Informationen zum Datenschutz

Hinweis: Dieses Dokument ist eine Darstellung über die Umsetzung von Datenschutz und insbesondere der DSGVO im Unternehmen XYZ GmbH

[I] maTrix
SO SIND DATEN SICHER

Datenschutz Grundverordnung (DSGVO)

- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele
- Umsetzung im Unternehmen
- Strafen/ Sanktionen

- Gültigkeit ab dem 25.5.2018 (Ende der Übergangsfrist)
- Löst die bestehende Datenschutz Richtlinie ab (unionsweites einheitliches Recht ab jetzt)
- Das österreichische Datenschutzgesetz ist bereits angepasst
- Die DSGVO gilt für natürliche und juristische Personen, Körperschaften und sonstige Organisationen jeglicher Größe, die personenbezogene Daten verarbeiten
- Die Pflichten des Verantwortlichen sind erweitert
- Rechte Betroffener sind gestärkt
- Die Datenschutzbehörde ist mit erweiterten Befugnissen ausgestattet
- Der mögliche Strafrahmen ist massiv erhöht

[I] matrix
SO SIND DATEN SICHER

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele
- Umsetzung im Unternehmen
- Strafen/ Sanktionen

[I] matrix
SO SIND DATEN SICHER

Was sind nun personenbezogene Daten?

Die Verordnung meint damit:

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte, oder auch eine identifizierbare natürliche Person beziehen

Persönliche Verhältnisse:
- Name
- Anschrift
- Geburtsdatum
- Foto
- Ausbildung, Beruf
- Beurteilungen
- Vorstrafen
- Etc……

Sachliche Verhältnisse:
- Einkommen/ Vermögen
- Schulden
- Eigentum
- Etc…….

Bestimmbare Daten
(Rückschluss möglich):
- Personalnummer
- Kennzeichen
- Etc…..

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele
- Umsetzung im Unternehmen
- Strafen/ Sanktionen

[I] matrix
SO SIND DATEN SICHER

Was sind nun personenbezogene Daten?

Die Verordnung beschreibt auch noch ganz besondere Arten von Daten:

Sensible Daten sind besonders schutzwürdige und geschützte Daten natürlicher Personen.

Dies sind: (taxative Aufzählung - nur diese gelten als sensible Daten)
- rassische und ethnische Herkunft
- politische Meinung
- religiöse oder weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- genetischen Daten
- biometrischen Daten
- Gesundheitsdaten
- sexuelle Orientierung

einer natürlichen Person (Inhalt des Artikel 9 DSGVO).

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele
- Umsetzung im Unternehmen
- Strafen/ Sanktionen

Was ist der Unterschied zwischen Datenschutz und Datensicherheit?

Datenschutz verlangt den täglichen, sorgsamen, Umgang mit Daten von betroffenen Personen. Dazu sind in der Verordnung sogenannte Gewährleistungsziele verankert.

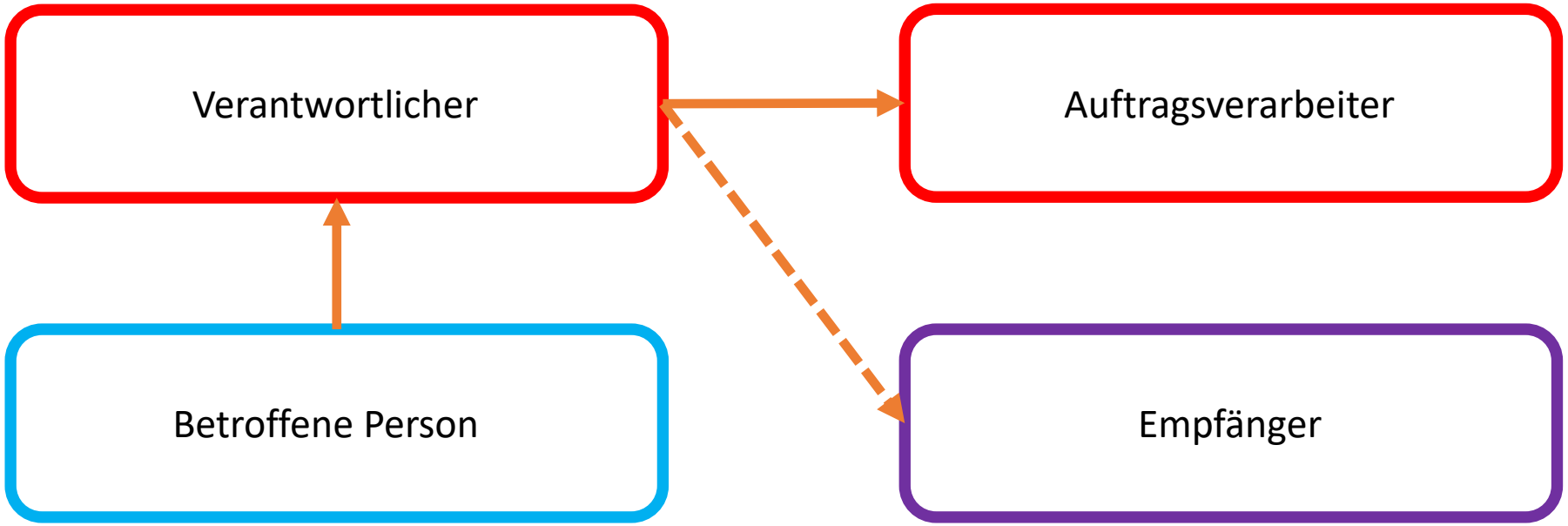
Datensicherheit und besonders die Informationssicherheit wird vor allem durch die IT Abteilung gewährleistet. Informationssicherheit stützt sich auf „nur“ drei Schutzziele. (Anm.: **Vertraulichkeit, Verfügbarkeit, Integrität**)

Die vier zusätzlichen Ziele des **Datenschutzes** weisen auf das wesentlich größere Feld der betroffenen Informationen, Daten und Personen hin. (Anm.: zusätzliche Ziele Datenschutz sind, **Datensparsamkeit**, **Nicht Verkettbarkeit, Transparenz** und **Intervenierbarkeit**)

[I] matrix
SO SIND DATEN SICHER

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele
- Umsetzung im Unternehmen
- Strafen/ Sanktionen

Welche Rollen gibt es im Datenschutz?



Verantwortlicher: natürliche oder juristische Person, Behörde, Einrichtung, oder andere Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

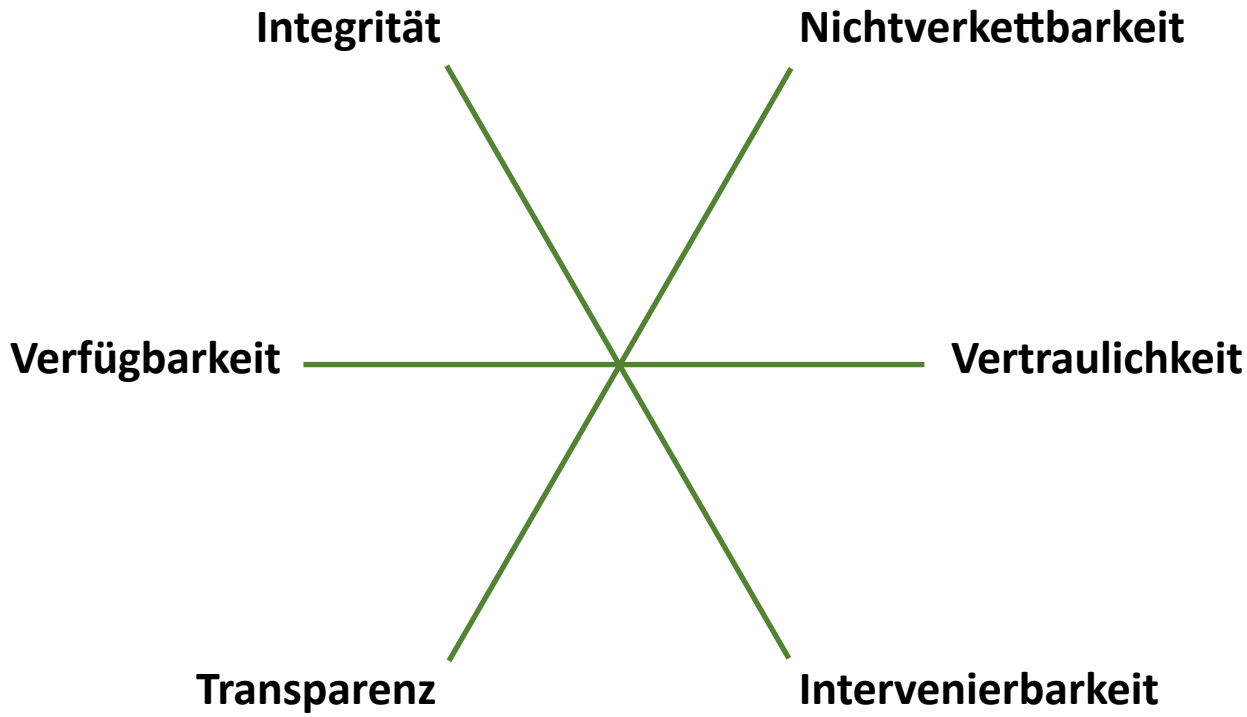
Auftragsverarbeiter: natürliche oder juristische Person, Behörde, Einrichtung, oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Betroffene Person: jene natürliche Person, auf die sich die personenbezogenen Daten der Verarbeitung beziehen.

[I] matrix
SO SIND DATEN SICHER

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele
- Umsetzung im Unternehmen
- Strafen/ Sanktionen

Die **Gewährleistungsziele** leiten sich vor allem aus dem **Artikel fünf DSGVO** ab.
Man kann sie als Wirkungspaare verstehen, die sich gegenseitig wechselseitig beeinflussen. Das heißt Gewährleistungsziele müssen immer im Ausgleich mit dem Wirkungspartner betrachtet werden. Die konkrete Ausprägung eines Gewährleistungszieles sind die sogenannten **TOMs** (vgl.: technische und organisatorische Maßnahmen)
Datensparsamkeit ist das oberste Gewährleistungsziel ohne Wirkungspartner



[I] maTrix
SO SIND DATEN SICHER

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele
- Umsetzung im Unternehmen
- Strafen/ Sanktionen

Datensparsamkeit - so wenig wie möglich, so viel als nötig - an personenbezogene Daten zu erheben, ist mit Datensparsamkeit gemeint. Damit wird einer möglichen Bevorratung, quasi auf Lager legen, von personenbezogenen Daten durch den Gesetzgeber entgegengewirkt.

Nichtverkettbarkeit ist dann gegeben, wenn Daten, Systeme und Prozesse ausschließlich für den definierten Anwendungszweck verwendet werden. **Transparenz** ist dann gegeben, wenn Daten, Systeme und Prozesse durchgängig prüffähig sind.

Vertraulichkeit ist für Daten und Systeme dann gegeben, wenn Verschlüsselung eingesetzt wird. In Prozesse dargestellte und organisatorisch umgesetzte Rechte- und Rollenkonzepte sind die entsprechenden Maßnahmen auf der Systemebene.
Verfügbarkeit für Daten, Systeme und Prozesse ist mit Redundanz, Schutz und Reparaturstrategie gegeben.

Intervenierbarkeit ist dann gegeben, wenn über definierte Punkte, Schnittstellen, auf Daten zugegriffen werden kann. **Integrität** ist dann gegeben, wenn die Unversehrtheit und Unverändertheit gewährleistet werden kann.

[I] maTrix
SO SIND DATEN SICHER

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele
- Umsetzung im Unternehmen
- Strafen/ Sanktionen

Umsetzung im Unternehmen – Was ist zu beachten?

- **Datenschutz** ist nicht Informationssicherheit und Datensicherheit.
- Datenschutz ist kein ausschließliches Thema der IT Abteilung, sondern **betrifft das ganze Unternehmen**.
- Die Umsetzung von Datenschutz ist ein sich immer **wiederholender Zyklus** und kein Einmalprojekt. (vgl.: PDCA – plan-do-check-act)
- Datenschutz wird über technische und organisatorische Maßnahmen (vgl.: **TOMs**) gesteuert.

Es gilt der Grundsatz, dass die **Umsetzung** nur **durch jeden einzelnen Mitarbeiter** erfolgen kann.

[I] matrix
SO SIND DATEN SICHER

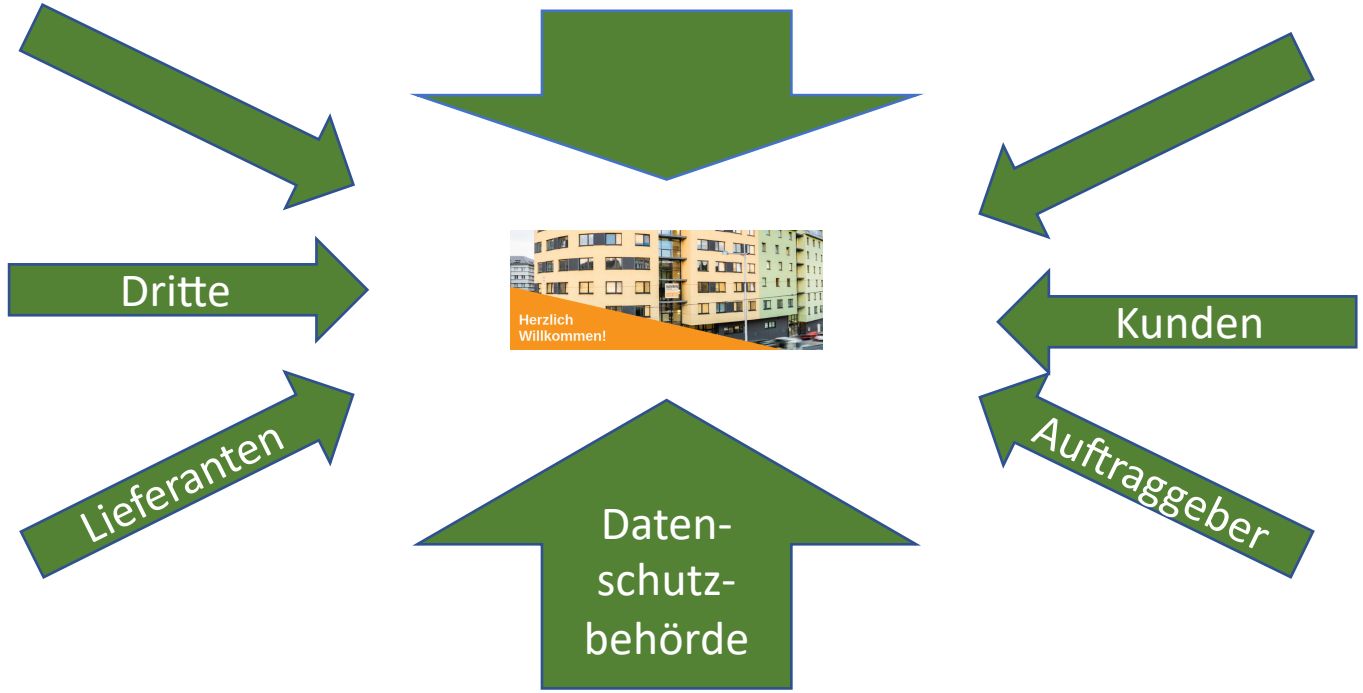
- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele

Umsetzung im Unternehmen

- Strafen/ Sanktionen

Betroffenenrechte – Was ist zu beachten?

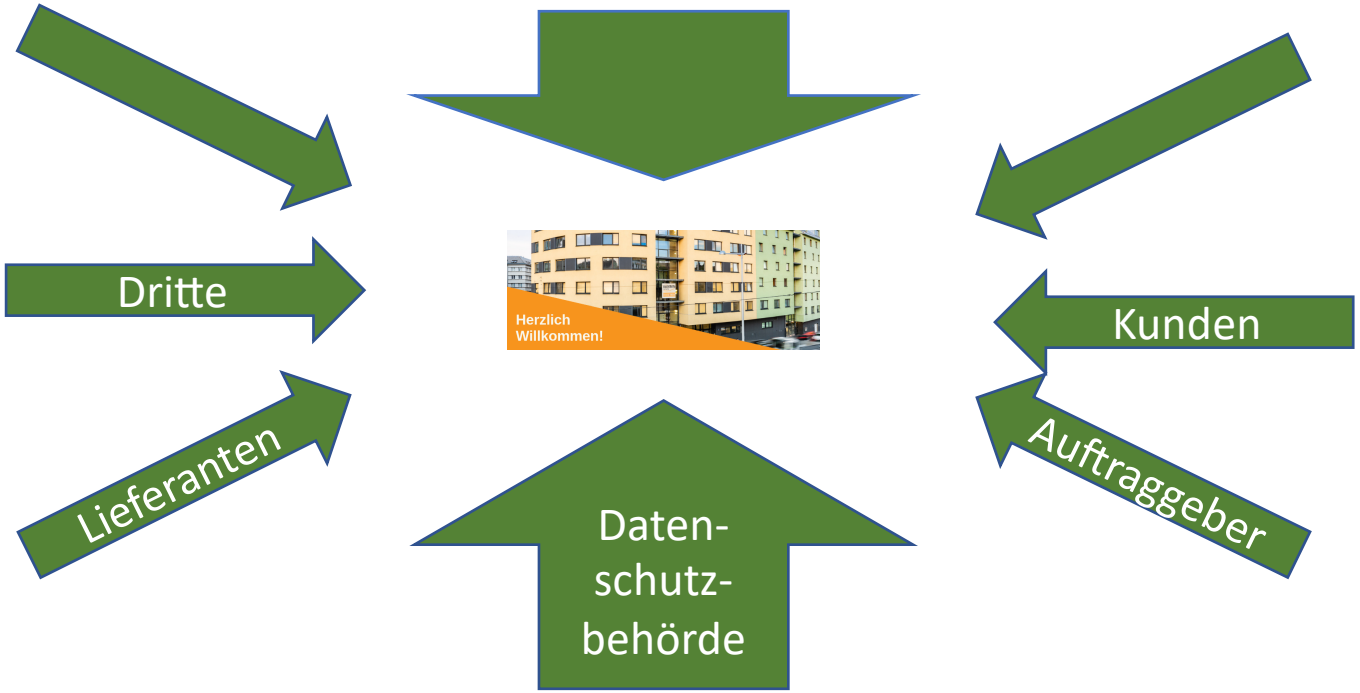
- Sämtliche **Anfragen** sind innerhalb einer bestimmten **Frist** zu erledigen.
- Betroffene haben das **Recht auf**
  - **Auskunft** (inkl. Übertragung)
  - **Richtigstellung**
  - **Einschränkung** der Verarbeitung
  - **Löschung**
- Abwicklung aller Datenschutzbelange nur über die Datenschutzorganisation. (dsgvo@imatrix.at)



[I] matrix
SO SIND DATEN SICHER

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele
- Umsetzung im Unternehmen
- Strafen/ Sanktionen

Betroffenenrechte – Was ist zu beachten?



Datenschutz Organisation ist erreichbar unter dsgvo@imatrix.at
- Geschäftsführung
- Datenschutzbeauftragter
- Datenschutzkoordinatoren

[I] matrix
SO SIND DATEN SICHER

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele

Umsetzung im Unternehmen

- Strafen/ Sanktionen

Betroffenenrechte – Was ist bei Datenschutzanfragen zu beachten?

Anfrage

MitarbeiterIn

Datenschutzorganisation

Rechte: Auskunft – ob und welche Daten
Berichtigung – der vorhandenen Daten
Löschung – der vorhandenen Daten
Übertragung – der vorhandenen Daten

Frist: 1 Monat – Fristenlauf beginnt mit Einlagen der Anfrage – umgehende Reaktion ist wichtig!

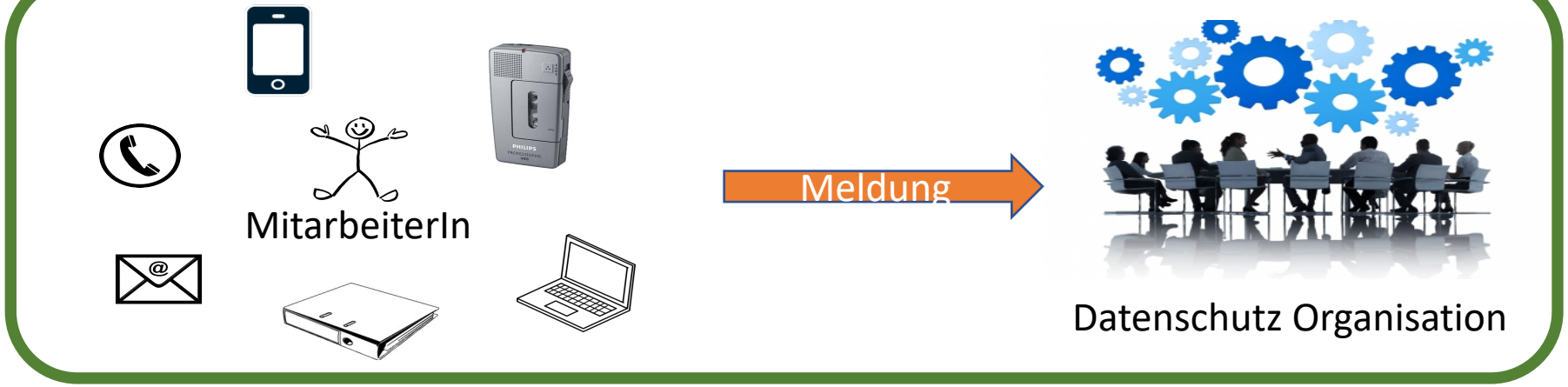
Reaktion: extern: „Vielen Dank – es wird sich unser Datenschutzteam melden!“
intern: Umgehende Meldung per E-Mail an Datenschutzorganisation

Keine selbstständige Beauskunftung, Löschung etc….

[I] matrix
SO SIND DATEN SICHER

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele
- Umsetzung im Unternehmen
- Strafen/ Sanktionen

Datenverlust – Was ist zu beachten?



Bei Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität von Daten ist unter Umständen eine **Meldung** an die Datenschutzbehörde abzusetzen.

Mögliche Szenarien:	Verlust von Datenträgern (Handy, Diktaphone, Laptop…) Verlust von Ordner, Notizblöcken oder Taschen Versand von Emails, Fax et al. an falsche Empfänger
Frist:	**72 h** - eine umgehende Reaktion ist wichtig!
Reaktion:	Umgehende Meldung per **eMail an Datenschutzorganisation und** an die **IT Abteilung**.

[I] matrix
SO SIND DATEN SICHER

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele

Umsetzung im Unternehmen

- Strafen/ Sanktionen

Wer ist in unserem Unternehmen für Datenschutz zuständig?

Zuständig für Datenschutz in unserem Unternehmen ist
- Stefan Schreiner (externer Datenschutzbeauftragter)
dsgvo@imatrix.at

Fragen zur Datensicherheit beantwortet
- IT Abteilung

Wenden Sie sich bei Unklarheiten oder Anfragen zum Thema Datenschutz an Ihre Führungskraft.

[I] matrix
SO SIND DATEN SICHER

- Datenschutz Grundverordnung (DSGVO)
- Datenschutz Begriffe
- Unterschied/ Trennung
- Akteure
- Gewährleistungsziele
- Umsetzung im Unternehmen
- Strafen/ Sanktionen

Sanktionen

- **Schadensersatz**
  - Verantwortlicher haftet
    - Gegenüber jeder Person, der ein materieller oder immaterieller Schaden entstanden ist (Kosten, Verdienstentgang, Schmerzensgeld)
    - Bei Verstoß gegen die DSGVO
  - Auftragsverarbeiter haftet nur für seine speziellen Pflichten
    - Diese müssen explizit vertraglich geregelt sein.
- **Strafen**
  - Verletzung von Pflichten des Verantwortlichen
    - Bis zu € 10 Millionen (bzw. 2% Konzernumsatz weltweit)
      - Verletzung TOMs
      - Verletzung der Vorschriften zum Verarbeitungsverzeichnis
      - Verletzung der Vorschriften zur Datenschutzfolgeabschätzung
  - Verletzung von Rechten Betroffener
    - Bis zu € 20 Millionen (bzw. 4% Konzernumsatz weltweit)
      - Verletzung von Rechten betroffener Personen
      - Verstoß gegen die Rechtmäßigkeit der Verarbeitung
      - Verletzung der Bestimmungen bzgl. internat. Datenverkehr

Anm.: Beschluss NR 20.4.2018 -> “Verwarnung statt Bestrafung“ (vorerst)

Hiermit bestätige ich die Informationen zum Datenschutz gelesen und verstanden zu haben und mir ist bekannt, an wen im Unternehmen ich mich bei Fragen wenden kann.

Name

Datum

Unterschrift

[I] matrix
SO SIND DATEN SICHER