Betriebliche Datenschutzpraxis 2019

Elf aktuelle Handlungs- und Prüffelder

Bearbeitungsstand: Fassung 1.0. 20.02.2019

Malte Jörg Uffeln

Mag.rer.publ.

Betrieblicher Datenschutzbeauftragter

www.maltejoerguffeln.de

I.

Wo kann ich mich informieren ?

www.maltejoerguffeln.de

Hilfreiche Links

www.datenschutz.hessen.de

www.lda.bayern.de

www.duesseldorfer-kreis.de

www.datenschutzzentrum.de

www.dsgvo-verstehen.bayern.de

Hilfreiche Literatur

Aichinger, Matthias / Dolezal, Andreas

„ Datenschutz in der Praxis“ ISBN 978-3-99070-898-9

Reimann, Grit

„Betrieblicher Datenschutz Schritt für Schritt – gemäß EU-Datenschutz- Grundverordnung“, 2. Auflage, Berlin, 2018. ISBN 978-3-410-27981-5

Laue, Philipp; Kremer, Sascha

„Das neue Datenschutzrecht in der betrieblichen Praxis“, 2. Auflage, baden- Baden 2019, ISBN 978-3-8487-4392-6

II.

Das Prinzip des Datenschutzes

Grundrecht auf informationelle Selbstbestimmung

(entwickelt aus Art. 2 GG)

Datenverarbeitung ist verboten,

es sei denn, Sie ist erlaubt !

(Verbot mit Erlaubnisvorbehalt)

Datenverarbeitung ist erlaubt

(Art. 6 I DS- GVO)...

a. Einwilligung

b. Vertrag oder vorvertragliche Maßnahmen

c.rechtlichen Verpflichtungen

d.lebenswichtigen Interessen

e. öffentlichem Interesse, Ausübung öffentlicher Gewalt

f. berechtigten Interessen eines Verantwortlichen oder Dritten

III.

Elf aktuelle Handlungs- und Prüffelder in der betrieblichen Datenschutzpraxis

1.

Der Fokus der Datenaufsichtsbehörden 2019

- **Datenerarbeitungsprozesse**
- **Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS- GVO)**
- **Technische- und Organisatorische Maßnahmen (TOM)**
- **Kundeninformation über Datenschutz (Art. 13 ff. DS- GVO)**
- **Auftragsverarbeitung (Art. 28 f. DS- GVO)**
- **Interner/externer Datenschutzbeauftragter ?**
- **Datenschutz- Folgenabschätzung (Art. 35 DS- GVO)**
- **Internet und Social- Media- Accounts**

2.
Informationspflichten
Rechte der Kunden

Information der Kunden über Rechte

nach Art. 13,14 DS- GVO (Erhebung), Art. 15 DS- GVO (Auskunft), Art. 16 DS- GVO(Berichtigung), Art. 18 DS- GVO

(Einschränkung der Bearbeitung), Art. 19 DS- GVO

(Berichtigung, Löschung, Einschränkung), Art. 20 DS- GVO (Datenübertragbarkeit), Art. 21 DS- GVO (Widerspruch), Art. 22 DS- GVO(automatisierte Entscheidung, Profiling)

Varianten:

1. Rundschreiben
2. Informationsschreiben auf Homepage
3. E-Mail-Newsletter an Kunden

3.

Datenschutz im Office, Kundenbereich

Mögliche Maßnahmen I

- ✓ **Verschlüsselte Übersendung von Kundendaten**
- ✓ **Klare Zugriffsberechtigungen für Mitarbeiter**
- ✓ **Wahrung der Diskretion im Kunden- und Wartebereich (Problem der „ spanischen Wände“, „hellhörigen Räume“)**
- ✓ **Abstandsschild am Tresen**
- ✓ **Sichere Verwahrung der Kundenakten, passwortgeschützer Computer, automatische Bildschirmsperre**
- ✓ **„Vertrauliche Gespräche“ stets in geschlossenen Räumen**

Mögliche Maßnahmen II

- ✓ **Telefonate: Identitätsfeststellung und – sicherung: ggf. gezielte Rückfragen und Rückruf**
- ✓ **E-Mail: Sender klar evaluieren und ggf. weitere Feststellungen zur Identität treffen**
- ✓ **Löschungskonzept für Daten erarbeiten**
- ✓ **„Weisungen“ im Umgang mit Datenpannen und evtl. Datenschutzverstößen**
- ✓ **Verpflichtung der Mitarbeiter auf das Datengeheimnis und die Verschwiegenheitspflicht**

4.

Bestellung eines Datenschutzbeauftragten (intern/extern) ?

(§ 38 I BDSG, Art. 37 DS- GVO)

„… in der Regel mindestens 10 Personen, die sich ständig mit der automatisierten Datenverarbeitung befassen...“

- **„ständig ?“**

(… weite Auslegung nach Meinungen in der Kommentarliteratur!)

5.
Verarbeitungsverzeichnis
(Art. 30 DS – GVO)

.Prozessorientierte Übersicht der Verarbeitungsvorgänge

.Schriftlich oder elektronisch

.**WER** ? verarbeitet **WANN**? und in WELCHEM **KONTEXT**? **WIE**? WELCHE DATEN zu WELCHEN ZWECKEN ?

Muster unter:

https://www.bitkom.org/sites/default/files/file/import/180529-LF-Verarbeitungsverzeichnis-online.pdf

https://www.datenschutz-bayern.de/datenschutzreform2018/verarbeitungsverzeichnis.pdf

https://www.lfd.niedersachsen.de/themen/wirtschaft/verfahrensverzeicnis_und_verfahrensregister_nach_bdsg/verfahrensregister-und-verfahrensbeschreibung-fuer-den-nicht-oeffentlichen-bereich-56247.html

6.

Kundenverwaltung in der Cloud

Auftragsdatenverarbeitung

- **„Dritter“ – externer - Dienstleister ist in der Regel Auftragsverarbeiter (Artt. 28,29 DS- GVO)**

- **Auftragsdatenverarbeitungsvertrag notwendig**
  - **Sorgfältige Auswahl**
  - **Sach- und fachkompetent**
  - **„Gewähr“ für Einhaltung der TOM**
- **Einhaltung der DS- GVO, Wahrung der Betroffenenrechte**

Vertrag über Auftragsdatenverarbeitung

„Mindestinhalte I“

- ✓ Gegenstand, Dauer der Verarbeitung
- ✓ Art. Zweck, Umfang
- ✓ Rechte und Pflichten des Auftragnehmers und des Auftraggebers, Klärung der Weisungsbefugnisse
- ✓ Verpflichtung zur Vertraulichkeit, Verschwiegenheitsverpflichtung
- ✓ Aufstellung der TOM
- ✓ Art und Umfang wechselseitiger „ informativer“ Unterstützung

Vertrag über Auftragsdatenverarbeitung „Mindestinhalte II“

- ✓ Verfahren bei Vertragsbeendigung. Rückgabe und Löschung von Daten
- ✓ Umgang mit Konflikten: ;Mediationsklausel
- ✓ Inspektionen durch Dritte, externe „Über“prüfungen

7.

TOM

Technisch – Organisatorische Maßnahmen

7.1.

Datensicherheitsmaßnahmen im Überblick

- **Zutrittskontrolle**
- **Datenträgerkontrolle**
- **Speicherkontrolle**
- **Benutzerkontrolle**
- **Zugriffskontrolle**
- **Übertragungskontrolle**
- **Eingabekontrolle**
- **Transportkontrolle**
- **Wiederherstellung**
- **Datenintegrität und Zuverlässigkeit**

7.2.

TOM konkret….

- Authentifizierung
- Passwortsicherheit
- Verschlüsselung mobiler Geräte
- Netzwerksicherheit (Firewall)
- Anti-Viren Software
- Verschwiegenheitspflichterklärung
- Schulung, Information, Aus- und Fortbildung
- Keine Doppelverwendung von User- Accounts
- Sichere Datenentsorgung
- Physische Zugangskontrolle
- regelmäßige Datensicherung
- Feuerlöscher

8.

Datenschutz-Folgenabschätzung (Art. 35 DS- GVO)

Vorgehensweise

Erfassen der Risiken

1. Liegt ein „hohes Risiko“ vor ?
2. Welche Daten werden verarbeitet ?
3. Ist die Datenverarbeitung rechtmäßig (Grundlage)?
4. Welche die Grundsätze der DS- GVO eingehalten ?
5. Welches Risiko besteht bzgl. Vertraulichkeit, Verfügbarkeit, Integrität ?
6. Wie hoch sind die Risiken ?
7. Welche Maßnahmen sind getroffen worden ?

Vorgehensweise

Datenschutzfolgenabschätzung konkret

A. Systematische Beschreibung der geplanten Bearbeitungsvorgänge (Zweck, Interessen)

B. Bewertung der Verarbeitungsvorgänge (Notwendigkeit, Zweckmäßigkeit, Verhältnismäßigkeit)

C. Bewertung der Risiken für Persönlichkeitsrechte

D. Beschreibung der Abhilfemaßnahmen (Garantien, Sicherheitsvorkehrungen, Verfahren)

9.

Internet- / Facebook- Seite

Anbieterkennung (§§ 5, 6 TMG)

Mindestinhalte

- ***Name, Anschrift der Firma , gesetzliche Vertreter***
- ***E-Mail-Adresse der Kontaktperson, des Vorstandes***
- ***VR- Nummer (bei e.V.)***
- ***Umsatzsteueridentifikationsnummer (§ 27 a UStG)***

<u>Weitere Begrifflichkeiten in der Praxis:</u>

„Impressum“, „Webimpressum“, „Anbieterkennzeichnung“ „Kontakt“.

Klare Datenschutzerklärung auf der Internetseite!

- ✓ Art und Umfang der Datenerhebung
- ✓ Datenspeicherung nur bei aktiver Übermittlung
- ✓ Verwendung der Daten (bspw. für Anfragen, Informationsschreiben etc.)
- ✓ Verwendung von Kontaktdaten ausschließlich zur Korrespondenz
- ✓ E- Mail- Adressen für e-mail-Newsletter

Mögliche Haftungsrisiken

- ✓ Domainname
- ✓ Inhaber der Domain
- ✓ Anbieterkennung
- ✓ Bilder (gemeinfrei, lizenzfrei, lizenzpflichtig)
- ✓ Texte und Zitate Dritter
- ✓ Urheberrechte Dritter
- ✓ Datenschutzbestimmungen
- ✓ Social-Media-embedding, facebook, youtube

(vgl. dazu:http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2015&Sort=3&nr=71618&pos=0&anz=115

Muster Datenschutzerklärung Internet

https://datenschutz-generator.de/

https://www.stuttgart.ihk24.de/Fuer-Unternehmen/recht_und_steuern/Datenschutzrecht/ihk-merkblaetter-dsgvo/datenschutz-fuer-kleine-unternehmen/3935426

10.

Videoüberwachung

(Art, 6 DS- GVO, § 4 BDSG nF)

VideoüberwachungsverbesserungsG

- **„Jedes berechtigte Interesse“ (dokumentieren!)**
- **Differenzierung „öffentliche“ vs. „nicht-öffentliche“ Stellen**
- **Stufensystem nach § 4 BDSG n.F.**

- Beobachtung

- **Speicherung oder Verwendung**
- **Kennzeichnung, Information, Löschung**

- **Verhältnismäßigkeitsprüfung bzgl. „jeder einzelnen Videokamera!“**

11.

Mitarbeiterdatenschutz

„Gläserne Belegschaften ???“

- **Mitarbeiteranschreiben (Art. 13 DS-GVO)über Art und Umfang der Erhebung personenbezogener Daten im Beschäftigungsverhältnis**

- **Betriebliche Datenverarbeitungsrichtlinie in der alle Punkte zu klären sind(bspw. Passwortschutz, e-mail-Nutzung, mobile Endgeräte etc.)**

Vielen Dank für Ihre Aufmerksamkeit und Ihre aktive Mitarbeit

Ihr

Malte Jörg Uffeln

www.maltejoerguffeln.de