DS- GVO

(Datenschutz-Grundverordnung VO(EU)2016/679)

für Kommunalverwaltungen

Fassung 1.0. Rechtsstand 4.6.2018

Malte Jörg Uffeln

Bürgermeister der Brüder-Grimm- Stadt Steinau an der Straße

Mag.rer.publ. Mediator (DAA) MentalTrainer

Lehrbeauftragter

Fortbildung in Krisenpädagogik nach Prof. Dr. Bijan Amini

Rechtsanwalt (Zulassung ruht nach § 47 BRAO)

www.maltejoerguffeln.de

Mein Service für Sie:

- ✓ **Vortrag DS- GVO für Kommunalverwaltungen**
- ✓ **Vortrag zur DS- GVO Fassung 6.0. (01.06.2018)**
- ✓ **Vortrag über Bürgerrechte im Datenschutz**
- ✓ **AUFSATZ zum Thema DS- GVO… Was jetzt getan werden muss !**
- ✓ **AUFSATZ zu Art. 6 Abs. 1 lit. f.) DS- GVO**
- ✓ **CHECKLISTE zur DS- GVO im kostenfreien download unter**
- ✓ **DS- GVO für Vereine 6 Folien in 6 Minuten**

www.maltejoerguffeln.de

I.

Sensibilisierung

Warming Up… I

87 Prozent der deutschen Firmen hinken bei der Umsetzung der DS-GVO hinterher

Quelle:

http://meedia.de/newsline-detail/87-prozent-der-deutschen-firmen-hinken-bei-der-umsetzung-der-dsgvo-hinterher/

- ***„große Verunsicherung“***
- ***„große Menge von Halbwissen“***
- ***„Vollzugsdefizit“***

Eine Meinung zur DS- GVO

Prof.Dr. Thomas Hoeren

„…eines der schlechtesten Gesetze des 21.Jahrhunderts…“

„…hirnlos…“

Quelle:

https://www.bdsg-externer-datenschutzbeauftragter.de/datenschutz/informationsrechtler-kuert-die-neue-europaeische-datenschutzverordnung-zu-einem-der-schlechtesten-gesetze-des-21-jahrhunderts/

Warming Up II

(https://www.ekom21.de/Service/einfo21_digital/Seiten/dsgvo.aspx)

Was kommt auf Kommunen zu?

Und damit die Verordnung auch Anwendung findet, stärkt die DS-GVO die Aufsicht durch Datenschutzbehörden und sieht bei Verstößen *empfindliche Geldstrafen* vor. Alle Entscheidungsträger in Behörden und Kommunen sollten sich der Auswirkungen der DS-GVO für den alltäglichen Betrieb bewusst sein. Denn verstoßen sie oder ihre Rechenzentrumsbetreiber gegen die DS-GVO, etwa indem sie die strengen Erlaubnistatbestände für die Verarbeitung personenbezogener Daten missachten, drohen *Sanktionen.*

Weiterführende Links:

www.bfdi.bund.de

www.lda.bayern.de

www.datenschutz.hessen.de

www.datenschutz.de

www.duesseldorfer-kreis.de

www.datenschutzbeauftragter-info.de

II.

Die Rechtsprechung des Bundesverfassungsgerichts zum Datenschutz

Volkszählungsurteil

„ Grundrecht auf informationelle Selbstbestimmung “

(BVerfGE 65,1 ff.)

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger

begründeten freiheitlichen demokratischen Gemeinwesens ist.

Hieraus folgt: Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.

Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

„Integritätsgrundrecht“

BVerfG, 1 BvR 370/07 und 1 BvR 595/07

Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Entwicklung der Rechtsprechung

BVerfGE 65,1 (Volkszählung)

BVerfGE 93, 181 (Rasterfahndung)

BVerfGE 100, 313 (Telekommunikationsüberwachung)

BVerfGE 103, 21 (Genetischer Fingerabdruck)

BVerfGE 103,44 (Fernsehaufnahmen im Gerichtssaal)

BVerfGE 112, 304 (GPS-Überwachung)

III.

Grundprinzipien

Datenschutz

=

Schutz der Menschen

Datensicherheit

=

Schutz der Daten

Die *LOGIK* des Datenschutzes:

VERBOT mit Erlaubnisvorbehalt

Aus der Praxis für die Praxis:

Dürfen wir Daten aus öffentlichen Quellen ohne Eiwilligung des Betroffenen verwenden ?

- Adress- und Telefonbücher
- Öffentliche Register
- Veröffentlichungen
- Internet – nicht passwortgeschützt

Grundsatz der Verhältnismäßigkeit

verlangt stets eine Güterabwägung der Rechte des Betroffenen zu den jeweiligen Zwecken der Kommune

Rechte des Betroffenen

- *Recht auf informationelle Selbstbestimmung*
- *Schutzgrad personenbezogener (auch sensibler) Daten*
- *weitere Grundrechte/Rechtsgüter*

(bspw. Unverletzlichkeit der Wohnung, Post- und Fernmeldegeheimnis, Sozialdatenschutz

Zwecke der Kommune

- *Auslegung der Hauptsatzung*
- *Zweckfestlegung und – bindung; Hauptsatzung, individuelle Satzungen, Verordnungen, Richtlinien*
- *technische und organisatorische Maßnahmen nach dem Stand der Technik*
- *Sanktionen (Androhung, Vollstreckung)*

IV.
Entwicklungen im Datenschutz

Allgemeine Entwicklungen im Datenschutz 2018 ff.

- **EU: „ Ausweitung Verbraucherrechte“**
- **BUND/LÄNDER „ Datenschutz- und Informationsfreiheitsgesetz“(https://netzpolitik.org/2017/schwarz-gruen-in-hessen-will-schlechtestes-informationsfreiheitsgesetz-deutschlands)**
- **Städte/Gemeinden „ IT- Audit (Prüfungen)“ ,**

  § 131 I Nr. 4 HGO
- **Neue Abmahngefahren; Zunahme von Abmahnungen**
- **Verstärkung der Kontrolldichte auf EU-Ebene**
- **„Mehr“ Bürokratie (Verarbeitungsverzeichnis!)**
- **Rechtsunsicherheiten bei einheitlicher Auslegungen der DS- GVO**

Erwartungen der Datenschutzbehörden an kommunale Datenverarbeiter I

Prüfpunkte: Wo/wie wird hingesehen ?

- ✓ Bestandsaufnahme der Datenverarbeitungsvorgänge (IST- Analyse)
- ✓ Prüfung der Legitimationen („Einwilligungen“)
- ✓ Erfüllung der Informationspflichten Führen eines Verfahrensverzeichnisses

Künftige Prüfungen (ab 25.5.2018) ?

„Vom situativen Eingreifen zur systematischen Kontrolle !!!“

Erwartungen der Datenschutzbehörden an kommunale Datenverarbeiter II

- ✓ Erfüllung der Rechenschaftspflicht (Artt. 5, 27 DS-GVO)
- ✓ Bestellung eines Datenschutzbeauftragten (Art. 37 DS-GVO)
- ✓ Erstellung eines Vereichnisses der Verarbeitungstätigkeiten (Art. 30 DS- GVO)
- ✓ Datenschutzmanagement (Art. 24 DS- GVO)
- ✓ Datenschutzfolgenabschätzung (Art. 35 DS- GVO)
- ✓ Einwilligungen prüfen (Beachte Koppelungsverbot Art. 7 IV DS- GVO)
- ✓ Verarbeitung von Mitarbeiterdaten (§§ 26 I,IV BDSG) klären

V.

Ziele der DS- GVO

Art. 288 AEUV

„Die Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat“

(Kritik: Verordnung mit Richtliniencharakter!)

Art. 8 GRCh der EU

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) 1Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. 2Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Art. 1 DS- GVO

- **Schutz von Menschen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr der Daten**

- **Schutz der Grundrechte und Grundfreiheiten von Menschen**

<u>Nicht geschützt:</u> Verstorbene (Problem bei Chroniken! <u>Aber:</u> postmortales Persönlichkeitsrecht. Beachte § 22 Satz 3,4 KUG)

Künftig sind zu beachten:

- **DS- GVO (99 Artikel)**
- **173 Erwägungsgründe zur DS-GVO**
- **BDSG (neu)**
- **Ausführungsgesetze zur DS-GVO**
- **Landesrechtliche Bestimmungen**

Öffentlicher Bereich

Nationale Sonderbestimmungen gelten fort !

Nicht- öffentlicher Bereich

(1)DS- GVO ersetzt BDSG, LDSG´s

(2) Umfangreiche Rechtsbereinigung in Sondergesetzen wie z.B.: Melderecht, Sozialrecht, TMG, TKG, BetrVG, UWG

VI.
DS- GVO
Grundwissen

1.

Rechtmäßigkeit der Datenverarbeitung

(Art. 6 DS- GVO)

Verbotsprinzip

„Verbot mit Erlaubnisvorbehalt“

Zulässigkeit der Datenverarbeitung

Erlaubnistatbestände des Art. 6 I DS- GVO

(a) Einwilligung

(b)Vertrag und vorvertragliche Maßnahmen

(c) Rechtliche Verpflichtungen

(d) Lebenswichtige Interessen

(e) Öffentliches Interesse, Ausübung öffentlicher Gewalt

(f) Berechtige Interessen eines Verantwortlichen oder Dritten

BEACHTE:

1.Art. 6 I lit. f.) gilt nicht für Behörden

2.Öffnungsklausel des Art. 6 II DS- GVO (weiter Spielraum)

Welche Daten „verarbeiten“ wir ?

- **Bestandsdaten**

Nutzungsdaten

- **Abrechnungsdaten**

1.1.

Einwilligung (Consent)

(Definition in Art. 4 Nr. 11 DS-GVO;

Art. 2 lit.h DSLR)

„Das Maß der Rechtmäßigkeit der Datenverarbeitung“

„Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Einwilligung = vorherige Zustimmung

- **stets vor der Verarbeitung!**
- **unmissverständlich, auch durch Mausklick!**

Wirksamkeitsvoraussetzungen:

Freiwillige(freely given) spezifisch informierte eindeutige Handlung ohne Zwang!

- **Freiwilligkeit und Kopplungsverbot**

(nicht erforderliche Daten dürfen nicht erhoben werden, keine allgemeine Datensammlung)

- **Informiertheit (konkreter Fall, Erklärung in Kenntnis der Sachlage)**
- **Schriftlich oder elektronisch oder mündlich**

Wirksamkeitsvoraussetzungen:

ErwG Nr. 5

- **„echte“ oder „freie“ Wahl**
- **„Weigerungsoption“, „Zurückziehungsoption“**
- **„ohne Nachteile zu erleiden“**

Betroffener muss wissen

- ✓ **WER soll die Daten nutzen dürfen ?**
- ✓ **WELCHE Daten sollen genutzt werden ?**
- ✓ **Zu WELCHEM ZEITPUNKT sollen die Daten genutzt werden dürfen?**
- ✓ **Darf der Verarbeiter die Daten weitergeben und wenn ja an wen konkret ?**
- ✓ **WIE LANGE darf die Nutzung andauern ?**

Fälle aus der kommunalen Praxis:

- **Bilder aus/von Kindergärten**
- **Veröffentlichungen von Geburtstagen, Ehejubiläen in Amtsblättern, Gemeindebriefen**

BEACHTE:

Nicht zulässig sind BLANKO- Einwilligungen

MERKSÄTZE

1.Nachweis über Einwilligung muss der verantwortliche Datenverarbeiter (Verein, Verband) führen

2.(Er-)neu(t)e Einwilligung kann „später“ bei Zweckänderungen erforderlich sein

(Beispiel: Dachverband verlangt weitere Mitgliederdaten)

3.Der Betroffene muss die Einwilligung jederzeit widerrufen können (Art. 7 Abs. 3 DS- GVO)

Formen der Einwilligung

- ✓ **schriftlich**
- ✓ **elektronisch**
- ✓ **Mündlich**
- ✓ **sonst eindeutigen bestätigenden Handlung (or by a clear affirmative action) = konkludent (schlüssiges Handeln)**

Praxisproblem:

Nachweispflicht (Art. 7 I DS- GVO)!!

MERKE:

- **Schweigen und Untätigkeit sind keine Erklärung**

(ErwG 32)

- **Dulden ist keine Handlung**

Praxisfall Fotos

- **„Anlächeln“ des Fotografen ist keine Einwilligung**
- **„Betreten“ eines videoüberwachten Gebietes ist keine Einwilligung**

Fiktive Einwilligung geht nicht!

Widerspruchslösung qua Satzung

Einwilligung wird unterstellt, wenn nicht widersprochen wird, *geht nicht!!!*

MUSTER einer Einwilligungserklärung

https://www.baden-wuerttemberg.datenschutz.de/datenschutz-im-verein/

„Intellektualität“/Sprache ?

- ✓ klar und einfach
- ✓ keine Verschleierung von Tatsachen
- ✓ Keine Schachtelsätze
- ✓ Vermeidung von Fachvokabular

Fall aus der kommunalen Praxis:

Umgang mit bereits bestehenden Einwilligungen nach dem 25.5.2018 ?

- ErwG 171 „Fortgeltung bisheriger Einwilligungen!!!“

1.2.
Besondere Datenkategorien
„Sensible Daten“
(Art. 9 DS- GVO)

Die Regel des Art. 9 I GS- DVO

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

2.

Prinzipien der Datenverarbeitung

(Art. 5 DS- GVO)

2.1.
Rechtmäßigkeit
Treu und Glauben
Transparenz

2.1.1.
Rechtmäßigkeit

- **Einwilligung**
- **sonstige Rechtsgrundlage**

2.1.2.

Treu und Glauben (fairly/loyale)

- „fair“
- vgl. auch: §§ 157,242,275 Abs. 2 S. 2,

  815 BGB
- Treuwidrig und „ nicht fair“ ist die Verwendung verborgener Techniken, wie die heimliche Videoüberwachung,Spyware

2.1.3.

Transparenz

- **keine heimlichen Verarbeitungen**
- **umfassende Informationen der betreffenden Person**
- **ErwG 39: Kriterien Umfang, Identitat,Errhebung,Verwendung, Einsicht, Zwecke etc.**

Der Fall aus der Praxis:

Videoüberwachung eines Dorfgemeinschaftshauses

- ✓ Transparenz schaffen: „Hinweisschild“
- ✓ Videoüberwachung ist „ ultima ratio“
- ✓ Erforderlichkeit ist bzgl. jeder einzelnen Kamera zu prüfen

2.2.
Zweckbindung

- ✓ **genau festgelegt**
- ✓ **eindeutig**
- ✓ **legitim**

Zwecke der Kommune

bestimmen über die

- **Zulässigkeit,**
- **Art und Weise**
- **Umfang der Datenverarbeitung**

<u>Stets Satzung prüfen und auslegen !!!</u>

Die personenbezogenen Daten müssen für den verfolgten Zweck *„erheblich“* und *„ angemessen“* sein

Erheblichkeit

Daten müssen für den Zweck relevant sein

✓ geeignet

✓ erforderlich)

Angemessenheit

Nicht erhebliche oder dem Zweck nicht dienende Daten dürfen nicht erhoben werden.

<u>Beachte:</u>

- **Grundsatz der Datenminimierung**
- **Satzungen von Dachverbänden**

Welche Daten sind dies ?

- Name und Anschrift
- Bankverbindung
- Eintrittsdatum
- Geburtsjahr (- datum)
- Kommunikationsverbindungen(?)
- Funktionen/Kenntnisse/Fähigkeiten(?)
- Kfz- Kennzeichen(?)
- Kreditkartennummer(?)

2.3.
Datenminimierung
Datensparsamkeit

Grundsatz der Datenminimierung

(alt: § 3 a BDSG; Datenvermeidung, Datensparsamkeit)

- **Verringerung der Anzahl der verarbeiteten Daten**
- **Verringerung der Anzahl der Nutzungen**
  (Rechtswidrigkeit von Mehrfachauswertungen)
- **Verringerung der Anzahl der Betroffenen**
- **Bereitstellung der Daten zum Lesen auf dem Bildschirm ohne Ausdruck**

2.4.
Richtigkeit

- ✓ **Sachlich richtige, aktuelle Daten**
- ✓ **Vorsorgen für unverzügliche Löschung**
- ✓ **Unaufgeforderte Berichtigung unzutreffender Daten**

2.5.
Speicherbegrenzung

2.6.
Integrität und Vertraulichkeit

Schutzvorkehrungen

(IT- Sicherheit) treffen vor

- **unrechtmäßiger Verarbeitung**
- **zufälligem Verlust**
- **zufälliger Zerstörung und (Be-)Schädigung**

2.7.

Rechenschaftspflicht

Informationspflichten

Umkehr der Beweislast:

„Der Verantwortliche muss…“

Verantwortlicher für Datenverarbeitung

- ***achtet auf*** **Einhaltung der Prinzipien**
- ***weisst*** **Einhaltung der Prinzipien *nach***

Grundsatz des risikobasierten Ansatzes

„ geeignete technische und organisatorische Maßnahmen“ sind zu treffen!

Datenschutzrechtliche Unterrichtung (Art. 13 I, II DS- GVO)

Informationspflichten des Datenverarbeiters

Beachte:

Nichterfüllung der Pflicht ist bußgeldbewehrt!

LINK:

Informationsblätter

https://www.baden-wuerttemberg.datenschutz.de/orientierungshilfen-merkblatter/

Hinweispflichten

- Name , Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Konkrete Zwecke der Verarbeitung
- Rechtsgrundlage der Verarbeitung
- Berechtigte Interessen (Art. 6 DS- GVO)
- Empfänger/Kategorien von Empfänger der Daten
- Absicht über Drittlandtransfer (Mitgliederverwaltung in einer cloud)
- Speicherdauer der personenbezogenen Daten
- Belehrung über Betroffenenrechte
- Hinweis auf jederzeitiges Widerrufsrecht der Einwilligung
- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde

Aus der Praxis für die Praxis:

Beispiel für eine umfassende Datenschutzerklärung

https://datenschutz.hessen.de/datenschutzerkl%C3%A4rung

3.

Datenportabilität

(Art. 20 DS-GVO)

Der Bürger hat ein Recht auf Datenübertragbarkeit!

Rechtsanspruch

(Herausgabeanspruch) auf Erhalt eigener personenbezogener Daten und auf Übertragung in Verarbeitungssystem eines anderen Verantwortlichen

(selbst oder mittelbar von Verantwortlichem zu Verantwortlichem)

„Grundsatz der Interoperabilität, Übertragung in ein gängiges Format“

4.

Recht auf Einschränkung der Verarbeitung

(Art. 18 DS- GVO)

„ Sperrung “(alt: § 35 II BDSG)

Fälle:

1. **Bestrittene Richtigkeit der Daten**
2. **Unrechtmässige Verarbeitung**
3. **Wegfall der Verarbeitungsnotwendigkeit**
4. **Widerspruch gegen die Verarbeitung nach Art. 21 Abs. 1 DS-GVO**

5.

Recht auf Vergessen werden

(Art. 17 Abs. 2 DS- GVO)

„Der digitale Radiergummi!“

Hintergrund:

Entscheidung des EuGH vom 13.5.2014 C 131/12

„Google spain“

Der Betroffene hat ein Recht auf Vergessen werden im Internet

Quelle:

http://curia.europa.eu/juris/liste.jsf?language=de&num=C-131/12

Art. 17 Abs. 1 DS- GVO

„Löschung“

Informationen Anderer über

- alle Links
- Kopien und Replikationen

Exkurs:

Löschfristen Arbeitsrecht

- § 17 Antidiskriminierungsgesetz: 6 Monate

  (abgelehnte Bewerber)

- Unterlagen nach AZG, MuSchG: 2 Jahre

- §§ 28 f SGB IV (Entgeltunterlagen; Unterlagen für Jahresabschluss, bspw. Lohnbuchhaltung. Zehn Jahre

  (§§ 257,147 AO)

6.

Im Überblick

Die Rechte des Bürgers….

Recht auf

- Auskunft
- Löschung
- Berichtigung
- Widerruf und Widerspruch
- Einschränkung
- Datenmitnahme
- Protokollierung
- Beschwerde bei der Aufsichtsbehörde
- Schadenersatz

VII.

Datenschutzbeauftragter

(Art. 37 I a DS- GVO; § 38 BDSG)

„Unabhängig“, „weisungsfrei“

Grundsatz der Selbstkontrolle

Das System der Datenschutzkontrolle

- **Selbstkontrolle** (Betroffene)
- **Eigenkontrolle**

(Datenschutzbeauftragte)

- **Fremdkontrolle**

(Aufsichtsbehörden)

Variante I

„verpflichtend“ für Unternehmen

(Art. 37 Abs. 1 DS- GVO)

„verpflichtend für Behörden“

(Art. 37 I a DS – GVO)

Variante II

„freiwillig“ in anderen Fällen

(… Verbänden, Vereinigungen…)

(Art. 37 Abs. 4 DS GVO, § 38 BDSG)

Kernbereiche der Tätigkeit

- **Sicherstellung des Datenschutzes**
- **Hinwirkung auf Einhaltung des Datenschutzes**
- **Überwachung der Organisation**

Bestellungsoptionen I

Variante 1

Interner Datenschutzbeauftragter

(keine Bestellung von: Leiter der IT- Abteilung, Behördenleiter, Personalleiter, Hauptamtsleiter, Webmaster)

Beachte: Art. 38 III 1 DS- GVO „ nicht weisungsgebunden“

Bestellungsoptionen II

Variante 2

Externer Datenschutzbeauftragter

(I.d.R. gegen Entgelt, § 611 BGB Dienstvertrag)

Bestellungsoptionen II

Variante 3

Gemeinsamer Datenschutzbeauftragter

(Art.37 III DS- GVO)

in Vollzeit und Teilzeit, je nach Größe der Kommune

Qualifikationen ?

Keine Regelung in der DS- GVO

Empfehlungen(!)

- **Fachwissen im Datenschutzrecht und der Datenschutzpraxis**
- **Technisches und organisatorisches Fachwissen**
- **Kommunikationsfähigkeit**

Information und Transparenz

- **Bestellung ggf. durch Beschluss des Vorstandes**
- **Namentliche Meldung an die Aufsichtsbehörde**
- **Mitteilung der Anschrift auf der Homepage des Vereins**
- **Spezieller e-mail-Account:**

datenschutzbeauftragter@gemeinde musterdorf.de

Praxis des Datenschutzbeauftragten I

- ✓ Beraten und unterrichten
- ✓ Überwachen und sanktionieren
- ✓ Datenschutzfolgen abschätzen und beraten
- ✓ Ansprechpartner zur Datenschutzaufsicht
- ✓ Zusammenarbeiten mit Vorstand und Datenschutzaufsicht
- ✓ Risikoabwägung
- ✓ Beraten lassen durch Datenschutzaufsicht

Praxis des Datenschutzbeauftragten II

Art. 39 DS- GVO

- Festlegung Überwachungsprozess
- Zuweisungen an einzelne Mitarbeiter

VIII.

Verarbeitungen, Prozesssicherheit

1.

Datenschutz durch Technikgestaltung (Privacy by Design) und datenschutzfreundliche Voreinstellung (Privacy by Default)

Art. 25 DS- GVO

2.
Datenschutz-Folgenabschätzung
(Art. 35 DS- GVO)

Mögliche Vorgehensweise:

1. Erforderlichkeit ? (Prozess und Ergebnis festhalten)
2. Mögliche Vorgaben der Aufsichtsbehörden
3. Prozessbeschreibung
4. „Vorherige Konsultation“ (der Aufsichtsbehörde) klären

3.

Sicherheit der Verarbeitung

(Art. 32 DS- GVO)

Angemessene Sicherheitsvorkehrungen

IT- Sicherheitsziele

- **Vertraulichkeit**
- **Integrität**
- **Verfügbarkeit**
- **Sicherheitsmanagement**

Exkurs:

Datensicherung digitaler und analoger Daten

3.1.
Digitale Daten

- ✓ **Passwortzugang für PC, Laptop**
- ✓ **Passwortschutz für mobile Datenträger (USB Stick, Festplatten)**
- ✓ **Sicherung auf einem externen Server**
- ✓ **Verschlüsselte Datenübermittlung**

3.2.
Analoge Daten

- ✓ **Lagerung in abgeschlossenen Räumen**
- ✓ **Lagerung in abschließbaren Schränken**
- ✓ **Digitalisieren(Scannen) und Integration in Software**
- ✓ **Schutzvor fremden Zugriff**

(nicht rumliegen lassen)

4.

Verzeichnis von Verarbeitungstätigkeiten(VVT)

(Art. 30 DS- GVO)

Muster:

https://dsgvo-vorlagen.de/bestandteile-muessen-in-verfahrensverzeichnis-dsgvo

https://www.datenschutz-praxis.de/fachnews/datenschutzkonferenz-bietet-muster-fuer-verarbeitungsverzeichnis/

Verantwortlicher:

Aufzeichnung aller Verarbeitungstätigkeiten

Auftragnehmer:

Aufzeichnung der durchgeführten Tätigkeiten

Weitere Dokumentationspflichten aus anderen Rechtvorschriften!!!

Formelle Anforderungen des VVT

- **Behördenleiter legt Verantwortlichen fest (Direktionsbefugnis § 106 GewO)**
- **„Chefsache“: Z- Abteilung oder Hauptamt**
- **VVT „manuell“ oder“ elektronisch“**

Inhaltliche Anforderungen des VVT

- **„prozessorientierter Übersicht der Verarbeitungen“**

Wer ? Was ? Wann ? Wie ? In welcher Art und Weise ?

- **ZIEL: Identifikation der Datenverarbeitungsprozesse**
- **BEACHTE: Art. 30 I lit. a- g DS- GVO**

VVT für alle kommunalen Prozesse erstellen

- Grundsteuer A und B
- Gewerbesteuer
- Hundesteuer
- Verbrauchsgebühren (insbes. Wasser, Abwasser)
- Friedshofswesen
- Firmendaten (Hochbau; Tiefbau)
- Freiwillige Leistungen…….

5.

Dokumentations- und Nachweispflichten

5.1. Dokumentationspflichten

- **Dokumentierte Weisungen**
- **Verzeichnete Verarbeitungstätigkeiten**
- **Verletzungen des Schutzes personenbezogener Daten**
- **Abwägungen**

5.2. Nachweispflichten

- **Einhaltung der Verarbeitungsprozesse**
- **Einwilligungen**
- **Unbegründetheit von Anträgen**
- **Erfassung der Verarbeitung**
- **Einhaltung der DS- GVO**
- **Kontrolle**

IX.

Bußgelder, Sanktionen

- ✓ **Wirksam**
- ✓ **verhältnismäßig**
- ✓ **abschreckend**

Bußgeld bis zu

10.000.000,00 € (bis zu 2%)

20.000.000,00 € (bis zu 4 %)

des weltweiten Umsatzes

Maßstäbe, Kriterien I

- ✓Art
- ✓Schwere
- ✓Dauer
- ✓Anzahl der Betroffenen

Maßstäbe, Kriterien II

- ✓Vorsatz oder Fahrlässigkeit
- des Verstoßes ***(verschärfend)***
- ✓ Maßnahmen zur Minderung des Schadens ***(mildernd)***

1.

Beschwerde bei der Aufsichtsbehörde

2.

Verbandsklage

Vertretung eines „Betroffenen“ durch einen Verband

(s.a. nationales Recht; UKlaG)

3.

Schadenersatz, Strafe

Bußgeld

X.

Sonderfälle

1.
Website- Compliance

Jetzt handeln:

Datenschutzerklärung anpassen an

DS- GVO

ePrivacy-Verordnung der EU betreffend Informationspflichten und Einwilligung bei der Nutzung von Cookies auf Webseiten umsetzen.

Weiter beachten:

§§ 11 ff. TMG, § 13 TMG

2.

Videoüberwachung

Nicht explizit geregelt in der DS- GVO !

Prüfung nach Art. 6 Abs. 1 Satz 1 lit f. DS- GVO

Grundsätzliche Anforderungen

- **Beschränkung auf das unbedingt notwendige Maß**
- **Intensität der Überwachung darf nicht außer Verhältnis zum verfolgten – präventiven- Zweck stehen !**

Ergo:

Verhältnismäßigkeitsprinzip

3.

Data Breach Notification

(Datenpannen… Was ist zu tun?)

Datenpannen

1. Datenschutzverletzung muss innerhalb von 72 Stunden der Aufsichtsbehörde gemeldet werden.
2. Meldung an die Betroffenen
3. Dokumentation

Notwendigkeit einer Cyberversicherung ?

Cyber-Versicherung I

Vielfältige Begrifflichkeit:

Data Protect, Datenschutz-Versicherung, Data-Risk, Cyber-Deckung, Hacker- Versicherung, ergänzend: Elektronikversicherung, Datenträgerversicherung

Ziel:

Schutz vor Hacker- Angriffen und Cyberkriminalität

Cyber-Versicherung II

Versicherungsumfang

- **Drittschäden (Datenrechtsverletzung durch VN)**
- **Eigenschäden (bspw. Hacker-Angriff, DoS-Attacke-Dienstverweigerung-)**

Cyber-Versicherung III

Kostenersatz:

- Wiederherstellung, Reparatur der IT-Systeme
- Kosten für Computer-Forensik-Analysten
- Fachanwälte für IT- Recht
- Krisenmanagement und PR
- Kreditschutz/-überwachung
- Interner Strafrechtsschutz (Strafverteidigung)
- Mehrkosten zur Fortführung des Betriebes

Cyber-Versicherung IV

<u>Mögliche Ergänzungen:</u>

- **Betriebsunterbrechungsversicherung**
- **Ertragsausfallversicherung (Umsatzausfälle!)**

4.

Datenschutzmanagementsystem

Verpflichtend für Unternehmen!

Vereine und Verbände: Empfehlung!

Weiterführender Link:

Leitfaden für die betriebliche Praxis

https://www.datenschutzbeauftragter-info.de/datenschutzmanagement-nach-der-dsgvo-leitfaden-fuer-die-praxis/

Der Datenschutzmanager

(DSM)

nach VdS 10010

(VdS Richtlinien zur Umsetzung der DSGVO)

- **implementiert ein Datenschutzmanagementsystem**
- **erarbeitet Verbesserungsvorschläge**
- **Unterstützt Vorstand nach § 26 BGB**
- **prüft und passt DS- Richtlinien jährlich an**
- **untersucht datenschutzrelevante Ereignisse**
- **ist Ansprechpartner bei Projekten**
- **berichtet jährlich an den Datenschutzbeauftragten**
- **ist Ansprechpartner, wenn kein Datenschutzbeauftragter bestellt ist**

XI.

Was müssen wir jetzt tun ?

Checkliste zur Umsetzung der DS- GVO

Papiere zur DS- GVO

https://www.lda.bayern.de/media/dsgvo_fragebogen.pdf

Checkliste

Unsere Fragen an uns ?!

Weiterführender Link:

http://ds-gvo.gesundheitsdatenschutz.org/html/checkliste.php

I. Der aktuelle IST- Zustand

1. Welche Daten verarbeiten wir ?
2. Wozu verarbeiten wir die Daten ?
3. Wie werden die Daten verarbeitet ?
4. Rechtsgrundlagen der Verarbeitung ?

5. Liegen Einwilligungen vor ?

5.1. schriftlich von den Betroffenen ?

5.2. Satzungsklausel ?

5.3. BDSG, DS- GVO

6. Unser Umgang mit den Rechten der Betroffenen ?

6.1. Verarbeitung

6.2. Sperrung

6.3. Löschung

7. Kritische Fälle aus der Vergangenheit ?

8. Haben wir einen Datenschutzbeauftragten ?

9. Welche internen Beschlüsse, Richtlinien etc. gibt es ?

10.Sicherheit unserer Datenverarbeitung ?

11. Datensensibilität ?

12. Anforderungen Dritter ?

II.

Der ab 25.5.2018 geforderte SOLL- Zustand nach DS- GVO

III.

Vergleich IST- Zustand zu SOLL- Zustand

IV.

Handeln, Umsetzen, Machen

1. Zeitplanung

Was? Wann ? Wie ? Wer konkret ?

1. Budgetplanung

2. Notwendige Maßnahmen

3.1. Einwilligungserklärungen neu fassen

3.2. Datenschutzklauseln in gemeindlichen Satzungen etc. ?

3.3. Verantwortlichkeiten in der Verwaltung klarstellen

3.4. Homepage checken

3.5. Änderungen in der e-mail-Korrespondenz ?

3.6. Mitarbeiter schulen

3.7……..

4. Compliance- System ?

5. Sanktionen ?

6. Offene Punkte _____

XIII.

Prozessevaluierungen über den 25.5.2018 hinaus

Dokumentieren und Risikoanalyse

Dokumentieren

1. Datenschutzdokumentation
2. Transparenz
3. Datenschutzfolgenabschätzung
4. Beschwerdemanagementsystem
5. Vertragsmanagement
6. Einwilligungsmanagement

Weitere hilfreiche LINKs:

https://www.datenschutz-nord-gruppe.de/

http://ds-gvo.gesundheitsdatenschutz.org/html/checkliste.php

http://www.hlfp.de/dokumente/blog/HLFP-Checkliste-DSGVO-DE.pdf

https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/160909-EU-DS-GVO-FAQ-03.pdf

https://www.it-zoom.de/it-mittelstand/e/checkliste-geruestet-fuer-den-eu-datenschutz-13730/

Bereich der Risikoanalyse I

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übertragungskontrolle

Bereich der Risikoanalyse II

- Eingabekontrolle
- Transportkontrolle
- Wiederherstellbarkeit
- Zuverlässigkeit
- Datenintegrität
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennbarkeit

XIV.

Einzelfälle aus der kommunalen Praxis

1.

Zusammenarbeit mit anderen Kommunen ?

- **Ja, bei Datenschutz und IT-Sicherheit (AK Datenschutz-, Datensicherheit)**
- **„gemeinsamer Datenschutzbeauftragter“**

2.

DS- GVO und Homepages der Gemeinde, Schule, Feuerwehren, Allianz

- **Jede Homepage einzeln prüfen und handeln**
- **Verantwortlichkeiten klarstellen**
- **Datenschutzerklärung auf Homepage**

3.

Umgang mit e- mails

- **BCC (Blind Copy) statt CC**
- **Art. 32 I Hs. 2 lit. a DS- GVO**

(<u>klare Empfehlung</u>: Verschlüsselung personenbezogener Daten)

4.

Anforderungen an Räumlichkeiten „offenliegende Akten“

- **Zugangskontrolle**
- **Nutzerkontrolle**

5.

Umgang mit Daten zwischen den Beschäftigten

- **DA= Dienstanweisung ist zu empfehlen**
- **Wer? nutzt? verarbeitet? welche Daten ? Wie ?**

6.

Notwendigkeit eines stv. Datenschutzbeauftragten ?

- **I.d.R. „nein“**
- **Regelung der Vertretung „intern“ bei Datenschutz/ Datensicherheit empfehlenswert**

7.

Datenschutzbeauftragter auf Homepage

JA, mit spezieller Adresse

datenschutzbeauftragter@gemeinde musterdorf.de

8.

Verlinkung auf andere Homepages

- **Inhalte „vor“ Verlinkung prüfen**
- **Seiteninhaber der verlinkten Seite auf Verlinkung hinweisen**
- **Verlinkte Seite ab und an prüfen und ggf. handeln**

9.

Datenschutz in gemeindlichen Satzungen

- **jede einzelne „neue“ Satzung individuell prüfen und handeln**
- **Empfehlungen Kommunalaufsicht, Datenschutzbeauftragter, Kommunaler Spitzenverband einholen**

10.

Datenschutz und Bürger

„Mitteilungen“

- **notwendige Einwilligungen i.R.v. Art. 6 DS- GVO einholen**
- **Ggf. „ erneutes“ Einwilligungserfordernis „ später“ prüfen**

11.

Datenschutz bei Vereinen und Verbänden

Punkt 1

Verantwortlichkeiten im Vorstand definieren

- Aufgabenzuweisungsbeschluss des Vorstandes
- GO/ Geschäfts-/Aufgabenzuweisungsplan

Punkt 2

Einwilligungserklärung

(Beitrittserklärung) prüfen und „ neu“ fassen

- Beitritts-,Einwilligungserklärung „alt“ prüfen und “neu“ fassen
- Art. 6 DS- GVO berücksichtigen

Punkt 3

Datenschutzklausel in der Satzung verankern

- Kombination Datenschutz, Foto-,Bild-, Urheberrechte in der Klausel
- MUSTER: www.maltejoerguffeln.de

Punkt 4

Brauchen wir einen Datenschutzbeauftragten(DSB) ?

- **„Mehr“ als 9 Menschen/mind. 10 Personen verarbeiten ständig automatisiert Daten ?**

- **JA: DSB bestellen mit Vorstandsbeschluss, DSB der Aufsichtsbehörde melden. DSB auf Homepage**

- **NEIN: Kein DSB. ABER: Verantwortlichkeit im Vorstand klar regeln !**

Punkt 5

Eigene Homepage checken !

- ✓ www.anbieterkennung.de
- ✓ §§ 5,6TMG beachten
- ✓ Haftungsrisiken evaluieren
- ✓ Verantwortlicher für Datenschutz auf die Homepage
- ✓ Klare Verantwortung des Webmasters regeln

Punkt 6

Verarbeitungsverzeichnis führen!

DS- GVO Ordner anlegen !

- ✓ Art. 30 DS- GVO beachten !
- ✓ „alle Verarbeitungsprozesse“

DS- GVO – Ordner anlegen mit Nachweis u.a. :

- Einwilligungen
- Beitragseinzügen (Lastschrift)
- Versendeten Newslettern
- E-mail- Einladungen zu Mitgliederversammlungen
- Werbe- e-mails

12.

Datenschutz bei Sammlungen personenbezogener Daten

(Outlook-Daten, Word- Excel Listen)

- „intern“ aus öffentlichen Quellen: machbar
- „interne Liste“ für internen Gebrauch, keine Herausgabe

13.

Verteilerliste eines Serienbriefes

- **Bleibt intern! Dokumentieren !**
- **Dokumentation zum Vorgang!**
- **BCC- e-mail statt CC- e-mail**

14.

Gefährdungsbeurteilung /IT-Riskmanagement/ IT- Compliance

TIPP:

https://www.amazon.de/Datenschutz-Compliance-nach-DS-GVO-Verantwortliche-Aufsichtsbeh%C3%B6rden/dp/3846207608/ref=sr_1_fkmr0_1?s=books&ie=UTF8&qid=1528114251&sr=1-1-fkmr0&keywords=IT+Compliance+Kranig

15.

Delegation Vollzug DS- GVO auf Mitarbeiter… Zeitumfang ?

- **unterschiedlich nach Art und Umfang der DV und Größe der Verwaltung**
- **Keine feste Richtschnur**

16.

Was ist eine Datenpanne?

- …Datenleck
- …Datenverlust
- …unbeabsichtigte Datenlöschung

Arbeitshilfe:

https://www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf

17.

Umgang mit Schreiben an Bürger
Löschungsanspruch ?

- **„gesetzliche Löschungsfristen“ aus sonderrechtlichen Bestimmungen gehen i.d.R. vor!**

18.

Whatsapp- Gruppen bspw. kommunale Jugendarbeit

- **Machbar für „Gruppenkommunikation“**
- **In der Regel nicht nutzbar für Einladungen etc.**
- **Trennung klar stellen: Private Kommunikation**

KEINE VERWENDUNG in kommunalen Verfahren !!!

WhatsApp sicher

- ✓ **Achtsam mit der Telefonnummer sein!**
- ✓ **Profilfoto klug auswählen!**
- ✓ **Sorgsamer Umgang mit privaten/intimen Bildern**
- ✓ **Onlinestatus und Lesebestätigung deaktivieren!**
- ✓ **Lästige/nervige Personen blockieren!**
- ✓ **Nutzung nur über geschützte WLAN-Netze!**
- ✓ **Regelmäßig updaten!**

Alternative zu WhatsApp:

Threema

(https://threema.ch/de)

Threema **ist so konzipiert, dass keine Datenspur entsteht. Gruppen und Kontaktlisten werden auf Ihrem Gerät verwaltet, nicht auf dem Server. Nachrichten werden sofort nach Zustellung gelöscht. So entstehen möglichst keine Metadaten. Beste Verschlüsselung**

19.

Kommunale Berichterstattung in Mitteilungsblättern etc.

- **Art. 85 DS- GVO „ nationale Sonderregelung fehlt bis dato(4.6.2018)**
- **Kollision Art. 6 DS- GVO zu §§ 22, 23 KUG !!! (ungeklärt!)**

Lösung über ErwG 152

„ Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, w e i t ausgelegt werden!

20.

Kontaktformulare auf Homepages

§ 13 Abs. 7 TMG: SSL Verbindung(Verschlüsselung)

https://www.datenschutz-ist-pflicht.de/kontaktformular/

21.

Hundebestandsaufnahme durch Private

Wohl „ noch“ nein

LINK:http://www.hundebestandsaufnahme.de/

22.

Tablets für Mandatsträger

Machbar mit klarer Regelung:

Richtlinien über Art und Umfang der Nutzung, bzw. Regelung in Hauptsatzung, Geschäftsordnung

LINK:

https://m.mainpost.de/regional/kitzingen/Digitaltechnik-Elektronik-und-Elektrotechnik-Papier-Sitzungen-Tablet-PC;art773,9411485

Hilfreiche Literatur:

Erste Hilfe zur Datenschutzgrundverordnung, Das Sofortmaßnahmen- Paket, ISBN 978-3-406-71662-1 € 5,50

Georg F. Schröder, Datenschutzrecht für die Praxis, Beck im dtV , ISBN 978-3-423-51202-2

€ 20,50

Dominik Lück „ Datenschutzreform – Auswirkungen auf die kommunale Praxis“ in: KommJur 3/2018, Seite 81 ff.

Vielen lieben

Dank für ihre Aufmerksamkeit und aktive Mitarbeit

Ihr

Malte Jörg Uffeln

www.maltejoerguffeln.de