Compliance im Griff
Bereit für die neue EU-DSGVO

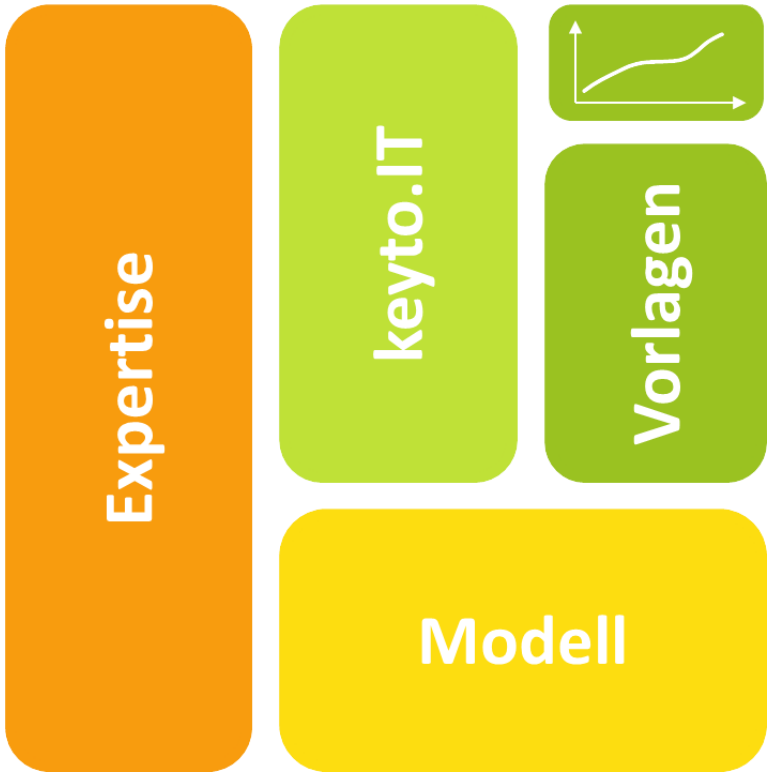
Dr. Andreas Knaus

LINJAL GmbH

- LINJAL GmbH liefert Lösungen und Beratung zur Steuerung von Service Providern:
  - Portfolio
  - Steuerungsprozesse
  - Performanceoptimierung
- Gegründet: 02.01.2014

  Standort: München
- Geschäftsführer:

  Dr. Andreas Knaus



LINJAL

Ganzheitliche Beratung, Analyse und Software
zur Steuerung von IT-Dienstleistungen

Preise und Kosten transparent gestalten

Prozesse, vom Vertrieb bis zur Delivery, optimieren

Technologie wertschöpfend nutzen

Portfolio bedarfs- und marktgerecht gestalten

für interne und externe IT Service Provider

Agenda

- Compliance – Die Regeln im Griff
- EU-DSGVO und BDSG (neu) – Was kommt auf die Unternehmen zu
- Steuerung – Nachhaltig gesichert

Compliance

Die Regeln im Griff

Compliance – Definition

Einhaltung von

- Gesetzlichen Bestimmungen
- Regulatorischer Standards
- Interne Vorgaben
  - Ethische Standards
  - Anforderungen

Beispiele

- Datenschutz & Datensicherheit
- Steuerliche Vorgaben
- Arbeitnehmerüberlassung
- Scheinselbständigkeit
- Verhaltenskodex (Code of Conduct)

Maßnahmen für die EU-DSGVO

(n = 329 Geschäftsführer/Vorstände Unternehmen über 20 Mio. Euro; Quelle: CARMAO)

EU-DSGVO und BDSG

Was kommt auf die Unternehmen zu

BDSG – EU-DSGVO

	Bundesdatenschutzgesetz	EU Datenschutz-Grundverordnung
Baujahr	1977	2016
Überarbeitungen	1990, 2001, 2003, 2006, 2009, 2017	2017
Gerichtsentscheidungen	über 700	1 (Datenschutzbehörde hat keine Ermächtigungsgrundlage vor Inkrafttreten der EU-DSGVO)
Umfang	ca. 26 Seiten	ca. 72 Seiten
Geltungsbereich	Deutschland	EU und weltweit
Bußgelder	„kann“ bis 300.000 € bzw. 2 Jahre Freiheitsstrafe	„muss“ bis 20.000.000 € bzw. 4% vom Konzern-Jahresumsatz
Schadensersatz	Nur für materielle Schäden	Für Schäden aller Art
Ziel	„nicht erwischen lassen“	Compliance erreichen und nachweisen

EU-Datenschutz-Grundverordnung: Entstehungsprozess

25.01.	06.06.	21.10	12.03	15.06	15.12	25.05	25.05
1.Entwurf durch die EU-Kommi-ssion	EU-Minister-rat tagt zur EU-DSGVO	Libe-Ausschuss nimmt Anträge an	2.Entwurf des EU-Parla-ments	3.Entwurf des EU-Minister-rats	Letztes Trilog-Treffen	Inkraft-treten	Anwen-dung

2012 | 2013 | 2014 | 2015 | 2016 | 2018

Übergang BSDG → EU-DSGVO

Geltungsreihenfolge

1. EU-DSGVO
2. BDSG

→ Bundesdatenschutzgesetz (BDSG, Mai 2017) im Kontext der EU-DSGVO auszulegen

Verordnung: Unmittelbar in allen Mitgliedsländern wirksam

Ziele und Grundsätze der DSGVO

Ziele

Schutz der Grundrechte
Grundfreiheiten natürlicher Personen
Freier Verkehr personenbezogener Daten
Recht auf Schutz vor personenbezogener Daten

Grundsätze

- Rechtmäßigkeit
- Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Inhalte der DSGVO

Kapitel	Inhalt	Artikel
I	Allgemeine Bestimmungen	1-4
II	Grundsätze	5-11
III	Rechte der betroffenen Person	12-23
IV	Verantwortlicher und Auftragsverarbeiter	24-43
V	Übermittlung personenbezogener Daten an Drittländer oder an internationale Orga.	44-50
VI	Vorschriften für besondere Verarbeitungssituationen	51-59
VII	Rechtsbehelfe, Haftung und Sanktionen	60-67
VIII	Unabhängigkeit der Aufsichtsbehörden	77-84
IX	Zusammenarbeit und Kohärenz	85-91
X	Delegierte Rechtsakte und Durchführungsrechtsakte	92-93
XI	Schlussbestimmungen	94-99

Einblick in die DSGVO

- Anwendungsbereich
  - Sachlich
  - Räumlich
- Besonderheiten
- Pflichten für Unternehmen
  - Auftragsdatenverarbeitung
  - Betrieblicher Datenschutzbeauftragter
  - Datensicherheit
    - Technisch-organisatorische Maßnahmen
  - Aufbau eines Datenschutzmanagementsystems
  - Bußgelder und Sanktionen

Anwendungsbereich

- Sachlich (Art. 2 ff. DSGVO)
  - Personenbezogene Daten
  - Automatisierte und nicht automatisierte Daten
- Räumlich (Art. 3 ff. DSGVO)
  - Niederlassung in der Union

Personenbezogene Daten

Keine personenbezogenen Daten → DSGVO nicht anzuwenden

Beispiele:

- Name
- Adresse
- Telefonnummer
- Autokennzeichen
- IP-Adresse

→ Aus Daten Personenbezug herstellbar

Automatisierte und nicht automatisierte Verarbeitung

- Elektronisch gespeicherte und verarbeitende Daten

Beispiele:

- Computer
- Smartphones
- Kameras
- Webcams
- Dashcams
- Scanner
- Kopierer

→ DSGVO anwendbar, wenn personenbezogene Daten betroffen sind

Niederlassung in der Union

DSGVO findet Anwendung auf die Verarbeitung personenbezogener Daten, wenn

- Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union
- Betroffene Personen sich in der Union befinden

Besonderheiten

- Anforderungen an eine Einwilligung
  - Gegenüber dem BDSG reduziert (Wegfall Schriftform)
- Begrenzung der verarbeiteten Daten
  - Grundsatz der Datenminimierung
  - Big Data-Massenverarbeitung
- Transparenz & Kontrolle
  - Recht auf Auskunft (Zweck, Empfänger, Verantwortliche der Datenverarbeitung, Dauer der Datenspeicherung)
  - Nach Art. 12 in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“
  - Recht auf Berichtigung falscher Daten
  - Recht auf „Vergessenwerden“
- Sanktionierung
  - Verpflichtende Sanktionierung

Pflichten für Unternehmen

Pflichten für Unternehmen (Art. 24 EU-DSGVO)

- Datenschutz mit Hilfe geeigneter technischer und organisatorischer Maßnahmen
- Berücksichtigung
  - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
  - Risiken für die persönlichen Rechte und Freiheiten
  - Eintrittswahrscheinlichkeit

Pflichten für Unternehmen

- Technischer Grundschutz
- Meldepflicht
- Datenschutz-Folgeabschätzung (Vorabkontrolle)

Technischer Grundschutz

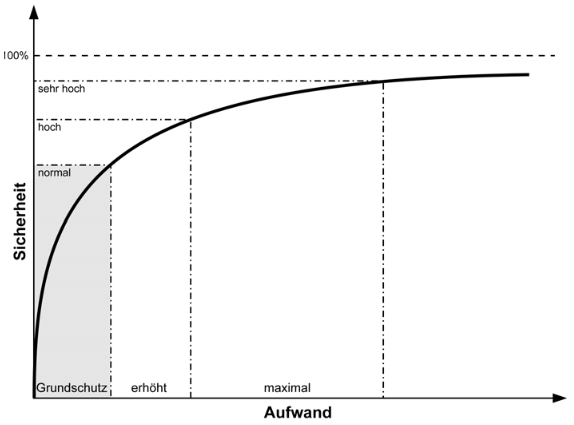
- Technischer Datenschutz
  - Technische und Organisatorische Maßnahmen
  - Grundsatz des Datenschutzes durch Technik (data protection by design)
  - Datenschutzfreundliche Voreinstellungen (data protection by default)
  - Verzeichnis von Verarbeitungstätigkeiten

Technischer Grundschutz – Angemessenheit

- Angemessenheit
  - In Bezug auf Risiko
  - Z. B. Risikoklassen BSI-Standard 100-2 „normal, „hoch“ und „sehr hoch“

Schutzbedarfskategorien	
"normal"	Die Schadensauswirkungen sind begrenzt und überschaubar.
"hoch"	Die Schadensauswirkungen können beträchtlich sein.
"sehr hoch"	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

  - Stand der Technik
    - Begriff nicht definiert



Technischer Grundschutz – Maßnahmen

- Beispiele:
  - Verarbeitung personenbezogener Daten minimieren
  - Personenbezogene Daten so schnell wie möglich pseudonymisieren
  - Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten
  - Betroffenen Person ermöglichen, die Datenverarbeitung zu überwachen
  - Sicherheitsfunktionen zu schaffen und zu verbessern

Technischer Grundsatz – Verzeichnis

- Namen und die Kontaktdaten
  - Verantwortlichen für die Verarbeitung
  - Vertreter (ggf.)
  - Datenschutzbeauftragter (ggf.)
- Zwecke der Verarbeitung
- Kategorie von
  - personenbezogenen Daten
  - betroffenen Personen
  - Empfängern der personenbezogenen Daten
- Übermittlungen von Daten
  - Drittland
  - internationale Organisation
- Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Meldepflicht

Verletzungen des Schutzes personenbezogener Daten sind Meldepflichtig

- Keine Meldepflicht
  - Risiko für Rechte und Freiheiten niedrig / unwahrscheinlich
- Frist
  - Unverzüglich
  - Möglichst innerhalb 72 Stunden nach bekannt werden der Verletzung
- Betroffener
  - Muss grundsätzlich informiert werden
  - Außer: Risiko niedrig
  - Inhalt der Information
    - Beschreibung der Art der Verletzung
    - Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen

Datenschutz-Folgeabschätzung

Unternehmen muss Datenschutz-Folgenabschätzung vornehmen (Art. 35 EU-DSGVO)

- Hohe Risikowahrscheinlichkeit
  - Neue Technologien
  - Beispiele
    - Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen aufgrund automatisierter Verarbeitung
    - Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten
    - Systematische weiträumige Überwachung öffentlich zugänglicher Bereiche
- Aufsichtsbehörde
  - ist zu informieren
  - Führt Positiv-/Negativ-Listen zu Technologien

Verantwortlicher

Definition Verantwortlicher (Art. 24 EU-DSGVO)

- natürliche oder juristische Person, Behörde, Einrichtung
- Entscheidet über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten (Art. 4 Nr. 7 EU-DSGVO)

Auftragsverarbeitung

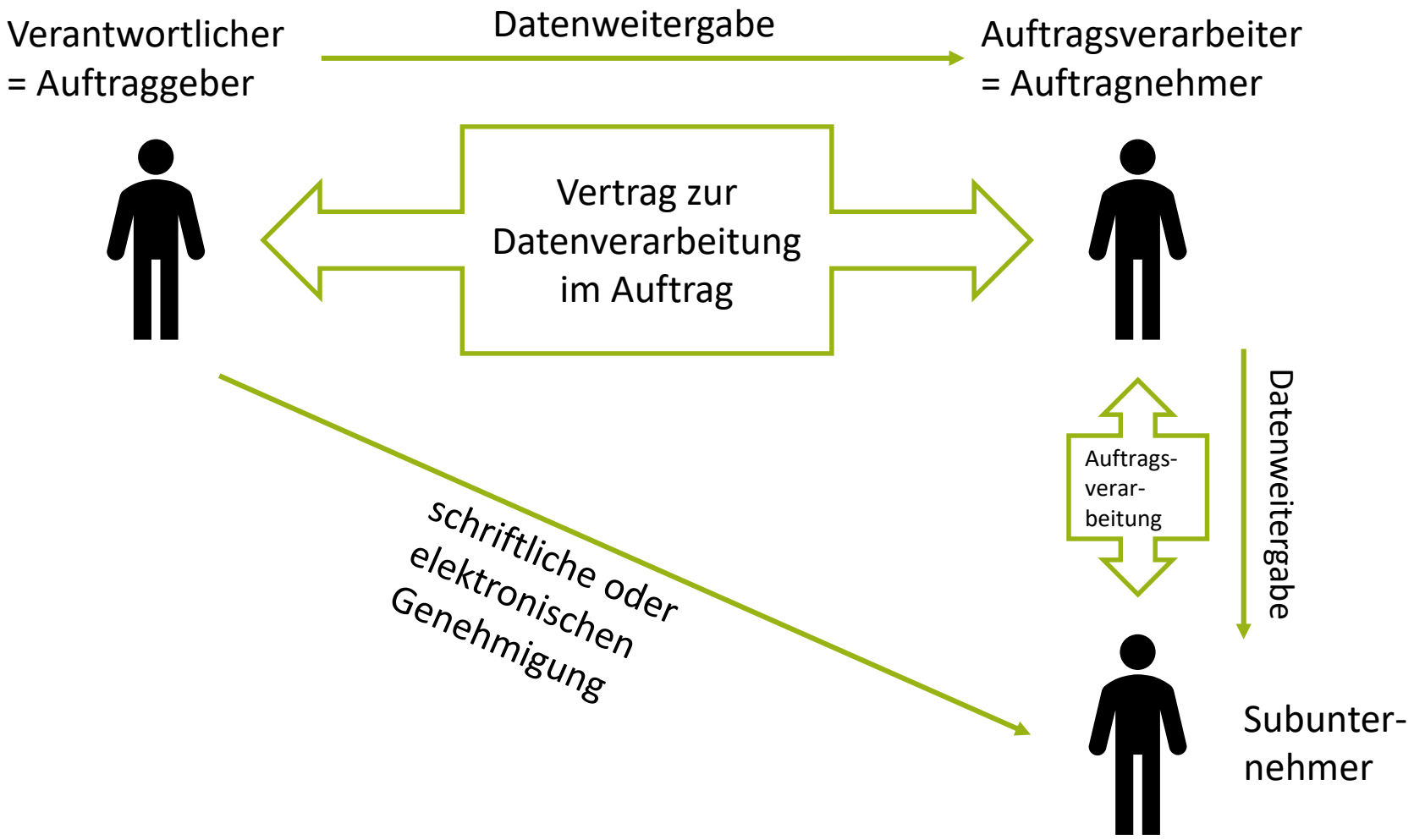
- Verarbeitung personenbezogener Daten durch Auftragnehmer:
  - Erhebung
  - Verarbeitung
  - Nutzung
- Grundlage
  - Weisung der verantwortlichen Stelle (Auftraggeber)
  - schriftlicher Vertrag

BDSG	Regelungsbereich	DSGVO	Veränderungen
§11	Auftragsdatenverarbeitung	Art. 28 Art. 29	• Sprachliche Änderung • Elektronisches Format zulässig • Datenverarbeitung im Auftrag auch außerhalb der EU • Gemeinsame Haftung der für die Verarbeitung Verantwortliche (AG) und der Auftragsverarbeiter (AN) gegenüber dem Betroffenen

Mitverantwortung und Pflichten

- Verantwortung kann nicht an Auftragsverarbeiter überwälzt werden
- Datenschutzrechtliche Pflichten des Auftragsverarbeiters (unter anderem)
  - Bestellung eines „Repräsentanten“ (Art. 27 Abs. 1 DSGVO)
  - Führung von Verfahrensverzeichnissen (Art. 30 Abs. 2 DSGVO)
  - Zusammenarbeit mit der Datenschutzaufsicht (Art. 31 DSGVO)
  - Technische und organisatorische Maßnahmen der Datensicherheit (Art. 32 Abs. 1 DSGVO)
  - Bestellung eines betrieblichen Datenschutzbeauftragten (Art. 37 Abs. 1 DSGVO)
  - Beschränkungen für den Datentransfer in Drittländer (Art. 44 DSGVO)

Subunternehmer



Inhalt eines ADV-Vertrages

Nach Art. 28 Abs. 3 EU-DSGVO:

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten & Kategorien von betroffenen Personen
- Umfang der Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit
- Sicherstellung von technischen & organisatorischen Maßnahmen
- Hinzuziehung von Subunternehmern
- Unterstützung des für die Verarbeitung Verantwortlichen bei Anfragen und Ansprüchen Betroffener
- Unterstützung des für die Verarbeitung Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsdatenverarbeitung
- Kontrollrechte des für die Verarbeitung Verantwortlichen und Duldungspflichten des Auftragsverarbeiters
- Pflicht des Auftragsverarbeiters, den Verantwortlichen zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt

Betrieblicher Datenschutzbeauftragter

- Erstmals eine europaweit geltende Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten (Art. 35 ff. DSGVO)
- Bestellungspflicht für
  - Min. 10 Personen beschäftigen sich mit el. Datenverarbeitung
    (20 Personen bei nicht el. Verarbeitung)
  - Schützenswerte Daten werden verarbeitet
    - z.B. Rasse, ethnische Herkunft, politische Meinung, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben
  - Unternehmen deren Tätigkeit einer besonderen datenschutzrechtlicher Kontrolle bedarf
    - z.B.: Auskunfteien, Versicherungsunternehmen, Gesundheitseinrichtungen, Beratungsstellen

Aufbau eines Datenschutz-managementsystems

Pflicht zur Einführung eines Datenschutzmanagement

Inhalt:

- Datenschutzrichtlinie
- Datenschutzorganisation und Verantwortlichkeiten
- Einbindung des Datenschutzbeauftragten
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutz-Folgenabschätzung
- Vertragsmanagement
- Verpflichtung auf das Datengeheimnis
- Datenschutz-Schulung
- Prozess für die Wahrnehmung von Betroffenenrechten
- Prozess für die Meldung von Datenschutzverstößen
- Nachweis der Datensicherheit

Bußgelder und Sanktionen

Bußgelder werden wahrscheinlicher

- Bußgeldvorschrift nach dem BDSG
  - Bußgeld (Bis zu 300.000 Euro pro Einzelfall, § 43 BDSG)
  - Strafrecht (Freiheitsstrafe bis zu zwei Jahren, § 44 BDSG)

- Bußgeldvorschrift nach der EU-DSGVO
  - Bis zu 20 Millionen Euro
  - Bzw. bis zu 4% des Konzernumsatzes (Weltweit)

Sanktionen der Aufsichtsbehörden

- Verwarnungen
- Widerruf einer Zertifizierung
- Untersuchungsbefugnisse

Bemessungskriterien des Bußgeldkatalogs nach Art. 83

- Art, Schwere und Dauer des Verstoßes
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
- Die getroffenen Maßnahmen zur Minderung des entstandenen Schadens
- Grad der Verantwortung unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen
- Etwaige einschlägige frühere Verstöße
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern
- Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind
- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere Selbstanzeige
- Einhaltung früher angeordneter Maßnahmen
- Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42
- Jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangten finanzielle Vorteile oder vermiedene Verluste

Steuerung

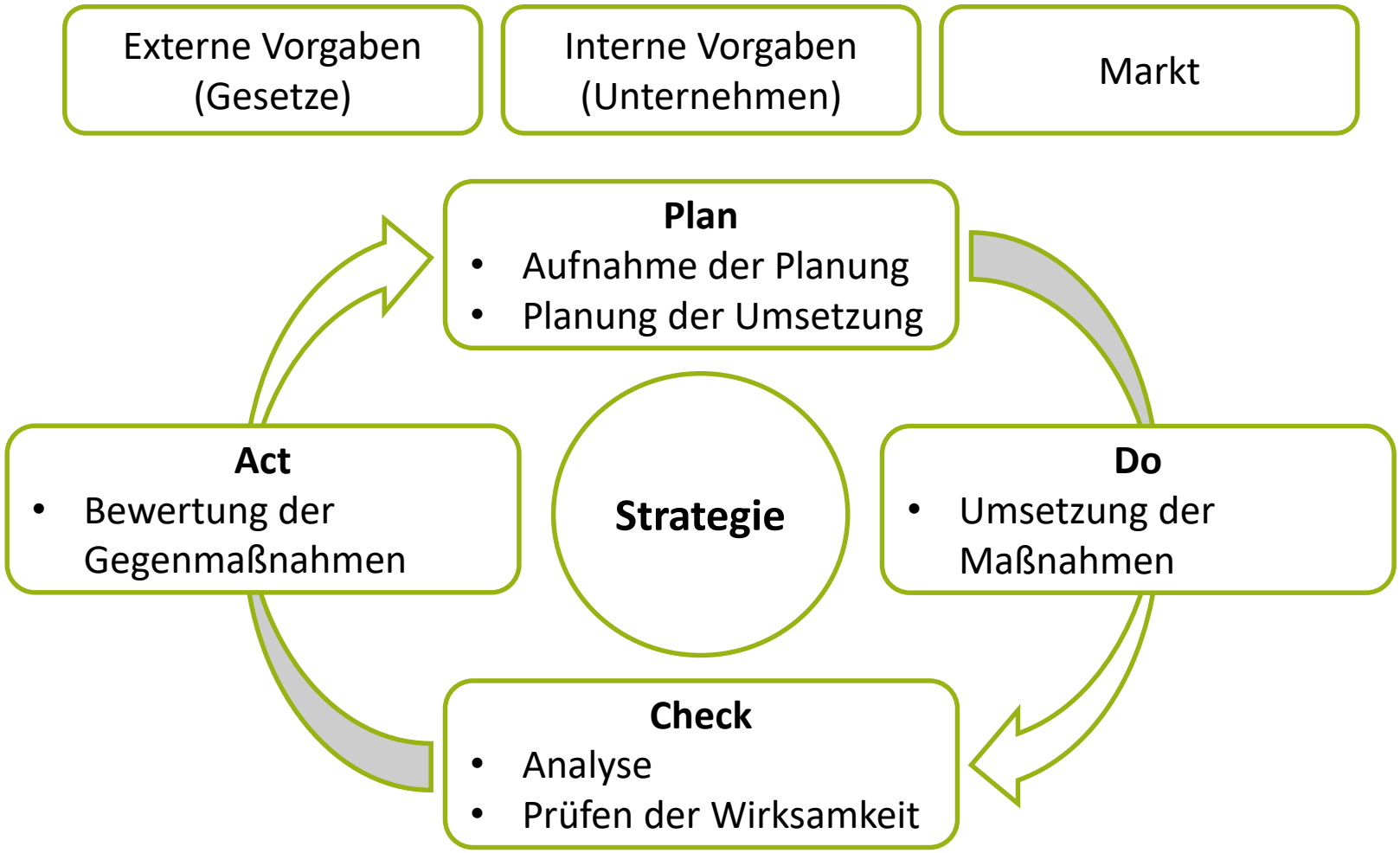
Nachhaltig gesichert

Ziele

- Hauptziel
  - Umsetzung der EU-DSGVO
  - Minimierung des Aufwands

- Vorgehen
  - Einbindung in Compliance-System des Unternehmens

Compliance System



Erste Schritte – kurzfristige Compliance

Wie weit sind Sie auf DSGVO vorbereitet?

Befindet sich die Verarbeitung bzw. die Person, deren Daten verarbeitet werden in der Union?

- Ja
- Nein

Welche Personenbezogenen Daten werden von Ihnen erfasst?

- Name
- Adresse
- Telefonnummer
- Geschlecht
- Religion
- Krankheiten
- IP-Adresse

Wo werden personenbezogene Daten in Ihrer Organisation gespeichert?

- Alle lokal
- Vorrangig lokal, teilweise in der Cloud
- Vorrangig in der Cloud, teilweise in lokal
- Vollständig in der Cloud

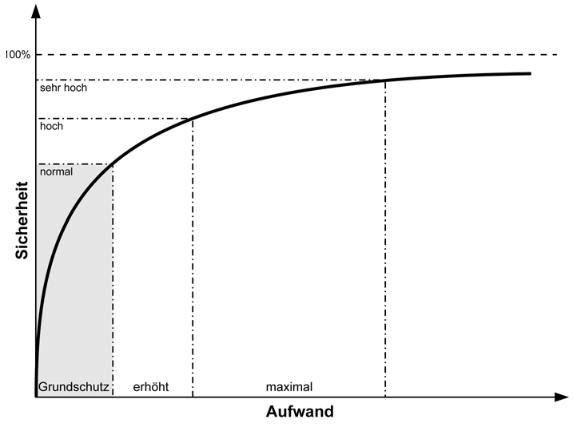
Welche Abteilung in Ihrer Organisation leitet die DSGVO-Einhaltung (oder wird diese leiten)?

- Governance
- Rechtsabteilung
- Finanzen
- IT
- Andere

Schutzklassenkonzepte zur DSGVO

Beispiel für die Ermittlung eines ausgewogenes Verhältnis aus Schutzbedarf und Aufwand

- Bestimmung des Risikos
- Abstufung des Schutzbedarfs



Daten – Schützen!

Beschreibung
Bei der Verarbeitung personenbezogener Daten sind angemessene „technisch-organisatorischen Maßnahmen“ notwendig um dem benötigten Schutzniveau Rechnung zu tragen.

Datenschutz-Grundverordnung
Nach Art. 25 DSGVO sind folgende Punkte zu berücksichtigen, um die Datenschutzgrundsätze einzuhalten:

- der Stand der Technik,
- die Implementierungskosten,
- Art, Umfang, Umstände und Zwecke der Verarbeitung
- und die Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen.

Kategorien personenbezogener Daten

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen oder
- die Gewerkschaftszugehörigkeit hervorgehen,
- genetische Daten,
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten und
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Bestimmung des Risikos

Risiken

Risiken identifizieren

- Art, Ursachen und Auswirkungen

Risiken analysieren

- Eintrittswahrscheinlichkeiten und Auswirkungen

Formel

Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe

Inhalt

Im Gegensatz zum klassischen Risikomanagement werden nicht die Risiken für das Unternehmen betrachtet, sondern diejenigen der Betroffenen Personen, deren Daten verarbeitet werden.

Die Verwendung von Risikoklassen vereinfachen die Identifikation und Analyse der einzelnen Risiken.

Abstufung des Schutzbedarfs

Normaler Schutzbedarf
Personenbezogene Daten, deren Verarbeitung keine besondere Beeinträchtigung des informationellen Selbstbestimmungsrechts erwarten lassen

Beispiele: Anschrift, Geburtsjahr, öffentliche Register, Telefonverzeichnisse.

Hoher Schutzbedarf
Gesellschaftliche Stellung oder wirtschaftliche Verhältnisse des Betroffenen können beeinträchtigt werden

Beispiele: Daten über Mietverhältnisse, Telefonverbindungsdaten, Kontenstände, Zeugnisse, rassische oder ethnische Herkunft, religiöse oder weltanschauliche Überzeugungen, Schülerdaten.

Sehr Hoher Schutzbedarf
Gesellschaftliche Stellung oder wirtschaftliche Verhältnisse des Betroffenen können **erheblich** beeinträchtigt werden

Beispiele: besonders sensible Krankendaten, besonders sensible Sozialdaten, Steuerdaten, strafbare Handlungen, Verwaltungsdaten entsprechend der „VS-Vertraulich“.

Kontakt

Dr. Andreas Knaus

Landwehrstr. 61

80336 München

aknaus@linjal.de

01523 1860455