WERNER RECHTSANWÄLTE INFORMATIKER

Art. 37 (5) DATENSCHUTZ FORTBILDUNG DS-GVO

Köln, 16. Juni 2020

# DSB-Fortbildung, Art. 37 (5) DS-GVO

**Rechtsanwalt Roman Pusep**
**Fachanwalt für IT-Recht**

**WERNER Rechtsanwälte Informatiker, Oppenheimstr. 16, 50668 Köln**
**https://www.werner-ri.de** **Telefon: 0 221 / 97 31 43 - 0**
**E-Mail: info@werner-ri.de** **Telefax: 0 221 / 97 31 43 - 99**



## Ihr Referent

**Roman Pusep**
Rechtsanwalt, Fachanwalt für IT-Recht
Zertifizierter externer Datenschutzbeauftragter (TÜV)

**WERNER Rechtsanwälte Informatiker**
Oppenheimstraße 16, 50668 Köln

Telefon 0 221 / 97 31 43 - 73
Telefax 0 221 / 97 31 43 - 99

roman.pusep@werner-ri.de
https://www.werner-ri.de

## Inhalte

- Einführung: Ausgewählte Datenschutzbegriffe
- Auswirkungen des 2. DSAnpUG-EU (Datenschutzanpassungsgesetz)
- Hinweise der DSK zu Bußgeldern
- Leitlinie des EDSA zu Cookies
- Erklärungen der Datenschutzbehörden und Urteile





## Präambel / Prolog / Ouvertüre / Disclaimer

- Immer noch kaum Rechtssicherheit
- Daher WICHTIG:

**Sie hören nur Meinungen!**

Es gibt zwar schon eine fundierte wissenschaftliche Auseinandersetzung mit vielen Themen, aber noch keine oder kaum Rechtsprechung, daher Vieles offen... **Folge:** Denken, Umsetzen, Dokumentieren

# Ticker: Corona-Warn-App (CWA)

- Seit 16.06.2020 im App Store und Google Play




DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

# Ticker: Corona-Warn-App (CWA)

- Verantwortlicher: **RKI**
  - Robert Koch-Institut = zentrale Einrichtung des Bundes im Bereich der öffentlichen Gesundheit und nationales Public-Health-Institut
- Funktion:
  - Aktivierte „**Risikoermittlung**" per BlueTooth
  - Entfernungsmessung aufgrund Signalstärke
  - Zufallscode (Zufalls-ID) für jedes Smartphone (alle 10 bis 20 min. neu)
  - Bei bestätigter Infektion => Information an Risikopersonen

# Ticker: Corona-Warn-App (CWA)

- Datenschutzaspekte
  - Datenarten
    - Zugriffsdaten (auf App-Server): IP-Adresse wird auf Load Balancer maskiert und gelangt nicht zum Server; Datum und Uhrzeit des Abrufs (Zeitstempel); übertragene Datenmenge (bzw. Paketlänge); Meldung über erfolgreichen Abruf – Technisch erforderlich, keine Speicherung
    - Begegnungsdaten: per Bluetooth Low Energy sendet das Smartphone an andere Smartphones die Zufalls-ID mit aktiver „**Kontaktaufzeichnung**" und empfängt solche Daten

      => Kontaktaufzeichnung ist eine Smartphone-Betriebssystem-Funktion



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

# Ticker: Corona-Warn-App (CWA)

- Datenschutzaspekte
  - Datenarten
    - Begegnungsdaten: Zusätzlich zur Zufalls-ID werden gespeichert:
      - Datum und Zeitpunkt des Kontakts
      - Dauer des Kontakts
      - Bluetooth-Signalstärke des Kontakts
      - Verschlüsselte Metadaten (Protokollversion und Sendestärke)

# Ticker: Corona-Warn-App (CWA)

- Datenschutzaspekte
  - Risiko-Ermittlung
    - Regelmäßiger Abruf von Zufalls-IDs von positiv getesteten Nutzern
    - Weitergabe der App-Daten an Kontaktaufzeichnung (intern; offline; lokal)
    - Abgleich zwischen gespeicherten und „positiven" Zufalls-IDs
    - Falls Übereinstimmung: Kontaktaufzeichnung gibt an App Begegnungsdaten (Datum, Dauer, Signalstärke), nicht jedoch die „positive" Zufalls-ID
    - App analysiert das individuelle Infektionsrisiko (Interpretation der Bewegungsdaten per Bewertungsalgorithmus)



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

# Ticker: Corona-Warn-App (CWA)

- Datenschutzaspekte
  - Test registrieren
    - QR-Code vom Arzt einscannen
    - Falls Labor an den CWA-Server (Testergebnis-Datenbank) angeschlossen ist, informiert die App, wenn der Test ausgewertet ist
    - Testergebnis kann übermittelt werden, hierfür **weitere Einwilligung** nötig
    - CWA-Server leitet das Testergebnis nur weiter, ohne Inhaltskenntnis

# Ticker: Corona-Warn-App (CWA)

- Datenschutzaspekte
  - Testergebnis teilen
    - App überträgt gespeicherte Zufalls-IDs der letzten 14 Tage an CWA-Server
    - CWA-Server trägt „positive" Zufalls-ID in „Positiv-Liste"/„Infizierten-Liste" ein
    - Funktion „Testergebnis teilen" unabhängig von „Test registrieren"
    - Verarbeitungsgrundlage: **weitere Einwilligung**
    - Folge des Widerrufs: „RKI hat keine Möglichkeit, bereits übermittelte Zufalls-IDs unmittelbar aus den bereitgestellten Listen und von Smartphones anderer Nutzer zu löschen." (**!?**)



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

# Ticker: Corona-Warn-App (CWA)

- Datenschutzaspekte
  - Datenlöschung
    - Zufalls-IDs (eigene und fremde) in der CWA-App nach 14 Tagen
    - Begegnungsdaten in der Smartphone-Kontaktaufzeichnung (Google/Apple ?)
  - IT-Unternehmen (AV-Vertrag nach Art. 28 DS-GVO)
    - T-Systems International GmbH
    - SAP Deutschland SE & Co. KG

# Ticker: Corona-Warn-App (CWA)

- Fragen/Themen
  - Blackbox „Google Apple Protokoll" (GAP)
  - Wie sieht eine Risikobenachrichtigung aus?
  - Sind Updates Pflicht (wg. Bewertungsalgorithmus)?





# Inhalte

- Einführung: Ausgewählte Datenschutzbegriffe
- Auswirkungen des 2. DSAnpUG-EU (Datenschutzanpassungsgesetz)
- Hinweise der DSK zu Bußgeldern
- Leitlinie des EDSA zu Cookies
- Erklärungen der Datenschutzbehörden und Urteile

# Einführung: Ausgewählte Datenschutzbegriffe

- **Art. 4 Nr. 4 DS-GVO – Verantwortlicher** ist …
  - die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
  - Wer konkret handelt, spielt also keine Rolle; bestätigt durch **DSK-Entschließung: Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten (03.04.2019)**
    - Art. 83 DS-GVO: Haftung für schuldhafte Datenschutzverstöße der Beschäftigten, sofern kein Exzess vorliegt



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

# Einführung: Ausgewählte Datenschutzbegriffe

- **Art. 4 Nr. 11 DS-GVO – Einwilligung** …
  - der betroffenen Person ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist
  - => Einwilligungen sind anspruchsvoll und komplex, sie sollten daher sparsam genutzt werden: ...

## Einführung: Ausgewählte Datenschutzbegriffe

- ErwG 32 DS-GVO (und Art. 4 Nr. 11 DS-GVO): Einwilligung erfolgt...
  - durch eine eindeutige, bestätigende Handlung
  - in informierter Weise (mindestens Information über Verantwortlichen und Zwecke, ErwG 42 DS-GVO)
  - nur freiwillig (dann, wenn echte oder freie Wahl, die Einwilligung ohne Nachteile zu verweigern oder zurückzuziehen, ErwG 42 DS-GVO)
  - für den konkreten Fall
  - in unmissverständlicher Weise: schriftlich, elektronisch, mündlich oder durch anderes aktives Verhalten





## Einführung: Ausgewählte Datenschutzbegriffe

- ErwG 42 DS-GVO
  - Verantwortlicher muss Einwilligung und Umfang nachweisen können (auch Art. 7 Abs. 1 DS-GVO)
  - vorformulierte Einwilligungserklärung (auch Art. 7 Abs. 2 DS-GVO)
    - muss verständlich sein
    - muss in leicht zugänglicher Form sein
    - muss in einfacher Sprache sein
    - darf keine missbräuchlichen Klauseln beinhalten

# Einführung: Ausgewählte Datenschutzbegriffe

- ErwG 43 DS-GVO (auch Art. 7 Abs. 4 DS-GVO)
  - Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.
  - => Unnötige Einwilligungen also kontraproduktiv!



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

# Einführung: Ausgewählte Datenschutzbegriffe

- Art. 7 Abs. 3 DS-GVO
  - Einwilligung ist jederzeit – für die Zukunft – widerruflich
  - Verantwortlicher informiert hierüber (vgl. Art. 13 Abs. 2 lit. c) DS-GVO)
  - Widerruf muss so einfach wie die Erteilung der Einwilligung sein
- Art. 20 DS-GVO
  - Datenübertragbarkeit bei Einwilligung und Vertragserfüllung

# Einführung: Ausgewählte Datenschutzbegriffe

- **Art. 4 Nr. 8 DS-GVO – Auftragsverarbeiter** ist …
  - eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
- Beschränkung?
  - Reicht eine Datenverarbeitung und ein Auftrag?
  - Einschränkung nach Kerntheorie?



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

# Einführung: Ausgewählte Datenschutzbegriffe

- **Art. 4 Nr. 8 DS-GVO – Auftragsverarbeiter**
- Folge: AV-Vertrag nach Art. 28 DS-GVO
  - **Verantwortlicher ist und bleibt verantwortlich!**
  - Auftragsverarbeiter haftet nur bei Verletzung des AV-Vertrages

# Einführung: Ausgewählte Datenschutzbegriffe

- **Widerruf und Widerspruch**
- Art. 7 Abs. 3 S. 1 DS-GVO – Widerruf
  - Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen.
  - **Folge**: Keine auf Einwilligung gestützte Datenverarbeitung in der Zukunft.





# Einführung: Ausgewählte Datenschutzbegriffe

- **Widerruf und Widerspruch**
- Art. 21 Abs. 1 DS-GVO – Widerspruch
  - Betroffener kann aus Gründen einer besonderen Situation jederzeit gegen die Datenverarbeitung nach Art. 6 Abs. 1 lit. f) DS-GVO widersprechen.
  - **Folge**: Prüfung der sich gegenüberstehenden Interessen: zwingende schutzwürdige Gründe für die Verarbeitung vs. besondere Situation.
  - Dann gegebenenfalls: Keine Datenverarbeitung in der Zukunft.

# Einführung: Ausgewählte Datenschutzbegriffe

- **Verschlüsselung**
  - Maßnahme zur Risikoeindämmung (Art. 83 DS-GVO)
  - Geeignete Garantien (Art. 6 Abs. 4 lit. e) DS-GVO)
  - Technische und organisatorische Maßnahmen – TOM (Art. 32 Abs. 1 lit. a) DS-GVO)
  - Kein hohes Risiko bei Datenpanne, sodass Betroffene nicht zu informieren sind (Art. 34 Abs. 3 lit. a) DS-GVO)



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

# Einführung: Ausgewählte Datenschutzbegriffe

- **Verschlüsselung** ist
  - Pseudonymisierung?
    - Art. 4 Nr. 5 DS-GVO: Pseudonymisierung ist Datenverarbeitung, sodass personenbezogene Daten nur mit zusätzlichen Informationen einer betroffenen Person zugeordnet werden können, sofern diese Informationen gesondert sicher aufbewahrt werden
  - Anonymisierung?
    - ErwG 26 DS-GVO: Anonyme Daten sind Informationen, die sich nicht (mehr) auf eine identifizierte oder identifizierbare Person beziehen. Sie sind nicht datenschutzrelevant.

# Einführung: Ausgewählte Datenschutzbegriffe

- **Verschlüsselung**
  - Pseudonymisierung und Anonymisierung vs. Verschlüsselung
    - Pseudonymisierte und anonymisierte Daten sind verwendbar und haben einen Wert; verschlüsselte Daten sind Datenmüll
  - Weitere Themen/Fragen:
    - Zwecke der Verschlüsselung (Transport, Speicherung)
    - Auf wen kommt es an (absoluter, relativer Ansatz, ErwG 26 DS-GVO)?
    - Qualität der Verschlüsselung
    - Schlüsselmanagement





# Inhalte

- Einführung: Ausgewählte Datenschutzbegriffe
- Auswirkungen des 2. DSAnpUG-EU (Datenschutzanpassungsgesetz)
- Hinweise der DSK zu Bußgeldern
- Leitlinie des EDSA zu Cookies
- Erklärungen der Datenschutzbehörden und Urteile

# 2. DSAnpUG-EU

- 2. Datenschutz-Anpassung- u. Umsetzungsgesetz, Entwurf 563 Seiten

| | |
|---|---|
| - Staatsangehörigkeitsgesetz | - Arzneimittelgesetz |
| - Bundesbeamtengesetz | - Straßenverkehrsgesetz |
| - De-Mail-Gesetz | - Anti-Doping-Gesetz |
| - Antiterrordateigesetz | - Hilfetelefongesetz |
| - E-Government-Gesetz | - Kulturgutschutzgesetz |
| - Waffengesetz | - Umsatzsteuergesetz |
| - **Bundesdatenschutzgesetz** | - Schornsteinfeger-Handwerksgesetz |
| - Informationsfreiheitsgesetz | - Tierschutzgesetz |
| - Personenstandsgesetz | - Fleischgesetz .... **+ 130 Gesetze** |





# 2. DSAnpUG-EU

- Übersicht der Änderungen, nicht vollständig (ein Auszug)
- Meist redaktionelle Änderungen:
  - „erheben, speichern und nutzen" durch verarbeiten
  - „erheben, verarbeiten und nutzen" durch verarbeiten
  - „sperren" durch „einschränken der Verarbeitung"
  - „Weitergabe" durch „Übermittlung"
  - „verwenden" durch „verarbeiten"

## 2. DSAnpUG-EU

- **BDSG (Bundesdatenschutzgesetz)**
- § 26 – Im Beschäftigungsverhältnis hat die Einwilligung grundsätzlich schriftlich oder elektronisch zu erfolgen
- § 38 – Erhöhung der Personengrenze für Datenschutzbeauftragten von 10 auf mindestens 20 Personen
- § 86 – Verarbeitung personenbezogener Daten für Zwecke staatlicher Auszeichnungen und Ehrungen



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

## 2. DSAnpUG-EU

- **BDBOS-Gesetz** (Behörden-/Polizeidigitalfunk)
- Definition der Verbindungsdaten, z.B. Gerätekennung, Einbuchung, Ausbuchung, Beginn und Ende von Verbindungen, Dienstedaten etc.
- Grundsätzliche Geltung des BDSG
- Rechtsgrundlage für Datenverarbeitung durch Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS)
  - u.a. für technische Zwecke und auch Übermittlung für Strafverfolgung und Gefahrenabwehr

## 2. DSAnpUG-EU

- **Beamtenstatusgesetz** und **Bundesbeamtengesetz** sowie **Soldatengesetz** und **Zivildienstgesetz**
- Personalakten dürfen nur mit Einwilligung der Betroffenen für andere Zwecke als Personalverwaltung verwendet werden.
- Auskunft: Beamte haben Anspruch auf Einsicht in die Personalakte, auch nach Beendigung des Beamtenverhältnisses.
- Erfüllung: Dem Beamten ist ein Ausdruck zu überlassen, wenn Daten automatisiert verarbeitet wurden
- Ausnahmen: Personenbezogene Daten Dritter und Sicherheitsakten



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

## 2. DSAnpUG-EU

- **BSI-Gesetz**
- Verarbeitungsgrundlage für Datenverarbeitung im Aufgabenbereich
- Trotz Art. 6 Abs. 4 DS-GVO auch zu anderen Zwecken als ursprünglich erhoben, wenn IT-Sicherheitsrisiken es gebieten und Interessen der Betroffenen nicht überwiegen
- Einschließlich sensibler Daten nach Art. 9 DS-GVO, wenn ansonsten Aufgabenerfüllung nicht möglich oder gefährdet wäre und Interessen der Betroffenen nicht überwiegen
- Ausnahmen, z.B. Information und Auskunft (Art. 13, 15 DS-GVO)

# 2. DSAnpUG-EU

- **DE-Mail-Gesetz**
- Löschpflicht der Identitätsdaten und/oder für das DE-Mail-Konto, wenn Nutzer oder die Behörde es verlangt, oder wenn Dienstleister die Tätigkeit einstellt
- Datenverarbeitung nur soweit für den DE-Mail-Dienst erforderlich
- Es gelten im Übrigen die DS-GVO das TMG, das TKG, das BDSG (**!?**)
- Datenschutz-Zertifizierung durch BSI, Bundesdatenschutzbeauftragten oder andere sachverständige Stelle für den Datenschutz





# 2. DSAnpUG-EU

- **E-Government-Gesetz**
- Direkte behördliche elektronische Einholung von Nachweisen nur mit Einwilligung
- Behörden dürfen gemeinsam Daten verarbeiten:
  - Vertrag nach Art. 26 DS-GVO erforderlich
  - Etwaige Auftragsverarbeitung nach Art. 28 DS-GVO ist zu regeln
  - Bei Kollision von Bundes- und/oder Landesrecht ist das für den Vertrag geltende Recht zu bestimmen (**!?**)

## 2. DSAnpUG-EU

- **Bundesmeldegesetz (BMG)**
- Datenverarbeitung nicht Meldepflichtiger nur mit deren Einwilligung
- Identitätsprüfung vor der Auskunft an den Betroffenen
- Auskunft elektronisch möglich, dabei TOMs einhalten
- Ausnahmen von der Auskunft, z.B. bei automatisierten Melderegisterauskünften und Übermittlungen an bestimmte Stellen für Zwecke der Strafverfolgung, einschließlich Zoll, Finanzamt etc.
- Weitere Ausnahmen der Auskunft und anderer Betroffenenrechte





## 2. DSAnpUG-EU

- **Arzneimittelgesetz (AMG), Viertes Gesetz zur Änderung arzneimittelrechtlicher Vorschriften und Transfusionsgesetz**
- Durch Rechtsverordnung des Bundeswirtschaftsministeriums werden Regelungen für Datenübermittlung von Bundes- und Landesbehörden an das DIMDI (Deutsches Institut für Medizinische Dokumentation und Information) bestimmt
- Neben schriftlicher Einwilligung nun auch elektronische Einwilligung möglich

# 2. DSAnpUG-EU

- **Weingesetz (WeinG)**
- Verarbeitungsgrundlage z.B.
  - für Übermittlung von Erklärungen, Flächenerhebungen, Erntemeldungen, Weinerzeugnismeldungen an Behörden
  - für Übermittlung an Zuständigen für Pflanzenschutz oder Qualitätssicherung

    => Diese Person darf die Daten ausschließlich zu dem Zweck verarbeiten, zudem sie die Daten erhielt (Beschränkung des Art. 6 Abs. 4 DS-GVO)





# 2. DSAnpUG-EU

- **Krankenhausfinanzierungsgesetz (KHG)**
- Bei Privatversicherten und Beihilfeberechtigten sind direkte Abrechnungen zwischen Krankenhaus und Kostenträger nur mit Einwilligung des Versicherten zulässig

## 2. DSAnpUG-EU

- **Infektionsschutzgesetz (IfSG)**
- Beim der Zusammenarbeit zwischen dem Robert Koch-Institut und bestimmten Stellen ist sicherzustellen, dass Daten nicht erhoben werden, die eine Identifizierung von Personen ermöglichen





## 2. DSAnpUG-EU

- **Deutsche-Welle-Gesetz**
- Haftung nach Art. 82 DS-GVO nur für unzureichende Maßnahmen nach Art. 5 Abs. 1 lit. f) DS-GVO (Integrität und Vertraulichkeit)
- Ausnahmen für Auskunftsrecht, v.a. aus Gründen des Quellenschutzes und zur Sicherstellung des journalistischen Angebots
- „Datenschutzbeauftragter" als Aufsichtsbehörde; Qualifikation und Abberufung; Befugnisse nach Art. 57 und 58 DS-GVO
- Daneben auch Datenschutzbeauftragter

## 2. DSAnpUG-EU

- **Gesetz über das Ausländerzentralregister (AZR-Gesetz)**
- Bundesverwaltungsamt verarbeitet die Daten im Auftrag und nach Weisung des Bundesamtes für Migration
- Übermittlungsermächtigung auch an Drittstaaten, jedoch unter Einhaltung von Übermittlungsvorschriften der DS-GVO (Kap. V)





## 2. DSAnpUG-EU

- **Asylgesetz (AsylG) und Aufenthaltsgesetz (AufenthG)**
- Verarbeitung besonderer Kategorien personenbezogener Daten zur Aufgabenerfüllung zulässig

## 2. DSAnpUG-EU

- **Börsengesetz (BörsenG)**
- Verarbeitungsgrundlage für Daten, soweit dies zur Aufgabenerfüllung der Börsenaufsichtsbehörde, des Börsenrates, der Geschäftsführung, der Handelsüberwachungsstelle und des Sanktionsausschusses
- Ausschluss der Betroffenenrechte (einschl. Art. 14 DS-GVO, wenn Unternehmen Daten an Aufsicht übermitteln) bei Gefährdung, z.B. von Finanzmärkten, Zwecken der Maßnahme, wichtige wirtschaftliche oder finanzielle Interessen von BRD oder EU oder EWR bzw. deren Mitlieder, Strafverfolgung oder Gefahrenabwehr





## 2. DSAnpUG-EU

- **Steuerberatungsgesetz (StBerG)**
- Verarbeitungsgrundlage für Zwecke der Aufgabenerfüllung
- ABER: Zu abstrakt und nicht als ausrechend empfunden, daher nur kurz später erneut angepasst und ausführlich geregelt:
  - Datenverarbeitung schließt besondere Kategorien personenbezogener Daten ein
  - Steuerberater arbeiten weisungsfrei und sind daher selbst Verantwortliche nach Art. 4 Nr. 7 DS-GVO
  - Folge: AV-Vertrag nach Art. 4 Nr. 11, 28 DS-GVO ist nicht erforderlich

# 2. DSAnpUG-EU

- **Einkommensteuergesetz (EStG)**
- Übermittlungsermächtigung an Finanzbehörden für diverse Daten, wie Daten über die Abgaben an Träger der Krankenversicherung (Vorsorgeaufwendungen)
- Speicherermächtigung für das Bundeszentralamt für Steuern
- Arbeitgeber darf Lohnsteuerabzugsmerkmale ausschließlich für Berechnung der Lohnsteuer und Kirchensteuer verarbeiten, außer es liegt Einwilligung vor oder eine gesetzliche Ermächtigung





# 2. DSAnpUG-EU

- **Medizinproduktegesetz**
- Einwilligung nicht nur schriftlich, sondern auch elektronisch
- Personenbezogene Daten dürfen auch nach Widerruf der Einwilligung verarbeitet werden, wenn dies u.a. erforderlich für klinische Prüfungen ist

## 2. DSAnpUG-EU

- **Schornsteinfegergesetz**
- Übermittlung der Daten aus dem Kehrbuch an die zuständigen Stellen, soweit diese zur Erfüllung der behördlichen Aufgaben erforderlich oder gesetzlich vorgeschrieben ist





## 2. DSAnpUG-EU

- **Bundeselterngeld- und Elternzeitgesetz (BEEG)**
- Das Bundesfamilienministerium darf ein Internetportal für die elektronische Antragstellung einrichten
- Das Bundesfamilienministerium ist datenschutzrechtlich verantwortlich (Art. 4 Nr. 7 DS-GVO)
- Verarbeitung der personenbezogenen Daten nur mit Einwilligung zulässig

## 2. DSAnpUG-EU

- **Zehntes Buch Sozialgesetzbuch (SGB X)** – Sozialdatenschutz
- Einwilligung in Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten sowie ~~Betriebs- und~~ Geschäftsgeheimnisse erfolgt grundsätzlich schriftlich oder elektronisch
- Ausnahme von § 80 Abs. 3 SGB X (Auftragsverarbeitung durch nicht-öffentliche Stellen):
  - Grundsätzlich nur, wenn sonst **störanfällig** und deutlich **teurer**
  - Ausnahme neu, wenn ein „**Staatsbetrieb**" (Bund oder Land) die Auftragsverarbeitung übernimmt und Oberbehörde dies genehmigt





## 2. DSAnpUG-EU

- **Postgesetz (PostG)**
- Es gelten DS-GVO u. BDSG; Postdienste-DS-VO (PDV) ist aufgehoben
- Aber Spezialvorschriften in §§ 41a bis 42 PostG
  - Austausch von Anschriftenänderungen zwischen den Postdienstleistern
  - Mitteilung neuer Anschrift an den Absender nur mit Einwilligung
  - Verarbeitungsgrundlage für Daten von Empfängern
  - Identifizierung per Vorlage des Ausweises darf verlangt werden; Ausweisdaten dürfen gespeichert werden

# Inhalte

- Einführung: Ausgewählte Datenschutzbegriffe
- Auswirkungen des 2. DSAnpUG-EU (Datenschutzanpassungsgesetz)
- Hinweise der DSK zu Bußgeldern
- Leitlinie des EDSA zu Cookies
- Erklärungen der Datenschutzbehörden und Urteile





# Hinweise der DSK zu Bußgeldern

- **Ausgangslage:**
- Europäischer Datenschutzausschuss (EDSA/EDBP) bestätigte nach Art. 70 Abs. 1 lit. k) DS-GVO die Bußgeld-Leitlinien der Artikel-29-Datenschutzgruppe vom 03.10.2017 (WP 253)
- Allgemeine Ausführungen, vor allem keine Berechnungsvorgaben; Konkretisierung der Festsetzungsmethodik blieb also den späteren Leitlinien des EDSA vorbehalten
- Daher befasste sich die Deutsche Datenschutzkonferenz (DSK) mit diesem Thema

## Hinweise der DSK zu Bußgeldern

- **Rechtsgrundlage für Bußgelder**
- Nach Art. 83 DS-GVO sind Verstöße gegen die DS-GVO bußgeldbewehrt:
  - Bei formellen Verstößen nach Art. 83 Abs. 4 DS-GVO beträgt das Höchstbußgeld 2 % des weltweiten Jahresumsatzes oder 10 Mio. €
  - Bei materiellen Verstößen nach § 83 Abs. 5, 6 DS-GVO beträgt das Höchstbußgeld 4 % des weltweiten Jahresumsatzes oder 20 Mio. €
- Nach Art. 83 Abs. 2 DS-GVO ist bei der Höhe des Bußgeldes die Schwere des Verstoßes nach verschiedenen Kriterien zu bestimmen





## Hinweise der DSK zu Bußgeldern

- Datenschutzkonferenz (DSK) – auch Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
- Gesetzlich nicht geregelt. Daher auch die verschiedenen Instrumente ohne Bindungskraft, wie
  - Entschließungen
  - Orientierungshilfen
  - Protokolle
  - Hinweise
  - Beschlüsse
  - Anwendungshinweise
  - Pressemitteilungen

# Hinweise der DSK zu Bußgeldern

- **Bußgeldkonzept**
  - Link: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf
- **Anwendungsbereich des Bußgeldkonzepts**
  - Bußgeldzumessung in Verfahren gegen Unternehmen im Anwendungsbereich der DS-GVO
  - Ausgenommen: Geldbußen gegen Vereine oder natürliche Personen außerhalb ihrer wirtschaftlichen Tätigkeit





# Hinweise der DSK zu Bußgeldern

- **Fünf-Stufen-Verfahren**
  - das betroffene Unternehmen einer Größenklasse zuordnen,
  - danach wird der mittlere Jahresumsatz der jeweiligen Untergruppe der Größenklasse bestimmt,
  - dann wird ein wirtschaftlicher Grundwert (Tagessatz) ermittelt,
  - dieser Grundwert mittels eines von der Schwere der Tatumstände abhängigen Faktors multipliziert und
  - den ermittelten Wert anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände anpassen.

# Hinweise der DSK zu Bußgeldern

- **1. Stufe: Unternehmen einer Größenklasse zuordnen**
  - Funktionaler Unternehmensbegriff nach ErwG 150 DS-GVO: Begriff „Unternehmen" im Sinne der Art. 101 und 102 AEUV
  - Vier Größenklassen (A bis D) mit Untergruppen (insgesamt 20 Klassen):
    - Kleinstunternehmen: Jahresumsatz bis 2 Mio. Euro
    - Kleine Unternehmen: Jahresumsatz über 2 bis 10 Mio. Euro
    - Mittlere Unternehmen: Jahresumsatz über 10 bis 50 Mio. Euro
    - Große Unternehmen: Jahresumsatz über 50 Mio. Euro





# Hinweise der DSK zu Bußgeldern

- **2. Stufe: Bestimmung des mittleren Jahresumsatzes der jeweiligen Untergruppe der Größenklasse**
  - Pauschal an der jeweiligen Einordnung des Unternehmens in die zuvor genannten Untergruppen ausgerichtet.
  - Bei Großunternehmen in der vierten Gruppe mit einem jährlichen Umsatz von über 500 Mio. € findet der prozentuale Bußgeldrahmen von 2 % bzw. 4 % des jährlichen Umsatzes als Höchstgrenze Anwendung:

    => Hier wird der durchschnittliche Jahresumsatz also konkret berechnet.

# Hinweise der DSK zu Bußgeldern

- **3. Stufe: Ermittlung des wirtschaftlichen Grundwerts (Tagessatz)**
  - der mittlere Jahresumsatz der Untergruppe / 360 (Tage)
  - der durchschnittliche Tagessatz wird auf die Vorkommastelle aufgerundet.





# Hinweise der DSK zu Bußgeldern

| Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU) | | | | | | Großunternehmen | |
|---|---|---|---|---|---|---|---|
| A | | B | | C | | D | |
| A.I | 972 € | B.I | 9.722 € | C.I | 31.250 € | D.I | 173.611 € |
| A.II | 2.917 € | B.II | 17.361 € | C.II | 38.194 € | D.II | 243.056 € |
| A.III | 4.722 € | B.III | 24.306 € | C.III | 48.611 € | D.III | 416.667 € |
| | | | | C.IV | 62.500 € | D.IV | 694.444 € |
| | | | | C.V | 76.389 € | D.V | 972.222 € |
| | | | | C.VI | 97.222 € | D.VI | 1,25 Mio. € |
| | | | | C.VII | 125.000 € | D.VII | konkreter Tagessatz |

# Hinweise der DSK zu Bußgeldern

- **4. Stufe: Multiplikation des Tagessatzes mit einem von der Schwere der Tatumstände abhängigen Faktor**
  - Tatbezogene Umstände des Einzelfalls (Art. 83 Abs. 2 Satz 2 DS-GVO)
  - Schweregrads der Tat: leicht, mittel, schwer oder sehr schwer
  - Für formelle (Art. 83 Abs. 4 DS-GVO) und materielle (Art. 83 Abs. 5, 6 DS-GVO) Verstöße gelten unterschiedliche Faktoren:
    - für formell: 1 bis 6 und mehr für sehr schwere Verstöße
    - für materiell: 1 bis 12 und mehr für sehr schwere Verstöße





# Hinweise der DSK zu Bußgeldern

- **5. Stufe: Anpassung des ermittelten Wertes anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände**
  - Insbesondere sämtliche täterbezogenen Umstände (vgl. Kriterienkatalog des Art. 83 Abs. 2 DS-GVO) sowie
  - Sonstige Umstände, wie z.B. eine lange Verfahrensdauer oder eine drohende Zahlungsunfähigkeit des Unternehmens
  - Sicherstellung, dass das verhängte Bußgeld die in Art. 83 Abs. 4 bis Abs. 6 DS-GVO genannten Höchstbeträge von 2 oder 4 % des Umsatzes bzw. von 10 Mio. oder 20 Mio. Euro nicht überschreitet

## Hinweise der DSK zu Bußgeldern

- **Problemfeld: Verhältnismäßigkeit**
  - Nach Art. 83 DS-GVO müssen verhängte Bußgelder „wirksam und abschreckend", aber auch verhältnismäßig sein
  - Das Konzept orientiert sich in erster Linie am Umsatz. Tat- und Schuldaspekte wirken nur korrigierend
  - Große Unternehmen müssen auch bei Kleinstverstößen hohe Bußgelder zahlen, weil der für sie ermittelte wirtschaftliche Tagessatz so hoch ist.
- **Folge des Konzeptes:** Der Faktor beträgt min. 1,0. So liegt das Mindestbußgeld bei einem Tagessatz. Kein Verstoß ohne Bußgeld (**!?**)





## Inhalte

- Einführung: Ausgewählte Datenschutzbegriffe
- Auswirkungen des 2. DSAnpUG-EU (Datenschutzanpassungsgesetz)
- Hinweise der DSK zu Bußgeldern
- Leitlinie des EDSA zu Cookies
- Erklärungen der Datenschutzbehörden und Urteile

# Leitlinie des EDSA zu Cookies

- **Ausgangslage**
  - Europäischer Datenschutzausschuss (EDSA/EDPB) eingerichtet nach Art. 68 bis 74 DS-GVO
  - Aufgaben sind in Art. 70 DS-GVO ausführlich beschrieben (lit. a bis y)); Primäraufgabe: Einheitliche Anwendung der DS-GVO
  - Instrumente sind v.a. Leitlinien, Empfehlungen, bewährte Verfahren

    **=>** Rechtliche Verbindlichkeit nicht geregelt, allenfalls sind diese Instrumente zu „berücksichtigen" (ErwG 125 DS-GVO)

    => Beschlüsse: Verbindlich beim Kohärenzverfahren



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

# Leitlinie des EDSA zu Cookies

- **Leitlinie** (Link):
  - https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf
- **Inhalt der Leitlinie**
  - Wahl der Rechtsgrundlage für Datenverarbeitung (Verarbeitungsgrundlage)
  - Wirksamkeit der Einwilligung, die von der betroffenen Person bei der Interaktion mit sog. „Cookie-Walls" gegeben wird und
  - vermeintlichen Einwilligung durch Scrollen auf einer Website

# Leitlinie des EDSA zu Cookies

- **Wechsel gewählter Rechtsgrundlage unzulässig**
  - **Vor** der Datenverarbeitung ist die Rechtsgrundlage zu bestimmen
  - Hierüber ist der Betroffene zu informieren (u.a. Art. 13 DS-GVO)
  - Ein Wechsel kann zu Benachteiligung der Betroffenen führen, weil sich der Betroffene auf die Rechtsgrundlage „einrichten" kann
  - Beruft sich der Verantwortliche auf eine Einwilligung als Verarbeitungsgrundlage, ist ein Wechsel auf eine andere Verarbeitungsgrundalge nicht möglich (Leitlinie, Seite 25, Rdnr. 123)
  - Zitat: *... the controller cannot swap from consent to other lawful bases.*





# Leitlinie des EDSA zu Cookies

- **Cookie-Walls**
  - Cookie Walls führen dazu, dass Betroffene eine Website nicht nutzen können, bevor sie in das Setzen von Cookies einwilligen
  - EDSA: Zugang zu einer Website darf nicht von der Einwilligung in das Setzen von Cookies abhängig gemacht werden. Einer solchen Einwilligung fehle es an der Freiwilligkeit (Leitlinie, Seite 12, Rdnr. 39)
  - Zitat: *In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls)*

# Leitlinie des EDSA zu Cookies

- **Keine Einwilligung durch Scrollen oder "Wischen"**
  - Der Verantwortliche hat die (technischen) Abläufe so zu gestalten, dass der Vorgang für die Abgabe der Einwilligung für den Betroffenen klar als solcher erkennbar ist
  - Durch bloße weitere Nutzung der Website, z.B. durch Scrollen oder durch „Wischen" auf der Website kann eine wirksame Einwilligung (Art. 6 Abs. 1 lit. a) und Art. 7 DS-GVO) nicht erteilt werden
  - Argument: Einwilligungs-Widerruf muss genauso möglich sein, wie Einwilligungserteilung. Wie soll der Widerruf durch bloße Weiternutzung erfolgen? Überhaupt nicht (Leitlinie, Seite 19, Rdnr. 84)



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

# Leitlinie des EDSA zu Cookies

- **Weitere Themen**
  - Gültigkeitsdauer der Einwilligung (Leitlinie, Seite 23, Rdnr. 110)
    - In der DS-GVO nicht vorgeschrieben. Im Einzelfall zu bestimmen.
    - Kriterien: Umfang der Datenverarbeitung, Erwartungen Betroffener
  - „Überschwemmung" mit Einwilligungen (Leitlinie, Seite 19, Rdnr. 87, 88)
    - Hohe Zahl von Einwilligungen und leichte Abgabe durch Wischfunktion könne die Warnfunktion abschwächen
    - Es sind weitere technisch-juristische Wege zu entwickeln

# Inhalte

- Einführung: Ausgewählte Datenschutzbegriffe
- Auswirkungen des 2. DSAnpUG-EU (Datenschutzanpassungsgesetz)
- Hinweise der DSK zu Bußgeldern
- Leitlinie des EDSA zu Cookies
- Erklärungen der Datenschutzbehörden und Urteile





# Erklärungen der Datenschutzbehörden und Urteile

- **Themen beim LDI NRW**
  - „Datenschutzbeauftragte für **Arztpraxen** und sonstige Angehörige eines Gesundheitsberufs - ergänzende Informationen"
    - Sind weniger als 20 Personen mit der Datenverarbeitung beschäftigt, muss im Regelfall **kein Datenschutzbeauftragter** benannt werden; das gilt auch für Gemeinschaftspraxen, vgl. auch DSK-Beschluss vom 26.04.2018
  - Presseinformation vom 12.05.2020
    - 12.500 Eingaben, davon 2.200 Datenpannen im Jahre 2019

# Erklärungen der Datenschutzbehörden und Urteile

- **Themen beim ULD SH**
  - Corona-VO: Datenschutz bei der Erhebung von Kontaktdaten
    - Umfang (Art der Daten) sind in der Landesverordnung geregelt
    - Formulare müssen Datenschutzhinweise enthalten
    - Daten sind zu schützen, Einzelformulare sind zu bevorzugen
  - Plötzlich Videokonferenz - und der Datenschutz?
    - Datenschutzfreundliche Einstellungen bei Online-Diensten
    - Veranstalter und Teilnehmer können Daten schützen





# Erklärungen der Datenschutzbehörden und Urteile

- **Themen beim LfD Nds.**
  - Corona-Verordnung, Hinweise für Betriebe und Einrichtungen
    - Es sollte taggenau archiviert werden, um Löschfristen umzusetzen
    - Auf datenschutzkonforme Vernichtung achten, also Schreddern
  - Corona-Datenverarbeitung in Sportvereinen
    - Angaben zu Fiber und anderen Symptomen ausschließlich aufgrund einer Einwilligung

# Erklärungen der Datenschutzbehörden und Urteile

- **Themen beim BayLfD und BayLDA**
  - Cyberattacken auf medizinische Einrichtungen vorbeugen
    - Checkliste vorbereitet mit Themen, wie Patch-Management, Malware-Schutz, Ransomware-Schutz, Passwortschutz, Zwei-Faktor-Authentifizierung, E-Mail-Sicherheit, Backups, Externe Dienstleister, Fernwartung und HomeOffice etc.



DSB-Fortbildung, Art. 37 (5) DS-GVO, 16. Juni 2020

# Erklärungen der Datenschutzbehörden und Urteile

- **OLG Naumburg,** Urteile vom 07.11.2019, Az. 9 U 6/19, 9 U 39/18
  - Sachverhalt: zwei Apotheker, von denen einer auch auf Amazon Medikamente verkauft. Der andere rügt, dies sei eine Datenschutzrechtsverletzung, weil die erforderlichen Einwilligungen der Betroffenen (Käufer) nicht vorlägen
  - Unterlassungsanspruch nach § 8 Abs. 1 S. 1 i.V.m. § 3a UWG wegen Verstoßes gegen Art. 9 Abs. 1 DS-GVO
  - OLG Naumburg: DS-GVO Regelungen hier Marktverhaltensregeln nach § 3a UWG (hier: Werbezwecke)

## Erklärungen der Datenschutzbehörden und Urteile

- **OLG Naumburg,** Urteile vom 07.11.2019, Az. 9 U 6/19, 9 U 39/18
  - Wettbewerbsrechtlich okay, Datenschutzrechtlich ... naja:
  - „*(Medikamenten-)Bestelldaten der Kunden sind Gesundheitsdaten nach Art. 9 Abs. 1 DS-GVO.*" => Halte ich für schwierig. Die Argumente, dass Bestellung mit Fake-Daten oder für Dritte, wie Familienangehörige erfolgen kann, lässt das OLG nicht gelten
  - „Datenverarbeitung durch Amazon ist keine Auftragsdatenverarbeitung" => soweit meines Erachtens richtig; es herrscht ohnehin ein AV-Wahn
  - Einwilligung wurde nicht vorgetragen und wann soll sie erfolgen?





## Danke

**Vielen Dank für die Aufmerksamkeit und Teilnahme!**

# Ihr Referent

**Roman Pusep**
Rechtsanwalt, Fachanwalt für IT-Recht
Zertifizierter externer Datenschutzbeauftragter (TÜV)

**WERNER Rechtsanwälte Informatiker**
Oppenheimstraße 16, 50668 Köln

Telefon 0 221 / 97 31 43 - 73
Telefax 0 221 / 97 31 43 - 99

roman.pusep@werner-ri.de
https://www.werner-ri.de