Thomas Schelly
STEUERBERATER

EU-Datenschutz-Grundverordnung

Mandanteninformation

Was ist eigentlich …

Thomas Schelly
STEUERBERATER

… 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.

Die EU-Datenschutz-Grundverordnung kurz erklärt

Thomas Schelly
STEUERBERATER

- 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 der EU-Datenschutz-Grundverordnung

Thomas Schelly
STEUERBERATER

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 des neuen Datenschutzrechts

Thomas Schelly
STEUERBERATER

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

Thomas Schelly
STEUERBERATER

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

Thomas Schelly
STEUERBERATER

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.

Die Ressourcen hierfür muss das Unternehmen bereitstellen!

… 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

2. Bestandsaufnahme durchführen

Thomas Schelly
STEUERBERATER

- 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

Thomas Schelly
STEUERBERATER

- Gemäß Art. 30 Abs. 1 DS-GVO ist vom Verantwortlichen ein Verzeichnis aller Verarbeitungstätigkeiten mit definierten Inhalten zu führen.
- Die Ausnahme in Absatz 6 greift nur bei risikoloser Verarbeitung. Diese wird in der Regel zu verneinen sein.
- 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

Thomas Schelly
STEUERBERATER

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

Thomas Schelly
STEUERBERATER

- **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

Thomas Schelly
STEUERBERATER

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

Thomas Schelly
STEUERBERATER

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

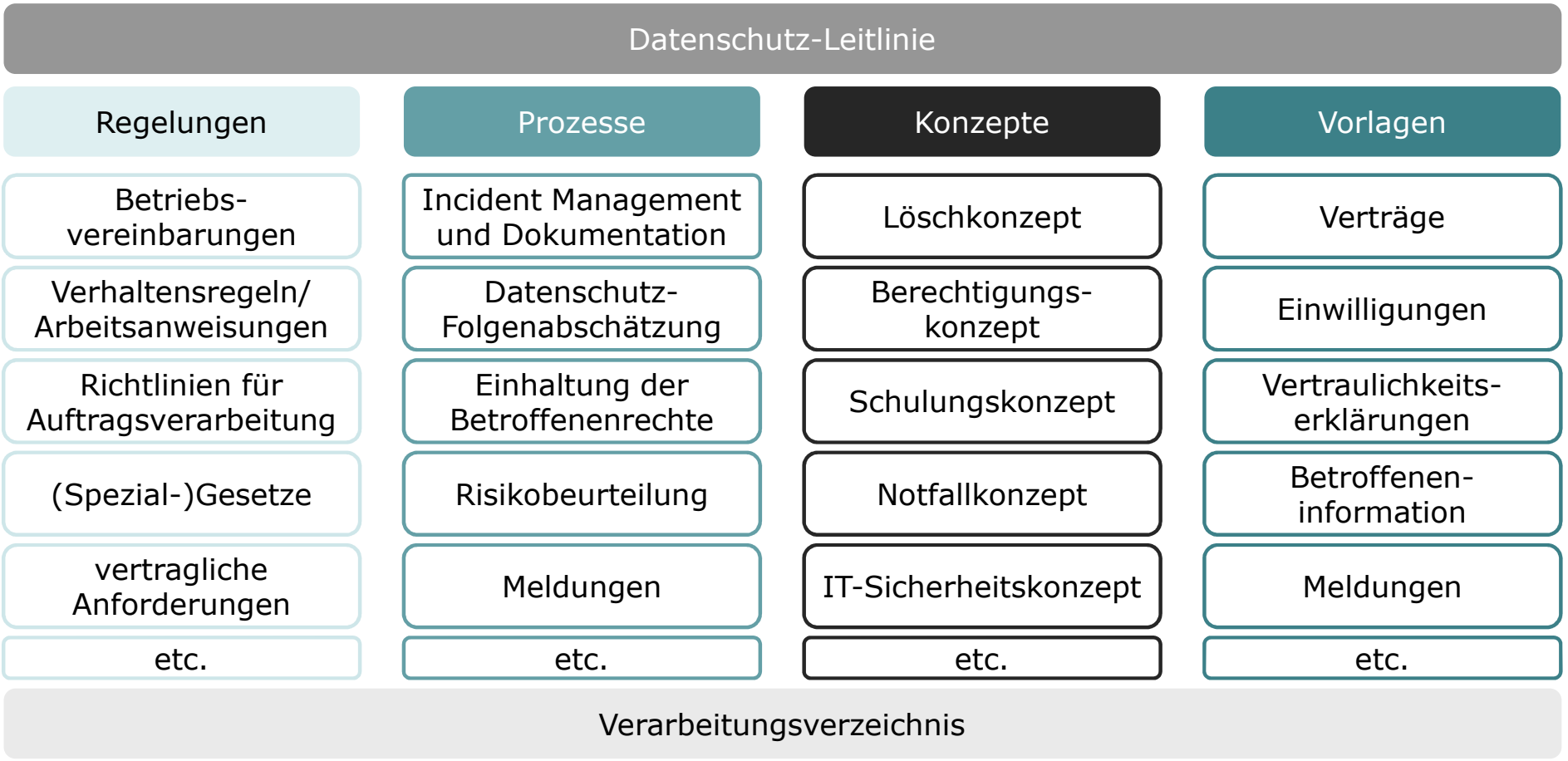
- Aufbewahrungs-pflichten

- zur Abwehr von Haftungsansprüchen

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

6. Datenschutz-Management-System aufbauen

Thomas Schelly
STEUERBERATER



6. Datenschutz-Management-System aufbauen

Thomas Schelly
STEUERBERATER

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

Thomas Schelly
STEUERBERATER

Der Betroffene ist vom Verantwortlichen über die Datenverarbeitung und seine Rechte zu informieren:

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

Thomas Schelly
STEUERBERATER

- 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

Thomas Schelly
STEUERBERATER

- 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

Thomas Schelly
STEUERBERATER

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

Thomas Schelly
STEUERBERATER

Daten identifizieren

- 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

Thomas Schelly
STEUERBERATER

- 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

Thomas Schelly
STEUERBERATER

Beispiele für verarbeitungsübergreifende Maßnahmen

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

Thomas Schelly
STEUERBERATER

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)

Konsequenzen aus der Nichtbefolgung der EU-Datenschutz-Grundverordnung

Thomas Schelly
STEUERBERATER

- 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)

Fazit

- Handlungsbedarf für bereits gut aufgestellte Unternehmen gibt es vor allem in zwei Bereichen:

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

- Einhaltung der Rechte Betroffener

- Aufgrund des Umfangs der Anpassungsmaßnahmen sollte mit der Umsetzung jetzt begonnen werden.
- Teilweise steht die endgültige Auslegung der Datenschutz-Grundverordnung noch nicht fest. Hier sollte die Meinungsbildung weiter beobachtet werden.
- Eine zentrale Aussage bleibt weiterhin gültig:
  Ihre Mitarbeiter schützen Ihre Daten und die Ihrer Kunden und Geschäftspartner!