Quo vadis, DSGVO?

Leben und Arbeiten mit dem neuen Datenschutzrecht

Familienrecht am Mittag
02. Juli 2018, Essen

Quo vadis, DSGVO?

SPIEGEL ONLINE
Kritik von Datenschützern
Daimler verlangt Blutproben von Bewerbern
Autokonzern verlangt nach NDR-Informationen Blutproben von Stellenbewerbern.
Datenschützer sind empört, das Unternehmen weist die Vorwürfe zurück.

DER TAGESSPIEGEL
Datenskandal bei Fahrdienstleister
22.11.2017 07:20 Uhr
Uber vertuscht Hackerangriff auf Fahrgastdaten
Schon im Herbst 2016 haben Hacker Daten von 57 Millionen Fahrgästen und Fahrern von Uber gestohlen. Doch der Fahrdienstvermittler schwieg - und zahlte.

Deutsche Post weist Kritik an Datenweitergabe zurück
Eine Tochterfirma der Post soll CDU und FDP im Bundestagswahlkampf personenbezogene Daten "vermietet" haben. Die Parteien beteuern, sie hätten den Datenschutz beachtet.
1. April 2018, 13:59 Uhr / Aktualisiert am 1. April 2018, 15:41 Uhr / Quelle: ZEIT ONLINE, AFP, dpa, cab,

tagesschau.de

Süddeutsche Zeitung
17. Mai 2010, 21:23 Uhr Handel: Datenskandal
Lidl feuert Deutschland-Chef
Erst der Skandal, dann der Rausschmiss: Der Discounter Lidl trennt sich von Deutschland-Chef Mros - weil er systematisch Krankenakten von Mitarbeitern anfertigen ließ.

ZEIT ONLINE
Daten von 17 Millionen Kunden gestohlen
Nur vier Monate nach Bekanntwerden der Spitzelaffäre muss der Konzern einräumen, dass persönliche Angaben von Millionen Kunden der Tochter T-Mobile entwendet wurden - darunter auch von zahlreichen Prominenten
4. Oktober 2008, 18:37 Uhr

zu 87 Millionen Nutzer betroffen
5.04.2018 00:05 Uhr
book-Skandal weitet sich aus. Die Daten von deutlich mehr Usern als bislang
men könnten mit der Firma Cambridge Analytica geteilt worden sein
nd sind bis zu 310.000 Geschädigte möglich.

WirtschaftsWoche
Postbank sperrt Kontoeinsicht für ihre Berater
27. Oktober 2009
Nach dem Vorwurf des Datenmissbrauchs sperrt die Postbank ihren Finanzberatern die Einsicht in Kundenkonten und prüft zunächst die rechtliche Zulässigkeit. Bank und Datenschützer sind hier uneins.

WirtschaftsWoche
Kabel Deutschland: Daten von Hunderttausenden von Kunden an dubiose Callcenter weitergeleitet
28. März 2009

ZEIT ONLINE
Datenleck bei der Deutschen Post
Eine Datenbank mit 200.000 Umzugsmitteilungen der Post lag ungesch
im Netz. Tausende andere Firmen aus aller Welt haben exakt den gleiche
Fehler gemacht.
5. Juli 2017, 13:59 Uhr

Index

1. DSGVO allgemein

Europäische Datenschutz-Grundverordnung (DSGVO)

- seit 25. Mai 2018 unmittelbare Geltung
- 99 Artikel, 173 Erwägungsgründe
  - Öffnungsklauseln = Gestaltungsspielraum für den nationalen Gesetzgeber ► seit 25. Mai 2018 neues BDSG

Vorteil:

- Vereinheitlichung des bisherigen Europäischen Datenschutz-Flickenteppichs

2. Anwendbarkeit der DSGVO

Sachliche Anwendung, wenn **personenbezogene Daten**

- digital oder
- in einem strukturierten Dateisystem in Papierform

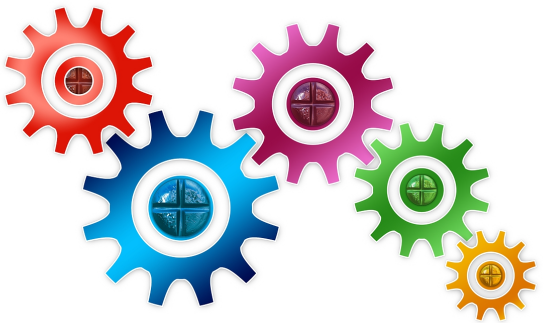
verarbeitet werden.

Weiter Begriff der Verarbeitung!

- Erhebung, Verwendung, Speicherung

Räumliche Anwendung abhängig von Niederlassung des Verarbeiters und/oder Aufenthalt der betroffenen Person in der EU

DSGVO gilt nicht für den ausschließlich persönlichen oder familiären Bereich!



2. Anwendbarkeit der DSGVO

PERSONENBEZOGENE DATEN (Art. 4 Nr. 1 DSGVO)

- alle Informationen, die sich auf identifizierte oder direkt oder indirekt identifizierbare natürliche Person beziehen.
  - z.B. Name, Adresse, Telefonnummer, Email-Adresse, Bankverbindung, Standortdaten, IP-Adresse, Cookie-ID, Endgeräte, … usw.
  - Besonderer Schutz für sensible Daten (vgl. Art. 9 DSGVO):
    - Gesundheitsdaten, biometrische Daten, rassische oder ethnische Herkunft, politische Meinung, sexuelle Orientierung usw.

3. Rechtmäßigkeit der Verarbeitung
3.1 Legitimationsgründe

VERBOT MIT ERLAUBNISVORBEHALT!

- Katalog der **Erlaubnistatbestände** in Art. 6 Abs. 1 DSGVO
  - Verarbeitung u.a. zulässig, wenn
    - **Einwilligung** des Betroffenen gegeben wurde oder
    - Durchführung eines Vertrages / vorvertraglicher Maßnahmen auf Anfrage des Betroffenen oder
    - **Wahrung berechtigter Interessen des Verantwortlichen**

3. Rechtmäßigkeit der Verarbeitung
3.1 Legitimationsgründe

Wirksame Einwilligung erfordert

- eine eindeutige Bestätigungshandlung
  - ihre Widerrufbarkeit
  - eine Information über Zweck und Umfang der Verarbeitung und den Verantwortlichen
- Freiwilligkeit
  - keine Einwilligung im Rahmen eines Koppelgeschäftes (vgl. Art. 7 Abs. 4 DSGVO)

3. Rechtmäßigkeit der Verarbeitung
3.1 Legitimationsgründe

Berechtigtes Interesse des Verantwortlichen rechtfertigt die Verarbeitung (Art. 6 Abs. 1 lit. f DSGVO),

- Sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen
- vernünftige Erwartungen der betroffenen Person, in Beziehung zum Verantwortlichen zu berücksichtigen.
    - z.B. bestehende Kundenbeziehung oder Dienstverhältnis
  - Konnte der Betroffene zum Zeitpunkt der Erhebung der Daten absehen, dass eine Verarbeitung erfolgen würde?
- besondere Schutzbedürftigkeit von Kindern (bis 18 Jahre)

3. Rechtmäßigkeit der Verarbeitung
3.2 Grundprinzipien der Verarbeitung

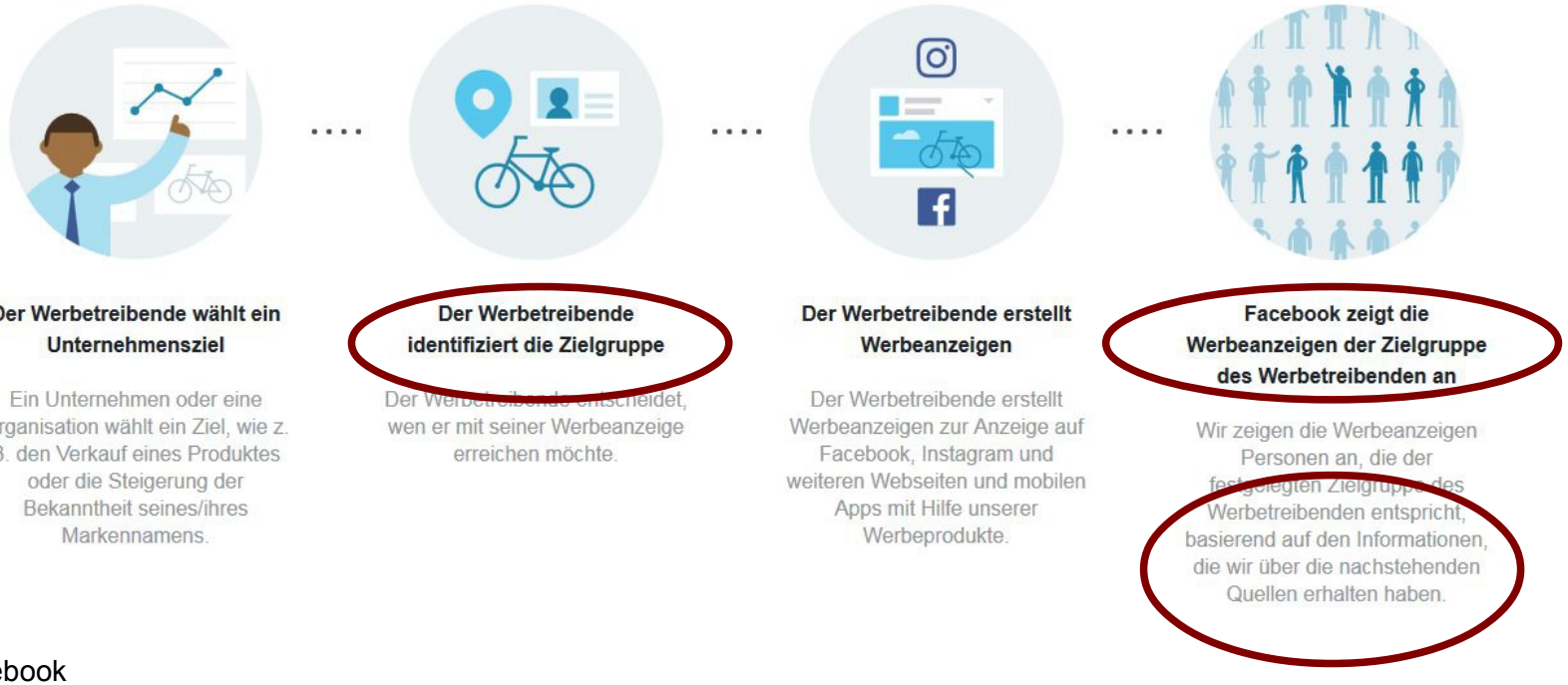
- Verarbeitung personenbezogener Daten sollte **rechtmäßig und nach Treu und Glauben** erfolgen.
- **Datenvermeidung und Datensparsamkeit**
- **Zweckbindung**
  - Erhebung für festgelegte, eindeutige und rechtmäßige Zwecke
- **Widerrufsrecht bei Einwilligung / Widerspruchsrecht bei berechtigten Interessen**
  - Ausdrücklich Widerspruchsrecht bei Direktwerbung und Profiling (OptOut-Möglichkeit zwingend!)

3. Rechtmäßigkeit der Verarbeitung
3.2 Grundprinzipien der Verarbeitung

- **Transparenz**
  - Informationspflicht bei Erhebung personenbezogener Daten (Art. 13 DSGVO):
    - Namen des Verantwortlichen, Zweck der Verarbeitung, Rechtsgrundlage/berechtigtes Interesse, Empfänger der Daten, Dauer der Speicherung
  - Hinweis des Betroffenen auf
    - Recht auf Berichtigung / Vervollständigung, Recht zur Löschung, „Recht auf Vergessenwerden“, „Recht auf Datenübertragung“, Widerrufsrecht / Widerspruchsrecht

4. DSGVO in der Praxis
4.1 Beispiel Online-Marketing

Beispiel: Online-Marketing



Quelle: facebook

4. DSGVO in der Praxis
4.1 Beispiel Online-Marketing

Mögen Sie „Cookies“?

- „xyz verwendet Cookies, um Ihnen den bestmöglichen Service zu gewährleisten. Wenn Sie auf dieser Seite weitersurfen, stimmen Sie der Cookie-Nutzung zu.“
- Cookies sind kleine Textdateien, die auf der Festplatte des Users gespeichert werden. Durch Cookies fließen dem Verarbeiter bestimmte Informationen zu.
- „Cookies machen Internetangebote nutzerfreundlicher und effektiver.“

Ihre Datenspuren

- https://www.story.wiwo.de/2018/05/datenspur/index.html

4. DSGVO in der Praxis
4.1 Beispiel Online-Marketing

Formen des Online Marketings

- Display-Werbung
- Targeting/Retargeting
- Email-Newsletter

Mögliche Probleme:
Rechtmäßigkeit der Verarbeitung

- Berechtigtes Interesse Direktmarketing, Information bei Erhebung, Double-OptIn, ePrivacy-Verordnung

4. DSGVO in der Praxis
4.2 Beispiel Meinungsfreiheit

Presse- und Meinungsfreiheit?

Art. 1 Abs. 1 DSGVO: DSGVO schützt Grundrechte und Grundfreiheiten nat. Personen und insbes. Recht auf Schutz personenbezogener Daten.

Art. 85 DSGVO: Mitgliedstaaten bringen Recht auf Schutz personenbezogener Daten durch **Rechtsvorschriften** in Einklang mit Recht auf

- freie Meinungsäußerung und Informationsfreiheit, einschließlich Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken.

Rechtsvorschrift ist auch GG, z.B. Art. 5 GG, samt der einschlägigen Rechtsprechung

- Meinungsfreiheit nach Art. 5 GG schützt Äußerung und Verbreitung von Meinung in Wort, Schrift und Bild, wenn und soweit sie eine wertenden, meinungsbildenden Inhalt hat.
    - auch für kommerzielle Meinungsäußerungen, sowie reine Wirtschafts- und Imagewerbung

4. DSGVO in der Praxis
4.2 Beispiel Meinungsfreiheit

Bundesgesetzgeber arbeitet NOCH! daran, nationales Recht an neues Datenschutzrecht (DSGVO plus BDSG) anzupassen (Stand 02. Juli 2018).

- Datenschutzrechtliche Regelungen im nationalen Recht sind grds. weiterhin anwendbar.
- „Nationale Normen sind insofern EU-rechtskonform auszulegen.“ (Quelle: Internetauftritt BMI)

Medienrecht:

- Aktualisierung der Rundfunkstaatsverträge und Landespressegesetze erfolgt
- Es gilt sog. Medienprivileg für Journalisten/Redaktionen (= Keine Auskunft über Rechercheergebnisse oder Löschung hiervon auf Verlangen)

4. DSGVO in der Praxis
4.2 Beispiel Meinungsfreiheit

Praxisfall:

Unter welchen Voraussetzungen ist das Anfertigen und Verbreiten personenbezogener Fotografien künftig zulässig?

- Anfertigung und Veröffentlichung personenbezogener Fotografie unterliegt allgemeinen Regelungen des Datenschutzrechts.
- Wie bisher dürfen Fotos daher nur verarbeitet werden, wenn betroffene Person eingewilligt hat **oder eine Rechtsgrundlage dies erlaubt**.
- Einwilligung jedoch vielfach keine praktikable Rechtsgrundlage (größere Menschenmengen, Widerspruchsrecht usw.).
- Weitere mögliche Rechtsgrundlagen:
  - Durchführung eines Vertrags oder
  - **Wahrnehmung berechtigter Interessen**

4. DSGVO in der Praxis
4.2 Beispiel Meinungsfreiheit

- Grundrechte (hier Meinungs- und Informationsfreiheit) stellen berechtigte Interessen nach Art. 6 Abs. 1 lit. f) der Datenschutz-Grundverordnung dar.
- Für Veröffentlichung von Fotografien enthält das Kunsturhebergesetz (KunstUrhG) ergänzende Regelungen, die auch unter Geltung der DSGVO fortbestehen.
    - Das KunstUrhG nutzt nationalen Gestaltungsspielraum nach Art. 85 Abs. 1 DSGVO zum Ausgleich zwischen Datenschutz und Meinungs- und Informationsfreiheit.

§ 23 KunstUrhG (verkürzt): Ohne die … erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

- Bildnisse aus Bereich der Zeitgeschichte; Bilder, auf denen Personen nur Beiwerk sind; Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen dargestellte Personen teilgenommen haben; Bildnisse, ... sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

Lösung:

Die DSGVO führt zu keinen wesentlichen Veränderungen der bisherigen Rechtslage im Umgang mit Fotografien!

5. Pflichten des Verantwortlichen
5.1 Beweislast und Dokumentation

Verzeichnis der Verarbeitungstätigkeiten

(Art. 30 DSGVO, § 70 BDSG)

- Immer, wenn die Verarbeitung nicht nur gelegentlich erfolgt!

- Umsetzung und **Dokumentation der Technischen und Organisatorischen Maßnahmen** (Art. 32 DSGVO, § 64 BDSG)
  - Speicher-, Zugriffs-, Übertragungs-, Eingabe-, Transportkontrolle, Widerherstellbarkeit, Zuverlässigkeit usw.
- Protokollierungspflichten
  - in automatisierten Verarbeitungssystemen
  - Erhebung, Veränderung, Abfrage, Offenlegung, Löschung

5. Pflichten des Verantwortlichen
5.1 Beispiel E-Mail Verschlüsselung

Art. 32 DSGVO: Sicherheit der Verarbeitung

- Schaffung eines dem Risiko angemessenes Schutzniveaus
- durch geeignete technische und organisatorische Maßnahmen
- unter Berücksichtigung des Stands der Technik, der Implementierungskosten und Art, Umfang und Zweck der Verarbeitung
- sowie der Eintrittswahrscheinlichkeit des Risikos

5. Pflichten des Verantwortlichen
5.2 Beispiel E-Mail Verschlüsselung

Art. 32 Abs. 1 lit. a DSGVO: …
Verschlüsselung personenbezogener Daten

- Transportverschlüsselung (TLS / SSL)
- End-to-End-Verschlüsselung (PGP, S/MIME)
- Containerlösung

  Einwilligung zum Verschlüsselungsverfahren durch den Mandanten möglich und erforderlich?

- Check TLS-Verschlüsselung auf Empfängerseite: https://www.checktls.com/TestReceiver

5. Pflichten des Verantwortlichen
5.3 Bennung eines DSB

Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO, § 38 BDSG)

… ist z.B. erforderlich

- soweit mindestens 10 Personen ständig mit automatisierter Verarbeitung personenbezogener Daten beschäftigt sind oder
- wenn „die Kerntätigkeit des Verantwortlichen … in der **umfangreichen Verarbeitung** besonderer Kategorien von Daten gem. Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 besteht“
- ...

5. Pflichten des Verantwortlichen
5.4 Prozesse

Sicherstellen, dass …

- Verträge datenschutzkonform geschlossen oder erweitert sind (Verträge über die Verarbeitung von personenbezogenen Daten im Auftrag erforderlich?)
- Auskunftsersuchen fristgerecht nachgekommen werden kann.
- Löschungen vorgenommen werden können.
- Meldung von Verstößen binnen 72 Stunden an Aufsichtsbehörden und u.U. Benachrichtigung an die Betroffenen erfolgen kann.

- **Prozesse aufsetzen und dokumentieren!**

5. Pflichten des Verantwortlichen
5.4 Sanktionen

Sanktionen

- Befugnisse der Aufsichtsbehörden:
  - **Untersuchung / Abhilfe** (Art. 58 DSGVO)
  - **Bußgelder** bis zu 4% des Jahresumsatzes bzw. bis zu 20 Mio. EUR … je nachdem, welcher Betrag höher ist.
  - Höhe im Einzelfall nach Art, Schwere und Dauer des Verstoßes
- **Schadensersatz** für mat. oder immat. Schäden (Art. 82 DSGVO)
- **Abmahnungen**
  - Sind Vorschriften der DSGVO Marktverhaltensregeln i.S.d. § 3a UWG?

5. Pflichten des Verantwortlichen
5.5 Sanktionen

Sanktionen

- Befugnisse der Aufsichtsbehörden:
  - **Untersuchung / Abhilfe** (Art. 58 DSGVO)
  - **Bußgelder** bis zu 4% des Jahresumsatzes bzw. bis zu 20 Mio. EUR … je nachdem, welcher Betrag höher ist.
  - Höhe im Einzelfall nach Art, Schwere und Dauer des Verstoßes
- **Schadensersatz** für mat. oder immat. Schäden (Art. 82 DSGVO)
- **Abmahnungen**
  - Sind Vorschriften der DSGVO Marktverhaltensregeln i.S.d. § 3a UWG?

Vielen Dank für Ihre Aufmerksamkeit!

Martin Erlewein
Rechtsanwalt, Steuerberater,
Fachanwalt für Steuerrecht
Datenschutzbeauftragter (extern)

Alte Poststr. 28b
42555 Velbert

Telefon: +49 (0) 2052 8352343
Mobil:: +49 (0) 176 85614332

E-Mail: info@kanzlei-erlewein.de

Internet: www.kanzlei-erlewein.de