Änderungen durch EU-Datenschutz-Grundverordnung und neues BDSG ab 2018

Weiterbildung Hessen e.V. 08.02.2018

Dr. Thomas Lapp, Frankfurt

Rechtsanwalt und Mediator

Gegenstand und Ziele – EU DSGV

- Diese Verordnung enthält Vorschriften zum **Schutz natürlicher Personen** bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
- Art. 1 Abs. 1 EU DSGV

Leute_by_S. Hofschlaeger_pixelio.de

Erwägungsgründe

- Die Verarbeitung personenbezogener Daten sollte im Dienste der **Menschheit** stehen. (Nr. 4)
- Die Vorschriften zum **Schutz der Grundrechte und Grundfreiheiten** von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden. (Nr. 10)

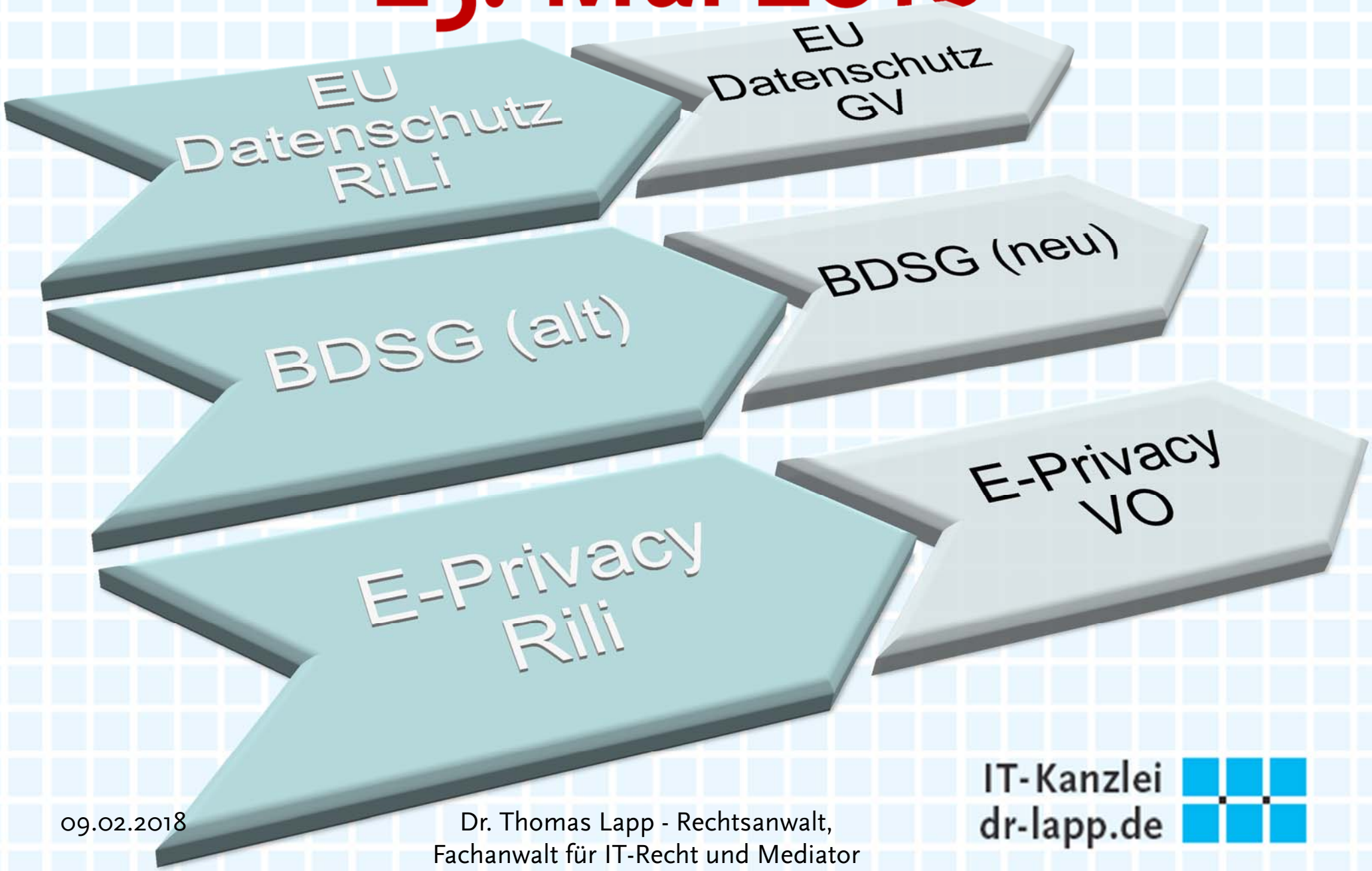
Wichtige Schritte zum Datenschutz

09.02.2018

Dr. Thomas Lapp - Rechtsanwalt,
Fachanwalt für IT-Recht und Mediator

IT-Kanzlei
dr-lapp.de

25. Mai 2018



09.02.2018

Dr. Thomas Lapp - Rechtsanwalt,
Fachanwalt für IT-Recht und Mediator

IT-Kanzlei
dr-lapp.de

Begriffsklärung

Die im Mai 2016 veröffentlichte Datenschutz-Grundverordnung (DSGVO) der Europäischen Union hebt die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (Data Protection Directive 95/46/EG) der Europäischen Gemeinschaft auf. Sie wird ersetzt durch die neue Richtlinie (EU) 2016/680 vom 27. April 2016.

GDPR = DSGVO

Englische Bezeichnung

> GDPR = General Data Protection Regulation

Deutsche Bezeichnung:

> DSGVO = Datenschutz-Grundverordnung

Besonderheit

Im Gegensatz zu einer Direktive (Directive), die in den EU-Ländern durch nationale Gesetze umgesetzt werden muss, handelt es sich um eine Verordnung. Diese gilt unmittelbar ab 25.5.2018 in der ganzen EU („Vollharmonisierung“), sie muss nicht im nationalen Recht umgesetzt werden wie Direktiven oder Richtlinien, sie gilt!

Lediglich „Gestaltung“ durch nationale Gesetze ist möglich.

Ersetzt nationales Recht, falls es GDPR widerspricht.

Gültigkeit – Betroffene – Ziele

Die DSGVO ist aufgeteilt in die Artikel und die Beschreibung der Erwägungsgründe, die als Erklärungen dienen sollen. Sie ist von der Gültigkeit her sehr weit gefasst.

Gültigkeit

Betroffene

Ziele

- EU-weite Vereinheitlichung des Datenschutzniveaus
- Betroffen ist jede Person, Behörde und Einrichtung, die über die Zwecke und Mitten der Verarbeitung personenbezogener Daten entscheidet
- Gleichwertiges Schutzniveau für Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten
- Verschärfung der Anforderungen für die Verarbeitung personenbezogener Daten
- Bessere Kontrolle der Betroffenen über ihre Daten
- Auch ausländische Unternehmen, die sich an EU-Bürger wenden (Marktforschung) müssen sich daran halten (Marktortprinzip)
- Es gibt „Öffnungsklauseln“ für nationale Gesetzgeber
- Zum Teil gibt es aber konkrete Regelungsaufträge
- Aufsichtsbehörde des Unternehmens ist im Land des Hauptsitzes des Unternehmens für alle Niederlassungen

Grundsätze, Art. 5 Abs. 1 DSGV

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit, Integrität und Vertraulichkeit

Paragraphenmännlein_by_Stephanie Hofschlaeger_pixelio

➢ Nicht völlig neu,
aber so anders, dass gehandelt werden muss

Handlungsbedarf im Unternehmen

- Projektteam zusammenstellen
- Budget- und Zeitplanung
- Gap-Analyse Datenschutz

Andreas Hermsdorf_pixelio

Bestandsaufnahme

- Wie ist bislang die Umsetzung der datenschutzrechtlichen Vorschriften erfolgt?
- Gibt es bereits einen Datenschutzbeauftragten?
- Gibt es ausreichende, regelmäßige Schulung der Mitarbeiter?
- Welche Verträge sind mit Dritten geschlossen?
- Welche technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind getroffen?

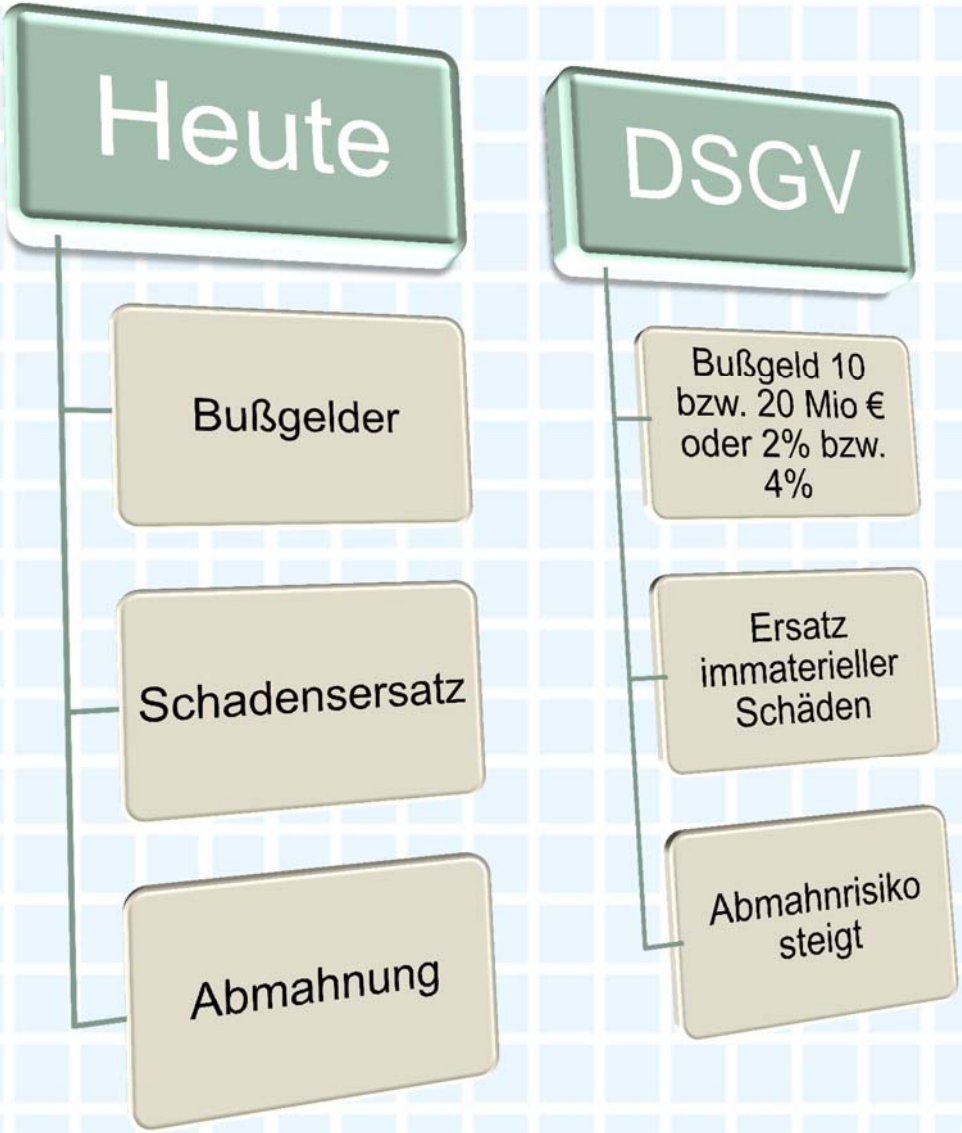
Erfüllungsauftrag

Folgende Maßnahmen sind in Vorbereitung auf die die DSGVO bzw. BDSG einzuleiten:

To Dos

- Keine Übergangsfrist
- Zahlreiche zusätzliche Pflichten des Datenschutzes
- Bestellung Datenschutzbeauftragten mit erweiterten Kompetenzen
- Vorbereitung, dass Anfragen Betroffener beantwortet werden können (Auskunftspflicht)
- Update Dokumentation: Einwilligung: z.B. Widerspruchsmöglichkeit beim Adressbroking
- Datenschutzfolgeabschätzung: Unternehmen müssen ihrerseits Risikoabschätzung des Datenschutzes vornehmen
- Interne Audits sind zu planen
- Information der Aufsichtsbehörde bei Risiken (im Vorfeld)
- Incident-Management: Es besteht eine 72 Stunden Meldepflicht bei Problemen
- Notfallkonzept, Backupkonzept müssen aufgestellt werden

Relevanz für Unternehmen



§ 43 BDSG (aktuell)

- Bußgeld bis 50.000 € bzw. 300.000 €
- Ausgleich auch des wirtschaftl. Vorteils

- **1,3 Mio €**
- **0,6 Mio €**

Erwägungsgründe (Auszug)

- <*Bei Verstößen*> ... sollte jedoch gebührend Rechnung getragen werden: der **Art, Schwere und Dauer** des Verstoßes, dem **vorsätzlichen Charakter** des Verstoßes, den Maßnahmen zur Minderung des entstandenen Schadens, dem Grad der Verantwortlichkeit oder **jeglichem früheren Verstoß**, der Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, ... und jedem anderen erschwerenden oder mildernden Umstand. (Nr. 148)

Art. 83 Geldbußen

- Aufsichtsbehörden stellen sicher, dass sie Geldbußen in jedem Einzelfall
  - wirksam,
  - verhältnismäßig und
  - abschreckend sind

Art. 83 Abs. 2 – Kriterien

- Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen des Ausmaßes des erlittenen Schadens

Art. 83 Abs. 2 – Kriterien

- Etwaige einschlägige frühere Verstöße
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
- Maßnahmen zur Schadensminderung
- Grad der Verantwortung unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen

Art. 83 Abs. 2 – Kriterien

- Umfang der Zusammenarbeit mit der Aufsichtsbehörde
- Kategorien der Betroffenen personenbezogenen Daten
- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde
- Einhaltung der angeordneten Maßnahmen
- Einhaltung von genehmigten Verhaltensregeln
- Jegliche anderen erschwerenden oder mildernden Umstände

Erwägungsgründe (Auszug)

- Eine Verletzung des Schutzes personenbezogener Daten kann … einen physischen, materiellen oder **immateriellen Schaden für natürliche Personen** nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten … (Nr. 85)

Haftung, Schadensersatz

- Anspruch auf Schadensersatz nach Art. 82 Abs. 1
  - materielle und immaterielle Schäden
- Jeder an der Verarbeitung beteiligte Verantwortliche haftet
- Auftragsverarbeiter haften unmittelbar, wenn sie
  - speziell in auferlegte Pflichten verletzen
  - rechtmäßige Anweisungen für die Verarbeitung missachten

Achtung: Abmahnung

- Verstöße gegen Datenschutzrecht können Abmahnungen von Wettbewerbern oder Schutzvereinigung führen

Lupo_pixelio

Personenbezogene Daten

- “personenbezogene Daten” sind als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (“betroffene Person”) beziehen

Thorben Wengert_pixelio.de

identifizierbar

- als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem **Namen**, zu einer **Kennnummer**, zu Standortdaten, zu einer **Online-Kennung** oder zu einem oder mehreren besonderen **Merkmalen** identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Nr. 1).

Art. 24 Verantwortung

- geeignete technische und organisatorische Maßnahmen
- in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten
- um sicherzustellen und
- den Nachweis dafür erbringen zu können,
- dass die Verarbeitung gemäß dieser Verordnung erfolgt

Verbotsprinzip, Einwilligung

09.02.2018

Dr. Thomas Lapp - Rechtsanwalt,
Fachanwalt für IT-Recht und Mediator

IT-Kanzlei
dr-lapp.de

Verbotsprinzip

- Verarbeitung personenbezogener Daten ist grundsätzlich verboten und nur zulässig, wenn
  - **die Verarbeitung gemäß Art. 6 DSGVO rechtmäßig ist**

Rechtmäßigkeit – Art. 6 DSGVO

- Einwilligung des Betroffenen
- Verarbeitung ist erforderlich …

Thorben Wengert_pixelio

Art. 6 DSGVO:
Verarbeitung ist erforderlich ...

- für die Erfüllung eines Vertrages
- Erfüllung einer rechtlichen Verpflichtung
- zur Wahrung einer Aufgabe im öffentlichen Interesse
- zur Wahrung der berechtigten Interessen, soweit nicht entgegenstehende Interessen, Grundrechte oder Grundfreiheiten der betroffenen Person überwiegen

Erwägungsgründe (Auszug)

- Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden... (Nr. 39)

Erwägungsgründe (Auszug)

- Die **Einwilligung** sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist ... (Nr. 32)

Einwilligung– Art. 4 Nr. 11 DSGVO

- Willenserklärung der betroffenen Person
- Auch als bestätigende Handlung möglich
- Einverständnis mit der Datenverarbeitung
- Freiwillig für den bestimmten Fall
- In informierter Weise und unmissverständlich

Bedingungen – Art. 7 DSGVO

- Nachweisbarkeit der Einwilligung
- Ersuchen um Einwilligung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen
- Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden

Freiwilligkeit

- Kein generelles Kopplungsverbot nach Art. 7 Abs. 4
- Erwägungsgrund 42 S. 5:
  - Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden

Betroffenenrechte

09.02.2018

Dr. Thomas Lapp - Rechtsanwalt,
Fachanwalt für IT-Recht und Mediator

IT-Kanzlei
dr-lapp.de

Transparenzgebot

- Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden.

  Erwägungsgrund 58

Transparenzgebot, Art. 12 I 1 EU DSGV

- Informationen sind in präziser, transparenter, verständlicher
- und leicht zugänglicher Form
- in einer klaren und einfachen Sprache zu übermitteln;
- dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.

➢ Entspricht die Datenschutzerklärung diesen Anforderungen?

Fristen: Art. 12 I 3/4 EU DSGV

- Innerhalb eines Monats sind der betroffenen Person auf Antrag die verlangten Informationen zugänglich zu machen oder
- die Frist um maximal zwei Monate zu verlängern oder
- unter Angabe von Gründen abzulehnen und auf Möglichkeit der Beschwerde bei der Aufsichtsbehörde oder gerichtliche Rechtsbehelfe hinzuweisen

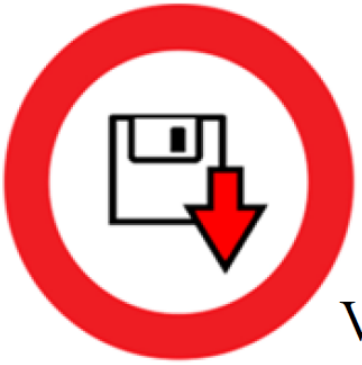
➢ Unternehmen müssen vorbereitet sein!

Standardisierte Bildsymbole Art. 12 Abs. 7 DSGV

- Die Informationen, die den betroffenen Personen gemäß den Artikeln 13 und 14 bereitzustellen sind, können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln.

➢ Kann Reizüberflutung durch Info zu Datenschutz vermeiden

Standardisierte Bildsymbole - Vorschläge

SYMBOL	WESENTLICHE INFORMATIONEN	ERFÜLLT
	Es werden nicht mehr personenbezogene Daten **erhoben**, als für die spezifischen Zwecke der Verarbeitung erforderlich sind.	
	Es werden nicht mehr personenbezogene Daten **gespeichert**, als für die spezifischen Zwecke der Verarbeitung erforderlich sind.	

Standardisierte Bildsymbole - Vorschläge

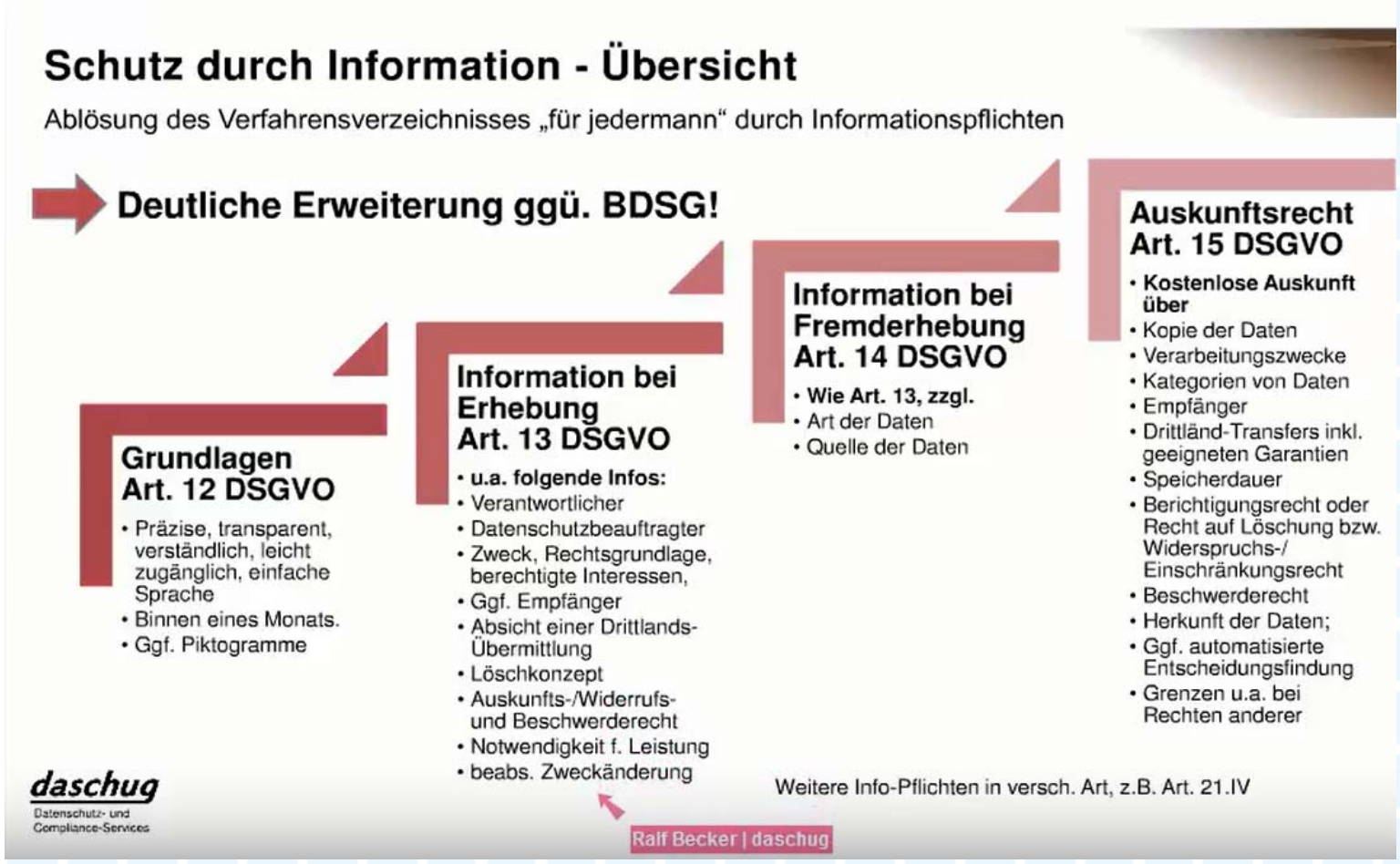
	Personenbezogene Daten werden nicht zu anderen als den Zwecken **verarbeitet**, für die sie erhoben wurden.	
	Es werden keine personenbezogenen Daten an gewerbliche Dritte **weitergegeben**.	

Standardisierte Bildsymbole - Vorschläge

	Es werden keine personenbezogenen Daten **verkauft oder verpachtet**.	
	Es werden keine personenbezogenen Daten **unverschlüsselt** aufbewahrt.	

Informationspflicht

Die Informationspflichten der Unternehmen sind in der DSGVO stark ausgeweitet:



Quelle Daschug Datenschutz, Darmstadt

Art. 16 Recht auf Berichtigung

- Berichtigung unrichtiger, das bedeutet unwahrer, personenbezogener Daten
- Vervollständigung unvollständiger personenbezogener Daten, mit denen der Verarbeitungszweck nicht erreicht wird, gegebenenfalls auch mittels einer ergänzenden Erklärung

Art. 16 Recht auf Berichtigung

- Berichtigung und Ergänzung müssen unverzüglich erfolgen, allerdings unter Berücksichtigung der konkreten Verarbeitung und das voraussichtlichen Berichtigungsaufwandes

Art. 17 Recht auf Löschung

- Recht auf Löschung – Recht auf Vergessenwerden
- Anspruch auf unverzügliche Löschung der personenbezogenen Daten
  - Daten sind für die Zwecke nicht mehr notwendig
  - Widerruf der Einwilligung, keine anderw. Rechtsgrundlage
  - Widerspruch gegen Verarbeitung nach Art. 21 Abs. 1 ohne vorrangige berechtigte Gründe zur Verarbeitung oder nach Art. 21 Abs. 2

Weitere Gründe nach Art. 17 Abs. 1

- Unrechtmäßige Verarbeitung personenbezogener Daten
- Rechtliche Verpflichtung des Verantwortlichen zur Löschung aufgrund EU-Recht oder nationalem Recht
- Personenbezogene Daten von Kindern, die nach Art. 8 Abs. 1 erhoben wurden und bei denen die Löschung beantragt wurde

Unverzügliche Löschung

- Rechtsfolge ist die unverzügliche Löschung
  - Maßstab unverzüglich: wie bei Berichtigung
- Verantwortliche hat hierfür entsprechende automatisierte Verfahren vorzusehen
- Technische Löschung bedeutet, dass auf die Daten nicht mehr mit den üblichen Verfahren zugegriffen werden kann und sie nicht mehr verarbeitet und nicht mehr ohne übermäßigen Aufwand wiederhergestellt werden können

Vergessenwerden – Abs. 2

- „Recht auf Vergessenwerden“
- Soweit personenbezogene Daten durch Verantwortliche öffentlich gemacht wurden und er zur Löschung verpflichtet ist
- unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten
- angemessene Maßnahmen, auch technischer Art,
- Information anderer für die Datenverarbeitung Verantwortliche

Verfahrensregeln

- Gem. Art. 70 Abs. 1 lit. d hat der Europäische Datenschutzausschuss die Aufgabe, Verfahrensregeln für die „Löschung“ von
  - Links zu personenbezogenen Daten,
  - Kopien oder
  - Replikationen dieser Daten aus öffentl. zugänglichen Kommunikationsdiensten bereitzustellen

Art. 18 Recht auf Einschränkung der Verarbeitung

- Während des Streits über die Richtigkeit für die Zeit, in der der Verantwortliche die Richtigkeit prüfen kann
- Bei unrechtmäßiger Verarbeitung und Ablehnung der Löschung durch die betroffene Person

Art. 18 Recht auf Einschränkung der Verarbeitung

- Wegfall des Verarbeitungzwecks, wenn betroffene Person die Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt
- Widerspruch gegen die Verarbeitung nach Art. 21 Abs. 1 eingelegt - bis Abschluss der Prüfung des Widerspruchs

Verarbeitungsrecht: Einschränkung

- Personenbezogene Daten dürfen nach Einschränkung nur noch gespeichert und in folgenden Fällen verarbeitet werden:
  - Einwilligung der betroffenen Person
  - Zur Geltendmachung und Ausübung von Rechtsansprüchen bzw. Verteidigung gegen Rechtsansprüche
  - Zum Schutz der Rechte einer anderen natürlichen oder juristischen Person
  - Wichtiges öffentliches Interesse der EU oder eines Mitglieds

Art. 19 Mitteilungspflicht

- Der Verantwortliche teilt allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Artikel 16, Artikel 17 Absatz 1 und Artikel 18 mit,
- Ausnahme:
  - dies erweist sich als unmöglich oder ist
  - mit einem unverhältnismäßigen Aufwand verbunden

Art. 20 Recht auf Datenübertragbarkeit

- Um im Fall der Verarbeitung personenbezogener Daten mit automatischen Mitteln eine bessere Kontrolle über die eigenen Daten zu haben, sollte die betroffene Person außerdem berechtigt sein, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen, maschinen-lesbaren und interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übermitteln.

Datenübertragbarkeit

- interoperable Formate fördern
- Ausdruck eines Wettbewerbs um datenschutzfreundliche(re) Technologien
- kartellrechtlich relevante „lock-in“-Effekte minimieren
- insbes. soziale Netzwerke im Fokus
- Grds. unentgeltlich

Be- und Einschränkungen

- Verarbeitung im öffentl. Interesse oder bei Ausübung öffentl. Gewalt
- offenkundig unbegründete oder exzessive Anträge
- mangelnder Identifizierbarkeit der betroffenen Person

➢ Sonst weiter Anwendungsbereich, auch für private Unternehmen, keine Einschränkungen im Wortlaut!

➢ Einzelheiten noch nicht abzuschätzen!

Beachten: Arbeitsverhältnisse

- Betriebsvereinbarungen zum Datenschutz, zur Nutzung von Internet, mobilen Endgeräten und bring your own device müssen auf Übereinstimmung mit Art. 88 DSGV geprüft werden
- Regelungen und Abläufe zur Compliance, Aufdeckung von Straftaten

Betriebliche Datenschutzbeauftragte

Bestellungspflicht, Aufgaben

09.02.2018

Dr. Thomas Lapp - Rechtsanwalt,
Fachanwalt für IT-Recht und Mediator

IT-Kanzlei
dr-lapp.de

Pflicht zur Bestellung – Art. 37 Abs. 2 DSGVO

- Durchführung von Verarbeitungsvorgängen, die umfangreiche, regelmäßige und systematische Überwachung erfordern
- Maßgebend Art, Umfang oder Zweck der Verarbeitung pbD
- Verarbeitung personenbezogener Daten muss Kerntätigkeit des Unternehmens, nicht bloße Nebentätigkeit sein = entscheidend für die Unternehmensstrategie und nicht bloße routinemäßige Verwaltungsaufgabe

Überwachungserfordernis - Beispiele

- Scoring-Maßnahmen durchführende Auskunfteien und Detekteien,
- Unternehmen mit persönlich individualisierten Marketingstrategien,
- Versicherungsunternehmen, die zur Risikobeurteilung eine Überwachung der Versicherungsnehmer vornehmen

Pflicht zur Bestellung – § 38 Abs. 1 BDSG-neu

- Verantwortliche Stellen oder Auftragsverarbeiter, die in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen
- Soweit eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich ist
- Datenverarbeitung zum Zweck der (anonymisierten) Übermittlung oder Markt- oder Meinungsforschung

Datenschutzbeauftragte (extern oder intern)

- Anforderungen nach Art. 37 Abs. 5 DSGVO
- Grundlage: berufliche Qualifikation und Fachwissen
  - Datenschutzrecht
  - Datenschutzpraxis
  - Fähigkeit, die Aufgaben nach Art. 39 DSGVO zu erfüllen

Erwägungsgrund 97

- Datenschutzbeauftragter muss über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügen.
- Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die vor von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten

Erwägungsgrund 97

- Sowohl interne als auch externe Datenschutzbeauftragte müssen ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können

Stellung des Datenschutzbeauftragten– Art. 38 DSGVO

- Ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden
- Unterstützung und Bereitstellung der erforderlichen Ressourcen
  - Räumlichkeiten, Infrastruktur, Finanzen (Fachliteratur, Fortbildung)
  - Freistellung von anderen Aufgaben, gegebenenfalls Personal

Wahrung der Unabhängigkeit

- Datenschutzbeauftragte sind im Rahmen der Aufgaben keinen Weisungen unterworfen
- dürfen nicht wegen ihrer Arbeit abberufen oder benachteiligt werden
- berichten unmittelbar der höchsten Managementebene

Konsultationsrecht

- Betroffene können sich mit allen Fragen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte an den Datenschutzbeauftragten wenden

Aufgaben des Datenschutzbeauftragten

- Beratung und Unterrichtung von Unternehmensleitung und Beschäftigten hinsichtlich der datenschutzrechtlichen Pflichten
- Überwachung der Einhaltung des Datenschutzrechts und der internen datenschutzrechtlichen Richtlinien
- Sensibilisierung und Schulung der Mitarbeiter
- Beratung und Überwachung bei Folgenabschätzung

Aufgaben – Aufsichtsbehörde

- Datenschutzbeauftragte müssen mit der Aufsichtsbehörde zusammenarbeiten und
- Der Aufsichtsbehörde als Anlaufstelle dienen

Auftrags(daten)verarbeitung

- Anforderungen sind verändert worden
- Alle Auftragsverhältnisse und alle Verträge sind zu prüfen, inwieweit die DSGV eingehalten wird

Abgrenzung Auftragsbearbeitung

- **Kooperation** zwischen zwei oder mehreren Verantwortlichen, die gemeinsam die Zwecke und Mittel der Verarbeitung festlegen regelt Art. 26
- **Funktionsübertragung** – Handeln im Interesse des Auftraggebers, aber mit weitgehender Selbständigkeit und eigener Entscheidungsbefugnis
  - Selbst verantwortliche Stelle
  - Weitergabe ist Übermittlung

Rechtsgrundlage

- Vertrag
- schriftlich oder elektronisch
  - Bindung des Auftragsverarbeiters an den Verantwortlichen
  - Wesentliche Inhalte der Verarbeitung

Wesentliche Inhalte der Verarbeitung Art. 28 Abs. 3

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
  - Erheben, Erfassen, Ordnen, Speichern, Auslesen etc.
  - Zweckbindung des Art. 5 Abs. 1 lit. b u. Art. 6 Abs. 4

Wesentliche Inhalte der Verarbeitung Art. 28 Abs. 3

- Art der personenbezogenen Daten, insb. Art. 9 und 10
- Kategorien betroffener Personen (Art. 30 Abs. 1c und Art. 33 Abs. 3a)
  - abstrakt zusammengefasste Gruppen, die gemeinsame Merkmale teilen, etwa „Beschäftigte“, „Verbraucher“ etc.
- Pflichten und Rechte der Verantwortlichen

Verzeichnis von Verarbeitungstätigkeiten

- Verfahrensverzeichnis nach 4 g Abs. 2 S. 1 i. V. m. 4e S. 1 BDSG (aktuell)
- Neu: Verzeichnis von Verarbeitungstätigkeiten nach Art. 30
- Ausnahme für kleine Unternehmen mit weniger als 250 Mitarbeiter und nur geringer Umfang und keine besonderen Datenkategorien

Neu: Verzeichnis von Verarbeitungstätigkeiten

- Verantwortlich Unternehmensleitung
- Auch Auftragverarbeiter verpflichtet
- Keine öffentlichen Verzeichnisse
- Bei Transfer in Drittstaat sind Risikoabschätzung und Schutzmaßnahmen zu dokumentieren – Art. 49 Abs. 6

Neu: Folgen- bzw. Risikoabschätzung

- Datenschutz-Folgenabschätzung nach Art. 25 DSGV ersetzt die Vorabkontrolle, ist aber deutlich umfangreicher
- Risiko-Abschätzung wird an mehreren Stellen der DSGV gefordert
  - Art. 24 DSGV – Verantwortung etc.
  - Erwägungsgrund 75 benennt diese Risiken

Abschied von der Verpflichtung auf das Datengeheimnis?

- § 5 BDSG (alt) fällt ersatzlos weg
- Art. 29 und Art. 32 Abs. 4 enthalten ähnliche Regelungen zu Pflichten der Mitarbeiter, aber ohne Verpflichtungserklärung
- Art. 5 Abs. 2 – Rechenschaftspflicht für Verantwortliche
- Art. 24 Abs. 1 verlangt vom Verantwortlichen, „den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“ (Dokumentationspflichten)

IT-Kanzlei dr-lapp.de

- Dr. Thomas Lapp
  Rechtsanwalt und Mediator

- Corinna Lapp
  Rechtsanwältin und Mediatorin,
  Fachanwältin für IT-Recht

Berkersheimer Bahnstraße 5
60435 Frankfurt
Tel.: 069/9540 8865
Fax: 069/9540 8864
anwalt@dr-lapp.de
www.dr-lapp.de