DEGA Unternehmensberatung GmbH

Mandanteninfo DSGVO

EU-Datenschutzgrundverordnung

Was ist eigentlich ...

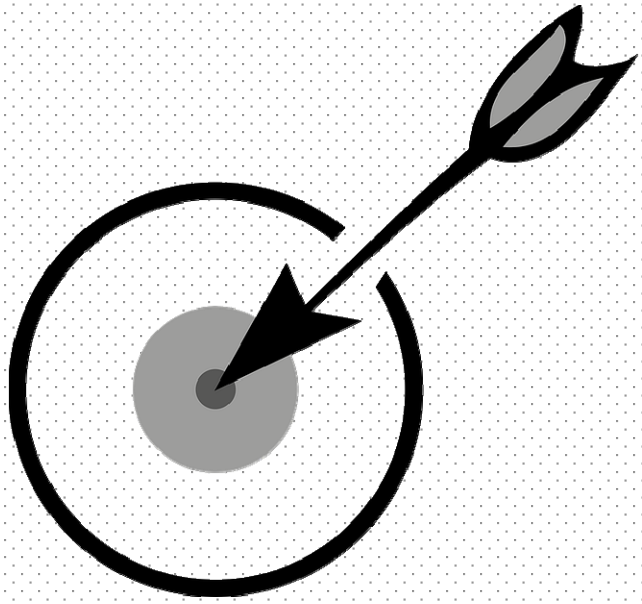
... Datenschutz?

Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird. Er beinhaltet technische und organisatorische Maßnahmen gegen den Missbrauch von Daten durch Organisationen.

Geschäftsführer, Vorstände und Inhaber von Unternehmen sind im Rahmen ihrer Sorgfaltspflichten angehalten, Missbrauch von den ihnen anvertrauten Daten zu verhindern.

Ziele der Datenschutzgrundverordnung - DSGVO

- „Schutz **natürlicher Personen** bei der Verarbeitung pbDaten und zum **freien Verkehr** solcher Daten.“ (Art.1 Abs.1)
  - „…schützt die **Grundrechte und Grundfreiheiten** natürlicher Personen und insbesondere deren *Recht auf Schutz personenbezogener Daten*“ (Art.1 Abs.2)
  - …ohne den **freien Verkehr** pbDaten in der Union einzuschränken. (vgl. Art.1 Abs.3)



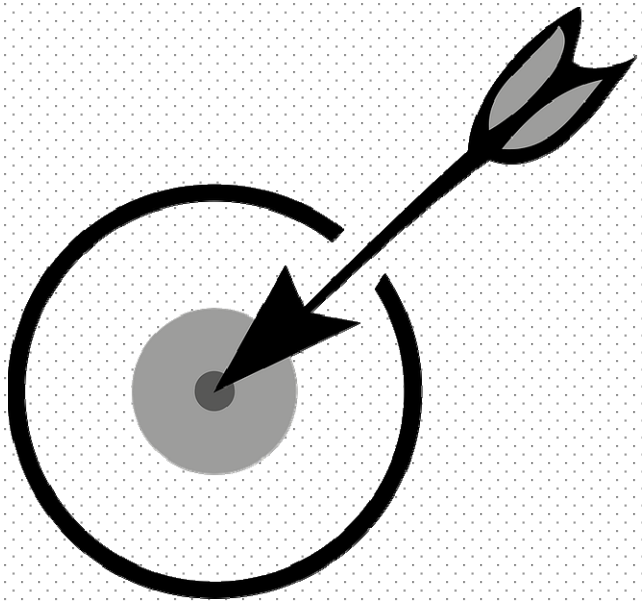
Prinzipien der Datenverarbeitung – Art. 5 DSGVO

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
Speicherbe-grenzung	• Speicherung mit Personenbezug höchstens so lange, wie es für die Verarbeitungszwecke erforderlich ist;
Integrität und Vertraulichkeit	• geeignete TOM zum angemessenen Schutz der Daten insbes. vor unbefugter oder unrechtmäßiger Verarbeitung, zufälligem Verlust, zufälliger Zerstörung oder Schädigung

Rechenschafts-pflicht (Account-ability):

- Verantwortung und
- Nachweispflicht

für die Einhaltung der Prinzipien



Die DSGVO kurz erklärt

- Die EU-DSGVO ist ein **europaweit einheitliches, unmittelbar geltendes Regelwerk** zum Datenschutz.
- Sie löst das deutsche **Bundesdatenschutzgesetz** (BDSG) am **25.05.2018** ab und gilt für alle Unternehmen und Behörden.
- **Zielsetzung** ist die Stärkung der Rechte von Betroffenen sowie ein europaweit einheitliches Datenschutzrecht und die Förderung des freien Datenverkehrs.
- Dort, wo die EU-DSGVO nicht greift oder es Öffnungsklauseln gibt, wird es weiterhin eine nationale Datenschutzgesetzgebung geben. Z. B. in einem neuen Bundesdatenschutzgesetz (**BDSG neu**) oder den Landesdatenschutzgesetzen (**LDSG**).

Die wesentlichen Umsetzungserfordernisse DSGVO

Grundsätzlich gilt: Wer unter dem alten BDSG gut aufgestellt war, wird es auch nach neuem Recht sein.

Trotzdem gibt es Handlungsbedarf!

- Erfüllung der Nachweispflicht
- Überarbeitung der Dokumentationen
- Einführung neuer Prozesse
- Bewertung von Schutzmaßnahmen
- Überarbeitung von Vorlagen

- Einhaltung der Rechte Betroffener

Vorgehen zur Umsetzung der DSGVO

1. Benennung eines fachkundigen Datenschutzbeauftragten
2. Bestandsaufnahme durchführen
3. Verzeichnis der Verarbeitungstätigkeiten erstellen
4. Festlegung des Dokumentationsumfangs zur Erfüllung der Rechenschaftspflichten
5. Rechtsgrundlagen der Verarbeitung überprüfen
6. Datenschutz-Management-System aufbauen
7. Umsetzung der Informationspflichten
8. Auftragsverarbeitung überprüfen
9. Überprüfung der technisch-organisatorischen Maßnahmen und PDCA-Zyklus etablieren
10. Mitarbeiter nach dem neuen Recht und seiner Umsetzung schulen

1. Benennung eines fachkundigen Datenschutzbeauftragten

Unternehmen müssen einen Datenschutzbeauftragten benennen, wenn …

… sie mindestens 10 Personen beschäftigen, die automatisiert Daten verarbeiten.

… ihre Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten besteht.

… sie Datenschutz-Folgenabschätzungen vornehmen.

Seine Kontaktdaten sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen!

1. Benennung eines fachkundigen Datenschutzbeauftragten

Der Datenschutzbeauftragte muss…

… fachkundig sein.

- Fachwissen im Datenschutzrecht
- Fachwissen in der Datenschutzpraxis
- Grundlage ist die berufliche Qualifikation

… zuverlässig sein.

- Die Wahrnehmung anderer Pflichten darf nicht zu einem Interessenkonflikt führen.

… in der Lage sein, seine Aufgaben zu erfüllen.

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten
- Überwachung der Einhaltung des Gesetzes, der Strategien zum Datenschutz, der Zuweisung von Zuständigkeiten und der Schulungen
- Beratung bei der Datenschutz-Folgenabschätzung
- Zusammenarbeit mit der Aufsichtsbehörde
- Ansprechpartner der Aufsichtsbehörde

Die Ressourcen hierfür muss das Unternehmen bereitstellen!

1. DSB – Evolution der Aufgabenstellung

Sicherstellungsauftrag

(§ 29 Abs. 1 BDSG 1977 / § 37 Abs. 1 BDSG 1990)

Hinwirkungsauftrag

(§ 4g Abs. 1 BDSG 2001)

Überwachungsauftrag
(Unterrichtung & Beratung)

(Art 39 Abs. 1 DS-GVO 2016)

2. Bestandsaufnahme durchführen

- Zunächst sollte ein Überblick über die vorhandene Datenschutzorganisation und die verarbeiteten Daten geschaffen werden:
  - Welche Daten werden verarbeitet? Wer sind die Betroffenen?
  - Im Rahmen welcher Prozesse bzw. Verarbeitungen?
  - Mit welchen Systemen?
  - Auf Basis welcher Rechtsgrundlage?
  - Welche Dokumente und Prozesse sind bereits vorhanden?
  - Welche Schutzmaßnahmen sind umgesetzt?
  - Werden Auftragsverarbeiter eingesetzt? Wohin werden Daten übermittelt?
  - etc.
- Die Bestandsaufnahme bildet die Basis für alle weiteren Schritte, insbesondere zum Aufbau der notwendigen Dokumentation.
- Alle Fachbereiche müssen hierzu eingebunden werden.
- Die Bestandsaufnahme sollte dokumentiert werden. Am Ende sollte ein Maßnahmenplan erstellt werden.

3. Verzeichnis der Verarbeitungstätigkeiten erstellen

- Gemäß Art. 30 Abs. 1 DS-GVO ist vom Verantwortlichen ein Verzeichnis aller Verarbeitungstätigkeiten mit definierten Inhalten zu führen.
- Die Ausnahme in Absatz 6 (250er-Regel) greift nur bei risikoloser Verarbeitung. Diese wird in der Regel zu verneinen sein. Ferner entgegengesetzte Regel im BDSG n.F.
- Auftragsverarbeiter führen neben einem Verzeichnis für die eigenen Verarbeitungen auch eines für Auftragsverarbeitungen (Art. 30 Abs. 2 DS-GVO).
- Um das Verzeichnis zu erstellen, werden die Fachabteilungen benötigt.
- Es ist schriftlich oder elektronisch zu führen und der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

  → Aufgrund des Umfangs ist eine „bedarfsorientierte“ Erstellung fast unmöglich!

3. Verzeichnis der Verarbeitungstätigkeiten erstellen

Verantwortlicher
ggf. Vertreter
ggf. Datenschutzbeauftragter

Verarbeitung 1	Verarbeitung 2	Verarbeitung n
a. ggfs. weitere, gemeinsame Verantwortliche b. Zweckbestimmung c. Betroffenengruppe und Daten-kategorien d. Empfänger e. Regelfristen Löschung f. geplante Über-mittlung in Dritt-staaten	a. ggfs. weitere, gemeinsame Verantwortliche b. Zweckbestimmung c. Betroffenengruppe und Daten-kategorien d. Empfänger e. Regelfristen Löschung f. geplante Über-mittlung in Dritt-staaten	a. ggfs. weitere, gemeinsame Verantwortliche b. Zweckbestimmung c. Betroffenengruppe und Daten-kategorien d. Empfänger e. Regelfristen Löschung f. geplante Über-mittlung in Dritt-staaten

übergreifende TOMs / Sicherheitskonzept

zusätzliche/ abweichende TOM*	zusätzliche/ abweichende TOM*	zusätzliche/ abweichende TOM*

Um die weiteren Aufgaben zu erleichtern, sollten zusätzliche Angaben erfasst werden:

- Rechtsgrundlagen
- Anwendungen
- Berechtigungen
- Ergebnisse der Risikoanalyse/ DSFA
- ggf. wofür welche Daten benötigt werden (Nachweis der Datenminimierung)
- Informationen zur Umsetzung der Betroffenenrechte

Bitkom, Leitfaden Verarbeitungsverzeichnis, 2017

* technisch-organisatorische Maßnahmen

3. Verzeichnis der Verarbeitungstätigkeiten erstellen

- **Beispiele für Verarbeitungstätigkeiten:**
  - Verarbeitungen für Kunden oder im Zusammenhang mit Lieferungen/Leistungen
    - Beratung
    - Angebotserstellung
    - Verkauf/Vertrieb
    - Bestellannahme
    - Reklamationen
  - Anbahnung von Kundenbeziehungen
  - Beendigung von Kundenbeziehungen
  - Abrechnung von Dienstleistungen/Lieferungen
  - Stammdatenverwaltung
  - Werbung/Marketing
  - Einkauf
  - eigene Buchführung
  - Controlling
  - Verwaltung und Abrechnung eigener Mitarbeiter
  - Zeiterfassung
  - Anbahnung von Beschäftigungsverhältnissen
  - Videoüberwachung
  - Archivierung
  - Passwortverwaltung (z. B. KeyPass)
  - Internetauftritt
  - Benutzerverwaltung in der IT
  - etc.

4. Festlegung des Dokumentationsumfangs zur Erfüllung der Rechenschaftspflichten

Rechenschaftspflicht
Die Einhaltung der Verarbeitungsgrundsätze muss jederzeit nachgewiesen werden können.
(Art. 5 Abs. 2 DS-GVO)

Dokumentation

Sicherheit

- Unterschrift des Betroffenen

Effizienz

- Prozess
- Arbeitsanweisung
- Aktennotizen

5. Rechtsgrundlagen der Verarbeitung prüfen

Zweckbindung: festgelegte, eindeutige und legitime Zwecke (Art. 5 Abs. 1 lit. b) DS-GVO)

Einwilligung
Art. 6 Abs. 1 lit. a)

Vertrag
Art. 6 Abs. 1 lit. b)

Rechtliche Verpflichtung
Art. 6 Abs. 1 lit. c)

Berechtigte Interessen
Art. 6 Abs. 1 lit. f)

Beispiele:

- Werbung

- Arbeitsvertrag
- Dienstleistungs-vertrag
- auch vorvertragliche Maßnahmen

- Aufbewahrungs-pflichten

- zur Abwehr von Haftungsansprüchen

Rechenschaftspflicht
Rechtmäßigkeit und Zweckbindung müssen jederzeit nachgewiesen werden können.
(Art. 5 Abs. 2 DS-GVO)

6. DSMS -Datenschutz-Management-System aufbauen

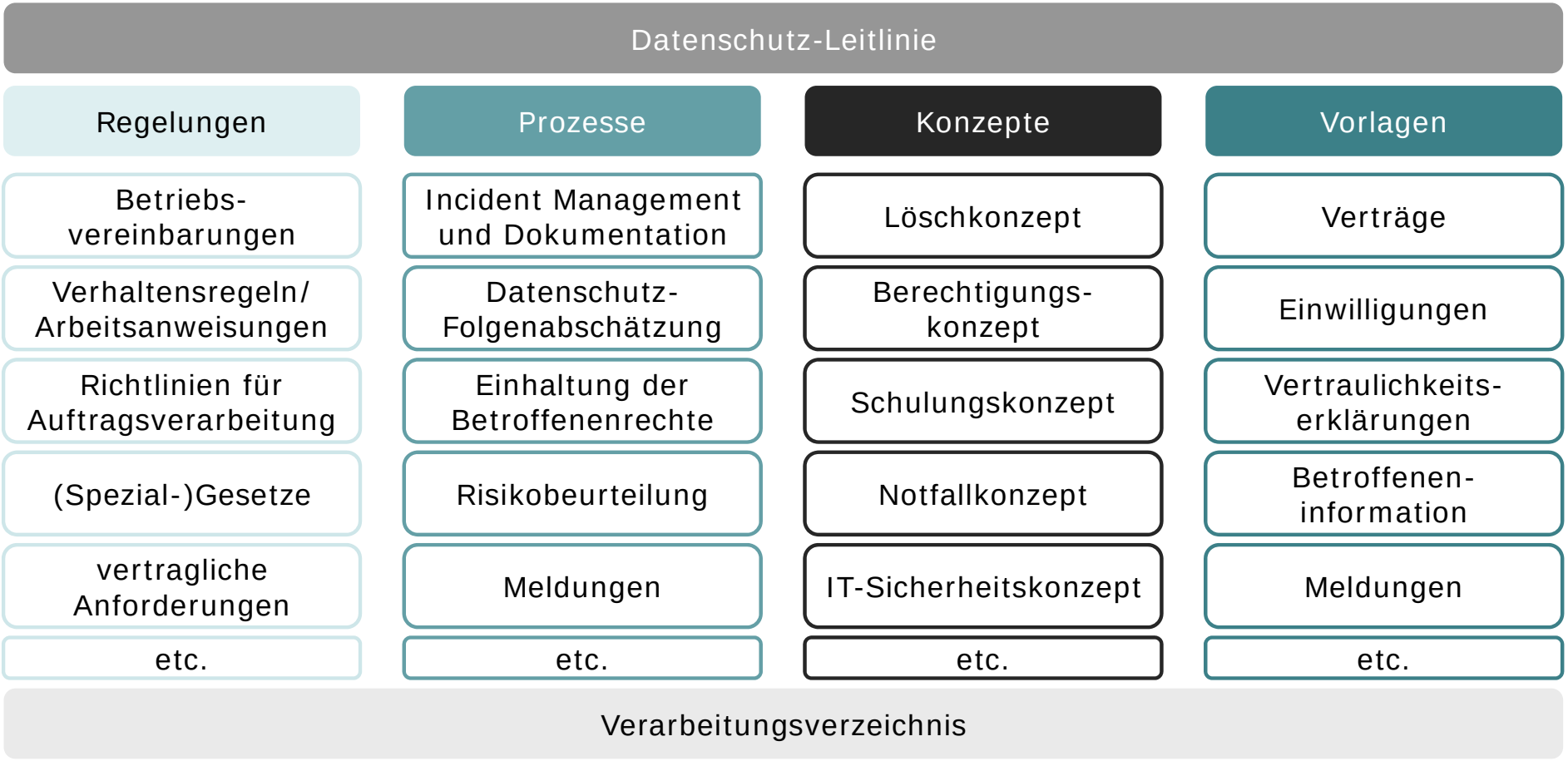
Definition & Aufgaben

Das Datenschutz-Management-System (DSMS) stellt die Gesamtheit aller dokumentierten und implementierten Regelungen, Prozesse und Maßnahmen dar, mit denen der datenschutzkonforme Umgang mit personenbezogenen Daten im Unternehmen systematisch gesteuert und kontrolliert wird.

Aufgaben

- Operative Auswirkungen des DS-Risiko-Managements umsetzen
- Festlegung sämtlicher Maßnahmen im DS
- Dokumentation und Kommunikation nach Innen und Außen
- Bei Einbezug des Datenschutzbeauftragten
- Langfristiger kontinuierlicher Verbesserungsprozess (KVP)

6. DSMS Bausteine



6. DSMS – Neue Datenschutz-Prozesse

Senden

Incident Management
Artt. 33, 34 DS-GVO

- Kenntnisnahme von Datenpannen
- Meldewege etablieren
- Verantwortung für die Beurteilung von Datenpannen festlegen
- Dokumentation von Datenpannen sicherstellen
- Meldung an die Aufsichts-behörde (72 Stunden) bei Risiko
- Benachrichtigung Betroffener (unverzüglich) bei hohem Risiko

Einhaltung der Betroffenenrechte
Artt. 15–22 DS-GVO

- Auskunft (inkl. Kopie)
- Berichtigung
- Löschung, Sperrung
- Datenübertragbarkeit
- Widerspruch
- Profiling
- innerhalb von einem Monat (weitere zwei bei Begründung)
- Identitätsprüfung
- keine Beeinträchtigung der Rechte und Freiheiten anderer Personen oder Verletzung von Verschwiegenheitspflichten

Datenschutz-Folgenabschätzung
Artt. 35, 36 DS-GVO

- bei besonders risikoreichen Verarbeitungen insb. mittels neuer Technologien
- Black- und Whitelist der Aufsichtsbehörde
- bei Videoüberwachung und umfangreicher Verarbeitung besonderer Kategorien personenbezogener Daten
- Einbezug des Datenschutzbeauftragten
- Beurteilung aus Sicht der betroffenen Personen

7. Umsetzung der Informationspflichten

Der Betroffene ist vom Verantwortlichen über die Datenverarbeitung und seine Rechte zu informieren (Artt. 13, 14 DSGVO):

Zum Zeitpunkt der Erhebung beim Betroffenen:

Kontaktdaten des Verantwortlichen	berechtigte Interessen	Dauer der Speicherung	Beschwerderecht bei der Aufsichtsbehörde
Kontaktdaten des Datenschutz-beauftragten	Kategorien von Empfänger/n	Betroffenenrechte	Pflicht zur Bereitstellung der Daten
Zwecke und Rechtsgrundlagen	beabsichtigte Drittlands-übermittlung	Recht, eine Einwilligung zu widerrufen	Logik und Tragweite eines möglichen Profilings

Zusätzlich bei Dritterhebung:

Datenkategorien	Datenquellen

Keine Informationspflicht, wenn der Betroffene die Informationen schon hat.

8. Auftragsverarbeitung prüfen

- Was sind Auftragsverarbeiter?

→ Jeder, der Daten im Auftrag und auf Weisung des Verantwortlichen verarbeitet, z. B.

System-Partner	DATEV	Aktenvernichter	Abrechnungsbüros
Rechenzentren/ Cloud Computing	Wartung von Telefonanlagen	Wartung von Multi-funktionsgeräten	Office-Dienstleister

- Auftragsverarbeitung ist grundsätzlich erlaubt, sofern die Anforderungen der EU-Datenschutz-Grundverordnung erfüllt sind:
  - sorgfältige Auswahl
  - Vertrag (auch elektronisch)
  - Arbeiten nur auf dokumentierte Weisung
  - Umsetzung von TOMs
  - Unterstützung des Verantwortlichen bei der Erfüllung seiner Pflichten
  - Regelung von Unterauftragsverhältnissen
  - Verpflichtung der Mitarbeiter zu Vertraulichkeit
  - Überprüfungen durch den Verantwortlichen

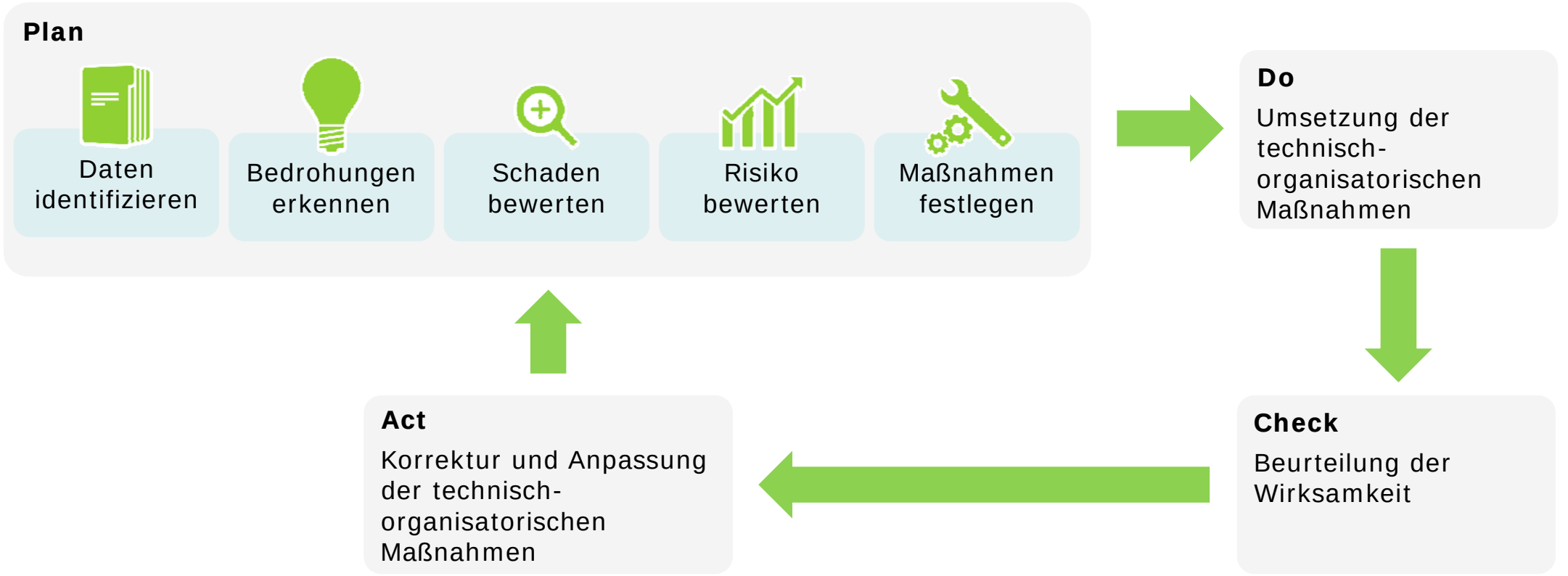
9. Überprüfung der technisch-organisatorischen Maßnahmen und PDCA-Zyklus etablieren

- Sicherheit der Verarbeitung (Art. 32 Abs. 1 DS-GVO):
  - Durch technisch-organisatorische Maßnahmen ist ein angemessenes Schutzniveau zu gewährleisten.
  - Die Ermittlung des angemessenen Schutzniveaus erfolgt unter Berücksichtigung der Risiken, d. h. es muss eine Risikoanalyse durchgeführt werden.

Höhe des Risikos für die Rechte und Freiheiten natürlicher Personen	=	Eintritts-wahrscheinlichkeit einer Bedrohung	x	schwere der Auswirkung (= Schadenspotenzial)

- Systeme müssen privacy by design/default (Art. 25 DS-GVO) umsetzen, z. B.
  - keine Datenerhebung nicht benötigter Daten oder
  - Rechtevergabe nach dem Freigabeprinzip.
- Bisherige Schutzmaßnahmen sind nicht notwendigerweise „falsch“, aber sie müssen nach diesen Prinzipien überprüft und es muss der Nachweis der Angemessenheit (Nachweispflicht gem. Art. 5 Abs. 2 DS-GVO) geführt werden.

9. Überprüfung der technisch-organisatorischen Maßnahmen und PDCA-Zyklus etablieren



9. Überprüfung der technisch-organisatorischen Maßnahmen und PDCA-Zyklus etablieren

- Die DS-GVO will natürliche Personen durch den Schutz ihrer personenbezogenen Daten schützen.
- Personenbezogene Daten sind alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare** natürliche Person beziehen (Art. 4 Nr. 1 S. 1 DS-GVO).
- Dazu gehören bspw.:
  - Name, Vorname, Geburtsdatum, Alter, Familienstand
  - Standortdaten (z. B. Anschrift)
  - „Online“-Kennungen (z. B. Telefonnummer, E-Mail-Adresse, IP-Adresse)
  - Kennnummern (z. B. Kontonummer, Kreditkartennummer, Kfz-Kennzeichen)
  - wirtschaftliche, kulturelle oder soziale Identität
  - Vorstrafen
  - Werturteile (z. B. Zeugnisse, Kreditwürdigkeit)
- Dazu zählen die Daten von Kunden, Lieferanten, ggf. deren Beschäftigten sowie den eigenen Beschäftigten.

9. Überprüfung der technisch-organisatorischen Maßnahmen und PDCA-Zyklus etablieren

- Möglichkeiten, mit Risiken zu verfahren:
  - Risikovermeidung
  - Risikotransfer
  - Risikoakzeptanz
  - Risikominimierung

  → Die DS-GVO betrachtet lediglich die Risikominimierung!

- Risikominimierung kann bedeuten,
  - die Schadenshöhe zu begrenzen.
  - die Eintrittswahrscheinlichkeit zu verringern.

- Vorgeschriebene Maßnahmen:
  - Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a) DS-GVO)
  - Informationssicherheits-Management (Art. 32 Abs. 1 lit. b) DS-GVO)
- Maßnahmenkataloge:
  - BSI IT-Grundschutz-Kataloge
  - ISO 29151
  - ISO 27.001 Anhang A, ISO 27.002

9. Überprüfung der technisch-organisatorischen Maßnahmen und PDCA-Zyklus etablieren

Beispiele für verarbeitungsübergreifende Maßnahmen

Gebäudesicherheit
Firewall
Virenschutz
Patchmanagement
Datensicherung
Passwortregeln
Verschlüsselung (von E-Mails, Datenträgern etc.)
Pseudonymisierung von Daten

- Verpflichtung von Mitarbeitern und Dienstleistern
- dezidierte Berechtigungsvergabe
- Notfallplan
- Server Sicherheit
- Arbeits- und Verhaltensanweisungen für Mitarbeiter
- Besprechungsraum
- etc.

10. Mitarbeiter nach dem neuen Recht und seiner Umsetzung schulen

Wann sollte geschult werden?

zu Beginn der Tätigkeit

Auffrischungs-schulungen (z. B. jährlich)

bei der Einführung neuer Verarbeitungen oder grundlegenden Änderungen

Was sind mögliche Inhalte?

- Grundlagenwissen Datenschutz und Verschwiegenheit
- Verbot mit Erlaubnisvorbehalt
- Verantwortung der Mitarbeiter
- Schutzmaßnahmen im Unternehmen (Handlungsanweisungen)
- aktuelle Themenstellungen (z. B. Kryptoviren)

Sanktionen bei Verstößen gegen DSGVO

- Bußgelder (Art. 83 Abs. 4–6 DS-GVO, wirksam, verhältnismäßig, abschreckend):

bis 10 Mio. Euro oder bis 2% des weltweiten Jahresumsatzes	bis 20 Mio. Euro oder bis 4% des weltweiten Jahresumsatzes
bei Verstößen gegen die Pflichten als Verantwortlicher	bei Verstößen gegen die Rechte Betroffener oder Anordnungen der Aufsichtsbehörden

- Recht auf Schadenersatz von materiellem oder immateriellem Schaden (Art. 82 Abs. 1 DS-GVO)
- gesamtschuldnerische Haftung von Verantwortlichen und Auftragsverarbeitern gegenüber den Betroffenen (Art. 82 Abs. 4 DS-GVO), Ausgleich im Innenverhältnis möglich (Art. 82 Abs. 5 DS-GVO)
- Abhilfe durch die Aufsichtsbehörde (u. a. Verwarnung, Anordnung von Maßnahmen, Verbot der Verarbeitung, Art. 58 Abs. 2 DS-GVO)
- **Hinweis:** Bußgelder können nicht als Betriebsausgabe geltend gemacht werden und sind nicht versicherbar!

Sanktionen - Systematik

Rechtswege:

- Beschwerde **bei** Aufsichtsbehörde
- Gerichtsverfahren **gegen** Aufsichts-behörde
- Gerichtsverfahren gegen Verantwort-lichen für die Verar-beitung / Auftrags-verarbeiter

Vertretung:

- Vertretung des Betroffenen durch einen Verband
- Verbandsklage-recht

(nach nationalem Recht)

Sanktionen:

- Schadensersatz
- Bußgeld
- Strafe (nach nationalem Recht)

Sanktionen – Bemessungskriterien Art. 83 DSGVO

- 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

Datenschutz-Risiken

- Prüfung durch Aufsichtsbehörde (anlasslos! oder nach Antrag)
- Datenpannen und Sicherheitsvorfälle, die zu melden sind
- Betroffene (z.B. Kunden, Lieferanten, Externe MA)
- Abmahnanwälte & Abmahnvereine
- Verbraucherschutzorganisationen
- Mitarbeiter
- Wettbewerber
- Investigative Journalisten
- „berufsmäßige“ Denunzianten
- alle, die wirtschaftlichen Vorteil ziehen können ☺

Hinweis:
Daten können heute über das Internet leicht automatisiert abgeglichen werden! Z.B. Internetseiten und Unternehmensregister auf Bestellung eines DSB.

...

Datenschutzrendite (ROPI) – Beispiel (1)

**** ROPI = Return on Privacy Investments***

Erwarteter Schaden - Informationspflicht nach Artt. 13/14 DSGVO nicht erfüllt.	**250.000 €/Fall**
Erwartete Eintrittshäufigkeit ohne die geplante Datenschutzkontrolle	5 x/Jahr
Erwartete Eintrittshäufigkeit mit eingeführter Datenschutzkontrolle	1 x/alle 4 Jahre
Kosten der Maßnahme (Bestellung Datenschutzbeauftragter (Extern), der regelmäßige interne Audits durchführt)	10.000 € / Jahr

$$\text{ROPI} = 525\ \% = \frac{(250.000\ € \ x\ 0{,}25\ \%) - 10.000\ €}{10.000\ €}$$

Datenschutzrendite (ROPI) – Beispiel (2)

**** ROPI = Return on Privacy Investments***

Erwarteter Schaden – DSB nicht bestellt nach Artt. 37-39 DSGVO)	**150.000 €/Fall**
Erwartete Eintrittshäufigkeit ohne die geplante Datenschutzkontrolle	1 x/Jahr
Erwartete Eintrittshäufigkeit mit eingeführter Datenschutzkontrolle	Entfällt wenn bestellt
Kosten der Maßnahme (Bestellung Datenschutzbeauftragter (Extern)	10.000 € / Jahr

$$\text{ROPI} = 1.400\ \% = \frac{(150.000\ €) - 10.000\ €}{10.000\ €}$$

Zu den Kosten DSB / DSMS

Der Aufwand für die Bestellung eines DSB sowie Aufbau und Pflege eines DSMS lassen sich als Gemeinkosten verrechnen – wie auch die für Steuer- & Rechtsberatung.

So können und sollten diese Kosten in die Preiskalkulation einbezogen werden!

Beispiel:
Ein Unternehmen mit 500.000 € Umsatz p.a. kann die Preise um ca. 2 % anheben, um die Anforderungen der DSGVO bei erwarteten 10.000 € p.a. ertragsneutral umzusetzen.

Hinweis:
Die Gesellschaft will den Datenschutz sowie Sicherheit: Also sollte Sie auch dafür bezahlen! In vergleichbaren Fällen wie Steuerberatung, Wirtschaftsprüfung, Arbeitsschutz sowie Sozialschutz tut sie es ja auch. Auch der Wettbewerb hat die DSGVO einzuhalten – so sind die höheren Preise am Markt problemlos durchzusetzen!

Interner DSB vs. Externer DSB

	Interner DSB	Externer DSB
Kosten	Gehalt, Sozialabgaben, Freistellung für Aufgaben	gering, bei KMU i.d.R. weniger als 10.000 € p.a.
Fachkunde	Gegeben, vom Unternehmen zu finanzieren	Gegeben, bringt der eDSB mit
Neutralität	gegeben, wenn wirklich frei	Gegeben, falls keine weiteren Mandate im Unternehmen
Haftung	keine	im Innenverhältnis
Know-How	gegeben	i.d.R. höher, wegen Erfahrungen in weiteren Mandaten
Kündigung	Kündigungsschutz	schnell möglich
Betriebsrat	Mitsprache	keine Mitsprache
Ressourcen	Freistellung für DSB	Keine Unternehmensressourcen freizugeben

✓ Einsatz eines Externen DSB bringt klare Vorteile!

Nutzen Umsetzung DSMS

Das Risiko einer Prüfung und nachfolgenden Sanktionierung nach DSGVO ist gegenüber dem BDSG a.F. deutlich gestiegen.

Die finanziellen Folgen liegen auf dem Niveau von Kartellrechtsverstößen und können die Existenz Ihres Unternehmens gefährden.

Es lohnt sich kaum, diese Risiken einzugehen, nur um den verhältnismäßig geringen Aufwand für die Einführung und Umsetzung eines DSMS einzusparen.

Durch Einführen eines DSMS und Bestellung eins Datenschutzbeauftragten senken Sie diese Risiken!

Fazit

- Aufgrund des Umfangs der Anpassungsmaßnahmen sollte mit der Umsetzung jetzt bzw. sofort begonnen werden.
- Teilweise steht die endgültige Auslegung der Datenschutz-Grundverordnung noch nicht fest. Hier sollte die Meinungsbildung weiter beobachtet werden.
- Auf jeden Fall gilt die Aussage: vernünftig umgesetzt finanzieren sich Datenschutz und Informationssicherheit von selbst!
- Die meisten Unternehmen fahren mit der Bestellung eines Extern Datenschutzbeauftragten (eDSB) besser.
- Der Aufbau eines DSMS unter Berücksichtigung des technisch organisatorischen Datenschutzes ist vielfach nützlich. Datenschutzrisiken werden minimiert – Erwartungen der Gesellschaft werden erfüllt (positives Image) – Informationsschutz führt zur Aufrechterhaltung der Betriebsbereitschaft.
- Eine zentrale Aussage bleibt weiterhin gültig:
  Ihre Mitarbeiter schützen Ihre Daten und die Ihrer Kunden und Geschäftspartner!
- Die **Verantwortung und Haftung liegt jedoch stets bei der Verantwortlichen Stelle**, d.h. letztlich der Geschäftsführung. Die Haftung lässt sich daher nicht einfach auf den DSB abwälzen.

DEGA - Datenschutzberatung

- Stellung eines Externen Datenschutzbeauftragten (DSB)
- Aufbau Datenschutz-Management-System (DSMS)
- Unterstützung Ihres Datenschutzbeauftragten
- Auftragskontrollen im Rahmen der ADV (Art. 28 DSGVO)
- Datenschutz-Audits / Datenschutzgütesiegel / Zertifizierung
- Schulung / Sensibilisierung MA in Datenschutz & Informationssicherheit
- Beratung bei Sicherheitsvorfällen
- Beratung bei Spezial-/Sonderfällen wie Revision-/Compliance-Prüfungen, Fraud-Investigation, Internen-Untersuchungen, Datenanalyse, IT-Forensik etc.

DEGA Berater

Unsere Berater verfügen über langjährige einschlägige Erfahrungen im Datenschutz-/Datenschutz-Audit, IT-Sicherheit sowie IT-Forensik.

Die Berater bilden sich regelmäßig fort und weisen damit stets die geforderte Zuverlässigkeit und Fachkunde nach.

Sprechen Sie uns an:
Gern erstellen wir Ihnen ein individuelles Angebot!

© Fotolia

Dipl.-Kfm.
Lutz Ressmann
- **Geschäftsführer**
- **Datenschutzsachverständiger**
- **Datenschutz-Auditor**

DEGA

Ortlohstraße 232
D-45665 Recklinghausen

Telefon: +49 (0) 2361 / 927640
Telefax: +49 (0) 2361 / 927641

E-Mail: info@degaberatung.de
Web: www.degaberatung.de