

Werkstattbericht - SAGA GWG

**Datenschutzprüfung
nach
§ 38 BDSG**

Vortragsgliederung:

Datenschutz im Unternehmen

Datenschutzprüfung durch die Aufsichtsbehörde nach § 38 BDSG

- Ankündigung
- Vorbereitung
- Prüfung
- Bericht
- Schlussfolgerungen

Datenschutzkonzept

Datenschutz – Grundsätze

- **Verbot mit Erlaubnisvorbehalt** (§ 4 Abs. 1 BDSG)
- **Datenvermeidung und Datensparsamkeit** (§ 3a BDSG)
- Direkterhebung (§ 4 Abs. 2 BDSG)
- **Zweckbindung** (§ 28 Abs. 1 S. 2 BDSG)
- Datensicherungsgebot (§ 9 BDSG)
- **Löschung** (§35 BDSG)
- **Transparenz der Datenverarbeitung / Wahrung der Rechte der Betroffenen**
 - Benachrichtigung (§ 33 BDSG)
 - Auskunft, Einsichtnahme (§ 34 BDSG)
 - **Berichtigung, Sperrung und Löschung** (§ 35 BDSG)
 - Schadensersatz (§ 7 BDSG)
 - Auskunft aus dem Verzeichnisse (§ 4e BDSG)

Datenschutz – Grundsätze

Personenbezogene Daten: „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person“

Name, Alter, Familienstand, Geburtsdatum
Anschrift, Telefonnummer, E-Mail Adresse
Konto-, Kreditkartennummer
Kraftfahrzeugnummer, Kfz-Kennzeichen
Personalausweisnummer,
Sozialversicherungsnummer
Vorstrafen
genetische Daten und Krankendaten
Werturteile wie zum Beispiel Zeugnisse

Besonders sensible
Daten :

Ethnische Herkunft
Religion
Gesundheit
Politische Meinung

Auch Fotos, Videoaufnahmen, Röntgenbilder oder Tonbandaufnahmen können personenbezogene Daten enthalten.

Besondere Beachtung bei folgenden Prozessen:

- ✓ **Anbahnung von Mietverhältnissen**, u.a. automatisierte Verfahren im Vertriebspool, Mietinteressentenbogen, Schufa-Auskünfte.
- ✓ **Bewirtschaftung von Mietverhältnissen**, u.a. Daten im ERP-, Vertriebs-, Inst.-, Mahn-System, etc. Weitergabe von Kundendaten
- ✓ **Kündigung von Mietverhältnissen**, u.a. Abstimmung der Weitergabe von Kontaktdaten, Verfahren Wiedervermietbarmachung, etc
- ✓ **Verkauf von Immobilienobjekten** an externe Kaufinteressenten und Mieter, u.a. automatisierte Verfahren zur Interessentenverwaltung, etc.
- ✓ **Verwaltung von Wohnungseigentumsgemeinschaften**, automatisierte Verfahren im ERP-System, etc.
- ✓ **Forderungsverfolgung** laufender und beendeter Mietverhältnisse, u.a. die automatisierten Verfahren in ERP- und Mahnsystemen sowie die Datenweitergabe an Dritte, (Behörden, Inkassounternehmen etc.)
- ✓ **Verwaltung von Mitarbeiterdaten** im Personalbereich, u.a. automatisierte Verfahren der Personalabrechnung, Zeugniserstellung, Bewerberdaten

Datenschutz – warum ?

Gründe für Datenschutz

- Reputation / Image
- Schutz vor Verlust
- Gesetze
- Compliance
- Ethik
- Kundenwunsch
- Aufsichtsbehörde

§ 38 BDSG - Aufsichtsbehörde

- Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln
...
- Die der Kontrolle unterliegenden Stellen ... haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. ...
- Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, ..., ... Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. ...

Prüfung nach § 38 BDSG in 2014 bei SAGA GWG

Anlassbezogen:

- SEPA - Anschreiben an ehemalige Mieter
- Vertrieb Neubauprojekt Suttnerpark
- neue Broschüre des HH-DSB zur Erhebung von Mieterdaten in Vermietungsprozess

Prüfungsschwerpunkte :

- Klärung Einzelfall SEPA - Anschreiben
- Betrieblicher DSB
- Technisch-organisatorische Maßnahmen (TOMSs)
- Verzeichnisverfahren
- Auftragsdatenverarbeitung (ADV)
- Sensibilisierung der Mitarbeiter (Verpflichtungserklärungen)

Ablauf der Datenschutzprüfung nach §38 BDSG

Ankündigung

- Prüfungsanmeldung mit Einzelthemen und Termin
- Anforderung von Unterlagen
- Fragebogen

Vorbereitung

- Unterlagen zusammenstellen
- Beschaffung einzelner Unterlagen
- Fragebogen ausfüllen
- Klärung weiterer Einzelfragen

Prüfungstermin

- Vorbereitung
- Teilnehmer

Nachfolgende Zulieferungen

Abschlussbericht / Protokoll

- Feststellungen
- Prüfhinweise
- Umsetzungshinweise

Rechnung

- Gebührenpflicht, wenn Anlass der Prüfung im Verantwortungsbereich der geprüften Gesellschaft liegt

Betrieblicher Datenschutzbeauftragter

- formell wirksame Bestellung
- Zuverlässigkeit
- Unabhängigkeit
- Fachkunde
- erweiterter Kündigungsschutz
- Verschwiegenheit
- notwendige zeitliche Kapazitäten
- Interessenkonflikte
- Regelmäßiger Tätigkeitsbericht

Technische und organisatorische Maßnahmen nach § 9 BDSG

Sicherung der Datenbestände und des Datenverarbeitungsbetriebs gegen Preisgabe, Verfälschung und Verlust

8 Gebote :

- ❖ Zutrittskontrolle / räumlich
- ❖ Zugangskontrolle / in die Datenverarbeitungssysteme
- ❖ Zugriffskontrolle / Berechtigungskonzept
- ❖ Weitergabekontrolle / Verschlüsselung , Transportsicherung
- ❖ Eingabekontrolle / Veränderung von Daten
- ❖ Auftragskontrolle /Auftragsdatenverarbeitung
- ❖ Verfügbarkeitskontrolle / Schutz vor Zerstörung und Verlust
- ❖ Trennungskontrolle / getrennte Datenbanken

E-Mail , privat oder nur dienstlich ? (TKG / TMG gilt)

Datenschutzprüfung – Schwerpunktthemen

- **Verfahrensverzeichnis (§ 4 e S. 1 BDSG)**
- **Auftragsdatenverarbeitung (§ 11 BDSG)**
- **Verpflichtung und Schulung der Mitarbeiter**
- **Umgang mit Beschäftigtendaten (§ 32 BDSG)**
- **Vorabkontrollen bei Verfahrenseinführung**
- **Datenhaltung / Löschkonzepte**
- **Videoüberwachung**
- **Allgemeine organisatorische Präventionsmaßnahmen (clean desk)**

Ergebnis der Prüfung bei SAGA GWG

- Datenschutz bei SAGA GWG grundsätzlich im Vergleich gut aufgestellt
- SEPA-Sachverhalt konnte erläutert werden
- Überarbeitung Verfahrensverzeichnis
- Optimierungsnotwendigkeit im Bereich der TOMs und der Prüfung der ADV-Verhältnisse auf Einhaltung der DS-Regeln
- Erarbeitung von Sensibilisierungs- bzw. Schulungskonzepten

Datenschutz bei SAGA GWG – wie ?

Sensibilisierung

Schlussfolgerungen

- Datenschutz im Unternehmen leben
- gesetzeskonform
- mit Augenmaß
- auf Basis eigener Einwertungen
- Überarbeitung der Datenschutzrichtlinie
- Einbindung in ein Datenschutzkonzept

Ziel: Integration des Themas Datenschutz in die Unternehmensprozesse

Datenschutzkonzept

- Statusbestimmung / Ist - Erhebung
- Konzepterstellung
 - Grundlagen
 - Betrieblicher DSB
 - Verfahrensverzeichnisse
 - ADV
 - TOMs
 - Verantwortung jedes Prozessteilnehmers / -verantwortlichen
 - Sensibilisierungs- und Schulungskonzepte
- Umsetzung
- Schulung / Sensibilisierung
- Gelebter Datenschutz

Vielen Dank für Ihre Aufmerksamkeit!

