DR. KOCH

www.ra-fmk.de

Datenschutz und Datensicherheit – Pflichten und Nutzen

2. Auflage 2018 - Stand 07.12.2020 -

DR. KOCH

Agenda

1. **Einleitung**
2. **Corona und Datenschutz**
3. **Key-Facts zur EU-DSGVO**
4. **Grundlagen des Datenschutzrechts**
5. **Auftrags-(daten-)verarbeitung**
6. **Datenschutzbeauftragter usw.**
7. **Vorgaben für IT gestützte Prozesse**
8. **Umsetzung EU-DSGVO – ToDo‘s**
9. **Do‘s und Dont‘s**

Einleitung

1

Meine Erwartung an die Veranstaltung

- ☐ Ich werde ab Freitag DSB
- ☐ Bestätigung das DV unproblematisch
- ☐ Weiß nicht

DR. KOCH

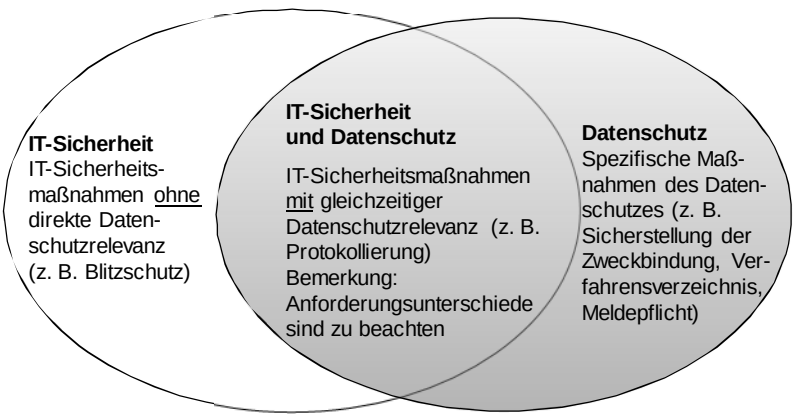
Betrieblicher Datenschutz

Einführung

Worum geht es?

DR. KOCH

Datenschutz vs. IT-Sicherheit



DR. KOCH

Aufgabe des Datenschutzes

Fall: **Die Pizzabestellung**

Hallo! Ist da Roccos Pizza-Sevice? Nein, hier ist Googles Pizza-Service.
Sorry, dann hab ich wohl die falsche Nummer...? Nein, Google hat die Nummer gekauft.
OK, dann möchte ich gerne.... Wollen Sie das Übliche?
Das Übliche? Wieso kennen Sie das?
Gemäß unseren Aufzeichnungen der letzten 12 Anrufe haben Sie Pizza mit Käse, Salami und Schinken bestellt.
OK, genau das will ich auch jetzt!
Dürfte ich vorschlagen, dass sie dieses Mal eine Pizza mit Ricotta, Rucola und getrockneten Tomaten bestellen?
Nein, ich hasse Gemüse!
Aber Ihr Cholesterin-Wert ist nicht gut.
Wie können Sie das wissen?
*Aus Ihrem **Gesundheits-Profil. Wir haben die Resultate Ihrer Blutwerte der letzten 7 Jahre.***
Okay, aber ich will nicht diese Pizza. Ich habe meine Medizin schon genommen.
Sie haben Ihre Medizin nicht regelmäßig eingenommen. Vor 4 Monaten haben Sie online eine Schachtel mit 30 Tabletten in der Versand-Apotheke 'Sunstore' gekauft. Die müsste längst leer sein.
Ich habe noch in einer anderen Apotheke eingekauft.
Das ist aber nicht auf Ihrer Kreditkarte abgebucht.
Ich habe bar bezahlt.
Gemäß Ihrem Bankkonto haben Sie dafür nicht genügend Bargeld bezogen.
Ich habe noch andere Geldquellen.
Das ist aus Ihrer letzten Steuererklärung nicht ersichtlich, also handelt es sich um nicht deklariertes Einkommen.
ZUM TEUFEL MIT IHNEN! Genug! Ich habe die Nase voll von Google, Facebook, Twitter, WhatsApp und Konsorten.
Ich werde auf eine Insel gehen ohne Internet, ohne Telefon und wo mich keiner ausspionieren kann.

Ich verstehe Sie, aber vorher müssen Sie Ihren Pass erneuern. Er ist vor 5 Jahren abgelaufen...

DR. KOCH

Aufgabe des Datenschutzes

Fall: *„Ein arbeitsloser Berliner und seine lettische Frau sind ihrem im Wachkoma und von einem ambulanten Pflegedienst betreuten Kind unterhaltsverpflichtet. Er stellte den in Russland lebenden Familienangehörigen und dortigen öffentlichen Stellen die Rechnungen für den ambulanten Pflegedienst zur Verfügung gestellt, um dort für Verständnis für die Verringerung Unterstützung zu werben. Dies Vorgehen erschien dem Pflegedienst bedenklich. - Dies Bedenken sind jedoch unbegründet, weil der Betroffene selbst Durchschriften seiner privaten Schreiben jedermann im In- und Ausland zur Verfügung stellen. Anders sähe es nur für den Pflegedienst selbst aus. Der Pflegedienst arbeitet im Anwendungsbereich des SGB und darf Angaben über persönliche und sachliche Verhältnisse eines Betroffenen nur dann offenbaren, wenn entweder die Voraussetzungen der §§ 67-78 SGB X erfüllt sind oder Betroffene eingewilligt hat. Hingegen wird der Betroffene einer Datenverarbeitung durch das SGB gerade nicht gebunden.“*
Dieser Fall ist dem Datenschutzbericht 1993 des Berliner Datenschutzbeauftragten entnommen und angepasst, Abgeordnetenhaus Berlin, Drucks. 12/4372.

DR. KOCH

Ziele der EU-DSGVO

- „Schutz **natürlicher Personen** bei der Verarbeitung personenbezogener Daten und zum **freien Verkehr** solcher Daten.“ (Art.1 Abs.1)
  - „...schützt die **Grundrechte und Grundfreiheiten** natürlicher Personen und insbesondere deren *Recht auf Schutz personenbezogener Daten“* (Art.1 Abs.2)
  - ...ohne den **freien Verkehr** personenbezogener Daten in der Union einzuschränken. (vgl. Art.1 Abs.3)
  - § 1 Abs.1 BDSG a. F.: „...Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem *Persönlichkeitsrecht* beeinträchtigt wird.“

DR. KOCH

Ich kenne das Datenschutzrecht

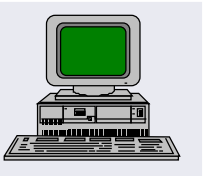
☐ **Ja**

☐ **Nein**

☐ **Weiß nicht**

DR. KOCH
Rechtsanwalt

Datenverarbeitung als Gefährdungspotential



- **Pro**
  - » **Rationeller Aufgabenvollzug**
    - **Vielzahl benötigter Daten**
    - **Universelle Bedeutung**
    - **Transparenz, Aktualität**
    - **Verarbeitungsintervalle**
    - **Übermittelbarkeit**

- **Contra**
  - **Mißbrauchspotentiale**
    - » **Sensibilität, Privatsphäre**
    - » **Machtfaktor**
    - » **Abhängigkeit**
    - » **Abstraktion der Sachverhalte**
    - » **Konformitätsdruck**
    - » **Übermittelbarkeit, Verknüpfbarkeit**

DR. KOCH
Rechtsanwalt

Gesetzliche Regelungen bis zum 24.05.2018

Gesetze

BDSG (Bundesdatenschutzgesetz)
ABMG (Autobahnmautgesetz)
AentG (Arbeitnehmer-Entsendegesetz)
AO (Abgabeordnung)
AufenthG (Aufenthaltsgesetz)
AZR-Gesetz (Ausländerzentralregistergesetz)
BND-Gesetz (Bundesnachrichtendienstgesetz)
BstatG (Bundesstatistikgesetz)
BArchG (Bundesarchivgesetz)
BKAG (Bundeskriminalamtgesetz)
BPolG (Bundespolizeigesetz)
BVerfSchG (Bundesverfassungsschutzgesetz)
BZRG (Bundeszentralregistergesetz)
ESt G (Einkommensteuergesetz)
KBAG (Gesetz Errichtung Kraftfahrt-Bundesamt)
PersAuswG (Gesetz über Personalausweise)
KapMuG (Kapitalanleger-Musterverfahrensgesetz)
KWG (Kreditwesengesetz)
MRRG (Melderechtsrahmengesetz)
PaßG (Paßgesetz)
PDSV (Postdienste-Datenschutzverordnung)
PostG (Postgesetz)
PStG (Personenstandsgesetz)
SchwarzArbG (Schwarzarbeitsbekämpfungsgesetz)
SGBI (Sozialgesetzbuch I)
SGBII (Sozialgesetzbuch II)
SGBIV (Sozialgesetzbuch IV)
SGBV (Sozialgesetzbuch V)
SGBX (Sozialgesetzbuch X)
SigG (Signaturgesetz)
StGB (Strafgesetzbuch)
StPO (Strafprozessordnung)
StUG (Stasi-Unterlagengesetz)
TKG (Telekommunikationsgesetz)
TKÜV (Telekommunikations-Überwachungsverordnung)
TMG (Telemediengesetz)
ZensVorbG (Zensusvorbereitungsgesetz)

DR. KOCH

Gesetzliche Regelungen ab 25.05.2018

EU

EU-Datenschutzgrund-verordnung EU-679/2016

- Enthält u. A. Regelungsaufträge für die Mitgliedstaaten.

EU RL 680/2016

- Verpflichtung der Mitgliedsstaaten bis zum 06. Mai 2018 die Richtlinie und die Verordnung in nationales Recht umzusetzen.

Gesetze

Datenschutz Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) v. 30.06.2017 bestehend aus:

- Bundesdatenschutzgesetz (BDSG n. F. ab 25.05.2018)
- Änderung des Bundesverfassungsschutzgesetzes
- Änderungen des MAD-Gesetzes, des BND-Gesetzes, des SicherheitsüberprüfungsG
- Verschiedene Folgeänderungen

DR. KOCH

Entwicklung des Datenschutzes in Deutschland

- 1970: Weltweit erstes Datenschutzgesetz in Hessen
  → „Datenschutz“ = „Datensicherheit“
- 1982: Volkszählungsgesetz
- 1983: Urteil zur Volkszählung
  → **Grundrecht auf informationelle Selbstbestimmung**
  → Beschränktes Eingriffsrecht des Staates
  → „Datenschutz“ = „Schutz der Person“
- 1990: **Bundesdatenschutzgesetz**
- 1998: Großer Lauschangriff
  → **Kernbereich der privaten Lebensgestaltung**
- 1999: Fernmeldeüberwachung
- 2001: Rasterfahndung
- 2008: Online-Durchsuchung/Bundestrojaner
  → **„Computer-Grundrecht“**
- 2008: Massenabgleich von KFZ-Kennzeichen
- **2009:** **Drei Novellierungen des BDSG** – Ende Übergangsregelung 31.08.2012

- **14.04.2016** Verabschiedung EU-Datenschutzgrundverordnung, Veröffentlichung im Amtsblatt am 04.05.2016 Inkrafttreten am **25.05.2018**.

- **30.06.2017:** Verkündung Anpassungs- und Durchführungsgesetz zur EUDSVGO.

DR. KOCH

Zeitliche Auswirkungen der Gesetzesänderung

Einigung im Trilog 17.12./18.12.2015 — 04.05.2016 Verkündung — 25.05.2018 Geltung – Ende Umsetzungsfrist

- **BDSG gilt weiter**
- **Beginn der Umsetzungsfrist**

(...Verarbeitungen, die zum Zeitpunkt des Inkrafttretens dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. ... (EG 171))

- Ermächtigung der Kommission zum Erlass **delegierter Rechtsakte** (Art. 92 Abs. 2) ab 24. Mai 2016

- **BDSG a. F. ist nicht mehr anwendbar BDSG n. F. gilt**
- **Aufhebung** der EU-DS-Rili (RL 95/46/EG) (Art 94)
- **Verarbeitungen** müssen im Einklang mit der GVO sein
- **Ablauf** diverser Melde-/ Erklärungspflichten der Mitgliedsstaaten bezüglich nationaler Regelungen

DR. KOCH

Das Recht am eigenen Bild

Grundsätzlich kann **jede Person** eigene Aufnahmen im Internet freigeben. Davon gibt es allerdings beachtliche Einschränkungen

- Stellt eine Aufnahme eine oder mehrere Personen dar, kann die Veröffentlichung durch Persönlichkeitsrechte der Abgebildeten eingeschränkt werden. Jeder Mensch darf grundsätzlich selbst darüber bestimmen, ob überhaupt und in welchem Kontext Bilder von ihm veröffentlicht werden – ohne Erlaubnis ist also ein Hochladen verboten. Ausnahmen:
  - Öffentliche Versammlungen oder Veranstaltungen
  - Absolute Person der Zeitgeschichte

Die Veröffentlichung von Fotos von urheberrechtlich geschützten **Gebäuden** (Werke der Architektur) in Deutschland (sowie in Österreich, der Schweiz und weiteren Ländern) ist generell durch die Panoramafreiheit gedeckt, jedoch nur:

- Lediglich die äußere Ansicht dargestellt wird (Urheberrecht des Architekten);
- Der Aufnahmestandort allgemein und ohne Hilfsmittel zugänglich ist.

Problem: Veröffentlichung von **Werkfotografien**, sofern sich das Werk in einem geschlossenen Raum und das Fotografieren untersagt ist.

DR. KOCH

Einführung einer Videoüberwachung

Der Eigentümer des Gebäudes, in dem er neben verschiedenen Einkaufs- und Gastronomiebetrieben und Sie eine Senioreneinrichtung betreiben, möchte eine Videoüberwachung einführen, da es vermehrt zu Einbrüchen gekommen ist und Junkies ihr Spritzbesteck bei den Müllcontainern ablegen.
Zweckbestimmung der geplanten Videoüberwachung ist:

- die abschreckende Wirkung auf jene Gäste und Besucher des Einkaufscenters, die Straftaten oder Ordnungswidrigkeiten planen,
- die Identifizierung von Personen im Anschluss an eine Straftat und / oder Ordnungswidrigkeit in Bezug auf geschützte Rechtsgüter des Eigentümers wie z.B.: Diebstahl, Sachbeschädigung, Vandalismus, Betäubungsmitteldelikten, Hausfriedensbruch oder Verletzung der Hausordnung, sowie deren Beweisführung,
- zum Schutze eigener Mitarbeiter, oder jener Mitarbeiter, welche für Mieter bzw. Unternehmen der geschäftlichen Räumlichkeiten des Einkaufscenters tätig sind,
- zum Schutze von Passanten oder Besuchern der Passage sowie der dort ansässigen Unternehmen

DR. KOCH

Einführung einer Videoüberwachung

- Nach § 6b Abs. 1 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. § 6b BDSG erfasst sowohl reine Kamera-Monitor Systeme, als auch die Speicherung von Aufnahmen.
- Der Anwendungsbereich des § 6b BDSG dürfte für die Einrichtung einer Videoüberwachung im Einkaufscenter grundsätzlich eröffnet sein. Das Einkaufscenter ist ein privater, allerdings öffentlich zugänglicher Raum im Sinne dieser Vorschrift.
- Die nach § 6 b Abs. 1 BDSG gebotene Güterabwägung kann nur unter Würdigung aller Umstände des Einzelfalles und durch Berücksichtigung aller rechtlich, insbesondere auch verfassungsrechtlich geschützten Positionen der Beteiligten durchgeführt werden (so schon vor Einführung des § 6b BDSG: *BGH*, NJW 1995, 1957). Vorliegend steht für den betroffenen Nutzer des Einkaufscenters sein Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V mit Art. 1 Abs. 1 GG) im Vordergrund, während der Gebäudeeigentümer sich auf ihr Eigentumsrecht bzw. ihr Recht am eingerichteten und ausgeübten Gewerbebetrieb aus den Art. 12, 14 GG berufen kann.
- Ob die schutzwürdigen Interessen des Betroffenen bei einer Videoüberwachung im öffentlich zugänglichen Raum überwiegen, ist situations- und kontextbezogen zu untersuchen (*Bizer*, in: *Simitis*, BDSG, § 6b Rdnr. 60). Berücksichtigt werden muss dabei auch, ob der überwachte Durchgangsraum rasch durchmessen werden kann oder spontan zur sozialen Kommunikation benutzt wird. So ist die Schutzbedürftigkeit in öffentlich zugänglichen Räumen dann höher, wenn sich Menschen dort typischerweise länger aufhalten und/oder miteinander kommunizieren (*Bizer*, in: *Simitis*, BDSG, § 6b Rdnr. 60).
- Von erheblich belastendem Gewicht ist eine Videoüberwachung darüber hinaus nur dann, wenn sie ununterbrochen einen Raum unter Kontrolle hält und die Betroffenen nicht ausweichen können (vgl. dazu *LG Braunschweig*, NJW 1998, 2458; *Bizer*, in: *Simitis*, BDSG, § 6b Rdnr. 64).
- § 4 BDSG n. F. erlaubt ab 25.05.2018 zukünftig die Videoüberwachung öffentlich zugänglicher Räume zur Wahrnehmung des Hausrechts und zur Wahrnehmung berechtigter Interessen bei Vorheriger Zweckfestsetzung.

DR. KOCH

Einführung Videoüberwachung

Fall1: **Der ambulante Pflegedienst – Sie betreuen Herrn A. in seiner privaten Wohnung. Herr A ist Wachkomapatient. Die Ehefrau B ist zur Betreuerin bestellt und arbeitet tagsüber Vollzeit. Frau B hat in allen Räumen der gemeinsamen Wohnung mit Herrn A Videokameras aufgestellt. Ihr Mitarbeiter C fühlt sich in seinem Persönlichkeitsrecht verletzt und fordert Frau B auf, die Kameras zu entfernen. Zu Recht?**

Fall2: **Wie Fall 1, nur dass Herr A ein in ambulanter Tagespflege betreuter Demenzkranker ist.**

§ 4 BDSG n. F. regelt die Videoüberwachung nur in öffentlich zugänglichen Räumen => für Privatwohnung unanwendbar.

§ 4 BDSG n. F. schränkt allerdings das Recht zur Videoüberwachung in öffentlich zugänglichen Räumen ein => in Privaträumen, die sich dadurch kennzeichnen, dass nicht jeder Zutritt hat grundsätzlich zulässig.

Aber: **Recht am eigenen Bild des Pflegers. Eine permanente Aufzeichnung wegen Drittbetroffenheit unzulässig, Anlassbezogen aber möglich. Im Übrigen nur Sichtkontrolle bei kurzer Speicherzeit und Verpixelung Gesicht.**

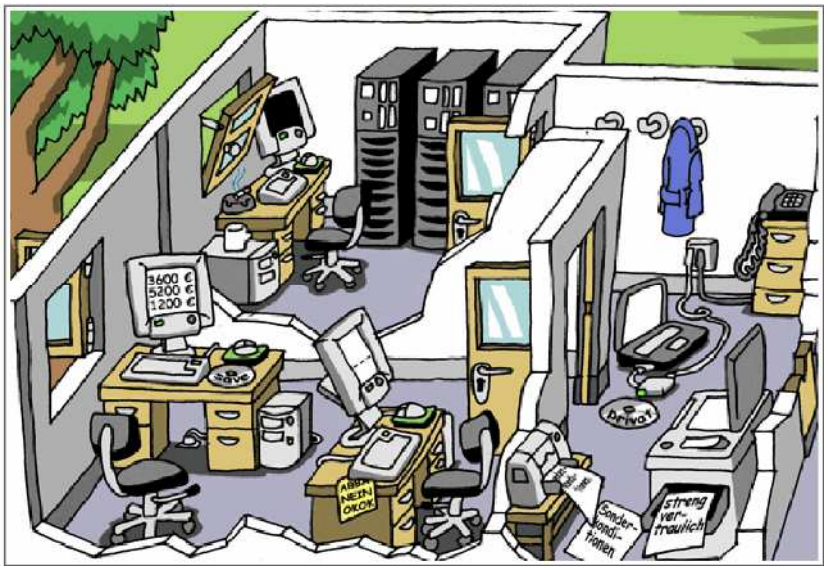
DR. KOCH

Datenschutz – American Style

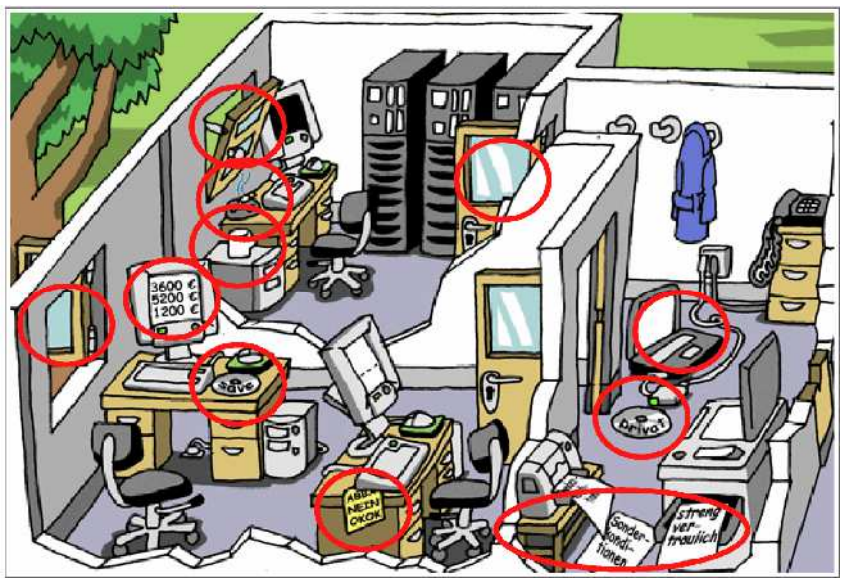
Geheimnisse der New Yorker Polizei liegen nach der Thanks-Giving Parade auf der Straße!!!

- Bei der traditionellen Parade zum Thanksgiving-Feiertag in New York regnete es Konfetti mit vertraulichen Informationen der Polizei;
- "Das waren ganze Sätze, Nummernschilder und Polizeiberichte", sagte der Anwalt Saul Finkelstein zu CNN.
- Selbst Sozialversicherungsnummern, für viele Amerikaner der wichtigste Ausweis ihrer Identität, seien lesbar gewesen.

DR. KOCH



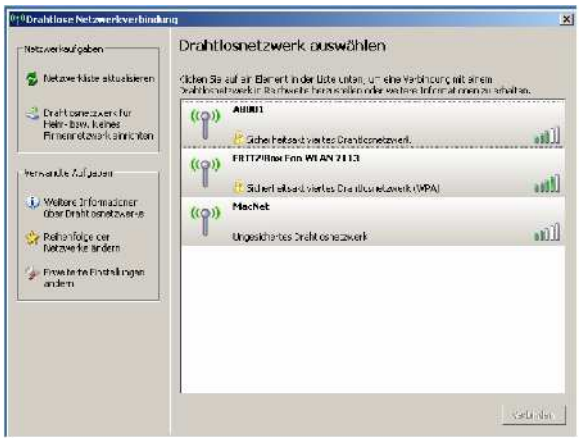
DR. KOCH



DR. KOCH

Rechtsanwalt

Sie überprüfen das WLAN….



DR. KOCH

Rechtsanwalt

Sie hacken das WLAN mit….

Das Hacken eines fremden WLAN's ist eine Straftat einige der hierfür genutzten Tools unterfallen § 202c StGB!!!

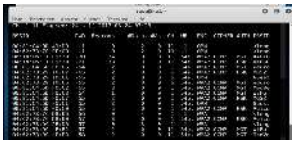
Sie brauchen:

- **Kali – eine Linux-Distribution die auf Penetrationstest optimiert ist – alle Tools an Bord.**
- **Eine WLAN-Karte die den Monitoring Modus unterstützt.**

Für das Hacken selbst:

- **Eine Liste möglicher Passwörter – Online bei Github.**
- **Die BSSID des Access-Points**
- **Einen mitgeschnittenen Handshake.**

Airodump-ng zeigt alle Access-Points in der Umgebung



Mit De-Auth-Attacke verbundene Endgeräte vom A-P schubsen mit Zwang zu Neuverbindung

Findet airodump-ng Handshake – Sicherung in Cab-Datei

DR. KOCH

Sie schützen Ihr WLAN durch....

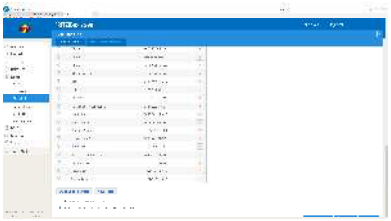
u.a. folgende Einstellungen am Router:

- **WLAN – unsichtbar machen.** Problem**: SSID lässt sich noch ermitteln (siehe S.24).** Lösung**: Namen ohne Bezug zum Unternehmen verwenden**

Netzwerk unsichtbar

- **Anmeldung beschränken auf bekannte Netzwerkgeräte – Neuanmeldungen ausschließen – Neuzugang also nur mit Admin möglich.**
- **Sichere WPA2 Kennwörter nutzen**
- **Gastzugang inaktiv oder über ein separates Netz betreiben.**

Zugang auf bekannte Endgeräte beschränkt



DR. KOCH

Meine Einrichtung beachtet den Datenschutz

Sind Sie sicher?

DR. KOCH

Datenschutz und Corona

2

DR. KOCH

Der Heimarbeitsplatz

DR. KOCH

Der Heimarbeitsplatz

Beim Heimarbeitsplatz sind unterschiedliche Fragestellungen zu unterscheiden:

- **Gibt es ein Recht auf Heimarbeit – nein, anders als in den Niederlanden, wo dieses 2015 eingeführt wurde;**
- **Darf ich in das Homeoffice, wenn ich Angst habe mich anzustecken – nein, selbst wenn sich ein Kollege positiv getestet wurde, kann ein Arbeitnehmer nicht zu Hause bleiben – Abstimmung mit dem Arbeitgeber und Entscheidung Gesundheitsamt;**
- **Bin ich im Homeoffice für den Datenschutz verantwortlich - Sie sind dazu verpflichtet, Betriebsgeheimnisse zu wahren und sich so zu verhalten, dass keine Informationen an unbefugte Personen gelangen.**
- **Muss ich mich im Homeoffice an die betriebliche Arbeitszeit halten - Ja, das muss man. Arbeitnehmer im Home-Office müssen die gleiche Arbeitszeit ableisten wie im Büro. Nur wenige Arbeitgeber überwachen dies allerdings genau – beispielsweise durch das Protokollieren Ihres Einloggens ins VPN-Netzwerk des Unternehmens, durch externe digitale Tools oder gar per Webcam – darf der Arbeitgeber dies?**

DR. KOCH

Der Heimarbeitsplatz II

- **Kinder und Beruf sind insbesondere im Homeoffice schwierig miteinander in Einklang zu bringen, muss der Arbeitgeber darauf Rücksicht nehmen? - Eine rechtliche Verpflichtung dazu besteht nicht. Die diversen rechtlichen Bestimmungen verlangen von Ihnen als Arbeitnehmer, alle zumutbaren Anstrengungen zu unternehmen, die Betreuung Ihrer Kinder während Ihrer Arbeitszeit sicherzustellen, ohne Ihre Berufstätigkeit zu beeinträchtigen. Zu solchen zumutbaren Anstrengungen kann es auch gehören, dass Sie versuchen, Resturlaub zu nehmen, Überstunden abzufeiern oder Zeitguthaben abzubauen, um die Bedürfnisse von Familie und Beruf auszubalancieren.**
- **Bin ich im Homeoffice versichert? - Die Versicherung gegen Arbeitsunfälle gilt im Home-Office genauso wie im Büro im Unternehmen. Abgrenzung kann aber schwierig sein. Wenn Ihnen also in Ihrem Home-Office der Laptop auf den Fuß fällt, dann ist dies ganz klar ein Arbeitsunfall. Aber bereits dann, wenn Sie sich vom Ihrem Heimarbeitsplatz zu Ihrer Toilette begeben und dabei ausrutschen, greift die Versicherung in der Regel nicht mehr. Gleiches gilt für das Kaffee holen.**
- **Das ArbZG gilt auch im Homeoffice – von 08:00 bis 23:00 Uhr unzulässig.**
- **Auch der Anhang 6 ArbStattV gilt.**

DR. KOCH

Der Heimarbeitsplatz III

- **Kann der Arbeitgeber einseitig eine Tätigkeit im Homeoffice anordnen? – § 106 GewO regelt hierzu wörtlich: „***Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, soweit diese Arbeitsbedingungen nicht durch den Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrags oder gesetzliche Vorschriften festgelegt sind.“* **Dies bedeutet, die Anordnung ist abhängig vom Arbeitsvertrag möglich.**
- **Ist im Arbeitsvertrag ein Arbeitsort festgelegt und keine Öffnung der Zuweisung eines anderen Arbeitsortes vertraglich vereinbart, scheidet die Zuweisung einer Tätigkeit im Homeoffice einseitig durch den Arbeitgeber aus. Im Übrigen spricht gegen die einseitige Anordnung von Homeoffice die Unververletzlichkeit der eigenen Wohnung, dafür spricht hingegen, aber den Arbeitgeber trifft nach §§ 3, 4 ArbSchG, § 618 Abs. 1 BGB und § 241 Abs. 2 BGB eine Rücksichtnahmepflicht sowie die Verantwortung für die Gesundheit der Arbeitnehmer (vgl. Krieger/Rudnik/Povedano, NZA 2020, S. 473).**
- **Die Ablehnung einer Tätigkeit im Homeoffice kann ein böswilliges Unterlassen des Erwerbs sein – Vergütungsanspruch geht verloren.**

DR. KOCH

Die Corona-Quarantäne

- **Sie sind positiv auf Covid19 getestet – müssen Sie davon den Arbeitgeber informieren? – Sie müssen Ihren Arbeitgeber wie bei jeder anderen Erkrankung auch innerhalb von drei Tagen ein ärztliches Attest vorlegen; viele Arbeitsverträge sehen sogar einen kürzeren Zeitraum vor.**
- **Ich war vor dem positiven Testergebnis noch in der Einrichtung – muss ich meinem Arbeitgeber diese Diagnose mitteilen. Generell gehen den Arbeitgeber Ihre Diagnosen nichts an, aber Sie sind verpflichtet das Gesundheitsamt zu informieren und sollten schon wegen des Bewohner- und Kollegenschutzes Ihre Infektion auch dem Arbeiteber mitteilen, um die Infektionskette zu unterbrechen, zumal die Erkrankung meldepflichtig ist.**
- **Können Sie, weil Sie symptomlos sind im Homeoffice arbeiten? – Wenn Sie schon im Homeoffice sind, ja, sonst muss eine Verständigung mit dem Arbeitgeber getroffen werden. Nur wenn Sie Ihre Arbeit nur in der Einrichtung verrichten können, regelt das Infektionsschutzgesetz eine Entgeltfortzahlung von bis zu 6 Wochen.**
- **Muss ich den Arbeitgeber über die Infektion informieren, wenn ich schon im Homeoffice bin? – Covid19 ist meldepflichtig, sofern Sie erkankt sind, gilt auch dann die im Arbeitsvertrag geregelte Meldepflicht.**

DR. KOCH

Die Corona Warn-App

- **Die Corona Warn-App verfolgt die Zielsetzung Infektionsketten nachverfolgen und unterbrechen zu können und deshalb den Nutzer (!!!) darüber warnen, wenn er sich in der Nähe eines Covid19 Erkrankten aufgehalten hat.**
- **Sobald eine Person positiv auf das Corona-Virus getestet wurde, soll eine Rückverfolgung von Kontaktketten (Contact Tracing) durch Mitarbeiter von Gesundheitsbehörden erfolgen können. Die App erzeugt und sendet in regelmäßigen Abständen mittels der Bluetooth-Technologie eine zufällige Zeichenfolge (TempID). Diese wechselt regelmäßig und lässt keinen direkten Rückschluss auf die konkrete Person zu. Wenn eine Person positiv getestet wurde, kann sie – nach entsprechender Freischaltung durch die Gesundheitsbehörden mittels eines QR-Codes oder per Telefon-TAN-Verfahren – die Daten freigeben. Die App übermittelt dann sämtliche TempIDs, die sie innerhalb der letzten Tage erzeugt und ausgesendet hat, an einen zentralen Server. Dort werden die Daten ohne Personenbezug gespeichert und können von allen anderen App-Benutzern regelmäßig heruntergeladen werden.**

DR. KOCH

Die Corona Warn-App II

- **Da die App personenbezogene Daten verarbeitet, bedarf es nach Art. 6 DS-GVO eines Erlaubnistatbestands. Alleine die Pseudonymisierung von Daten in Form von TempIDs führt nicht dazu, dass der Personenbezug verlorengeht. Die Pseudonymisierung erfolgt nach der Definition in Art. 4 Nr. 5 DS-GVO – anders als die Anonymisierung – in rücknehmbarer Weise, so dass zumindest, wenn die Zuordnungsregeln bekannt sind, wieder ein Personenbezug hergestellt werden kann.**
- **Hinsichtlich der Verbreitung der App ist ein enormes Spannungsfeld aufgetreten: Während eine wirkungsvolle Pandemiebekämpfung einerseits nur bei einem sehr hohen Verbreitungsgrad der App erfolgen kann, soll die Nutzung aber trotzdem freiwillig sein und bleiben.**

DR. KOCH

Die Corona Warn-App III

- **Nach Art. 6 I 1 Buchst. d DS-GVO kann die Verarbeitung zulässig sein, um lebenswichtige Interessen der betroffenen Person oder einer anderen Person zu schützen. Dazu kann nach Erwägungsgrund 45 DS-GVO auch die „*Überwachung von Epidemien*“ zählen. Aber wegen Art. 9 II Buchst. c DS-GVO ist die Einwilligung bei Gesundheitsdaten stets vorrangig.**
- **Denkbar erscheint eine Erlaubnis auf Grundlage des Art. 6 I 1 Buchst. e DS-GVO. Danach ist die Verarbeitung von Daten zulässig, wenn sie zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist. Allerdings erfordert dies eine konkrete Rechtsgrundlage im Unionsrecht oder im Recht eines Mitgliedstaats, die den Anforderungen von Art. 6 III DS-GVO genügt.**

DR. KOCH

Corona und Infektionsschutz

Fall1: **Sie sind Einrichtungsleitung und bemerken bei einem Heimbewohner Atemnotsymptome o. ä., die mit einer Covid19 Erkrankung im Zusammenhang stehen könnten. Müssen Sie das Gesundheitsamt informieren?**

Covid19 ist eine meldepflichtige Erkrankung. Bemerken Sie bei einem Bewohner Symptome, die mit einer solchen Erkrankung einhergehen könnten und haben Sie keine Möglichkeit einen Schnelltest am Bewohner durchführen zu lassen, müssten Sie sich mit dem Gesundheitsamt in Verbindung setzen – Gesundheitsschutz geht vor Datenschutz!

Fall2: **Die von Ihnen geführte Einrichtung hat einen Betriebsrat und Sie sind zur Teilnahme an einer Sitzung eingeladen, weil Sie über den Dienstplan für Januar 2021 verhandeln. Sie kommen zur Sitzung und betreten das 30qm große Betriebsratsbüro. Sie finden dort 9 Betriebsratsmitglieder bei geschlossenem Fenster vor, ohne Maske. Was ist zu tun?**

Fall 2a: **Im Rahmen der Betriebsratssitzung erfahren Sie, dass 4 Betriebsratsmitglieder von einer anderen Einrichtung mit einer Fahrgemeinschaft zu der Sitzung gefahren sind – ohne Maske. Was ist hier zu tun?**

Fall 3: **Sie haben eine Fachkraft und eine Hilfskraft – Ehepaar – zum Nachtdienst am Samstag geplant. Um 17 Uhr rufen diese an und teilen Ihnen mit, dass diese nicht kommen könnten, da ein Familienangehöriger positiv auf Covid19 getestet worden sei. Ihre Nachfrage, ob sie einen Test durchgeführt hätten, verneinen sie. Was ist zu tun?**

DR. KOCH

Corona und das Arbeitsverhältnis

- Fall1: **Der Arbeitnehmer X hat sich beim Betreiber Y GmbH um eine Tätigkeit als Pflegekraft beworben. Im Rahmen der Einstellung wird ihm ein Fragebogen vorgelegt, in welchem nachgefragt wird, ob er eine Corona-Impfung gemacht habe.**

  Welche Fragen im Rahmen einer Einstellung gestellt werden dürfen, richtet sich nach dem jeweiligen Einzelfall. So darf z. b. bei einer Einstellung im Labor nach der Schwangerschaft wegen der Risiken für den Fötus und bei einer Einstellung in der Pflege eines Krankenhauses nach einer TBC Infektion gefragt werden.

- Fall2: **Die Pflegekraft X möchte eine Impfung mit dem Corona-Impfstoff durchführen. Ihm wird bei der Anmeldung zu einem Impftermin im Impfzentrum Z mitgeteilt, dass er sich noch gedulden müsse, da zunächst die Risikogruppen nach dem Alter und die Pflegekräfte in Krankenhäusern geimpft werden müssten.**

  Zur Zeit wird diskutiert, ob die Impfreihenfolge durch Verordnung (BGM) oder Gesetz (Parlamentsdienst) festgelegt werden müsse. Wegen der Einschränkungen der Handlungsfreiheit (siehe unter 4.) dürfte eine Regelung durch Gesetz zwingend erforderlich sein.

DR. KOCH

Key-Facts zur EU-DSGVO

3

DR. KOCH

Datenschutz-Grundverordnung (DSGVO)

Stichtag ist der 25.05.2018

Es gibt keine Übergangsfrist für Anpassungen!!!

- Die DSGVO tritt am **25.05.2018** in Kraft.
- Es bestand/besteht also die Verpflichtung sich bis zum **24.05.2018 um 23.59 Uhr** auf die neue Rechtslage eingestellt zu haben.

DR. KOCH

Datenschutz-Grundverordnung (DSGVO)

Stichtag ist der 25.05.2018

Die früheren, nationalen Gesetze fallen weg

- Bundesdatenschutzgesetz alte Fassung (BDSG a. F.)
- Telemediengesetz (TMG)

  - Aber: ca. 50 Öffnungsklauseln in de DSGVO für nationale Regelungen -> Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) (in Kraft zum 30.06.2017) bedingt die Einführung eines neuen Bundesdatenschutzgesetzes (BDSG n. F. – Inkrafttreten 25.05.2018).

DR. KOCH

Datenschutz-Grundverordnung (DSGVO)

... und die Nichtbeachtung des Datenschutzes wird teuer!

Je nach Verstoß können Bußgelder verhängt werden

- bis zu 10 Mio. EUR bzw.
- bis zu 20 Mio. EUR bzw.
  - oder bis zu 4 % des gesamten, weltweit erzielten Jahresumsatzes,
  - je nachdem, welcher Betrag höher ist.

DR. KOCH

Datenschutz-Grundverordnung (DSGVO)

Und: Flucht ist keine Option!

Die DSGVO gilt, wenn personenbezogene Daten von **EU-Bürgern** verarbeitet werden

- durch **Unternehmen mit Niederlassung in der EU**, auch wenn die Datenverarbeitung außerhalb der EU stattfindet,
- durch **Unternehmen mit Niederlassung außerhalb der EU** bei Datenverarbeitung im Zusammenhang mit
  - dem (auch kostenlosen) Anbieten von Waren oder Dienstleistungen
  - der Beobachtung des Verhaltens von Bürgern innerhalb der EU

DR. KOCH

Wirkungen der EU-DSGVO

Art. 99:
„ … Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedsstaat.“

- Die DS-GVO ist eine allgemeine Regelung mit unmittelbarer innerstaatlicher Geltung
  -> „**Durchgriffswirkung**“
- Grundsätzliche Vollharmonisierung im nicht-öffentlichen Bereich
- Ersetzt nationales Datenschutzrecht, führt grds. zur Unanwendbarkeit entgegenstehender nationaler Regelungen
- Öffnungsklauseln für nationalen Gesetzgeber in bestimmten Bereichen – Richtlinien-Charakter im öffentlichen Bereich
- Zweijährige Anpassungsphase für Rechtsbereinigung und Folgeänderungen

DR. KOCH

Öffnungsklauseln

- Ca. 50 – 60 Öffnungsklauseln:
  - bei Rechtsgrundlagen der Datenverarbeitung
  - für spezifischere nationale Regelungen
  - für Ausnahmen von Betroffenenrechten
  - für andere Fälle

DR. KOCH

Auswirkungen auf bestehende Regelungen

National

öffentlicher Bereich: Fortbestand der wesentlichen allgemeinen und der bereichsspezifischen Regelungen

nicht-öffentlicher Bereich: weitgehende Ersetzung durch DS-GVO

Rechtsbereinigungsaufgaben im

BDSG

LDSG´s

BereichsspezifischenDatenschutzrecht wie Melderecht, Sozialrecht usw.

Nicht betroffen sind z. B. (zunächst)

TMG?, TKG, BetrVG, UWG

Europa

- EU-DS-RiL (RL 95/46/EG) wird aufgehoben
- E-Privacy-RL 2002/58 bleibt bestehen, aber Reformpflicht
  - Reformpflicht der VO 45/2001
  - Fortbestand (bis auf Widerruf) der Angemessenheitsbeschlüsse für Drittländer
  - BCR (Binding Corporate Rules) - Anerkennungen
  - Standardvertragsklauseln
  - Bestehenden Einwilligungen
  - Aufbau des Europäischen Datenschutzausschusses

DR. KOCH

Anpassungen in Deutschland

DR. KOCH

Stand der nationalen Umsetzungsgesetzgebung

Erster Entwurf eines Umsetzungsgesetzes EU (DSAnpUG-EU) im September 2016 wurde innerhalb weniger Tage wegen umfassender Kritik zurückgezogen.

Zweiter Referentenentwurf vom 11.11.2016 wurde am 01.02.2017 vom Bundeskabinett beschlossen und am 10.03.2017 erfolgte Stellungnahme des Bundesrates. Am 30.06.2017 wurde die gesetzliche Neuregung verkündet und ist als BDSG n. F. zeitgleich zur EU-DSGVO in Kraft getreten.

Es bestehen insbesondere folgende Abweichungen zur EU-DSGVO:

- **EU-DSGVO gilt für jede Verarbeitung personenbezogener Daten (Rdn. 22 EU-DSGVO), das BDSG gilt hingegen gem. § 1 Abs. 1 BDSG n. F. nur für automatisierte Verarbeitung.**
- **Einschränkung der Informationspflicht nach Art. 13, 14 EU-DSGVO bei Unmöglichkeit, unverhältnismäßigem Aufwand, Verarbeitungsziele würden unmöglich oder ernsthaft beeinträchtigt.**
- **§ 4 BDSG-E schränkt die Möglichkeit der Videoüberwachung im Verhältnis zur EU-DSGVO im privaten Bereich ein, und erweitert die Überwachungsmöglichkeiten im öffentlichen Bereich.**
- **Datenschutzbeauftragter ist gemäß § 38 BDSG-E auch zukünftig bei Beschäftigung von 10 Personen in der Verarbeitung personenbezogener Daten.**
- **Regelungen in §§57-72 BDSG-E zur Auftragsdatenverarbeitung trotz bestehendem Wiederholungsverbot.**
- **Beschäftigtendatenschutz in § 23 BDSG-E weicht von Art. 88 Abs. 2 DSGVO ab.**

=> Nationaler Gesetzgeber trifft Regelungen ohne Rücksicht auf Vereinbarkeit mit der DSGVO!!! Wirksamkeit also unklar!!!

DR. KOCH

BMF Schreiben v. 14.11.2014 zum GoBD

Festlegungen des Bundesfinanzministeriums zum Führen von Büchern sowie zum Datenzugriff GoBD v. 14.11.2014 in Kraft getreten zum 01.01.2015. Diese Vorgaben entsprechen § 21 BDSG n. F. und sind ab 25.05.2018 zu beachten.

Vorgaben zu IT-gestützten steuerrelevanten Prozessen mit Vorgaben zu:

- **Datensicherheit – Daten sind gegen Verlust und unberechtigten Zugriff zu sichern (Verschlüsselung).**
- **Unveränderbarkeit – Daten dürfen nicht ohne entsprechende Kenntlichmachung überschrieben, verändert oder ersetzt werden.**
- **Ordnungsmäßigkeit - alle buchungsrelevanten Daten, Aufzeichnungen und Vorgänge müssen nachvollziehbar, nachprüfbar, vollständig, richtig, zeitgerecht/zeitnah, geordnet und unveränderbar sein**
- **Aufzeichnungspflicht - alle relevanten Geschäftsvorfälle müssen in zeitlicher Reihenfolge und in sachlicher Gliederung darstellbar sein; zudem müssen auch alle zusätzlich notwendigen Tabellendaten, Historisierungen und Programme gespeichert werden**
- **Aufbewahrungspflicht - aufbewahrungs- und aufzeichnungspflichtige Daten, Datensätze, elektronische Dokumente sowie elektronische Unterlagen sind geordnet und grundsätzlich im Original – also etwa auch in ihrem elektronischen Ursprungsformat – aufzubewahren**

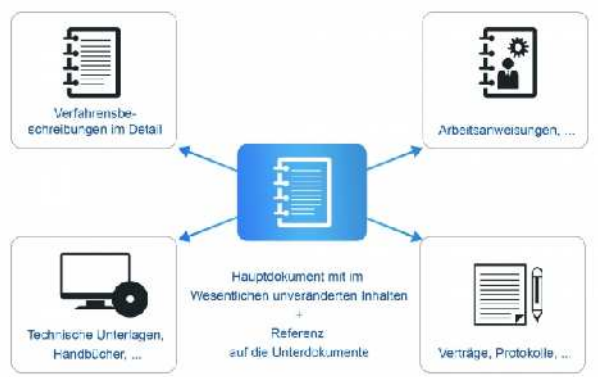
Vorgaben zum Datenzugriff der Finanzverwaltung

- **Unmittelbarer Datenzugriff - Direkter Lesezugriff für die Finanzbehörde über das DV-System des Unternehmens auf alle aufzeichnungs- und aufbewahrungspflichtigen Daten**
- **Mittelbarer Datenzugriff - Maschinelle Auswertung aller aufzeichnungs- und aufbewahrungspflichtigen Daten durch das Unternehmen oder einen Dritten**
- **Datenträgerüberlassung - Bereitstellung aller aufzeichnungs- und aufbewahrungspflichtigen Daten nebst allen zur Auswertung nötigen Tabellendaten sowie Verknüpfungen auf einem maschinell auswertbaren Datenträger**

DR. KOCH

BMF Schreiben v. 14.11.2014 zum GoBD

Umfassende Verfahrensdokumentation **ist erforderlich. Besonderes Augenmerk sollten Unternehmen auf das immer wieder im BMF-Schreiben betonte Führen einer konkreten und vollständigen Verfahrensdokumentation legen. Die konkrete Ausgestaltung der Verfahrensdokumentation ist insbesondere abhängig von der Komplexität des eingesetzten DV-Systems. Es empfiehlt sich eine systematische Dokumentation, beispielsweise mit Master und Sekundärdokumenten sowie die Verschlüssel der Daten.**



DR. KOCH

BMF Schreiben v. 14.11.2014 zum GoBD

Archivierung belegloser Meldungen

So müssen belegloseMeldungen **– etwa über den sogenannten „Electronic Data Interchange" (EDI) – vom Empfänger der Rechnung** in ihrem Ursprungsformat gespeichert **werden. Dies entspricht der gelebten Praxis, nach welcher es sich bei EDI-Belegen um originär elektronische Unterlagen handelt, die entsprechend originär elektronisch vorzuhalten sind. Neben EDI dürfte dies insbesondere für den XML-basierten Rechnungsaustausch von Bedeutung sein, der – Beispiel** ZUGFeRD-Standard **(ZUGFeRD basiert auf PDF/A-3 und bietet die Möglichkeit, eine XML-Rechnung in ein PDF einzubetten und dadurch sowohl strukturierte Rechnungsdaten (XML) als auch das Rechnungsbild (PDF) gleichzeitig per Mail zu übermitteln) – ein immer breiteres Anwendungsspektrum in der Praxis einnimmt. Kommt es beim Rechnungsempfänger zu einer Konvertierung der Rechnungsdaten in ein hauseigenes Format, ist er verpflichtet, die Kopie als solche zu kennzeichnen und beide Varianten aufzubewahren. Dabei ist – so die Empfehlung der Praxis - gerade auch im Hinblick auf eine Archivierung in einem gesonderten Archivsystem sicherzustellen, dass die** Rechnungsdaten jederzeit visuell darstellbar **sind.**

Übermittlung von Rechnungen als E-Mail Anhang

Die GoBD bringen zu dem Klarheit in der Frage, ob beim Eingang einer elektronischen Rechnung als Attachement an einer E-Mail **lediglich das angehängte Rechnungsdokument oder auch die (nur zur Übermittlung genutzte) E-Mail zu speichern ist. So muss eine E-Mail, die lediglich zur Übermittlung dient und keine buchungsrelevanten Informationen enthält,** analog zum Briefumschlag **nicht zusätzlich aufbewahrt werden. Eine Klarstellung, die in der alltäglichen Praxis beim elektronischen Rechnungsaustausch deutlich für Erleichterung sorgen sollte. Die latente Problematik der inhaltlich identischen Mehrstücke bei Rechnungen im Hybridformat oder bei der mehrfachen Übermittlung auf z.B. postalischem und digitalem Weg, klammern die neuen GoBD dagegen zum bedauern vieler Experten aus.**

DR. KOCH

Ich kenne das Datenschutzrecht

Sind Sie immer noch sicher?

DR. KOCH

Meine Einrichtung beachtet den Datenschutz

☐ **Ja**

☐ **Nein**

☐ **Weiß nicht**

Grundlagen des Datenschutzrechts

4

Grundlagen des Datenschutzrechts

Datenschutz ist ein durch das Grundgesetz geschütztes Grundrecht.

Jeder Mensch soll grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen.
Konsequenz: EU-Recht kann in keine Grundrechtspositionen eingreifen!!!

Der Umgang mit personenbezogenen Daten wird durch das Datenschutzrecht geregelt.

Es kommt zur Anwendung, wenn Sie Daten bearbeiten, die **einem Menschen zugeordnet** werden können.

DR. KOCH

Allgemeines Persönlichkeitsrecht

Inhalt

Das Recht der Betroffenen zur aktiven und individuellen Gestaltung der Persönlichkeit in den von der Verfassung und den Gesetzen gezogen Grenzen, soweit es nicht bereits Gegenstand spezialgesetzlicher Vorschriften oder Verfassungsnormen ist.

Bestandteile

Menschenwürde (Art. 1 Abs. 1 GG)

- Persönlichkeitsgüter (Geist, Körper, Gesundheit, Existenz)
- Individualität (äußeres Erscheinungsbild, Auftreten, Äußerungsformen, persönliche Anlagen, Besonderheiten

allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG)

aktive (freie) Gestaltung der Lebensführung

Schranken

unmittelbarer Verfassungs- und Gesetzesvorbehalt

DR. KOCH

Allgemeines Persönlichkeitsrecht

Fall („My Home is my castle): *Die Hauseigentümerin B liegt Tiere und auch Ratten, ihr Nachbar N schätzt letztere Gattung dagegen weniger. N hat Kinder im Alter von 1, 3 und 5 Jahren. Die B füttert auf ihrem 1000 qm großen Grundstück die von ihr geliebten Ratten fleißig, so daß nach einer gewissen Zeit die dort lebende Rattenpopulation etwa 1000 Stück erreicht hat. Da das Grundstück der B von der Größe nicht mehr ausreicht, nutzen die Ratten nunmehr auch den Garten sowie das Mauerwerk des Hauses von N als Behausung. N, der um die Gesundheit seiner Kinder, und fordert das Gesundheitsamt zum Einschreiten auf. Als die zuständigen „Kammerjäger" die Behausungen der Ratten „vergasen" wollen und das Gesundheitsamt der B untersagt die Ratten weiter zu füttern, verweigert die B ihnen den Zutritt auf ihr Grundstück. Sie fühlt sich in ihrem Eigentumsrecht sowie in ihrer allgemeinen Handlungsfreiheit verletzt. - Zu Unrecht, die N muß die „Vergasung" dulden. Sowohl das Eigentum nach Art. 14 Abs. 1 GG als auch die allgemeine Handlungsfreiheit nach Art. 2 Abs. 1 GG stehen unter einem allgemeinen Gesetzesvorbehalt. Die Ratten ist als Träger von Krankheitserregern die die Gesundheit des Menschen gefährden können bekannt. Da es sich bei der Rate um ein Tier handelt ist das BundesseuchenG nicht anwendbar. Gleiches gilt für das TierseuchenG, da die Ratte Träger von menschlichen und nicht tierlichen Krankheitserregern ist. Wohl aber ist das ASOG als allgemeines Ordnungsgesetz zur Gefahrenabwehr anwendbar. Vorliegend könnte dabei § 14 Abs. 1 ASOG einschlägig sein, da die Gefahr von Tieren ausgeht. Allerdings ist die B nur Inhaberin der Herrschaftsmacht bezüglich des Grundstückes und nicht der Ratten, da es sich bei diesen nicht um Haustiere im Sinne von § 1 Abs. 2 Nr. 1 TierseuchenG handelt, da sie nicht von der B gehalten werden, auch wenn sie von ihr gefüttert werden. Mithin ist § 14 ASOG unanwendbar. Wohl aber ist § 17 ASOG als allgemeine Gefahrenklausel anwendbar, da von den Ratten Gesundheitsgefahren für die Kinder des N sowie die anderen Nachbarn ausgehen. Die Vergasung ist unzweifelhaft eine Möglichkeit um diese Gefahren zu beseitigen, ein milderes Mittel ist nicht möglich, da allein das Untersagen des Fütterns die Rattenpopulation nicht vernichten würde, sondern nur zur Folge hätte, daß die Ratten sich das Futter woanders beschaffen, was noch eine Verstärkung der Gesundheitgefahren für Dritte zur Folge hätte. Das Vergasen ist auch hauptsächlich nur vom Grundstück der N aus möglich, da sich dort die meisten Behausungen befinden. Daher hat die B das Betreten ihres Grundstückes nach § 17 ASOG zu dulden. Gleiches gilt für die Anordnung des Unterlassens des Fütterns, da die allgemeine Handlungsfreiheit jedenfalls dort ihre Grenze findet, wo andere geschädigt werden (soziale Verpflichtung der Handlungsfreiheit) und zudem gesetzliche Beschränkungen ohnehin ausdrücklich zugelassen sind. Eine solche Anordnung nach § 17 ASOG ist auch unzweifelhaft geeignet, ein erneutes Ansteigen der Rattenpopulation zu verhindern, nach dem diese vergast und damit weitestgehend vernichtet worden ist.*

DR. KOCH

Recht auf informationelle Selbstbestimmung

Inhalt

Das Recht des Betroffenen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen er persönliche Lebensverhältnisse offenbart

Reichweite

im öffentlichen Bereich	im nicht-öffentlichen Bereich
stellt die Grundbedingung jeglicher Datenverarbeit dar und betrifft daher die datenschutzrechtliche Ordnung insgesamt	ist nicht nur nur Abwehrrecht, sondern gilt auch im Privatrecht und strahlt nicht nur als Interpretationshilfe bei der Auslegung von Generalklauseln ein

Einschränkbarkeit

- im überwiegenden Allgemeininteresse

Voraussetzungen

- die Einschränkung bedarf einer (verfassungsmäßigen) Grundlage (Gesetzesvorbehalt)
- Aus der gesetzlichen Regelung müssen der Tatbestand und die Rechtsfolge geregelt und ersichtlich sein
- die Norm muß verhältnismäßig sein (geeignet, erforderlich und angemessen)
- es müssen ausreichende organisatorische und verfahrensrechtliche Regelungen zum Schutz des Betroffenen enthalten sein (Transparenz)
- die Norm muß eine eindeutige Bestimmung des Verwendungszweckes enthalten (Zweckbindung)

Abb. 3

DR. KOCH

Personenbezogene Daten

Personenbezogene Daten sind alle Angaben, die sich auf eine bestimmte oder aber auch nur bestimmbare Person beziehen zukünftig in § 46 BDSG n. F. geregelt.

Beispiele:

Name, Geburtsjahr, Telefonnummer, Wohnverhältnisse, Kreditkartennummer, Vermögensverhältnisse, Gehalt, Adresse

DR. KOCH

Bestimmt ist eine Person, wenn sich ihre Identität direkt aus dem Datum selbst ergibt.

Name

Dr. Koch - Rechtsanwalt

59

DR. KOCH

Bestimmt ist eine Person, wenn sich ihre Identität direkt aus dem Datum selbst ergibt.

Bestimmbar wird eine Person, wenn ihre Identität durch die Kombination des Datums mit einer anderen Information feststellbar wird.

IP-Adresse

Abgleich mit Providerdaten

Dr. Koch - Rechtsanwalt

60

DR. KOCH

Begriff der personenbezogenen Daten

Fall: *Eine Frau Rosa S. schreibt an den Aufsichtsratsvorsitzenden einer stationären Pflegeeinrichtung eine Beschwerde wg. angeblichen Verstoßes gegen das Datenschutzrecht, da der Geschäftsführer der Einrichtung und ihr Datenschutzbeauftragter außerhalb der Pflegeeinrichtung in einer Gesellschaft Beratungen im Datenschutz erbringt zusammenarbeiten würden, so dass der Datenschutzbeauftragte nicht ausreichend unabhängig vom Geschäftsführer sei. Daten über Frau Rosa S. waren in der Einrichtung nicht auffindbar. Eine Überprüfung der in der Signatur angegebenen Daten (Name, Vorname, Adresse, Handynummer) ergab, das hierunter eine Rosa S. nicht ermittelbar war.*

- *Da die Angaben in der Signatur fehlerhaft waren und der Verfasser nicht ohne Zusatzmaßnahmen ermittelt werden kann – Angaben in der Signatur* ***nicht personenbeziehbar****.*
- ***Betroffenenrechte****: Können von Frau Rosa S. nicht geltend gemacht werden, da keine Daten über diese erfasst.*
- ***Unabhängigkeit DSB****: Ist gegeben, da gesellschaftsrechtliche Verknüpfung zwischen Geschäftsführer und Datenschutzbeauftragter in externer Gesellschaft keine Wirkung für Anstellungsverträge in der Einrichtung hat.*

DR. KOCH

Begriff der Datei

Fall: *Der A ist in der Pflegeeinrichtung B beschäftigt. In dem Stationszimmer hängt ein Urlaubsplan für das laufende und zukünftige Jahr aus, in dem sich die Mitarbeiter jährlicher im November für das folgende Kalenderjahr zwecks Planung eintragen und den Urlaub der Kollegen ablesen können. Ferner wird in der Personalabteilung eine Urlaubs- und Krankheitskartei geführt, zu der die Mitarbeiter ihre konkreten Urlaubsanträge und Krankschreiben einreichen müssen und die dort aufbewahrt werden. Schließlich müssen die Mitarbeiter beim Betreten und Verlassen des Betriebes ihre Stempelkarte stempeln lassen, die sich neben der mechanischen Zeituhr in offen zugänglichen Fächern befinden. A will wissen ob Urlaubsplan, Kartei und Stempelkarten dem § 46 Abs. 2 BDSG n. F. unterfallen? - Der* ***Urlaubsplan****, der anders als die Kartei nicht der Auswertung über die Anwesenheit zwecks Vergütungsberechnung dient - nein. Die* ***Urlaubs- und Krankheitskartei****, die der Ermittlung der Anwesenheit dienen - ja. Die* ***Stempelkarten*** *unterfallen dem BDSG, wegen der auf ihnen vorhandenen personenbezogenen Daten (Namen usw.) dann, wenn mehr als eine in einer Aufbewahrungsvorrichtung aufbewahrt werden, da es sich dann um eine nicht automatisierte Datei handelt*

Achtung: § 4 Abs. 2 EU-DSGVO unterscheidet nicht mehr zwischen automatisierter und nicht automatisierter Verarbeitung. § 38 BDSG n. F. (Datenschutzbeauftragter) behält die bisherige Differenzierung hingegen bei. Widerspruch nationales Recht zur EU-DSGVO!!!

DR. KOCH

Besondere personenbezogene Daten

Weitaus strengere Regeln gibt es für den Umgang mit sogenannten besonderen Arten personenbezogener Daten (Art. 4 Abs. 15 und Art 9 Abs. 1 EU-DSGVO, da diese besonders schützenswert sind.

Politische Meinung

Gewerkschafts-zugehörigkeit

Ethnische Herkunft

Religiöse Überzeugung

Gesundheit § 22 Abs. 1 Nr. 1 lit. b) BDSG n. F.

Sexual-leben

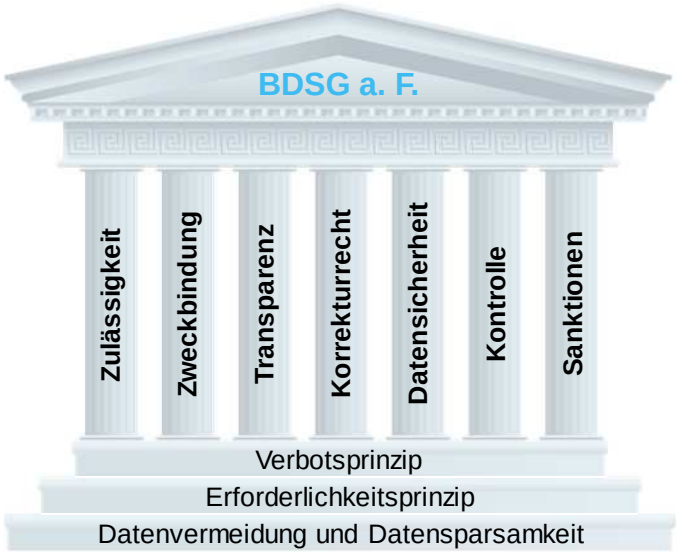
DR. KOCH

Grundsätze für die Verarbeitung personenbezogener Daten, Art. 5 DSGVO

- Rechtmäßigkeit
- Treu und Glauben
- Transparenz
- Zweckbindung
- Datensparsamkeit
- Richtigkeit
- Begrenzte Speicherung
- Integrität und Vertraulichkeit

Was davon ist neu?

DR. KOCH



DR. KOCH

EU-DSGVO – Was ist zu tun?

BDSG	EU DS GVO	Bewertung
Regelung des Ob und Wie der Datenverarbeitung: **Ob?** • Verbot mit Erlaubnisvorbehalt • Erforderlichkeit • Zweckbindung • Transparenz **Wie?** • Datenschutzmanagement (betrieblicher DSB, Verfahrensverzeichnis, Vorabkontrolle) • Technisch- organisatorische Maßnahmen • Regelungen für Auftragsdatenverarbeitung	**Ob?** • Rechtmäßigkeit der Verarbeitung • Erforderlichkeit • Zweckbindung • Transparenz **Wie?** • Datenschutzmanage -ment • Stärkere Verantwortlichkeit von Datenverarbeiter & Auftragsdatenverarbeit er • Datenschutzfreundlic he Technik & Voreinstellung	➢ **Vieles ist bekannt** ➢ **Manches wurde verschärft** (Informationspflichten, Prozesse Betroffenenrechte) ➢ **Manches ist besser zu dokumentieren** (Nachweis der getroffenen Maßnahmen) ➢ **IT-Systeme sind auf DS-GVO-Tauglichkeit zu prüfen und ggf. anzupassen**

DR. KOCH

Was ist wirklich neu in der EU-DSGVO

Wesentliche Änderungen sind z. B.

- **Die Dokumentationspflichten werden deutlich ausgeweitet (vgl. Art.5 Abs.2 EU-DSGVO)**
- **Die Betroffenenrechte werden deutlich ausgeweitet und es wird eine Reaktionsfrist verbindlich festgelegt (vgl. Art. 12-23 EU-DSGVO)**
- **Vorgaben für IT gestützte Prozesse gemäß § 22 BDSG n. F. entsprechend BMF Rundschreiben vom 14.11.2014 für die Behandlung von Geschäftsvorfällen.**
- **Es werden neue Bußgeldtatbestände eingeführt**
- **Die Bußgelder erhöhen sich drastisch auf bis zu 20 Mio € oder 4% des weltweiten Jahresumsatzes, je nach dem, welcher Betrag höher ist.**

DR. KOCH

Verbot mit Erlaubnisvorbehalt

Die Datenverarbeitung ist grundsätzlich nur dann erlaubt, wenn eine dieser Voraussetzungen erfüllt ist (Art. 6 DSGVO):

- Es liegt die **Einwilligung** der betroffenen Person vor;
- Es liegt ein **berechtigtes Interesse (was ist das?)** an der Datenverarbeitung vor und schutzwürdige Interessen des Betroffenen (insbesondere von Kindern) stehen dem nicht entgegen;
- Oder die Datenverarbeitung ist **erforderlich**
  - zur **Erfüllung eines Vertrags** der auf Anfrage des Betroffenen geschlossen wurde;
  - für **vorvertragliche Maßnahmen** auf eine Anfrage des Betroffenen hin;
  - zur **Erfüllung einer rechtlichen Verpflichtung** des Verantwortlichen;
  - zum **Schutz lebenswichtiger Interessen** der betroffenen Person oder einer anderen natürlichen Person;
- im **öffentlichen Interesse** oder in Ausübung **öffentlicher Gewalt**.

DR. KOCH

Namensschild Klingelanlage/Eingang Einrichtung

Das AG Schöneberg hat schon in einer Entscheidung vom 07.05.1990 bereits ausgeführt:

Diese Rechte stehen den Klägern entsprechend §§ 12, 823, 862, 1004 BGB zu. Sie sind Ausdruck des allgemeinen Persönlichkeitsrechts der Kläger, das im Namensrecht in § 12 BGB für einen Teilbereich besonderen und in §§ 823 Abs. 1, 1004 Abs. 1 BGB durch Zuerkennung von Abwehrrechten gegenüber rechtswidrigen Beeinträchtigungen allgemeinen Schutz gefunden hat.

Eine Beeinträchtigung des Persönlichkeitsrechts liegt auch darin, gegen den Willen des Berechtigten durch Anbringung von Hinweiszeichen, insbesondere Namensschildern seinen privaten Aufenthaltsbereich für Dritte kenntlich zu machen. Das gilt folglich auch für die hier interessierende Kennzeichnung der Wohnung der Kläger an der Klingelanlage des Hauses.

BZ v. 18.10.2018:

„Zum Schutz der Privatsphäre der Mieter könnten demnächst in ganz Deutschland die Namenschilder an der Klingel durch Wohnungsnummern ersetzt werden. Schuld daran ist die Europäische Datenschutzgrundverordnung (DSGVO). Die Verordnung, die seit Mai in ganz Europa gilt, soll die Privatsphäre aller Bürger schützen. Ob darunter auch ein Name auf einem Klingelschild fällt, ist unklar.“

DR. KOCH

Art. 6 Abs. 1 EU-DSGVO

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) **Die** betroffene Person **hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;**

b) **die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die** auf Anfrage der betroffenen Person **erfolgen;**

c) **die Verarbeitung ist zur Erfüllung einer** rechtlichen Verpflichtung **erforderlich, der** der Verantwortliche unterliegt**;**

d) **die Verarbeitung ist erforderlich, um** lebenswichtige Interessen der betroffenen Person **oder einer anderen natürlichen Person zu schützen;**

e) **die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im** öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt **erfolgt, die dem Verantwortlichen übertragen wurde;**

f) **die Verarbeitung ist zur Wahrung der** berechtigten Interessen des Verantwortlichen **oder eines Dritten erforderlich, sofern nicht die** Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person**, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt**

DR. KOCH

Die neue Einwilligung nach Art. 7, 8 DSGVO)

- Der Verantwortliche muss die Einwilligung **nachweisen** können
  - Ist die Einwilligung Teil weiterer schriftlicher Erklärungen, muss klar unterschieden werden
- Hinweis auf das Widerrufsrecht des Betroffenen bei der Einwilligung
- Widerruf muss so einfach wie die Einwilligung sein
- Kopplungsverbot
- Opt-In: Nicht vorab angeklickte Checkboxen mit Double-Opt-In

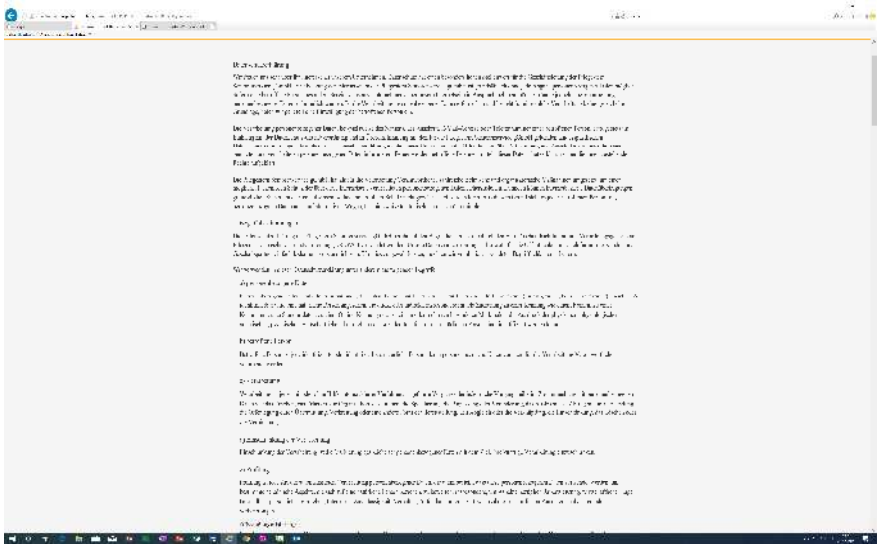
DR. KOCH

Das neue berechtigte Interesse nach Art. 6 Abs. 1 f DSGVO

- **Berechtigtes Interesse** an der Datenverarbeitung und schutzwürdige Interessen des Betroffenen (insbesondere von Kindern) stehen dem nicht entgegen;
- Dass es sich bei den **Werbeinteressen** der Onlinebranche um „berechtigte Interessen" im Sinne der DSGVO handeln kann, ergibt sich aus dem Erwägungsgrund 47. Dieser stellt ausdrücklich klar, dass die Durchführung von Direktmarketing als berechtigtes Interesse betrachtet werden **kann – also nicht muss!!!**

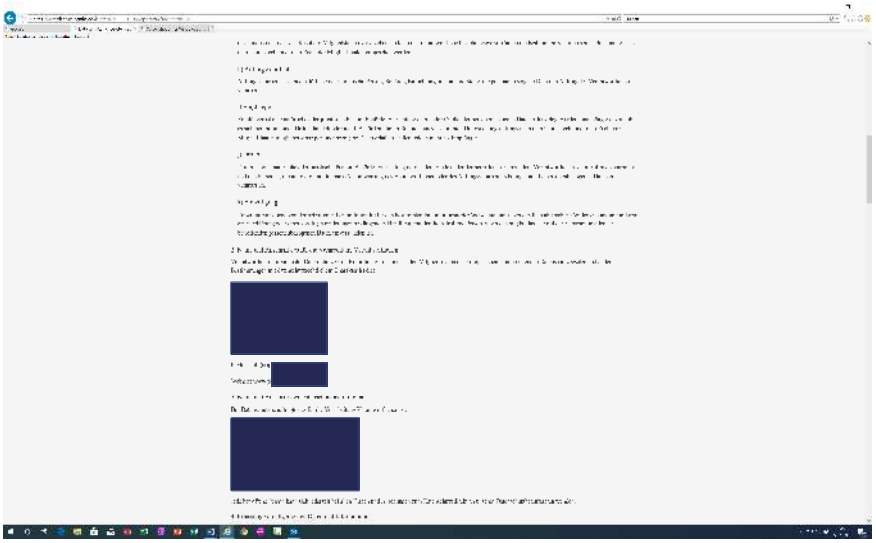
DR. KOCH

Datenschutzerklärung nach Art. 12 DSGVO



DR. KOCH

Datenschutzerklärung nach Art. 12 DSGVO



DR. KOCH

Transparenzgebot des Art. 12 Abs. 1 EU-DSGVO

§ 12 Abs. 1 EU-DSGVO regelt wörtlich:

- *Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen,* ***in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln****; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.* [2]*Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch.* [3]*Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.*

DR. KOCH

Das sind die neuen Informationspflichten für Unternehmen Art. 13, 14 DSGVO

- **Namen und Kontaktdaten** der verantwortlichen Stelle und ggf. des Vertreters;
- ggf. Kontaktdaten des **Datenschutzbeauftragten**;
- **Zweck und Rechtsgrundlage** der Datenverarbeitung; sollen z. B. „berechtigte Interessen“ die Rechtsgrundlage sein, ist dazulegen, worin sie bestehen;
- ggf. die **Empfänger oder Kategorien von Empfängern** der personenbezogenen Daten
- ggf. Informationen zum **Datentransfer in Drittstaaten** einschließlich der Rechtsgrundlage
- Angaben zur **Speicherdauer** personenbezogener Daten bzw. Kriterien, nach denen sich die Speicherdauer bestimmt;

DR. KOCH

Das sind die neuen Informationspflichten für Unternehmen Art. 13, 14 DSGVO

- Information über das Bestehen des **Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs-, Widerspruchs- oder ggf. Widerrufsrecht sowie das Recht auf Übertragbarkeit der Daten und das Recht auf Beschwerde bei einer Aufsichtsbehörde**;
- Hinweis, ob der der Betroffene **gesetzlich** oder **vertraglich** zur Bereitstellung personenbezogener Daten verpflichtet ist
- ggf. Hinweis und Information zum Profiling oder eine andere Art von automatisierter Einzelfallentscheidung;
- ggf. Herkunft der Daten: Werden die Daten nicht bei dem Betroffenen erhoben, sind die die Quellen anzugeben.

DR. KOCH

Wann muss der Bewohner/Patient informiert werden?

Fall: *Die Pflegeeinrichtung P erteilt die Hinweise zur Datenverarbeitung nach Art. 13, 14 EU-DSGVO bei der Aufnahme des Bewohners A in der Einrichtung. Die Einrichtung erfasst die Daten des A allerdings schon im Zusammenhang mit der Vertragsanbahnung. Bei einer Betriebsprüfung beanstandet der Landesdatenschutzbeauftragte diese Praxis. Er ist der Auffassung, dass die Hinweise, vor Beginn der vorvertraglichen Verarbeitung im Sinne von Art. 6 EU-DSGVO erfolgen müsse.*

Zu Recht: *Die Hinweise und Informationen zur Datenverarbeitung müssen vor Beginn einer Datenverarbeitung erteilt werden.*

Achtung: Eine Einwilligung in die Datenverarbeitung kann nur wirksam erteilt werden, wenn **vor** Beginn die Hinweise in die Datenverarbeitung wirksam und vollständig erteilt wurden!!!

Fall: *Das Hinweisformular der Pflegeeinrichtung P gibt den Verantwortlichen und den Datenschutzbeauftragten wieder, enthält dann umfangreiche Begriffsdefinitionen z. B. zu personenbezogenen Daten erteilt die Hinweise nach Art. 13, 14 EU-DSGVO dann aber, in dem einfach auf Art. 13, 14 EU-DSGVO verwiesen wird. Die geplante Datenverarbeitung wird nicht dargestellt. Sind diese Hinweise wirksam?*

Nein: Gemäß Art. 12 EU-DSGVO muss eine transparente Information über die geplante Verarbeitung der Daten erteilt werden. Dies ist vorliegend nicht gegeben.

DR. KOCH

Datenschutzerklärung Homepage – Social Media Plug-In‘s

Fall1: *Die Pflegeeinrichtung P hat eine eigene Homepage. Auf dieser Homepage sind auch Verlinkungen zu Facebook, Instagram, Twitter, Youtube usw., auch ein Like-Button ist auf der Seite integriert. Z. B. Facebook speichert die Daten eines Besuchers der Homepage, wenn dieser selbst einen Facebook-Account hat. Muss der Besucher im Rahmen der Datenschutzerklärung hierauf hingewiesen werden.*

Ja: *Nach der Entscheidung des EuGH v. 29.07.2019 – C40/17 – ist der Betreiber der Homepage verpflichtet für die Aufklärung des Besuchers über die Verarbeitungen durch Facebook usw. Sorge zu tragen*

Fall2: *Wie Fall1 jedoch hat die Pflegeeinrichtung P auch noch eine eigene Facebook-Seite. Muss die Datenschutzhinweiserklärung (kurz: Datenschutzerklärung) auch in diese Seite integriert werden oder reicht eine Verlinkung insoweit auf die Homepage ausreichend? Wie ist es, wenn der Interessent keinen Facebook-Account hat und gegenüber Facebook nicht in seine Verarbeitung eingewilligt hat.*

Antwort: Gemäß Art. 12 EU-DSGVO muss eine transparente Information über die geplante Verarbeitung der Daten **vor Beginn** einer Verarbeitung erteilt werden. Dies dürfte bei einer Verlinkung nicht gewährleistet sein. Ein Pop-Up mit der Erklärung wäre daher sinnvoll. Auf die Einwilligung gegenüber Facebook kommt es nicht an, da der Betreiber der Seite – also die Einrichtung P – für die Erteilung der Hinweise nach dem EuGH verantwortlich ist.

DR. KOCH

Datenschutzerklärung Homepage – Social Media Plug-In‘s

Fall3: *Wie Fall2, jedoch hat die Pflegeeinrichtung P derzeit Like-Button auf der Homepage eine eigene Homepage und eine Facebook-Seite. Auf der Facebook-Seite findet sich ein Link zur Homepage der Pflegeeinrichtung P. Der Administrator möchte einen Link auf der Facebook-Seite auf die Datenschutzerklärung der Homepage aufnehmen reicht das?*

Nein: Gemäß Art. 12 EU-DSGVO muss eine transparente Information über die geplante Verarbeitung der Daten **vor Beginn** einer Verarbeitung erteilt werden. Dies dürfte bei einer Verlinkung wie im Fall 2 nicht gewährleistet sein. Ein Pop-Up mit der Erklärung auch hier wäre daher sinnvoll. Auf die Einwilligung gegenüber Facebook kommt es nicht an, da der Betreiber der Seite – also die Einrichtung P – für die Erteilung der Hinweise nach dem EuGH verantwortlich ist.
Außerdem sollte vorsorglich auch in der Homepage ein Zusatz bezüglich der Verarbeitung im Rahmen der Facebook-Seite mit Hinweisen zur Nutzung von Facebook aufgenommen werden.

DR. KOCH

Das sind die sonstigen neuen Pflichten für Unternehmen Art. 24 ff. DSGVO

- **Dokumentationspflicht** (ggf. mit **Datenschutzfolgeabschätzung**);
- Umsetzung von technischen und organisatorischen Maßnahmen zum Datenschutz:
  - **„Datenschutz by Design“**: Sicherstellung des Datenschutzes durch technische Maßnahmen. Dazu sind interne Maßnahmen und Strategien im Unternehmen **festzulegen** und **nachzuweisen**;
  - **„Datenschutz by Default“**: Einhaltung der Anforderung zu datenschutzfreundlichen Voreinstellungen;
  - **Beispiele:** Trennung der Daten nach Verarbeitungszweck, Verarbeitung nur der erforderlichen Daten, Zugriffsschutz Anonymisierung und Pseudonymisierung der Daten, Verschlüsselte Kommunikation, Zertifizierungen

DR. KOCH

Das sind die sonstigen neuen Pflichten für Unternehmen Art. 24 ff. DSGVO

- **Meldepflichten** bei Datenpannen gegenüber der Aufsichtsbehörde (binnen 72 Stunden) und gegenüber den betroffenen Personen (unverzüglich);
- **Monatsfrist:** Machen Betroffene ihre Rechte auf Auskunft, Berichtigung, Löschung usw. geltend, muss der Verantwortliche „unverzüglich“ tätig werden und hat längstens eine Reaktionszeit von 1 Monat.
- **Konsultation** der Aufsichtsbehörde oder des Datenschutzbeauftragten

DR. KOCH

Das sind die (neuen???) Rechte der Betroffenen Art. 15 ff DSGVO

- Auskunft
- Löschung
- Recht auf Vergessenwerden
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Recht auf Einschränkung der Verarbeitung

DR. KOCH

Datenerhebung

Das BDSG verbietet grundsätzlich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, erlaubt diese aber unter bestimmten Voraussetzungen (Verbot mit Erlaubnisvorbehalt). § 9 Abs. 1 EU-DSGVO regelt gleiches Für Gesundheitsdaten!!!

Datenerhebung insbesondere von Gesundheitsdaten ist somit zulässig, wenn sie …

durch das BDSG/EU-DSGVO 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.

DR. KOCH

Datenverarbeitung

Erheben

Beschaffen von Daten:

- Die Daten sind direkt beim Betroffenen zu erheben *(Grundsatz des Vorrangs der Direkterhebung)*.
- Dadurch kann der Betroffene im Sinne des informationellen Selbstbestimmungsrechts die Datenerhebung maßgeblich beeinflussen.

Verarbeiten

Umgang mit den Daten in der Praxis:

- Speichern
- Verändern
- Übermitteln
- Sperren
- Löschen

Nutzen

Jede sonstige Verwendung, z. B.

- zur Korrespondenz mit dem Betroffenen
- Duplizieren, kopieren
- Auswertungen
- zur Information des Betroffenen über das Vorhandensein von Daten
- Übersendung zur Auftragsdatenverarbeitung sowie Rückgabe nach derselben

DR. KOCH

Zweckbindung bedeutet:

(1) Personenbezogene Daten ….dürfen von der verantwortlichen Stelle **nur für den Zweck** verarbeitet oder genutzt werden, für den sie sie erhalten hat….

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.(§3a BDSG)

DR. KOCH

Erforderlichkeit bedeutet

Rechtsprinzip (auch BDSG), das allgemein zum Ausdruck bringt, dass Maßnahmen, die in die Rechte des Betroffenen eingreifen, voraussetzen, dass die Maß-nahmen unabdingbar sein **müssen, um einen bestimmten Zweck zu erreichen.**

Es steht keine gleichermaßen wirksame Maßnahme zur Verfügung, mit der der angestrebte Zweck erreicht werden kann.

Damit genügt es nicht, dass die Datenerhebung eine grundsätzlich dienliche oder „brauchbare" Maßnahme ist.

DR. KOCH

Erforderlichkeit der Datenverarbeitung

***Fall**: Im Rahmen einer ärztlichen Aufnahmeuntersuchung wird dem A im Rahmen der allgemein anamnestischen Untersuchung wird auch eine Blutprobe entnommen. Dies Blutprobe wird ohne Einwilligung des A als „Serviceleistung" auch auf den HIV-Virus untersucht. A ist empört und hält diese Untersuchung für rechtswidrig. - Zu Recht. Die Untersuchung einer Blutprobe auf das HIV-Virus stellt einen Eingriff in das informationelle Selbstbestimmungsrecht dar. An einem Anlass zu einer solchen Untersuchung bestehen ebenfalls Zweifel. Ferner braucht der A auch in die Entnahme der Blutprobe nicht einzuwilligen, aber doch zur Feststellung des allgemeinen körperlichen Befindens als allgemein anamnestische Maßnahme stets erforderlich ist. Dies gilt aber nicht für die Vornahme des HIV-Tests, für den keine ausdrückliche Einwilligung vorlag, da der Untersuchungsauftrag beschränkt war, also nicht etwa der Verdacht nahelag, die Erkrankung AIDS würde zwingend einen anderen Umgang mit A zur Folge haben. Zudem bestünden erhebliche Bedenken bezüglich der Angemessenheit der Untersuchung der Blutprobe auf den HIV-Virus auch deshalb, weil hier doch sehr intensiv in die Intimsphäre des Betroffenen A eingegriffen wird. Mithin war die Erhebung zur Aufgabenerfüllung nicht erforderlich und A hat einen Anspruch auf Löschung der diagnostisch erhobenen Daten.*

DR. KOCH

Sparsamkeit bedeutet

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, **so wenig personenbezogene Daten wie möglich** zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Gesundheitsdaten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. (§48 BDSG n. F.). Gesundheitsdaten müssen außerdem getrennt von anderen Daten gespeichert werden, verschlüsselt werden, spezifische Regeln zur Verarbeitung festgelegt werden und die an der Verarbeitung Beteiligten sensibilisiert werden (§ 48 BDSG).

DR. KOCH

Zulässigkeit einer Übermittlung

Fall: **Der Kostenträger verlangt von einem Pflegedienst die Übermittlung der Qualifikationsdaten der eingesetzten Pflegekräfte im Rahmen der Wachkomabetreuung. Sofern Voraussetzung für die abgerechnete Fallpauschale auch die Qualifikation der Mitarbeiter ist – zu Recht.**

Problem: **Es handelt sich insoweit um personenbezogene Daten der Mitarbeiter. Hierfür ist daher eine Einwilligung in die Datenerhebung, -speicherung und –übermittlung im Rahmen des Arbeitsverhältnisses durch den betroffenen Arbeitnehmer erforderlich.**

DR. KOCH

Betroffenenrechte

Unternehmenspflicht zur Auskunft und zur Wahrung der Betroffenenrechte gemäß §55-58 BDSG n. F.

Information bei Erhebung oder Benachrichtigung bei Speicherung

Betroffener  **Unternehmen**

Benachrichtigung
Auskunftsrecht
Berichtigungsanspruch
Löschungsanspruch
Sperrungsanspruch

DR. KOCH

Betroffenenrechte

Fall: *Der Ehemann einer ehemaligen Patientin rügt, dass das Ehepaar auf ausdrücklichen Wunsch seiner Ehefrau von einer privaten Tagesklinik bei der ein ehemaliger Krankenhausarzt nunmehr als Geschäftsführer und Arzt tätig ist Werbematerial übersandt bekommen hat. Er verlangt die Löschung der über seine Ehefrau gespeicherten Namen und Anschrift. Im Krankenhaus hatte seine Ehefrau in einer Einwilligungserklärung nach § 51 BDSG n. F. auch in die Übermittlung an nicht näher bezeichnete Dritte eingewilligt. - Wohl zu unrecht. Zwar mag die Einwilligungserklärung wegen der nicht näheren Bezeichnung der Dritten zu pauschal und damit unwirksam sein, aber sie ist die Betroffene der Datenverarbeitung und allein ihr steht der Löschungsanspruch auch zu, nicht dem Ehemann.*

DR. KOCH

Auftrags-(daten-)verarbeitung

5

DR. KOCH

Cloud als neue Betriebsform

DR. KOCH

Weltweite Rechenzentren

- Automatische Auswahl der Rechenzentren und Provisionierung
- Geo redundante Datenhaltung
- Zertifizierung der Rechenzentren durch CyberTrust

Update: Microsoft wird ein Rechenzentrum in Deutschland einrichten.

DR. KOCH

Office 365

Fall: *Ein Dienstleister möchte einen Care-Net Dienst einrichten, durch den ältere Menschen im Bedarfsfall über Tablet-Bedienflächen ihren Pflegedienst, den Arzt usw. über Hilfsituationen informieren können. Das Tablett nutzt die Office 365 Apps.*

Bei Einsatz von Office 365 wird bei der Installation bei Anwendung der Standardeinstellungen die Streaming- und Virtualisierungstechnik genutzt, so dass für eine Nutzung der Anwendung der Produktdownload nicht abgeschlossen sein muss. Die Standardrichtlinieneinstellungen der Software bewirken zudem, dass die Cloud Speicherorte von Microsoft als vertrauenswürdig eingestuft werden.

Die Richtlinieneinstellungen und die Roamingeinstellungen müssen angepasst werden, um eine Speicherung von Dateien im Ausland zu verhindern, teilweise sind sie zu deaktivieren, teilweise bedarf es der Anpassung von Gruppenrichtlinien, um den Speicherort zu verändern.

Bei der Office 365 ProPlus Anwendung lässt sich auch die Virtualisierungstechnik abschalten und eine Offline Installation durchführen.

Update*: Microsoft betreibt für seinen Cloud-Dienst „OneDrive“ein Rechenzentrum in Deutschland welches bei Bezug der Software über Microsoft Deutschland genutzt wird. Die Lizenzgebühren sind allerdings teurer. Auf die Version achten.*

DR. KOCH

Übermittlung ins Ausland (§ 78 BDSG n. F.)

- **Zulässig nur, wenn hinreichendes Datenschutzniveau sichergestellt ist**
  - Unproblematisch bei Übermittlung innerhalb der EU/EWR
  - Datenübermittlung in Ländern mit verbindlicher Feststellung eines hinreichendes Datenschutzniveaus durch die Kommission (z. B. Schweiz, Kanada) durch einen Angemessenenbeschluss
  - USA: Safe-Harbor-Lösung
  - Sicherstellung durch Vertragsgestaltung (Hinreichende Sanktionierung)

DR. KOCH

DV außerhalb des EU-/EWR-Raumes

- Clouds außerhalb EU-/EWR-Raum sind generell unzulässig Optionsmöglichkeit der räumlichen Einschränkung
- Ausnahmemöglichkeit bei festgestellter Angemessenheit des DS-Niveaus (§ 4b II 2, 3 BDSG): CH, CN, Argent.
- Safe-Harbor-Selbst-Zertifizierung von US-Unternehmen genügt nicht
- EU-Standardvertragsklauseln zur DViA (Art. 26 II EU-DSRL)
- Analog Binding Corporate Rules (BDRs)

DR. KOCH

1. Hintergrund: Warum ist dies kritisch?

Die Datenweitergabe an den Dienstleister ist der kritische Prozess, weil eine Datenweitergabe Im Krankenhaus/Seniorenheim besonders sanktioniert ist.

Es besteht eine besondere Pflicht für diese Arbeitsphase – die unbefugte Weitergabe ist strafbar.

= „ärztliche Schweigepflicht“ § 203 StGB

DR. KOCH

1. Hintergrund: Wer sind Geheimnisträger?

Einer vergleichbaren Geheimhaltungspflicht unterliegen alle in § 203 StGB aufgezählten Personengruppen:

1. Arzt, Zahnarzt, Tierarzt, Apotheker, Heilberufsangehöriger
2. Berufspsychologen
3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen
5. Schwangerschaftsabbruchsberater, anerkannte Sozialarbeiter
6. Angehörige eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle

Fall: In einem Arbeitsgerichtsprozess reicht eine Altenpflegerin ein ärztliches Attest zum Unterlassen der Mobilisierung eines Bewohners beim Arbeitsgericht ungeschwärzt ein, welches die Behandelnde Ärztin für den Betreuer zur Beschaffung von Bettgittern zur Vorlage beim Amtsgericht für den Bewohner erstellt hat. Zulässig?

DR. KOCH

Die „Auftragsdatenverarbeitung“ nach dem jetzigen BDSG wird zur Auftragsverarbeitung

- Früher: „***Auftragsdatenverarbeitung***“ nach BDSG ist Datenverarbeitung im Auftrag und auf Weisung durch einen Auftragnehmer; der Auftraggeber bleibt dabei der allein Verantwortliche.

- Neu: Es ist nur noch ein **Auftragsverhältnis** bezüglich der Datenverarbeitung erforderlich und darauf, ob der Auftragsnehmer dabei weisungsgebunden arbeitet oder nicht, kommt es nicht mehr an. Auch Auftragnehmer haftet jetzt.

DR. KOCH

Die „Auftragsdatenverarbeitung“ nach dem jetzigen BDSG wird zur Auftragsverarbeitung

- **Beispiele:**
  - Speicherung Patientendaten in der Cloud – Nutzung Abrechnungsservice ohne Forderungs-Factoring
  - Lohnbuchhaltung in der Cloud oder Lohnbuchhaltung durch Lohnbüro;
  - Nutzen einer CRM-Anwendung in der Cloud;
  - Versendung von Newslettern und Mailings über einen Cloud-Anbieter;
  - Nutzen eines externen Call-Centers für den Kundenservice;
  - Nutzen eines Anrufdienstes für eingehende Anrufe;
  - Durchführung von Gewinnspielen über eine externe Agentur;
  - Managed Hosting von Webseiten/Onlineshops

DR. KOCH

Apotheke und Ärzte in den Einrichtungen

Fall: *Die Einrichtung P bezieht die Medikamente für seine Bewohner bei der Apotheke A. Außerdem werden in erheblichen Umfang Patienten Bewohner der Einrichtung in erheblichen Umfang durch den Arzt B ärztlich versorgt. Die Einrichtung P ist der Auffassung, dass A und B als Auftragsverarbeiter tätig werden und verlangt von diesen jeweils den Abschluss eines Auftragsverarbeitungsvertrages. Zu Recht?*

Nein: Die Apotheke A hat soweit Sie Medikamente für einzelne Bewohner bereitstellt, anders als im Krankenhaus, eine eigene Vertragsbeziehung zu dem jeweiligen Bewohner. Gleiches gilt für den Arzt B, der die Bewohner gleichfalls auf der Grundlage eines eigenen Behandlungsvertrages versorgt. Eine Auftragsverarbeitung liegt nicht vor. Dies bedingt auch, dass A und B nicht in die Verarbeitung von Daten der P einbezogen sind. Die P benötigt daher einer gesonderten Einwilligung, um Bewohnerdaten an die A oder den B übermitteln zu können.

DR. KOCH

Pflegesatzverhandlungen für Einrichtungen

Fall: *Die Einrichtung P beauftragt den Servicedienstleister A mit der Führung von Pflegesatzverhandlungen. Hierfür übermittelt sie an den Servicedienstleister eine nicht anonymisierte Personalliste ihrer Beschäftigten. Die Einrichtung P ist der Auffassung, dass A als Auftragsverarbeiter tätig werden und verlangt von diesen jeweils den Abschluss eines Auftragsverarbeitungsvertrages. Zu Recht?*

Nein: Für die Führung von Pflegesatzverhandlungen ist im Regelfall – Ausnahme Verhandlung von Ausbildungszuschüssen – keine nicht anonymisierte Personalliste erforderlich. Um eine nicht anonymisierte Personalliste an die Servicegesellschaft A übermitteln zu können, benötigt die P daher einer gesonderten Einwilligung ihrer Mitarbeiter, da diese Übermittlung nicht erforderlich ist. Da die Servicegesellschaft A für die Pflegesatzverhandlungen keine personenbezogenen Daten der Mitarbeiter benötigt und zudem auch nicht für die P verarbeitet, ist sie auch kein Auftragsverarbeiter.

Datenschutzbeauftragter usw.

6

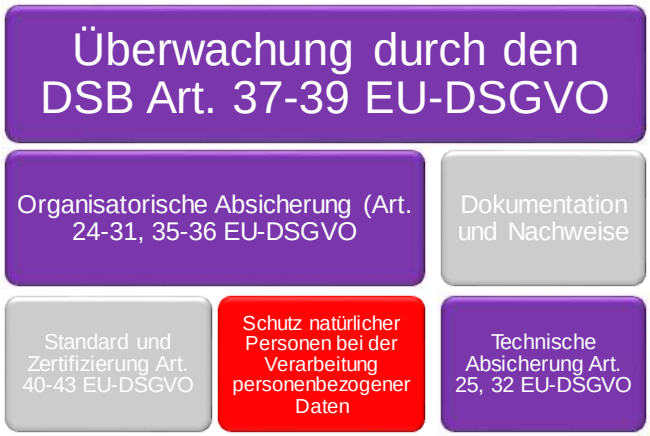
Der Datenschutzbeauftragte

- **Bis 25.05.2018:** Muss u. a. bestellt werden, wenn 9 Personen personenbezogene Daten **automatisiert verarbeiten** oder weniger als 20 Personen personenbezogene Daten nicht-automatisiert verarbeiten;
- **Neu:** DSB ist zu bestellen (**egal ob automatisiert oder nicht**), wenn zu den Kernaktivitäten des Unternehmens
  - die umfangreiche und sytematische Überwachung von Betroffenen oder
  - die umfangreiche Verarbeitung **sensitiver Daten** (Gesundheitsdaten z. B. Patienten/Betreute/Bewohner) zählt

=> Aber: Ab 10 Mitarbeitern muss ein DSB bestellt werden, wenn die personenbezogenen Daten elektronisch verarbeitet werden (§ 38 Abs. 1 S. BDSG n. F.) **=> Widerspruch zu Art. 4 Abs. 2 EU-DSGVO**

DR. KOCH

Schutzkonzept des Datenschutzes durch den DSB



DR. KOCH

Betrieblicher Datenschutzbeauftragter

Datenschutzbeauftragter – Anforderungen

- Fachkunde
- Zuverlässigkeit

Pflichten:

- Den gesetzlichen Regelungen unterworfen & zur Verschwiegenheit verpflichtet
- Zusammenarbeitsgebot mit dem Betriebsrat
- Zusammenarbeit erwünscht mit den angrenzenden Fachstellen (CISO, CIO, interne Revision, Risikomanagement etc.)
- Recherchen zur aktuellen Rechtslage
- Lesen und Auswerten von Fachartikeln, Weiterbildungsmaßnahmen
- Datenschutzaudit (per Gesetz ab 2009) durchzuführen
- Zentraler Ansprechpartner für alle Datenschutz-relevanten Themen

DR. KOCH

Betrieblicher Datenschutzbeauftragter

Datenschutzbeauftragter – Rechte

- Weisungsfreiheit
- Direkt der Geschäftsführung unterstellt, Management Commitment
- Vom Unternehmen durch „Hilfspersonal, Räume, Einrichtungen, Geräte und Mittel“ zu unterstützen
- Aktives und passives Informationsrecht
- Zugangsrecht zu Gebäuden und Räumen
- Benachteiligungsverbot (Besonderer Kündigungsschutz für interne Datenschutzbeauftragte und ausreichende Vertragslaufzeit (mindestens 3 Jahre) für externe Datenschutzbeauftragte
- Akten und andere Schriftstücke unterliegen Beschlagnahmeverbot
- Aufsichtsbehörde als zentraler Ansprechpartner verfügbar

DR. KOCH

Betrieblicher Datenschutzbeauftragter

Datenschutzbeauftragter – Aufgaben

- Koordination aller Datenschutz-relevanten Tätigkeiten im Unternehmen
- Hinwirken auf die Einhaltung datenschutzrechtlicher Vorschriften
- Überwachung der automatisierten Verarbeitung, bei welcher personenbezogene Daten verarbeitet werden (Datenschutzaudit)
- Datenschutzrechtliche und –technische Schulung und Sensibilisierung der Personen, die personenbezogene Daten erheben, verarbeiten oder nutzen
- Durchführung von Vorabkontrollen
- Beratung des Unternehmens bei datenschutzrechtlichen Fragen
- Vertretung des Unternehmens in Gesprächen mit Aufsichtsbehörden
- Aktive Pflege des Verfahrensverzeichnis
- Ansprechpartner für Betroffene

DR. KOCH

Betrieblicher Datenschutzbeauftragter

Fall (die säumige Pflegeeinrichtung): Die Pflegeeinrichtung P hat den Dienstleister H mit der Wahrnehmung der Aufgaben als Datenschutzbeauftragter beauftragt. Der Dienstleister H möchte zur Wahrnehmung seiner Aufgaben den Ist-Bestand vor-Ort feststellen. Die Einrichtung P weigert sich die Pauschale zu bezahlen.

H will den Vertrag kündigen und verlangt von P die Bestellung zum Datenschutzbeauftragten zu widerrufen, da er seine Aufgaben nicht wahrnehmen könne.

Zu Recht: Ohne Feststellung des datenschutzrechtlichen Ist-Zustandes ist die Wahrnehmung der Beratungsaufgaben als Datenschutzbeauftragter nicht möglich. Sollte P die Bestellung nicht widerrufen und auch nicht bezahlen, kann H dem Landesdatenschutzbeauftragten mitteilen, dass der Dienstleistungsvertrag fristlos gekündigt worden sei und er das Amt niederlege. Von P kann H die Löschung der Benennung als DSB in der Datenschutzerklärung verlangen.

DR. KOCH

Verzeichnis von Verarbeitungstätigkeiten Art. 30 DSGVO

- Verantwortlicher (Abs.1): „Verzeichnis aller Verarbeitungstätigkeiten"
- Auftragsverarbeiter (Abs.2): "Im Auftrag durchgeführten Tätigkeiten ..."
- Nicht öffentlich / Einsicht für Aufsichtsbehörden (auf Anfrage)
- Dokumentation ähnlich Verfahrensverzeichnis
- Zusätzlich aufzunehmen: Beurteilung und Garantien bei Drittlandsübermittlungen gemäß Art. 49 Abs. 1 Unterabs. 2
- Ausnahmen für Unternehmen unter 250 MA – häufig nicht einschlägig
- **Achtung:** Daneben bestehen weitere Dokumentationspflichten

DR. KOCH

Datenerhebung nicht beim Betroffenen

- **Bis 25.05.2018:** Grundsatz der Direkterhebung beim Betroffenen (vgl. § 4 Abs. 2 BDSG), Ausn.: gesetzliche Erlaubnis, Erforderlichkeit der Datenerhebung ohne Mitwirken des Betroffenen wegen Geschäftszweck, unverhältnismäßiger Aufwand der Direkterhebung;
- **Neu:** Für die Erhebung der Daten nicht direkt beim Betroffenen muss kein besonderer Grund mehr vorliegen. Aber:
- Informationspflicht nach Art. 14 DSGVO u.a. darüber,
  - welche Daten
  - wo erhoben werden

DR. KOCH

Widersprüche zwischen EU-DSGVO und BDSG n.F.

Es bestehen insbesondere folgende Abweichungen zur EU-DSGVO:

- **EU-DSGVO gilt für jede Verarbeitung personenbezogener Daten (Rdn. 22 EU-DSGVO), das BDSG gilt hingegen gem. § 1 Abs. 1 BDSG n. F. nur für automatisierte Verarbeitung.**
- **Einschränkung der Informationspflicht nach Art. 13, 14 EU-DSGVO bei Unmöglichkeit, unverhältnismäßigem Aufwand, Verarbeitungsziele würden unmöglich oder ernsthaft beeinträchtigt.**
- **§ 4 BDSG n. F. schränkt die Möglichkeit der Videoüberwachung im Verhältnis zur EU-DSGVO im privaten Bereich ein, und erweitert die Überwachungsmöglichkeiten im öffentlichen Bereich.**
- **Datenschutzbeauftragter ist gemäß § 38 BDSG n. F. auch zukünftig bei Beschäftigung von 10 Personen in der Verarbeitung personenbezogener Daten.**
- **Regelungen in §§57-72 BDSG n. F. zur Auftragsdatenverarbeitung trotz bestehendem Wiederholungsverbot.**
- **Beschäftigtendatenschutz in § 23 BDSG n. F. weicht von Art. 88 Abs. 2 DSGVO ab.**

DR. KOCH

Die EU-ePrivacy-Verordnung (EU-ePriv-VO)

- Die EU-ePriv-VO konkretisiert und ergänzt die EU-DSGVO, insoweit in der EU-ePriv-VO die Verarbeitung personenbezogener Daten geregelt ist (Art 1 Abs. 3 EU-ePriv-VO).
- Die Regelungen im TKG und TMG, die auf der EU-ePrivacy-Richtlinie basieren, werden durch die entsprechenden Regelungen der EU-ePriv-VO verdrängt.
- Einige Regelungen gelten nur für die Telekommunikationsbranche, andere Regelungen (z.B. zu Cookies und zu werblichen Ansprache per elektronischer Medien) gelten für alle Unternehmen!
- Die auf der EU-ePrivacy-Richtlinie basierenden Regelungen zur werblichen Ansprache per elektronischer Kommunikation (Telefon, FAX, E-Mail, SMS, ...) im § 7 UWG werden – im Anwendungsbereich der EU-ePriv-VO – durch deren Regelungen verdrängt.
- Die in Deutschland durch § 7 Abs. 3 UWG umgesetzten Regelungen zur vereinfachten Erlaubnis zur Nutzung von E-Mail-Adressen (oder SMS-Nummern) für eigene Werbezwecke, wenn die dortigen Bedingungen erfüllt sind, bleiben grundsätzlich erhalten (Art. 16 Abs. 2 EU-ePriv-VO).

DR. KOCH

Beschäftigtendatenschutz § 26 BDSG n. F.

- Gemäß der zum 1. 9. 2009 in Kraft getretenen Bestimmung des § 32 Absatz 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach dessen Begründung für seine Durchführung oder Beendigung erforderlich ist (vgl. BAG Urt. v. 20.06.2013 – 2 AZR 546/12 – Rdn. 23; Urt. v. 12.02.2015 – 6 AZR 845/13 – Rdn. 70).
- Nach der Gesetzesbegründung sollte die Regelung des § 32 BDSG die bislang von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen (vgl. BAG Urt. v. 20.06.2013 a.a.O. Rdn. 26).
- Durch § 32 Absatz 2 BDSG wird die grundsätzliche Beschränkung der Anwendung des dritten Abschnitts des Bundesdatenschutzgesetzes auf dateigebundene bzw. automatisierte Verarbeitungen (§ 1 Absatz 2 Nr. 3, § 27 Absatz 1 BDSG) ausdrücklich aufgehoben (so BAG Urt. v. 12.02.2015 a.a.O. Rdn. 72).
- § 26 Abs. 1 S. 1 BDSG n. F. entspricht weitgehend der bisherigen Regelung des § 32 Abs. 1 S.1 BDSG.
- Eine Einwilligung in die Datenerhebung, -verarbeitung und -nutzung gemäß § 4 a BDSG im Arbeitsverhältnis ist grundsätzlich zulässig. Weder kann dem Gesetz selbst ein genereller Ausschluss der Erteilung einer Einwilligung im Arbeitsverhältnis entnommen werden, noch impliziert das strukturelle Machtungleichgewicht zwischen Arbeitnehmer und Arbeitgeber per se, dass jede Einwilligung des Arbeitnehmers unfreiwillig wäre, da der Arbeitnehmer auch im Arbeitsverhältnis frei über seine informationelle Selbstbestimmung entscheiden könne (so OVG Saarlouis Urt. v. 14.12.2017 – 2 A 662/17; BAG Urt. v. 11.12.2014 – 8 AZR 1010/13 – Rdn. 32). Dies wird von Landesdatenschutzbeauftragten abweichend gesehen, die eine wirksame Einwilligung im Arbeitsverhältnis generell ablehnen (https://www.lda.bayern.de/media/dsk_kpnr_14_beschaeftigtendatenschutz.pdf) und nur bei einem Vorteil für möglich erachten (z. B. Dienstwagenregelung usw.).

DR. KOCH

Vorgaben für IT-gestützte Prozesse

7

DR. KOCH

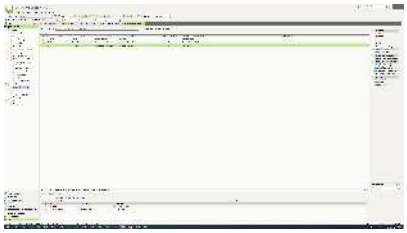
Festlegungen für IT gestützte Prozesse § 22 BDSG n. F.

- **Festlegungen des Bundesfinanzministeriums zum Führen von Büchern sowie zum Datenzugriff GoBD v. 14.11.2014 in Kraft getreten zum 01.01.2015. Diese Vorgaben entsprechen § 22 Abs. 2 BDSG n. F. für besondere personenbezogene Daten iSv § 46 Abs. 14, § 48 Abs. 2 BDSG n. F. und sind ab 25.05.2018 zu beachten.**
- **Vorgaben zu IT-gestützten steuerrelevanten Prozessen seit dem 01.01.2015 mit Vorgaben zu:**
  - **Datensicherheit – Daten sind gegen Verlust und unberechtigten Zugriff zu sichern (Verschlüsselung) und von anderen Daten zu trennen.**
  - **Unveränderbarkeit – Daten dürfen nicht ohne entsprechende Kenntlichmachung überschrieben, verändert oder ersetzt werden.**
  - **Ordnungsmäßigkeit - alle buchungsrelevanten Daten, Aufzeichnungen und Vorgänge müssen nachvollziehbar, nachprüfbar, vollständig, richtig, zeitgerecht/zeitnah, geordnet und unveränderbar sein**
  - **Aufzeichnungspflicht - alle relevanten Geschäftsvorfälle müssen in zeitlicher Reihenfolge und in sachlicher Gliederung darstellbar sein; zudem müssen auch alle zusätzlich notwendigen Tabellendaten, Historisierungen und Programme gespeichert werden**
  - **Aufbewahrungspflicht - aufbewahrungs- und aufzeichnungspflichtige Daten, Datensätze, elektronische Dokumente sowie elektronische Unterlagen sind geordnet und grundsätzlich im Original – also etwa auch in ihrem elektronischen Ursprungsformat – aufzubewahren**

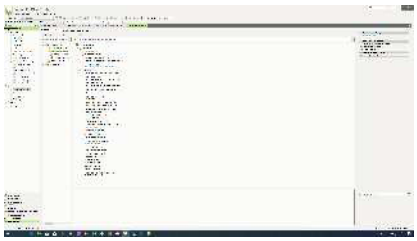
DR. KOCH

Festlegungen für IT gestützte Prozesse § 22 BDSG n. F.

- **Zugriff nur für in der Anwendung eingetragene Benutzer der Domäne**



- **Festlegung in der Dokumentenmanagement Software (DMS) wer hat Zugriff auf was**



DR. KOCH

Sicherheit der Verarbeitung – Art. 32 DSGVO

- Angemessen, unter Beachtung insbes. des „Stands der Technik", Risikoadäquat
- Fokussierung auf die IT-Sicherheitsziele:

  Vertraulichkeit

  Integrität

  Verfügbarkeit
- Sicherheitsmanagement

Durch die Dienstleister müssen ausreichende Nachweise zur Verfügung gestellt werden können

DR. KOCH

Kontrollmaßnahmen Art. 32 EU-DSGVO früher § 9 BDSG

Zutrittskontrolle

Unbefugten ist der "körperliche" Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

Zugangskontrolle

Trennungsgebot

§ 9 BDSG

Eingabekontrolle

Auftragskontrolle

Zugriffskontrolle

Weitergabekontrolle

Dr. Koch - Rechtsanwalt

121

DR. KOCH

Kontrollmaßnahmen Art. 32 EU-DSGVO früher § 9 BDSG

Zutrittskontrolle

Verfügbarkeitskontrolle

Zugangskontrolle

Verhinderung der unbefugten Nutzung von Datenverarbeitungsanlagen, also dem Eindringen in das EDV-System seitens unbefugter (externer) Personen sowie die geregelte Zugangskontrolle eines grundsätzlich Berechtigten.

Trennungsgebot

Eingabekontrolle

Auftragskontrolle

Zugriffskontrolle

Weitergabekontrolle

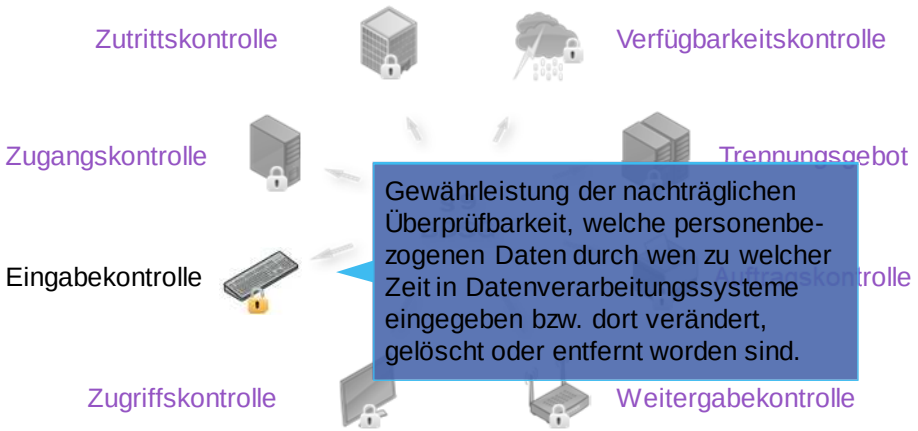
Dr. Koch - Rechtsanwalt

122

DR. KOCH

Pflichten des Unternehmens

Kontrollmaßnahmen Art. 32 EU-DSGVO früher § 9 BDSG

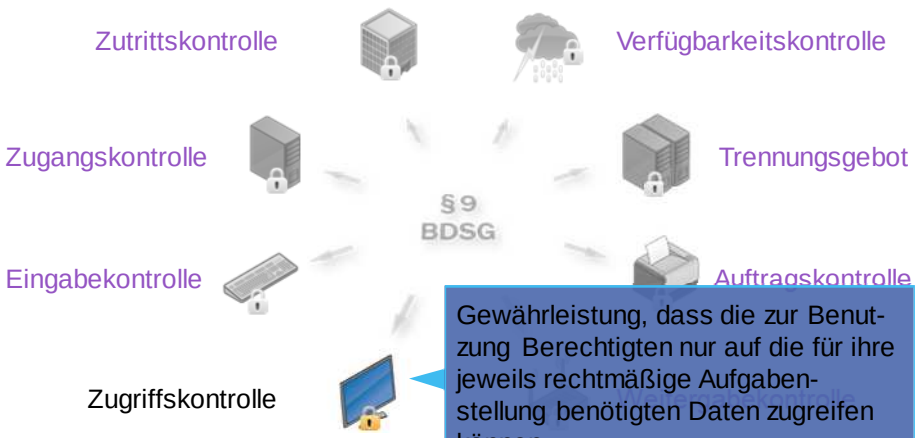


Gewährleistung der nachträglichen Überprüfbarkeit, welche personenbezogenen Daten durch wen zu welcher Zeit in Datenverarbeitungssysteme eingegeben bzw. dort verändert, gelöscht oder entfernt worden sind.

DR. KOCH

Pflichten des Unternehmens

Kontrollmaßnahmen Art. 32 EU-DSGVO früher § 9 BDSG

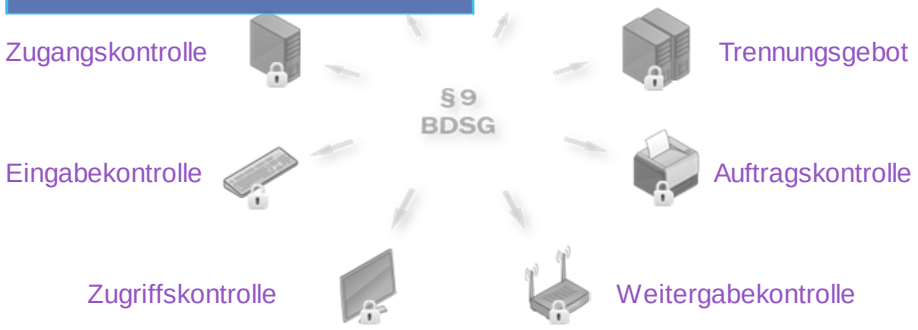


Gewährleistung, dass die zur Benutzung Berechtigten nur auf die für ihre jeweils rechtmäßige Aufgabenstellung benötigten Daten zugreifen können.

DR. KOCH

Kontrollmaßnahmen Art. 32 EU-DSGVO früher § 9 BDSG

Die **Verfügbarkeitskontrolle** zielt auf den Schutz vor zufälliger Zerstörung ab, wie z.B. Wasserschäden, Brand, Blitzschlag, Stromausfall.



Dr. Koch - Rechtsanwalt

125

DR. KOCH

Kontrollmaßnahmen Art. 32 EU-DSGVO früher § 9 BDSG

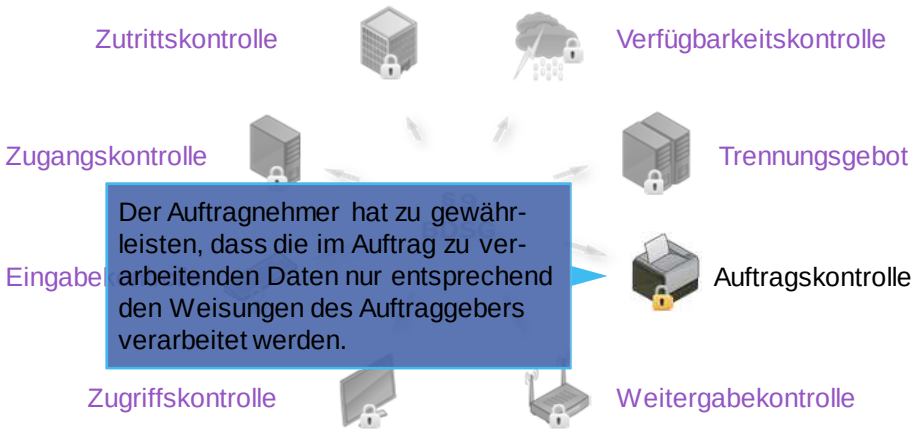
Technische Sicherstellung der zweckbestimmten Verarbeitung von persönlichen Daten. Gemeint ist damit zumindest eine logische Trennung

Dr. Koch - Rechtsanwalt

126

DR. KOCH

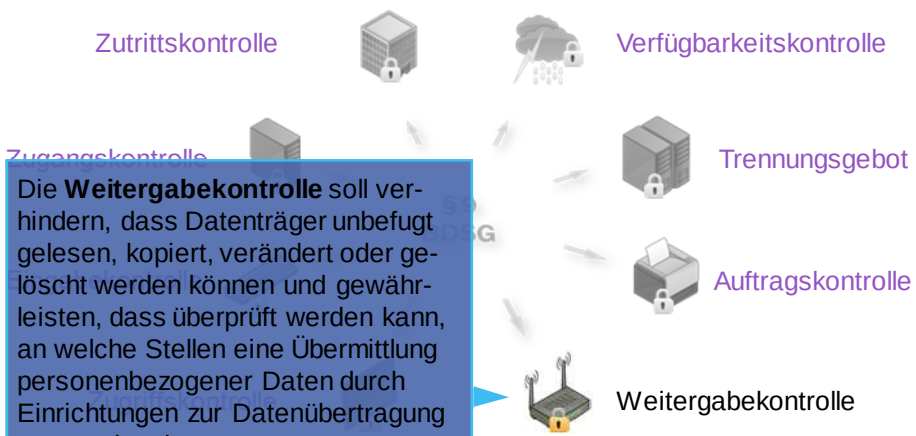
Kontrollmaßnahmen Art. 32 EU-DSGVO früher § 9 BDSG



Der Auftragnehmer hat zu gewährleisten, dass die im Auftrag zu verarbeitenden Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

DR. KOCH

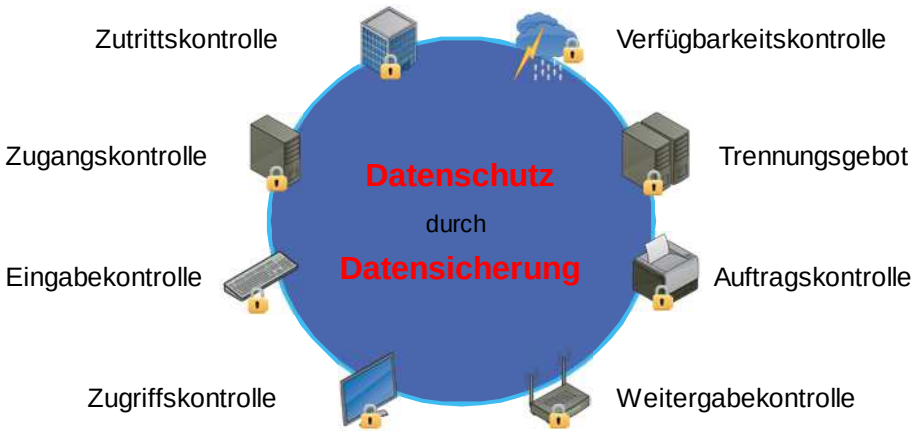
Kontrollmaßnahmen Art. 32 EU-DSGVO früher § 9 BDSG



Die **Weitergabekontrolle** soll verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder gelöscht werden können und gewährleisten, dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

DR. KOCH

Kontrollmaßnahmen Art. 32 EU-DSGVO früher § 9 BDSG



DR. KOCH

Datenschutzfolgenabschätzung – Art. 35 DSGVO

Art. 35

Abs. 7 Die Folgenabschätzung enthält zumindest Folgendes:

a. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen;

b. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Ausreichende Dokumentationen hierzu müssen vorhanden sein

DR. KOCH

Dokumentations- und Nachweispflichten

- Art 28 Abs.3 a)
  - Dokumentierte Weisungen
  - Dokumentierte Weisung für Verarbeitung im Drittland
- Art 30: Verzeichnis von Verarbeitungstätigkeiten
- Art 33: Dokumentation aller Verletzungen des Schutzes personenbezogener Daten
- Art 47 Abs. 2: Dokumentation von Abwägungen und Garantien bei Drittlandübermittlungen
- Art 5 Abs. 2: Nachweis der Einhaltung der Verarbeitungsprinzipien
- Art 7 & 8: Nachweis der Einwilligung
- Art 12: Nachweis der Unbegründetheit des Antrags
- Art 21: Nachweis für die Erforderlichkeit der Verarbeitung
- Art 24: Nachweis für die rechtmäßige Verarbeitung
- Art 28: Nachweis im Rahmen der Kontrolle
- Art 35: Nachweis zur Einhaltung der DS-GVO (Folgenabschätzung)

Viele Dokumentationen und Nachweise müssen erbracht werden können

DR. KOCH

Anpassung der IT-Struktur

Was ist also genau zu tun?

- **Zuständigkeiten/Team** im Unternehmen festlegen (Datenschutzbeauftragter?), aber Haftung bleibt beim **Verantwortlichen!!!**
- **Ermittlung** der vorhandenen EDV-Struktur (Eingesetzte Programme, Verarbeitungsprozesse, Art der verwendeten Daten – personenbezogene Daten, besondere personenbezogene Daten, Feststellung des vorhandenen Berechtigungskonzeptes, Stand Datentrennung/-verschlüsselung) und derzeitiger Schutzlücken anhand eines Datenschutzaudits
- Der **Stand der Vorbereitung** auf die EU-DSGVO kann z. B. mit https://www.lda.bayern.de/tool/start.html in 28 Schritten geprüft werden.
- Festlegung eines **Umsetzungsplans** zur Durchführung notwendiger Anpassungen, Festlegung einer Zeitschiene mit Meilensteinen zur Kontrolle des Standes der Umsetzung (PDCA-Zyklus).

DR. KOCH

Umsetzung EU-DSGVO – ToDo‘s

8

DR. KOCH

Was ist zur Umsetzung der EU-DSGVO zu tun?

- **Analyse der aktuellen Situation um die zu erledigenden Punkte zu identifizieren**
- **Festlegung der zeitlichen Abläufe und Verantwortlichkeiten** in Bezug **auf die Umsetzung**
- **Beginn und Nachverfolgung der Umsetzung**
- **Beginnen Sie den Datenschutz im Unternehmen ernst nehmen!**
- **Ein (internes oder externes) Datenschutzaudit durchführen, um zu wissen, auf welchem Stand die Umsetzung des Datenschutzes im Unternehmen sich befindet.**

DR. KOCH

Vorbereitung der Umsetzung der EU-DSGVO

- **Da durch die EU-DSGVO die Datenschutzdokumentation wichtiger wird denn je (vgl. Art. 5 Abs. 2 EU-DSGVO), sollten alle datenschutzrelevanten Dokumente auf den aktuellen Stand (und bei der Gelegenheit mit Datum und Versionsnummer versehen) werden.**
- **Stellen Sie daher zur Vorbereitung einer Umsetzung folgende Unterlagen zum Ist-Zustand zusammen:**
  - **Netzwerkübersicht, Soft- und Hardwareübersicht**
  - **Internes Verfahrensverzeichnis**
  - **Datenschutzkonzept, -handbuch**
  - **Datenschutzrichtlinien inkl. Dokumentation der Verantwortlichkeiten**
  - **Dokumentation der bestehenden technischen und organisatorischen Maßnahmen**

DR. KOCH

Schritt 1: Auflistung aller Prozesse

Auflistung aller Prozesse im Unternehmen, in denen personenbezogene Daten erhoben und verarbeitet werden.

- CRM (Customer-Relationship-Management Software
- Newsletter-System
- Webseiten-Tracking (IP-Adresse!)
- Personal-Management-System
- Dienstplansoftware
- Abrechnungssystem
- Dokumentationssoftware Behandlung/Betreuung
- …

DR. KOCH

Schritt 1: Auflistung aller Prozesse

Es kommen umfangreiche Dokumentationspflichten auf Sie zu, die Sie bereits JETZT vorbereiten müssen!

- Bislang gab es im BDSG schon die (öffentlichen) Verfahrensverzeichnisse, zuständig war der Datenschutzbeauftragte.
- Jetzt neu: „**Verzeichnis von Verarbeitungstätigkeiten**“ (nicht mehr öffentlich)
- Neu: Zuständig ist der Verantwortliche, d.h. die **Unternehmensführung**

DR. KOCH

Schritt 1: Auflistung aller Prozesse

Dokumentationspflichten: Einschränkung für kleine Unternehmen mit < 250 Mitarbeitern, WENN (!!!)

- die von ihnen vorgenommene Verarbeitung **kein Risiko** für die Rechte und Freiheiten der betroffenen Personen birgt,
- oder die Verarbeitung **nur gelegentlich** erfolgt,
- oder **keine sensitive Daten** verarbeitet werden (z. B. Gesundheitsdaten, Daten aus Strafregistern ...)

Soweit Sie Gesundheitsdaten verarbeiten (Patienten/Betreute/ Bewohner) ist ein Verfahrensverzeichnis immer erforderlich!!!

DR. KOCH

Schritt 1: Auflistung aller Prozesse

Dokumentationspflichten: Was muss ins Verzeichnis?

- **Zweck** der Datenverarbeitung;
- Beschreibung der **Kategorien** der betroffenen Personen und der personenbezogener Daten;
- Kategorien von Empfängern, ggü. denen die **Daten offengelegt** wurden und noch werden (auch im Ausland)
- **Fristen** für die Löschung der Daten;
- Ggf. **Datenübermittlung in Drittstaaten**
- Beschreibung der **TOMs** (**T**echnische und **O**rganisatorische **M**aßnahmen) die die Datensicherheit gewährleisten
- . . .

DR. KOCH

Schritt 2: Vornahme Datenschutzfolgeabschätzung

Nehmen Sie eine Datenschutz-Folgenabschätzung VOR (!!!) der Aufnahme der Verarbeitung vor, wenn

... die Datenverarbeitung voraussichtlich ein hohes Risiko für die Betroffenen hat ...

- muss der Verantwortliche ein Abschätzung der Folgen vornehmen
- Gilt wahrscheinlich nicht für bereits bestehende **(rechtmäßige !!!)** Verarbeitungen (DSAnpUG-EU)

Beispiele:

- Systematische Bewertung der Persönlichkeit einschl. Profiling als Grundlage für Entscheidungen mit Rechtswirkung
- Verarbeitung von **sensitiven Daten** (Gesundheitsdaten usw).

=> Ambulante Pflegedienste, Pflegeeinrichtungen usw. also immer

DR. KOCH

Schritt 2: Vornahme Datenschutzfolgeabschätzung

Was muss rein?

- Beschreibung
  - des **Ablaufs und des Zwecks** der Verarbeitungsverfahren
  - der **Notwendigkeit und Verhältnismäßigkeit** der einzelnen Verarbeitungsverfahren
  - der **Risiken** für die Betroffenen
  - **Technische und Organisatorische Maßnahmen** zur Gewährleistung der Datensicherheit
- **Früher:** Vorab-Kontrolle nach BDSG

DR. KOCH

Schritt 2: Vornahme Datenschutzfolgeabschätzung

Konsultationspflichten

- Ggf. muss der Standpunkt der **Betroffenen** zu der beabsichtigten Verarbeitung eingeholt werden;
- Gibt es einen **Datenschutzbeauftragten**, ist dessen Rat bei Durchführung der Datenschutz-Folgenabschätzung einzuholen;
- Ergibt die Abschätzung ein hohes Risiko für die Betroffenen, ohne dass Maßnahmen zur Eindämmung des Risikos getroffen sind, ist die vor der Verarbeitung die **Aufsichtsbehörde** zu konsultieren.
- Bei **Meinungsverschiedenheiten** zwischen dem Verantwortlichen und den Datenschutzbeauftragten muss die Aufsichtsbehörde angerufen/konsultiert werden.

DR. KOCH

Schritt 3: Informationspflichten

Anpassung sämtlicher Rechtstexte wie Einwilligungstexte, Datenschutzinformationen, ggf. Allgemeine Geschäftsbedingungen oder sonstige Informationstexte (online, offline) in Bezug auf die Informationspflichten

- Verantwortlicher muss informieren über (siehe oben) ...
  - Zweck und Rechtsgrundlage der Datenverarbeitung;
  - ggf. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
  - Datentransfer in Drittstaaten einschließlich der Rechtsgrundlage
  - Speicherdauer;
  - Bestehen des Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs-, Widerspruchs- oder ggf. Widerrufsrecht sowie das Recht auf Übertragbarkeit der Daten und das Recht auf Beschwerde bei einer Aufsichtsbehörde
  - usw.

DR. KOCH

Schritt 4: Überprüfung der Erlaubnistatbestände und Einwilligungen

Das ist wichtig für eine wirksame Einwilligung

- **Nachweisbar** - also mit Protokollierung und Double Opt-In
- Betroffener muss bei Einwilligung (also im Onlineformular oder im Papierformular) darüber informiert werden,
  - dass er ein **Widerrufsrecht** hat
  - zu welchem **Zweck** die Datenverarbeitung erfolgt
  - wer der **Verantwortliche** ist
- nicht vorab angeklickte **Checkbox** oder Vertragsformulare ohne Auswahlmöglichkeit
  - Untätigkeit/Schweigen reicht nicht aus
- Nach den Erwägungsgründen dürfen „**Altdaten**“ über den 25.05.2018 hinaus weiter genutzt werden, wenn die Einwilligung **bereits bis zum 24.05.2018** nach den DSGVO-Anforderungen eingeholt wurden

DR. KOCH

Schritt 5: Überprüfung und Anpassung aller Auftragsverarbeitungsverträge

Auftragsdatenverarbeitung wird zur Auftragsverarbeitung

- Es ist nur noch ein **Auftragsverhältnis** bezüglich der Datenverarbeitung erforderlich und darauf, ob der Auftragsnehmer dabei weisungsgebunden arbeitet oder nicht, kommt es nicht mehr an. Auch Auftragnehmer haftet jetzt!!!
- **Früher:** „Funktionsübertragungen“ nach BDSG
- **Neu:** Entweder **Auftragsverarbeitung** mit ggf. erweiterten Zuständigkeiten für den Auftragsverarbeiter
- oder „**gemeinsame Verantwortung**“ mehrerer Stellen nach Art. 26 EU-DSGVO
  - entweder gleichberechtigt für einen gemeinsamen Bereich
  - oder jede verantwortliche Stelle ist eigenverantwortlich für einen eigenen Bereich zuständig

DR. KOCH

Schritt 5: Überprüfung und Anpassung aller Auftragsverarbeitungsverträge

Auftragsdatenverarbeitung wird zur Auftragsverarbeitung

- Verträge sind mit **neuen Pflichten und Technischen Organisatorischen Maßnahmen** (**TOM‘s**) zu aktualisieren, u. a:
  - Zusammenarbeit mit der Datenschutzaufsicht Unterstützung des Auftragsgebers
  - bei TOMs zur Datensicherheit
  - bei der Meldung von Datenpannen
  - bei der Durchführung von Folgenabschätzungen
  - …

DR. KOCH

Schritt 6: Einrichtung der Betriebsprozesse auf die Betroffenenrechte

Können Ihre jetzigen Prozesse das?

- Auskunftsrecht dazu, ob und welche personenbezogene Daten verarbeitet werden
- Berichtigungsrecht
- Löschungsrecht;
- Recht auf Vergessenwerden
- Recht auf Datenübertragbarkeit;
- Widerspruchsrecht
- …

DR. KOCH

Schritt 6: Einrichtung der Betriebsprozesse auf die Betroffenenrechte

Können Ihre jetzigen Prozesse das?

- Eingehende **Anträge** von Betroffenen müssen unverzüglich, in jedem Fall aber **innerhalb eines Monats** erledigt werden.
- Diese Frist kann um zwei Monate **verlängert** werden, wenn erforderlich ist. Dann müssen dem Betroffenen aber die Gründe für die Verzögerung mitgeteilt werden.
- Wird der Verantwortliche nicht tätig, ist der Betroffene spätestens innerhalb eines Monats über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen, zu **unterrichten**.
- **Anträge von Betroffenen** müssen als solche **erkannt** werden.

Schritt 6: Einrichtung der Betriebsprozesse auf die Betroffenenrechte

Können Sie eigentlich Löschen?

- In welchen **Systemen** befinden sich die Datensätze zu einem Betroffenen? Gibt es mehrere? Können alle gleichzeitig gelöscht werden?
- Gibt es Daten, die **nicht gelöscht** werden dürfen? – z.B. vertragliche Daten mit gesetzlichen Aufbewahrungsfristen?
- Sind alle Daten in allen Systemen **aktuell**, so dass Sie den Betroffenen überhaupt noch wiederfinden?

Do‘s und Dont‘s

9

DR. KOCH

Aktenarchive

- Fall (**Aktenvernichtung**): *Die Personalabteilung der Einrichtung H&H zieht in das neue Bürogebäude der Zentrale um und bestellt deshalb zwei verschließbare Aktencontainer des Aktenvernichters A. Nach Befüllung mit etwa 40 Personalakten werden die Container über Nacht auf dem Hof abgestellt. Am nächsten Morgen stellt die Personalabteilung fest, dass die Container gestohlen wurden. Angaben welche Akten gestohlen wurden, sind nicht möglich, da nicht protokolliert wurde, wessen Personalakten eingelegt wurden. Was war falsch?*
  - Der Zugang zum Archiv ist zu protokollieren (Revisionsfähigkeit).
  - Entnommene Unterlagen sind zu dokumentieren.
  - Der zugelassene Personenkreis sollte beschränkt sein (Zweckbindung)
  - für Aktenarchive sollte Schutzmaßnahmen realisiert sein (Wasser, Feuer, Dienstahl..)

DR. KOCH

Auskünfte

- Auskünfte an den legitimierten Adressatenkreis (wie geht es meinem Vater?) sind grundsätzlich möglich. Bei Anrufen besteht jedoch die Schwierigkeit, festzustellen, ob der Anfrager zum legitimierten Personenkreis gehört.
- In jedem Fall: Sparsamkeitsgebot
- aktive Auskunft nur bei Notfällen
- Bei VIP´s - wenn möglich - mögliche Adressaten und im voraus klären!
- in jedem Fall nur knapp / allgemein Auskunft geben (Sparsamkeit)
- keine Auskünfte über den Dienstplan
- Dienstplan darf nicht mit nach Hause genommen werden

DR. KOCH

Auskünfte/Einsichtnahmen

- durch erb- und vermögensrechtliche Aspekte besonders schwierig
- grundsätzlich **verbietet** der Geheimnisverrat eine Weitergabe auch an Angehörige, auch nach dem Tod; Einschätzung immer nach der Situation (was will der Bewohner / was wollte der Verstorbene?), z. B. bei begründetem Verdacht auf eine Straftat.
- wenn Ansprüche gegen die Einrichtung geltend gemacht werden (sollen) oder angedroht werden, grundsätzlich warten, bis eine juristisch belegte Forderung vorliegt.
- keine Aktion ohne Rechtsbeistand!

DR. KOCH

Auskünfte Presse

- Auskünfte möglich, soweit die Daten schon öffentlich sind
- sonst **strikte Schweigeverpflichtung**
- besondere Vorsicht bei VIP´s!
- Einrichtung sollte Notfallplan haben, der auch Pressemanagement einschließt; **klare Regelung, wer im Krisenfall Pressekontakt hat, „gut gemeinte“ Offenheit führt regelmäßig zum Schaden der Einrichtung.**
- **Einrichtungen des Gesundheits- und Sozialwesens stehen im besonderen Interesse der Öffentlichkeit.**

DR. KOCH

Auskünfte – Polizei und Staatsanwaltschaft

- Ruhe bewahren und Konfrontation vermeiden.
- Keine Angaben zum Tatvorwurf oder Sachverhalt machen
- Diskretion wahren (separater Raum)
- Anwalt verständigen
- Kontaktdaten der Untersuchungsbeamten
- Vorlage des Durchsuchungs- und Beschlagnahme-beschlusses, sonst Darlegung erforderlich, warum Gefahr im Verzug ist – **Achtung**: dies muss im Herausgabeprotokoll auch dokumentiert werden.
- Beamten Unterlagen nicht selbst suchen lassen (Festlegung Umfang, Zufallsbefunde)
- Formaler Widerspruch, sonst keine Prüfung möglich und Verstoß gegen §203 StGB
- Durchschrift des Beschlagnahmeprotokolls

DR. KOCH

Benutzerrichtlinien - Regularien

- zur Installation / Einsatz eigener Programme oder Hardware.
- zum Gebrauch des Internets: was dürfen die Mitarbeitenden herunterladen, was nicht (Informationen, Programme, etc.)? .
- zu Nutzungsverboten: Chatrooms, Websites mit pornografischen, rassistischen und Gewalt verherrlichenden Inhalten
- zur Art und Weise der Datensicherung, insb. bei Notebooks
- zum Umgang mit Sicherheits-Updates und Antivirus-Programmen
- zum Umgang mit Passwörtern
- zum Gebrauch von E-Mails: z. B. keine personenbezogenen oder vertraulichen Daten, kein Weiterleiten an private E-Mail-Adressen

DR. KOCH

Benutzerrichtlinien - Regularien

- zum Verhalten bei sicherheitsrelevanten Vorkommnissen, z.B. Viruswarnungen, Diebstählen und Verlusten (z. B. Notebooks / Passwörter).
- zur Nutzung bzw. Sperrung von Laufwerken
- zur Nutzung mobiler Datenträger
- zu den Rechten des Administrators
- zu Sanktionen beim Verstoß gegen die Benutzerrichtlinien

DR. KOCH

E-Mail

- grundsätzlich **keine Übertragung** personenbezogener Daten **ohne Verschlüsselung**!
- Ausnahme: Gefahr im Verzug
- auch bei legitimierten eMail-Verkehr nur minimalen Datenumfang versenden (Sparsamkeit)
- Inhouse-Verkehr problemlos

DR. KOCH

Entsorgung

- **grundsätzlich nicht in normalen Abfall!**
- Papier:
  kontrollierte Aktenvernichtung mit Sicherheitsstufen 3 der DIN 32757
- Vorsicht bei „Zwischenlägern“ und Papierkörben neben Kopierern
- Datenträger (auch FAX oder Telefon):
  kontrollierte Vernichtung oder professionelle Löschung der Daten
- Dienstleister gut einsetzbar, auch Aktenvernichtung vor Ort

DR. KOCH

Externe Archivierung

- **grundsätzlich möglich, aber hohe Anforderungen an den Inhalt des Vertragsverhältnis und Dienstleister**
- Dienstleister darf von personenbezogene Daten keine Kenntnis erlangen / Versiegelung der Akten
- Verwendung verschließbarer Transportbehälter
- technisch-organisatorische Maßnahmen, um Beschädigung und Untergang von Akten zu verhindern
- detaillierte Prozessgestaltung und – dokumentation
- kontrollierte Aktenvernichtung
- Problem – Beschlagnahme, Dienstleister unterliegt im Regelfall nicht § 203 StGB
- dringend anzuraten: nur Dienstleister wählen, für die ein positives Votum aus allen Bundesländern vorliegt

DR. KOCH

Externe Archivierung

- ev. muss eigenes Personal gestellt werden
- Ausnahme: möglich bei konkreter Einwilligung
- Genaue vertragliche Regelungen und Prozessdokumentation
- Verpflichtung aller Mitarbeiter des Dienstleisters auf das Datengeheimnis
- Benennung aller Mitarbeiter bei Auftraggeber und Dienstleister, die zum Kontakt berechtigt sind

DR. KOCH

Externer Schreibdienst

- **grundsätzlich nicht möglich – keine gesetzliche Offenbarungsbefugnis!!!!**
- Ausnahme: möglich bei konkreter Einwilligung
- kein Aktentransport aus der Einrichtung
- detaillierte Prozessgestaltung und – dokumentation
- soweit möglich: Zuordnung von Schreibaufrägen, die am wenigsten sensitiv sind
- Genaue vertragliche Regelungen, genaue Prozessdokumentation
- Verpflichtung des Dienstleisters auf das Datengeheimnis

DR. KOCH

Fax

- grundsätzlich **keine Übertragung** personenbezogener Daten per FAX!
- Ausnahme: Gefahr im Verzug
- Verschlüsselung möglich, aber sehr aufwendig.
- wenn in FAX-Versand eingewilligt wurde, sollten Vorkehrungen getroffen werden, dass auch beim Empfänger organisatorische Regeln beim Faxbetrieb sichergestellt sind (insb. Zugang, Standort, Berechtigte, Änderungen von Rufnummern – also vor der Versendung anrufen)
- eigenes Fax vor Zugang von Dritten schützen

DR. KOCH

Gespräche

- dienstlich: wenn Gespräche mit Bewohnern / Pflegenden erforderlich sind, sicherstellen, dass keine Dritten mithören, insb. Besucher, besonders wichtig bei sensiblen Inhalten
- konkludente Einwilligung möglich, insb. in häuslicher Umgebung
- meist schwierig im Eingangs- / Empfangsbereiche
- kein Mithören von Telefonaten
- privat: keine Personen nennen oder Angaben machen die Rückschluss auf Personen ermöglichen
- auch unter Geheimnisträger (z. B. Ärzte) **keine Datenweitergabe erlaubt – Ausnahme Mitbehandlung!**

DR. KOCH

Räume - Zugang

- wenn personenbezogene Unterlagen zugänglich sind, muss der Raum immer abgeschlossen oder besetzt sein.
- wenn **Dritte**, z. B. Dienstleister Zutritt zu den Räumen haben, zusätzlich Verschluss an den Schränken erforderlich
- kein Mithören von Telefonaten
- keine Lesemöglichkeit von Unterlagen (Bildschirm oder Papierakte)

DR. KOCH

Was tun, wenn es passiert ist?

DR. KOCH

Was tun, wenn es passiert ist?

§ 66 Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Von der Benachrichtigung kann abgesehen werden, wenn
1. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewandt wurden….
2. der Verantwortliche durch im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach keine erhebliche Gefahr ….
3. dies mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall hat stattdessen eine öffentliche Bekanntmachung

Fazit:
➔ **Erarbeitung von Verfahrensregelungen**
➔ **Konzept für Öffentlichkeitsarbeit**

DR. KOCH

Sanktionen gemäß §42, 43, 83 BDSG n. F.

Ordnungswidrigkeiten

sind bestimmte **vorsätzliche oder fahrlässige Datenschutzverstöße,** z. B. Verstöße gegen Melde-, Dokumentations- oder Informationspflichten sowie um unbefugte Datenerhebungs- oder Verarbeitungsschritte.

Straftaten

sind vorsätzliche, unzulässige Datenverarbeitungen, die **gegen Entgelt oder in Schädigungs- oder Bereicherungsabsicht** begangen werden.

Bußgelder bei OwiG bis zu EUR 50.000,00 und bei Straftaten **Freiheitsstrafe** bis zu zwei Jahren oder Geldstrafe.

Schadensersatz und **Entschädigung** gemäß § 83 BDSG n. F.

DR. KOCH

Ihr Team

Für praktisch/technischen Fragen des Datenschutzes

HWH – Gesellschaft für Datenschutz und Beratung
Tel.: 08091 / 39398 - 60
Fax: 08091 / 39398 - 69
Kooperationspartner der bpa Servicegesellschaft

Für alle rechtlichen Fragen des Datenschutzes
Dr. Koch - Rechtsanwalt
Dr. Franz-Michael Koch
Tel. 030 / 70 20 60 40
Fax: 030 / 70 76 73 87
Nähere Informationen und Download: www.ra-fmk.de

GKD – Rechtsanwälte
Dr. Thomas Zürcher
Telefon: +49 (761) 590 004-0
Telefax: +49 (761) 590 004-99
Internet: www.gkd-rechtsanwaelte.de

DR. KOCH

Dr. Franz-Michael Koch (Universitätsverwaltungsoberrat a. D.)
Berlin

Spezialisierungen/Tätigkeitsschwerpunkte
Arbeitsrecht, öffentliches Dienstrecht
Vergaberecht, Hochschul- und
Krankenhausrecht, Outsourcing, IT- und Datenschutzrecht,
Tarifrecht/Tarifverhandlungen, betriebliche Vergütungssysteme

Beratungsschwerpunkte
- Beratung von Umstrukturierungsprozessen
- Begleitung von Mergers & Acquisitions Projekten
- Begleitung von Kostenoptimierungsprozessen (betriebliche Vergütungsstrukturen usw.)
- Begleitung der Abwicklung investiver Fördermittelprojekte im Gesundheitswesen (Vorbereitung, Realisierung und Umsetzung von Baumaßnahmen im Altenheim-, Krankenhaus- und Reha-Bereich)
- Optimierung der Erlösstrukturen
- Begleitung Einführung EU-DSGVO
- Prozessführung (forensische Tätigkeit) – z. B. Kündigungs- und Gewährleistungsverfahren aller Art

Ausbildung und Werdegang
Geboren 1965.
- Studium der Rechtswissenschaften in Berlin 1985-1989.
- Erstellung der Dissertation Januar-Juni 1990 im Bereich korrektives Arbeitsrecht
- Tätigkeit als Justitiar des Virchow-Klinikums und des Universitätsklinikums Charité in Berlin 1993 - 1998.
- Lehrbeauftragter an der Fachhochschule für Verwaltung und Rechtspflege in Berlin vom 1994 - 1998.
- Als Rechtsanwalt zugelassen seit 1999.
- Aufbau des Standortes Berlin von Schrade & Partner Rechtsanwälte 2000-2012 Schwerpunkt Gesundheitswesen – Mitgesellschafter ab 2008
- Aufbau eigener Anwaltskanzlei seit 2013, 2017 Neubau Büroräume in Berlin-Marzahn

DR. KOCH

HWH-Gesellschaft für Datenschutz GmbH
Tel.: 08091 / 39398 - 60
Fax: 08091 / 39398 - 69


Spezialisierungen

- Beratung und Betreuung als externen Datenschutzbeauftragter
- IT - Projektmanagement
- Pflegesatzverhandlungen nach §85 SGB XI
- Kostenrechnung und externes Controlling
- Standort- und Wertanalysen

Professionelle Beratung im Bereich des Gesundheitswesens und der Pflege? Wir helfen Ihnen dabei.

Wir sind ein hochspezialisiertes Beratungsteam und beraten Sie individuell und auf Ihre spezifischen Bedürfnisse angepasst. Unsere Kompetenzen reichen von der klassischen Unternehmensberatung zur Pflegesatzverhandlung bis hin zum externen Datenschutzbeauftragten.

Wir sind sympathische, kreative und professionelle Berater für sympathische, kreative und professionelle Kunden. Unsere Lösungsstrategien für Ihre Bedürfnisse sind immer auf Sie, Ihr Team und Ihre Ziele zugeschnitten, denn die beste Strategie ist nur zu verwirklichen, wenn auch die Menschen da sind sie zu leben. Daher behalten wir in unserer Beratung immer die Umsetzbarkeit Ihrer Ziele im Auge. „Wir sind Idealisten, aber keine Träumer".

Diese Ehrlichkeit in der Beratung mit der Fähigkeit auch mal „Nein" sagen zu können zeichnet uns aus.
Wir sind kreative Querdenker und keine Mitläufer.

Kooperationspartner
bpa servicegesellschaft

DR. KOCH

GKD // RECHTSANWÄLTE

THOMAS ZÜRCHER LL.M.
RECHTSANWALT

Spezialisierungen/Tätigkeitsschwerpunkte

Individual- und Kollektivarbeitsrecht, Dienstvertragsrecht, Datenschutzrecht, Handels- und Gesellschaftsrecht

Bismarckallee 15
79098 Freiburg i. Br.
Telefon: +49/761/59 00 04 0
Telefax: +49/761/59 00 04 99
zuercher@gkd-partner.de
www.gkd-partner.de

DR. KOCH

Ich danke Ihnen für Ihre Aufmerksamkeit