Datenschutz und Datensicherheit

Akutsprechstunde zur praktischen Umsetzung der EU-DSGVO

K.-H. Erkens

5. Juli 2018

arbor consulting

Inhalt

Handlungsbedarf, Aktualität

Grundlagen und Einordnung

Begriffe nach Art. 4 DSGVO

Guter Datenschutz schafft Vertrauen

Handlungsfelder und Vorgehen

Praktische Umsetzung

ISO 27001, Unternehmenspflichten

Datenschutzbeauftragter

Fragenkomplexe

Mehr Datenschutz

VON REINHARD KOWALEWSKY

Die Vielzahl neuer Datenskandale wie bei SchülerVZ, Telekom und dem Finanzdienstleister AWD macht klar: Der Missbrauch gespeicherter Informationen entwickelt sich zur Plage des digitalen Jahrhunderts. Datenspeicherung und -übertragung kosten praktisch nichts mehr, umso ernsthafter müssen sich Nutzer, Firmen und Staat mit der Gefahr auseinandersetzen.

Zuerst sind die Kunden gefragt: Wer sensible Informationen online preisgibt, ist naiv. Das „Netz" hat dank gigantischer Server ein langes Gedächtnis. Also sollten Schulen und Eltern mit Teenagern üben, wie sie sich nur selektiv offenbaren und ihre Seiten bei Facebook oder SchülerVZ nur Freunden öffnen.

Aber auch Unternehmen wie die Telekom müssen Datenschutz ernster nehmen. Sonst riskieren sie ihr Geschäft. Es ist ein Zeichen der Hilflosigkeit, wenn die Telekom nun mit Wettbewerbern die Vertriebsprovisionen kürzen will, damit es sich für Call-Center nicht mehr so lohnt, illegal kopierte Kundenlisten durchzutelefonieren. Man muss eben sicherstellen, dass die Daten sicher sind. Das ist Chefaufgabe.

Und der Staat? Datenmissbrauch von Unternehmen muss konsequenter bestraft werden. Und wer Daten schlampig schützt, sollte dafür haften.

BERICHT: FESTNAHME ... TITELSEITE

DIE ZEIT N° 26

BIG DATA

WIRTSCH

Achtung, Missbrauch!

Facebook, Google und andere Konzerne sind zu mächtig geworden. Es wird Zeit, unsere Daten zu verteidigen.

Die EU-Datenschutz-Grundverordnung (EU-DSGVO) ist am 25.05.2018 in Kraft getreten, knapp zwei Jahre nach ihrer Verabschiedung – eine lange Zeit für ein „modernes" Datenschutzrecht.

Schutz und Sicherheit von Daten und Systemen

Grundrecht auf informationelle Selbstbestimmung

Gesetze, Vorgaben, Standards

Notwendigkeit
Maßnahmen gegen
Verlust, Zerstörung,
Missbrauch durch Unbefugte
Nachvollziehbarkeit
Erfassung von Prozessen/
Beteiligte

Informationssicherheit
jeder Art und Herkunft

Zulässigkeit
Verbot mit Erlaubnisvorbehalt
Anonymität
Löschen von Spuren
Datenvermeidung

Bedrohungen durch
Verletzung von
Persönlichkeitsrechten

Schnittmengen: Vertraulichkeit, Integrität, Verfügbarkeit

Datenschutz ist gesetzlich tief verankert:

- Charta der Grundrechte der Europäischen Union (GRC)
- Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK)
- Grundgesetz für die Bundesrepublik Deutschland (GG)
- Das BDSG-neu trat am 25. Mai 2018 in Kraft und ersetzt in Verbindung mit der EU-Datenschutz-Grundverordnung (DSGVO) das bisherige BDSG.

Nicht erlaubt ist grundsätzlich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, erlaubt ist diese jedoch unter bestimmten Voraussetzungen (Prinzip: Verbot mit Erlaubnisvorbehalt).

Datenerhebung ist somit zulässig, wenn sie ...

durch die Datenschutzregeln selbst ...
Beispiel: öffentlich zugängliche Daten

oder durch eine andere Rechtsvorschrift ...
Beispiel: Steuern, Abgaben

oder durch die Einwilligung des Betroffenen ...
Beispiel: Einverständniserklärung zur Datennutzung

... erlaubt wird.

- **Personenbezogene Daten**

  Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

- **Verarbeitung**

  Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang

- **Verantwortlicher**

  Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle mit „Organisationsgewalt“

- **Auftragsdatenverarbeiter**

  Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet

Der Schutz natürlicher Personen bei der **Verarbeitung personenbezogener Daten** ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Welche Unternehmen sind betroffen:

- **Europäische Unternehmen, die personenbezogene Daten verarbeiten, und außereuropäische Unternehmen, die ihre Waren und Dienstleistungen innerhalb der EU vertreiben**
- **Ob sie in einem EU-Staat ansässig sind oder nicht – wenn ein Unternehmen personenbezogene Daten von EU-Bürgern verarbeitet, speichert oder übermittelt, gilt nach den Regeln die Verpflichtung, die Datenschutz-Grundverordnung einzuhalten.**

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person.

Beispiele:

Vermögens-verhältnisse | Name | Adresse | Kreditkarten-nummer | Telefon-nummer

Wohn-verhältnisse | Geburtsjahr | Gehalt

Weitaus strengere Regeln gibt es für den Umgang mit sogenannten besonderen Arten personenbezogener Daten, da diese besonders schützenswert sind.

Politische Meinung | Gewerkschafts-zugehörigkeit | Rassische und ethnische Herkunft | Religiöse oder philosophische Überzeugung | Sexual-leben

Gesundheit

- **Umsetzung der rechtlichen Anforderungen**
- **Verantwortlichkeit des Managements über die Gestaltung und die Abwicklung der Geschäftsprozesse**
- **Technische und organisatorische Maßnahmen**
- **Herausforderungen durch neue Technologien und Systeme als Teil der Digitalisierung**

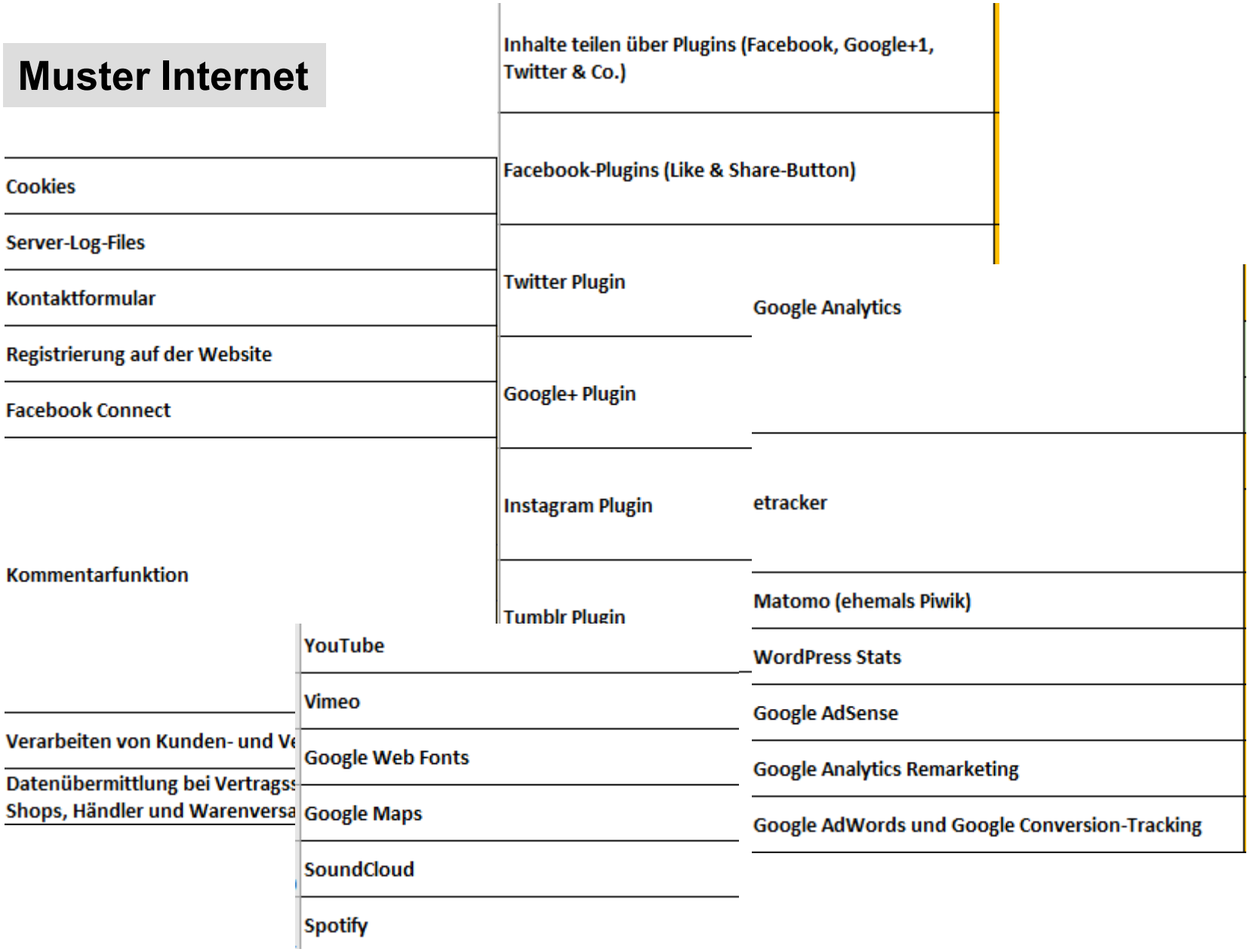
Checkliste I

- Verträge mit Dienstleistern, Lieferanten/Dokumente dazu (Auftragsdatenverarbeitung, Übersicht)
- Geschäftsprozesse/Organisation als Basis für das Verarbeitungsverzeichnis
- Internetnutzung/Homepage/Datenschutzerklärung/Nutzung von Cookies etc./Messenger
- IT und TK-Technik inkl. techn. und organisatorischer Maßnahmen (Inventar, Struktur, Diagramm)

Checkliste II

- Rechte der Betroffenen (Mailverkehr, Löschung etc.);
  Recht auf Information (Artikel 13 und 14, DSGVO)
- Mitarbeiter, Beschäftigtendaten
- Informationssammlung zum Datenschutz
- Handlung bei Vorkommnissen (Pannen) und deren Dokumentation
- Regelungen Datenschutzbeauftragter (Bestellung, Meldung Kontaktdaten an Aufsichtsbehörde)

Muster Internet



Muster DASU-Erklärung

Datenschutz

Der Betreiber dieser Seiten nimmt den Schutz Ihrer persönlichen Daten sehr ernst. Wir behandeln Ihre personenbezogenen Daten vertraulich und entsprechend der gesetzlichen Datenschutzvorschriften sowie dieser Datenschutzerklärung.

Die Nutzung unserer Webseite ist in der Regel ohne Angabe personenbezogener Daten möglich. Soweit auf unseren Seiten personenbezogene Daten (beispielsweise Name, Anschrift oder E-Mail-Adressen) erhoben werden, erfolgt dies stets auf freiwilliger Basis zum Zwecke der Bearbeitung Ihrer Anfrage. Die Verarbeitung von personenbezogenen Daten ist notwendig für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen, die auf Ihre Anfrage hin erfolgen (Artikel 6 Abs.1b DSGVO).

Sie werden nur solange gespeichert, wie es die Geschäftsbeziehung mit Ihnen erfordert. Eine automatische Erhebung Ihrer Daten findet nicht statt.

Mit Ihrer Zustimmung erhobene Daten werden ohne Ihre ausdrückliche Zustimmung nicht an Dritte weitergegeben.

Wir weisen darauf hin, dass die Datenübertragung im Internet (z.B. bei der Kommunikation per E-Mail) Sicherheitslücken aufweisen kann. Ein lückenloser Schutz der Daten vor dem Zugriff durch Dritte ist nicht möglich. Daten, die durch die Nutzung unserer Mailseite entstehen (bspw. Server-Logfiles), werden nach Abschluss des Zugriffs gelöscht. Rückschlüsse auf personenbezogene Daten sind nicht möglich.

Muster TOM

Musterinhaltsverzeichnis – Datensicherheitskonzept -

1 IST Zustand / Systemlandschaft

1.1 Räume, Standorte

1.2 Systemlandschaft / Diagramm Systemstruktur

1.3 IT-Anlagen Beschreibung

1.4 Arbeitsplatz-PCs

1.5 Detailbeschreibung Server und PCs

1.5.1 TK-Anlage

1.5.2 Netzwerkstruktur

2. Sicherheit / Gefährdungspotentiale

2.1 Einbruch/Vandalismus

2.2 Virtuell über das Netzwerk

2.3 Elementarschäden

3. Maßnahmen zu Datensicherheit

3.1 Aufbau der technischen Datensicher

3.1.1 Tägliche Sicherung auf Dateiebene

3.1.2 Tägliche Sicherung der virtuellen Computer

3.1.3 Tägliche Sicherung der/s gesamten Server/s

3.2 Aufbau des Virenschutzes

3.2.1 Server

3.2.2 Sonstige Systeme

3.2.3 Arbeitsplatzsysteme

3.2.4 Externe Arbeitsplätze

4 Updateinstallationen (Vorgehen und Nutzen)

4.1 Server

4.2 Arbeitsplatzsysteme

4.3 Virenscanner Updates

4.4 Hardwareupdates

4.4.1 Server

4.4.2 Arbeitsplatzsysteme

5 Schulungsmaßnahmen der Mitarbeiter zum Umgang mit Systemt

5.1 Schutzmaßnahmen mit dem Umgang der Hardware

5.2 Schutzmaßnahmen im Umgang mit der Software

5.2.1 Handhabung der Passwortänderung alle X Monate

5.2.2 Internet (Erkennung von E-Mails (Erkennung von Spam/Viren/Trojaner, etc.)

5.2.3 Anwendungssoftware/Office-Dateien

5.2.4 Notfallplan

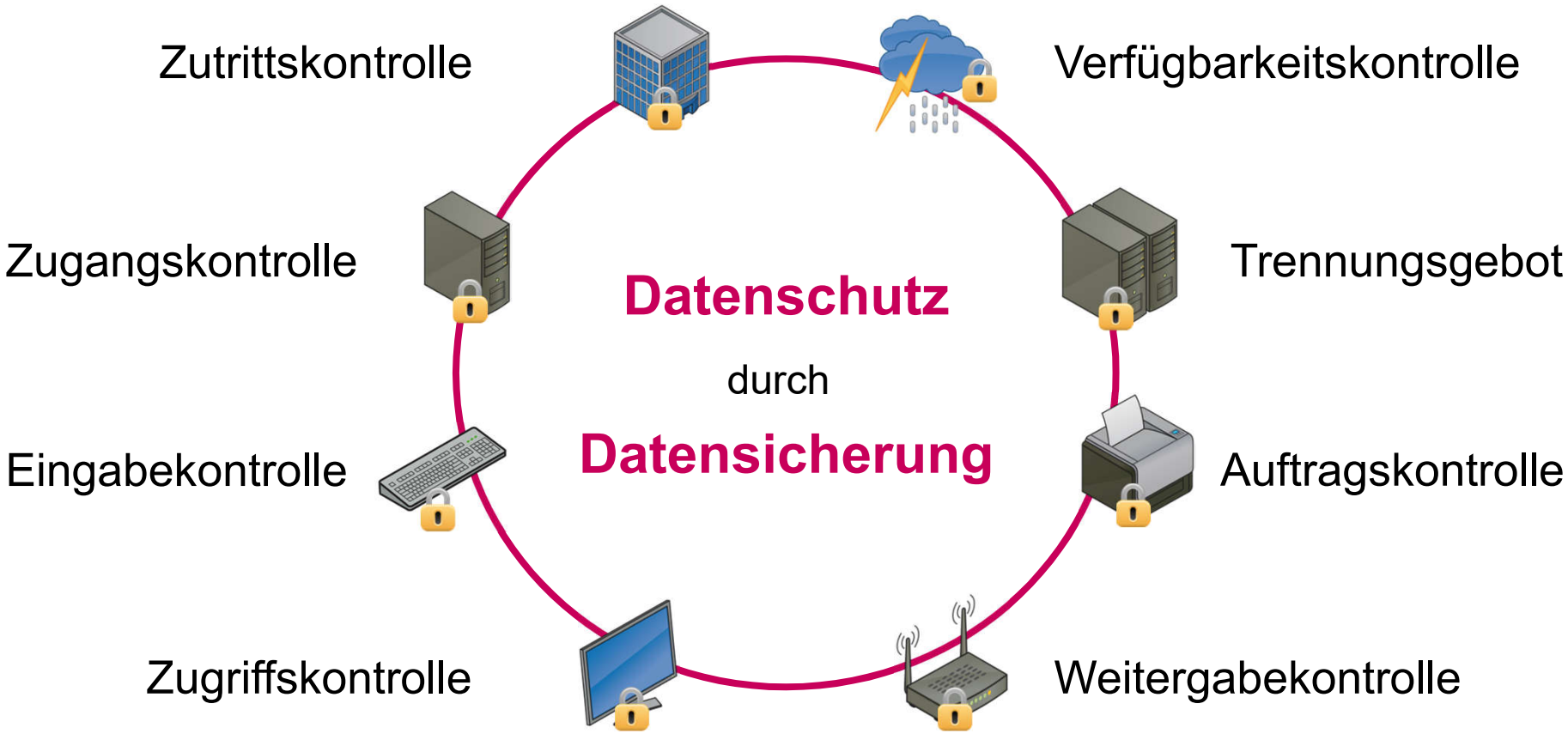
6 Berechtigungen

6.1 MitarbeiterInnen

6.2 Administrator

Management der Informationssicherheit
ISMS
Compliance
Sicherheitsregelwerk
Management des kontinuierlichen Geschäftsbetriebs
Sicherheitsorganisation
non-IT
Informations-sicherheit
Management von Vorfällen
Management der Unternehmenswerte (Assets)
IT-Sicherheit
Beschaffung, Entwicklung und Wartung
Personelle Sicherheit
Physische Sicherheit
Zugriffkontrolle
Kommunikation und Betrieb
Die Informationssicherheit – gemäß ISO 27001 - umfasst die Geschäftsprozesse und damit den Geschäftsbetrieb.

Kontrollmaßnahmen bei der Verarbeitung



Der Datenschutzbeauftragte ...

- wirkt auf die Einhaltung des Datenschutzrechts hin
- berät Geschäftsführung und Mitarbeiter bei Fragen, die den Datenschutz betreffen
- unterliegt der Verschwiegenheitspflicht
- hat das Recht, sich in Zweifelsfällen an die Aufsichtsbehörde zu wenden
- berät bei der Einführung neuer Verfahren

- Angst, die dem Bürger eingeflößt wird, und Verallgemeinerungen helfen nicht weiter.
- Totale Sicherheit gibt es nicht. Einen rechtswidrigen Umgang mit Daten kann man nicht ausschließen.
- Die Ansichten von informationeller Freiheit sind durchaus verschieden, was freiwillig eingestellte Informationen in sozialen Netzwerken zeigen.
- Es gibt viele Hilfen zu den Themen Datenschutz und Datensicherheit, die man nutzen kann (DIN, ISO, IT-Grundschutz).
- Das Bewusstsein der Menschen für den Datenschutz wurde geschärft, Verbesserungen wurden durch rechtliche Regelungen erreicht.

Vielen Dank!

Haben Sie Fragen?

+49 (02153 951240) / info@arbor-consulting.de

arbor consulting