.

Wie den Datenschutz in der Mitarbeitervertretung und bei Klienten einhalten?

Vortrag auf der Datenschutz-Veranstaltung der agmav Westfalen-Lippe am 13.11.2019, in der BAUA, Dortmund

Jürgen Fickert, Berater zu IT-Systemen und Datenschutz

Langjähriger Mitarbeiter der TBS NRW e.V.

Der Datenschutz-Standard

Der Standard zum Datenschutz ist die

europäische Datenschutz-Grundverordnung DS GVO

Das Datenschutzgesetz der evangelischen Kirche -

das DSG EKD - ist im Vergleich zur DS GVO in wichtigen Punkten ungenauer und schlechter.

Einige Beispiele.

Rechtliche Grundlage der Datenverarbeitung

DS GVO	DSG EKD
Artikel 6 **Rechtmäßigkeit der Verarbeitung** (1) Die Verarbeitung ist nur rechtmäßig, ... die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen ... erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, ...	**§ 6 Rechtmäßigkeit der Verarbeitung** Die Verarbeitung ist nur rechtmäßig, ... 4. die Verarbeitung ist für die Wahrnehmung einer sonstigen Aufgabe erforderlich, die im kirchlichen Interesse liegt,

Bußgelder

DS GVO	DSG EKD
Artikel 83 ...Verhängung von Geldbußen Bei Verstößen ... werden ... Geldbußen von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, ...	§ 45 Geldbußen (1) Verstößt eine verantwortliche Stelle vorsätzlich oder fahrlässig gegen Bestimmungen dieses Kirchengesetzes, so können die Aufsichtsbehörden Geldbußen verhängen ... Gegen verantwortliche Stellen sind Geldbußen nur zu verhängen, soweit sie als Unternehmen ... am Wettbewerb teilnehmen. ... (5) Bei Verstößen werden im Einklang mit Absatz 3 Geldbußen von bis zu 500.000 Euro verhängt.

Verarbeitung **besonderer Kategorien personen-bezogener Daten (**Gesundheit, Religion, ...)

DS GVO /	§ 13 DSG EKD Verarbeitung besonderer
Im Kern:	(2) Abweichend dürfen ...sie verarbeitet werden, wenn
Nur bei persönlicher Einwilligung, wie beim Arzt	1. die betroffene Person in die Verarbeitung der genannten personenbezogenen Daten ... ausdrücklich eingewilligt hat; 2. die Verarbeitung erforderlich ist, damit die verantwortliche Stelle oder die betroffene Person die ihr aus dem Arbeits- und Dienstrecht sowie ... und ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach kirchlichem oder staatlichem Recht oder nach einer Dienstvereinbarung nach den kirchlichen ... (MVG) die geeignete Garantien für die Rechte und die Interessen der betroffenen Person vorsehen, rechtmäßig ist; 8. die Verarbeitung für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, ... oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage kirchlichen oder staatlichen Rechts oder ...

Wer ist verantwortlich, den Datenschutz einzuhalten?

Die evangelische Kirche, d.h. die jeweilige Dienststellenleitung, ist dafür verantwortlich, dass die Bestimmungen des DSG EKD eingehalten und umgesetzt werden.

- Sie prüft die rechtlichen Grundlagen
- Sie hat die Rechenschafts- und Dokumentationspflichten.
- Sie verabschiedet konkrete Datenschutzmassnahmen, z.B. Umgang mit Handy, Patientendaten, Verschlüsselung, Datensicherung oder Löschungen.
- Sie muss datenschutzkonforme IT-Geräte und Software einsetzen.
- Die Beschäftigten müssen über die Maßnahmen geschult werden und sie ggf. in der Praxis anwenden.
- Bei Unklarheiten die Dienstleitung oder die örtlichen Beauftragten für den Datenschutz fragen - am besten schriftlich.

Kapitel 4 DSG EKD Pflichten der verantwortlichen Stelle ...

§ 26 Datengeheimnis

§ 27 Technische und organisatorische Maßnahmen, IT-Sicherheit

§ 28 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen ...

§ 30 Verarbeitung von personenbezogenen Daten im Auftrag

§ 31 Verzeichnis von Verarbeitungstätigkeiten - mit konkreten Löschfristen!

§ 32 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

§ 33 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

§ 34 Datenschutz-Folgenabschätzung

§ 35 Audit und Zertifizierung

Diese Unterlagen enthalten wertvolle Informationen für die MAVen bei der Verarbeitung von Beschäftigtendaten

Dienstliche Daten auf privaten IT-Geräten

Dienstliche Daten, insbesondere sensible Daten zu Gesundheit, Religion, ... haben auf privaten IT-Systemen nichts zu suchen.

Risiko der Haftung, Bußgelder !!

Verantwortlich ist die Diakonie, da „ihre“ Daten.

Ordnet die Dienststelle - schriftlich! - die Verarbeitung dienstlicher Daten auf privater IT an, so ist sie für die Einhaltung des Datenschutzes verantwortlich! Mitarbeiter muss zustimmen und angeordnete Maßnahmen umsetzen, z.B. Verschlüsselung.

Smartphone darf z.B. in diesem Fall nicht an Familienangehörige gegeben werden.

Weitere Fragen

- Whats App – dienstliche Nutzung eines messenger Dienstes müßte die Diakonie erlauben/ anordnen. Alternativen sind Threema, Signal, … .
- Welche Daten müssen/ dürfen/ dürfen nicht gesammelt werden? Für das Dienstgeschäft, z.B. zu "Standard-Software" muss dies die EKD festlegen, konkret. Erhält Mitarbeiter*in z.B. in der ambulanten Pflege konkrete, aktuelle Informationen z.B. über familiäre Situation, so darf sie diese Angaben nur an Personal weitergeben, die diese Informationen zwingend benötigen, z.B. per Telefonat, Dienst-E-Mail (!). Löschfristen der Mails muss Diakonie festlegen.
- Keine allgemeinen Informationstafeln/ Boards, mit offenem Zugang

Rechtsrahmen der MAV zum Datenschutz

Verantwortlich im Sinne DSG EKD für den Datenschutz im MAV-Büro ist die Dienststellenleitung, da sie an erster Stelle

- personenzogene Daten erhebt und verarbeitet
- die Rechtsgrundlagen und die Zwecke der Datenverarbeitung festlegt,
- Verarbeitungsverzeichnisse, Datenschutzkonzepte usw. verabschiedet (vgl. Anforderungen nach Kap. 4 DSG).
- Daten an die MAV weitergibt.

Erst an zweiter Stelle erhält die MAV im Rahmen ihrer Aufgaben nach MVG EKD diese Daten und muss ggf. ergänzende DS-Maßnahmen ergreifen.

Beispielhafte Datenschutz-Checkliste für die MAV

- Zugang zum MAV-Büro
- Schlüsselvergabe zum MAV-Büro; Reinigungsdienst
- Verschließbare Schränke
- Nachvollziehbare Systematik der Ordner, Transparenz ; Trennung sensibler Daten
- Sichere Hauspost, verschlossene Umschläge
- Datenschutz-Tonne und Shredder vorhanden
- Standort Drucker und Kopierer – nur für MAV?
- MAV-PC mit Zugang zum Unternehmens-Netz
- Verschlüsselte Speicherung der Daten auf Servern
- Gesicherter, vertrauenswürdiger Speicherbereich auf Unternehmens-Server
- Erforderliche Softwareausstattung wie MS-Office, Internetzugang, Mail, …
- Betriebliche Handys, SmartPhone / Dienst- und MAV-Kommunikation trennen?
- Private Geräte wie SmartPhone, Notebook nutzen? - so Datenschutz einhalten
- Gesicherte Datenübertragung im Unternehmen
- Eigene Datensicherung,…
- Kommunikation und Datenübermittlung im Betrieb
- Austausch mit Dienststelle, Personalwesen per aus Post, die Mail?
- Umgang mit E-Mail, systematisch ablegen, ausdrucken, löschen
- Verfahren, Einladungen und Protokolle zu versenden, Hauspost, Mail, ...

Handlungshilfe für MAVen

- Handlungshilfe „Datenschutz im Personalrat“, vom
- LDI NRW Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
- von 2012, im Internet abrufbar, suche „ LDI NRW Personalrat“
- https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/7_Datenschutz_im_Personalrat/Datenschutz_im_Personalrat_2012.pdf

Seminare für die MAVen

- **Teilnahme MAV-Vertreter an EKD-Programm der EKD-Datenschutzbeauftragten klären**
- **z.B. https://datenschutz.ekd.de/veranstaltung/grundseminar-fuer-datenschutzbeauftragte-16/**
- **TBS NRW e.V. kann maßgeschneidertes Seminar anbieten, nicht nur rechtlich, auch mit Hinweisen zur Umsetzung tbs-nrw.de**