Datenschutz in Kommunen: aktuelle Probleme und Empfehlungen

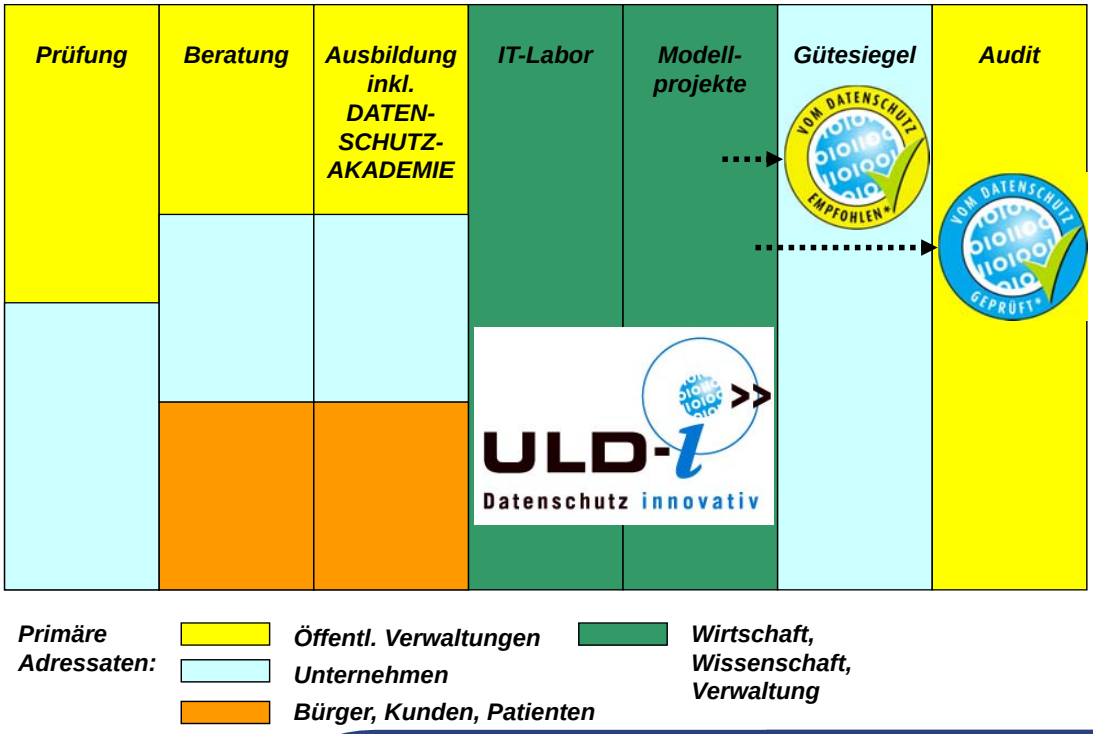
Marit Hansen
Landesbeauftragte für Datenschutz
Schleswig-Holstein

Bürgermeister-Fachkonferenz, Alt Duvenstedt,
30.09.2016

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Kurzvorstellung: Was macht das ULD?

Datenschutz und Informationsfreiheit



Überblick

- Aktuelles Recht
- Änderungen durch die EU-Datenschutzreform
- Risiken durch Einbindung externer Angebote
- Einbindung von Bürgerinnen und Bürgern
- Angebot: Datenschutz-Audit

ULD www.datenschutzzentrum.de

Überblick

- Aktuelles Recht
- Änderungen durch die EU-Datenschutzreform
- Risiken durch Einbindung externer Angebote
- Einbindung von Bürgerinnen und Bürgern
- Angebot: Datenschutz-Audit

Begriffe

- Eine datenverarbeitende Stelle

§ 2 Abs. 3 LDSG
(3) Datenverarbeitende Stelle ist jede öffentliche Stelle im Sinne von § 3 Abs. 1, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.

- verarbeitet

§ 3 Abs. 1 LDSG
(1) Dieses Gesetz gilt für öffentliche Stellen. Öffentliche Stellen im Sinne dieses Gesetzes sind Behörden und sonstige öffentliche Stellen der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung.

- personenbezogene Daten.

ULD www.datenschutzzentrum.de

Begriffe

- Eine datenverarbeitende Stelle
- verarbeitet

§ 2 Abs. 2 LDSG
(2) Datenverarbeitung ist die Verwendung personenbezogener Daten. [...]

[...]
Erheben [...],
Speichern [...],
Übermitteln [...],
Sperren [...],
Löschen [...]

- personenbezogene Daten.

Begriffe

- Eine datenverarbeitende Stelle
- verarbeitet
- personenbezogene Daten.

§ 2 Abs. 1 LDSG
(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffene oder Betroffener).

ULD www.datenschutzzentrum.de

Die 7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

Für jede Datenverarbeitung ist eine rechtliche Grundlage nötig, z.B. Gesetz, Vertrag, Einwilligung.

Die 7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

Einwilligung bedeutet:
Der Betroffene wurde ausreichend informiert und hat freiwillig eingewilligt.

§ 12 LDSG
Form der Einwilligung

ULD www.datenschutzzentrum.de

Die 7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

Personenbezogene Daten dürfen nur für den angegebenen Zweck verarbeitet werden.

§ 13 LDSG
Erhebung, Zweckbindung

Die 7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

Es dürfen nur die personenbezogenen Daten verwendet werden, die für den jeweiligen Zweck erforderlich sind.

Die Daten müssen gelöscht werden, sobald sie nicht mehr benötigt werden.

- § 11 LDSG
  Zulässigkeit der Datenverarbeitung
- § 28 LDSG
  Berichtigung, Löschung, Sperrung
- § 4 LDSG
  Datenvermeidung und Datensparsamkeit [...]

ULD www.datenschutzzentrum.de

Die 7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit u
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

Erhebung und Verarbeitung personenbezogener Daten müssen gegenüber Betroffenen transparent sein.

Betroffene haben Rechte auf Auskunft und Berichtigung sowie (eingeschränkt) auf Sperrung und Löschung.

- § 26 LDSG: Aufklärung, Benachrichtigung
- § 27 LDSG: Auskunft an Betroffene
- § 28 LDSG: Berichtigung, Löschung, Sperrung
- § 29 LDSG: Einwand gegen die Verarbeitung
- § 27a LDSG: Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Die 7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

- § 5 LDSG
  Allgemeine Maßnahmen zur Datensicherheit
- § 6 LDSG
  Besondere Maßnahmen zur Datensicherheit
  bei Einsatz automatisierter Verfahren
- Datenschutzverordnung (DSVO)

Unberechtigte Zugriffe auf die Daten müssen durch technische und organisatorische Maßnahmen ausgeschlossen werden.

ULD www.datenschutzzentrum.de

Die 7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

- Kontrollpflichten, z.B. bei Auftragsdatenverarbeitung (§ 17 LDSG)
- § 39 LDSG
  Aufgaben des ULD

Die Datenverarbeitung muss einer internen und externen Kontrolle unterliegen.

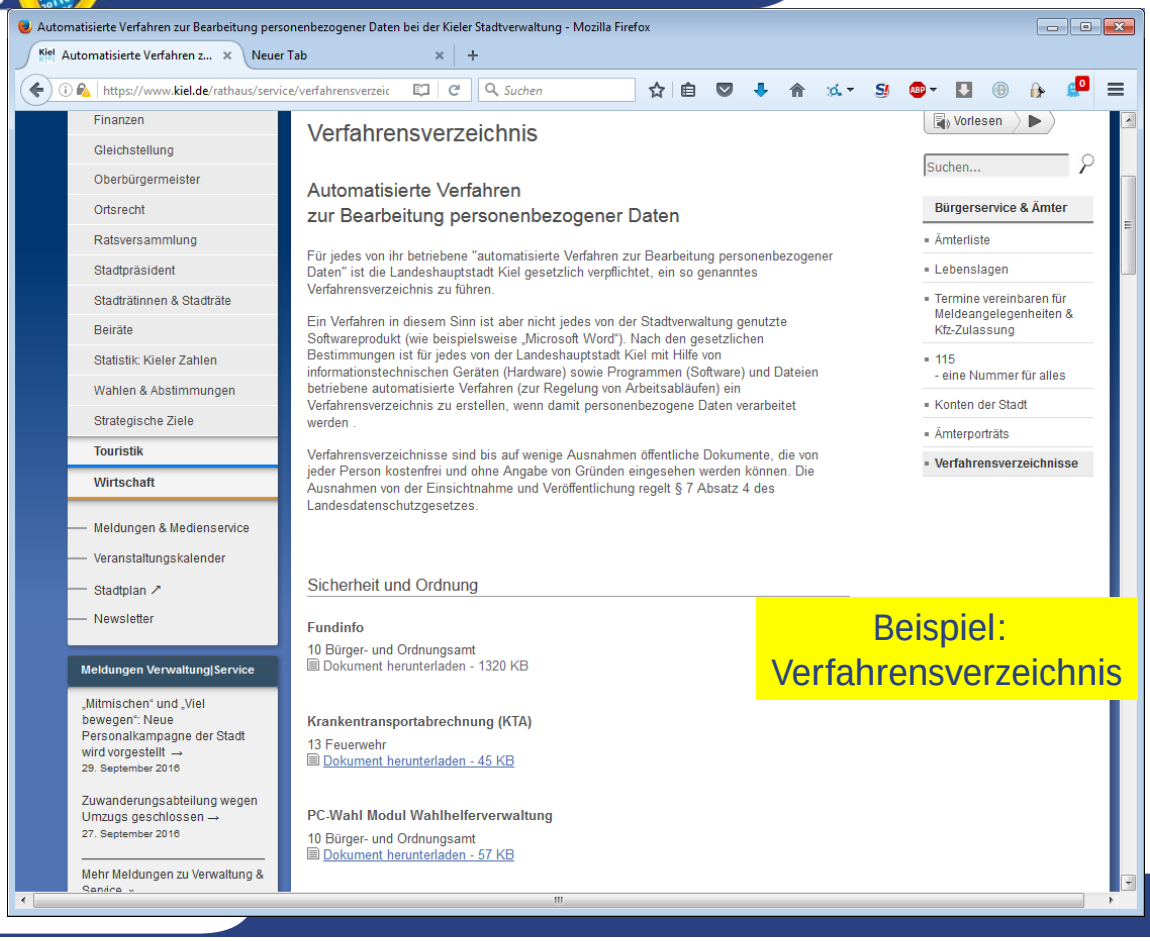
Datenschutzregelungen im kommunalen Bereich

- Viele spezialgesetzliche Regelungen mit einzelnen Paragraphen zur Datenverarbeitung

- Subsidiär:
  - Landesdatenschutzgesetz (LDSG) Schleswig-Holstein
  - Datenschutzverordnung (DSVO) (nur in Schleswig-Holstein)

- Hilfreich: behördliche(r) Datenschutzbeauftragte(r)
- Aber: laut LDSG nicht verpflichtend

ULD www.datenschutzzentrum.de



Beispiel:
Verfahrensverzeichnis

Landes-
hauptstadt Kiel

Verfahrensverzeichnis

gemäß § 7 Landesdatenschutzgesetz Schleswig-Holstein (LDSG)
bestimmt zur Einsichtnahme für jede Person (§ 7 Abs. 4 LDSG)

Verfahren	Finanzbuchhaltung newsystem®kommunal- Neues Kommunales Rechnungswesen (DOPPIK)

Version: 9 / 15 gültig ab: 2009 / 2015 bis (sofern bestimmbar):

1. Daten verarbeitende Stelle:

	Landeshauptstadt Kiel, Fleethörn 9 (Rathaus), 24103 Kiel
Amt/Abteilung	*Amt für Finanzwirtschaft*
Aktenzeichen	*90*
Kontakt	*Fachanwendungsbetreuer/in (Key User):* *Datenschutzbeauftragter: Herr Amann, Tel. 901 2771, datenschutz@kiel.de*

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

Zweckbestimmung	Die Landeshauptstadt Kiel hat mit Wirkung vom 01. Januar 2009 das kamerale Haushalts- und Rechnungswesen auf die doppelte Buchführung (Doppik) gemäß den Vorgaben der Gemeindehaushaltsverordnung des Landes Schleswig-Holstein umgestellt. Als Finanzsoftware wird *newsystem®kommunal* der Firma INFOMA eingesetzt. Diese Software unterstützt derzeit mindestens die folgenden Aufgabenbereiche: Planung / Konsolidierung, Finanzbuchhaltung, Bilanzbuchhaltung mit Jahresabschluss, Stadtkasse, Vollstreckung, Kosten- und Leistungsrechnung, Anlagenbuchhaltung und die Veranlagung.
Rechtsgrundlage	Grundlage für die Einführung sind die Empfehlungen der Innenministerkonferenz, die Empfehlungen des Innovationsringes Schleswig-Holstein in der jeweils aktuellen Fassung, die gesetzlichen Regelungen des Landes Schleswig-Holstein einschließlich Verordnungen, insbesondere die Gemeindeordnung (GO) und die Gemeindehaushaltsverordnung Doppik (GemHVO-Doppik).

3. Kreis der Betroffenen:

1	Debitoren aller Art (Steuer- und Gebührenzahler/innen)
2	Kreditoren aller Art (Firmen, Lieferanten, Leistungsempfänger …)

4. Kategorien verarbeiteter Daten, Löschungs-, Aufbewahrungsfristen, Zugriffsberechtigungen

Blick ins LDSG

§ 5 Allgemeine Maßnahmen zur Datensicherheit

(1) [1]Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz im Sinne von § 3 Abs. 3 ist durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. [2]Sie müssen gewährleisten, dass

1. Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (Verfügbarkeit),
2. Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (Integrität),
3. nur befugt auf Verfahren und Daten zugegriffen werden kann (Vertraulichkeit),
4. die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann (Transparenz),
5. personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (Nicht-Verkettbarkeit) und
6. Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte nach den § 26 bis 30 wirksam ermöglichen (Intervenierbarkeit).

Gewährleistungsziele

- Vertraulichkeit (z.B. Verschlüsselung, Zugriffsschutz)
- Integrität, Authentizität (Zugriffskontrolle, digitale Signatur)
- Verfügbarkeit (USV, Backup, Datenmanagement)
- Nicht-Verkettbarkeit (Datensparsamkeit, Trennung)
- Intervenierbarkeit (Löschen, Sperren, Beauskunften, Change Management, Deaktivieren/Stoppen der DV)
- Transparenz, Revisionsfähigkeit (Protokollierung, Kontrolle der SysAdmin, Dokumentation, Anwenderhandbücher, Information bei Erhebung, Benachrichtigung bei Bearbeitung)

Blick in die DSVO: Datenschutzmanagementsystem

§ 4 Dokumentation der Sicherheitsmaßnahmen

(1) [1]Die technischen und organisatorischen Maßnahmen, die gemäß der §§ 5, 6 und 8 LDSG getroffen wurden, sind zu dokumentieren. [2]Dabei kann auf die Darstellung nach § 3 Abs. 2 Bezug genommen werden.

(6) [1]Es ist zu dokumentieren, welche technischen und organisatorischen Maßnahmen getroffen wurden, um die Tätigkeiten gemäß § 6 Abs. 5, § 8 Abs. 4 und § 10 Abs. 4 LDSG zu ermöglichen und zu unterstützen (Datenschutzmanagementsystem).

Datenschutzmanagementsystem

Einrichten eines Datenschutzmanagementsystems

- Überwachung und Kontrolle der ordnungsgemäßen Anwendung der Verfahren
- Monitoring von und Reaktion auf Änderungen (von außen, von innen)
- Zulässigkeit der Datenübermittlung bei gemeinsamen Verfahren
- Aufgaben des behördlichen Datenschutzbeauftragten

Grundlage für ein Behörden-Datenschutzaudit

Überblick

- Aktuelles Recht
- Änderungen durch die EU-Datenschutzreform
- Risiken durch Einbindung externer Angebote
- Einbindung von Bürgerinnen und Bürgern
- Angebot: Datenschutz-Audit

Normen-hierarchie

Primärrecht

Vertrag über die Europäische Union

Vertrag über die Arbeitsweise der Europäischen Union

EU-Grundrechtecharta

Sekundärrecht

Richtlinie
In nationales Recht umzusetzen

Verordnung
Gilt unmittelbar

Datenschutz-Richtlinie 95/46/EG

Nationales Recht

Bundes-gesetz | Landes-gesetz

Bundes-verordnung | Landes-verordnung

BDSG

<keine VO>

LDSG

DSVO DSGSVO DSVO-Schule

ULD-Entgeltsatzung

ULD www.datenschutzzentrum.de

Normen-hierarchie

Primärrecht

Vertrag über die Europäische Union

Vertrag über die Arbeitsweise der Europäischen Union

EU-Grundrechtecharta

Sekundärrecht

Richtlinie
In nationales Recht umzusetzen

Verordnung
Gilt unmittelbar

Datenschutz-JI-Richtlinie 2016/680

Datenschutz-Grundverordnung 2016/679

Nationales Recht

Bundes-gesetz | Landes-gesetz

Bundes-verordnung | Landes-verordnung

Entwurf ABDSG

<keine VO>

LDSG

DSVO DSGSVO DSVO-Schule

ULD-Entgeltsatzung

Datenschutz in Kommunen

Datenschutz-Grundverordnung

- Nachfolger der EU-Datenschutz-Richtlinie von 1995
- Konstrukt „Verordnung“: unmittelbar anwendbar
- Anwendungsvorrang gegenüber nationalem Recht
- 70 Öffnungsklauseln (Regelungsaufträge und Regelungsoptionen) für nationalen Gesetzgeber
- Geltung ab 25.05.2018


VERORDNUNGEN

- Marktortprinzip
- One-Stop-Shop:
  einfacher für Verbraucher(innen)
- Kohärenzmechanismus:
  Einigung der Aufsichtsbehörden

DS-GVO: Ziele erreicht?

- Harmonisierung ☐
  - Abstraktheit der Regeln ↯
  - Öffnungsklauseln ↯
- Wettbewerbsangleichung ☐
  - Marktortprinzip ✓
  - Siehe oben ↯
- Modernisierung ☐
  - Im Vergleich zu 1995 ✓
  - Im Vergleich zu 2001 ↯
  - Zukunftsfähig ↯?
- Neuer Startpunkt ☑

https://www.forum-privatheit.de/

Neu in der DS-GVO

- Bezogen auf das Risiko
  für die Rechte und Freiheiten der betroffenen Person
- Schärferes Schwert der Sanktion:
  - Bis 10 Mio. € oder bis 2% des Jahresumsatzes bzw.
  - bis 20 Mio. € oder bis 4% des Jahresumsatzes
- Neue Instrumente
  - Datenschutz durch Technikgestaltung
  - Datenschutz durch datenschutzfreundliche Voreinstellungen
  - Datenschutz-Folgenabschätzung
  - Meldung von Datenschutzvorfällen
  - Genehmigte Verhaltensregeln
  - Zertifizierung

Art. 37 DS-GVO – Benennung eines bDSB

Artikel 37 Benennung eines Datenschutzbeauftragten

(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird,

[...]

(3) Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.

Art. 37 DS-GVO – Benennung eines bDSB

Artikel 37 Benennung eines Datenschutzbeauftragten

[...]

(5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.

(6) Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

Achtung: Prüfmöglichkeit in den Daten der Kommune

(7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

ULD www.datenschutzzentrum.de

Art. 39 DS-GVO – Aufgaben eines bDSB

(1) Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung [...];

b) Überwachung der Einhaltung dieser Verordnung [...] sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

c) Beratung [...] im Zusammenhang mit der Datenschutz-Folgen-abschätzung und Überwachung ihrer Durchführung gemäß Art. 35;

d) Zusammenarbeit mit der Aufsichtsbehörde;

e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, [...]

Hausaufgaben

- Datenschutz-Grundverordnung
  (und kommender Nachfolger der E-Privacy-Richtlinie)
  - Für Bundes- und Landesgesetzgeber
  - Für Datenschutzaufsichtsbehörden
  - Für Unternehmen
  - Für den öffentlichen Dienst
  - (Indirekt für Hersteller)
- Datenschutz-JI-Richtlinie
  - Siehe oben, soweit für den Bereich Polizei/Justiz/Inneres
- Viel zu tun bis Mai 2018!

Beispiel: Videoüberwachung

Zurzeit speziell geregelt (§ 20 LDSG, § 6b BDSG) – künftig auch?

§ 20 LDSG Video-Überwachung und -Aufzeichnung

(1) Öffentliche Stellen dürfen mit optisch-elektronischen Einrichtungen öffentlich zugängliche Räume beobachten (Video-Überwachung), soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrnehmung eines Hausrechts erforderlich ist und schutzwürdige Belange Betroffener nicht überwiegen.

(2) Der Umstand der Beobachtung und die dafür verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Speicherung oder weitere Verarbeitung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über die Speicherung oder Verarbeitung entsprechend § 26 zu unterrichten.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Beispiel: Videoüberwachung

Zurzeit speziell geregelt (§ 20 LDSG, § 6b BDSG) – künftig auch?

§ 20 LDSG

- Aufgabenwahrnehmung und Hausrecht contra schutzwürdige Betroffeneninteressen
- Hinweispflicht
- Datensparsamkeit (Monitorverfahren, kurze Löschfristen), Zweckbindung
- Verfahrensrechtliche Absicherungen

- Standortveröffentlichung im Netz möglich

Überblick

- Aktuelles Recht

- Änderungen durch die EU-Datenschutzreform

- Risiken durch Einbindung externer Angebote

- Einbindung von Bürgerinnen und Bürgern

- Angebot: Datenschutz-Audit

Beispiel: Hundebestandsaufnahme

- Frage:
  Dürfen Kommunen private Firmen mit einer Bestandsaufnahme von Hunden beauftragen, um auf dieser Basis die Hundesteuer eintreiben zu können?

- Antwort:
  Nein, im Steuerbereich keine privaten Dienstleister erlaubt, da Gesetzgeber besonders hohe Anforderungen stellt. Stattdessen kommunale Mitarbeiter der Steuerabteilung.

  Gesetzesänderung in Sicht, dass AuftragsDV erlaubt?
  ULD-Vorschlag: öffentliche Auftragnehmer

Beispiel: Tablets für Gemeindevertreter

- Frage:
  Wie können Mandatsträger Tablets einsetzen?

- Eine Antwort:
  Gemeinde stellt Mandatsträgern die Hardware für die Zeit des Mandats zur Verfügung und unterstützt beim datenschutzgerechten Einsatz:
  - Typisierung der Dokumente und Zugriffsrechte
  - Nutzungsbedingungen (z.B. keine private Nutzung)
  - Integration ins Sicherheitskonzept
  - Management-Software zur Pflege und Wartung

https://www.datenschutzzentrum.de/artikel/913-Verwendung-von-Tablets-durch-Gemeindevertreter.html

Beispiel: WhatsApp zur Kommunikation

- Frage:
  Darf WhatsApp zur Kommunikation mit Bürgerinnen und Bürgern eingesetzt werden?

- Antwort:
  WhatsApp ignoriert bislang die Anforderungen des deutschen und europäischen Datenschutzrechts:
  Aus dem Handy werden sämtliche Telefonnummern des Adressbuchs ausgelesen und in den USA verarbeitet.
  Kommunale Verfahren dürfen WhatsApp nicht verwenden.

Überblick

- Aktuelles Recht
- Änderungen durch die EU-Datenschutzreform
- Risiken durch Einbindung externer Angebote
- Einbindung von Bürgerinnen und Bürgern
- Angebot: Datenschutz-Audit

Beispiel: Ortsbeiräte und weitere Ehrenamtler

- Mitwirkung von Ehrenamtlern zu begrüßen
- Aber:
  - Wie werden die Verschwiegenheitspflichten garantiert?
  - Werden die Ehrenamtler bei der Verarbeitung der Daten unterstützt?
- Fälle, dass Familienmitglieder regelmäßig personenbezogene Daten zur Kenntnis bekommen haben
- Erhebliches Risiko einer ungeregelten Verwendung persönlicher (IT-)Datenverarbeitungssysteme

Überblick

- Aktuelles Recht
- Änderungen durch die EU-Datenschutzreform
- Risiken durch Einbindung externer Angebote
- Einbindung von Bürgerinnen und Bürgern
- Angebot: Datenschutz-Audit

Datenschutzaudit nach dem Landesdatenschutzgesetz Schleswig-Holstein

§ 43 Abs. 2 LDSG SH

Öffentliche Stellen können ihr Datenschutzkonzept durch das Unabhängige Landeszentrum für Datenschutz prüfen und beurteilen lassen.

Auditverfahren

- Auf freiwilliger Basis (Vertrag mit dem ULD)
- Gegenstand des Audits
  - Behörden
  - Abgrenzbare Teile von Behörden
  - Einzelne Verfahren
- Voraudit und Hauptaudit
- Auditfähigkeit in 3 Schritten
  - Bestandsaufnahme
  - Festlegung der Datenschutzziele
  - Einrichtung eines Datenschutzmanagementsystems
- Begutachtung des Prozesses durch das ULD
- Auditverleihung
  - Veröffentlichung des Kurzgutachtens des ULD
  - Befristung des Audits für 3 Jahre

Datenschutzmanagement: Bedingung für ein Datenschutzaudit

Hinweise des ULD:

8. Datenschutzmanagementsystem

8.1 Die Daten verarbeitende Stelle richtet ein Datenschutzmanagementsystem ein. Dieses dient als Mittel zur Umsetzung des Datenschutzkonzepts.

8.2 Das Datenschutzmanagementsystem stellt die interne Organisation der Daten verarbeitenden Stelle im Hinblick auf die Einhaltung der datenschutzrechtlichen und sicherheitstechnischen Vorgaben dar. Es ist die Gesamtheit aus Zuständigkeiten, vorgeschriebenen Verhaltensweisen und Abläufen sowie sächlichen Mitteln, die zur Erreichung der im Datenschutzkonzept festgelegten Regelungen dienen.

ULD www.datenschutzzentrum.de

Datenschutzmanagement: Bedingung für ein Datenschutzaudit

Hinweise des ULD:

8. Datenschutzmanagementsystem

[...]

8.3 Das Datenschutzmanagementsystem sieht zur Dokumentation und Überwachung des Datenschutz- und Sicherheitsprozesses Verfahrensweisen vor. Es muss über alle Veränderungen am Auditgegenstand informiert werden. Ferner sind wesentliche Änderungen des Auditgegenstandes zu dokumentieren und dem ULD mitzuteilen.

https://www.datenschutzzentrum.de/gesetze/hinweise-audit/#8

„Das Auditzeichen bescheinigt, dass sich die Gemeindeverwaltung vorbildlich um Datensicherheit kümmert. Dies ist in der heutigen Zeit alles andere als selbstverständlich", sagte Marit Hansen bei der Übergabe.

„Das zeigt uns, dass wir mit unserem Anspruch hinsichtlich Datenschutz und –sicherheit auf einem guten Weg sind", freute sich Bürgermeister Thomas Keller. Er betonte jedoch, dass seine Mitarbeiter den größten Teil der Arbeit geleistet hätten. So waren bei der Zertifikats-Übergabe auch die Hauptamtsmitarbeiter Marlies Schönrock als Datenschutzbeauftragte der Gemeinde, die stellvertretende Hauptamtsleiterin Ilka Böhm, Systemadministrator Stefan Georgi-Scholl und sein Stellvertreter Alexander Rieck dabei.

Marit Hansen und Heiko Behrendt vom Unabhängigen Landeszentrum für Datenschutz (2.v.r.) überreichten Bürgermeister Thomas Keller (rechts) sowie den Mitarbeitern Marlies Schönrock, Ilka Böhm, Alexander Rieck und Stefan Georgi-Scholl (von links) die Zertifikate und ein Hinweisschild für besonders geprüfte Datensicherheit im Ratekauer Rathaus.

„Es ist keine Selbstverständlichkeit, dass eine Gemeinde eine Datenschutzbeauftragte hat", lobte Marit Hansen und die stets offene Zusammenarbeit mit allen Verantwortlichen während des Audits.

„Dass die Daten geschützt werden müssen, ist in Landes- und Bundesgesetzen geregelt und die Einhaltung der Vorschriften ist noch kein Grund für die Ausstellung eines Zertifikats", ergänzte Heiko Behrendt, der Auditor des ULD. Das wird erst ausgestellt, wenn sich eine Gemeinde darüber hinaus freiwillig einer Begutachtung und Bewertung stellt. Auch damit sei die Gemeinde Ratekau herausragend, wenn man die Gemeinden im Umfeld betrachte.

Beispiel: Audit Ratekau

Funktionierendes Datenschutz-management

ULD www.datenschutzzentrum.de

Schlussfolgerungen

- Verantwortung für Datenschutz bedeutet, dass die Erfüllung der rechtlichen Anforderungen nachgewiesen werden können
  - Festlegung der Arbeitsabläufe
  - Dokumentation der automatisierten Verfahren und Entscheidungen
  - Bewusstsein für Risiken und Risikobehandlung
- Unterstützung durch behördliche Datenschutzbeauftragte und das ULD
- Kommunaler Datenschutz und Informationsfreiheit erhöhen Bürgervertrauen und demokratische Transparenz
- Moderne und sichere Verwaltung ist kommunaler Standortfaktor

Vielen Dank für Ihre Aufmerksamkeit!

Marit Hansen
Unabhängiges Landeszentrum für Datenschutz
Holstenstraße 98, 24103 Kiel

Quellen

- ULD-Webseite
  https://www.datenschutzzentrum.de/
- Virtuelles Datenschutzbüro
  http://www.datenschutz.de/
- Dr. jur. Martin Zilkens:
  Datenschutz in der Kommunalverwaltung,
  4. Aufl. 2014, 687 S.