

DATENSCHUTZ BEI VEREINEN

Datenschutz nach der Datenschutz-
Grundverordnung (DSGVO)

Düsseldorf, März 2023

1	Grundlagen zum allgemeinen Datenschutz
2	Grundlagen zum Arbeitnehmerdatenschutz
3	Beispiele aus Ihrer täglichen Arbeit mit Daten

Woraus resultiert das Datenschutzrecht?



- Datenschutz-Grundverordnung (DSGVO) = Verordnung der Europäischen Union
- Deutsches Bundesdatenschutzgesetz (BDSG) = Ergänzung der DSGVO
- DSGVO ist „Magna Carta“ des Datenschutzrechts; BDSG regelt nur Spezialfälle

Woraus resultiert das Datenschutzrecht?

- DSGVO besteht aus 11 Kapiteln mit 99 Artikeln
- In vielen Teilen auch für Laien gut verständlich (Nachlesen!)
- Für Sie besonders relevant:

Kapitel 1: Art. 1 – 4 Allgemeine Bestimmungen

Für welche Daten gilt die DSGVO? Was bedeuten die Begriffe?

Kapitel 2: Art. 5 – 11 Grundsätze der Datenverarbeitung

Wann ist Datenverarbeitung erlaubt?

Kapitel 3: Art. 12 – 23 Rechte der betroffenen Person

Wann besteht ein Recht auf Löschung oder Auskunft?

Kapitel 4: Art. 24 – 43 Verantwortlicher + Auftragsverarbeiter

Welche Sicherheitsmaßnahmen und welche Verträge sind nötig?

Für was gilt die DSGVO?

Personenbezogene Daten...

...sind alle Informationen, durch die eine natürliche Person direkt oder indirekt identifiziert werden kann.

Keine personenbezogenen Daten...

...sind Daten über den Verein, wie z.B. „Achse e.V., Drontheimer Str., Berlin “; in den Daten über einen Verein können aber personenbezogene Daten enthalten sein, wie z.B. „Mitarbeiterin Mirjam Mann des Achse e.V.“

Für was gilt die DSGVO?

Beispiele....

Daten, die immer eine Identifizierung ermöglichen:

z.B. Name, Sozialversicherungsnummer, Steuer-ID, Personalnummer, Personalausweisnummer, Reisepassnummer, E-Mail-Adressen, IP-Adresse

Daten, die im Zusammenspiel eine Identifizierung ermöglichen:

z.B. Kombination aus Geburtsdatum, Adresse, Bankdaten, Beruf

Daten, die ein „Wiedererkennen“ ermöglichen (Name nicht notwendig!):

z.B. Bilder und Videos mit Personen

(Alle) Daten, die mit der Identifizierbarkeit zusammenhängen:

z.B. Schuhgröße, Vorstrafen, Krankendaten, Religionsangehörigkeit, Politische Meinungen, Herkunft, genetische oder biometrische Daten, Leistungsdaten

Für wen gilt die DSGVO?

Das Datenschutzrecht gilt für jeden, es sei denn...

- es handelt sich um ungeordnete, analoge Dokumente (z.B. Notizzettel)
- es handelt sich um Daten für persönliche/familiäre Tätigkeiten (z.B. private Kontakt- und Freundeslisten im Mobiltelefon)

„Verantwortlicher“ im Sinne des Datenschutzrechts ist...

...die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

... **also der VEREIN, egal wie klein!!!**

Uns alle trifft die Pflicht, das Datengeheimnis zu wahren!

Was heißt Datenverarbeitung?

Datenverarbeitung....

Erheben

Erfassen

Ordnen

Speichern

Anpassen

Auslesen

Abfragen

Verwenden

Übermitteln (= Dritten/Externen offenlegen)

... darf ich das?

Wie dürfen diese Daten verarbeitet werden?

Verbot mit Erlaubnisvorbehalt...

... Datenverarbeitung verboten, es sei denn es wird durch das Gesetz erlaubt



Wie dürfen diese Daten verarbeitet werden?

Erlaubnisse zur Datenverarbeitung

(Art. 6 DSGVO)

Einwilligung des Betroffenen

Erforderlich zur Vertragserfüllung

Rechtliche Verpflichtung

Lebenswichtiges Interesse

Aufgabe im öffentlichen Interesse

Interessenabwägung



Erforderlich zur Vertragserfüllung?

„die Verarbeitung ist für die Erfüllung eines Vertrags [...] oder zur Durchführung vorvertraglicher Maßnahmen erforderlich [...]“



Erforderlich zur Vertragserfüllung?

„die Verarbeitung ist für die Erfüllung eines Vertrags [...] oder zur Durchführung vorvertraglicher Maßnahmen erforderlich [...]“

Geburtsdatum des Kunden wird erhoben und in Datenbank gespeichert, um Glückwünsche per E-Mail zu schicken



Praktisch, aber nicht erforderlich



Erforderlich zur Vertragserfüllung?

„die Verarbeitung ist für die Erfüllung eines Vertrags [...] oder zur Durchführung vorvertraglicher Maßnahmen erforderlich [...]“

Adresse des Kunden wird gespeichert und an Logistikunternehmen für Versendung übermittelt



Erforderlich zur Vertragsabwicklung

Wann brauche ich eine Einwilligung?

...immer dann, wenn die Datenverarbeitung nicht zur Vertragserfüllung erforderlich ist und kein überwiegendes Interesse für unseren Verein an der Datenverarbeitung besteht.

Newsletter

Geburtstagslisten

Bonitätsabfragen

Persönlichkeitsprofile

Veranstaltungsfotos

Wie hole ich eine **Einwilligung** ein?

Nachweisbar

Schriftlich oder elektronisch, nicht mündlich

Freiwillig

Keine Kopplung mit Vertragsleistung; keine Zwangslage

Informiert

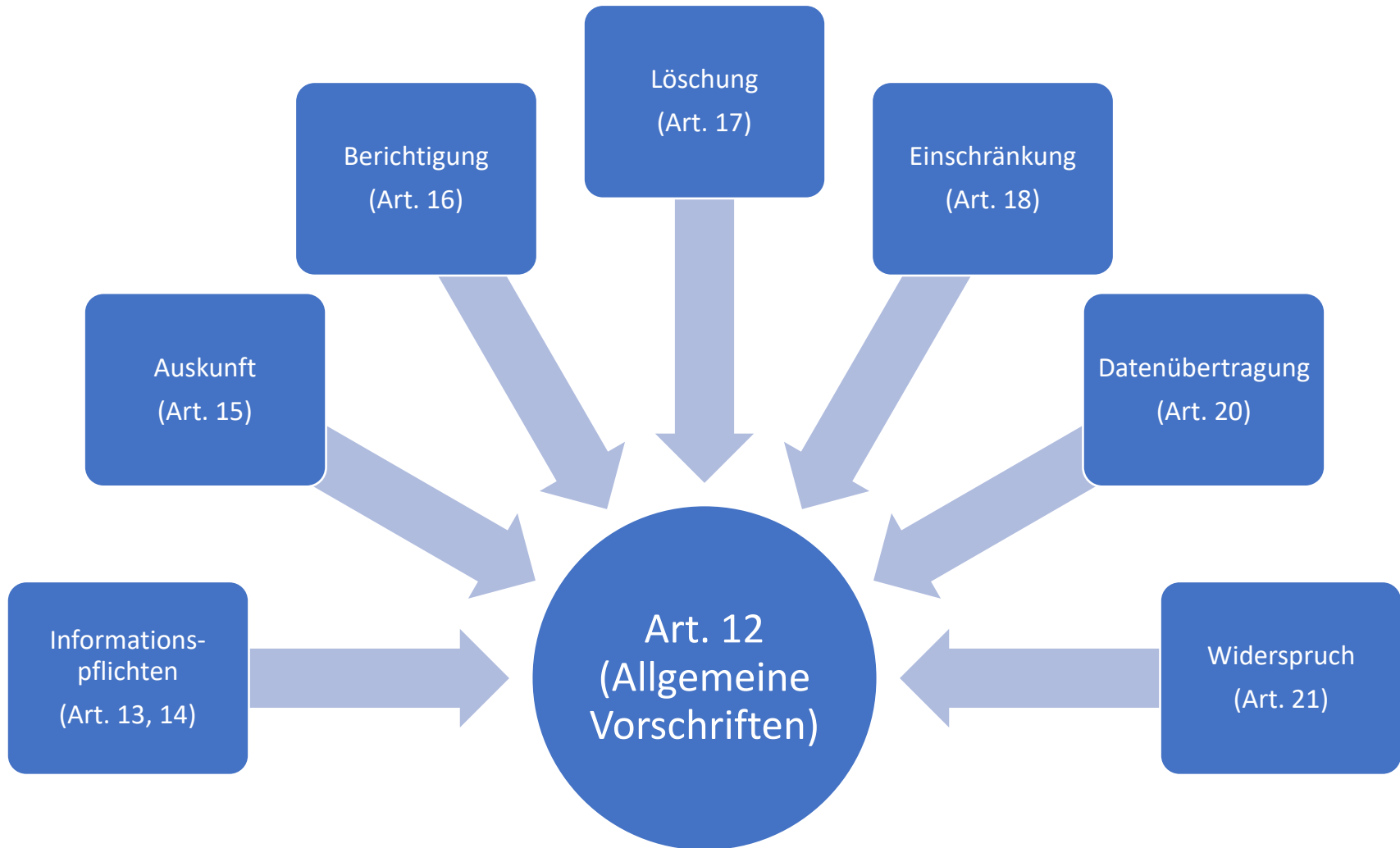
Welche Daten? Welcher Zweck? Empfänger?

Unmissverständlich

Ausdrückliches Handeln; Opt-in; kein Opt-out

Datenschutzbeauftragten einbeziehen!

Welche Betroffenenrechte gibt es?



Was tun, wenn ein **Betroffener** anfragt?

Kunde Max Mustermann fordert per E-Mail Auskunft über seine Daten....

Unser Unternehmen ist gesetzlich verpflichtet, unverzüglich zu reagieren

- ... dokumentieren Sie den Eingang der Anfrage
- ... vergewissern Sie sich über die Identität des Anfragenden
- ... schalten Sie den Datenschutzbeauftragten ein
- ... Koordinieren Sie mit dem Datenschutzbeauftragten die Beantwortung
- ... dokumentieren Sie wann und wie die Anfrage beantwortet wurde

„Nichts-Tun“ kann für unser Unternehmen schwerwiegende Folgen haben; nach Ablauf von einem Monat ab Anfrage drohen...

- ... Bußgelder
- ... Maßnahmen der Aufsichtsbehörden
- ... Abmahnungen durch den Rechtsanwalt des Betroffenen

Was gilt bei Einschaltung von Dienstleistern?

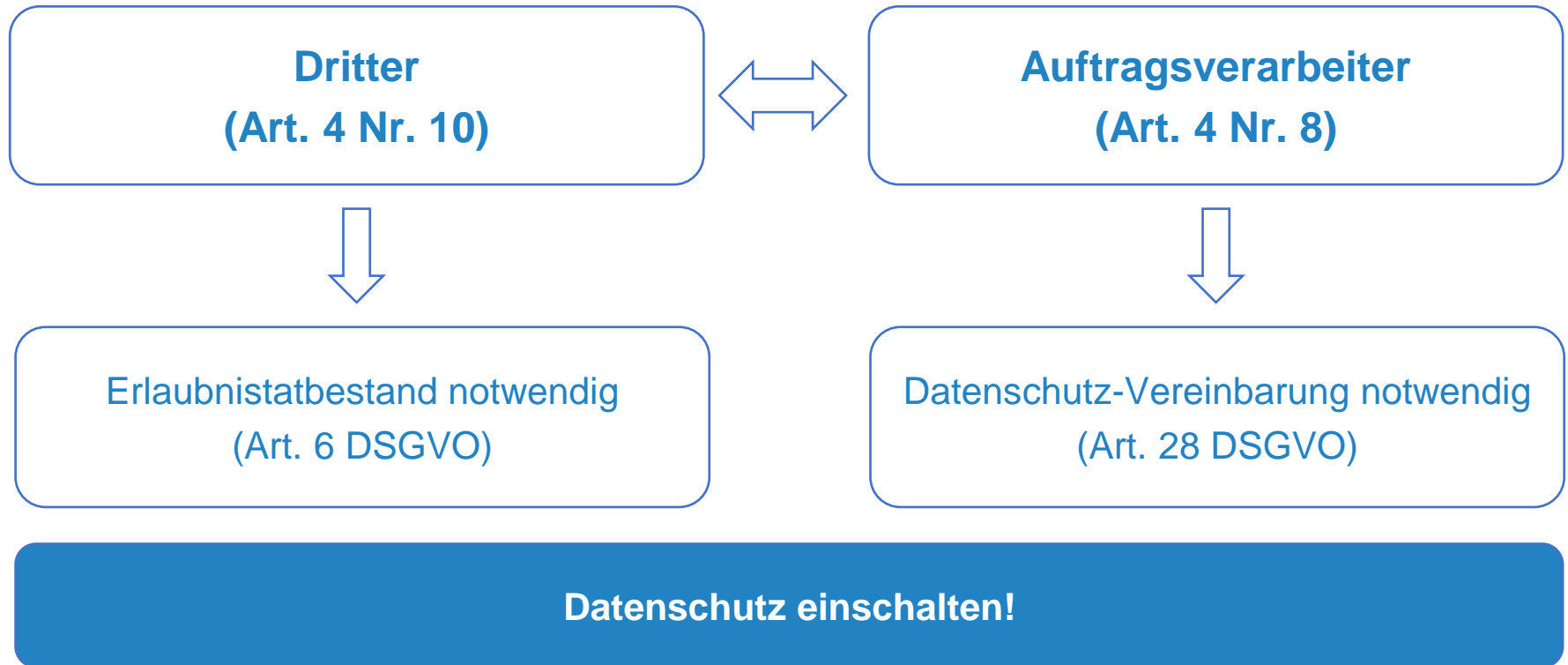
Beispiele:

- Marketingagentur wird mit Kundenmailings beauftragt
- Bestellung von Cloud-Speicherplatz für Kundendatenbank geplant
- Online-Software (SaaS, ASP) wird eingesetzt
- Dienstleister übernimmt Personenkontrollen / Videoüberwachung
- EDV-Dienstleister bekommt Remote-Zugriff auf Datenbanken

Dienstleister sind in der Regel sog. **Auftragsverarbeiter**



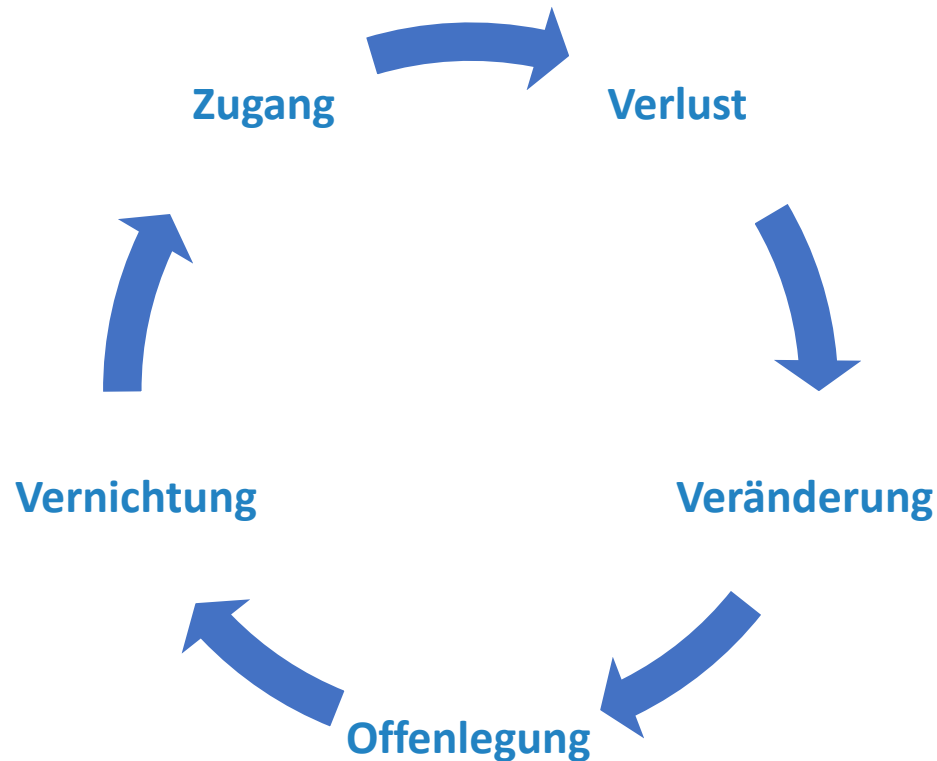
Was gilt bei Einschaltung von Dienstleistern?



Was bedeutet Datensicherheit?

Unser Verein ist verpflichtet, technische und organisatorische Maßnahmen (TOMs) zu treffen, um ein dem Risiko angemessenes Schutzniveau für die personenbezogenen Daten zu gewährleisten

Schutz der personenbezogenen Daten vor....



Was bedeutet Datensicherheit?

Datensicherheit betrifft nicht nur unternehmensweite Maßnahmen...

Verschlüsselung von Daten/Netzwerken; Passwort-Policy; Rechtevergabe für Mitarbeiter; Festlegung der Zugriffsberechtigungen; Virens Scanner; Firewalls; Datentrennung; Pseudonymisierung; Sicherungskopien und Backups; Protokollierung von Eingaben/Löschungen; Brandmeldeanlagen; Notfallpläne; Soft- und Firmwareupdates; Sicherheitstrainings und Schulungen; IT-Sicherheitskonzepte; Evaluierung der Maßnahmen

...sondern auch Ihr ganz persönliches Verhalten am Arbeitsplatz

Sperren Sie Ihren PC beim Verlassen (Tastenkombination „Windows“ + „L“); Verwahren Sie Ihre Schlüssel zum Büro, Schreibtisch usw. sicher; Verschließen Sie Unterlagen mit personenbezogenem Daten bei Abwesenheit (Schrank, Schreibtisch); Schreddern Sie Unterlagen mit personenbezogenen Daten; Geben Sie alte/defekte Datenträger zur datenschutzgerechten Vernichtung ab; Installieren Sie keine private Software oder Datenträger (z.B. USB-Sticks); Wählen Sie ein sicheres Passwort und halten Sie es geheim; Löschen Sie nicht mehr benötigte Daten/E-Mails/Ordner; Lassen Sie Besucher nicht unbeaufsichtigt mit Zugriffsmöglichkeiten auf Ihre Unterlagen

Was passiert, wenn ich ein **Datenleck** feststelle?



**Auslöser der Meldepflicht:
Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12)**

Was passiert, wenn ich ein **Datenleck** feststelle?

- Wir haben **nur 72 Stunden Zeit**, der Aufsichtsbehörde den Vorfall zu melden
- „Nichts-Tun“ kann für unser Unternehmen zu Bußgeldern bis zu 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes führen
- Melden Sie den Vorfall **sofort** unserem Datenschutzbeauftragten, wenn möglich mit:
 - Beschreibung der Verletzung
 - Zahl der Betroffenen
 - Zahl der Datensätze
 - Möglichen Folgen des Datenlecks



1

Grundlagen zum Datenschutz

2

Grundlagen zum Arbeitnehmerdatenschutz

3

Beispiele aus Ihrer täglichen Arbeit mit Daten

Wieso sind **Beschäftigtendaten** besonders?

- Auch die Daten unserer Mitarbeiter sind personenbezogene Daten

Personalnummer, Adresse, Geburtstag, Familienstand, Telefonnummer, Gehalt, Eingruppierung, Sozialdaten, Kfz-Kennzeichen, Abschlüsse, Leistungsdaten

- Arbeitnehmerdaten enthalten häufig besonders geschützte Daten, die nur unter sehr engen Bedingungen verarbeitet werden dürfen

Gewerkschaftszugehörigkeit, Gesundheits- / Krankendaten, Religionszugehörigkeit, Rassische / ethnische Herkunft, Biometrische Daten (Finderabdruck)

- Arbeitnehmerdaten sind auch dann geschützt, wenn Sie nicht digitalisiert verarbeitet oder in einem Dateisystem gespeichert werden

Handschriftliche Beurteilungen durch den Vorgesetzten; Visitenkarten; Notizen nach einem Personalgespräch; Ausgehängte Geburtstagslisten

Wann darf ich **Beschäftigtendaten** verarbeiten?

Wenn dies erforderlich für das Beschäftigungsverhältnis ist...

Bankverbindung zur Überweisung des Gehalts; Leistungsdaten, Abschlüsse und Qualifikationen zur Beurteilung der Eignung/Befähigung; Abmahnungen und Fehlverhalten für später ggf. notwendige Kündigung

...eine Betriebsvereinbarung mit dem Betriebsrat vorliegt...

Datenübermittlung innerhalb der Unternehmen unserer Gruppe; Videoüberwachung unserer Unternehmensgeländes; Fingerabdruckkontrolle in besonders sensiblen Bereichen; Datenverarbeitung der Zeiterfassung

... oder eine freiwillige Einwilligung unserer Mitarbeiter eingeholt wurde.

Testfrage zur Freiwilligkeit: Gibt es für den Mitarbeiter durch die Einwilligung einen Vorteil oder verfolgen wir zumindest gleichartige Interessen?

Wann erfolgt die Einwilligung freiwillig?

Beispiele

1. Gesundheitsmanagement zur Gesundheitsförderung

Vorteil

2. Erlaubnis zur Privatnutzung von IT-Systemen

Vorteil

3. Nutzung von Fotos für das Intranet

Gleichart. In.

4. Abfrage von Krankheitsdiagnosen bei Versicherung

Nachteil

5. Videoüberwachung der Toilettenräume

Nachteil

Überblick

1

Grundlagen zum Datenschutz

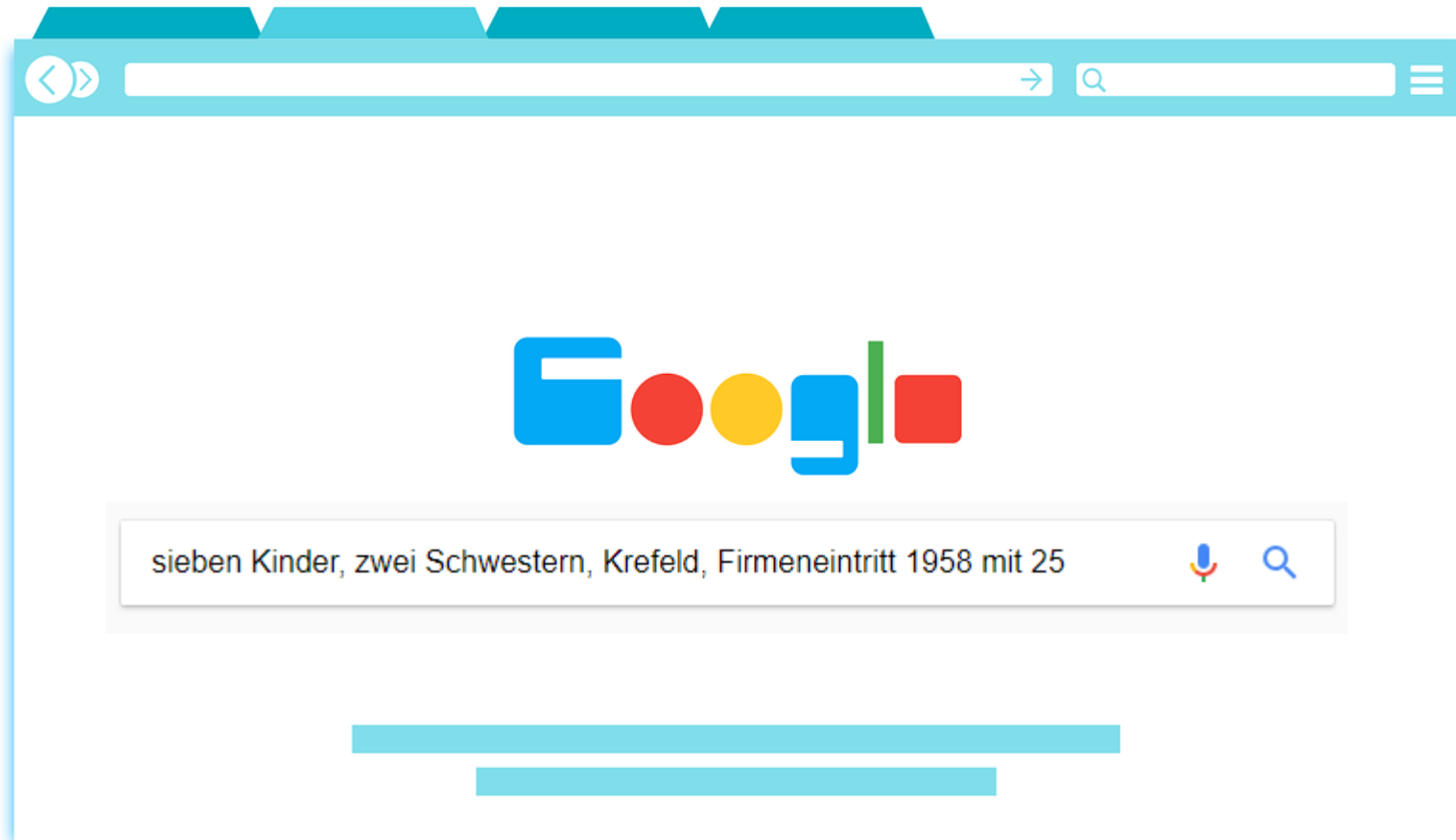
2

Grundlagen zum Arbeitnehmerdatenschutz

3

Beispiele aus Ihrer täglichen Arbeit mit Daten

Fallbeispiel 1: Personenbezogene Daten



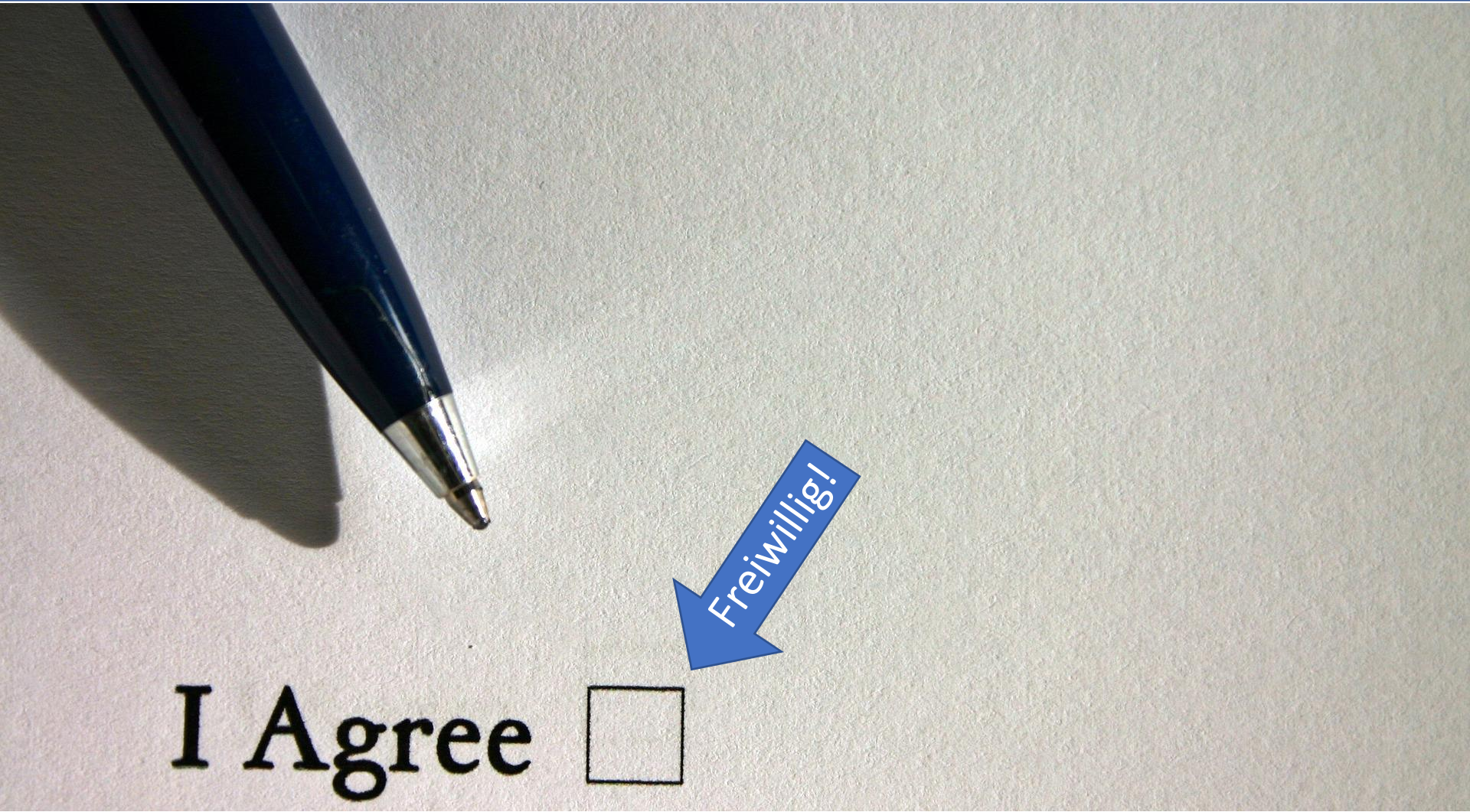
Fallbeispiel 2: Geburtstagslisten



- Max Müller, 05.03.
- Petra Muster, 21.04.
- Klaus Schmitz, 08.06.
- Gudrun Meier, 03.07.
- Jan Müller, 30.08.
- Dieter Weber , 06.09.
- Inga Fischer, 11.10.
- Alex Koch, 22.11.
- Sara Becker, 24.12.

Erforderlich für das
Beschäftigungsverhältnis?

Fallbeispiel 2: Geburtstagslisten



Fallbeispiel 3: Datenübermittlung an Dritte

2. Angaben zu den persönlichen Daten der Arbeitnehmerin/des Arbeitnehmers

Familienname: _____
Vorname: _____
Straße: _____ Hausnummer: _____
Anschriфтenzusatz: _____
Postleitzahl: _____ Wohnort: _____
Rentenversicherungsnummer (wenn nicht bekannt, Geburtsdatum): _____

2.1 Lohnsteuerabzugsmerkmale im Lohnsteuerabzugsverfahren zu Beginn des Jahres, in dem das Beschäftigungsverhältnis endete

Jahr: _____ Lohnsteuerklasse: _____ ggf. Faktor: _____ Zahl der Kinderfreibeträge: _____

Hinweis: Hat das Arbeitsverhältnis im laufenden Jahr begonnen, bitte Eintragungen bezogen auf den Beginn des Arbeitsverhältnisses vornehmen.

Erfolgt später Änderungen? Ja Nein

Wenn ja: mit Wirkung ab: _____ Lohnsteuerklasse: _____ ggf. Faktor: _____ Zahl der Kinderfreibeträge: _____

3. Angaben zum Beschäftigungsverhältnis

(bei den Fragen 3.1 - 3.3 sind Angaben für die letzten 5 Jahre vor dem Ende des Beschäftigungsverhältnisses erforderlich)

3.1 Die Arbeitnehmerin/Der Arbeitnehmer war innerhalb der letzten 5 Jahre beschäftigt

von: _____ bis: _____ zuletzt als: _____

letzter Beschäftigungsort: _____

3.2 Das Arbeitsverhältnis hat geendet zum: _____

BA II 2 - 03.17



Fallbeispiel 3: Datenübermittlung an Dritte

Zur Erinnerung: Verbot mit Erlaubnisvorbehalt...

... Datenverarbeitung verboten, es sei denn es wird durch das Gesetz erlaubt



Fallbeispiel 3: Datenübermittlung an Dritte

Bundesagentur für Arbeit **Arbeitsbescheinigung**
nach § 312 Drittes Buch Sozialgesetzbuch (SGB III)

Kundennummer

Betriebsnummer des Arbeitgebers
(s. Hinweis zum Vordruck „Arbeitsbescheinigung“)

Betriebsnummer bitte immer eintragen!

(1) Der Arbeitgeber hat auf Verlangen [...] der Bundesagentur alle Tatsachen zu bescheinigen, die für die Entscheidung über den Anspruch auf Arbeitslosengeld oder Übergangsgeld erheblich sein können (Arbeitsbescheinigung); dabei hat er den von der Bundesagentur hierfür vorgesehenen Vordruck zu benutzen.

DSGVO?!

Art. 6 Abs. 1 DSGVO: Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

Fallbeispiel 4: Nutzung von Visitenkarten



Gilt das Datenschutzrecht? Darf ich die Daten speichern?

Fallbeispiel 4: Nutzung von Visitenkarten



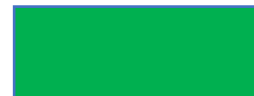
Fallbeispiel 4: Nutzung von Visitenkarten



Speichern und Nutzen für Vertragserfüllung (Vertragsansprechpartner)



Speichern und Nutzen für Vertragsverhandlungen



Speichern und Nutzen für Newsletter/Werbemails



* Es sei denn, die Visitenkarte wurde explizit hierfür übergeben (= Einwilligung); dann aber Nachweisbarkeit problematisch!

Fallbeispiel 5: Umgang mit Bewerbungen



Fallbeispiel 5: Umgang mit Bewerbungen

„Personenbezogene Daten von Beschäftigten dürfen [...] verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses [...] erforderlich ist“ - § 26 BDSG



Nutzung zur Auswahl durch Personalabteilung / -verantwortliche



Bewerbung an alle interessierten Kollegen weiterleiten



Speichern und Nutzen für Newsletter/Werbemails



Dauerhafte Speicherung im Ordner „Bewerberdatenbank“

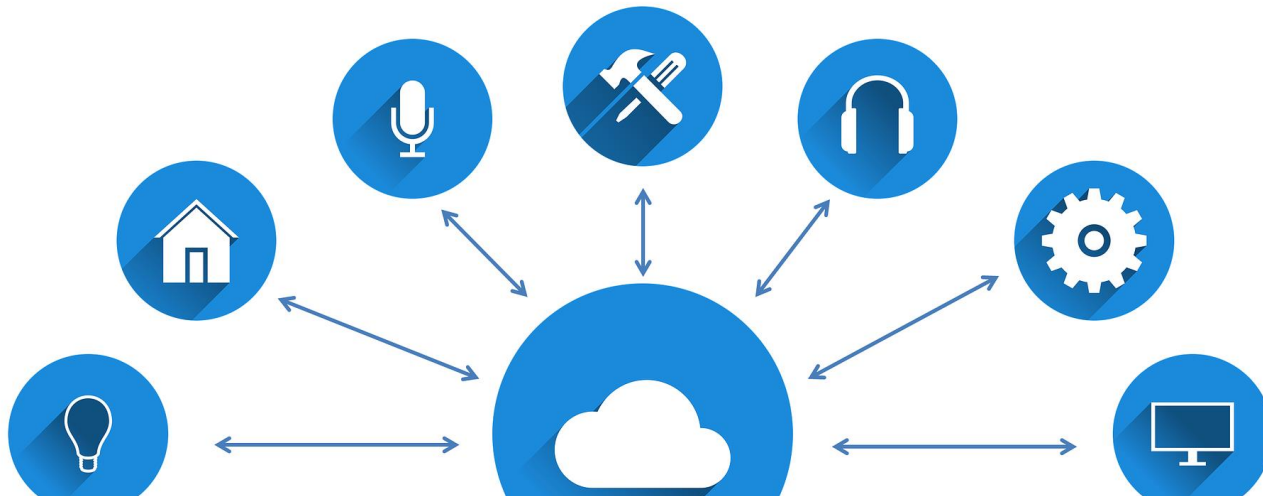


Fallbeispiel 6: Umgang mit Dienstleistern

- Das Mitglied X bittet um Bereitstellung aller Daten zum Download
- Das Projektteam Y möchte eine zentrale Plattform für alle Daten
- Mitarbeiter Z will einen Scan mit Bewerbungen weiterleiten

Einfachste Lösung:

„Mal eben“ die private Cloud (Dropbox, Google Drive, WeTransfer)?



Fallbeispiel 6: Umgang mit Dienstleistern

Nutzungsbedingungen verbieten häufig die kommerzielle Nutzung



Anbieter räumen sich häufig weitgehende Nutzungsrechte ein



Daten dürfen nur mit Datenschutzvereinbarung übermittelt werden

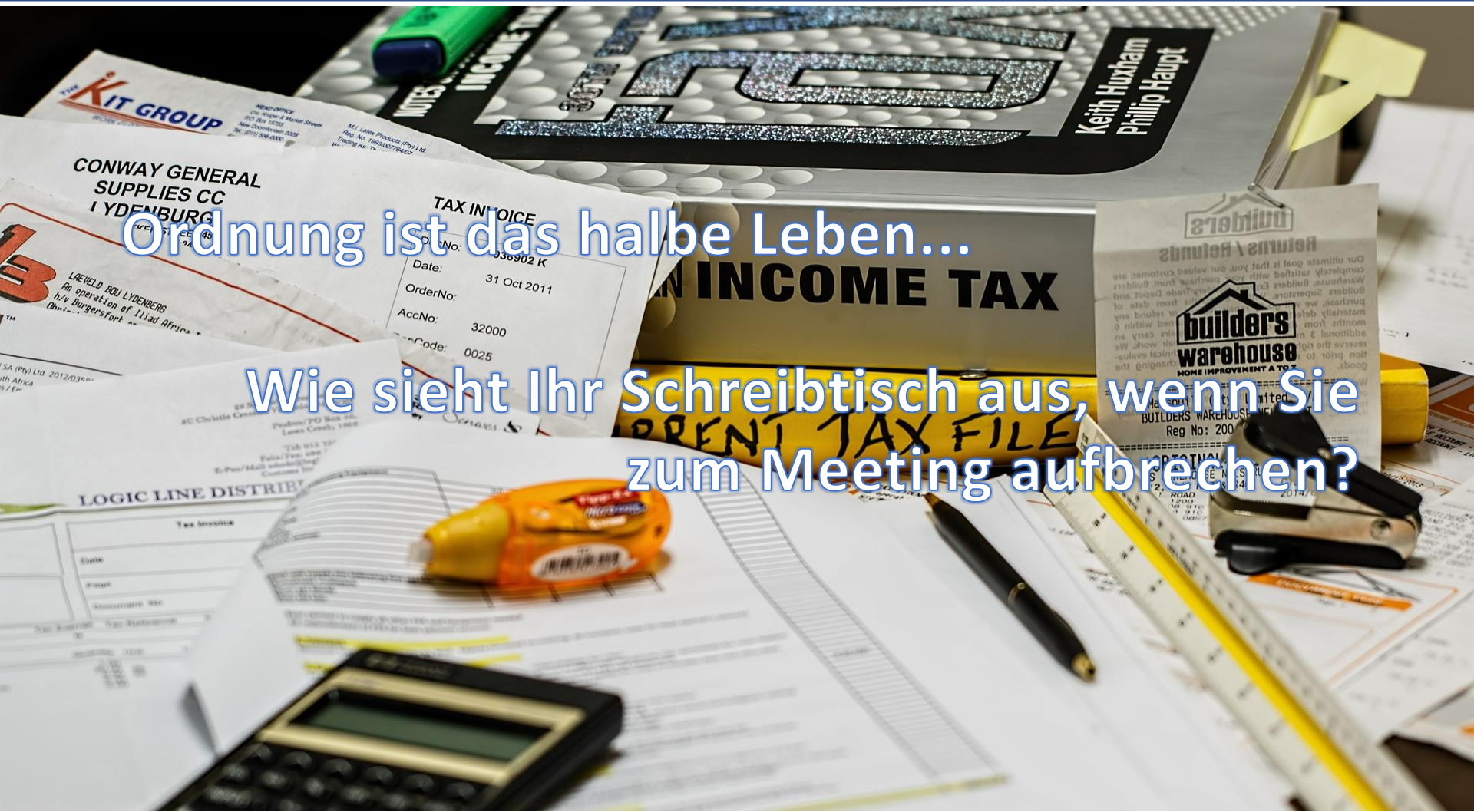


Bußgeldrisiko für unser Unternehmen und Sie persönlich



Nutzen Sie nur Speicherplätze, die von unserem Unternehmen bereitgestellt werden!

Fallbeispiel 7: Datensicherheit



Ordnung ist das halbe Leben...

Wie sieht Ihr Schreibtisch aus, wenn Sie zum Meeting aufbrechen?

Fallbeispiel 7: Datensicherheit

„Clean-Desk-Policy“

1. Sperrbildschirm aktivieren (Tastenkombination „Windows“ + „L“);
2. Alle Unterlagen in Schubladen verstauen
3. Besonders sensible Daten in Schränken wegschließen
4. Nicht mehr benötigte Unterlagen direkt zum Schreddern mitnehmen
5. Passwörter / Chipkarten nicht liegen lassen

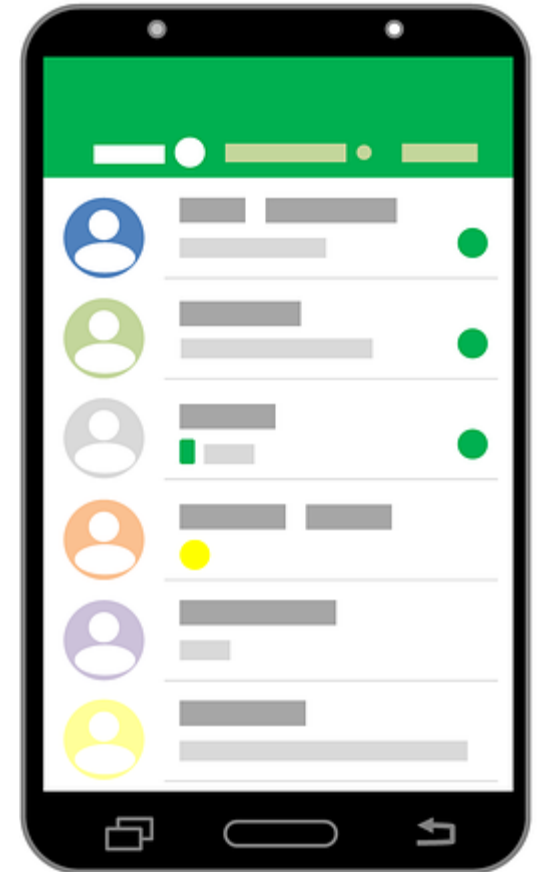
Fallbeispiel 8: Private Nutzung

Sie speichern die Adresse Ihres Arbeitskollegen, um ihm eine Postkarte aus dem Urlaub zu schicken

Sie gründen mit Ihren Arbeitskollegen eine Whatsapp-Gruppe, um sich Abends zum Tennis zu verabreden

Sie installieren Whatsapp auf Ihrem Firmenhandy, um mit der Familie aber auch Kunden in Kontakt zu bleiben

Sie speichern Kunden-Ansprechpartner trotz Firmenhandy Privat, um Kontakte schnell zur Hand zu haben



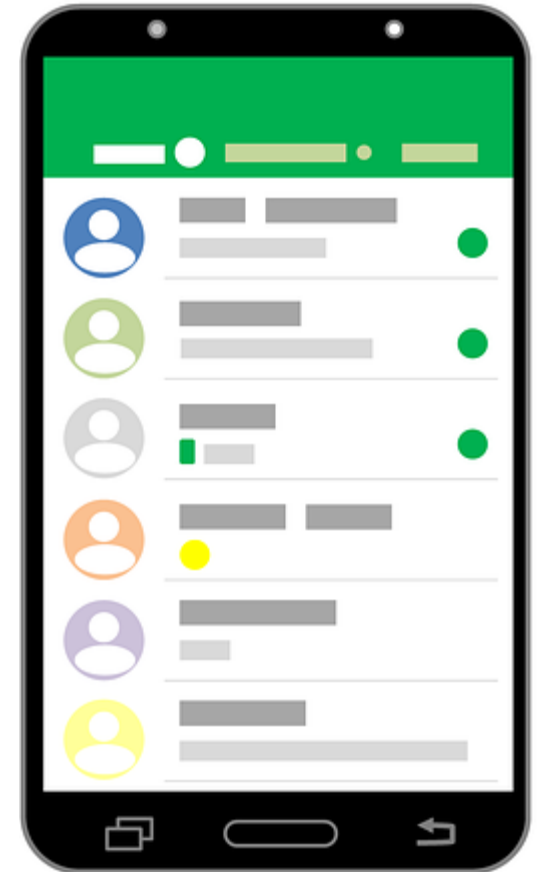
Fallbeispiel 8: Private Nutzung

Sie speichern die Adresse Ihres Arbeitskollegen, um ihm eine Postkarte aus dem Urlaub zu schicken

Sie gründen mit Ihren Arbeitskollegen eine Whatsapp-Gruppe, um sich Abends zum Tennis zu verabreden

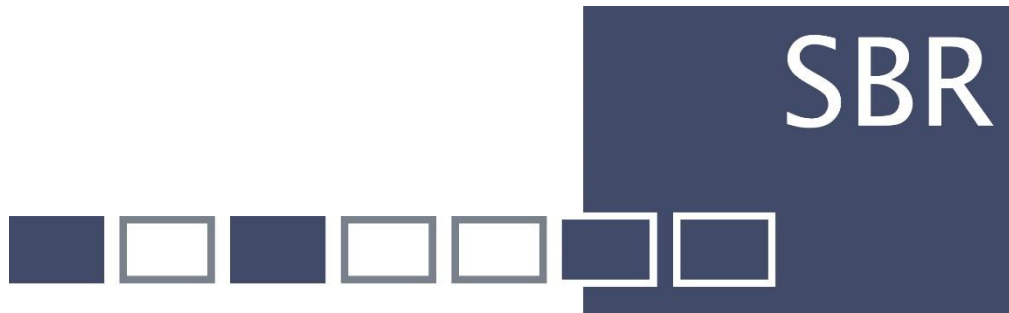
Sie installieren Whatsapp auf Ihrem Firmenhandy, um mit der Familie aber auch Kunden in Kontakt zu bleiben

Sie speichern Kunden-Ansprechpartner trotz Firmenhandy Privat, um Kontakte schnell zur Hand zu haben



- Bildnachweise: Pixabay.com jeweils unter Creative Commons CC0:
 - DSGVO-Symbol: BenediktGeyer
 - Verboten + Warnung: Clker-Free-Vector-Images
 - Approved: InspiredImages
 - Geburtstag Schleifen: maciej326
 - Gehirn: ElisaRiva
 - Paket/Versand: OpenClipart-Vectors
 - Macbook: Free-Photos
 - Schreibtisch: stevepb
 - Bewerbung: loufre
 - Visitenkarten-Hand: jarmoluk
 - Visitenkarte: DavidZydd
 - Jobcenter: andreas160578
 - Visitenkartenhalter: adnovak
 - Happy Birthday: geralt
 - I agree / Zustimmung: Catkin
 - Whatsapp Smartphone: Tumisu

Vielen Dank für die Aufmerksamkeit



Prof. Dr. Fabian Schuster

E-Mail: schuster@sbr-net.com
Tel: + 49 211 68 78 88 28
Fax: + 49 211 68 78 88 68

SBR Schuster & Partner Rechtsanwälte mbB

Goethestr. 8
40237 Düsseldorf