artus UNTERNEHMENSBERATUNG GMBH & CO. KG

DS-GVO und ihre Auswirkungen

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

artus UNTERNEHMENSBERATUNG GMBH & CO. KG

Wichtige Änderungen

To-do

Zeitplan

Sanktionen

Bußgelder Bundesdatenschutzgesetz (BDSG)

- 50.000 bzw. 300.000 Euro

Bußgelder DS-GVO (Art. 83 DS-GVO)

- 2 % des weltweiten Jahresumsatzes bzw. bis zu 10 Millionen Euro, je nachdem, welcher Betrag höher ist

- 4 % des weltweiten Jahresumsatzes bzw. bis zu 20 Millionen Euro, je nachdem, welcher Betrag höher ist
  - z. B. bei unrechtmäßiger Datenverarbeitung, Verstoß gegen Transparenzpflichten („Datenschutzerklärung"), unrechtmäßige Datenweitergabe in ein Drittland, Verwendung einer unwirksamen Einwilligungserklärung

Änderungen

Compliance Pflichten

- Ernennung eines Datenschutzbeauftragten
- Führen eines Verzeichnisses der Verarbeitungstätigkeiten
- Durchführen einer Datenschutzfolgenabschätzung
- Unternehmen muss technische und organisatorische Maßnahmen treffen, die Einhaltung von Datenschutz sichererstellen und dies dokumentieren (= Datenschutz Compliance Management System)

Bußgelder für Verstoß gegen Compliance Pflichten

- Für jeden einzelnen Verstoß gegen die Compliance Pflichten kann ebenfalls ein Bußgeld von bis zu EUR 10. Mio oder 2% des weltweiten Jahresumsatzes verhängt werden…
  - …und das auch wenn die Datenverarbeitung an sich zulässig war und alle sonstigen Pflichten erfüllt waren

Änderungen

Einwilligungen

- Strenge Bedingungen für Einwilligungen gem. Art. 7 DS-GVO und Erwägungsgrund 32
  - Sie müssen den Zweck der Datenverarbeitung klar erkennen lassen.
  - Sie müssen nachweisbar sein.
  - Sie müssen für die betroffene Person verständlich sein.

Betroffenenrechte (Artt. 13 und 14 DS-GVO)

- Deutlich umfangreichere Informationspflichten gegenüber der betroffenen Person bei Erhebung der Daten, wie z. B.
  - die Rechtsgrundlage der Verarbeitung
  - die voraussichtliche Dauer der Speicherung
  - die Darlegung der Abwägungsgründe, sofern eine Abwägung von Interessen stattgefunden hat
- Unverzüglich, spätestens aber innerhalb eines Monats nach Eingang des Antrags

Änderungen

Integrität und Vertraulichkeit

Entgegen der Regelungen des BDSG genügt nicht mehr die allgemeine Beschreibung der technisch-organisatorischen Maßnahmen (TOM). Die DS-GVO fordert:

- durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Gemessen am:
  - Stand der Technik,
  - den Implementierungskosten,
  - der Art, dem Umfang, den Umständen und dem Zweck der Verarbeitung,
  - sowie der unterschiedlichen Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der Betroffenen.

Ein Verstoß ist bußgeldbewehrt! (10 Mio. € / 2% Vorjahresumsatz)

Änderungen

Rechenschaftspflichten

Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO)

- Auflistung aller Verfahren, in welchen personenbezogene Daten verarbeitet werden (ähnlich BDSG)
  - Datenkategorien,
  - Kategorien der betroffenen Personen,
  - mögliche Datenübermittlungen in Drittländer,
  - Löschfristen,
  - Abwägungsgründe (s. a. Datenschutzfolgeabschätzung), sowie
  - technisch organisatorische Schutzmaßnahmen

- Unabhängig davon, ob die Daten automatisiert verarbeitet werden. (BDSG: nur automatisiert und Beschäftigtendaten)

artus UNTERNEHMENSBERATUNG GMBH & CO. KG

Änderungen

Datenschutzfolgeabschätzung (Art. 35 DS-GVO)

- Wesentlich häufigere Beurteilung als beim BDSG (Vorabkontrolle)
- Risikobetrachtung der Verfahren mit Abwägung der Interessen
- Dokumentation der Ergebnisse
- Bei hohen Risiken ggf. vorherige Einbindung der Aufsichtsbehörde

Datenschutz by Design und by Default (ErwGrr 28-29 + 75-78 zu Art. 25 DS-GVO)

- Vor der Verarbeitung ist mittels strategischer Planung der Schutz der Betroffenenrechte zu berücksichtigen.
- Grundsätze des Datenschutzes durch Technik (data protection by design) und datenschutzfreundliche Voreinstellungen (data protection by default)
- Details können von den europäischen Institutionen noch vorgegeben werden.

artus UNTERNEHMENSBERATUNG GMBH & CO. KG

Änderungen

Data Protection Officer (DPO) (Art. 37 DS-GVO)

- Nicht für alle EU-Länder generell verpflichtend vorgeschrieben
- Öffnungsklausel für Mitgliedsstaaten - Öffnungsklausel Art. 37 Abs. 4 DS-GVO
  - Deutschland hat sich entschieden (BDSG-Neu) ab 10 MA in der Datenverarbeitung Pflicht
- „Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens […], das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt,"
- Aufgaben des Verantwortlichen gem. DS-GVO müssen auch ohne DPO wahrgenommen werden

Stellung des Data Protection Officer und Aufgaben (Artt. 38 + 39 DS-GVO)

- Abs. 3: „berichtet unmittelbar der höchsten Managementebene des Verantwortlichen"
- Abberufungs- und Benachteiligungsschutz (engl. Version: dismissed)
- Frühzeitige Einbindung (vom Verantwortlichen sicherzustellen)
- Überwachung […] sowie der Strategien des Verantwortlichen […] für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten

artus UNTERNEHMENSBERATUNG GMBH & CO. KG

Änderungen

Meldepflicht bei Datenpannen (Art. 4, Abs. 12 + Art. 33 DS-GVO)

- Im BDSG nur besondere Datenkategorien
- DS-GVO : Nahezu jeder Sicherheitsvorfall ist binnen 72 Stunden meldepflichtig!
  - Wenige Ausnahmen

Auftragsverarbeitung durch Dritte (Art. 28 DS-GVO)

- Privilegierung des Auftragnehmers bleibt bestehen
- Gesamtschuldnerische Haftung von Auftraggeber und –nehmer
- Auch der Auftragnehmer muss die Verfahren dokumentieren
- Neue Pflichtinhalte der Verträge
  - Angemessenheit der Schutzmaßnahmen
  - Einwilligung zur Einbindung von Subunternehmern verpflichtend

artus UNTERNEHMENSBERATUNG GMBH & CO. KG

Wichtige Änderungen

To-do

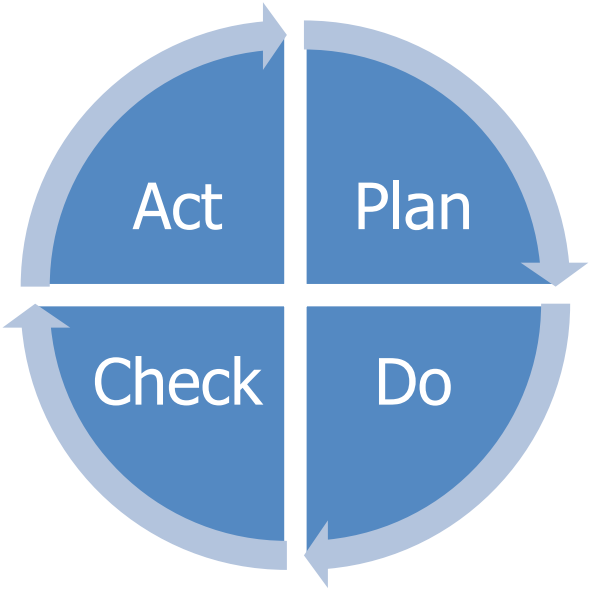
Zeitplan

Aufbau Datenschutzmanagementsystem

Die DS-GVO fordert eine kontinuierliche Überarbeitung und Kontrolle der Verfahren und Prozesse zum Schutz personenbezogener Daten (Datenschutz Compliance Management System).

- Einrichten eines Dokumentationssystems
- Festlegen von Prüfzyklen
- Festlegen von Prüfungsmaßnahmen
- Festlegen von Prüfungsverantwortlichen
- Klassischer P-D-C-A Zyklus wie bei anderen Systemen

- Datenschutzorganisation zur Sicherstellung der Anforderungen wie Meldepflicht und Auskunftsersuchen



artus UNTERNEHMENSBERATUNG GMBH & CO. KG

Überprüfung interner Prozesse

- Zuordnung der Verantwortlichkeiten

- Erstellung bzw. Überarbeitung des Verzeichnisses der Verarbeitungstätigkeiten (Analyse des Ist-Zustandes")
  - Alle Fachabteilungen müssen Daten liefern
  - Drittlandsübermittlung zu beachten
  - Auftragsverarbeitung zu beachten
- Auf Basis der Analyse des Ist-Zustandes
  - Prüfung der Rechtmäßigkeitsregelungen (später)
  - Datenschutz-Folgeabschätzung (später)
  - Bei Bedarf Klärung von Einzelfragen durch (externen oder internen/Rechtsrat) oder Konsultation der Aufsichtsbehörden

- Sicherstellung der Rechte der betroffenen Personen (z. B. Informationspflichten)

Weitere To-dos

Fachabteilungen

- Überprüfung interner und externer Prozesse
  - Vereinbarungen über die Auftragsverarbeitung
  - Datenübermittlungen zur Funktionserfüllung
  - Einwilligungen
  - Angemessene Schutzmaßnahmen

Geschäftsführung

- Freigabe des Budget
- Bestimmen der Projektleitung und weiteren Verantwortlichkeiten (ggf. der neuen Organisation)
- Managementinformation der Organisation
- Übernimmt Projekt-Sponsoring
- Projektfreigabe

artus UNTERNEHMENSBERATUNG GMBH & CO. KG

Wichtige Änderungen

To-do

Zeitplan

730 Tage Zeit …

… jedoch beginnend am 24.05.2016

	Stand: 23.03.2018
24.05.2016	25.05.2018

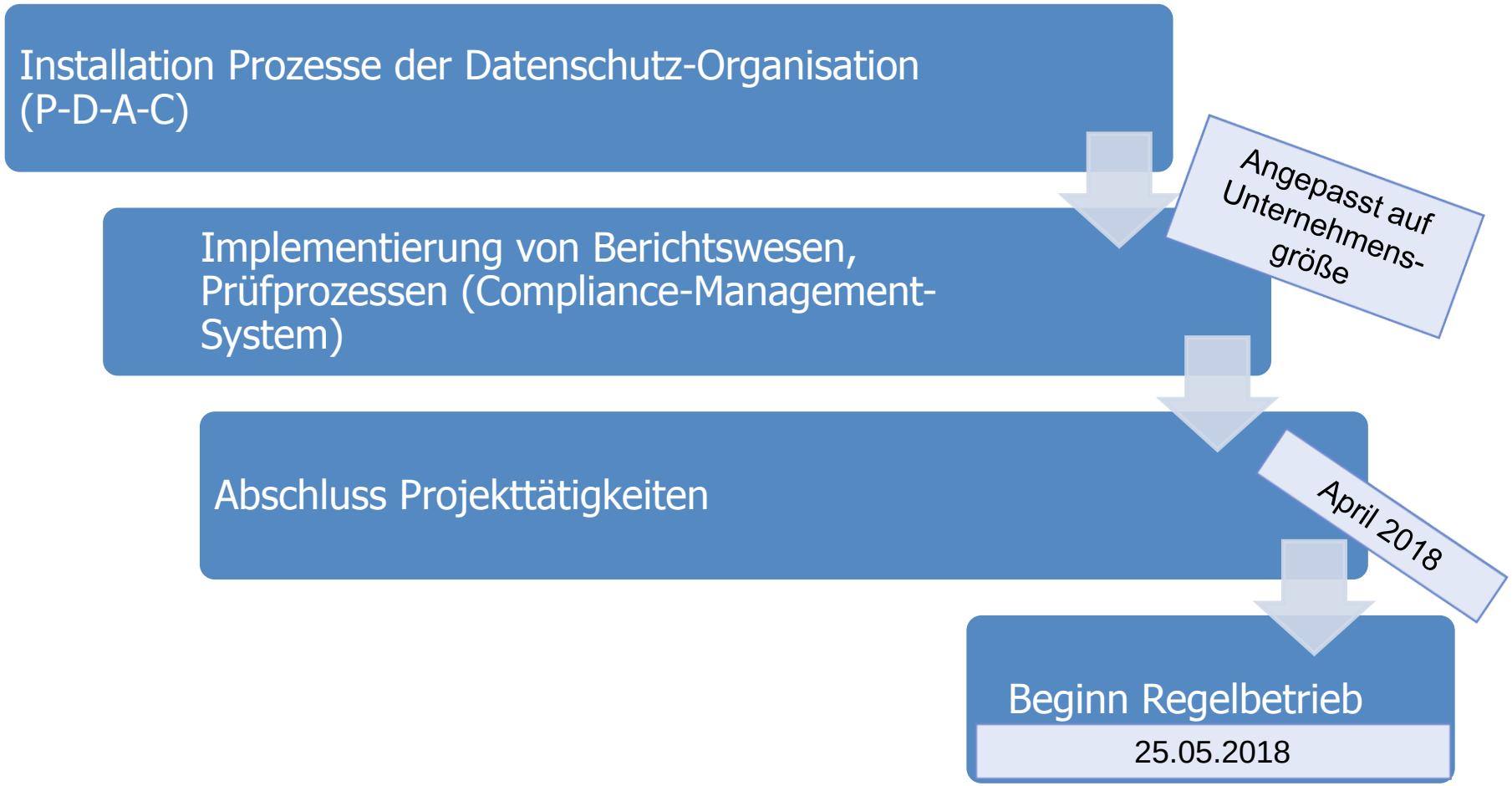
Ablauf nach Aktionsplan DS-GVO

Start: Sofort nach Entscheidung GF

- Zuweisung der Verantwortlichkeit
- Ist-Analyse
- Erstellung des Verzeichnisses der Verarbeitungstätigkeit
- Dokumentierte Prüfung der Erfüllung sämtlicher Pflichten der DS-GVO
- Ggf. Anpassung von Verfahren

artus UNTERNEHMENSBERATUNG GMBH & CO. KG

Ablauf



Haben Sie Fragen oder sind Sie nur entsetzt ?

Quelle: Pixabay.com

artus UNTERNEHMENSBERATUNG GMBH & CO. KG

Ihr Datenschutzbeauftragter

Name: Oliver Luerweg

geboren: 1968

Externer DSB seit: 2004

Tätigkeiten: Geschäftsführender Gesellschafter

DATEV-Systempartner

Luerweg und Brinkmann GmbH seit 1992

Qualifikationen: Fachkraft für Datenschutz ***DEKRA***

Geprüfter Datenschutzbeauftragter ***DESAG*** und Mitglied im Berufsfachverband für das Sachverständigen- und Gutachterwesen ***BSG***

Zertifizierter Datenschutzbeauftragter ***TÜV / DATEV***

Zertifizierter Datenschutz-Manager & Datenschutz-Auditor ***TÜV***

Mitglied des Berufsverbandes der Datenschutzbeauftragten Deutschlands e.V. **BvD**

Mitglied der Gesellschaft für Datenschutz und Datensicherheit ***GDD***

EDV-Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung im kaufmännisch-administrativen Bereich

Kontakt: **Schaafsweg 42, 47559 Kranenburg**

02821/76060 **luerweg@luerweg.de**