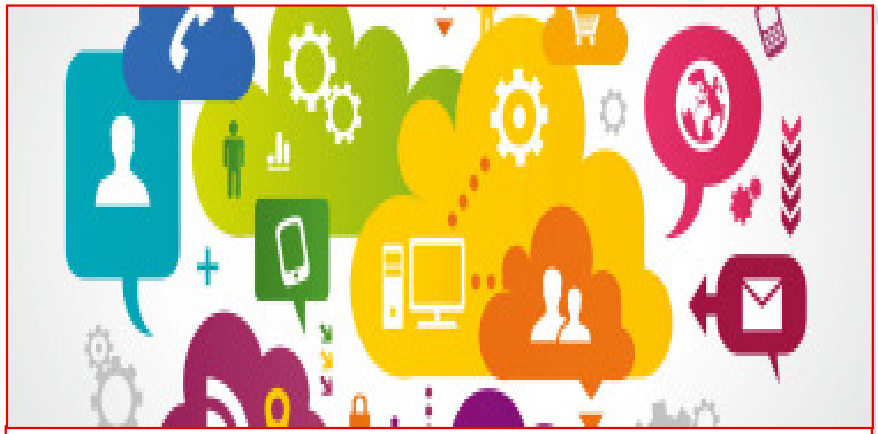
VSE NET Telekommunikation

Die EU-Datenschutz-Grundverordnung: Auswirkungen auf Ihr Unternehmen

IT-Tag Saar, 6. Oktober 2016

SAARLAND

Datenschutzrechtliche Herausforderungen der digitalen Welt



Globalisierung, Social-Media, Cloud-Computing, Wirtschaft 4.0, Internet der Dinge und Digitalisierung sind Entwicklungen hinsichtlich der **Art und Weise** wie wir **heute Daten nutzen, austauschen und speichern**.

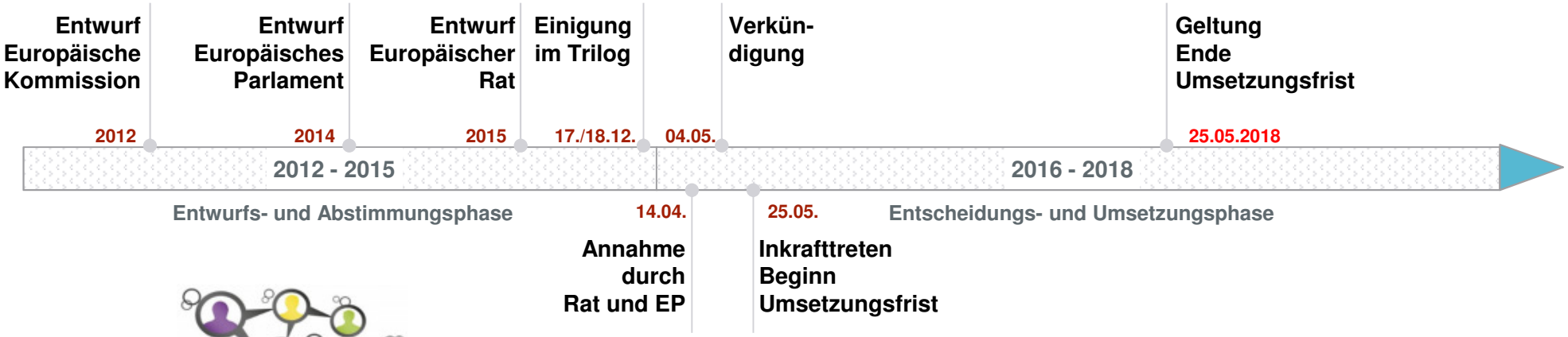
- Durchdringung aller Lebensbereiche
- Zweckübergreifende Auswertung
- Allgegenwärtigkeit (z. B. kontaktlose Chips, Sensorik)
- Autonome Steuerungen (z. B. Autos)
- Infrastruktur nicht vertrauenswürdig
- Datenspuren und Verknüpfungsmöglichkeiten
- Dominante Anbieter mit riesigen Datenmengen

Quelle: ULD

Erfordernis eines einheitliches Datenschutzrechts in Europa, das an die heutigen Bedürfnisse im Umgang mit Daten und deren Schutz ausgerichtet ist.

Der lange Weg zum neuen europäischen Datenschutzrecht

Phasen 2012 bis 2018



- Mehr als 3.300 Änderungsanträge zum 1. Entwurf
- Massives Lobbying insbes. US-amerikanischer IT- und Technologieunternehmen
- Verzögerungen durch Neuwahlen

- **BDSG gilt weiter**
- Umsetzungsfrist (2 Jahre)
  (Verarbeitungen, die zum Zeitpunkt des Inkrafttretens bereits begonnen haben, sollen innerhalb von 2 Jahren mit der EU-DS-GVO in Einklang gebracht werden.)
- Ermächtigung der Kommission zum Erlass delegierter Rechtsakte
  (Ergänzung/Präzisierung/Änderung nicht wesentlicher Punkte)

- **BDSG nicht mehr anwendbar**
- Aufhebung EU-DS-Richtlinie
- Verarbeitungen müssen im Einklang mit EU-DS-GVO sein.
- Ablauf diverser Melde-/Erklärungspflichten der Mitgliedstaaten

Ziele eines europäisch einheitlichen Datenschutzes nicht von heute auf morgen erreichbar

Wesentliche Ziele

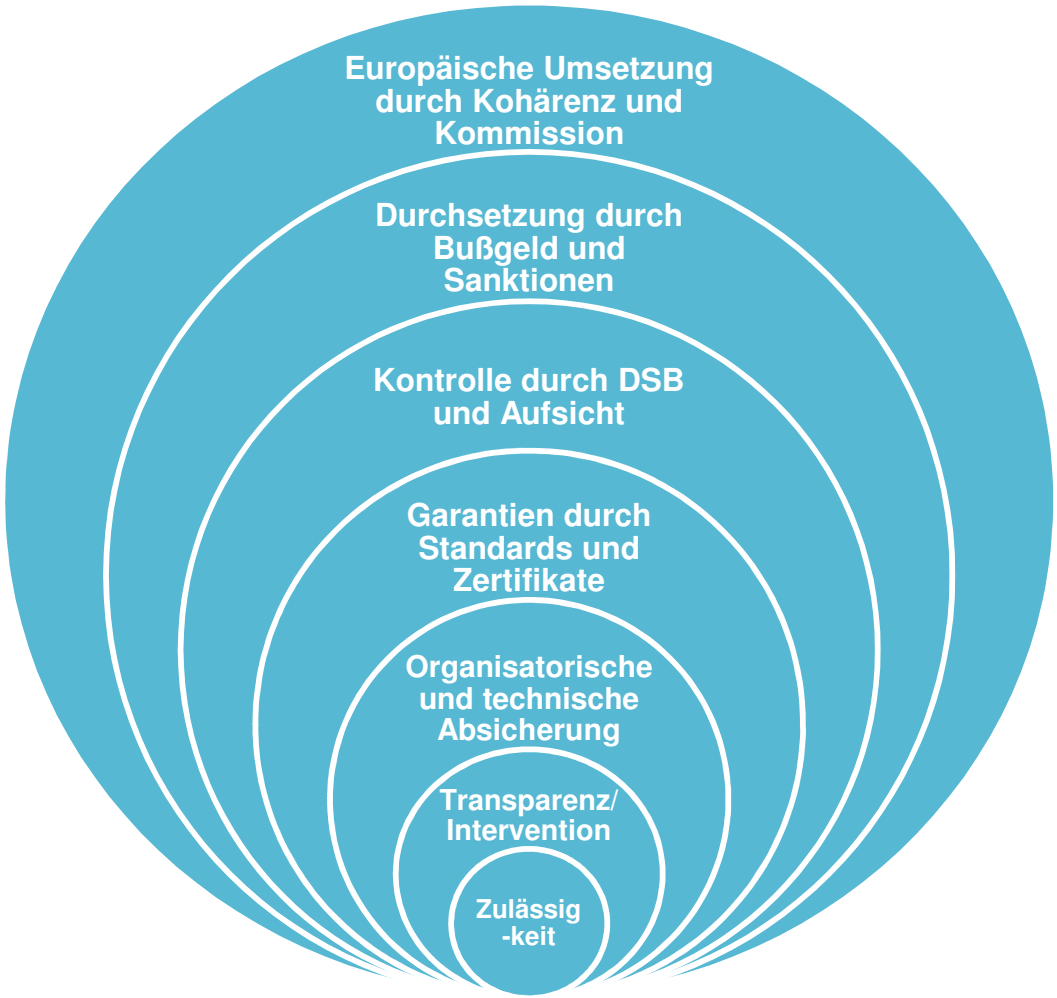
- **Schutz der Grundrechte und -freiheiten** natürlicher Personen sowie freier Verkehr personenbezogener (pb) Daten
- **Stärkung der Betroffenenrechte** (Informationspflichten, Recht auf Vergessenwerden und Daten-portabilität, Privacy-by-Default und Privacy-by-Design)
- **Schaffung eines homogenen Datenschutzrechts** in Europa; Kohärenzverfahren sichert einheitliche Auslegung und Anwendung des Gesetzes (Europäischer Datenschutzausschuss)
- **Sicherstellen eines einheitlichen Datenschutzniveaus und einheitlicher Schutzstandards** in allen EU-Mitgliedsstaaten
- Anwendung des Datenschutzrechts für Unternehmen aus Nicht-EU-Ländern (-> **Marktortprinzip**)
- **Effiziente Kooperation** der Datenschutzaufsichtsbehörden

Mögliche Hemmnisse bei der Zielerreichung

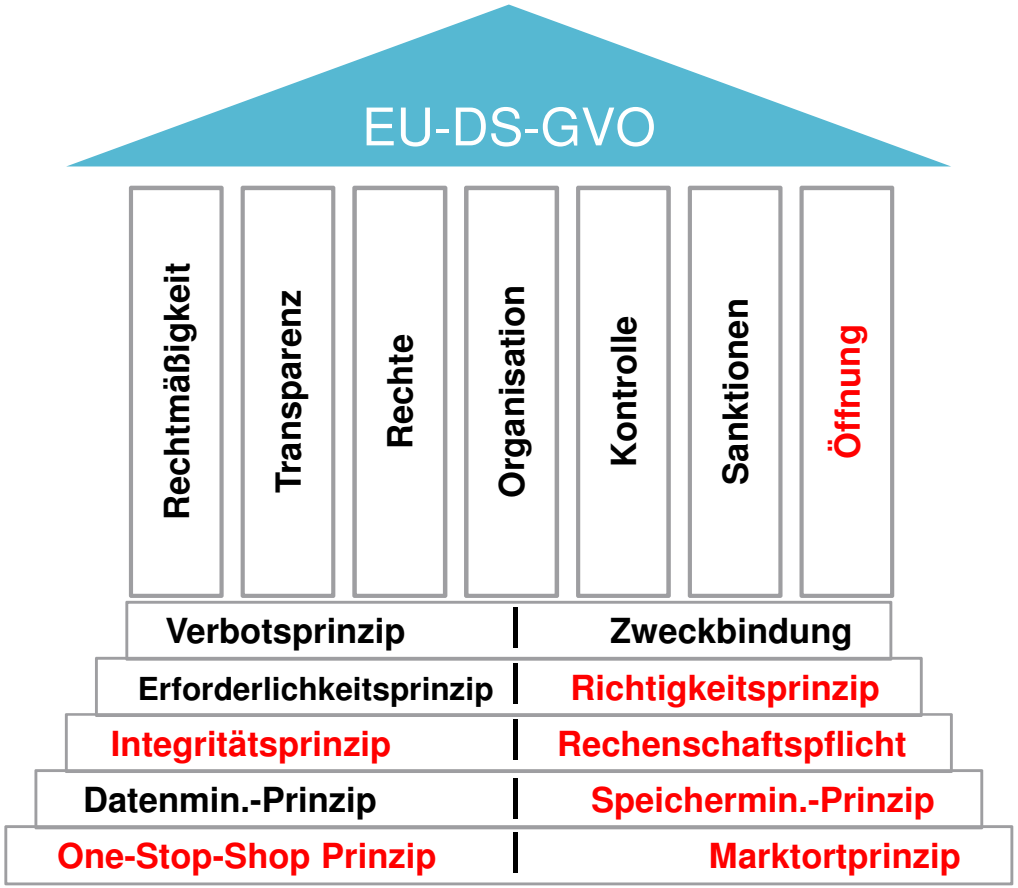
- ↘ **Einheitlichkeit** wird **nur bedingt** erreicht, an über 50 Stellen finden sich sog. **Öffnungsklauseln** (vornehmlich für den öffentlichen Bereich, aber auch Beschäftigtendatenschutz).
- ↘ Unklar, wann und in welchem Ausmaß **nationale Sondervorschriften** in den Mitgliedsstaaten erlassen werden und diese bei grenzüberschreitenden Datenverarbeitungen zur Anwendung kommen.
- ↘ Viel **Interpretationsspielraum mit höherer Rechtsunsicherheit** in der Startphase, u. a. 172 **Erwägungsgründe**, unterschiedliche Ausgangssituationen und gelebter Datenschutz.

Dies bietet Unternehmen aber auch Chancen bei der Umsetzung und Anwendung des neuen Rechts.

Aufbau der EU-Datenschutz-Grundverordnung



Prinzipien des neuen europäischen Datenschutzrechts



Rote Schrift = neue/erweiterte Prinzipien

- EU-DS-GVO ist **unmittelbares Recht**. -> Durchgriffswirkung
- EU-DS-GVO **ersetzt nationales Recht**, führt grds. zur Unanwendbarkeit entgegenstehender nationaler Regelungen (aber: **Öffnungsklauseln**).
- mit der EU-DS-GVO **entfallen Regelungen** zahlreicher BDSG-**Spezialtatbestände** (z.B. Videoüberwachung, Werbung, Scoring).
- EU-DS-GVO definiert mehr allgemeine Grundsätze, insbes. den **Grundsatz von Treu und Glauben** (Art. 5 Nr. 1a) als Auffangtatbestand und die neue **Rechenschaftspflicht** (accountability = responsible for and to be able to demonstrate compliance).

BDSG = Bundesdatenschutzgesetz

Der für die Verarbeitung Verantwortliche unterliegt einer Rechenschaftspflicht (Accountability)

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	Verarbeitung auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für den Betroffenen nachvollziehbaren Weise
Zweckbindung	Erhebung für festgelegte, eindeutige und rechtmäßige Zwecke und Verbot der Weiterverarbeitung in einer mit diesen Zwecken nicht zu vereinbarenden Weise
Datenminimierung	Beschränkung auf das für den Zweck der Verarbeitung angemessene und sachlich relevante sowie notwendige Maß
Richtigkeit	Sachlich richtige und ggf. aktuellste Daten; Vorsehen von Maßnahmen zur unverzüglichen Löschung oder Berichtigung von unzutreffenden Daten
Speicherbegrenzung	Speicherung mit Personenbezug höchstens so lange, wie es für die Verarbeitungszwecke erforderlich ist
Integrität und Vertraulichkeit	Geeignete technisch-organisatorische Maßnahmen (TOM) zum Schutz der Daten, insbes. vor unbefugter oder unrechtmäßiger Verarbeitung, zufälligem Verlust, zufälliger Zerstörung oder Schädigung

Rechenschaftspflicht (Accountability):

- **Verantwortung**

und

- **Nachweispflicht**

für die Einhaltung der Prinzipien

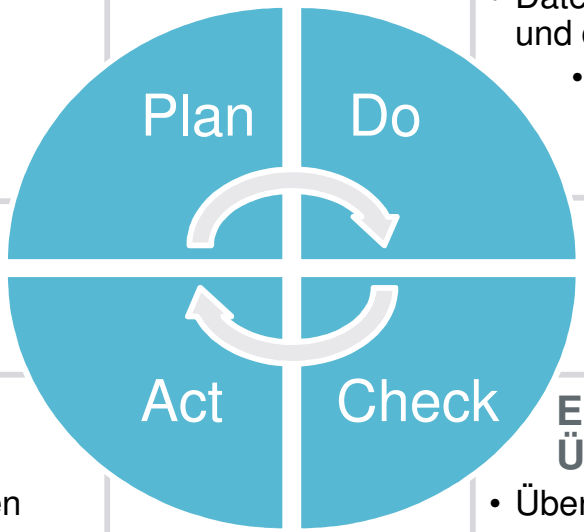
Einhaltung und Umsetzung der Prinzipien stellt (neue) Anforderungen an die Datenschutzorganisation

- **Policy:** definiert die **grundsätzlichen Leitlinien** des Unternehmens im Hinblick auf die **Einhaltung der Prinzipien und Grundsätze zur Datenverarbeitung**.
- **Directive:** Grundlegende **Festlegungen zur Datenschutzorganisation** sowie zu weiteren **nachweisbaren Datenschutzvorkehrungen**, z. B. Zuweisung von Zuständigkeiten, Schulungen, Vorgaben zur operativen Datenverarbeitung. Auch spezifische Festlegungen zu über den gesetzlichen Rahmen hinausgehende **Aufgaben des Datenschutzbeauftragten**.
- **Leitfäden** und **Checklisten** : **Handlungsempfehlungen** des Datenschutz für operative Datenschutzthemen.
- **Verzeichnis aller Verarbeitungstätigkeiten** : **Verzeichnisführung** aller Prozesse/Verfahren mit Verarbeitung pb Daten.

Ganzheitliches und risikobasiertes Datenschutz-Managementsystem erforderlich

Planung und Konzeption
- Risikobewertung:
  - Art, Umfang, Umstände und Zweck der Verarbeitung
  - Eintrittswahrscheinlichkeit
  - Risiken für die persönlichen Rechte und Freiheiten

Umsetzung
- Geeignete technische und organisatorische Maßnahmen
- Datenschutzvorkehrungen (policy und directive)
  - Nachweis der Verarbeitung in Übereinstimmung mit der EU-DS-GVO



Optimierung und Verbesserung
- Aktualisierung der Maßnahmen

Erfolgskontrolle und Überwachung
- Überprüfung der Maßnahmen

Zusätzliche Transparenz-, Dokumentations-, Nachweis- und Rechenschaftspflichten sowie die Datenschutz-Folgenabschätzung führen zu höherem bürokratischen Aufwand.

Evolution der Rolle des Datenschutzbeauftragten

1977/ 1990 — **Sicherstellungs-auftrag**
§ 29 Abs. 1 BDSG/
§ 37 Abs. 1 BDSG

2001 — **Hinwirkungs-auftrag**
§ 4g Abs. 1 BDSG

2018 — **Überwachungs-auftrag**
Art. 36 Abs. 1
EU-DS-GVO

- Erstmal **gesetzliche europaweite Pflicht zur Bestellung eines Datenschutzbeauftragten (DSB)**, zumindest wenn das Geschäftsmodell im Kern auf der Verarbeitung pb Daten beruht
- **Öffnungsklausel** ermöglicht weitergehende nationale Festlegungen; Deutschland: vrs. keine Änderung
- **Rolle des DSB** entwickelt sich in **Richtung Überwachungsfunktion** (->DS-Compliance)
  - EU-DS-GVO und andere Rechtsvorschriften
  - Strategien (Policies), insbes. hinsichtlich
    - Zuweisung von Zuständigkeiten
    - Sensibilisierung und Schulung der Mitarbeiter
    - Überprüfungen (z. B. Audits, Zertifizierungen)
- **Unmittelbarer Bericht** an höchste Managementebene
- **Verpflichtung** des Unternehmens (Verantwortliche Stelle) zur **ordnungsgemäßen und frühzeitigen Einbindung** des DSB „in alle mit dem Schutz pb Daten zusammenhängenden Fragen“
- Ernennung durch Gruppe von Unternehmen möglich

Wesentliche Pflichten für Unternehmen
- Vorgaben zur operativen Datenverarbeitung (1) -

- Nach Art. 25 EU-DS-GVO sind der Grundsatz **„Datenschutz durch Technik“** (**data protection by design**) und datenschutzfreundliche Voreinstellungen (**data protection by default**) sicherzustellen, z. B. Minimierung der Verarbeitung von pb Daten, Pseudonymisierung, Herstellen von Transparenz und Möglichkeiten für den Betroffenen zur Überwachung. **Es werden Sicherheitsziele wie Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme definiert. Wirksamkeitstests gefordert.**
- Nach Art. 30 EU-DS-GVO ist ein **Verzeichnis aller Verarbeitungstätigkeiten** mit festgelegten Einzelangaben zu führen (entspricht weitgehend dem heutigen internen Verfahrensverzeichnis):
  - Es gibt kein öffentliches Verfahrensverzeichnis mehr!
  - Auftragsverarbeiter müssen zukünftig auch ein Verzeichnis der Verarbeitungstätigkeiten führen!
- Gem. Art. 33 EU-DS-GVO sind **Verletzungen des Schutzes pb Daten** an die **Aufsichtsbehörde** zu melden, und zwar unabhängig von den betroffenen Daten und der Art der **Datenschutzverletzung** (keine Analogie zu § 42 a-Meldungen BDSG, Analogie zur heutigen § 109 a-Meldung TKG)
  - Meldefrist: 72 Stunden
  - Keine Meldepflicht, wenn Risiko für Rechte und Freiheiten von Individuen unwahrscheinlich
- Nach Art. 34 EU-DS-GVO muss auch eine **Information** an die **Betroffenen** erfolgen; es sei denn, es wurden geeignete technisch-organisatorische Maßnahmen getroffen, die die Daten für Dritte unverständlich machen (z. B. **Verschlüsselung**).
- **Alle etwaigen Verletzungen des Schutzes pb Daten** sind unter Beschreibung aller im Zusammenhang mit der Verletzung stehenden Fakten, deren Auswirkungen und der ergriffenen Abwehrmaßnahmen zu **dokumentieren.** Insbesondere bei Fällen, die keine Meldepflicht auslösen, ist schriftlich vom DSB festzuhalten, mit welcher Argumentation von einer Meldung abgesehen wurde!

Wesentliche Pflichten für Unternehmen
- Vorgaben zur operativen Datenverarbeitung (2) -

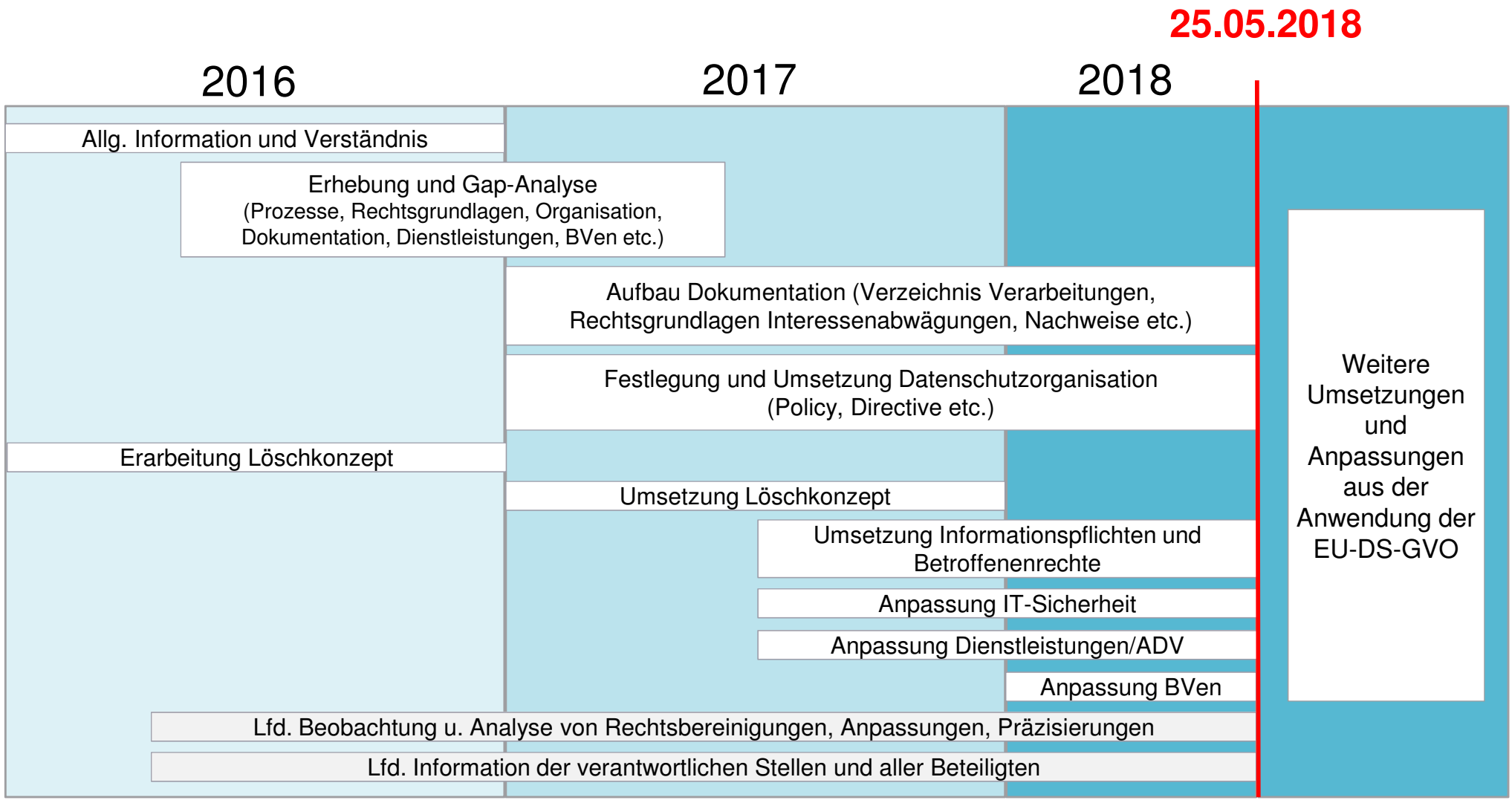
- Gem. Art. 35 ist eine **Datenschutz-Folgenabschätzung** unter Einbindung des DSB vorzunehmen, wenn eine Verarbeitung wahrscheinlich ein hohes Risiko verursacht (z. B. neue Technologien, automatisierte Verarbeitung); die bisherige Vorabkontrolle bei sensiblen Daten durch den DSB entfällt.
  - Einbindung Behörde nach Art. 36 EU-DS-GVO, wenn Folgenabschätzung ergibt, dass Datenverarbeitung ohne Maßnahmen ein hohes Risiko bedeutet.
  - Behörden werden Positiv-/Negativ-Listen veröffentlichen.
- Eine **Verpflichtung auf das Datengeheimnis** gibt es in der EU-DS-GVO nicht mehr, es wird trotzdem empfohlen, eine Verpflichtungserklärung aufgrund der erweiterten Nachweispflichten weiter im Einsatz zu halten.
- Die Rechtslage bei **„Einwilligungen“** ändert sich grundsätzlich nicht; lediglich bei Minderjährigen unter 16 Jahren ist darauf zu achten, dass die Sorgeberechtigten einwilligen/zustimmen.
- Die **Informations- und Mitteilungspflichten** (Art. 13 - 15 EU-DS-GVO) werden erweitert, gefordert wird eine präzise und transparente Information in einer klaren und einfachen Sprache (Aufbau und Ausgestaltung erfordern Zeit und Fingerspitzengefühl!)
- Das **Recht** der Betroffenen **auf Vergessenwerden** (Art. 17 EU-DS-GVO) erfordert die Implementierung vollständiger **Löschroutinen. Umfangreiche Auskunftsrechte** (Art. 15 EU-DS-GVO): **auch durch Kopie aller pb Daten in elektronischer Form in einem gängigen Format (Anpassung an IT-Systeme!)** .
- In Art. 47 EU-DS-GVO wird ein „**kleines Konzernprivileg**“ konstituiert, dass bei Gewährleistung eines angemessenen und einheitlichen Datenschutzniveaus die Datenweitergabe zwischen verbundenen Unternehmen erleichtert.
- Art. 26 EU-DS-GVO regelt **gemeinsam für die Verarbeitung Verantwortliche („Joint Control“),** hierbei legen mehrere Verantwortliche die Zwecke und Mittel gleichberechtigt und gemeinsam transparent fest

Verschärfung der Bußgeldvorschriften

Art 83 Abs. 4	Art. 83 Abs. 5	Art. 83 Abs. 6
Bis 10 Mio. EUR oder bis 2% des weltweiten Vorjahresumsatzes	Bis 20 Mio. EUR oder 4% des weltweiten Vorjahresumsatzes	Bis 20 Mio. EUR oder 4% des weltweiten Vorjahresumsatzes
	je nachdem, was höher ist !!!	
Verstöße gegen Regelungen, z.B. - **Schutzmaßnahmen (TOM)** - **Auftragsverarbeitung** (NEU: auch gegen Auftragsverarbeiter) - **Verzeichnis der Verar-beitungstätigkeiten** - Datenschutz-Folgenabschätzung - Bestellung DSB - Zertifizierung - …	Verstöße gegen Regelungen, z.B. - Grundsätze (Art. 5) - Rechtmäßigkeit - Einwilligung - **Rechte Betroffener** - Drittlandsübermittlung - Zusammenarbeit mit Aufsichtsbehörde - …	Verstöße gegen Anordnungen der Aufsichtsbehörde

Von den Bußgeldregelungen werden Unternehmen mit Sitz in der EU und Unternehmen, die personenbezogene Daten über in der EU ansässige Personen verarbeiten, erfasst.
Der Begriff „Unternehmen“ knüpft nicht mehr wie beim BDSG am Rechtssubjekt (juristische Person) an, sondern am Marktverhalten der wirtschaftlichen Einheit insgesamt (somit auch Konzerne).

Grober Maßnahmenplan – Der Countdown läuft



Vielen Dank für Ihre Aufmerksamkeit!

KONTAKT

Wolfgang Schütz
RWE Konzern-Datenschutz

- VSE NET GmbH
- Nell-Breuning-Allee 6, 66115 Saarbrücken
- wolfgang.schuetz@rwe.com

BACKUP

Telekommunikation aus einer Hand

Kurzportrait VSE NET

Alles aus einer Hand – das Leistungsportfolio

VERNETZUNG

- Festverbindungen, Leased Lines
- Standortvernetzung
- Carrier- und Satellitendienste

INTERNET

- Internetzugang
- IP-VPN
- Security
- Managed Router
- TV

SPRACHE

- Festnetz-Telefonie (Analog/ISDN)
- Voice over IP
- SIP Trunking
- Betriebsfunk

RECHENZENTRUM

- Managed Server
- Hosting
- Housing

CLOUD SERVICES

- virtuelle ACD
- virtuelles Callcenter
- Konferenzdienste
- intelligentes Stör- und Ansage Management
- Mehrwertdienste (0800, 0180 etc.)
- voice-to-mail / -to-fax /- to-SMS
- mail-to-fax

VSE NET - Auf einen Blick

- gegründet 1998
- eingebunden in das saarländische Traditionsunternehmen VSE AG
- die Unternehmen VSE NET und ihre Schwestergesellschaft Cegecom bündeln ihre Aktivitäten in der artelis-Gruppe
- ca. 160 Mitarbeiter insgesamt in der artelis-Gruppe
- Geschäftsführung: Michael Leidinger und Georges Muller
- Standorte: Saarbrücken und Geislautern

KONTAKT

- Bernd Trampert
  Leiter Vertrieb & Marketing Saarland
- VSE NET GmbH
  Nell-Breuning-Allee 6
  66115 Saarbrücken
- Telefon: 0681 607-5076
- Telefax: 0681 607-1112
- bernd.trampert@vsenet.de
- www.vsenet.de