The next big thing
–
Was Administratoren jetzt über DSGVO und ePrivacy-Verordnung wissen müssen

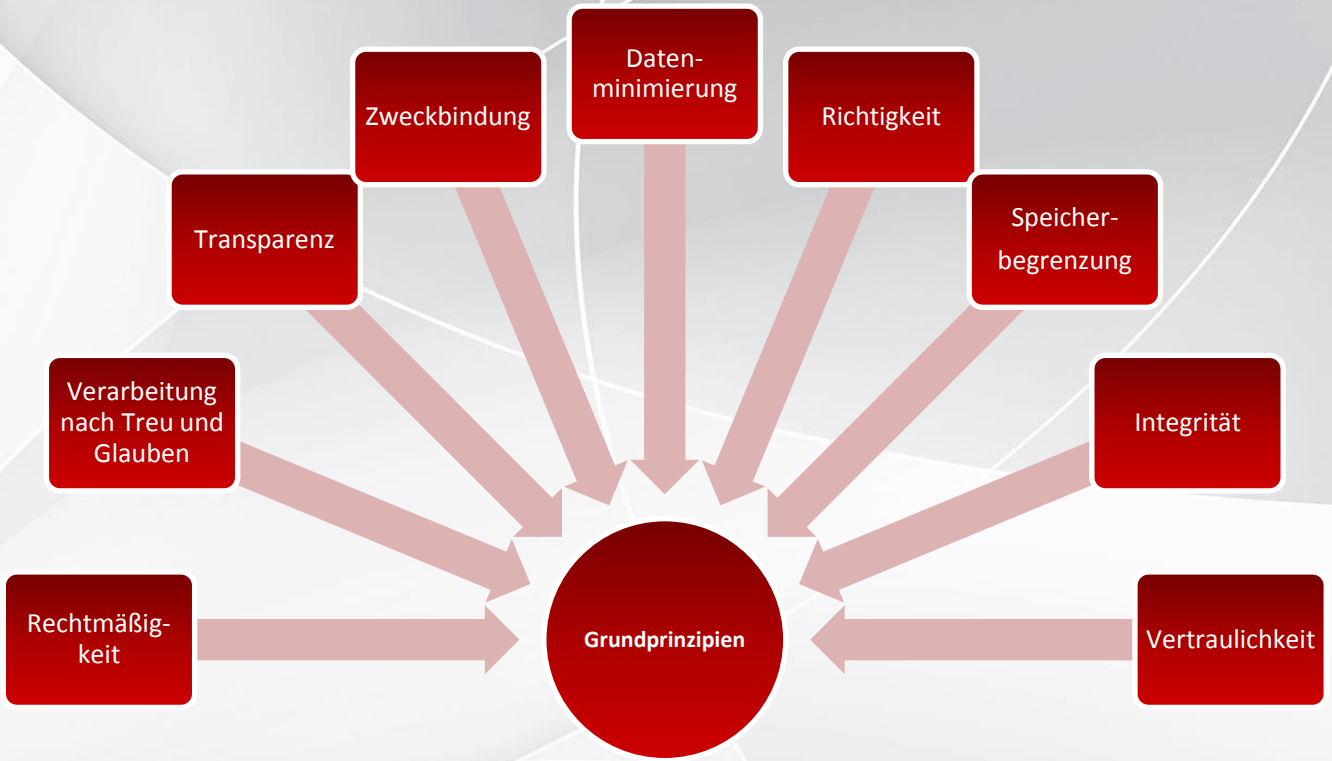
GLOBAL DATA PROTECTION CONSULTING

Securing Business for the Future

Agenda

I. Grundsätzliches zur DSGVO
II. Administratoren und DSGVO
III. Schwerpunkt Data-Breach
IV. ePrivacy-VO
V. Allgemeines zur ePrivacy-VO
VI. Regelungsinhalte
VII. Offene Fragen

Grundsätze der DSGVO




Rechenschaftspflicht
Grundsatz der Zweckbindung
Verbot mit Erlaubnisvorbehalt
Grundsatz der Speicherbegrenzung
Grundsatz der Datenminimierung
Verarbeitung auf rechtmäßige und transparente Weise sowie nach Treu und Glauben
Grundsätze der Integrität und Vertraulichkeit
Vorgaben für die transparente Information und Kommunikation
Berichtigung
Auskunftspflichten
Datenportabilität
Widerspruchsrecht
Benachrichtigungen
Benennung eines Vertreters
Nachweispflicht
Informationspflichten
Informationspflichten
Rechenschaftspflicht
Richtigkeitsgrundsatz
Grundsatz der Zweckbindung
Geheimhaltungsvorschriften.
Sonderregeln für nationale Kennziffern
Widerspruchsrecht
Datenportabilität
Berichtigung
Benachrichtigungen
Verbot mit Erlaubnisvorbehalt
Vervollständigung
Richtigkeitsgrundsatz
Nachweispflicht
Auskunftspflichten
Schutzvorschriften zu Gunsten von Kindern

Administrator im Spannungsfeld

Beispiel Auftragsverarbeitung

- Bsp.: Administrator des Unternehmens hat den Auftrag, eine Speicherlösung in der Cloud auszuwählen.
- Spannungsverhältnis Informationssicherheit vs. Datenschutz

- Technische Geeignetheit (bspw. entsprechende Zertifizierungen)

- Standorte: Innerhalb EWR; geeignete Garantien; Angemessenheitsbeschl. Kommission
- Kontrollmöglichkeit?
- Hat der Auftragsverarbeiter einen DSB bestellt?
- Rechtsgrundlage der Auftragsverarbeitung?
- Regelungen zur Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten im Auftrag enthalten?
- Unterstützungspflichten klar geregelt?
- …

Datenportabilität

- „Digitaler Umzugsservice“ primär für soziale Netzwerke, aber auch bspw. E-Mail-Provider.
- Achtung: Umfasst sind nur Daten, die der Betroffene direkt selbst bereitgestellt hat, nicht Daten, die der Verantwortliche aus diesen Daten selbst generiert hat
- Die DSGVO erlaubt die Speicherung personenbezogener Daten in strukturierter, maschinenlesbarer Form und wahrt damit das Recht des Betroffenen, diese Daten auf ein anderes Unternehmen zu übertragen.

Handlungsbedarf

- Speichermedium mit Sicherheitsfunktionen wie Verschlüsselung, Integritätskontrolle
- Vor dem Datenträgertransport Vollsicherungen der Daten (Schutz vor Datenverlust)
- Zugriffsschutz vor, während und nach dem Datenträgertransport (unter anderem Verschlüsselung)
- Schriftliche Regelung des Transports der Datenträger
- Revisionsfähige Aufzeichnungen über den Datenträgeraustausch
- Versand von Datenträgern ausschließlich mit Begleitpapieren
- Identitätsprüfung beim Empfänger der Daten
- Verschließbare Transportbehältnisse, genaue Schlüsselregelungen
- Trennung der Daten verschiedener Kunden bei dem Datenträgertransport.

Datenpannen Einführung

- IT-technische und tatsächliche Bedrohungen sind ubiquitär
- Regelungen zum Umgang mit Datenpannen seit Längerem (z.B. ePrivacy RL und VO/EU Nr. 611/2013)
- Anzahl gemeldeter „Datenpannen steigt (national)
  - 305 gemeldete Fälle zu 177 einschlägigen Fällen, Stand 2013
  - Dunkelziffer wohl weit höher <10000
- Negative Auswirkungen durch Datenpannen
  - Hohe Bußgelder bei Verstößen
  - Schadensersatzansprüche
  - Reputative Schäden

Arten von Schutzverletzungen

- Vernichtung (alle Formen von Datenlöschung)
- Verlust (temporär oder dauerhaft)
- Veränderung (inhaltliches Umgestalten - Datenintegrität)
- Unbefugte Offenlegung und Zugang

- Im Falle einer SV Meldung innerhalb 72h bei der Aufsichtsbehörde. Außer SV führt nicht zu einem (normalen) Risiko für die Betroffenen.

Typische Fälle von Datenpannen

Bedrohung von Innen
z.B. Mitarbeiter

Bedrohung von Außen,
z.B. Hacker

<u>Beispiele</u>
Verlust Smartphone/Laptop

Falschversendung oder Veröffentlichung von Daten

IT-und Funktionsfehler

<u>Beispiele</u>
Datenverlust (Social Engineering)

Hackerangriff auf Datenbank

Unverzüglichkeit der Benachrichtigung

- Anknüpfungspunkt?
  - Feststellung der Schutzverletzung? (-)
  - Feststellung des Risikos? (+)
    - Zweck: Begrenzung der Risiken für Betroffene
    - Art und Schwere der möglichen Folgen maßgebend

- Konsequenz:
  - „Sofortige“ Feststellung = längere Frist
  - „Verzögerte“ Feststellung = kürzere Frist

Benachrichtigung Aufsichtsbehörde

- Beschreibung der Art der Schutzverletzung (bspw. Vernichtung etc.)
- Kategorien der betroffenen Personen (Mitarbeiter, Kunden, Lieferanten)
- Ungefähre Anzahl der Betroffenen
- Kategorien der Daten und Anzahl der Datensätze
- Name und Kontakt des DSB oder sonstige Anlaufstelle (auch Admin)
- Beschreibung der wahrscheinlichen Folgen der Schutzverletzung (Identidätsdiebstahl; Kreditkatenmissbrauch etc.)
- Beschreibung der ergriffenen oder vorgeschlagenen Gegenmaßnahmen

Handlungsbedarf

- Einführung Data-Breach-Management-Systems
  - 1. Planen und Feststellen (Data Loss Detection, EG 87)
  - 2. Bewertung der Schutzverletzung
  - 3. Meldung, Abstimmung und Kommunikation
  - 4. Ermittlungen tätigen und Dokumentation
  - 5. Verbesserung/Anpassung der Systeme und Maßnahmen
- Abstimmung mit Aufsichtsbehörden bei Beurteilung der Schutzverletzung, auch bei Anwendbarkeit von Ausnahmen
- Falls möglich – Rückgriff auf Ergebnisse aus Datenschutz-Folgenabschätzung bei Beurteilung des durch die Schutzverletzung entstandenen Risikos empfehlenswert

Handlungsbedarf

- Zur Schutzverletzung :
  - Präventive Fokussierung auf Hauptziele der IT-Sicherheit in einem Sicherheits- und Notfallkonzept
  - Lebenszyklusplan für die Daten erstellen
  - Strenge Zugangs- und Berechtigungskonzepte etablieren

- Zur Feststellung der Schutzverletzung:
  - Zeitnahe Feststellung der Schutzverletzung durch geeignete weitere Maßnahmen und Prozesse
  - Vertragliche Festlegung von Ermittlungs- und Mitteilungspflichten des Auftragsverarbeiters inkl. des Unterstützungsumfangs – Übermittlung in Textform

Handlungsbedarf

- Zur Benachrichtigung:
  - Unverzüglichkeit und Informationsgehalt im Fokus
  - Zeitnahe Ermittlung aller notwendigen Informationen
  - Effiziente Anpassung interne Abstimmungs- und Kommunikationsprozesse

- Zur Vermeidung von „hohen Risiken“:
  - Fokussierung auf die zur Beurteilung von Risiken wichtigen Parameter (Kontext, Wesen, Umfang, Zweck sowie Art, Inhalt und Umfang der Daten)
  - Klassifizierung von Daten nach Risikopotenzial und szenarienspezifische Risikoermittlung von „häufigen“ Schutzverletzungen im Vorfeld

ePrivacy-Regulierung bis dato

- 1997: RL 97/66EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation „ISDN-Richtlinie“
- 2002: RL 2002/58/EG Datenschutzrichtlinie für elektronische Kommunikation „ePrivacy-RL“ mit Änderungen durch RL 2009/136/EG

Umsetzung ePrivacy

- **TKG** Teil 7 (§§ 88 – 115): Fernmeldegeheimnis, Datenschutz, öffentliche Sicherheit
- **TMG** §§ 11 – 16: Verarbeitung von Cookies durch Telemedienanbieter
- **UWG** § 7: Unzulässigkeit von Direktwerbung
- **StGB**: installieren von Spyware/Malware auf Endgeräten


11.4.2016
Start der öffentlichen Konsultation zur Überarbeitung der ePrivacy-RL
5.7.2016
Abschluss der Konsultation
4.8.2016
Veröffentlichung der Ergebnisse
10.1.2017
EU-Kommission veröffentlicht ersten Entwurf
15.2.2017
Veröffentlichung der amtlichen deutschen Version
22.5.2017
Stellungnahme ITRE-Ausschuss
29.5.2017
Stellungnahme IMCO-Ausschuss
9.6.2017
Stellungnahme LIBE-Ausschuss
10.6.2017
LIBE-Ausschuss übermittelt Änderungsvorschläge an EU-Parlament
26.10.2017
Beschluss des EU-Parlamentsentwurfs
1711.2017
Veröffentlichung Sachstandsbericht EU-Ratspräsidentschaft
6.2018
Gemeinsamer Standpunkt EU-Rat
Ende 2018
Trilog-Verhandlungen
Anfang 2019
Inkrafttreten
2016
2017
2018
2019

Inhalte der ePrivacy-Verordnung

- Vertraulichkeit der Kommunikation
- Rechtmäßigkeit der Verarbeitung
- Schutz vor Informationen aus Endeinrichtungen
- „traditionelle“ Regelungen zu Rufnummern
- Öffentlich zugängliche Verzeichnisse
- Direktwerbung
- Aufsicht

ePrivacy-VO / DSGVO

- Lex specialis bei Verarbeitung personenbezogener Daten natürlicher Personen
  - Kommunikationsdaten
  - Informationen aus Endeinrichtungen
  - Aufsicht
- Lex generalis
  - Vertraulichkeit der Kommunikation
  - Verarbeitung von Daten juristischer Personen

Anpassung TKG

- Anpassung an DSGVO
  - Aufhebung der Vorschriften im Anwendungsbereich der DSGVO, die nicht die ePrivacy-RL umsetzen
  - Kurzfristig im Rahmen eines Omnibusgesetzes zur Anpassung von Spezialgesetzen an die DSGVO
- Anpassung an Kodex nach Abschluss der Kodex-Verhandlungen
- Anpassung an ePrivacy-VO nach Abschluss der ePrivacy-Verhandlungen

Anpassung TMG

- DSGVO lässt keine Sonderregelung für Dienste der Informationsgesellschaft
- Grundsätzlich: Aufhebung von TMG-Vorschriften im Anwendungsbereich der DSGVO
- Aber: weiterhin Umsetzung der Cookie-Regelung
- Problem: Rechtsunsicherheit durch voranschreitende Rechtsentwicklung
  - EuGH C-673/17: BGH-Vorlagefrage zur Auslegung von Art. 5 Abs. 3 ePrivacy-RL
  - Neuregelung durch die ePrivacy-VO
- Lösung: vorerst keine Anpassung des TMG, bis ePrivacy-VO abgeschlossen ist
- DSGVO gilt für Reichweitenmessung und Einsatz von Tracking-Mechanismen

ePrivacy-VO – Offene Fragen

- Bezugnahme auf Definitionen
  - DSGVO
  - Kodex
- M2M-Kommunikation
- Beschränkung auf den Übertragungsvorgang
- Zusätzliche Befugnisse zur Verarbeitung von:
  - Kommunikationsmetadaten
  - Informationen aus Endeinrichtungen
- Anforderungen an Browsersoftware
- Regelungen zu öffentlich zugänglichen Verzeichnissen
- Aufsicht

Sicherheitspflichten Betreiber elektronischer Kommunikationsdienste

- Endnutzer sind über Sicherheitsrisiken zu informieren
- Ausreichend vor unbefugtem Zugriff geschützt
- Vertraulichkeit und Integrität
- Optionaler Selbstdatenschutz darf nicht verhindert werden
- Data-breach-Notification gem. Art. 33 /34 DSGVO bleibt unberührt

Beschränkung auf Übertragung

- Wann endet der Übertragungsvorgang?
  - Sind Daten beim Provider noch „in transmission“, wenn der Endnutzer Zugriff darauf hat (Mailbox)?
- Wann muss der Provider löschen?
- Wann darf der Provider nach der DSGVO weiter verarbeiten?
- Rechtslage in Deutschland
  - Fernmeldegeheimnis gilt auch nach Ende des Übertragungsvorgangs
  - Daten beim Endnutzer fallen nicht unter das Fernmeldegeheimnis, sondern unter allgemeinen Datenschutz

Definitionen

- Kodex: insbesondere elektronische Kommunikationsnetze und –dienste sowie Endnutzer
  - Wird an einer Stelle diskutiert
  - Problem: Einbeziehung von Diensten mit Kommunikation als Nebenfunktion
- DSGVO: insbesondere Bedingungen für die Einwilligung
  - Problem: Einwilligung für juristische Personen
  - Problem: Einwilligung mittels Browsereinstellungen

M2M-Kommunikation

- Derzeit: keine besondere Erwähnung in der ePrivacy-RL
- ePrivacy-VO:
  - Kommission schlägt Erwägungsgrund vor: Schutz der Privatsphäre der Endnutzer auch bei M2M
  - Rat prüft Einbeziehung in Art. 5 (Vertraulichkeit der Kommunikation)
- Problem: Unscharfe Trennung zwischen M2M-Diensten und Übermittlung
- Erlaubt:
  - Nötig für die Herstellung einer vom Nutzer angeforderten Verbindung
  - Einwilligung
  - Eindämmung der Risiken
- Risiko: Innovationshemmnis durch ePrivacy

Kommunikationsmetadaten

- Hilfreich: Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten
  - Quelle/Adressat einer Nachricht
  - Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung
  - Art einer Nachrichtenübermittlung
  - Rufnummern, Gerätekennungen
  - Standortdaten (Cell-ID)
- Abschließende Tatbestände in Art. 6
- Unproblematisch, wenn für Durchführung der Übermittlung der Kommunikation nötig

Kommunikationsinhalte

- Generell: Einwilligungserfordernis
- Parlamentsposition sieht Relativierung vor, wenn durch die angeforderte Verarbeitung die Grundrechte und Interessen eines anderen Nutzers oder mehrerer anderer Nutzer nicht beeinträchtigt werden

Anforderungen an (Browser-)Software

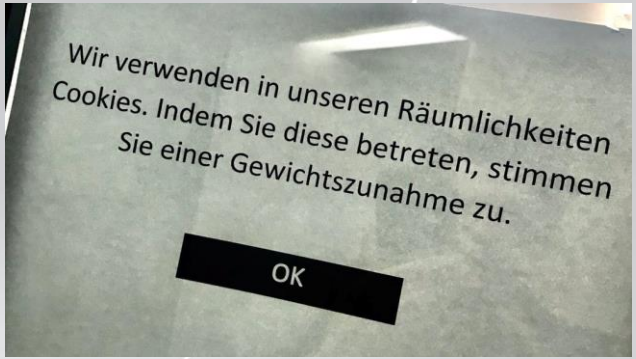
- Neu: (Browser-)Software soll bei Installation oder erstmaliger Nutzung
  - Endnutzer über Einstellungen zum Schutz der Privatsphäre informieren
  - Endnutzer soll in Einstellungen einwilligen
- Das Speichern von Informationen durch Dritte und unberechtigte Kenntnisnahme gespeicherter Informationen muss verhindert werden

Schutz der Endeinrichtungen

- Bisher: Art. 5 Abs. 3 ePrivacy-RL (Cookie-Regelung)
- Enge gesetzliche Befugnis zur Verarbeitung von Informationen aus Endeinrichtungen
- Einwilligungsprinzip
- Problem: Einwilligungsbedingungen der DSGVO erscheinen nicht praktikabel für Einwilligung per Mausklick
- Strittig: besondere Betrachtung der Auswirkungen auf werbefinanzierte Online-Dienste (Drittanbieter-Cookies)

Cookies und DSGVO

- Cookies sind gem. DSGVO sog. Online-Kennungen
- Einsatz ohne explizite Nutzereinwilligung nur in sehr eng begrenzten Voraussetzungen
- Positionsbestimmung DSK: Einwilligung immer erforderlich



Frederick Richter via Twitter

Pflichten für die Betreiber öffentlich zugänglicher Verzeichnisse

- Art. 15 e-Privacy-VO-E befasst sich mit der Regelung öffentlich zugänglicher Verzeichnisse
- Konsequenzen:
  - Einholung der Einwilligung nat. Personen in die Aufnahme des Verzeichnisdienstes
  - Überprüfungs-, Berichtigungs-, Löschungsanspruch für nat. Personen
  - Einwilligung bez. der Suchfunktionalitäten
  - Widerspruchs-, Überprüfungs-, Berichtigungs-, Löschungsanspruch für juristische Personen
  - Kostenlos
  - Ex ante Nutzerinformation

Öffentlich zugängliche Verzeichnisse im Anwendungsbereich der ePrivacy-VO

- Art. 4 Abs. 3 lit. d e-Privacy-VO-E
  - Öffentliche Verzeichnisse in gedruckter oder elektronischer Form
  - Verzeichnis von Endnutzern
  - Auch mit Verzeichnisauskunftsdienst
- EG 30 Satz 1 e-Privacy-VO-E
  - Informationen wie: Telefonnummern, E-Mail-Adressen und andere Kontaktangaben

Pflichten für die Betreiber öffentlich zugänglicher Verzeichnisse

- Parlamentsposition:
  - Sämtliche Anbieter elektronischer Kommunikationsdienste (Legislativbericht v. 20.10.2017, Amendment 128, S. 74)
- Ratsposition:
  - Lediglich Inanspruchnahme Nummerngebundener interpersoneller Kommunikationsdienste (Ratsdokument 13217/17 v. 16.10.2017, S. 13).

- Trilog-Verfahren ist entscheidend

Vielen Dank für die Aufmerksamkeit

GLOBAL DATA PROTECTION CONSULTING

Securing Business for the Future

Stephan Blazy

Ludwig-Erhard-Str. 12

34131 Kassel

stephan.blazy@gdpc.de