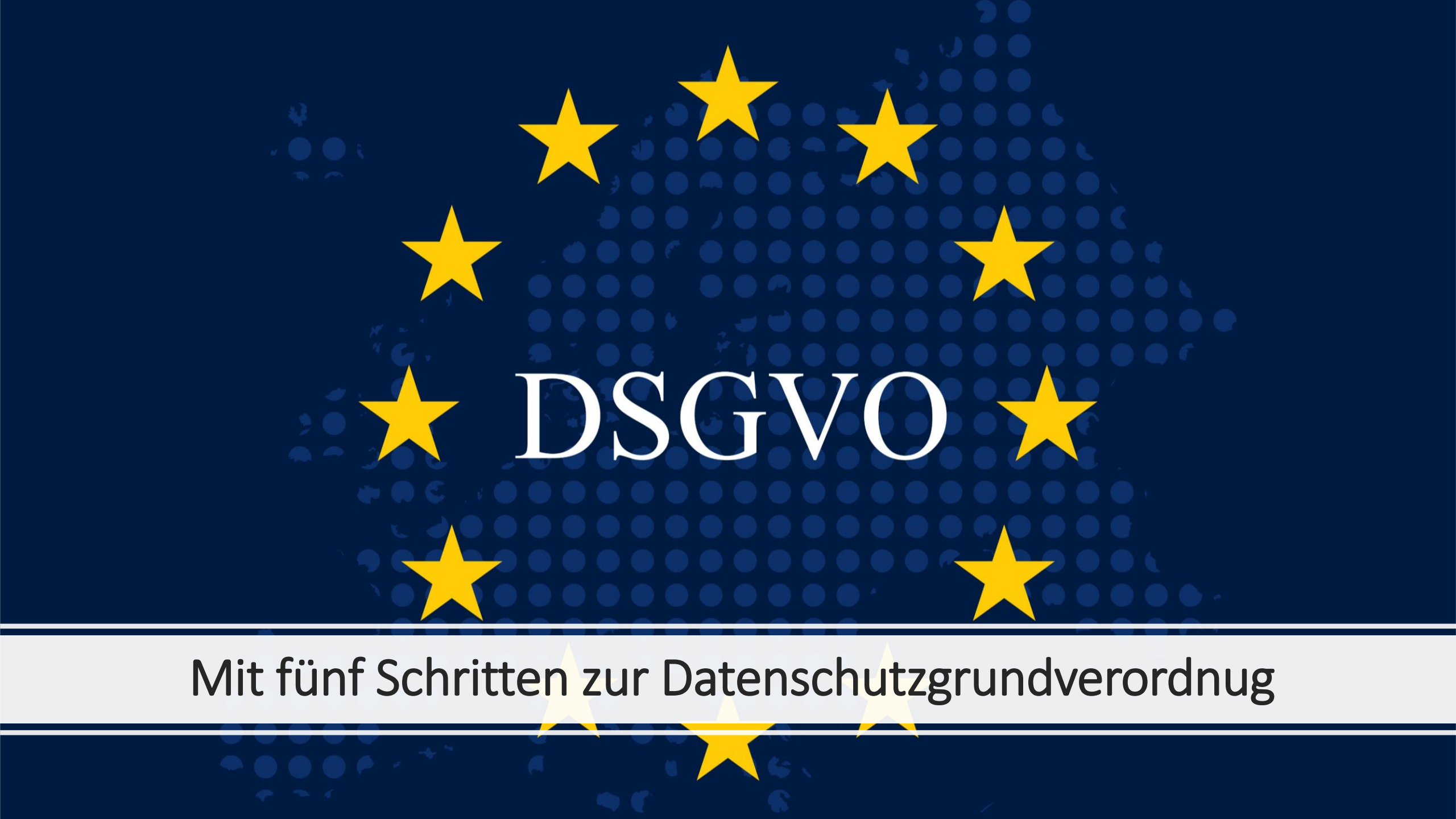


Mit fünf Schritten zur Datenschutzgrundverordnug

1. Der Status quo

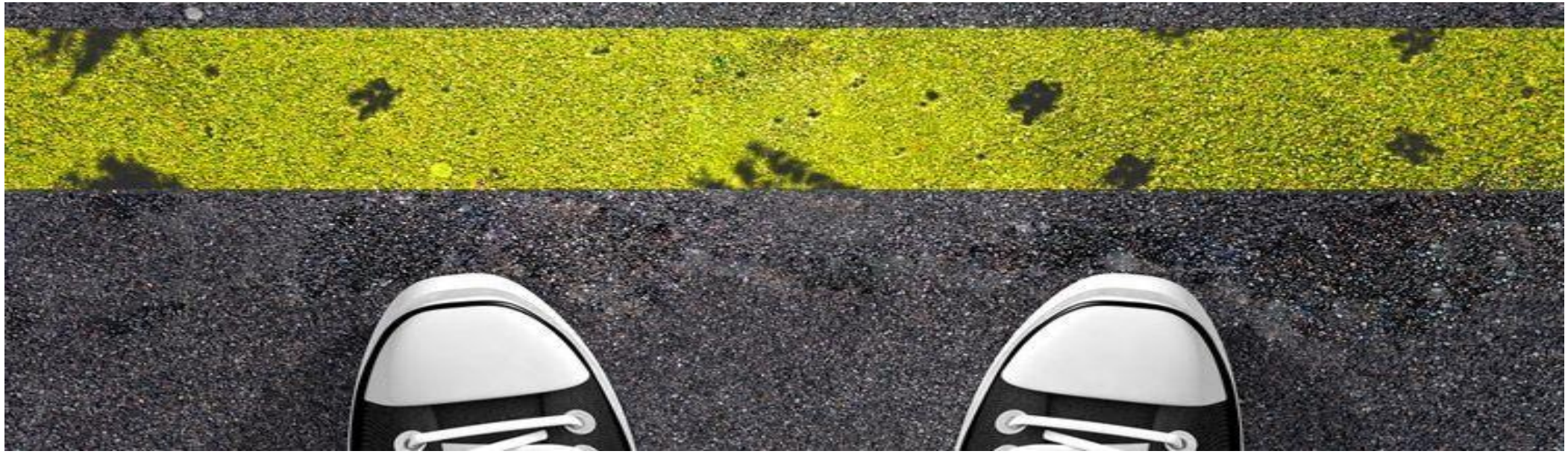
In einem ersten Schritt sollte eine Bestandsaufnahme der vorhandenen datenschutzrechtlich relevanten Prozesse durchgeführt werden, um zu sehen an welchen Stellen das Unternehmen überhaupt Änderungsbedarf hat. Dann kann im Rahmen dieser sogenannten GAP-Analyse geklärt werden, auf welchem Stand sich der Datenschutz im Unternehmen befindet.

Auf Grund der daraus resultierenden Feststellungen kann dann geprüft werden, inwieweit der Ist-Zustand von den Anforderungen der DSGVO abweicht. Anschließend sollte ein geeigneter Fahrplan für die verbleibende Umsetzungszeit festgelegt werden. So lässt sich systematisch mit entsprechenden Maßnahmen nach und nach der gewünschte Soll-Zustand erreichen.

2. Verzeichnis von Verarbeitungstätigkeiten aufbauen

Das Verzeichnis von Verarbeitungstätigkeiten nach der DSGVO ist im Grundsatz nichts anderes, als das altbekannte Verfahrensverzeichnis nach §§ 4g Abs. 2, 4e BDSG. Es handelt sich also um eine Dokumentation und Übersicht über Verfahren, bei denen personenbezogene Daten verarbeitet werden.

Die Pflicht das Verzeichnis von Verarbeitungstätigkeiten zu führen trifft sowohl den Verantwortlichen als auch den Auftragsverarbeiter. Inhaltlich werden aber geringere Anforderungen an das Verzeichnis von Verarbeitungstätigkeiten eines Auftragsverarbeiters gestellt. Aus Art.30 Abs. 5 DSGVO ergeben sich auch Ausnahmen für die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten. Die Pflicht zur Führung gilt dann nicht, wenn der Verantwortliche oder Auftragsverarbeiter weniger als 250 Beschäftigte hat, es sei denn, die von vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder die Verarbeitung keine besonders sensiblen Datenkategorien oder strafrechtlich relevanten Daten betrifft.



3. Pflicht statt Kür – das Datenschutz-Management-System

Die DSGVO verpflichtet Unternehmen zudem ein Datenschutz-Management-System einzuführen. Zentrale Normen sind hier Art. 5 und Art. 24 DSGVO, aus denen sich eine Nachweis- und Rechenschaftspflicht für Unternehmen ableitet. Künftig müssen Unternehmen nämlich nicht nur sicherstellen, dass datenschutzrechtliche Vorgaben eingehalten werden, sondern sie müssen dies auch nachweisen können.

Gleiches gilt auch im Bereich Datensicherheit – denn auch hier bedarf es eines Nachweises, dass „geeignete technische und organisatorische Maßnahmen“ eingesetzt werden, die dem Schutz der betroffenen Personen dienen. Im Klartext heißt das, dass künftig Dokumentationen etwa aus den Bereichen:

3. Pflicht statt Kür – das Datenschutz-Management-System

- **Datenschutzorganisation und Verantwortlichkeit für Datenverarbeitungen**
- **Einbindung des Datenschutzbeauftragten (Fälle, in denen Mitarbeiter sich an den Datenschutzbeauftragten wenden sollten)**
- **Verzeichnis von Verarbeitungstätigkeiten (an welchen Stellen liegen personenbezogenen Daten im Unternehmen vor?)**
- **Datenschutz-Folgeabschätzung, Art. 35 DSGVO (wie Vorabkontrolle nach § 4d Abs. 5 BDSG beim Umgang mit sensiblen Daten, Videoüberwachung)**
- **Vertragsmanagement (welche Dienstleister werden eingesetzt?)**
- **Datenschutz-Schulung und Verpflichtung auf das Datengeheimnis**
- **Prozess zur Wahrnehmung von Betroffenenrechten**
- **Meldung von Datenschutzverstößen**
- **Nachweis der Datensicherheit (Umsetzung von technischen und organisatorischen Maßnahmen)**

  angelegt und gepflegt werden sollten.

Ein DMS kann zwar bei unbeabsichtigten Datenschutzverstößen nicht mit Sicherheit den Vorwurf der Fahrlässigkeit entfallen lassen, ist jedoch nach Art. 83 Abs. 2 d) DSGVO zumindest bußgeldmindernd zu berücksichtigen. Zudem ermöglicht ein effizientes System eine schnelle Reaktion des Unternehmens, falls es tatsächlich zu Datenschutzverstößen kommt.

4. Zulässigkeit der Datenverarbeitung

Des Weiteren ist auch zu überprüfen, ob die Verarbeitung und Nutzung personenbezogener Daten mit der erforderlichen Erlaubnis erfolgt. Daher sollten die Rechtsgrundlagen und Einwilligungen überprüft werden. In Betracht kommen die Artikel 6 bis 11 DSGVO. Aus Art. 7 DSGVO ergeben sich die Bedingungen, unter denen eine Einwilligung künftig rechtskonform sein wird:

- **Freie Entscheidung des Betroffenen**
- **Ausführliche, erkennbare und bestimmte Information des Betroffenen**
- **Schriftform der Einwilligungserklärung**
- **Widerruflichkeit der Einwilligungserklärung**

Eine Neuerung ergibt sich im Bereich der Einwilligung von Minderjährigen unter 16 Jahren (bzw. unter 13 Jahren wenn das nationale Recht dies vorsieht). Diese sollen generell nur wirksam sein, wenn und insoweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird ((Art. 8 Abs. 1 DSGVO)

5. Informationspflichten

Informationspflichten bei Datenerhebung und -verarbeitung sind fester Bestandteil des Datenschutzrechts. Unter der DSGVO vervielfachen sich jedoch die von Unternehmen und Verantwortlichen zu berücksichtigenden Pflichten in Bezug auf die Information von Betroffenen. Maßgebliche Normen sind hier Art. 13 und Art. 14 DSGVO. Nach Art. 13 DSGVO sind insbesondere die folgenden Informationen dem Betroffenen in präziser, transparenter, verständlicher und leicht zugänglicher Form zu erteilen:

5. Informationspflichten

Identität des Verantwortlichen - Kontaktdaten des Datenschutzbeauftragten - Empfänger

Übermittlung der Daten in Drittstaaten - Dauer der Speicherung - Betroffenenrechte

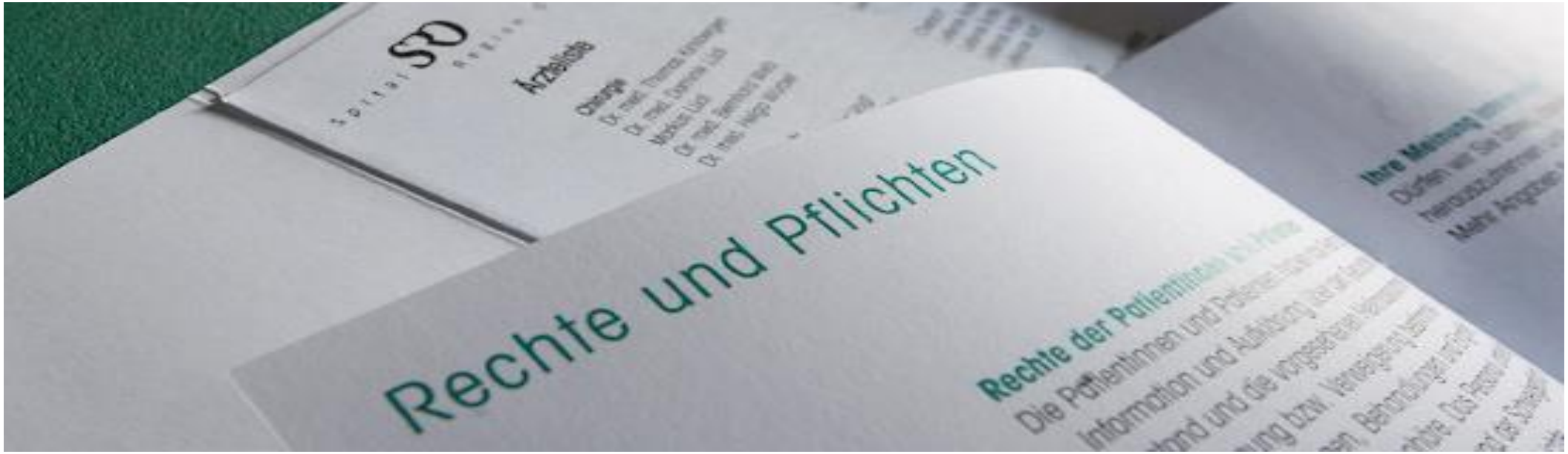
Widerrufbarkeit von Einwilligungen - Beschwerderecht bei der Aufsichtsbehörde

Verarbeitungszwecke und Rechtsgrundlagen - Berechtigtes Interesse

Verpflichtung zur Bereitstellung personenbezogener Daten

Automatisierte Entscheidungsfindung und Profiling

Aus Art. 14 DSGVO ergibt sich, dass nahezu dieselben Informationspflichten bestehen, wenn die Daten nicht beim Betroffenen selbst erhoben werden.



Jetzt im Schnelldurchlauf

1. Der Status quo

- ✓ Verarbeitungsübersicht erstellen
- ✓ Schwachstellen ermitteln
- ✓ Maßnahmen festlegen und planen

2. Verzeichnis von Verarbeitungstätigkeiten aufbauen

- ✓ Betroffene Personengruppe definieren
- ✓ Welche Daten werden zu welchem Zweck verwendet
- ✓ Werden Daten an Ditte weitergeleitet (Auftragtsverarbeitung)
- ✓ Übermittlung an Drittstaaten oder internationale Organisationen
- ✓ Sicherheit der Verarbeitung (Technische Organisatorische Maßnahmen (TOM´S)

3. Pflicht das Datenschutz-Management-System

- ✓ Dokumentation- und Nachweispflichten aufbauen
- ✓ Einwilligung des Betroffenen sicherstellen
- ✓ Rechtsgrundlage der Verarbeitung nachweisen
- ✓ Nachweis sicherer IT-Systeme, Anwendungen und Papierakten
- ✓ Verträge mit Dienstleistern abschließen
- ✓ Löschkonzept nachweisen

4. Zulässigkeit der Datenverarbeitung

- ✓ Einwilligung des Betroffenen
- ✓ Rechtsgrundlagen
- ✓ Verarbeitung von Daten von Kindern
- ✓ Zweckbindung der Verarbeitung
- ✓ Betroffenen Rechte einhalten
- ✓ Recht auf Vergessenwerden (Löschen)

5. Informationspflichten

- ✓ Information des Betroffenen
- ✓ Meldung bei Datenschutzpannen an Behörde
- ✓ Meldung des Datenschutzbeauftragten an Behörde

Tintus Consulting GmbH & Winfried Rau Consulting

Contact: Winfried Rau

67281 Bissersheim, Hollergasse 10

web: htts://www.tintus-consulting.de

fon: 06359 8727507

mobil: 0173 7555203

e-mail: mail@tintus-consulting.de