Datenschutzgrundverordnung

DSGVO – Was zählt wirklich
Version L vom 20.06.2018

Inhalt

1.Was ist „DSGVO" oder „GDPR"

Die Datenschutzgrundverordnung (Verordnung EU 2016/679) ist ein Europäisches Gesetz... das in allen EU-Mitgliedsländern in nationales Recht übergeführt wurde. Damit werden die Regeln der Verarbeitung von personenbezogenen Daten EU-weit vereinheitlicht.

Die wichtigsten Inhalte der DSGVO:

1. **Schutz der Grundrechte und Grundfreiheiten natürlicher Personen**
2. **Schutz personenbezogener Daten**
3. **Freier Datenverkehr in Europa**
4. **Regelung des internationalen Datenverkehrs**
5. **Ablöse von nationalen Verordnungen**
6. **GÜLTIG seit 25.Mai 2018**

MEDIAN DATENSCHUTZ www.median.one

1.Was ist „DSGVO" oder „GDPR"

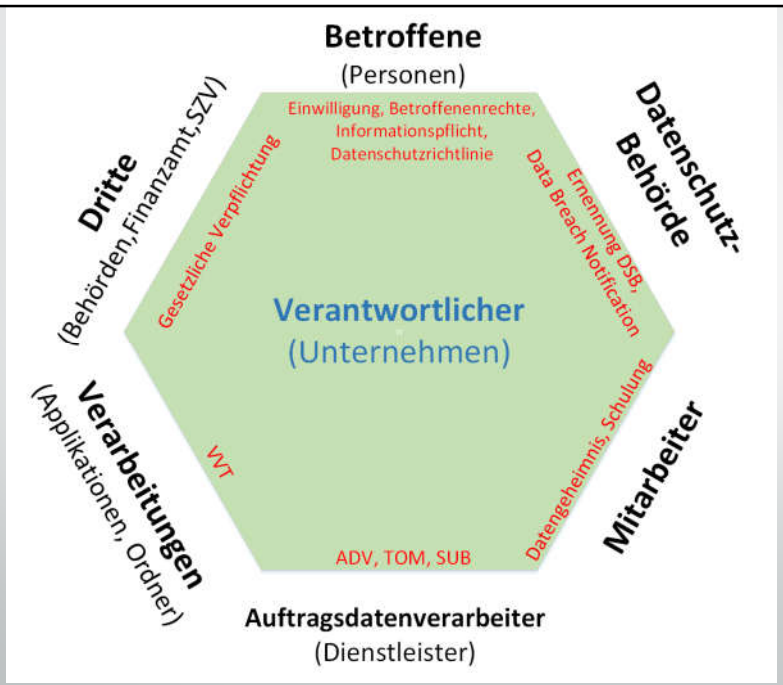
- Die DSGVO ist ein EU-Gesetz, das in allen Unions-Ländern ein verlässliches Datenschutzniveau herstellt.
- In Folge existieren ZWEI Datenschutzgesetze in Österreich:
  - DSGVO EU 2016/679
  - DSG (als Container für die Österreichischen „Öffnungsklauseln")
- Die „ePrivacy-Verordnung" wird im Rahmen der DSGVO den Umgang mit digitalen Medien und elektrischer Kommunikation regeln.

MEDIAN DATENSCHUTZ www.median.one

1.Was ist „DSGVO" oder „GDPR"

- Die DSGVO ist ein EU-Gesetz, das in allen Unions-Ländern ein verlässliches Datenschutzniveau herst t.
- In Folge existieren Zw Daten tzg e in Österreich:
  - DSGVO EU 2016/679
  - DSG (als Contain ein")
- Die „ePrivacy-Verordn VO den Umgang mit digitalen Medien un n regeln.

DSG verstößt gegenwärtig gegen EU-RECHT! Wird aufgehoben, repariert oder ignoriert

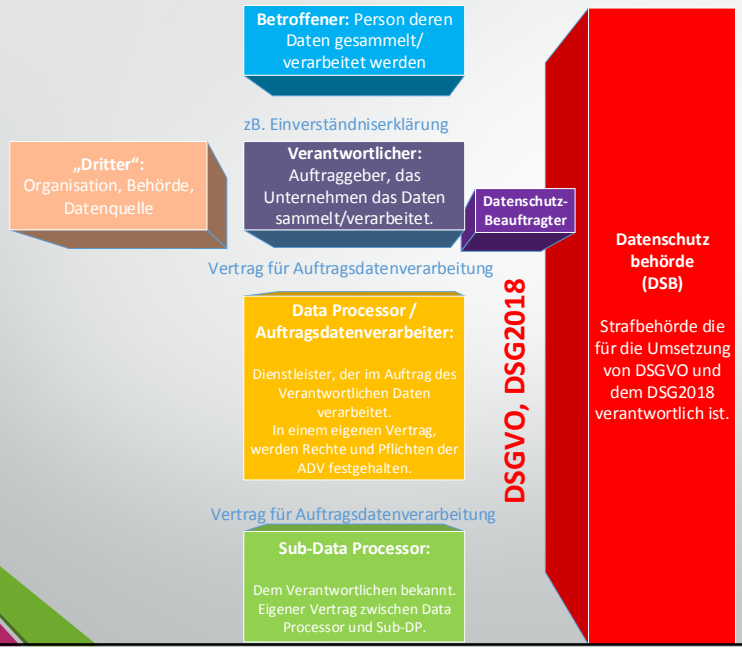


1.Was ist „DSGVO" oder „GDPR"

Gilt nicht :

- Betroffene außerhalb der Union (vgl. 4. Amendement USA)
- Grenzschutz, Asylverfahren,...
- Haushaltsregelung
- Ermittlung, Aufdeckung und Verfolgen von Straftaten durch Behörden
- Wenn das „öffentliche Interesse überwiegt"
- Für Daten von Verstorbenen
- Unternehmensdaten

Rollen in der DSGVO



2. Was sind „Personenbezogene Daten“?

Browser-Cookies

genetische Daten

Gehalt

Fingerabdrücke

Stimme

Adresse

IP-Adresse

Intelligenzquotient

- Private
- Berufliche
- wirtschaftliche Informationen
- Eigenschaften
- Kenntnisse
- physiologische Merkmale

Bild

Schulden

Vermögen

Name

Log-File-Eintrag

Geburtsdatum

Lebensstil

2. Was sind „Personenbezogene Daten“?

- **Besondere Kategorien von Personenbezogenen Daten**:
  - Rassisch oder ethnische Herkunft
  - Politische Ansichten
  - Religiöse oder Weltanschauliche Überzeugung
  - Gewerkschaftszugehörigkeit
  - Genetische Daten
  - Biometrische Daten (die eine Person eindeutig identifizieren können)
  - Gesundheitsdaten
  - Daten zum Sexualleben / zur sexuellen Orientierung

Unterliegen speziellem Schutz und Vorkehrungen. Die Verarbeitung ist generell verboten – mit einigen Ausnahmen

3. Was ist „Datenverarbeitung"?

Erheben… Erfassen… Organisation… Ordnen… Speicherung… Anpassung… Veränderung… Auslesen… Abfragen… Verwendung… Offenlegung durch Übermittlung… Verbreitung… Bereitstellung… Abgleich… Verknüpfung… Einschränkung… Löschen… Vernichtung

- Eine sortierte Sammlung von Visitenkarten,
- Abgelegte Mails sind Datenverarbeitung!
- Nach Kunden sortierte Ordner sind Datenverarbeitung!

3. Was ist „Datenverarbeitung"?

Normale Personenbezogene Daten (Art 5 DSGVO) dürfen wie folgt verarbeitet werden:

- Für den „Betroffenen" **transparent**
- **Eindeutige Zwecke**
- Auf das notwendige Maß reduziert (**Datenminimierung**)
- Sachlich **richtig** und **aktuell**
- Solange ein **berechtigter Grund** dafür existiert
- Unter ausreichendem **technischen und organisatorischem Schutz**

Die Nachweispflicht für die Rechtmäßigkeit liegt hier IMMER beim Verarbeiter

3. Was ist „Datenverarbeitung“?

Was sind legale Gründe um personenbezogene Daten nach diesen Grundsätzen verarbeiten?

- **Einverständniserklärung**: klar formuliert, welche Daten und für welchen Zweck. Widerruf jederzeit möglich
- **Erfüllung von Verträgen:** Daten dürfen im notwendigen Ausmaß verarbeitet werden
- **Gesetze:** Verpflichten zu Aufbewahrungsfristen. Nach Ablauf der Frist ist die Löschung verpflichtend
- **„Berechtigtes Interesse“:** Solange das Interesse des Verantwortlichen nicht die Grundrechte des Betroffenen verletzt.
  Im EG47 wird das zB. mit einer Kunden-Lieferanten-Beziehung gleichgesetzt.

Die rechtliche Basis einer Verarbeitung muss immer dokumentiert werden, damit sie bei einer Überprüfung Gültigkeit hat!! -> VVT

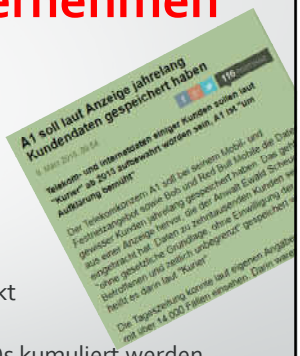
3. Was ist „Datenverarbeitung“?

Besondere Kategorien von Personenbezogene Daten (Art 9 DSGVO) dürfen NICHT verarbeitet werden… außer:

- Der Betroffene erlaubt es explizit (und das nationale Recht erlaubt das auch)
- Der Betroffene braucht die Verarbeitung für seinen Beruf (Fingerabdruck für Zutritt, Retinascan,..)
- Zum Schutz des Lebens von Personen
- Die Daten wurden vom Betroffenen bereits allgemein öffentlich gemacht
- Gesundheitsvorsorge oder Arbeitsmedizin
- Öffentliches Interesse (zB.: drohende Epidemie,..)

Die Mitgliedsstaaten können zusätzliche nationale Regeln für besondere personenbezogene Daten einführen

4. Größte DSGVO-Gefahren für Unternehmen


A1 soll laut Anzeige jahrelang Kundendaten gespeichert haben

- **Imageschaden:** Datenschutzvergehen werden öffentlich
- **Verbot der Verarbeitung:** Durch Datenschutzbehörde bei hohem Risiko
- **Personalaufwand**: Die Sicherstellung des Datenschutz bringt hohe Aufwendungen mit sich
- **Bußgeld/Strafen:** Datenschutzbehörde ist eine Strafbehörde und kann direkt Verwaltungsstrafen verhängen
- **Schadenersatz-Forderungen**: können bei vielen Einzelpersonen durch NGOs kumuliert werden
- **Betroffenen-Rechte:** Einzelpersonen können massiven Aufwand verursachen, oder eine Prüfung durch die Datenschutzbehörde herbeiführen

www.median.one MEDIAN DATENSCHUTZ

4. Größte DSGVO-Gefahren für Unternehmen

Wer kann wie gestraft werden?

- DSGVO: Juristische Person des „Verantwortlichen" wird primäres Ziel für Verwaltungsstrafen sein (theoretisch auch gegen Organe möglich, aber nicht beides) 20/10 Mio o. 4/2 %
- DSG: natürliche oder juristische Person Strafen bis 50.000 € bei nationalen Strafbestimmungen
- Gerichtlich strafbarer Tatbestand: Freiheitsstrafen bis 1 Jahr oder 720 Tagsätze bei Datenverarbeitung in Gewinn – oder Schädigungsabsicht

www.median.one MEDIAN DATENSCHUTZ

Exkurs: **Datenschutzbehörde**

- **Leitung**: Frau Mag. Dr. Andrea Jelinek
- **Bisher** konnte die DSB bei einem Datenschutzvergehen Anzeige erstatten
  - Behandlung vor einem ordentlichen Gericht
  - Strafmaß max. 20.000€, größte in AT je ausgesprochene Strafe: 1.970 €
- **Ab 25.05.2018** ist die DSB eine unabhängige Strafbehörde (wie FMA)
  - Wenn ersichtlich ist, dass die DSGVO ernst genommen wird, gilt vor allem am Anfang das Prinzip „Beraten statt Strafen" und „Ermahnung statt Geldbuße"
  - Die Bemessung der Geldbuße wird nach einer europäisch abgestimmten Formel errechnet
  - Nur gegen die Höhe der Geldbuße sind Rechtsmittel möglich

Exkurs: **Datenschutzbehörde**

Wie wird die Datenschutzbehörde auf Sie aufmerksam?

- **Branchenschwerpunkt:** jährlich festgelegt (zuletzt Banken und Versicherungen) – ***NICHT 2018***
- **Beschwerde eines Betroffenen:** führt zu Untersuchung
- **Meldung einer Datenschutzpanne:** Pflicht des Verantwortlichen

5. Informations-Pflicht

(bei Erhebung von personenbezogenen Daten)

- Die Information über die **neue** Erhebung (zB. Useranlage) muss zum Zeitpunkt der Erhebung erfolgen
- Bei jeder Zweckänderung der Verarbeitung muss ebenfalls informiert werden
- Art 13: bei der Person selbst erhobene Daten
- Art 14: bei Dritten erhobene Daten
- Information an die Mitarbeiter: Beschreibung der Verwendung von Mitarbeiterdaten

5. Informations-Pflicht

(bei Erhebung von personenbezogenen Daten)

Die Information muss folgende Punkte enthalten:

- Verantwortlicher
- DSBer bzw. Ansprechperson
- Zweck der Verarbeitung
- Rechtsgrundlage
- Empfänger im Drittland?
- Speicherdauer
- Hinweis auf Betroffenenrechte
- Beschwerderecht
- Eventuelle Empfänger
- Bei Art 14: Quelle der Daten

WIE: Informationsblatt, Email, Datenschutzrichtlinie auf Homepage

5. Informations-Pflicht

(bei Erhebung von personenbezogenen Daten)

- Webseiten:
  - Verfassung in allgemein verständlicher Sprache
  - Datenschutzrichtlinie listet genau auf, was mit den PBD auf der Webseite passiert
  - Details über das Unternehmen und den gesetzlichen Vertreter
  - Weiterleitungen an Dritte (zB. Google Analytics)
  - Bei Bezahl-Lösungen auch den Payment-Partner.
  - Social Media – Abhängigkeiten („like this page")
  - Verlinkt bei „Einverständniserklärungen"

6. Betroffenen-Rechte

- Recht auf Auskunft (Art 15)
- Recht auf Berichtigung (Art 16)
- Recht auf Löschung (Art 17)
- Recht auf Einschränkung (Art 18)
- Mitteilungspflicht iZm Art 15 – Art 21 (Art 19)
- Recht auf Datenübertragung (Art 20)
- Recht auf Widerspruch (Art 21)

6. Betroffenen-Rechte

- Für die Sicherstellung der Betroffenen-Rechte müssen im Unternehmen **Prozesse** definiert werden.
- **Jeder** Mitarbeiter kann für das Unternehmen eine Datenschutzverletzung verursachen ->
- Jeder Mitarbeiter muss diese Prozesse kennen und befolgen
- Fristen, Zuständigkeiten, Verantwortung müssen geschult werden!
- Verletzung von Betroffenen-Rechten: Strafen bis zu **20 Mio €** oder **4% Konzernumsatz**

6. Betroffenen-Rechte

Beispiel: **Recht auf Auskunft** nach Art. 15 DSGVO

Die DSGVO räumt natürlichen Personen ein Auskunftsrecht ein

- Sicherstellung der Identität (zB. Ausweiskopie)
- Antrag kann formlos gestellt werden – sogar mündlich
- Inhalt der Auskunft:
  - Kategorien und Herkunft der Daten die verarbeitet wurden
  - Zwecke der Verarbeitung
  - Hinweis auf Berichtigung oder Löschung
  - Auszug der personenbezogenen Daten (incl. Emails, Logfiles,...)
- Frist: innerhalb eines Monats (bei hoher Komplexität auf 3 Monate erweiterbar)

6. Betroffenen-Rechte

Beispiel: **Recht auf Löschen, Einschränkung** nach Art. 17,18 DSGVO

- **Wie bei Auskunftsrecht.**
- **Aber:** Was bedeutet das für Daten in Backups?
- **Das DSG (2018) hilft uns hier:**

  § 4. Abs2. Kann die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO bis zu diesem Zeitpunkt einzuschränken.

- **Wichtig**: Backup-Zyklus dokumentieren und Verwendung der Daten in aktiven Systemen einschränken.

6. Betroffenen-Rechte

Achtung: Bei automatischer Analyse der Kreditwürdigkeit eines Kunden.

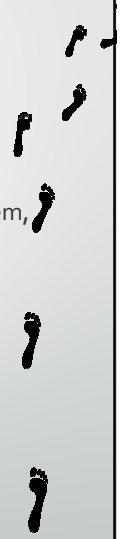
- Art. 22: Ein Kunde hat das Recht, dass die eine automatische Entscheidung – incl. Profiling- von einer natürlichen Person geprüft wird
- Eine automatische Entscheidung in Folge einer Ediktsdatei-Abfrage ist Profiling
- Automatische Entscheidungen auf Basis von „besonderen Kategorien von Daten" sind extrem gefährlich (zB. Kreditwürdigkeit auf Basis Gesundheitsdaten, Herkunft,..)

Unbedingt immer Zustimmung einholen!

7. Die wichtigsten Schritte

- **STRATEGIE**: Wo begründen wir und wo verändern wir?
- **Datenschutzorganisation**: Zuständige Rollen im Unternehmen
- **Bewusstseinsbildung**: Schulung, gutes Beispiel, Kontrolle
- **Prozesse**: Voraussetzung um Fristeinhaltung und Datenschutz sicherzustellen
- **Informationssicherheit**: Überprüfen, ggf. erweitern, dokumentieren
- **Drittland-Datenübermittlung**: Rechtsbasis vorhanden?

7. Die wichtigsten Schritte



- **7.1.Verzeichnis der Verarbeitungstätigkeiten(Art 30 DSGVO)**: Welche Daten werden von wem, mit welchem Ziel wie verarbeitet und gespeichert
- **7.2.Datenschutz-Folgeabschätzungen(Art 35 DSGVO)**: Bei hohem Risiko, systematischer Verarbeitung von besonderen Kategorien von Daten und neuer Technologie Pflicht!
- **7.3.Data Breach Notification(Art 33,34 DSGVO):** Wie schafft man es bei einer Datenpanne in 72 h eine korrekte Meldung durchzuführen?
- **7.4.Verträge für Auftragsverarbeiter (Art 4):** Definition welche Themen der DSGVO, welche Kategorien von Daten, zu welchen Zwecken vom Dienstleister erbracht werden
- **7.5.Prozesse für DSGVO(Art 13-21,…) einführen**: Richtige, zeitgerechte Reaktion auf Anfragen, Meldung an die Datenschutzbehörde, Schulung der Mitarbeiter
- **7.6.Datenschutzbeauftragter**: Klärung ob ein DSB verpflichtend ist

7.1. Verzeichnis für Verarbeitungstätigkeiten

- Unternehmen mit weniger als 250 Mitarbeitern sind vom VVT befreit **AUSSER**:
  - Die verarbeiteten Daten bergen Risiken für die Personen (zB. Videoüberwachung)
  - Die Verarbeitung passiert regelmäßig und nicht nur gelegentlich (zB. CRM-System, Verrechnungssysteme, Gehaltsabrechnung,...)
  - Besondere Kategorien von Daten sind betroffen (zB. Gesundheitsdaten, Strafregister,..)
- Das VVT ist das einfachste Mittel um die im Betrieb verwendeten personen-bezogenen Daten mit geringem Aufwand kennenzulernen!
- Generell: **Bei allen Personenbezogenen Daten auf die eine Gruppe von Mitarbeitern Zugriff hat, ist ein VVT Pflicht**.
- **Ein Datenschutz-Vergehen wird strenger bewertet, wenn kein VVT erstellt wurde!**

www.median.one MEDIAN DATENSCHUTZ

7.1. Verzeichnis für Verarbeitungstätigkeiten

Inhalt des VVT:

- **Namen und die Kontaktdaten** des für die Verarbeitung Verantwortlichen (ggf. auch Vertreter und Datenschutzbeauftragten)
- **Zweckbestimmung** der Datenerhebung, Verarbeitung oder Nutzung
- **Kategorien von betroffenen Personen** und personenbezogenen Daten
- **Kategorien von Empfängern,** an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden (auch in Drittländern)
- **Übermittlungen** von Daten an ein **Drittland** oder an eine internationale Organisation
- Vorgesehene **Fristen für die Löschung** der verschiedenen Datenkategorien
- Eine allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**

www.median.one MEDIAN DATENSCHUTZ

7.2. Risikoanalyse

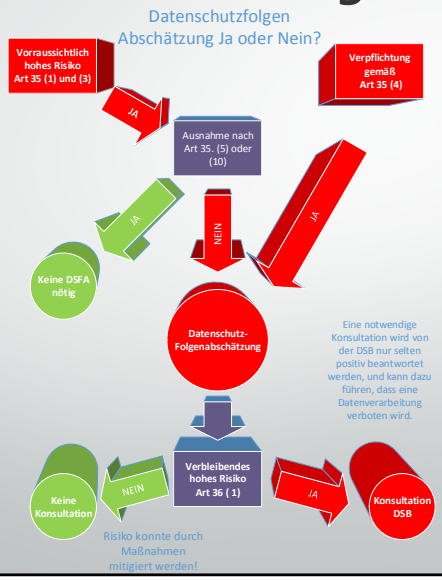
- Risiken identifizieren
  - Welche Daten können bedroht sein und in Folge ein Risiko für die Rechte von Personen darstellen
    (und Probleme für das Unternehmen mit sich bringen)?
- Risiken bewerten
  - Wie wahrscheinlich ist es, dass dieses Risiko zum Tragen kommt.
  - Schwere des Risikos – Einbindung des Managements!!
- Datenschutzfolgenabschätzung(DSF)
  - Bei einem hohen Risiko ist eine DSF unbedingt durchzuführen

7.2 Datenschutz-Folgenabschätzung

- Wird immer dann notwendig:
  - Wenn neue Technologien eingesetzt werden, die hohe Risiken mit sich bringen können
  - Umfangreiche systematische Erfassung von persönlichen Aspekten, Profiling
  - Umfangreiche Verarbeitung von besonderen Datenkategorien (zB. Datawarehouse)
  - Neue Ergebnisse aus bestehenden Daten werden abgeleitet (zB. BI-Reports,...)
  - systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Pseudonymisierung kann jeden dieser Gründe nichtig machen

7.2 Datenschutz-Folgenabschätzung



7.2 Datenschutz-Folgenabschätzung

Inhalt:

- systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (-> Risikobewertung)
- Maßnahmen die geeignet sind ein hohes Risiko zu mitigieren
- Datum der nächsten Überprüfung

Form: schriftlich, incl. Risikobewertung, Technisch-Organisatorischen Maßnahmen, ggf. Statement der Betroffenen

Konsultation: Kann das Risiko nicht mitigiert werden, muss die DSB konsultiert werden, die in der Norm die Verarbeitung verbieten wird, bis geeignete Maßnahmen getroffen werden.

7.3 Data Breach Notification

Bei einer Datenschutzverletzung muss das Unternehmen innerhalb von 72 h eine Meldung bei der Datenschutzbehörde vornehmen.

- Klare Verantwortungen
  - Intern (Management, Datenschutzbeauftragte, Techniker)
  - Extern (Datenverarbeiter [Dienstleister], Spezialunternehmen, externer DSB)
- Möglichst genaue Identifikation der Datenschutzverletzung
- Eindämmung der Gefahr (um weitere Verletzungen zu vermeiden)
- Meldung an Datenschutzbehörde
- Ggf. Meldung an die Betroffenen wenn sensible Daten betroffen sind

Die Data Breach Notification muss als Prozess definiert, geschult und regelmäßig „geübt" werden.

7.4.Verträge für Auftragsverarbeiter

Die Verpflichtung für einen Vertrag für Auftragsverarbeitung trifft Auftraggeber und Dienstleister!

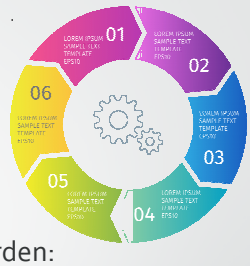
Inhalt:

- Der Auftragsverarbeiter (AV) garantiert Einhaltung der DSGVO (zB. Hosting, Betriebssupport)
- Sub-Auftragsverarbeiter werden dem Verantwortlichen zu Kenntnis gebracht
- Verarbeitung von Personenbezogenen Dateien erfolgt nur auf Weisung des Verantwortlichen
- Mitarbeiter des AV unterliegen der Schweigepflicht; zur Verschwiegenheit verpflichtet
- Der Verantwortliche wird bei der Wahrung von Betroffenen-Rechten(->) unterstützt
- Der Verantwortliche wird bei DSGVO-Audits unterstützt
- Der ADV wendet **angemessene** Sicherheitsmaßnahmen (zB. Pseudonymisierung) an

Ohne Vertrag:

- **Datenschutzverletzung**
- Keine Verpflichtung des Dienstleisters zur DSGVO und keine Kontrolle möglich

7.5 Prozesse für DSGVO



Für folgende Themen müssen Prozesse im Unternehmen verankert werden:

- Einhaltung der Betroffenen-Rechte (zB. Auskunftsrecht,..)
- Meldung bei der Datenschutzbehörde (72h Reaktionszeit)
- Aufnahme in das Verzeichnis für Verarbeitungstätigkeiten
- Risikoanalyse von Verarbeitungen
- Datenschutz-Folgenabschätzung
- Jährliche, dokumentierte Schulung aller Mitarbeiter bez. Datenschutz

Jährliche Kontrolle der Prozesse und Abläufe auf Aktualität!

7.6 Datenschutzbeauftragter

Ist verpflichtend:

- Für Behörden und öffentliche Stellen
- Die Kerntätigkeit macht eine systematische Überwachung von Personen nötig
- Die Kerntätigkeit in der systematischen Verarbeitung von besonderen Daten besteht

Der Datenschutzbeauftragte:

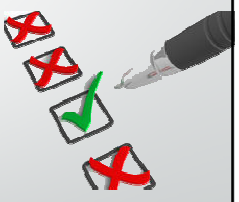
- Muss in seiner Aufgabe weisungsfrei arbeiten können
- Braucht Zugang zu Geschäftsführung/Vorstand des Verantwortlichen Unternehmen

8. Informationssicherheit, TOMs

- Kein Unternehmen (über)lebt heute ohne Informationssicherheit
- Für die DSGVO ist es wichtig zu dokumentieren, was es schon gibt (Sicherheitskonzept, ISMS).
- Welche technischen und organisatorischen Maßnahmen (TOMs) können Sie zusätzlich einleiten um
  - Einen Data Breach zu verhindern?
  - Bei einer Überprüfung durch die Datenschutzbehöre keine Probleme zu bekommen?
- Bei der Auswahl von neuen Applikationen ist die DSGVO-Eignung ein wichtiges Entscheidungskriterium!

8.1 Anforderungen an eingesetzte Applikationen

- Die DSGVO verstärkt die Anforderungen an Applikationen
- Grundsätze der Datenverarbeitung (Art.5)
  - Integrität und Vertraulichkeit
    - Angemessene Sicherheit
    - Schutz vor unbefugter oder unrechtmäßiger Verarbeitung
    - Schutz vor unbeabsichtigtem Verlust oder Zerstörung
  - Datenminimierung
    - Es werden nur jene Daten verarbeitet, die auch wirklich benötigt werden
  - Rechenschaftspflicht
    - Einhaltung dieser Punkte muss vom Unternehmen nachgewiesen werden können



WICHTIG: verheimlichen Sie keine Datenverarbeitung vor den Betroffenen!!

8.1 Anforderungen an eingesetzte Applikationen

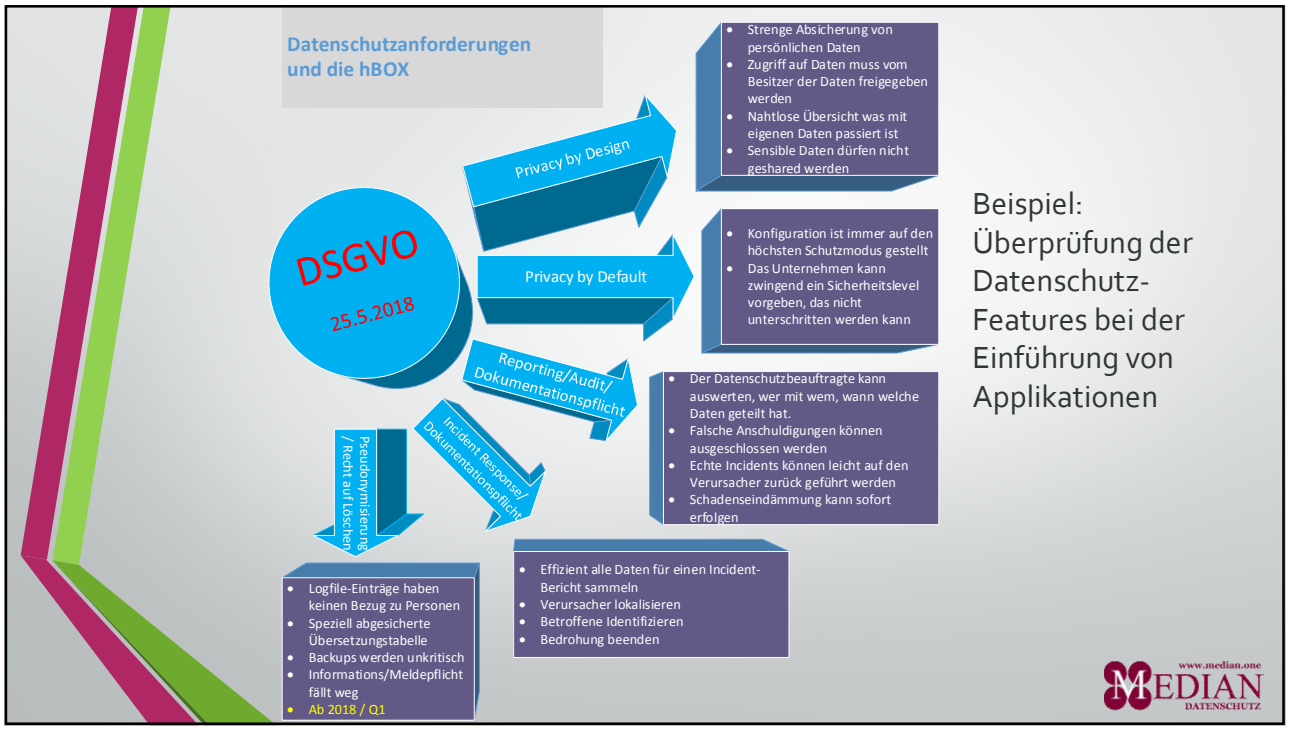
Privacy by Design - Datenschutz durch Technikgestaltung

- **MINIMISE**: Die Menge der verarbeiteten Daten sollte so gering wie möglich sein (Pseudonymisierung!!).
- **HIDE**: Alle personenbezogenen Daten und ihre Zusammenhänge sollten möglichst verborgen bleiben.
- **SEPARATE**: Personenbezogene Daten sollten möglichst verteilt verarbeitet und getrennt gespeichert werden.
- **AGGREGATE**: Personenbezogene Daten sollten im höchsten Aggregationsniveau und mit dem niedrigsten Detailgrad verarbeitet werden, in dem sie (noch) ihren Zweck erfüllen.
- **INFORM**: Betroffene sollten angemessen informiert werden, wann immer ihre personenbezogenen Daten verarbeitet werden.
- **CONTROL**: Betroffene sollten Kontrolle über die Verarbeitung ihrer personenbezogenen Daten erhalten.

8.1 Anforderungen an eingesetzte Applikationen

Privacy by Default – Datenschutz-freundliche Voreinstellungen

- Rechte für andere Personen einschränken
- Passwortschutz für Inhalte obligatorisch
- Zeitliches Limit für Freigaben
- Dem Benutzer freistellen ob er persönliche Daten im System verwendet
- Weiterleitung von Daten aus dem System erfolgen nur nach Intervention mit dem Betroffenen



Beispiel: Überprüfung der Datenschutz-Features bei der Einführung von Applikationen

8.2 Sicherheit der Verarbeitung(Art. 32)

Verantwortliche und der Auftragsverarbeiter treffen geeignete TOMs, um ein dem **Risiko angemessenes Schutzniveau** zu gewährleisten

- Unter Berücksichtigung des **Stands der Technik**
- Der **Implementierungskosten**
- **Umfang und Zwecke der Verarbeitung**
- **Eintrittswahrscheinlichkeit und Schwere des Risikos**

8.2 Sicherheit der Verarbeitung(Art. 32)

DSGVO – Sicherheits-Maßnahmen

- die **Pseudonymisierung und Verschlüsselung** personenbezogener Daten
- **Betriebstauglichkeit**: **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung **auf Dauer sicherstellen**
- **Backup/Restore:** Bei einem **physischen oder technischen Zwischenfall sind die Daten in einem definierten Zeitraum wieder hergestellt**;
- **Audit**: **Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen** zur Gewährleistung der Sicherheit der Verarbeitung

8.3 Organisatorische Maßnahmen

- Datenschutzkonzept nach ART 5 (2)
  - Verzeichnis für Verarbeitungstätigkeiten incl. TOMs
  - Risikobewertungen / Analysen
  - Datenschutz-Folgenabschätzung
  - DSMS – analog zum ISMS
  - Schulung der Mitarbeiter
  - Richtlinien und BV
  - ADV – Verträge
  - Datenschutzrichtlinie
  - Begründungen für interne Abläufe

8.4 Informationssicherheit

Einige Themen lassen sich nicht mehr leicht beheben:

- Verlust eines Laptops ohne Verschlüsselung
  - Festplatte kann wie ein USB-Stick ausgelesen werden
- Verlust eines Handys ohne Zugriffsschutz und Verschlüsselung
  - Zugriff auf Unternehmensressourcen
- Verlust eines unverschlüsselte USB-Sticks, Cdrom, DVD,…

8.4 Informationssicherheit

Zugriffskontrolle – Identitäts- u. Berechtigungsmgmt

- **Authentifizierung - Authentication**
  - o Passwort-Policy!
  - o Bei höheren Anforderungen: Mehrfaktor-Authentifzierung
- **Autorisierung - Authorization**
  - o Verwaltung der Berechtigungen - rollenbasierte Zugriffsmodelle
  - o Least Privilege: minimal notwendige Berechtigungen
  - o Separation of Duties: Aufgabentrennung (z.B. Aktion/Kontrolle)
    - o Unterschiedliche **Accounts** für unterschiedliche **Aufgaben**,
    - o Unterschiedliche **Vorgaben** für unterschiedliche **Risiken**
- **Auditing**
  - o Nachvollziehbarkeit von Aktionen
  - o Kontrolle des Lebenszyklus von Accounts
- **SIEM-Tool / Logfile-Management**
  - o Automatisierte, policy-basierende Untersuchung von Logfiles

8.4 Informationssicherheit

Schutz vor Schadsoftware

- **Mehrstufiges Malware-Schutzkonzept**
  - o E-Mail Server / Mail-Gateway
  - o Firewall / Web-Proxy
  - o Dateiserver / Ablagen, Client-Systeme
- **Unterschiedliche / komplementäre Technologien**
  - o Antivirus / Endpoint Protection (Signatur, Heuristik, Sandbox, etc.)
  - o „Next-Gen" Antivirus (Machine-Learning, Cloud-Intelligence)
  - o Exploit-Prevention / Host Intrusion Detection/Prevention

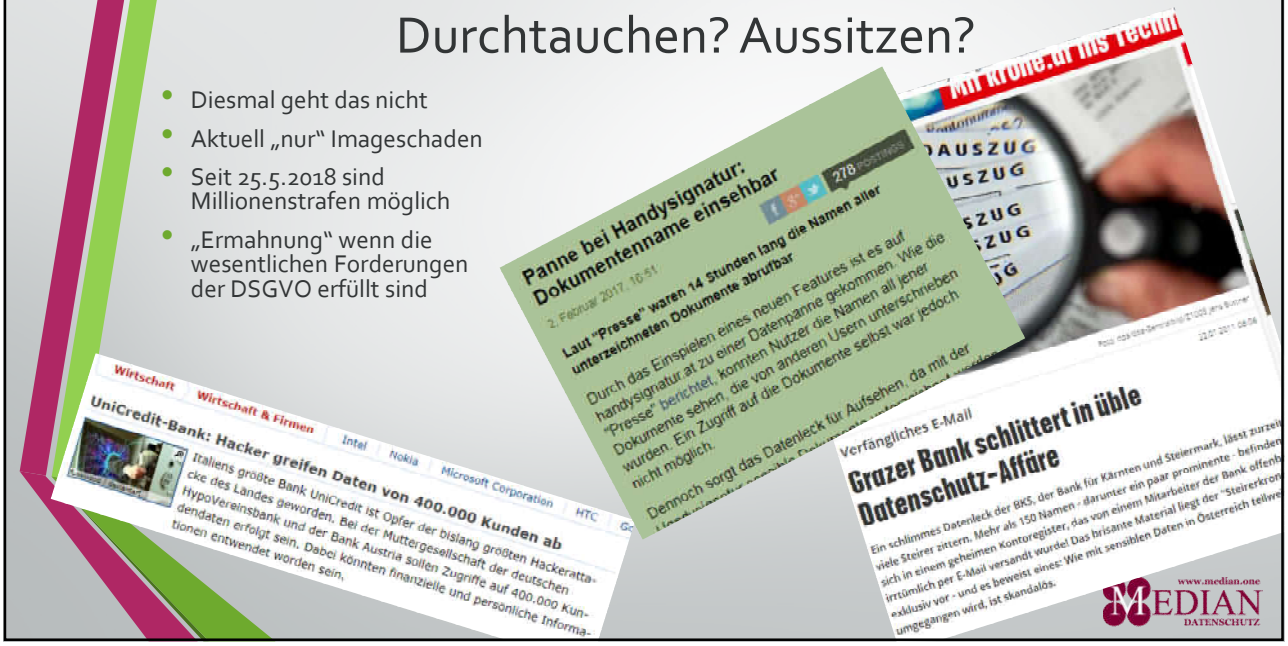
8.4 Informationssicherheit

Patchmanagement und Updates

- **Prozess definieren**
- Ermitteln verfügbarer/notwendiger Updates
  - o Vorhandene Systeme/Versionen/Patchstände
  - o Informationen über neue Updates/Patches
- Ausrollen von Updates/Patches
  - o Planung
  - o Automatisierung
- Prüfung / Kontrolle
  - o Erfolgreiche Installation von Patches
  - o Seiteneffekte

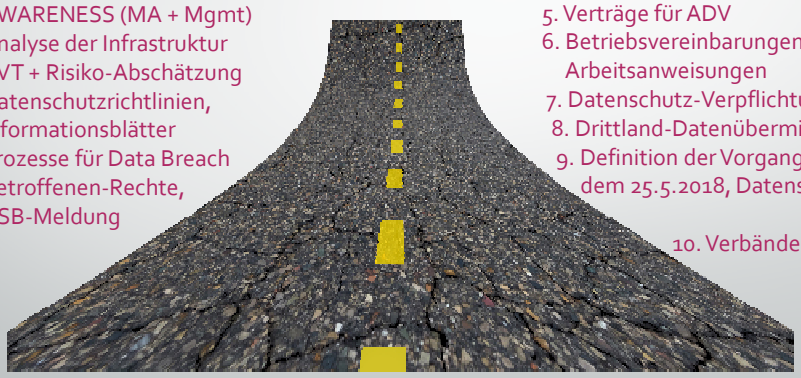
Durchtauchen? Aussitzen?

- Diesmal geht das nicht
- Aktuell „nur" Imageschaden
- Seit 25.5.2018 sind Millionenstrafen möglich
- „Ermahnung" wenn die wesentlichen Forderungen der DSGVO erfüllt sind



9. DSGVO-Fastlane

0. AWARENESS (MA + Mgmt)
1. Analyse der Infrastruktur
2. VVT + Risiko-Abschätzung
3. Datenschutzrichtlinien, Informationsblätter
4. Prozesse für Data Breach Betroffenen-Rechte, DSB-Meldung



5. Verträge für ADV
6. Betriebsvereinbarungen/ Arbeitsanweisungen
7. Datenschutz-Verpflichtungserklärungen
8. Drittland-Datenübermittlung?
9. Definition der Vorgangsweise nach dem 25.5.2018, Datenschutzbeauftragter?
10. Verbände: Code of Conduct

www.median.one
MEDIAN
DATENSCHUTZ

10. Code of Conduct

- Als Verband oder Interessensvertretung besteht die Möglichkeit eines „Code of Conducts"(CoC) im Sinne der DSGVO Art. 40
- Damit werden Verhaltensregeln definiert und vorab mit der Datenschutzbehörde(DSB) abgestimmt
- Nach Genehmigung der DSB hat der CoC Rechtsgültigkeit für Unternehmen die dem CoC beigetreten sind
- Vorteile:
  - Abstrakte Regelungen im Gesetz werden auf tatsächliche Geschäftsfälle abgebildet
  - Definition des „berechtigten Interesses"
  - Außergerichtliche Streitbeilegung bei Betroffenenrechten
  - Der genehmigte CoC wird von der DSB in einem öffentlichen Verzeichnis eingetragen
- Beispiel: Abfrage bei „Ediktsdatei"-Service wird als nicht „Profiling" definiert -> nur Widerruf, keine Erlaubnis nötig (Opt-Out)

11. e-PRIVACY-Verordnung (Entwurf)

- Detailumsetzung der DSGVO (zuständig: DSB)
- Umsetzung wird üblich
- Neue Regeln für digitale Medien und elektronische Kommunikationsdienste
  - OPT-IN (zB. für Tracking-Cookie´s wie Google Analytics)
  - Privacy by Default
- **Grundsatz**: Verarbeitung von Daten iZm. elektronischer Kommunikation ist generell verboten, es sei denn gültige Zustimmung des Betroffenen oder Ausnahmefälle
  - Verrechnung
  - Eigentlicher Grund des Service (zB. Anmeldung für Zugriff auf Daten)
- Massive Anpassung der Browser oder Webserver-Code notwendig
- Bestimmungen zur unerbetenen Kommunikation (Cold Call, Verzeichnisse,...)
  - Entspricht im wesentlichen dem österr. Telekommunikations-Gesetz
- Strafbestimmungen:
  - Anpassung an die DSGVO. -> 20 Mio o. 4%
    - Schadenersatz auch für immateriellen Schaden

Ing. Wolfgang Mader
Geschäftsführer
+43 664 350 21 96
wm@median.red

Datenschutzgrundverordnung

Danke für Ihre Aufmerksamkeit