Einführung in den Datenschutz

Die neue EU Datenschutz Grundverordnung (DSGVO)
Stand: Juli 2018, Ergänzungen aus 2021

General Data Protection Regulation – GDPR (GB)
Regolamento generale sulla protezione dei dati – RGPD (I)
Règlement sur la protection des données générales – RPDG (F)
Regulamentação europeia de proteção de dados (PT)
General andmekaitse määruse – GAM (EST)

Peter Klatecki

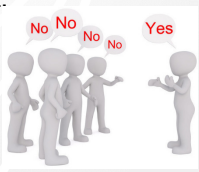
Inhalt

1. Entstehung der DSGVO
2. Grundsätze des Datenschutzes
3. Rechtlicher Rahmen und wesentliche Begriffe des Datenschutzes
   - Datengeheimnis
4. Der Datenschutzbeauftragte
5. Betroffenenrechte
6. Datenschutzverletzungen und Verstößen
7. „Unwuchten“ der DSGVO
8. Hinweise zu den technischen und organisatorischen Maßnahmen / zur Datensicherheit
9. Hinweise zu mobilen Geräten
10. Wert von Daten (in Euro)
11. Folgen

2

Entstehung der DSGVO

- 2012 bis 2014, Entwurf und Ausarbeitung durch den deutschen Europaabgeordneten **Jan-Philipp Albrecht** (38, Grüne) und der Luxemburgerin **Viviane Reding** (70, damals Vizepräsidentin der Europäischen Kommission und Kommissarin für das Ressort Justiz. Grundrechte und Bürgerschaft)
- Starke Lobbyarbeit dagegen, zwischenzeitlich über 4000 Änderungsanträge und damit eigentlich „tot“
- Und dann kam … :
  Edward Snowden und die NSA-Affäre (Sommer 2013)
- Beschluss am 14. April 2016 durch das EU-Parlament, wurde am 04.05.2016 im Amtsblatt der Europäisches Union veröffentlicht, in Kraft am 25.05.2016



Grundsätze des Datenschutzes

Was will die DSGVO?

- **Verbraucherschutz / Schutz der Person**
- Europaweite Vereinheitlichung des Datenschutzes (Gesetzeskraft, keine nationale Umsetzung notwendig!!!)
- Anpassung an die Herausforderungen der Digitalisierung
- **technikneutrale** Ausgestaltung
- Management in die Haftung nehmen
- Wirksame Strafen

Ziel: Google, Facebook, Amazon & Co.

4

Grundsätze des Datenschutzes

- Datenschutz ist ein Grundrecht
  - Jeder Mensch soll **im Grundsatz** (weitgehend) selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen.
- **Grundsätze** für die Verarbeitung personenbezogener Daten, Art. 5 DSGVO
  - Rechtmäßigkeit
  - Treu und Glauben (vom Betroffenen nachvollziehbar)
  - Transparenz
  - Zweckbindung (eindeutig, zweckmäßig, Verbot der Weitergabe)
  - Datensparsamkeit (Minimierung, nur nötige Daten)
  - Richtigkeit (und aktuell / richtig)
  - Begrenzte Speicherung (Befristung)
  - Integrität und Vertraulichkeit (Technische Maßnahmen zum Schutz)

5

Rechtlicher Rahmen und Begriffe

Datenschutz-Grundverordnung (DSGVO)

Stichtag: 25.05.2018, in Kraft seit 25.05.2016

- Gilt für alle Organisationen, die (automatisiert) personenbezogene Daten verarbeiten (Unternehmen, Behörden, Vereine, …)
- **Gilt nicht für Privatpersonen**, wenn diese Daten **für persönliche oder familiäre Zwecke** verwenden.
- Die bisherigen, nationalen Gesetze fallen weg
  - Bundesdatenschutzgesetz (BDSG alt)
    - Ersetzt durch BDSG neu !! Auch ab 25.05.2018.
  - Telemediengesetz (TMG -> TMG neu)
- Je nach Verstoß können Bußgelder verhängt werden
  - bis zu 20 Mio. EUR oder bis zu 4 % des gesamten, weltweit erzielten Jahresumsatzes, je nachdem, welcher Betrag höher ist.

Es ist nur noch datenschutzkonform, was der DSGVO entspricht.

6

Rechtlicher Rahmen und Begriffe

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

- für alle innerhalb der EU (Business und Privat - falls nicht persönlich oder familiär)
- 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 innerhalb der EU
  - der Beobachtung des Verhaltens von Bürgern innerhalb der EU

7

Rechtlicher Rahmen und Begriffe

- Der **Umgang mit personenbezogenen Daten** wird somit durch das Datenschutzrecht geregelt.
  - Es kommt zur Anwendung, wenn Sie Daten bearbeiten, die einem **Menschen** zugeordnet werden können.
  - Daten von **juristischen Personen**, Vereinen, Verbänden etc. sind durch die DSGVO **nicht geschützt.**
- Personenbezogene Daten sind alle Angaben, die sich auf eine **identifizierbare** (bisher bestimmbare) Person beziehen.
  - Name, Adresse, Geburtsdatum, Telefonnummer, Vermögen, Gehalt, Bankkonten, IP-Adresse, …, (es gibt weitgehende Möglichkeiten zur Identifikation, Bsp.: Tippgeschwindigkeit, Fahrverhalten bei Telemetrie …, Rechnerkonfiguration)
- Erhebung und Verarbeitung von personenbezogenen Daten ist nur unter **bestimmten Voraussetzungen** erlaubt. (Art. 6 DSGVO)
  - jeder Vorgang (**Gewinnung, Speicherung, Löschung, …)**
  - **Nicht nur für elektronische Verarbeitung!!**

8

Rechtlicher Rahmen und Begriffe

Abgrenzung bzw. Überschneidung

- Persönlichkeitsrecht
- Recht am eigenen Bild
- Recht auf Privatsphäre
  - Unverletzlichkeit der Wohnung
- Selbst-
  - -bestimmung
  - -bewahrung
  - -darstellung
- …

Diese Rechte sind obligatorisch

7

Rechtlicher Rahmen und Begriffe

Identifizierbar

- … ist eine Person, wenn sich ihre Identität direkt aus dem Datum selbst ergibt.
  - Bsp.: Name
- … wird eine Person, wenn ihre Identität durch die Kombination des Datums mit einer anderen Information feststellbar wird.
  - Bsp.: IP-Adresse kombiniert mit Providerdaten

Identifikation durch Merkmale der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität.

10

Rechtlicher Rahmen und Begriffe

Relevante Vorgänge

DSGVO Neu:

- *Verarbeiten*

Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Bereitstellen, Abgleichen, Verknüpfen, Einschränken, Löschen, Vernichten, …

Alles, was man mit Daten anstellen kann!

- **Verbot mit Erlaubnisvorbehalt !**
  - D.h. grundsätzlich unzulässig, sofern keine Ausnahme/Erlaubnis vorliegt.

11

Rechtlicher Rahmen und Begriffe

Die Datenverarbeitung ist **grundsätzlich erlaubt**, wenn (Art. 6 DSGVO) …

- Ein **berechtigtes Interesse** an der Datenverarbeitung vorliegt und schutzwürdige Interessen des **Betroffenen** (insbesondere Kindern) **dem nicht entgegen stehen** (Art. 6 Abs. 1 f DSGVO)

Anmerkung:
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 u.a. die Durchführung von Direktmarketing als berechtigtes Interesse betrachtet werden kann.

*„Die **Rechtmäßigkeit der Verarbeitung** kann durch **die berechtigten Interessen eines Verantwortlichen**, auch eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, oder eines Dritten begründet sein, **sofern die Interessen** oder die **Grundrechte und Grundfreiheiten** der betroffenen Person **nicht überwiegen**; dabei sind die **vernünftigen Erwartungen** der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen."*

Z.B. … maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen (als Kunde, als Beschäftigter, …)

12

Rechtlicher Rahmen und Begriffe

Die Datenverarbeitung ist **grundsätzlich erlaubt**, wenn (Art. 6 DSGVO) …

- Die Datenverarbeitung **erforderlich** ist,
  - zur Erfüllung eines Vertrags
  - für vorvertragliche Maßnahmen auf eine Anfrage 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**
  - **Vgl. auch §26 BDSG (Beschäftigungsverhältnisse)**

13

Rechtlicher Rahmen und Begriffe

Die Datenverarbeitung ist **grundsätzlich erlaubt**, wenn (Art. 6 DSGVO) …

- **Einwilligung** der betroffenen Person vorliegt (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 (mit anderen Einwilligungen, etwa AGB)
  - Opt-In,
    Nicht vorab angeklickte Checkboxen mit Opt-Out

14

Rechtlicher Rahmen und Begriffe

Besondere Arten personenbezogener Daten
(sensible Daten) Art. 9

- Religion, sexuelle Orientierung, Ethnische Herkunft, politische Meinung, Gesundheit, Gewerkschaft, neu: **Genetik, Biometrie**
- **Weitaus strengere Regeln**, da besonders schützenswert

diese Daten dürfen **nur** verarbeitet werden:

- zur Erfüllung von gesetzlichen Pflichten (Arbeit, Soziale Sicherheit)
- zum Schutz lebenswichtiger Interessen (wenn nicht in der Lage z. Einwilligung)
- Daten waren bereits öffentlich
- Im Rahmen der Justiz / bei Rechtsansprüchen
- Gesundheitsvorsorge und Arbeitsmedizin
- Im öffentlichen Interesse, bei verpflichtetem Fachpersonal
- Organisationen o. Gewinnerzielungsabsicht, (ehem.) Mitglieder und Kontaktpersonen
- **mit ausdrücklicher Einwilligung der betroffenen Person**

- Strafregister nur mit behördlicher Aufsicht (Art. 10)
- Daten von **Kindern und Jugendlichen** unter 16 nur mit **ausdrücklicher Einwilligung** der Eltern

15

Rechtlicher Rahmen und Begriffe

Informationspflicht

- Werden personenbezogene Daten bei der betroffenen Person **direkt** erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:
  - Name und Kontaktdaten des für die Datenerhebung Verantwortlichen (Quelle)
  - die Kontaktdaten des Datenschutzbeauftragten
  - die Zwecke und die Rechtsgrundlage der Verarbeitung
  - Dauer der Speicherung
  - das berechtigte Interesse des Verantwortlichen oder eines Dritten
  - Empfänger der personenbezogenen Daten
  - die Absicht der Übermittlung an ein Drittland oder eine internationale Organisation
  - Widerrufbarkeit
  - …

Rechtlicher Rahmen und Begriffe

Informationspflicht

- Werden personenbezogene Daten **nicht** bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person … **in max. einem Monat** Folgendes mit:

Etwa wie bei direkt, allerdings:

„In ***Ausnahmefällen*** muss der Informationspflicht nicht nachgekommen werden. Etwa wenn dies **unmöglich** oder **unverhältnismäßig aufwendig** ist, die Erhebung und/oder Übermittlung gesetzlich vorgeschrieben ist oder ein Berufsgeheimnis oder eine sonstige satzungsmäßige Geheimhaltungspflicht besteht."

Oder der Betroffene bereits über diese Informationen verfügt.

Rechtlicher Rahmen und Begriffe

Datengeheimnis (Artikel 29 DSGVO)

- Den bei der Datenverarbeitung beschäftigten Personen ist **untersagt**, personenbezogene Daten **unbefugt** zu erheben, zu verarbeiten oder zu nutzen.
- Diese Personen **sind**, soweit sie bei nichtöffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis **zu verpflichten**
- Das Datengeheimnis **besteht auch nach Beendigung** ihrer Tätigkeit fort.

18

Betroffenenrechte

Rechte der Betroffenen (Art. 15 ff DSGVO)

- Aufklärung *(umfassend, Link in E-Mail, Rechnung, …)*
- Auskunft *(Kopie der Daten, **ID prüfen !!!**, klein anfangen)*
- Löschung *(Recht auf Vergessenwerden)*
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht *(+Berichtigung)*
- Recht auf Einschränkung der Verarbeitung
  - (Richtigkeit wird bestritten, keine Löschung da rechtlich benötigt / unrechtmäßige Verarbeitung / Widerspruch gegen berechtigtes Interesse)
- Keine ausschließlich automatisierte Entscheidung
- Rechtsbehelf, Schadenersatz

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.

19

Betroffenenrechte

- Auskunftsrecht
  - Auf Facebook: „Deine Facebook-Informationen“
  - Google: myaccount.google.com
  - Snapchat: accounts.snapchat.com
  - Apple: privacy.apple.com
  - Amazon: E-Mail schreiben
  - …

  - Ohne Account / Musterschreiben Verbraucherzentrale: ***Musterbrief Auskunft nach Art.15 DSGVO***

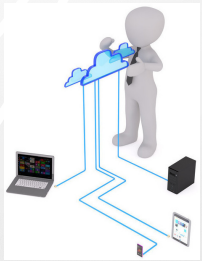
  - Schufa: Datenkopie (nach Art. 15 DSGVO)

Der Datenschutzbeauftragte

Freiwillig, oder

Pflicht nach DSGVO wenn:

- die **Kerntätigkeit** :
  - in der Verarbeitung besonderer Kategorien von Daten (Art. 9 der DSGVO) **oder** über strafrechtliche Verurteilung oder Straftaten besteht
  - eine **"umfangreiche regelmäßige und systematische Überwachung"** von betroffenen Personen erfordert



Pflicht nach BDSG neu wenn:

- 20 Personen oder mehr (als Angestellte oder auch freie Mitarbeiter) regelmäßig **mit der automatisierten Verarbeitung** personenbezogener Daten befasst sind
- Daten mit **Folgenabschätzung** vorliegen (Art. 35)
- Bei Markt- u. Meinungsforschung

21

Der Datenschutzbeauftragte

- **Kerntätigkeit,** Art. 37 Abs. 1 b
  - liegt vor, wenn es sich um eine **für die Geschäftstätigkeit** oder die Unternehmensstrategie **wichtige Tätigkeit** handelt und nicht bloß um routinemäßige Verwaltungsaufgaben, die in jedem Unternehmen als Nebentätigkeit vorkommen.

  - Unternehmen die Scoring- oder Profiling-Maßnahmen anbieten
  - Markt- und Meinungsforschungsunternehmen
  - Sicherheits- und Überwachungsunternehmen
  - Social-Media-Anbieter
  - Versicherungsunternehmen
  - Adressenhandel
  - …

Bezogen auf besondere Kategorien von Daten (nicht nur) sind z.B. Arztpraxen, Labors, Krankenhäuser, unter Umständen auch Rechtsanwälte (bspw. Medizinrecht, Arbeitsrecht etc.) zu nennen.

22

Der Datenschutzbeauftragte

- **Umfangreiche, regelmäßige und systematische Überwachung**
  (z.B. alle Arten des Internettrackings und –profilings)

- Umfangreich
  - Faktoren:
    - Anzahl der betroffenen Personen
    - Datenvolumen
    - Dauer der Verarbeitung
    - geografische Ausdehnung der Verarbeitung
    - Risiken für die betroffenen Personen

u.a. die Verarbeitung von Gesundheitsdaten in einem Krankenhaus oder die Verarbeitung von personenbezogenen Daten für Werbezwecke durch Suchmaschinen für verhaltensbedingte Werbevorschläge

Anmerkung: Cookie-Hinweise, Cookies sind eine überholte Technik

23

Der Datenschutzbeauftragte

Kriterien für einen DSB

- Die ausgewählte Person **soll** gewisse Anforderungen erfüllen, Art. 37 Abs. 5
  - eine gewisse berufliche Qualifikation
  - Fachwissen auf dem Gebiet des Datenschutzes und der Datenschutzpraxis
  - Fähigkeiten zur Erfüllung der gesetzlich definierten Aufgaben
  - kein Interessenskonflikt
    (IT-Abteilung, Personalabteilung und der Geschäftsführung)
  - Laufende Weiterbildung im IT- und juristischen Bereich
  - Aber: **Jeder** kann (theor.) DSB sein
  - Bestellung **intern** oder **extern** möglich (unterschdl. Haftung)

- Hat besonderen Kündigungsschutz, Verschwiegenheitspflicht, Zeugnisverweigerungsrecht

24

Der Datenschutzbeauftragte

Aufgaben

- Überwachung der Einhaltung der Datenschutzgrundsätze in der Organisation
- **Verarbeitungsverzeichnis** führen
- Schnittstelle zwischen der/dem IT(-Marketing) und Geschäftsführung
- Ansprechpartner der Kunden und Datenschutzbehörden bei Fragen zum Umgang mit personenbezogenen Daten
- **Verantwortlicher** / Zuständiger bei Datenschutzfragen
- Ansprechpartner der s.g. Betroffenen

Hierarchie

- Ist der höchsten Leitungsebene unterstellt und berichtet dorthin
- **Keine** Weisungsbefugnis (Beratung)

Kann im Unternehmen auch andere Tätigkeiten ausführen.
Muss der Aufsichtsbehörde bekannt gemacht werden.

25

Der Datenschutzbeauftragte

Ja …

das alles gilt auch für Vereine!

Der Datenschutzbeauftragte

- Datenschutzbeauftragter unserer Firma ist:

Roland Schwalm, Vertreter Stephan Schneider

Kontakt:
bits + bytes it-solutions
GmbH & Co. KG
Bahnhof Weidenau 6
57076 Siegen
Mail: datenschutz@bits-bytes.de
Tel: 0700 / 20 30 10 30

DSGVO Infos:
www.jasper-gmbh.de/DSGVO.html (Datenverarbeitung)
www.jasper-gmbh.de/datenschutz.html (Erklärung)

27

Verfahrensverzeichnis

- Verzeichnis von Verarbeitungstätigkeiten
  Art. 30 (5) DSGVO, nicht mehr öffentlich wie nach BDSG
- Pflicht wenn:
  - >= 250 Mitarbeiter
- oder:
  - Die Verarbeitung erfolgt **nicht nur gelegentlich**
  - Bei besonderen Kategorien von Daten
  - Bei Risiko für Rechte und Freiheiten
  - Bei Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

(nur ein Kriterium muss zutreffen)

Auftragsverarbeitung

Datenübermittlung

- nur dann erlaubt, wenn
  - Einwilligung der betroffenen Person liegt vor
  - Das Gesetz erlaubt es und Person wurde benachrichtigt
- **Oder** bei **Auftragsverarbeitung**, dann
  - Keine Einwilligung nötig
  - Keine gesetzliche Erlaubnis nötig
  - Keine Benachrichtigung nötig
  - **Verarbeitung auch außerhalb der EU möglich (neu)!**
  - **(In der Regel) Vertrag mit Verarbeiter nötig !!!**

Problem:

- Mit wem ist ein Vertrag wirklich nötig ? Wer ist Auftragsverarbeiter ?
- **Zertifizierung** des Auftragsverarbeiters !

Auftragsverarbeitung

Wann liegt Auftragsverarbeitung vor?

- Kriterien (Fragen)
  - Wesentlicher Zweck bei der Verarbeitung ist „**für den Auftraggeber**“, kein eigenes Interesse des Dienstleisters
  - Zweck und Mittel werden durch den Auftraggeber festgelegt (im Wesentlichen)
  - Datenverarbeitende Stelle hat ausschließlich eine Hilfs- oder Unterstützungsfunktion (technisch)

Wenn diese **Kriterien zutreffen**, dann in der Regel Auftragsverarbeitung

Hinweis auf AV in der Datenschutzerklärung !!

Auftragsverarbeitung

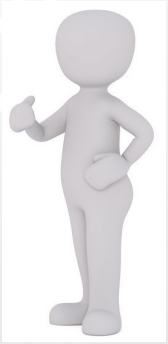
Typische Fälle von Auftragsverarbeitung

- externe Lohn- oder Gehaltsabrechnung (nicht b. Steuerberater)
- Newsletter Versand durch eine Marketingagentur
- Nutzung von Cloud-Diensten zur Personal- und Kundenverwaltung
- Datenträgerentsorgung, Aktenvernichtung
- Letter Shops, die in Auftrag Werbung an Kunden versenden
- Webanalyse- und Tracking-Dienste wie Google Analytics
- Kunden-Helpdesks
- Ausgelagerte Rechenzentren
- Callcenter, die Kundendaten ohne wesentliche eigenen Entscheidungsspielräume verarbeiten
- Dienste, die Daten erfassen, konvertieren oder Dokumente einscannen
- Auslagerung der Backup-Sicherheitsspeicherung und anderer Archivierungen

Auftragsverarbeitung

keine Auftragsverarbeitung wenn

- nicht mehr selbst „Herr der Daten
  - Keine Entscheidung über Zugang, Löschen, nicht mehr zuständig für Auskünfte
  - Dienstleister handelt eigenverantwortlich (Funktionsübertragung, **weisungsfrei**)
- Regelung durch spezielle Gesetze
  - Telekommunikation, Post
- Rein technische Wartung



Auftragsverarbeitung

Keine Auftragsverarbeitung in folgenden Fällen

- Finanzberater
- Steuerberater (StBerG, weisungsfrei)
- Unternehmensberater
- Rechtsanwalt
- Wirtschaftsprüfer
- externer Betriebsarzt
- Inkassobüro (mit Forderungsübertragung)
- Bankinstitut für den Geldtransfer
- Postdienst für den Brieftransport
- Installation und Wartung von Netzwerken, Hardware, Telefonanlagen
- Pflege von Software
- Programmentwicklungen und Tests

Datenschutzverletzungen und Verstöße

Typische Datenschutzverletzungen

Schwachstellen

- Mitarbeiter
- Papierentsorgung & Abfalleimer (ohne Shreddern)
- USB-Sticks, Speicherkarten & sonstige Datenträger
- „Mobile Devices“
- Kommunikation & E-Mail (Versand über priv. Account)
- Datensicherung & Datensicherheit
- Rechtesystem (LAN, Server, …)
- BYOD (private Geräte)
- …

34

Datenschutzverletzungen und Verstöße

Typische Datenschutzverletzungen

Fehler

- Unkontrollierter Zugang zu Betriebsräumen
- Unnötige Aussagen am Telefon
- Vertrauliche Unterlagen liegen offen
- Datenschutz nur im Büro
  (vs. Reise, HomeOffice, …)
- Schwache Passwörter & Weitergabe dieser
- Schlecht gewartete Hard- und Software (Updates)
- Unnötige (alte) Daten auf Arbeitsrechner
- „Flurfunk“

35

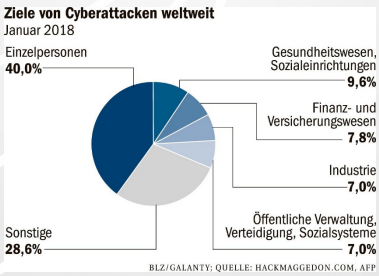
Datenschutzverletzungen und Verstöße

Angriffsszenarien

- Intern / persönlich (Nicht über die Netzwerkverbindung)
  (Social Hacking, Datenklau, ... **> 90% aller Fälle**!)

Der Rest

- Trojaner, Phishing, Viren, Erpressung
- Zero-Day-Exploits
- Automatisierte Angriffe/
  Hardware-Fehler
- Reputation
- Distributed Denial of Service
  (DDoS)



36

Datenschutzverletzungen und Verstöße

Bei (potentiellen) Verletzungen oder Verstößen

Beobachtungen, Verlust von Dokumenten/Datenträgern, ungewöhnliches Verhalten von Systemen, …

- Meldung an Vorgesetzten
  - Bei personellen Vorfällen
- Meldung an IT
  - Bei IT bezogenen Vorfällen
- Meldung an Datenschutzbeauftragten

Immer die Außenwirkung im Hinterkopf haben!!!
Presse, Strafen nach DSGVO (Meldepflicht, 72 Stunden, Aufsichtsbehörde).

Nicht, wenn diese Verletzung „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“ (Art. 33 DSGVO)

37

Datenschutzverletzungen und Verstöße

Bußgeldvorschriften, Artikel 83 Abs. 4,5,6

○ Bis zu 10.000.000 EUR oder im Fall eines Unternehmens bis zu 2 % seines weltweiten Jahresumsatzes, je nach dem, was höher ist	Pflichten gemäß den Artikeln 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43;	Verantwortliche; Auftragsverarbeiter
	42, 43	Zertifizierungsstelle
	41 Abs. 4	Überwachungsstelle
○ Bis zu 20.000.000 EUR oder im Fall eines Unternehmens bis zu 4 % seines weltweiten Jahresumsatzes, je nach dem, was höher ist	Verstöße gegen die folgenden Bestim-mungen: Artikel 5, 6, 7 und 9, 12-22, 44-49, 58 Abs. 1, 2,	Verantwortliche, Auftragsverarbeiter

In jedem Fall aber: „wirksam, verhältnismäßig und abschreckend“

38

Datenschutzverletzungen und Verstöße

(DSGVO-) Abmahnungen

- gibt es (bisher) nicht
  (Abmahnung ist national / deutsch, DSGVO ist europäisch)
- (wahrscheinlich nur) wegen Wettbewerbsrecht möglich (Datenschutz ist Menschenrecht, nicht Recht als Marktteilnehmer)
- DSGVO ist (vermutlich) abschließende Regelung
  (d.h. enth. alle Sanktionsmöglichkeiten)
- Abwehr via Anwalt
  Eine unberechtigte Abmahnung ist selbst ein Wettbewerbsverstoß
- **Keine rechtlich ungeprüfte Unterlassungserklärung abgeben!**

Die Rechtslage ist vor allem für ein Unternehmen sehr unsicher, das Abmahnungen aussprechen will. Im Moment besteht eine sehr hohe Chance, dass Abmahnungen von Mitbewerbern gar nicht erfolgreich sind – oder abgewehrt werden können. Damit bliebe ein abmahnendes Unternehmen schlussendlich auf den eigenen Rechtskosten sitzen.

Ohne Worte

Aus c´t 11/2018

Österreich hat die Preise noch rechtzeitig gesenkt (ÖVP/FPÖ).

- Ersttäter verwarnen
- Strafe nur bei „schweren Fällen" oder Wiederholung … oder die Schuld einem untergebenen Mitarbeiter geben
- *Gelockerter Datenschutz für Strafverfolger*, +Militär, +Spione, +Private Spione wenn für EU-Staat spioniert wird
- Keine Sammelklagen gegen **ausl.** Unternehmen (wie Google z.B.!!!)
- Bundestrojaner
- Abschaffung anonymer Handynummern
- Keine Auskunft wenn Geschäfts- oder Betriebsgeheimnis (auch eines Dritten) gefährdet ist

Vertragsverletzungsverfahren wird angeregt (Epicenter.Works, SPÖ)

Österreich entwaffnet den Datenschutz

Wenn am 25. Mai die Datenschutzgrundverordnung (DSGVO) in der EU in Kraft tritt, kann es für Datensünder teuer werden – außer in Österreich. Dort hat die rechtskonservative Koalition aus ÖVP und FPÖ das ebenfalls Ende Mai in Kraft tretende „Datenschutz-Deregulierungs-Gesetz" in einem plötzlichen Abänderungsantrag umgeschrieben. Wer dort künftig gegen den Datenschutz verstößt, muss kaum Strafen fürchten.

Die Datenschutzbehörde verhängt künftig nur noch in schweren Fällen oder bei hartnäckigen Wiederholungen Geldbußen. Ersttäter sollen verwarnt werden. Selbst wenn eine Firma wiederholt erwischt wird, kann sie sich vor einer Strafe drücken. Das Management muss den Fehler bloß einem untergebenen Mitarbeiter zuschreiben, um die Firma straffrei zu halten. Ein anderer Trick ist, sich im Tatzusammenhang eine kleine Verwaltungsstrafe abzuholen. Die Datenschutzbehörde darf dann im selben Fall nicht mehr strafen. Behörden und andere öffentliche Stellen können sogar nie bestraft werden – Polizei, Gemeinden und das GEZ-Pendant GIS dürfen sich freuen.

Der für Strafverfolger gelockerte Datenschutz wird auf das Militär sowie auf Spione ausgedehnt – in- wie ausländische. Sogar private Spione werden bevorzugt behandelt, wenn sie im Auftrag eines EU-Staats spionieren.

Das von der DSGVO gewährte Recht, wonach Betroffene Auskunft und Kopien der über sie gespeicherten Daten erhalten können, wird ebenfalls ausgehöhlt. Die Auskunft darf verweigert werden, wenn sie „ein Geschäfts- oder Betriebsgeheimnis des Verantwortlichen bzw. Dritter gefährden" würde.

Betroffene haben nach der DSGVO Anspruch auf Schadenersatz, der meist nur wenige Euro ausmacht. Einzelne können diesen normalerweise an gemeinnützige Organisationen abtreten, die dann Sammelbeträge einklagen. Der neue Gesetzestext versperrt diesen Weg jedoch. Damit will die Regierung offensichtlich Datenschutz-Organisationen wie Epicenter.Works oder Max Schrems' Noyb (none of your business) den Boden entziehen. Allerdings fällt die Verbandsklage nur gegenüber ausländischen Unternehmen weg. Gegen in Österreich ansässige Firmen sind sie weiterhin möglich. „Diese Regierung hat es voll-

Kanzler Kurz (ÖVP) und sein Vize Strache (FPÖ) legen Datenschutz als Schutz der Datensammler aus.

bracht, dass es nun einfacher ist, lokale Unternehmen zu verklagen als Google oder Facebook. Das ist ein Schuss ins Knie des Wirtschaftsstandorts", kommentiert Schrems.

Parallel beschloss das österreichische Parlament die Einführung des Bundestrojaners zur geheimen Überwachung, die Abschaffung anonymer Handynummern sowie neue Datenschutzbestimmungen in über 120 weiteren Gesetzen. Die Opposition beschwerte sich über zu wenig Zeit, vor der Abstimmung die neuen Gesetze lesen zu können. Dort mögen sich noch allerlei Überraschungen verbergen.

Für die Entwaffnung des Datenschutzes stimmten die Regierungsparteien ÖVP und FPÖ. Mit ihnen freute sich die Wirtschaftskammer über den neuen Grundsatz „Beraten statt strafen". Die SPÖ sprach hingegen von einem „schwarzen Tag für den Datenschutz" und stimmte mit Abgeordneten der Liste Pilz und der Neos dagegen. Epicenter.Works will der EU-Kommission ein Vertragsverletzungsverfahren gegen Österreich nahelegen. *(Daniel AJ Sokolov/hag@ct.de)*

40

„Unwuchten“ der DSGVO

- Ein Blogger mit ein paar Euro Verdienst hat (nahezu) die gleichen Pflichten wie ein multinationaler Konzern.
- Regionale Regeln (EU) für ein globales Netz
  - Stress bei EU-Unternehmen, Lockerheit außerhalb.
- Mindestalter, 16 Jahre
  - USA 13 Jahre
  - SnapChat hat viele junge Nutzer, auch nach dem 25. Mai 2018 ohne Zustimmung der Eltern
  - Verifizierung des Alters?

41

„Unwuchten“ der DSGVO

Fotografen

- Bisher: Kunst Urheber Gesetz (KUG) über BDSG
  - Erlaubte Fotos im öffentlichen Raum (Versammlungen, Prominente, …)
- Digitalfotografie **ist Datenverarbeitung** nach DSGVO, **wenn Gesichter von Personen** abgebildet sind
  - *Erlaubt für „hauptberufliche, angestellte Fotojournalisten“*

KUG sollte bei Kunst und Meinungsfreiheit **Vorrang** haben ! (Möglich nach Öffnungsklausel 85, in Schweden bereits umgesetzt). Evtl. in BDSG neu.

Stellungnahme Bundesinnenministerium: KUG weiter Vorrang. (14. Mai) juristisch nicht bindend, sollte aber Ärger vorbeugen

Nach der Entscheidung des BGH vom 7. Juli 2020 (Az.: VI ZR 246/19) findet das KUG (nur) **im journalistischen Bereich weiterhin Anwendung**

42

„Unwuchten“ der DSGVO

Unklare Rechtsauffassung

- Konferenz der Datenschutzbehörden veröffentlichte am 26. April 2018 (!) die Auffassung, das beim s.g. Tracking **immer** die Einwilligung der Nutzer **vorliegen muss** (vor dem Beginn des Trackings).

  Dies **entspricht nicht** dem bisherigen TMG als auch nicht der aktuellen DSGVO, §6 (berechtigtes Interesse)

  Aber **die Behördenleiter** verschicken die Bußgeldbescheide …

  (eine Folge: die Cookie-Hinweise im Web)

Dies leistet evtl. Vorschub für Unterlassungsklageverbände und entsprechende Kanzleien.

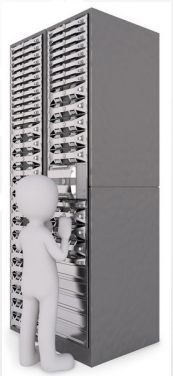
(Anmerkung: bisher nicht)

43

Technische/organisatorische Maßnahmen

Prinzipien

- **Privacy by Design /** „Datenschutz durch Technikgestaltung“
  - Grundgedanke: Datenschutz lässt sich am besten einhalten wenn er bereits in den Datenverarbeitungsvorgang technisch integriert ist.
- **Privacy by Default /** „Datenschutz durch datenschutzfreundliche Voreinstellungen“
  - Werkeinstellungen sind datenschutz-freundlich auszugestalten. Insbesondere die Nutzer schützen, die sich weniger mit Technik auskennen/beschäftigen und dadurch datenschutzrechtliche Einstellungen nicht ihren Wünschen entsprechend anpassen.

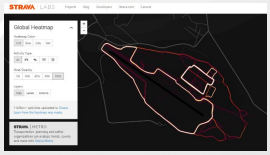


Nutzerauthentifizierung, Pseudonymisierung, Anonymisierung, Verschlüsselung, Widerspruchsrecht (technisch ermöglichen)

Technische/organisatorische Maßnahmen

Privacy by Default

- Beispiel: DNS Server von Quad9 im Router
  - DNS: Name in IP Adresse auflösen
  - Quad 9 (IBM, Packet Clearing House und Global Cypher Alliance u.a.)
  - Sammelt keine Daten
  - Blockiert Phishing und Malware Seiten
  - TLS und DNSSEC möglich
  - Finanziert durch Spenden und Beiträge der öffentlichen Hand (weltweit)
  - **9.9.9.9** (IP V4) / **2620:fe::fe** (IP V6)
  - Google DNS: 8.8.8.8



Technische/organisatorische Maßnahmen

Datenschutz fängt bei der täglichen Arbeit an.

- Geben Sie niemals Ihre Benutzerkennungen weiter!
- Schließen Sie Räume, die länger unbesetzt sind ab! (wenn sinnvoll und möglich)
- Sperren Sie Ihren (Arbeitsplatz-)Rechner! (WIN+L)
  - Im Büro
  - Auf der Baustelle
- Verwenden Sie sichere Passwörter!
- Verwahren Sie Daten, Datenträger und Ausdrucke stets sicher!
- Shreddern Sie nicht mehr benötigte Dokumente!
- Verwehren Sie Unbefugten Einsicht in vertrauliche Unterlagen!
- Begleitung von betriebsfremden Personen

46

Technische/organisatorische Maßnahmen

Sonstige Maßnahmen

- Datensparsamkeit am Telefon
  - Kollege ist nicht da, ist krank/im Urlaub, in der Kur, in psychiatrischer Behandlung, …

und natürlich

- „Gesunder Menschenverstand“

47

Technische/organisatorische Maßnahmen

Sicherheit der Verarbeitung

- Angemessen, unter Beachtung insbes. des „Stands der Technik“, und **risikoadäquat**
  - Berechtigungen (Login, Software-Ebene)
  - FireWall (welche?)
  - Verschlüsselung (E-Mail, VPN)
- Fokussierung auf die IT Sicherheitsziele:
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit (Backup)

48

Technische/organisatorische Maßnahmen

E-Mail Verschlüsselung

- **SSL** (Secure Sockets Layer, alt) oder **TLS** (Transport Layer Security, Nachfolger).
  Alle Provider bieten das an bzw. Zugriff nur noch verschlüsselt möglich
- Komfortable Verschlüsselung bis zum (eigenen) Mailserver
  danach verschlüsselte Übertragung durch nachfolgende Systeme
- Ende-zu-Ende Mail Verschlüsselung nur durch zusätzlichen Aufwand
  (eigene Zertifikate)

Einsatz mobiler Geräte

Notebooks, Tablets, Smartphones, USB-Sticks, Rechner in betriebsfremder Umgebung

- Unterliegen einer höheren Gefährdung bzgl. Diebstahls
- Benutzung möglich nur nach Passwort / Pin / Biometrie
- Sollten nur für den Einsatzfall notwendige Daten enthalten
  - Verschlüsselung (Bitlocker / Veracrypt)
- Sollten nur für den Einsatzfall notwendige Software enthalten
- Sind beim Verlassen immer zu sperren
- Bei Nichtbenutzung sicher verwahren
  (vor fremdem Zugriff)

50

Einsatz mobiler Geräte

Das „WhatsApp-Problem“

- Dies nur als Bezeichnung, es umfasst auch verschiedene andere Messenger, Social-Media, Online-Spiele usw. welche ungefragt Daten transferieren.
- Das Adressbuch (z.B.) eines Nutzers mit allen Kontakten einschließlich E-Mail Adresse und Telefonnummern wird an WhatsApp und damit an Facebook übertragen. **Es ist völlig unklar**, wohin und zu welchem Zweck diese Daten übertragen und verarbeitet werden.
  - Ausdrückliche Einwilligung des Betroffenen fehlt (in der Regel)
  - Informationsrecht des Betroffenen kann nicht erfüllt werden („Download my Data“ ist nicht ausreichend)
  - Recht auf Vergessenwerden kann nicht erfüllt werden
  - Recht auf Übertragenwerden kann nicht erfüllt werden
  - Datentransfer in die USA = geringeres Schutzniveau

51

Einsatz mobiler Geräte

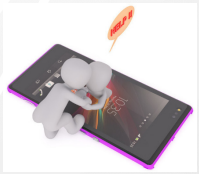
- **„NSA bestätigt: Seit WhatsApp verschlüsselt, werden deutlich mehr Nacktbilder verschickt“**
  https://www.der-postillon.com/2016/04/nsa-whatsapp.html
- Seit 2016 verschlüsselt WhatsApp Ende-zu-Ende
  - allerdings **nicht** die gesendeten Fotos
- Niemand kann sicher sagen, dass die NSA Texte nicht trotzdem lesen kann.
  - (Export von Verschlüsselungssoftware in s.g. sicherheitskritische Staaten ist in den USA verboten!)
  - Amerika hat eine Krypto-Exportbeschränkung von max. 64 Bit (symmetrisch), max. 768 Bit (Public-Key, asymmetrisch) und 128 Bit für Elliptische-Kurven-Kryptografie. Alle kommerziellen Produkten die darüber sind, müssen gemeldet werden und werden anschließend vom BIS (Bureau of Industry and Security) überprüft. Auch Open-Source Projekte müssen dem BIS vor Veröffentlichung des Quellcodes gemeldet werden.

Einsatz mobiler Geräte

- **Continental verbietet WhatsApp und Snapchat auf Diensthandys**
  - Der Autozulieferer Continental untersagt den Mitarbeitern wegen Datenschutzbedenken von sofort an den Einsatz von Social-Media-Apps wie WhatsApp und Snapchat auf Diensthandys.

    Dies gelte im weltweiten Unternehmensnetzwerk und betreffe mehr als 36.000 Mobiltelefone, teilte Continental mit. Continental sorgt sich um Verstöße gegen die neue DSGVO. Denn die Dienste greifen auf persönliche und damit potenziell vertrauliche Kontaktdaten im Adressbuch der Nutzer zu.

    Spiegel Online 05.06.2018



53

Wert von Daten

Je detaillierter, desto höher der Preis

(Beispiele, Datenhandel normal in 1000 Blocks)

- Wohnort 5,00 €
- Rabattkarte 0,80 €
- Politikinteresse 1,40 €
- Abnehmwunsch 8,00 €
- Umzug 6,20 €
- Heirat 8,80 €
- Kinder 8,40 €
- Jobwechsel 5,50 €
- Krankheit 19,00 €

Quelle: WDR Mediathek: Die tägliche Datenspur, **Wie das digitale Ich entsteht**

So viel kosten Ihre Daten

Kreditkartendaten	6 – 20 Dollar
Führerschein-Scan	5 – 25 Dollar
Ausweis-Scan	6 – 15 Dollar
Zugangsdaten Abodienst	0,5 – 8 Dollar
Personalausweis (Name, Sozialversicherungsnumer, Geburtsdatum, E-Mail-Adresse, Handynumer	0,5 – 10 Dollar
Selfie mit Dokument	40 – 60 Dollar
Krankenakten	1 – 30 Dollar
Zugang Online-Banking	1 – 10 Prozent des Werts
Zugangsdaten PayPal	50 – 500 Dollar

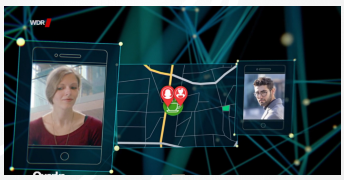
54

Folgen von Datenzusammenführung

Warum Facebook weiß, dass du schwanger bist
Quelle: WDR, Mediathek, Quarks
15.05.2018 | 3 Min. | Verfügbar bis 15.05.2023

Die FaceBook Datenbank weiß z.B.:

- Adina, geb. 22.01.1992
  Wohnort Köln, geboren in Siegen
  Bürokommunikationskauffrau, studiert BWL
- Mag Clueso, Bayer Leverkusen, ihr Fitnessstudio
- Ihre Likes, Ihre Freunde,
  ihre privaten Nachrichten (Inhalte)
- Aktivierter Standortzugriff (regelmäßige Aufenthalte);
  wer ist regelmäßig in der Nähe (auch nachts, Freund)
- Anderes Profil in der Nähe (Arbeitskollege),
  manchmal auch nachts
- Bei Anmeldung durch Facebook Account
  bei Online Bestellung, Vorlieben und deren Änderung
- Verweildauer bei Fotos (Baby ??)



www.ardmediathek.de

55

Skurrile Folgen der DSGVO

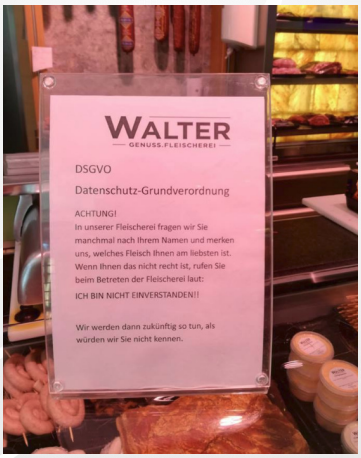
Die DSGVO betrifft auch Metzger.
Fleischermeister Walter (Salzburg) geht ganz eigen damit um.

- Weil die europäische DSGVO offensichtlich nicht jeder versteht, hilft der Österreicher jetzt mit einem Schild nach

  "In unserer Fleischerei fragen wir sie manchmal nach Ihrem Namen und merken uns, welches Fleisch Ihnen am liebsten ist."

  Um die Kundenrechte zu waren, bietet der Metzger eine Einspruchsmöglichkeit:

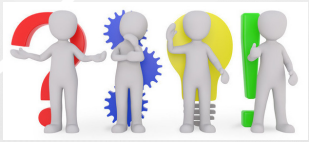
  "Wenn Ihnen das nicht recht ist, rufen Sie beim Betreten der Fleischerei laut: ICH BIN NICHT EINVERSTANDEN! Wir werden dann künftig so tun, als würden wir Sie nicht kennen."



56

Fazit

- Datenschutz nach DSGVO/BDSG betrifft uns alle!
  - als Betroffener
  - als Verarbeiter
- DSGVO gilt **nicht** im privaten/familiären Bereich
  - Kriterium Gewinnerzielung (Werbung auf Webseite reicht)
- Bei personenbezogenen Daten, **Aufklärungspflicht**!
  - (ggf. über Link auf spezielle Webseite)
  - Ausdrückliche Einwilligung ist überwiegend nicht erforderlich
- TOM / Verhaltensregeln beachten
- Bei Schutzverletzung, Meldepflicht!
  - (knappe Fristen)



Ende

- Achten Sie auf Ihre Daten!

- Quellen:
  - Pixabay (3D-men)
  - WDR
  - Wikipedia
  - …

58