Dr. Thomas Schweiger, LL.M.

Wien, 13.03.2018

nur mehr **72 Tage** und damit
weniger als 3 Monate
bis zum **25.05.2018**

Datenschutz-Grundverordnung (DSGVO) und Auswirkungen auf Transport & Logistik

Nutzung von WhatsApp am „Diensthandy“

Über unsere Dienste

Registrierung. Du musst dich für unsere Dienste registrieren und dafür korrekte Daten verwenden, deine aktuelle Mobiltelefonnummer angeben und diese im Falle einer Änderung unter Nutzung unserer In-App-Funktion „Nummer ändern“ aktualisieren. Du stimmst zu, SMS und Telefonanrufe mit Codes zur Registrierung für unsere Dienste (von uns oder unseren Drittanbietern) zu erhalten.

Adressbuch. Du stellst uns regelmäßig die Telefonnummern von WhatsApp-Nutzern und deinen sonstigen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung. Du bestätigst, dass du autorisiert bist, uns solche Telefonnummern zur Verfügung zu stellen, damit wir unsere Dienste anbieten können.

Rechtsanwalt Dr. Thomas Schweiger, LL.M. (Duke), CIPP/E

Rechtsanwalt in Linz seit 09.09.1999

zertifizierter Datenschutzbeauftragter (DATB)

vorwiegend im Bereich Beratung tätig

Publikationen im Bereich IT-Recht

Spezialgebiet: Datenschutz

www.dataprotect.at / www.it-recht.at

t: @dataprotect_at

f: dataprotect

Datenschutz-grundverordnung

Das Infopaket der WKO Fachgruppe Finanzdienstleister

Inhalt

- Grundprinzipien des Datenschutzes nach der DSGVO und DSG
- Anleitung / Anmerkungen zum Verzeichnis von Verarbeitungstätigkeiten
- Infos über „TOMs“ (technische und organisatorische Maßnahmen)
- Muster und Infos zur Einwilligungserklärung zur Zusendung von Informationsmaterial
- Muster für eine Verpflichtungserklärung zur Einhaltung des DSG für Dienstnehmer/innen
- Muster für ein Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter
- Muster für ein Verzeichnis von Verarbeitungstätigkeiten für Finanzdienstleister als Verantwortliche
- Musterschreiben zur Zusendung des Identitätsnachweises für ein Auskunftsbegehren nach Art 15 DSGVO

Grundprinzipien des Datenschutzes nach der DSGVO und DSG

1. Rechtmäßigkeit

- *„the processing shall be lawful only …“* (lawfulness)
- Grundsatz: die Verarbeitung ist verboten
- Grundlage für die (erlaubte) Verarbeitung

Art 6 DSGVO:

Einwilligung 👍🏻
Vertrag/Anbahnung 🤝
gesetzl Verpflichtung 🛂
lebenswichtiges Interesse 🚑
öff Interesse/Aufgabe 👩🏻‍🎓
berechtigtes Interesse ⚖️

(c) Eduardo Usturan

Rechtmäßigkeit

keine andere Grundlage

keine „Rechtsbeziehung“

Einwilligung der betroffenen Personen

freiwillig, informiert

widerrufbar

keine Kopplung

Einwilligungen richtig gestalten

- Wer / Was / Warum / Wohin?
- Transparenz
- Nachweispflicht soll erfüllbar sein
- Freiwilligkeit & Kopplungsverbot
- Widerrufsmöglichkeit
- Anwendung: Newsletter/Marketing, Beschäftigte (Fotos)

..... (Name)	..... (Vorname)	..... (Postadresse)
..... (Email-Adresse)	..... (Festnetz)	..... (Mobiltelefon)

erklärt die Einwilligung, dass die **oben bekannt gegebenen Daten** von xxx zu **Werbezwecken** verwendet werden dürfen.

Diese Einwilligung kann jederzeit widerrufen werden.

Ein Widerruf kann z.B. per Email an [Email-Adresse] oder auch auf jede andere Art und Weise erfolgen.

Der Widerruf gilt für die Zukunft und hat zur Folge, dass keine weiteren Zusendungen oder Kontaktaufnahmen erfolgen. Die Verarbeitung der Daten vor dem Widerruf ist nicht davon betroffen. Die Daten werden dann lediglich zum Nachweis der korrekten Abwicklung der bisherigen Tätigkeit (z.B. Dokumentation der Einwilligung, bisherige Zusendung der Werbemittel) verwendet. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf verarbeiteten Daten nicht berührt.

XXX verarbeitet die Daten in Übereinstimmung mit den datenschutzrechtlichen Bestimmungen. Nähere Informationen finden Sie [am Messestand] oder finden diese auch im Internet unter [www.[...]/Datenschutz]

..... (Datum)

..... (Unterschrift)

Transparenz bei der Einwilligung?

Art 13 DSGVO – Information bei der Erhebung der Daten -> wie kann dass erfüllt werden?

Verantwortlicher:	(Firmenwortlaut/ Name, Adresse und Telefonnummer)
Datenschutz-beauftragter:	Es ist kein Datenschutzbeauftragter bestellt, da keine gesetzliche Notwendigkeit besteht.
Zu welchem Zweck verarbeiten wir Ihre Daten:	Werbung und Information über die Produkte/Dienstleistungen
Rechtsgrundlage:	Einwilligung (diese kann jederzeit widerrufen werden)

Transparenz bei der Einwilligung?

Speicherdauer	Die Daten werden für den Zeitraum von 3 (drei) Jahren ab dem letzten Kontakt gespeichert.
Empfänger-kategorien	Die Daten werden nur zur Abwicklung der Werbemaßnahmen verwendet und dabei an die Auftragsverarbeiter (IT-Dienstleister, Service-Unternehmen bei der Abwicklung, Zusteller) sowie unsere allgemeinen Auftragsverarbeiter (IT-Service-Dienstleister) sowie an Behörden und unsere Auftragnehmer (Steuerberater, Rechtsvertreter) weitergegeben. Es werden die Daten nicht an Dritte weitergegeben, die damit eigne Zwecke verfolgen.
Datenübertrag-barkeit:	Es besteht kein Recht auf Datenübertragbarkeit.

Eine Übermittlung an Empfänger in einem Drittland (außerhalb der EU) oder an eine internationale Organisation ist/ ist nicht *(Nichtzutreffendes streichen)* vorgesehen. Es besteht keine automatisierte Entscheidungsfindung (Profiling).

Es ist weder vertraglich noch gesetzlich vorgeschrieben, dass die Daten bereitgestellt werden und es gibt auch keine Verpflichtung dazu. Die Daten sind allerdings erforderlich, damit die Werbemaßnahmen ordnungsgemäß durchgeführt werden können.

Als betroffener Person stehen Ihnen grundsätzlich das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung und Widerspruch zu. Zur Ausübung Ihrer Rechte wenden Sie sich bitte an:
[Unternehmen und die Kontaktdaten ergänzen (Telefon, E-Mail)]

Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in irgendeiner Weise verletzt worden sind, steht es Ihnen frei, bei der Datenschutzbehörde Beschwerde zu erheben.

Vertrag & Vertragsanbahnung

alle personenbezogenen Daten die erforderlich sind

Vertrag mit der betroffenen Person

Verträge mit Kunden, Versicherungen, Banken, Beschäftigten …

direkte Beziehung mit der betroffenen Person

rechtliche Verpflichtung

- gesetzliche (normative) Verpflichtungen des MS/Union
- Arbeitsrecht (Arbeitszeit, Krankenstandsaufzeichnungen)
- Aufzeichnungspflichten nach WAG (kundenseitig)
- steuerliche Aufbewahrungspflichten

Beschäftigte & Datenschutz

- Verarbeitung von Daten von beschäftigten Personen
- Verarbeitung von Daten durch beschäftigte Personen
- § 6 DSG - Datengeheimnis

Das Datengeheimnis (§ 6 DSG)

Datengeheimnis

§ 6. (1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

Das Datengeheimnis (§ 6 DSG)

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

Diese Verpflichtungserklärung betrifft:

Familienname: _____ **(in BLOCKSCHRIFT)**

Vornamen: _____ **(in BLOCKSCHRIFT)**

1) VERPFLICHTUNGSERKLÄRUNG

Im Zuge des Dienstverhältnisses erhält die obgenannte Person voraussichtlich Kenntnis über Personen und personenbezogene Umstände und Daten (*insbes. auch Bonitätsdaten oder Gesundheitsdaten z.B. bei der Abwicklung von Kranken- oder Lebensversicherungen)* sowie über technische Daten betreffend die technische Infrastruktur und den strukturellen Aufbau von Verarbeitungsvorgängen.

Alle diese Daten sind absolut **vertraulich** zu behandeln, nicht an unberechtigte Empfänger weiterzugeben und unterliegen den Bestimmungen des österreichischen Datenschutzgesetzes.

Diese Verpflichtungserklärung betrifft:

Familienname: _____ **(in BLOCKSCHRIFT)**

Vornamen: _____ **(in BLOCKSCHRIFT)**

1) VERPFLICHTUNGSERKLÄRUNG

Im Zuge des Dienstverhältnisses erhält die obgenannte Person voraussichtlich Kenntnis über Personen und personenbezogene Umstände und Daten (*insbes. auch Bonitätsdaten oder Gesundheitsdaten z.B. bei der Abwicklung von Kranken- oder Lebensversicherungen)* sowie über technische Daten betreffend die technische Infrastruktur und den strukturellen Aufbau von Verarbeitungsvorgängen.

Alle diese Daten sind absolut **vertraulich** zu behandeln, nicht an unberechtigte Empfänger weiterzugeben und unterliegen den Bestimmungen des österreichischen Datenschutzgesetzes.

Transparenz

- für die betroffene Person nachvollziehbar
- was geschieht mit „meinen Daten“
- umfassende **Informationspflichten**
  - **bei der Erhebung von pb Daten**
  - **bei der Verwendung von pb Daten**
- **Datenschutzpolicy & -erklärung**
- **Rechte der Betroffenen**

DATENSCHUTZINFORMATION PERSONALVERWALTUNG

- BESCHÄFTIGTE IM UNTERNEHMEN -

Verantwortlicher	*Firmawortlaut, Adresse, Kontaktdaten*
Datenschutz-beauftragter	Es ist kein Datenschutzbeauftragter bestellt, da keine gesetzliche Notwendigkeit besteht.*[1]
Zweck	Personalverwaltung inkl. gesamter Abwicklung des Beschäftigungsverhältnisses
Rechtsgrundlage	Vertrag (Beschäftigungsverhältnis) sowie gesetzliche Grundlage; berechtigtes Interesse: Eigentumsschutz bei Videoüberwachungsanlagen sowie Sicherstellung der Verfügbarkeit der IT-Systeme und IT-Sicherheit
Speicherdauer	Die Daten werden während der gesamten Vertragslaufzeit und zumindest 7 Jahre nach Beendigung des Geschäftsjahres, in dem das Beschäftigungsverhältnis geendet hat, aufbewahrt, sofern diese nicht im Rahmen von Behördenverfahren länger benötigt werden. Daten, die die Ausstellung eines Dienstzeugnisses betreffen, werden 30 Jahre aufbewahrt.

DATENSCHUTZINFORMATION PERSONALVERWALTUNG

Empfänger-kategorien:	Abteilungen des Unternehmens, die im Rahmen des Beschäftigungsverhältnisses die Daten notwendigerweise erhalten müssen (z.B. EDV, sonstige Verwaltungseinheiten). Gesellschaften der Unternehmensgruppe (z.B. zur Abwicklung gemeinsamer Projekte), Dienstleister, die bei der Erfüllung der Rechte und Pflichten aus dem Beschäftigungsverhältnis eingesetzt werden (z.B. Steuerberater, Lohnverrechnung, Rechtsanwalt) sowie Behörden (Sozialversicherung, Finanzamt, sonstige Behörden), Rechtsvertreter (bei der Durchsetzung von Rechten oder Abwehr von Ansprüchen oder im Rahmen von Behördenverfahren) oder Unternehmen, die im Rahmen des Betreuung der IT-Infrastruktur (Software, Hardware) als Auftragnehmer tätig sind. Diese Empfänger verarbeiten die Daten in unserem Auftrag zur Erfüllung unserer Leistung. Die Daten werden nicht an Empfänger weitergegeben, die mit diesen Daten eigene Zwecke verfolgen.
Datenübertragbarkeit	Es besteht kein Recht auf Datenübertragbarkeit.

Eine Übermittlung an Empfänger in einem Drittland (außerhalb der EU) oder an eine internationale Organisation ist/ist nicht (Nichtzutreffendes streichen) vorgesehen. Es besteht keine automatisierte Entscheidungsfindung (Profiling).

Es ist weder vertraglich noch gesetzlich vorgeschrieben, dass die Daten bereitgestellt werden und es gibt auch keine Verpflichtung dazu. Die Daten sind erforderlich, damit das Vertragsverhältnis ordnungsgemäß durchgeführt werden kann.

DATENSCHUTZINFORMATION PERSONALVERWALTUNG

Als betroffener Person steht Ihnen grundsätzlich das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung und Widerspruch zu. Zur Ausübung Ihrer Rechte wenden Sie sich bitte an:

[Unternehmen und die Kontaktdaten ergänzen (Telefon, E-Mail)]

Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in irgendeiner Weise verletzt worden sind, steht es Ihnen frei, bei der Datenschutzbehörde Beschwerde zu erheben.

Die übergebene Visitenkarte?

Übergabe einer Visitenkarte → personenbezogene Daten?

Erhebung von Daten? → Information gem. Art 13 DSGVO

Prozess?

Wie soll das erfolgen? → Email bei Aufnahme ins CRM-System?

Datenschutz-grundverordnung

technische & organisatorische Maßnahmen (TOMs) im Überblick

Technische & organisatorische Maßnahmen – TOMs

- Datensicherheit zum Schutz vor
  - unbefugter / unrechtmäßiger Verarbeitung
  - unbeabsichtigem Verlust
  - unbeabsichtiger Zerstörung
  - unbeabsichtiger Schädigung
- www.it-safe.at

IT-Sicherheitshandbuch für KMU

8. Auflage › mehr

Checkliste für EPU

IT-Sicherheit – Checkliste für Ein-Personen-Unternehmen - 3. Auflage, Jänner 2018 › mehr

IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter

8. Auflage › mehr

wko.at/site/it-safe/mitarbeiter-handbuch.html

Veranstaltung

Webinar „Datenschutz jetzt neu angehen“

Nachlese › mehr

Was sind „TOMs“ (technische und organisatorische Maßnahmen) iSd DSGVO?

Auszug aus Art. 32 DSGVO Sicherheit der Verarbeitung

1. *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 technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:*
   - *die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;*
   - *die Fähigkeit, die **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Belastbarkeit der Systeme** und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
   - *die Fähigkeit, die **Verfügbarkeit der personenbezogenen Daten** und den **Zugang** zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*
   - *ein Verfahren zur **regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*
2. *Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die **Risiken** zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung, Verlust oder Veränderung**, ob **unbeabsichtigt oder unrechtmäßig**, oder **unbefugte Offenlegung** von beziehungsweise **unbefugten Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden –*

Zugangskontrolle	**Der Serverraum ist versperrt; der Laptop/PC wird in einem versperrten Kasten verwahrt; der Zutritt zum Serverraum wird protokolliert und es sind nur diejenigen Personen zutritts- bzw. zugriffsberechtigt, die dazu von der Leitung berechtigt wurden**
Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte	
Datenträgerkontrolle	**Die Daten sind ausschließlich auf dem einem bestimmten Laufwerk des Servers Laptop/PC gespeichert, der im .. [Bezeichnung: z.B. xxx verwahrt wird**
Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern	
Speicherkontrolle	**Die personenbezogenen Daten sind nur von Berechtigten mit Passwort zugänglich; Zugriffe werden protokolliert (need to know)**
Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten	
Benutzerkontrolle	**Der IT-Administrator vergibt die Benutzerrechte im Rahmen des Notwendigen (need to know Prinzip, dh es können nur Befugte auf Daten zugreifen)**
Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte	
Zugriffskontrolle	**Es besteht eine Passwort-Policy und diese ist den Befugten auch bekannt**
Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben	

Übertragungskontrolle	**Daten werden nur an berechtigte Empfänger (z.B. Banken im Rahmen des Zahlungsverkehrs) elektronisch übertragen; bei Verwendung der Daten für Schriftstücke gibt es ein Vier-Augen-Prinzip**
Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können	
Eingabekontrolle	**Es wird - wenn mehrere Benutzer bestehen - mitprotokolliert, welcher Benutzer auf welche Daten zu welchem Zeitpunkt zugegriffen hat; diese Protokolle stehen der IT-Administration zur Verfügung**
Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (Eingabekontrolle)	
Transportkontrolle	**Es besteht die Weisung, dass Daten nicht auf mobilen Datenträgern gespeichert werden (USB-Sticks, Smartphones); der Laptop/PC darf nur von befugten Personen verwendet und transportiert werden. Wenn der Laptop z.B. zur Reparatur außer Haus gebracht wird, ist sichergestellt, dass der Empfänger die Daten vertraulich behandelt (Vertrag)**
Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können	
Wiederherstellung	**Es besteht eine Sicherung der Daten (Form der Sicherung: ..., zeitlicher Abstand der Sicherung: ...). Die IT-Administration ist in der Lage, die Sicherung zeitnahe einzuspielen; das Szenario wird in periodischen Abständen getestet**
Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können	
Datenintegrität	**Es erfolgen die notwendigen Updates des Betriebssystemes und der sonstigen Programme; es gibt einen ausreichend Schutz gegen Intrusion und Viren. Es ist im Rahmen des Prozesses der Aufnahme neuer betroffener Personen sichergestellt, dass es einen Auftrag (...) gibt**
Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden und gespeicherte personenbezogene Daten	

Was gibt es Neues in der DSGVO ?

VV / VVT

DSFA

DSBA

DBN

Sanktionen

Das Verzeichnis von Verarbeitungstätigkeiten

Wer muss es erstellen?

Das “Musterverzeichnis”

Verzeichnis von Verarbeitungstätigkeiten (VV)

- Ausnahme: < 250 MA, kein Risiko, Verarbeitung gelegentlich, keine Art. 9 / 10 Daten
- Inhalt:
  - **Namen** und **Kontaktdaten** des Verantwortlichen
  - **Zweck(e)** der Verarbeitung
  - Kategorien der betroffenen **Personen** & **Daten**
  - Kategorien der **Empfänger**
  - **Löschungsfrist**
  - technische u organisatorische Maßnahmen (**TOMs**)

Name und Anschr	Nr	(gemeinsam) Verantwortliche	Zweck	Betroffenengruppe	Datenkategorien
	Auftragsabwicklung				
		Geschäftsleitung	**Geschäftsabwicklung (allgemein) inklusive der notwendigen Korrespondenz mit Kunden, Lieferanten und Anbietern der vertriebenen Dienstleistungen und Produkte sowie Ablage / Speicherung der personenbezogenen Daten**	Kunden Interessenten Mitarbeiter / Beschäftigte Werkvertragsnehmer Ansprechpartner bei Kunden / Dienstleistern / Versicherungen / Banken Prämienzahler sonstige an der Vertragsbeziehung beteiligte Personen (z.B. Begünstigte)	Kundennummer oder sonstiges individuelles Kennzeichen Stammdaten Kontaktdaten Kommunikationsdaten Daten zum Vertragsverhältnis (z.B. auch Gesundheitsdaten bei Unfall-, Kranken- und Lebensversicherungen) Daten über Vertragsanbahung / Beratungsprotokolle Daten über die Vertragsabwicklung inkl. Vorschreibungen und Zahlungsdaten Daten über die Vertragsbeendigung (z.B. auch Storno) Daten über Versicherungsfälle (inkl. Gesundheitsdaten bei Schadensfällen Bankverbindung der Kunden Daten über die Vertragsbeendigung (z.B. auch Storno) Daten über Versicherungsfälle (inkl. Gesundheitsdaten bei Schadensfällen Bankverbindung der Kunden
				Interessenten Prämienzahler Ansprechpartner bei Kunden und Lieferanten sonstige an den Vertragsbeziehungen beteilgte dritte Personen (z.B. Begünstigte)	

Datenkategorien	Empfänger Intern	Empfänger Extern	Übermittlung Drittstaaten	Rechtsgrundlage*	Löschfrist / Aufbewahrungsd	Techn. U. organisatorische Maßnahmen (Abweichungen)
Kundennummer oder sonstiges individuelles Kennzeichen Stammdaten Kontaktdaten Kommunikationsdaten Daten zum Vertragsverhältnis (z.B. auch Gesundheitsdaten bei Unfall-, Kranken- und Lebensversicherungen) Daten über Vertragsanbahung / Beratungsprotokolle Daten über die Vertragsabwicklung inkl. Vorschreibungen und Zahlungsdaten Daten über die Vertragsbeendigung (z.B. auch Storno) Daten über Versicherungsfälle (inkl. Gesundheitsdaten bei Schadensfällen Bankverbindung der Kunden	unterschiedliche Abteilungen je nach den betrieblichen organisatorischen Notwendigkeiten	Versicherungen, Banken als Vertragspartner des Kunden im Rahmen der Vermittlung Kunden selbst Haftungsdach freie Mitarbeiter Partner, Tochtergesellschaften oder verbundene Unternehmen z.B. im Rahmen von Büro-gemeinschaften	grunsätzlich nein, nur dann wenn, die Versicherung oder Bank (als Vertragspartner des Kunden) im EWR-Ausland ihren Sitz hat (Standardvertragsklauseln)	Vertrag gesetzliche Verpflichtung bei Newsletter: Einwilligung bei Werbemaßnahmen per Post: berechtigtes Interesse	7 Jahre nach Ende des Geschäftsjahres, in dem die Daten angefallen sind (§ 132 BAO) und darüberhinaus zur Geltendmachung von Ansprüchen oder Abwehr von Ansprüche (z.B. auch bei steuerlichen Fragen) bei Newsletter / Werbemaßnahmen: 3 Jahre nach dem letzten Kontakt	keine
Daten über die Vertragsbeendigung (z.B. auch Storno) Daten über Versicherungsfälle (inkl. Gesundheitsdaten bei Schadensfällen Bankverbindung der Kunden		Gutachter, Rechtsvertreter, Steuerberater, Wirtschaftsprüfer Finanzamt und sonstige Behörden / Ombudsstelle an einem Schadensfall beteiligte Personen				

Zweck	Zweck	Zweck
Rechnungswesen Verarbeitung und Übermittlung von Daten im Rahmen einer Geschäftsbeziehung mit Kunden und Lieferanten,	Kundengewinnung und Kundenbetreuung Information von Kunden durch Newsletter Website-Analyse-Tool Auswertung der Websitenutzung Reportzusammenstellung Sicherstellung der IT- und Netzwerksicherheit Cookies zur Auspielung von Banner-Werbung und sonstiger Werbung auf Websiten	Verwaltung der Beschäftigten im Rahmen des Beschäftigungsverhältnisses

Wie erstellt man ein Verzeichnis?

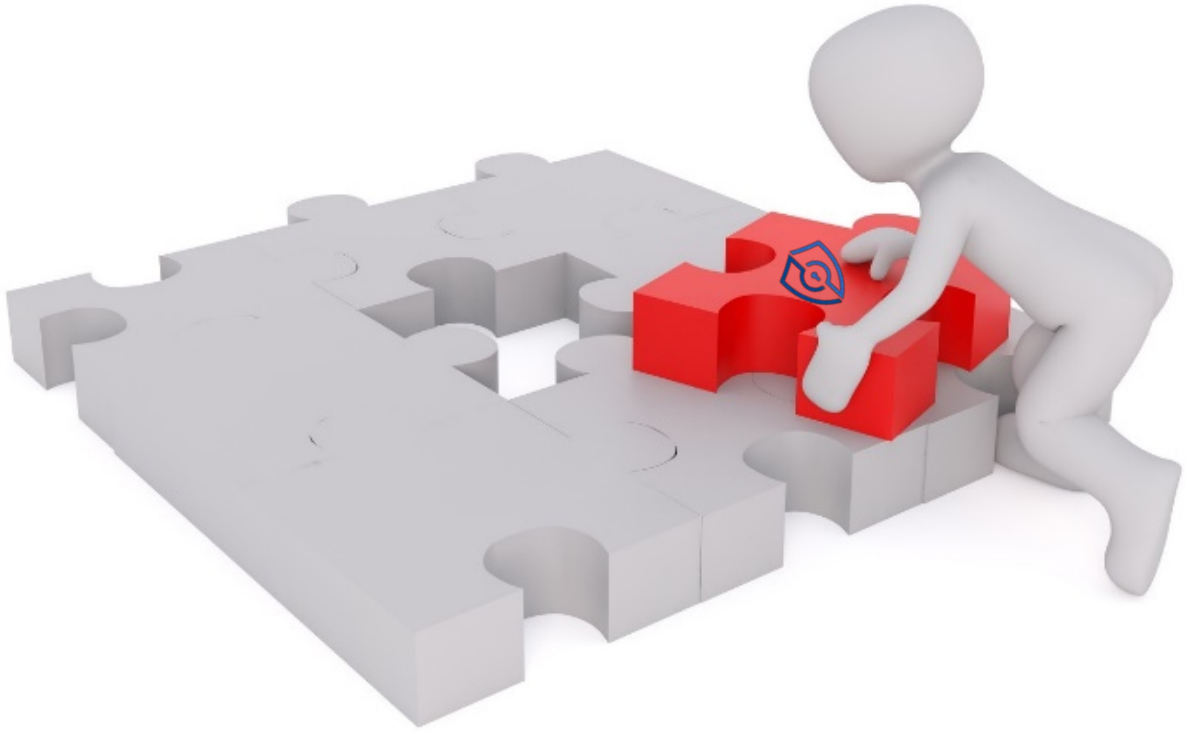
- Suchen Sie betroffene Personen im Unternehmen
- Welche Zwecke (Unternehmensabläufe) gibt es im Unternehmen?
- Ermitteln Sie die Datenkategorien
- Definieren Sie den Datenfluss im Unternehmen und nach außen
- Wer sind Ihre Dienstleister?
- Was ist die Rechtsgrundlage der Verarbeitung?

DSGVO-Projektplan

Dr. Thomas Schweiger, LL.M. (Duke), CIPP/E
zertifizierter Datenschutzbeauftragter (DATB)

dataprotect it-recht

Strategie & Commitment mit dem Top-Management erstellen



Prüfung, ob ein Datenschutzbeauftragter (DSBA) notwendig ist?

Behörde / öffentliche Stelle?

Unternehmen, sonstige Organisation:

<u>Was ist die Kerntätigkeit?</u>
1. regelmäßige & systematische Überwachung von betroffenen Personen
2. Verarbeitung von besonderen Datenarten oder Daten über Straftaten

Ist die Tätigkeit “umfangreich” iS DSGVO?

DataManager benennen & Rssourcen bereitstellen

- Finanzmittel und Humanressourcen sind bereitzustellen
- DM übernimmt die Projektplanung & -leitung
- DM weist die „To-Dos“ zu und fordert diese zeitgerecht ein
- DM berichtet an das Board über die Fortschritte (Zwischenberichte)

Datenlandkarte erheben

Verzeichnis gem. Art 30 → Zweck → Betroffene

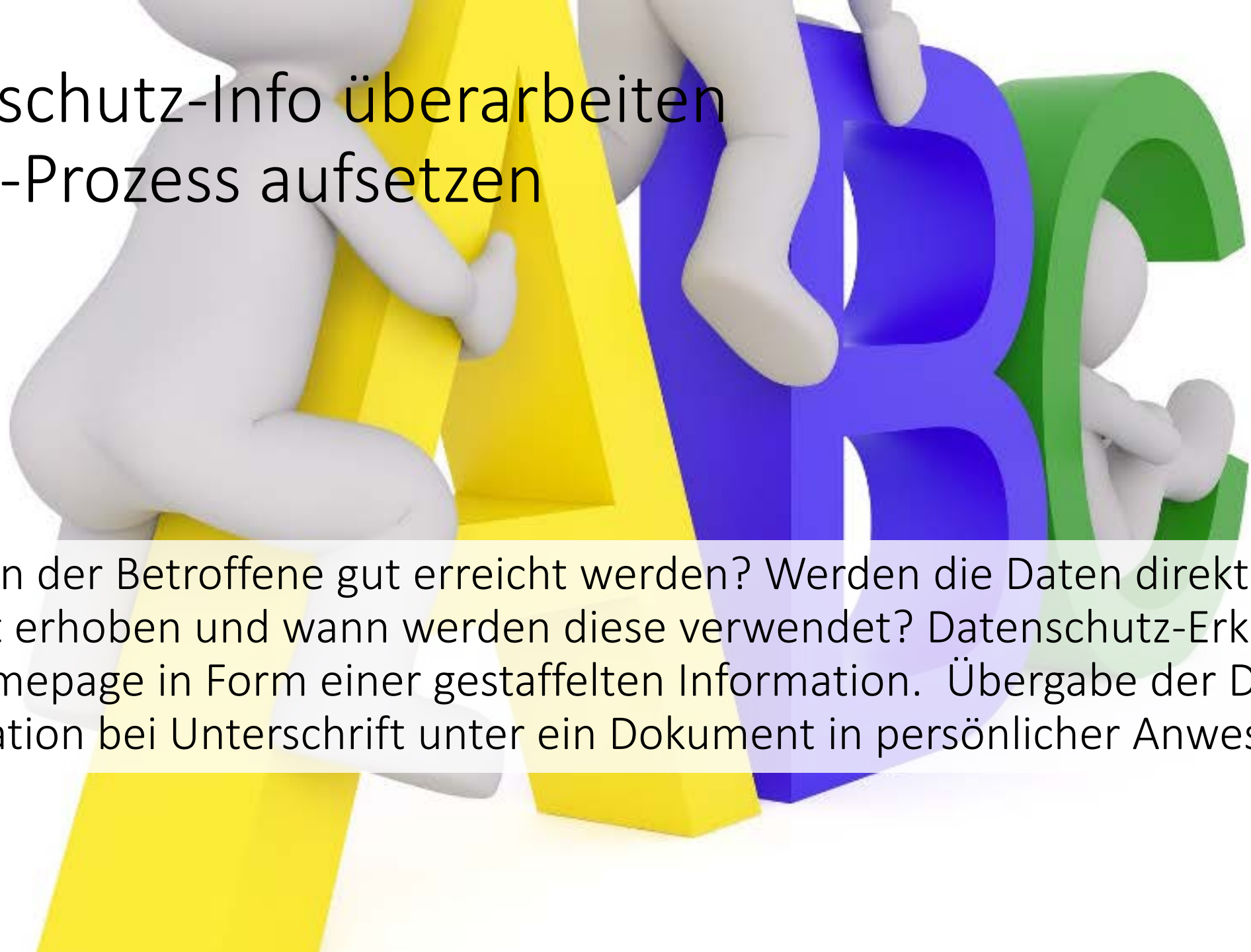
Daten → Empfänger → Drittländer

Löschfrist → TOMs

Zusätze → Rechtsgrundlage

Herkunft

Datenschutz-Info überarbeiten & Info-Prozess aufsetzen



Wo kann der Betroffene gut erreicht werden? Werden die Daten direkt oder indirekt erhoben und wann werden diese verwendet? Datenschutz-Erklärung auf der Homepage in Form einer gestaffelten Information. Übergabe der DS-Information bei Unterschrift unter ein Dokument in persönlicher Anwesenheit?

Auftragsverarbeiter prüfen

Identifikation → Kontaktaufnahme

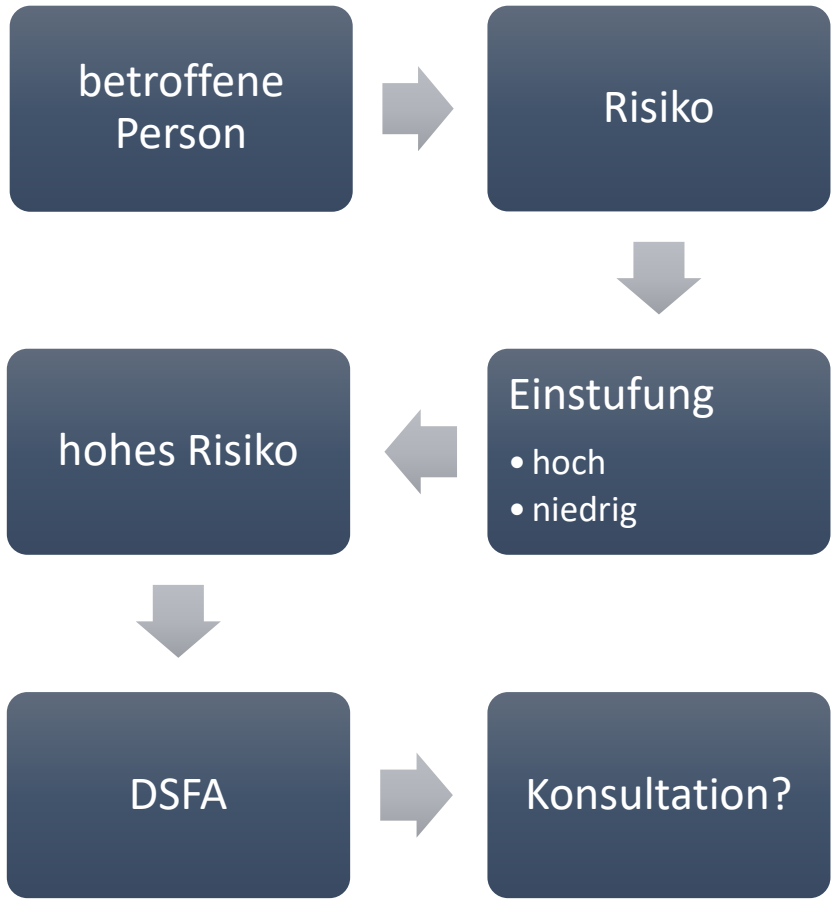
↓

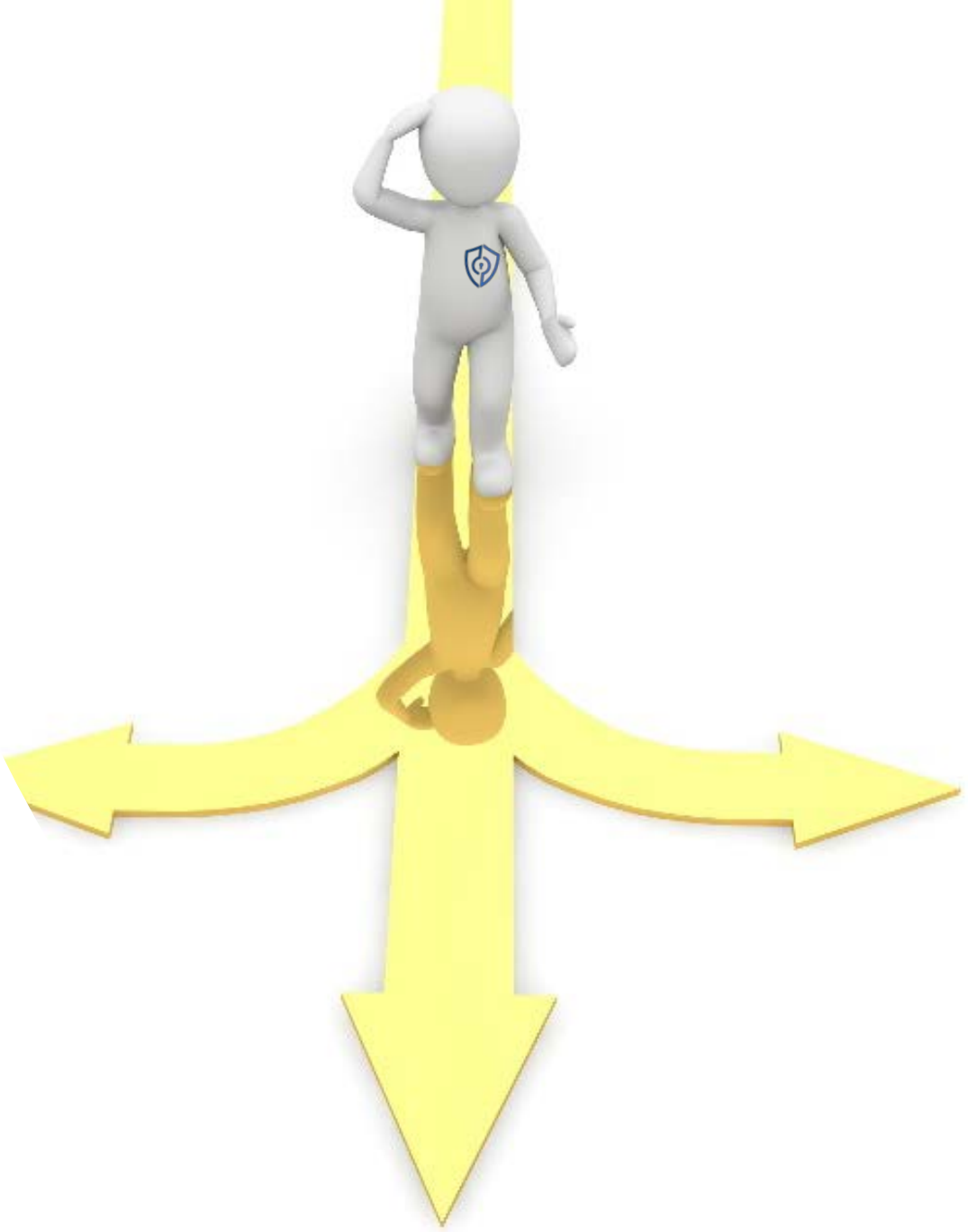
Verträge anfragen → Verträge prüfen

↓

Verträge anpassen

Prüfung, ob eine Datenschutz-Folgenabschätzung (DSFA) notwendig ist?





Data Breach Notification – Prozess erstellen

Meldung an die Aufsichtsbehörde (wenn Risiko nicht ausgeschlossen)

Meldung an die betroffenen Personen (wenn hohes Risiko)

Leitfaden für Betroffenenrechte erstellen

Bestätigung & Auskunft
Berichtigung, Einschränkung & Löschung
Datenübertragbarkeit
Eingriff in automatisierte Entscheidungsfindung
Widerruf & Beschwerde

Awareness schaffen

Beschäftigte schulen

Review-Cycle implementieren

Danke für die Aufmerksamkeit

@dataprotect_at

dataprotect

Newsletter / Blog:
www.dataprotect.at