz in Kleinunternehmen

## Datenschutz – Häufige Lücken.

- Internetauftritt oder Online-Shop,
- Jedermann-Verfahrensverzeichnis,
- Vertragsregelungen bei Auftragsdatenverarbeitung,
- Einbeziehung des Datenschutzbeauftragten in IT-Projekte,
- Schulung der Mitarbeiter,
- Ausbildung und Arbeitszeit des Datenschutzbeauftragten,
- Löschung von Daten oft nicht möglich,
- Keine Regelungen für Auskunftsanfragen von Dritten,
- ...

# Datenschutz in Kleinunternehmen

## Links für weitere Informationen:

[www.bfdi.bund.de](http://www.bfdi.bund.de)

<http://www.bsi.de/gshb/baustein-datenschutz/index.htm>

[www.datenschutz.de](http://www.datenschutz.de)

[www.bvdnet.de](http://www.bvdnet.de)

[www.gdd.de](http://www.gdd.de)

[www.dvd.de](http://www.dvd.de)

# Datenschutz in Kleinunternehmen

**Vielen Dank für Ihre Aufmerksamkeit.**



IT-Sicherheitsmanagement • Datenschutz • IT-Strategie

**Dipl.-Ing. (FH) Jörg Jarick**  
TISP • ISO/IEC 27001 ISMS Auditor  
Datenschutzauditor (TÜV)

INTRAKONZEPT - Beratung für Managementsysteme • Scherlstraße 7, 04103 Leipzig  
Telefon: +49 (0) 341 98973810 • Telefax: +49 (0) 341 98973819 • Mobiltelefon: +49 (0) 1522 1964204  
E-Mail: [joerg.jarick@intrakonzert.net](mailto:joerg.jarick@intrakonzert.net) • Internet: <http://www.intrakonzert.de>