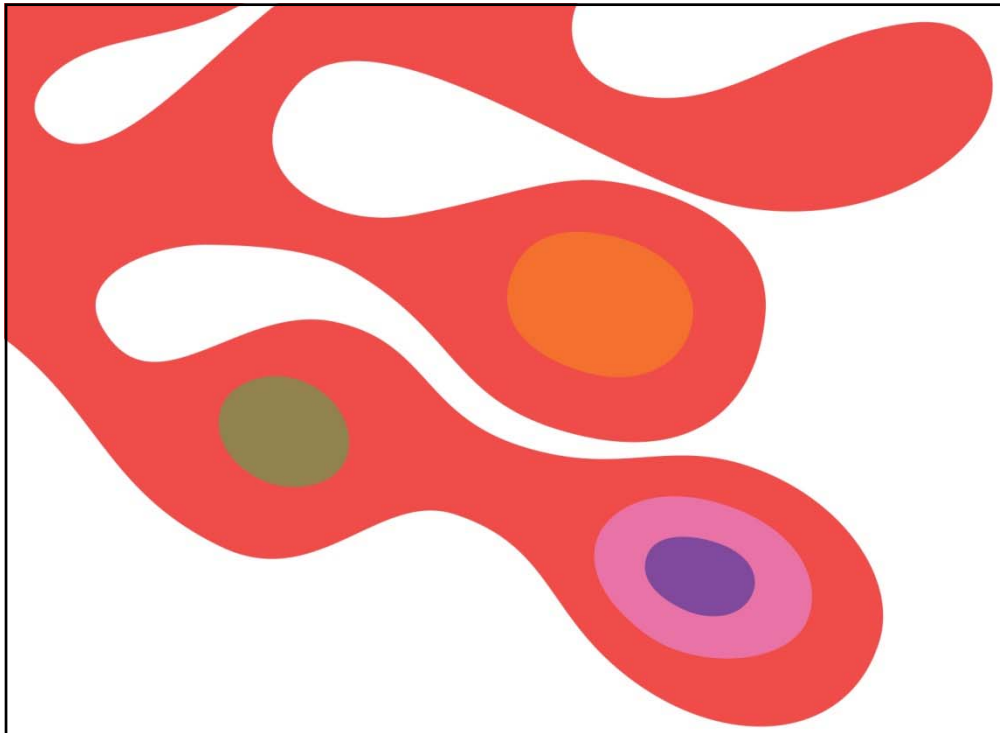


Die DSGVO steht vor der Tür – erste Erfahrungen aus einer Umsetzung

Dr. Natalie Ségur-Cabanac
Head of Regulatory, Hutchison Drei Austria GmbH

November 17

Datenschutzgrund verordnung.

Die EU Datenschutzgrundverordnung.

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)

25. Mai 2018

Das große Neue: sehr hohe Strafen

Die Kunst: Wo fange ich an? Wann fange ich an?

Zahlreiche neue Verpflichtungen, aber auch viele alte Bekannte

?

!

Grundsätze

- Zweckbindung
- Rechtmäßigkeit, Richtigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Datenminimierung und Speicherbegrenzung
- Data Privacy by design/Data Privacy by Default
- Integrität und Vertraulichkeit
- Verfahrensverzeichnis/Datenschutzfolgeabschätzung
- Datenschutzbeauftragte
- ……..

Der/Die Daten verarbeitet, muss stets nachweisen können, dass die DSGVO eingehalten wird

Sanktionen

- **Verwaltungsstrafen durch DSB**
  - Bis zu 20 Mio Euro oder 4 % des weltweiten jährlichen Konzernumsatzes des letzten Finanzjahres
  - Bisher nur Bezirksverwaltungsbehörden zuständig, max 35.000 Euro, nun auch DSB selbst
- **Gerichtsverfahren**
  - Unterlassung und Schadenersatz

Hohe Strafen, Reputationsverlust, Vetrauensverlust können existenzbedrohlich sein

Der Weg ist das Ziel.

Bestandsaufnahme und Gapanalyse

- Festlegen von Kriterien/Fragen für Erfassung der Ist Situation („Bestandsaufnahme“); Eventuell schon Struktur des späteren Verfahrensverzeichnisses verwenden;
- Im Fokus dabei steht jeweils ein bestimmter Zweck einer Datenverarbeitung, nicht ein System an sich;
- Systeme in einer eigenen Bestandsaufnahme (Technical Inventory) erfassen nach Kriterien von Data Privacy by Design und by Default
- Alle Beteiligten brauchen gemeinsames Verständnis über die Zielsetzungen und Anforderungen;
- Data Ownerships definieren!

Lerne Deine Organisation kennen, begebe Dich auf die Suche nach den Daten und Verantwortlichen und Du wirst viele Überraschungen erleben

Bestandsaufnahme und Gapanalyse

- Jemand sollte bereits hier den Hut des/der Datenschutzbeauftragten aufhaben und unterstützen;
- Verfassen von Guidelines und FAQs, die allen zugänglich sind, kann sehr hilfreich sein;
- Klare Information Security Anforderungen als enabler für die Einhaltung der DSGVO Anforderung durch Mitarbeiter etablieren;
- Prozesse und Richtlinien schriftlich verfassen und kommunizieren
- Fokus der Bestandsaufnahme und Gapanalyse liegt auf der Feststellung der Ist-Situation und Aufzeigen von notwendigen Maßnahmen und Investitionen zur Schließung allfälliger Gaps;

Bestandsaufnahme – Struktur hilft.

Data Privacy

Project Management

- Project Setup
- Project Controlling
- Project Closing
- Trigger Follow Up Activities

Project Content

Business inventory of products and processes

- New customers and prospects
- MVNO / Wholesale
- Existing customers
- Properties
- Finance (CF, Accounting, Controlling)
- Eety
- Marketing Intelligence
- Employees
- Vendors and contractors

Gap analysis and specification of required changes

- New customers and prospects
- MVNO / Wholesale
- Existing customers
- Properties
- Finance (CF, Accounting, Controlling)
- Eety
- Marketing Intelligence
- Employees
- Vendors and contractors

Further obligations

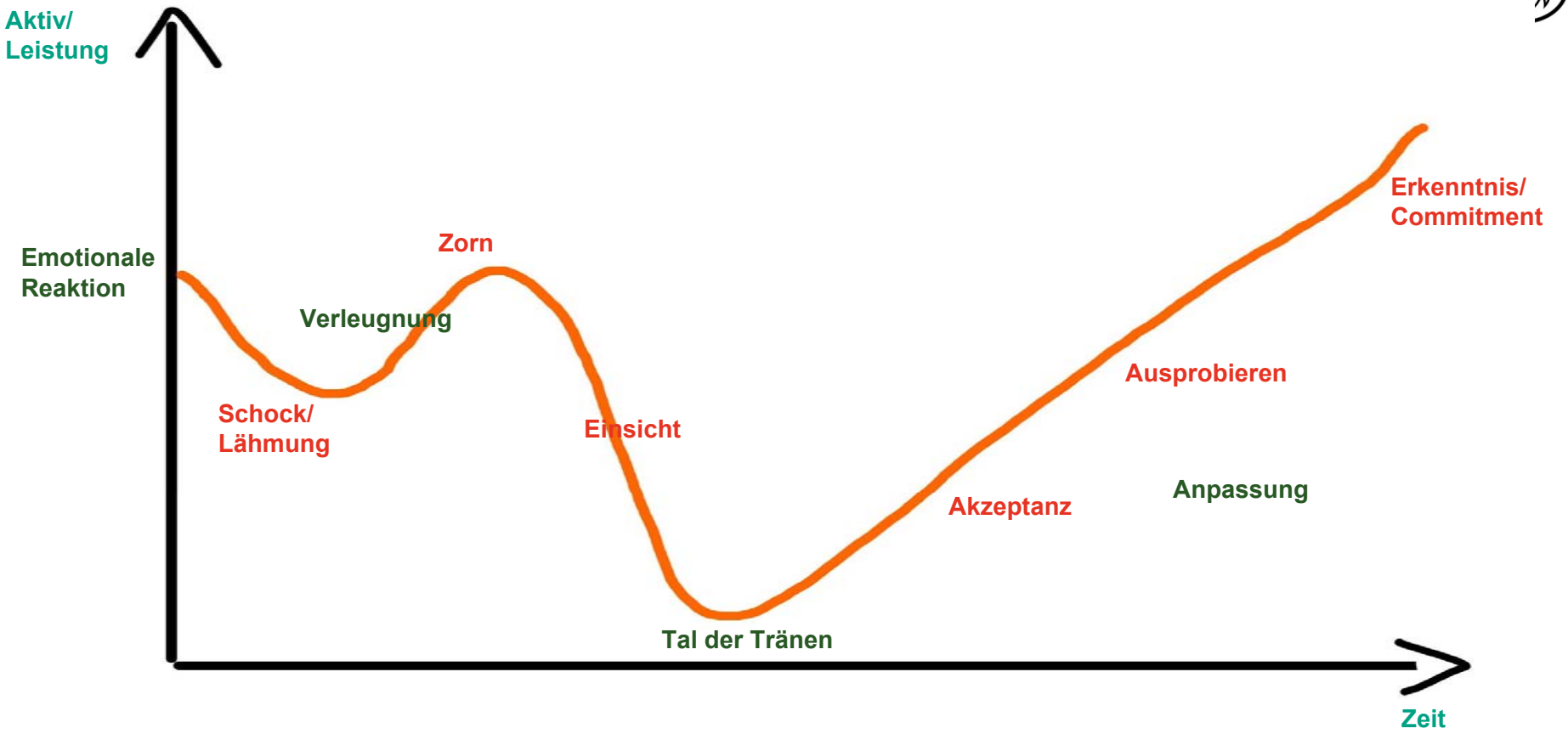
- Records of processing activities
- Data protection impact assessment
- Security of processing
- Data protection by design and by default
- Notification of personal data breach
- Introduction of Data protection Officer
- Codes of conduct and certification
- Transfer of PD to 3rd countries / binding corp. rules

Technical system inventory

- IT
- Core
- RAN
- SQM
- T&TC

Ein echter Change.

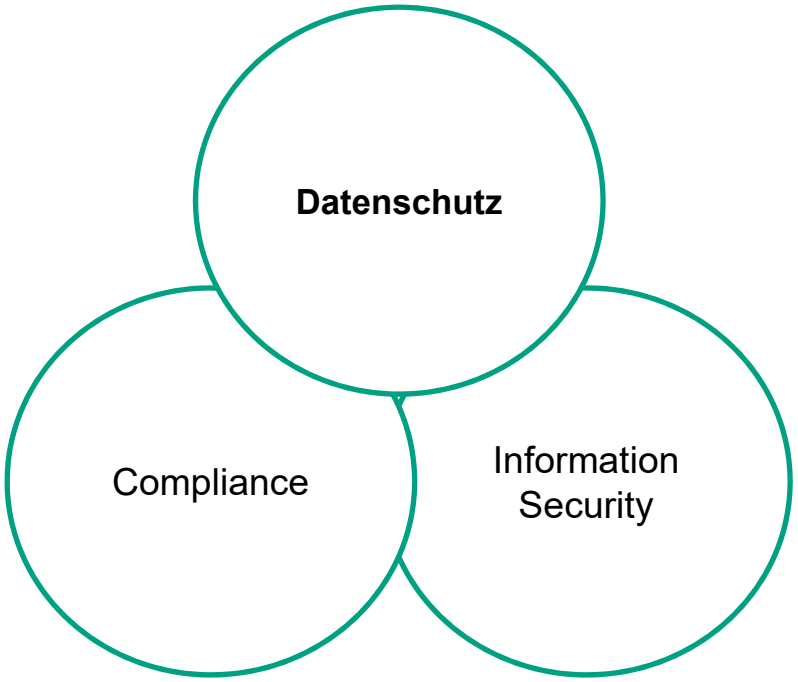
Achtung, Veränderung!



Team - works

Vernetzung schafft Verständnis

Datenschutzmanagementsystem.



Diverse Bereiche überschneiden sich, gehören aber klar abgegrenzt

Rechenschaftspflicht.

Compliance mit DSGVO

Grundsätze der Datenverarbeitung (Art 5 Abs 1 DSGVO)

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

Rechenschaftspflicht (Artikel 5 Abs 2 DSGVO):

Der Verantwortliche ist für die Einhaltung des Absatz 1 verantwortlich und muss dessen Einhaltung nachweisen können.

Umfassende Dokumentation

- Rechenschaftspflicht trifft laut DSGVO Verantwortlichen
- Verantwortliche und Auftragsverarbeiter sollten ausreichend dokumentieren
- Was nicht schriftlich festgehalten ist, hat im Zweifel nicht stattgefunden

Verfahrensverzeichnis

- Verpflichtend für Organisationen mit mehr als 250 Mitarbeitern;
- Wichtiges Werkzeug, hilft eine Datenverarbeitung strukturiert nach den Anforderungen der DSGVO zu prüfen;
- Elektronischer Workflow empfohlen (Nachweisbarkeit, Auditfähigkeit von Genehmigungen, Versionenhistorie, etc.);
- Review alle 2 Jahre oder bei inhaltlicher Änderung der Datenverarbeitung;
- Aufbau gemäß DSGVO inklusive erste Risikoabschätzung/Risikobewertung (für Entscheidung, ob DSFA notwendig oder nicht);
- Schulungen anbieten; viele Fachleute mit einbeziehen;

Datenschutzfolgeabschätzung

- Artikel 35 ff DSGVO

  - ✓ eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

  - ✓ eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

  - ✓ eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

  - ✓ die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Datenschutzfolgeabschätzung

- DSGVO erlaubt mit risikobasiertem Ansatz mehr Spielraum;
- DSFA wichtiges Tool, um
  - Risiken einer Datenverarbeitung zu erkennen,
  - Risiken abzuwägen
  - Mitigierungsmaßnahmen festzulegen
- Einheitliches Template für Dokumentation wichtig; Richtlinie/Policy (warum DSFA, wann genau? Wie genau? etc.) erstellen;
- Guidelines WP 248 der Art 29 WP beachten;
- Datenschutzbeauftragter sollte zu Rate beigezogen werden und die DSFA frei geben;
- Review alle 2 Jahre

PIA ≠ DPIA

Privacy Impact Assessment

Evaluierung aller Prozesse und Informationsflüsse in einer Organisation, die personenbezogene Daten beinhalten:

- Prüfung, ob ein PIA notwendig ist
- Beschreibung der Informationsflüsse
- Identifizierung von Risiken für die persönlichen Rechte und Freiheiten von Betroffenen
- Identifizierung von möglichen Maßnahmen zur Sicherstellung der persönlichen Rechte und Freiheiten von Betroffenen
- Erstellen eines Prüfberichts und Integration der Ergebnisse in alle Projektpläne und Vorhaben

DSGVO

Data Privacy Impact Assessment

Tiefergehende Prüfung einer konkreten Datenverarbeitung zur Risikominimierung

Rechenschaftspflicht Art 5 Abs 2 DSGVO

Betroffene.

Betroffenenrechte

Wie bisher:

- Recht auf Information;
- Recht auf Auskunft
- Recht auf Richtigstellung
- Recht auf Löschung

Neu hinzugekommen:

- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Recht auf Vergessenwerden (= Recht auf Löschung)

Betroffenenrechte

- Erster Schritt: Wer sind meine Betroffene?

  => Identifizierung der Betroffenen, zB Kunden, Mitarbeiter, Lieferanten, Spender, Patienten, Klienten etc

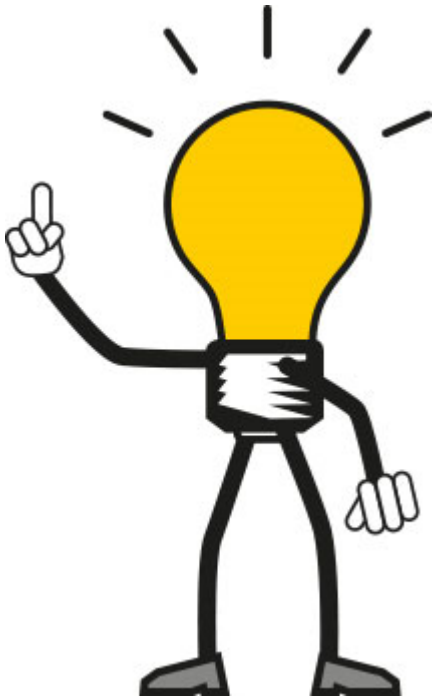
- Sicherstellung, dass alle Betroffenenrechte erfüllt sind

- Nicht vergessen: Mitarbeiter sind Betroffene!

- Tipp für Informationspflichten/Datenschutzerklärung: Produkt/Serviceverantwortliche beschreiben selber die Datenverarbeitung

Datenschutzbeauftragte/r.

Der/die Datenschutzbeauftragte wird's schon richten



Klarheit über Zuständigkeiten essentiell

Aufgaben Unternehmen.

Rechenschaft

- Verfahrensverzeichnis
- Management der Auftragsverarbeiter
- Privacy By Design
- Privacy by Default
- Compliance bei neuen Datenanwendungen
- Durchführung von Datenschutzfolge-abschätzungen (DPIA)

Transparenz

- Etablierung eines Datenschutz-management-systems
- Informationen an Betroffene
- Regeln für Datentransfer in nicht EU Länder

Information

- Beratung und Schulung der Mitarbeiter
- Fortbildungen/ Ausbildungen

Kommunikation

- Zusammenarbeit mit der Aufsichtsbehörde
- Bearbeitung und Beantwortung von Anfragen von Betroffenen
- Bearbeitung und Meldung von Sicherheitsvorfälle

Aufgaben Datenschutzbeauftragte(r).

Kontakt

- Zusammenarbeit mit der Aufsichtsbehörde
- Ansprechpartner für Aufsichtsbehörde

Beratung

- Beratung des Managements
- Beratung der Mitarbeiter
- Beratung der Betroffenen

Training

- Schulung der Mitarbeiter

Kontrolle

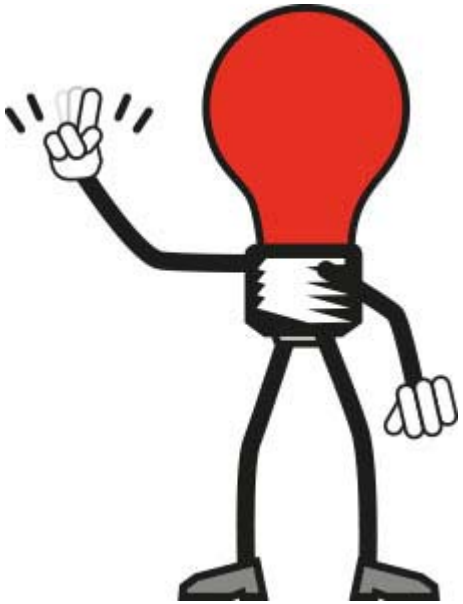
- Datenschutzfolge-abschätzung
- Kontrolle der Befolgung der DSGVO
- Kontrolle ob Datenschutz-management-system gelebt wird
- Berichte an oberstes Management

Die Rolle des/der Datenschutzbeauftragten

- DSB ist ein wichtiges Instrument für die Etablierung der DSGVO;
- DSB ist Helfer, Berater, aber kann nicht die Letztverantwortung tragen. DSB kann nicht GF/Senior Manager sein und auch nicht § 9 VstG Verantwortlicher;
- DSB kann nur so viel wissen, wie man ihn/sie wissen lässt;
- DSB muss das Vertrauen des obersten Managements haben und selber Geheimhaltung/Vertraulichkeit strikt einhalten;
- Stellung des DSB muss seine Weisungsfreiheit und Unabhängigkeit sicherstellen;

Die Rolle des DSB – Stellung

- DSB ist frühzeitig in alle datenschutzrelevanten Themen einzubeziehen
  => Besser zu viel als zu wenig DSB einbeziehen, DSB sollte sich ein gesamtes Bild machen können;
- DSB sollte die finanziellen und zeitlichen Ressourcen bekommen, sich fortzubilden;
- DSB sollte interne Schulungen durchführen; im persönlichen Kontakt lernt man nicht nur die Leute, sondern vor Allem die echten datenschutzrechtlichen Themen im Unternehmen kennen!
- offenes Ohr für alle Mitarbeiter und auch alle Fragen von Betroffenen von Datenverarbeitungen des Unternehmens



Datenschutzbeauftragte im Fokus……

Können Datenschutzbeauftragte für alle Fragen und Themen rund um Datenschutz zuständig gemacht werden?

…. Grenzen ziehen und sichtbar machen

Datenschutzbeauftragte dürfen keine Tätigkeiten/Verantwortlichkeiten übernehmen, die nicht mit ihrer Unabhängigkeit und Weisungsfreiheit vereinbar sind

Auftragsverarbeitung.

Auftragsverarbeitung

- Alle bestehenden Verträge mit Dritten prüfen, ob personenbezogene Daten verarbeitet werden (Achtung, auch Zugriffe auf Daten im Supportfall ist Auftragsverarbeitung!);
- Interne Verantwortliche für die Partnerverträge identizifizieren/definieren;
- Bestehende Verträge auf Anforderungen der DSGVO überprüfen und bei Bedarf einen neuen Vertrag/Änderungen gem. DSGVO abschließen;
- Achtung auf neue Anforderungen wie zB:
  - Auswahlsorgfaltspflicht des Verantwortlichen bei Auswahl von Auftragsverarbeitern
  - Subauftragnehmer müssen vom VV genehmigt werden
  - Auftragsverarbeiter direkt strafbar gem. DSGVO
  - Auditrechte vorbehalten
  - Zertifizierung verlangen oder technische Mindestanforderungen vorgeben/festlegen

Auftragsverarbeitung

- Achtung Cloud Services
  - Genaue Qualifikation des Services
  - Erstellung von Cloud Services Policy wird empfohlen inklusive
    - Kriterien, die ein Cloud Service bzw. ein Cloud Service Anbieter erfüllen muss sowie
    - Welche Daten/Datenkategorien dürfen in einer Cloud verarbeitet werden

- Was noch wichtig ist
  - Darauf achten, dass die Datenverarbeitung in der EU erfolgt;
  - Partner außerhalb der EU: Abschluss der EU Standardvertragsklauseln sinnvoll/notwendig; (Achtung: unterliegen derzeit auch einer Prüfung durch den EUGH);
  - Bei US Bezug: Privacy Shield Zertifizierung des Anbieters vorhanden? Wenn ja, genau prüfen, ob sich diese auf die beauftragte Datenverarbeitung bezieht!

Auftragsverarbeitung

- Praxis: Juristen, Einkauf, Technik, Business verhandelt Vertrag und auch AV. Für AV bietet sich der/die Datenschutzbeauftragte(r) („DSB“) an. **DSB soll und darf selber nicht für Verhandlungen verantwortlich sein, spießt sich mit Unabhängigkeit und Weisungsfreiheit**;

  => Bewährt hat sich daher: Verhandlungsteam inkl Juristen für AV Verhandlung verantwortlich und DSB berät.

- Mit **Management Rahmen der Haftungsgrenzen festlegen**:
  - Wer entscheidet, wenn Verhandlungen kein Ergebnis in diesem Rahmen bringen?
  - Was sind die Kriterien für mein Unternehmen? Woran orientiere ich mich? Großes/kleines Unternehmen des AV/Vertragswert/Risiko/Strafe gemäß DSGVO?
  - Eventuell schon mal Datenschutzfolgeabschätzung vorbereiten/machen, um die Risiken abschätzen zu können;

- Viele Vertragspartner, vor Allem aus dem amerikanischen Raum sind noch nicht fit in der DSGVO, das verzögert den Vertragsverhandlungsprozess mitunter beträchtlich;

Privacyofficers.at

Verein Privacyofficers.at

- **aktives Netzwerk** betrieblicher und behördlicher Datenschutzbeauftragter und sonstiger mit dem Thema Datenschutz Betrauter
- Entwicklung, Darstellung sowie Förderung des **Berufsbildes eines Datenschutzbeauftragten**
- **Plattform** zum Informations- und Erfahrungsaustausch
- fachliche Anleitungen und Empfehlungen (**Best Practice**)
- **Entwicklung von Ausbildungsinhalten** und Förderung entsprechender Maßnahmen im privaten und öffentlichen Bereich
- **Kooperation** mit in- und ausländischen Berufsvereinigungen und internationalen Fachorganisationen aus dem Bereich Datenschutz

Alle Infos: ww.privacyofficers.at

Verein Privacyofficers.at

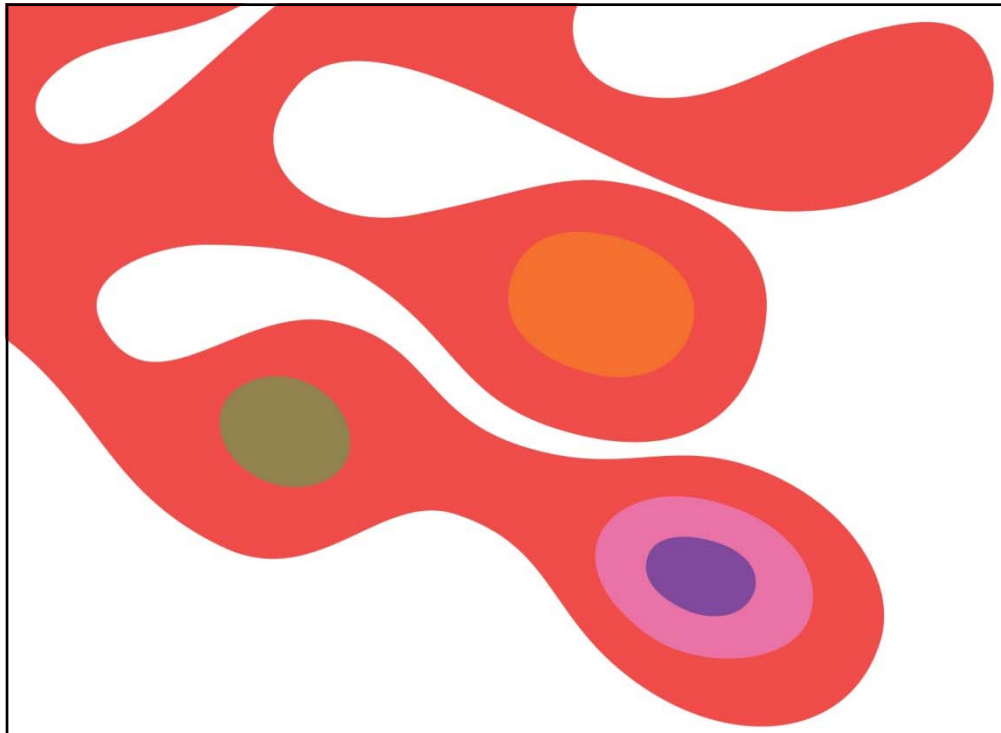
- **Checkliste Umsetzung der DSGVO**

  https://www.privacyofficers.at/Privacyofficers_Checkliste_Umsetzung_DSGVO_v2.0.pdf

- **Rollenbild der österreichischen betrieblichen und behördlichen Datenschutzbeauftragten**

  https://www.privacyofficers.at/Privacyofficers_Rollenbild_v1.0.pdf

Danke.



Es geht auch anders.