GEISTWERT
RECHTSANWÄLTE LAWYERS AVVOCATI

„Predictive Data Protection Maintenance“

… oder:

GEISTWERT
RECHTSANWÄLTE LAWYERS AVVOCATI

Technik, Recht und Organisation müssen gemeinsam ein Datenschutz-Managementsystem entwickeln!

Jede juristische Präsentation beginnt
(i) mit einem Witz, oder
(ii) mit Angst

(Witze sind heute leider aus)

Warum DSGVO-Projekt?

- Bisher „stiefmütterlich“ ... nunmehr Sanktionen:
  - Geldbußen bis EUR 20 Mio oder 4% Welt-Jahres-Konzern-Umsatzes (je nachdem, was höher)
  - Persönliche Haftung der Täter
  - materieller oder immaterieller Schadenersatz mit Beweislastumkehr
  - Strafbemessungsgründe in DSGVO

„Schaumgebremst in AT“?

heise online > News > 04/2018 > Keine Strafen: Österreich zieht neuem Datenschutz die Zähne

Keine Strafen: Österreich zieht neuem Datenschutz die Zähne

24.04.2018 16:43 Uhr – Daniel AJ Sokolov vorlesen

(Bild: Daniel AJ Sokolov)

In letzter Minute nimmt Österreich der neuen EU-Datenschutzverordnung den Biss, die meisten Verstöße werden straffrei bleiben. Und Datenschutz-NGOs dürfen keinen Schadenersatz eintreiben.

„Schaumgebremst in AT“?

- „Fake News“:
- Verwarnung durch die Datenschutzbehörde: „§ 11. Die Datenschutzbehörde wird den Katalog des Art. 83 Abs. 2 bis 6 DSGVO so zur Anwendung bringen, dass die Verhältnismäßigkeit gewahrt wird. Insbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen.“

→ Die Behörde kann auch beim ersten Verstoß bestrafen

„Schaumgebremst in AT“?

- „DSG“-Haftung:
  - zwar juristische Person haftbar, aber viele Einzelunternehmer
  - Es ist (!) von der Bestrafung der Geschäftsführung bei juristischen Personen abzusehen, wenn juristische Person bestraft wird
  - Gegen Behörden und öffentliche Stellen können keine Geldbußen verhängt werden → Wettbewerbsverzerrung im Bereich „Staat als Unternehmer“?

(Doch nicht) „Schaumgebremst“?

Wer mit Bereicherungsvorsatz oder Schädigungs-absicht das „berufsmäßige Datengeheimnis“ verletzt oder widerrechtlich verschaffte Daten verarbeitet, ist vom Gericht mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

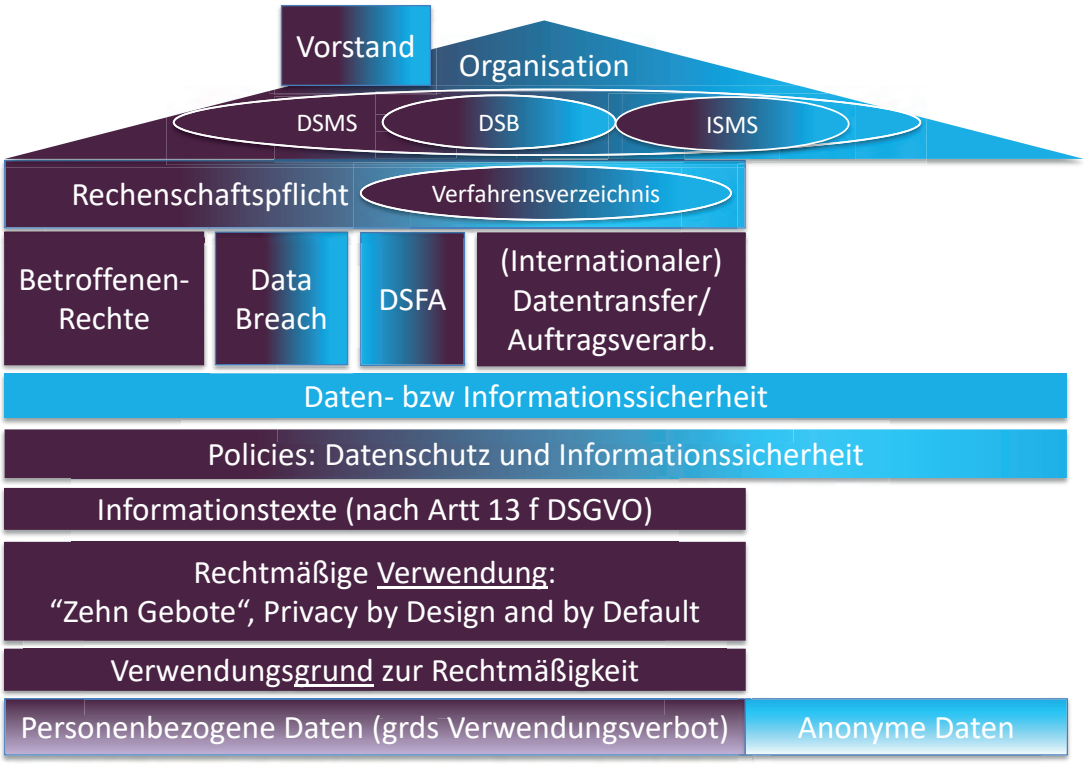
Daher:

DS-Compliance ist dynamisch: Vom DSGVO-(Implementierungs)Projekt zum DSGVO-Management/ Prozess

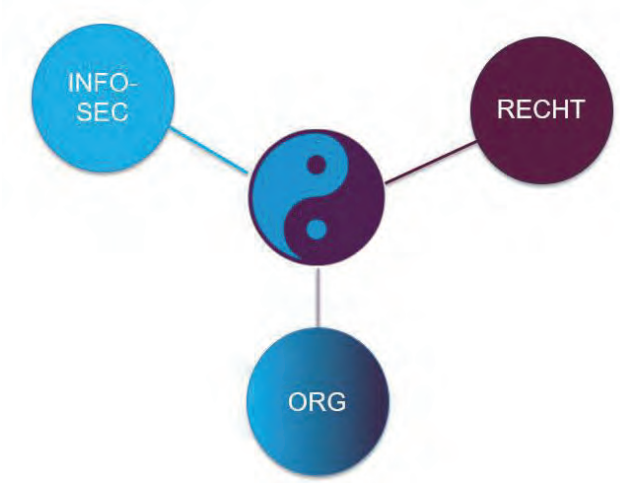
… jeweils mit Technik-Support-Bedarf!

Wir haben ein Haus zu bauen …

- DSGVO ist ein komplexes Regelungswerk
- Datenschutz betrifft jeden „Lebensbereich“ einer Organisation
- Sowohl die Erfassung als auch das Management der Verarbeitungstätigkeiten bedarf Technik-Support



Fast alle Schritte interdisziplinär



Wie ist das mit dem DSB?

Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen DSB, wenn

a) Behörde oder öffentlichen Stelle;

b) die Kerntätigkeit eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht; oder

c) die Kerntätigkeit Verarbeitung „sensibler Daten“ (Definition kommt dann gleich).

Worum geht es denn rechtlich eigentlich?!

Datenverarbeitungsverbot mit Erlaubnisvorbehalt

Verbot personenbezogene Daten zu verarbeiten, außer ein gesetzlich normierter Erlaubnisgrund „rechtfertigt“ die Datenverarbeitung.

→ „liberaler Rechtsstaat steht Kopf“

Personenbezogene Daten …

… sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. […]

(27) Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.

Personenbezogene Daten und …

… juristische Personen?!

§ 1 DSG. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht.

Personenbezogene Daten

Identifizierbar ist eine Person, die direkt oder indirekt, insb mittels Zuordnung zu einer Kennung wie Namen, (Online-)Kennnummer, Standortdaten, oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Pseudonyme Daten

(26) […] Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. […].

Anonyme Daten

(26) […] Die Grundsätze des Datenschutzes sollten [sic!] […] nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen […].

Anonyme Daten

(26) […] Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern […].

Anonyme Daten

(26) […] Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind […].

Verarbeitung

jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten …

→ Nichtautomatisiert in Dateisystem (strukturierte Sammlung: zB Karteikartensystem)

Verarbeitung

… wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Schutzstufen „personenbezogen“ und „sensibel“

(i) personenbezogene Daten (schon erklärt)

(ii) „sensible Daten“ („besondere Kategorien“) sind (abschließende Liste) personenbezogener Daten, aus denen die
- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen oder
- die Gewerkschaftszugehörigkeit hervorgehen, sowie

Schutzstufen „personenbezogen“ und „sensibel“

- genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten, oder
- Daten zum Sexualleben oder der sexuellen Orientierung.

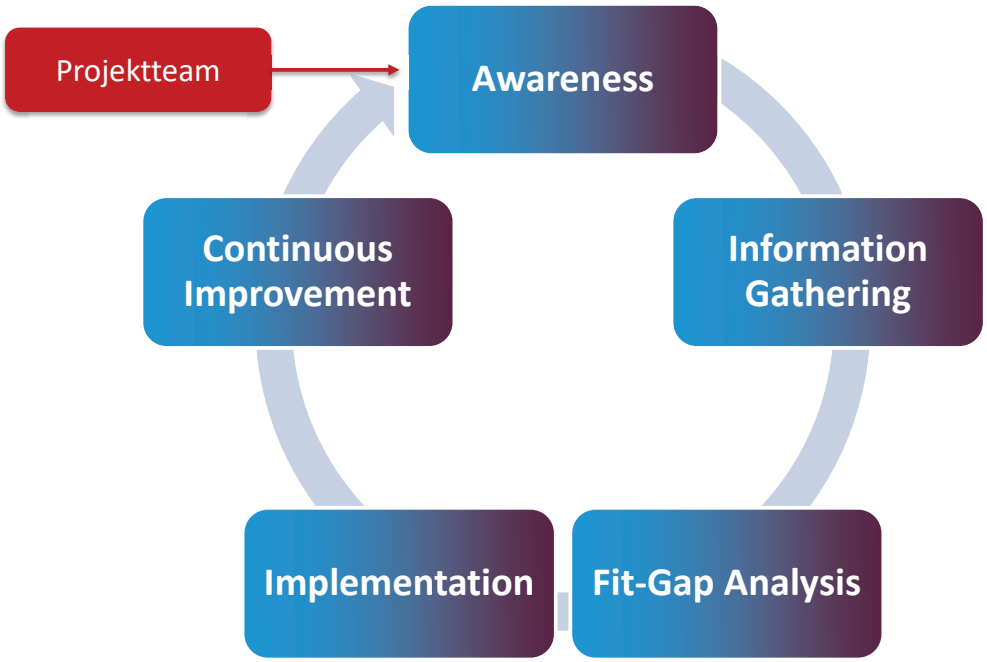
„Verbot unter Erlaubnisvorbehalt“ ist nicht neu!

Aber das „Wie“ und die „Rahmenbedingungen“ sind zT durch DSGVO neu!

„Zehn Gebote“ des Verantwortlichen

- Rechtmäßigkeit (viele Gründe, aber im Einzelfall zu prüfen)
- Treu und Glauben („Erwartbarkeit“)
- Transparenz (= „Informationspflicht“ (statt DVR))
- Zweckbindung (mit möglichen Ausnahmen)
- Datenminimierung (= „Notwendigkeitsbegrenzung“)
- Richtigkeit (und Aktualität)
- Speicher(dauer)begrenzung
- Integrität (= „IT-Sicherheit“)
- Vertraulichkeit (= „Daten-Sicherheit“)
- Rechenschaftspflicht = („Verfahrensverzeichnis“)

DSGVO-Projekt zur Dokumentation und Implementierung des „Wie“ und der „Rahmenbedingungen“



Rechenschaftspflicht

Der Verantwortliche ist für die Einhaltung der vorgenannten 9 Gebote verantwortlich und muss dessen Einhaltung nachweisen können.

→„qualifizierte Dokumentationspflicht“:

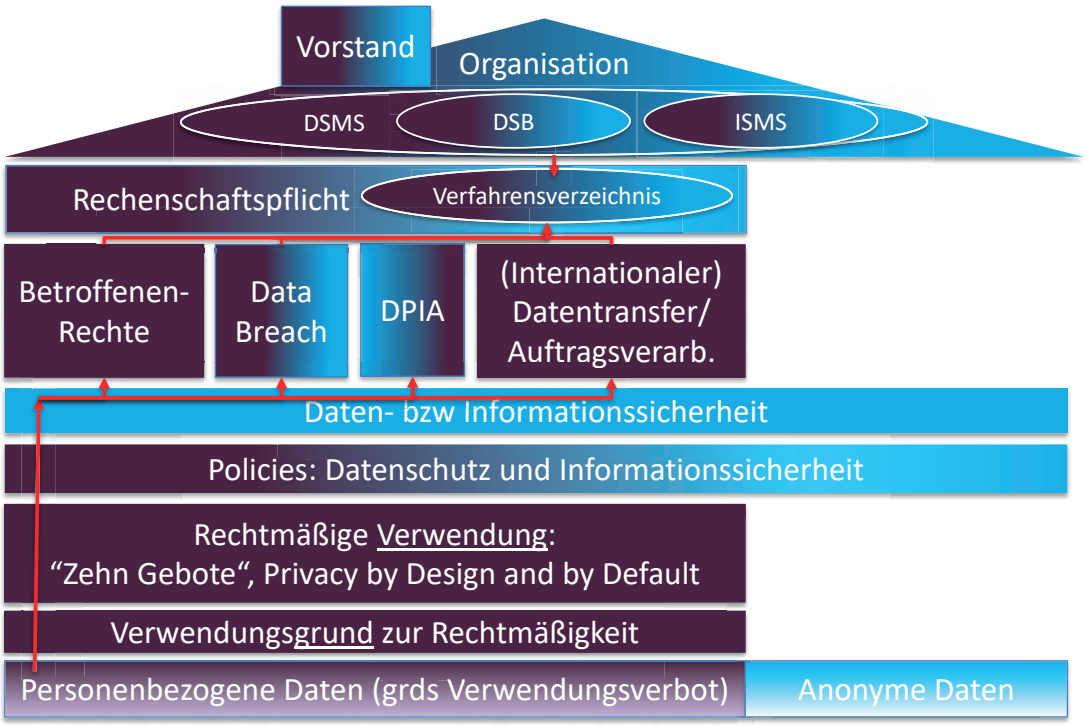
- → Verzeichnis der Verarbeitungstätigkeiten
- → Auftragsverarbeiter- und Gemeinsam Verantw-Verträge
- → Einwilligungs- und Widerrufsverwaltung
- → Datenschutz-Folgenabschätzung → uU Konsultation
- → Verletzung der Sicherheit → uU Meldepflicht

Verarbeitungstätigkeit = „Anwendungsfall"

Anwendungsfälle („Use-Cases“) werden durch

- den Zweck
- die Betroffenen
- die Datenkategorien
- die Empfängerkreise (und deren Sitz)

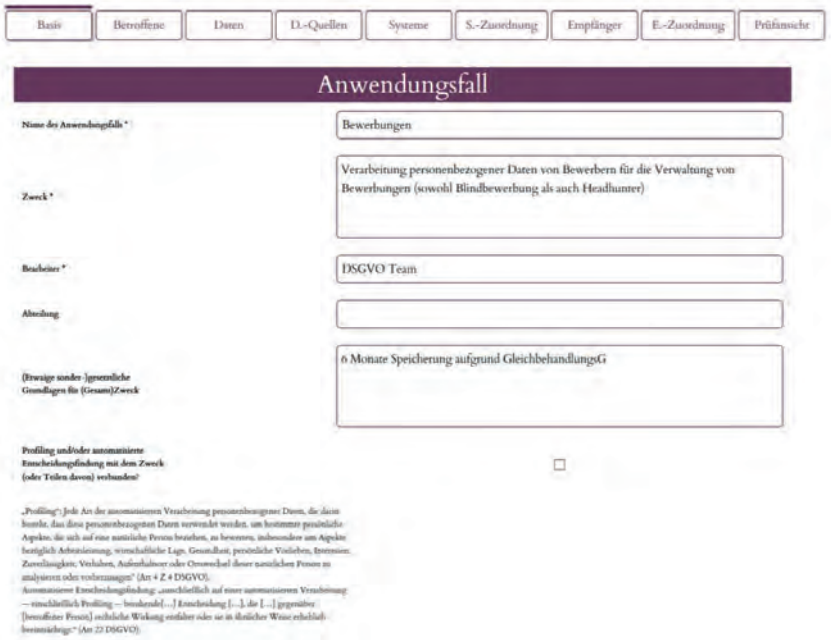
der Datenanwendung definiert.



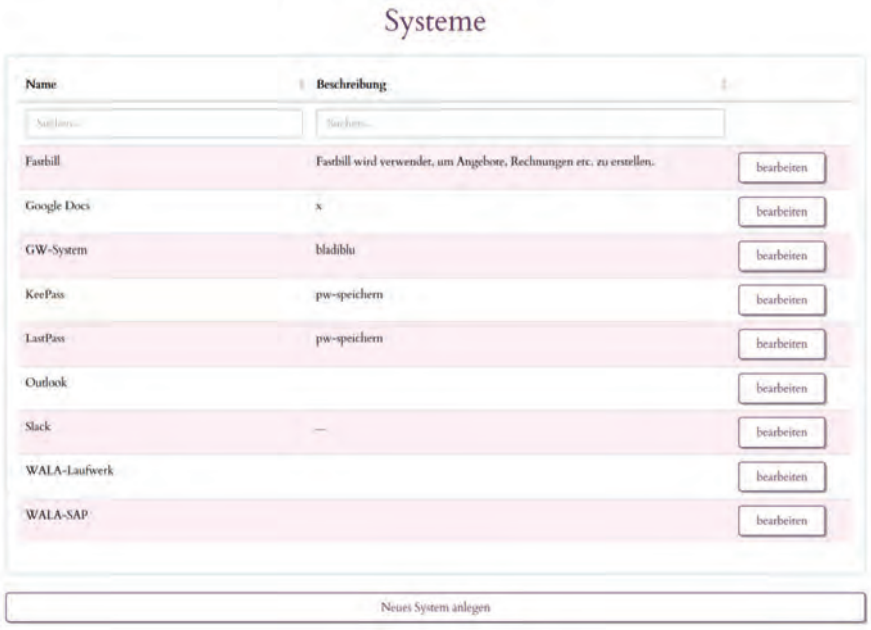
GEISTWERT DSGVO-Tool

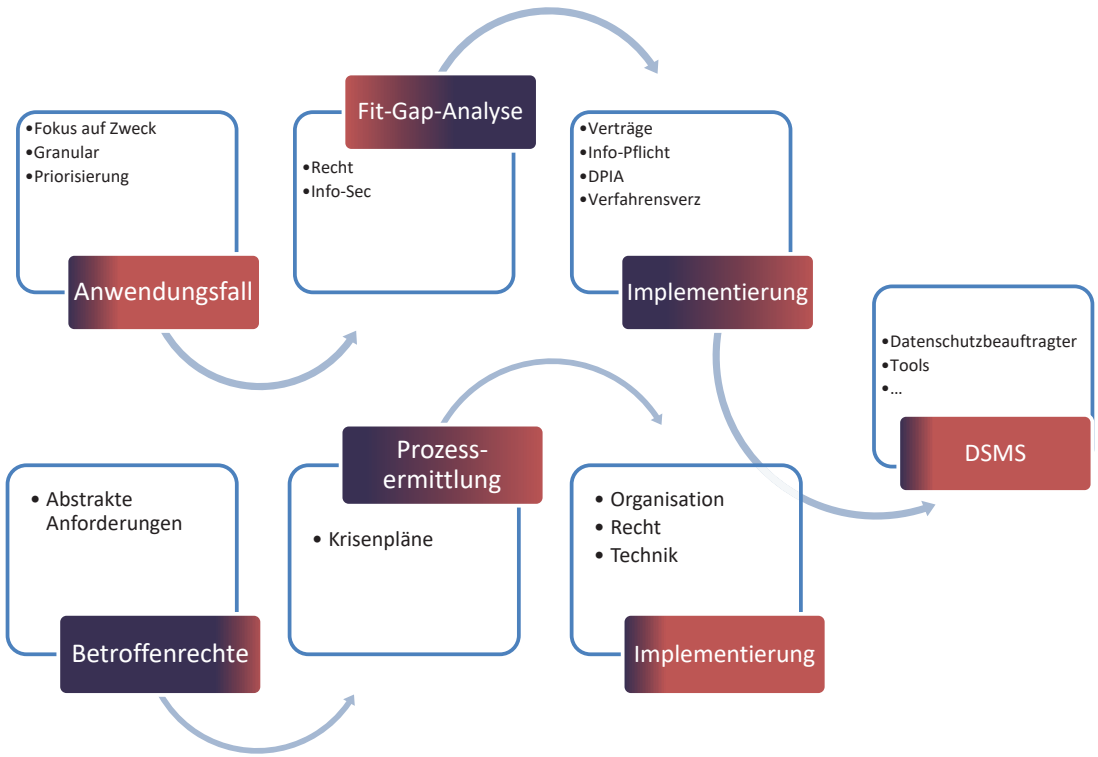
GEISTWERT DSGVO-Tool

Anwendungsfall: Bewerbungen

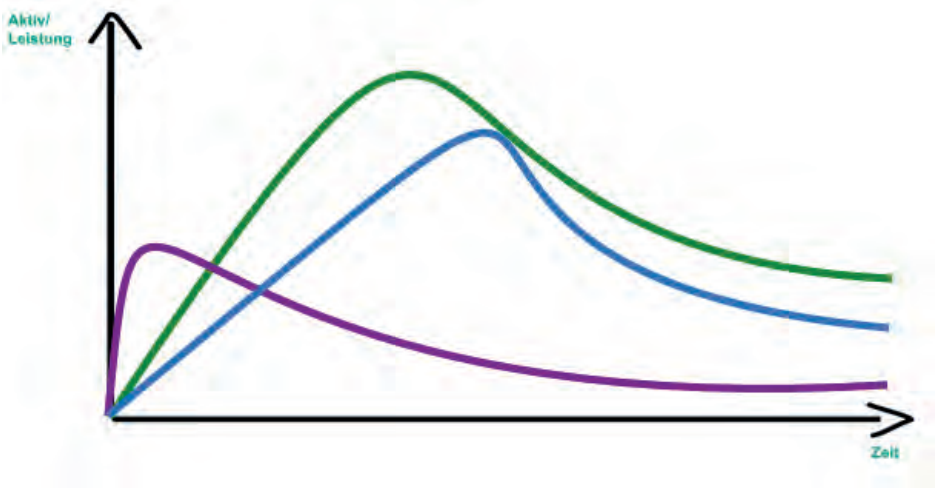


GEISTWERT DSGVO-Tool





DSGVO-“Aufwandswelle“



DSGVO-“Projektwelle“

Betroffenenrechte in die Prozesse der Organisation integrieren

Betroffenenrechte

Betroffene haben uU (!) das Recht auf…

- Information (aktiv und äußerst umfassend)
- Auskunft (inkl Kopie der Daten)
- Richtigstellung
- Löschung (komplexer Prüfungsprozess)
- Einschränkung (als „Nebenrecht“)
- Datenübertragbarkeit (Einwilligung oder Vertrag)
- Widerspruch (bei öffentl/ berecht Interesse, insb Offline(!)-Direktmarketing)
- Beschwerde bei der Aufsichtsbehörde

Betroffenenrechte

Umsetzung in der Praxis:

- Klare Prozesse definieren

- Tool-Support als logische Konsequenz

Informationssicherheit in die Prozesse der Organisation integrieren

Integrität und Vertraulichkeit

Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete TOMs.

"Privacy by Design“

Unter Berücksichtigung des

- Stands der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
- sowie der Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken

"Privacy by Design"

trifft der Verantwortliche

- sowohl zum Zeitpunkt der Festlegung der Mittel
- als auch zum Zeitpunkt der eigentlichen Verarbeitung

geeignete technische und organisatorische Maßnahmen („TOMs“)

"Privacy by Default"

Der Verantwortliche trifft (!)

- geeignete TOMs, die sicherstellen, dass
- durch Voreinstellung grundsätzlich nur erforderliche (!) personenbezogene Daten verarbeitet werden

Gelebter Datenschutz

Umsetzung in der Praxis:

- Klare Prozesse definieren

- Tool-Support als logische Konsequenz

Vom Informations-Sicherheits-Management-System zum Daten-Schutz-Management-System

Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete TOMs, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Maßnahmen

diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

Maßnahmen

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

DSGVO Artikel 32 – **Sicherheit der Verarbeitung**

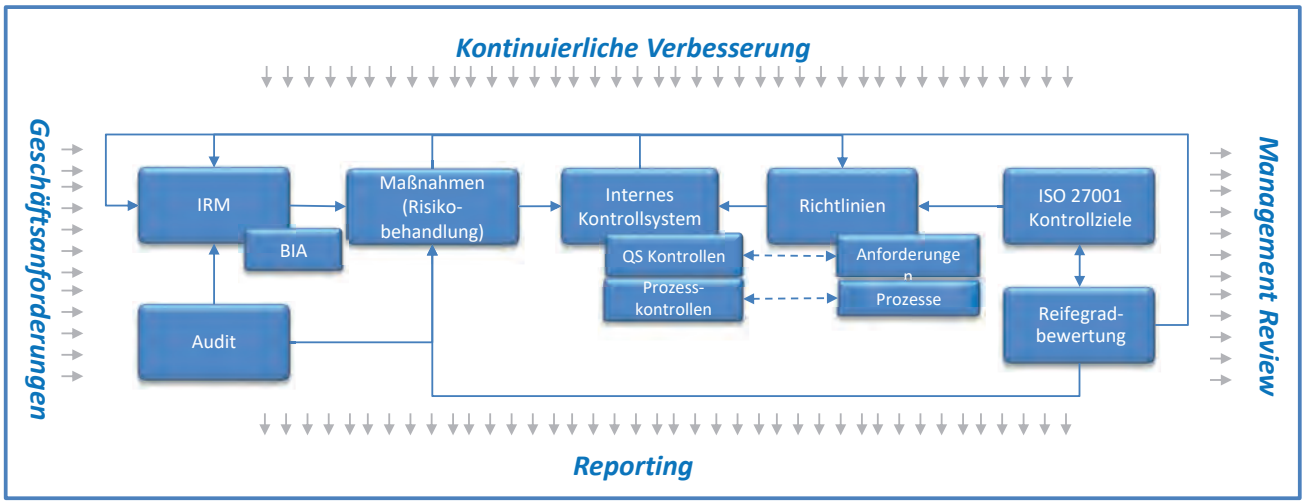
…**geeignete technische und organisatorische Maßnahmen**, um ein dem **Risiko angemessenes Schutzniveau** zu gewährleisten

Verfahren zur **regelmäßigen Überprüfung**, **Bewertung** und **Evaluierung** der **Wirksamkeit** der technischen und organisatorischen Maßnahmen

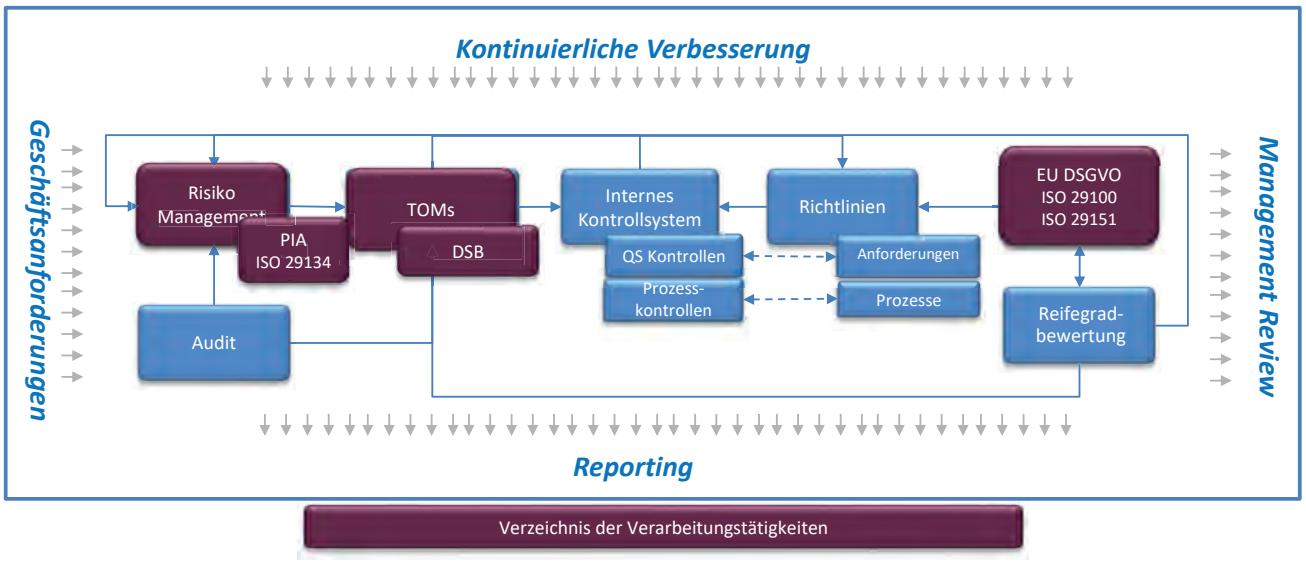
ISO 27001 zertifiziert ein Informationssicherheits-managementsystem (ISMS)

"… ist der Teil des gesamten Managementsystems, der **basierend auf einem Geschäftsrisikoansatz** die **Errichtung**, **Umsetzung**, **Betrieb**, **Überwachung**, **Überprüfung**, **Instandhaltung** und die **Verbesserung** der Informationssicherheit abdeckt."

ISMS Life Cycle

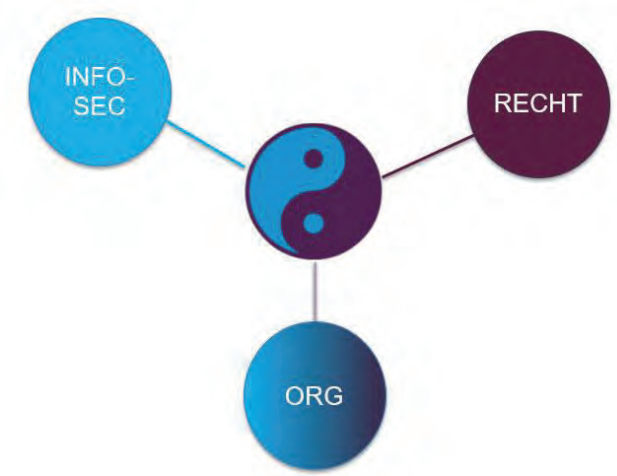


DSMS Life Cycle



Schlusswort

Wir müssen zusammenarbeiten



GEISTWERT

RECHTSANWÄLTE LAWYERS AVVOCATI

MMag.

JULIANE MESSNER

Partner

tel +43 1 585 03 03-20
fax +43 1 585 03 03-99

Linke Wienzeile 4
1060 Wien · Vienna · Austria

juliane.messner@geistwert.at
www.geistwert.at