EU-Datenschutz-Grundverordnung

(EU-DSGVO)

Kompakt-Darstellung der Kernelemente

shutterstock.com/ KB-photodesign; Ket4up

Stichtag ist der 25.05.2018

Es gibt keine Übergangsfrist

- Die EU-DSGVO tritt am 25.05.2018 in Kraft.
- Alles muss also bis zum 24.05.2018 um 23.59 Uhr auf die neue Rechtslage eingestellt sein.

… und es wird teuer!

Je nach Verstoß können Bußgelder verhängt werden

- bis zu 10 Mio. EUR bzw.
- bis zu 20 Mio. EUR bzw.

- oder bis zu 4 % des gesamten, weltweit erzielten Jahresumsatzes

- je nachdem, welcher Betrag höher ist

EIN BISSCHEN THEORIE ….

Grundsätze für die Verarbeitung personenbezogener Daten, Art. 5 EU-DSGVO

- Rechtmäßigkeit/Treu und Glauben
- Transparenz
- Zweckbindung
- Datensparsamkeit
- Richtigkeit
- Begrenzte Speicherung
- Integrität und Vertraulichkeit

EU-Datenschutz-Grundverordnung (EU-DSGVO)

Die Datenverarbeitung personenbezogener Daten ist grundsätzlich VERBOTEN, wenn nicht eine dieser Voraussetzungen erfüllt ist!
Art. 6 EU-DSGVO

- Es liegt die **Einwilligung** der betroffenen Person vor
- Es liegt ein **berechtigtes Interesse** an der Datenverarbeitung vor und schutzwürdige Interessen des Betroffenen (insbesondere von Kindern) stehen dem nicht entgegen
- Die Datenverarbeitung ist erforderlich…
  - 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**

Die neue Einwilligung nach Art. 7, 8 EU-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
- Opt-In: Nicht vorab angeklickte Checkboxen mit Double-Opt-In

Das sind die neuen Informationspflichten für Unternehmen Art. 13, 14 EU-DSGVO – 1/2

- **Namen und Kontaktdaten** der verantwortlichen Stelle und ggf. des Vertreters
- ggf. Kontaktdaten des **Datenschutzbeauftragten**
- **Zweck und Rechtsgrundlage** der Datenverarbeitung; sollen z. B. „berechtigte Interessen“ die Rechtsgrundlage sein, ist dazulegen, worin sie bestehen
- ggf. die **Empfänger oder Kategorien von Empfängern** der personenbezogenen Daten
- ggf. Informationen zum **Datentransfer in Drittstaaten** einschließlich der Rechtsgrundlage
- Angaben zur **Speicherdauer** personenbezogener Daten bzw. Kriterien, nach denen sich die Speicherdauer bestimmt

Das sind die neuen Informationspflichten für Unternehmen Art. 13, 14 EU-DSGVO – 2/2

- Information über das Bestehen des **Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs-, Widerspruchs- oder ggf. Widerrufsrecht sowie das Recht auf Übertragbarkeit der Daten und das Recht auf Beschwerde bei einer Aufsichtsbehörde**

- Hinweis, ob der der Betroffene gesetzlich oder vertraglich zur Bereitstellung personenbezogener Daten verpflichtet ist

- ggf. Hinweis und Information zum Profiling oder eine andere Art von automatisierter Einzelfallentscheidung

- ggf. Herkunft der Daten: Werden die Daten nicht bei dem Betroffenen erhoben, sind die die Quellen anzugeben.

Das sind die sonstigen neuen Pflichten für Unternehmen Art. 24 ff. EU-DSGVO – 1/2

- **Dokumentationspflicht** (ggf. mit **Datenschutzfolgeabschätzung**)
- Umsetzung von technischen und organisatorischen Maßnahmen zum Datenschutz:
  - **„Datenschutz by Design“**: Sicherstellung des Datenschutzes durch technische Maßnahmen. Dazu sind interne Maßnahmen und Strategien im Unternehmen festzulegen und nachzuweisen
  - **„Datenschutz by Default“**: Einhaltung der Anforderung zu datenschutzfreundlichen Voreinstellungen

    Beispiele: Trennung der Daten nach Verarbeitungszweck, Verarbeitung nur der erforderlichen Daten, Zugriffsschutz, Anonymisierung oder Pseudonymisierung der Daten, verschlüsselte Kommunikation, Zertifizierungen

Das sind die sonstigen neuen Pflichten für Unternehmen Art. 24 ff. EU-DSGVO – 2/2

- **Meldepflichten** bei Datenpannen gegenüber der Aufsichtsbehörde (binnen 72 Stunden) und gegenüber den betroffenen Personen (unverzüglich)
- **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
- **Konsultation** der Aufsichtsbehörde oder des Datenschutzbeauftragten

Das sind die neuen Rechte der Betroffenen
Art. 15 ff. EU-DSGVO

- Auskunft
- Löschung
- Recht auf Vergessenwerden
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Recht auf Einschränkung der Verarbeitung

Die „Auftragsdatenverarbeitung“ nach dem jetzigen BDSG wird zur Auftragsverarbeitung

- **Früher:** „Auftragsdatenverarbeitung“ nach BDSG ist Datenverarbeitung im Auftrag und auf Weisung durch einen Auftragnehmer; der Auftraggeber bleibt dabei der allein Verantwortliche.

- **Neu:** Es ist nur noch ein **Auftragsverhältnis** bezüglich der Datenverarbeitung erforderlich und darauf, ob der Auftragsnehmer dabei weisungsgebunden arbeitet oder nicht, kommt es nicht mehr an.
  Auch Auftragnehmer haftet jetzt

  Beispiele:
  - Lohnbuchhaltung in der Cloud
  - Versendung von Newslettern und Mailings über einen Cloud-Anbieter
  - Nutzen eines Anrufdienstes für eingehende Anrufe
  - Managed Hosting von Webseiten/Onlineshops
  - …

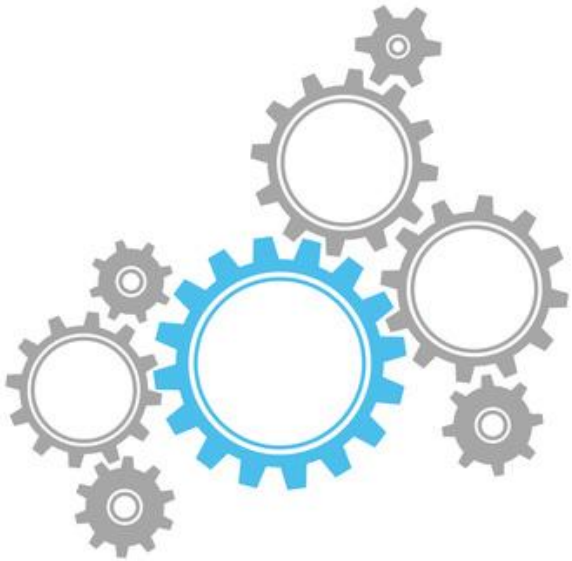
UND JETZT ZU DEN TO DO´S…

To Do 1- Auflistung aller Prozesse,

in denen personenbezogene Daten erhoben und verarbeitet werden

Beispiele:

- Mitgliederverwaltung (CRM)
- Newsletter-System
- Webseiten-Tracking (IP-Adresse!)
- Personal-Management-System
- …

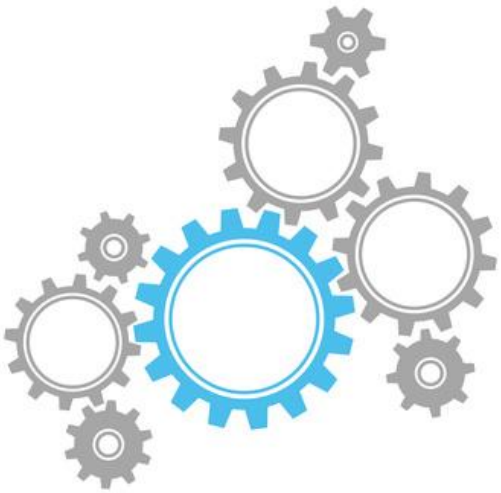


Jan Engel@Fotolia.com

To Do 1 - Auflistung aller Prozesse…

Es kommen umfangreiche Dokumentationspflichten auf Sie zu, die Sie bereits JETZT vorbereiten müssen!

- Bislang gab es im BDSG schon die (öffentlichen) Verfahrensverzeichnisse, zuständig war der Datenschutzbeauftragte
- Jetzt neu: **„Verzeichnis von Verarbeitungstätigkeiten“** (nicht mehr öffentlich)
- Neu: Zuständig ist der Verantwortliche, d.h. der **Vorstand**



Jan Engel@Fotolia.com

To Do 2 - Durchführung einer Datenschutz-Folgenabschätzung VOR der Aufnahme der Verarbeitung

… wenn die Datenverarbeitung voraussichtlich ein hohes Risiko für die Betroffenen hat …

- muss der Verantwortliche ein Abschätzung der Folgen vornehmen
- Beispiele:
  - Systematische Bewertung der Persönlichkeit einschl. Profiling als Grundlage für Entscheidungen mit Rechtswirkung
  - Verarbeitung von sensitiven Daten (Gesundheitsdaten usw).

To Do 3 - Anpassung sämtlicher Rechtstexte wie Einwilligungstexte, Datenschutzinformationen, ggf. Allgemeine Geschäftsbedingungen oder sonstige Informationstexte (online, offline) in Bezug auf die Informationspflichten

Verantwortlicher muss informieren über *(siehe oben)* **…**

- Zweck und Rechtsgrundlage der Datenverarbeitung
- ggf. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- Datentransfer in Drittstaaten einschließlich der Rechtsgrundlage
- Speicherdauer
- Bestehen des Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs-, Widerspruchs- oder ggf. Widerrufsrecht sowie das Recht auf Übertragbarkeit der Daten und das Recht auf Beschwerde bei einer Aufsichtsbehörde
- usw.

To Do 4 - Überprüfung aller Erlaubnistatbestände und Einwilligungsprozesse

Die Datenverarbeitung ist nur erlaubt, wenn …

- wenn die **Einwilligung** des Betroffen vorliegt
- oder ein **berechtigtes Interesse** an der Datenverarbeitung besteht und schutzwürdige Interessen des Betroffenen dem nicht entgegen stehen
- oder die Datenverarbeitung **erforderlich** ist
  - zur Erfüllung eines Vertrags
  - für vorvertragliche Maßnahmen auf eine Anfrage hin
  - zur Erfüllung einer rechtlichen Verpflichtung
  - …

To Do 4 - Überprüfung aller Erlaubnistatbestände und Einwilligungsprozesse

Das ist wichtig zur Einwilligung:

- **Nachweisbar** - also mit Protokollierung und Double Opt-In!
- Betroffener muss bei Einwilligung (also im Onlineformular) darüber informiert werden,
  - dass er ein **Widerrufsrecht** hat
  - zu welchem **Zweck** die Datenverarbeitung erfolgt
  - wer der **Verantwortliche** ist
- nicht vorab angeklickte **Checkbox**
  - Untätigkeit/Schweigen reicht nicht aus!

mipan@fotolia.com

To Do 5 - Überprüfung und Anpassung aller Auftragsverarbeitungsverträge

Auftragsdatenverarbeitung wird zur „Auftragsverarbeitung“

- Verträge sind mit **neuen Pflichten und TOM‘s** zu aktualisieren, u.a:

- Zusammenarbeit mit der Datenschutzaufsicht
- Unterstützung des Auftraggebers
  - bei TOM‘s zur Datensicherheit
  - bei der Meldung von Datenpannen
  - bei der Durchführung von Folgenabschätzungen
- –…

massimo_g-Fotolia

To Do 6 - Einrichtung der Prozesse auf die neuen Betroffenenrechte

Können die jetzigen Prozesse das?

- Auskunftsrecht dazu, ob und welche personenbezogene Daten verarbeitet werden
- Berichtigungsrecht
- Löschungsrecht
- Recht auf Vergessenwerden
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- …

Coloures-pic-Fotolia

To Do 6 - Einrichtung der Prozesse auf die neuen Betroffenenrechte

Können Sie eigentlich löschen?

- In welchen **Systemen** befinden sich die Datensätze zu einem Betroffenen? Gibt es mehrere? Können alle gleichzeitig gelöscht werden?
- Gibt es Daten, die **nicht gelöscht** werden dürfen? z.B. vertragliche Daten mit gesetzlichen Aufbewahrungsfristen?
- Sind alle Daten in allen Systemen **aktuell**, so dass Sie den Betroffenen überhaupt noch wiederfinden?

Coloures-pic-Fotolia

To Do 7 - Bestellung eines Datenschutzbeauftragten

Ist ein DSB nötig? *(…freiwillig kann dieser immer bestellt werden)*

- Der Vorstand muss einen Datenschutzbeauftragten bestellen, wenn **mindestens 10 Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. (§ 38 BDSG-neu)
  (Ein personalisierter E-Mail-Account reicht aus, um als Mitarbeiter mitgezählt zu werden!)

- Es ist in jedem Fall ein Datenschutzbeauftragter zu benennen, wenn…
  - nach Artikel 37 (1b) EU-DSGVO müssen jene Unternehmen und Organisationen einen DSB benennen, die im Rahmen ihrer unternehmerischen **Kerntätigkeit** eine **umfangreiche, regelmäßige und systematische Überwachung von Menschen** durchführen
  - oder die nach Artikel 37 (1c) EU-DSGVO im Rahmen ihrer **Kerntätigkeit besondere Kategorien von Daten gemäß Artikel 9** (genetischen Daten, biometrischen Daten, Gesundheitsdaten, etc.) verarbeiten

Coloures-pic-Fotolia

To Do 7 - Bestellung eines Datenschutzbeauftragten

Aufgaben des DSB gem. Art. 39 EU-DSGVO:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters
- Überwachung ob die EU-DSGVO sowie andere Vorschriften eingehalten werden
- Beratung in Bezug auf Datenschutz-Folgenabschätzungen
- Zusammenarbeit mit der Aufsichtsbehörde

Anforderungen an den DSB:

- Intern oder externe Beauftragung ist möglich
- Schriftform ist zwingend vorgeschrieben
- Interessenkonflikt mit der auszuübenden Funktion ist zu vermeiden
- Fachwissen ist nötig

VIELEN DANK FÜR DIE AUFMERKSAMKEIT!

datenschutz@brandenburg.dlrg.de
https://brandenburg.dlrg.de/datenschutz