Die neue EU-Datenschutz-grundverordnung (DS-GVO)

SoftENGINE

Die neue EU-Datenschutz-grundverordnung (DS-GVO)

Begriffserklärungen, wichtige Bestandteile und Aktionen zum Start...

SoftENGINE

wird angewandt ab:

Die neue Datenschutzgrundverordnung
wurde schon 2016 verabschiedet.
Die Anwendung erfolgt
ab dem 25.05.2018.

Die Verordnung konkretisiert
bestehende Verordnungen und
gleicht die nationalen Gesetze
einander an.

Worum geht’s…?

…um den Schutz
personenbezogener Daten

Was sind personenbezogene Daten?

Personenbezogene Daten sind all jene Informationen,
die sich auf eine natürliche Person beziehen
oder zumindest beziehbar sind und so Rückschlüsse
auf deren Persönlichkeit erlauben.

Lt. DSGVO:
Personenbezogene Daten sind lt. DSGVO Angaben,
die bei Zuordnung zu einer natürlichen Person Einblicke
ermöglichen in deren physische, physiologische, genetische,
psychische, wirtschaftliche, kulturelle oder soziale Identität
(Artikel 4 Ziffer 1 DSGVO).

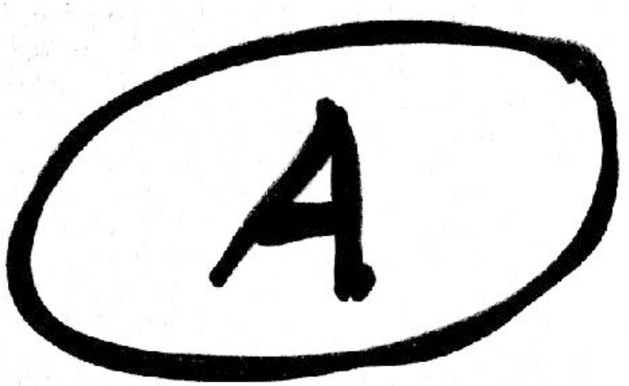
Beispiele für personenbezogene Daten:

- allgemeine Personendaten, wie bspw. Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer…
- Kennnummern - u.a. Sozialversicherungsnummer, Steueridentifikationsnummer, Personalausweisnummer, Passnummer…
- Bankdaten (Kontonummern, Kreditinformationen, Kontostände)
- Online-Daten (z.B. IP-Adresse)
- physische Merkmale (Geschlecht, Haarfarbe, Statur, Kleidergröße …)
- Besitzangaben (Fahrzeuge, Immobilieneigentum,Kfz-Kennzeichen, Zulassungsdaten …)
- Kundendaten (z.B. Belege)

Die EU-DSGVO

- hat unmittelbare Geltung in allen Mitgliedstaaten
- gilt vorrangig vor nationalem Recht
- Nationale Regelungen gelten neben der DS-GVO nur, soweit Bestimmungen der DS-GVO nicht entgegenstehen

Die künftige Rechtslage:



Datenschutz-Anpassungs-
und Umsetzungsgesetz EU
(DSAnpUG-EU) im Juni 2017
im Bundesgesetzblatt verkündet

„Datenschutz-Anpassungsgesetz 2018“
Novelle des DSG 2000 (künftig: DSG).

Wer ist betroffen?

- Unternehmen und Vereine, die in der EU Waren oder Leistungen anbieten, Mitarbeiter beschäftigen oder Mitglieder haben.

Wer ist verantwortlich?

- Geschäftsführer
- Inhaber
- Vorsitzende

Wer ist verantwortlich?

- Geschäftsführer
- Inhaber
- Vorsitzende

Die Verantwortung kann nicht delegiert werden!

Bestandteile der EU-DSGVO:

- Kopf (Titel, Grundlage, Verfahren)
- 173 Erwägungsgründe (zur Auslegung der Artikel)
- 99 Artikel (=verbindlicher Gesetzestext)

Klares Vorgehen hilft!

Lernen Sie zunächst wichtige Begriffe kennen…

Grundsätze für die Verarbeitung personenbezogener Daten

Klares Vorgehen! Begriffe kennen

Grundsätze für die Verarbeitung personenbezogener Daten

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Art. 5 (1) a) DS-GVO
- Zweckbindung, Art. 5 (1) b) DS-GVO
- Datenminimierung, Art. 5 (1) c) DS-GVO
- Richtigkeit, Art. 5 (1) d) DS-GVO
- Speicherbegrenzung, Art. 5 (1) e) DS-GVO
- Integrität und Vertraulichkeit, Art. 5 (1) f) DS-GVO
- Rechenschaftspflicht, Art. 5 (2) DS-GVO

Klares Vorgehen! Begriffe kennen

Was ist das? **Rechtmäßigkeit der Datenverarbeitung**

Für die Verarbeitung personenbezogener Daten gilt als allgemeiner Grundsatz ein sogenanntes

Verbot mit Erlaubnisvorbehalt

Die **Verarbeitung von Daten ist demnach nur zulässig,**
wenn eine Einwilligung oder eine andere in dieser Vorschrift normierte Ausnahme vorliegt.

Klares Vorgehen! Begriffe kennen

Was ist das? **Datensparsamkeit**

Nach Art 5 Abs 1 DSGVO muss die Verarbeitung personenbezogener Daten dem Zweck angemessen und sachlich relevant sowie auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein.

Klares Vorgehen! Begriffe kennen

Was ist das? **Zweckbindung**

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden.

Zudem sind grundsätzlich nur solche Änderungen des Verarbeitungszwecks erlaubt, die mit dem ursprünglichen Erhebungszweck vereinbar sind.
Dabei stellt die Datenschutz-Grundverordnung in Art 6 Abs 4 Kriterien auf, die bei der Beurteilung der Vereinbarkeit einer Zweckänderung zu berücksichtigen sind.

Klares Vorgehen! Begriffe kennen

Was ist das? **Datensicherheit**

Unter Berücksichtigung des Stands der Technik,
der Implementierungskosten sowie der Art, der Umstände und Zweck der Datenverarbeitung, aber auch der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten haben der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen umzusetzen und dadurch Datenschutzverletzungen zu vermeiden.

Dabei muss das Sicherheitslevel im Verhältnis zum Risiko angemessen sein

Klares Vorgehen! Begriffe kennen

Was ist das? **Übermittlung in Drittstaaten (außer EU)**

Eine Übermittlung von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die im Kapitel V zur Datenübermittlung in Drittländer und zu internationalen Organisationen niedergelegten Bedingungen erfüllen und auch die sonstigen Bestimmungen der Datenschutz-Grundverordnung beachtet werden (Art 44 DSGVO)

Klares Vorgehen! Begriffe kennen

Was ist das? **Betroffenenrechte**

Anforderungen an die **Transparenz** der Informationen

Katalog produktiver **Benachrichtigungen**

Auskunftsrecht der Betroffenen

Recht auf Berichtigung/Vervollständigung der erhobenen Daten

Recht auf Löschung = „**Recht auf Vergessenwerden**“

Einschränkung der Verarbeitung

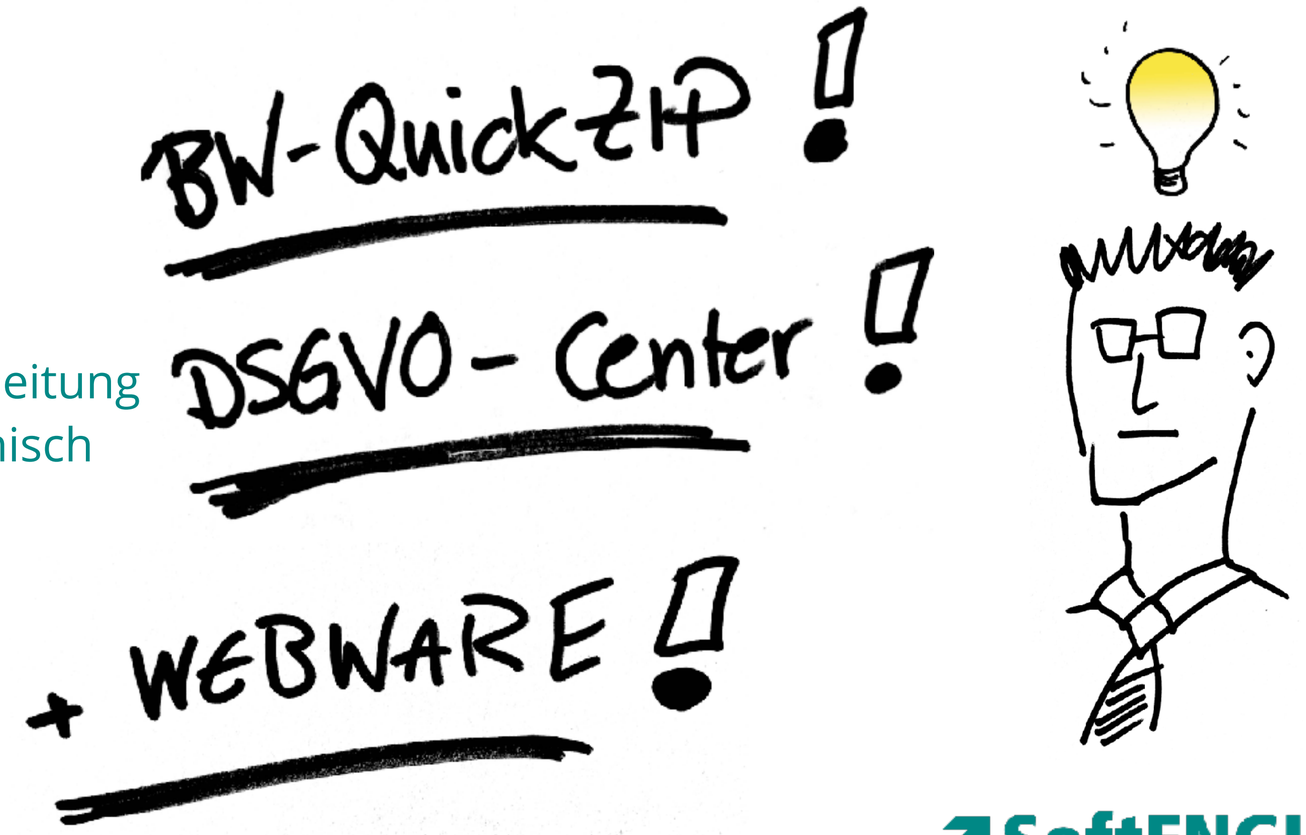
Recht auf Datenübertragbarkeit (Daten mitnehmen, z.B. zu anderem, Anbieter)

Allgemeines **Widerspruchsrecht** gegen die Verarbeitung

Klares Vorgehen! Begriffe kennen

Was ist das? „**Privacy by Design**“

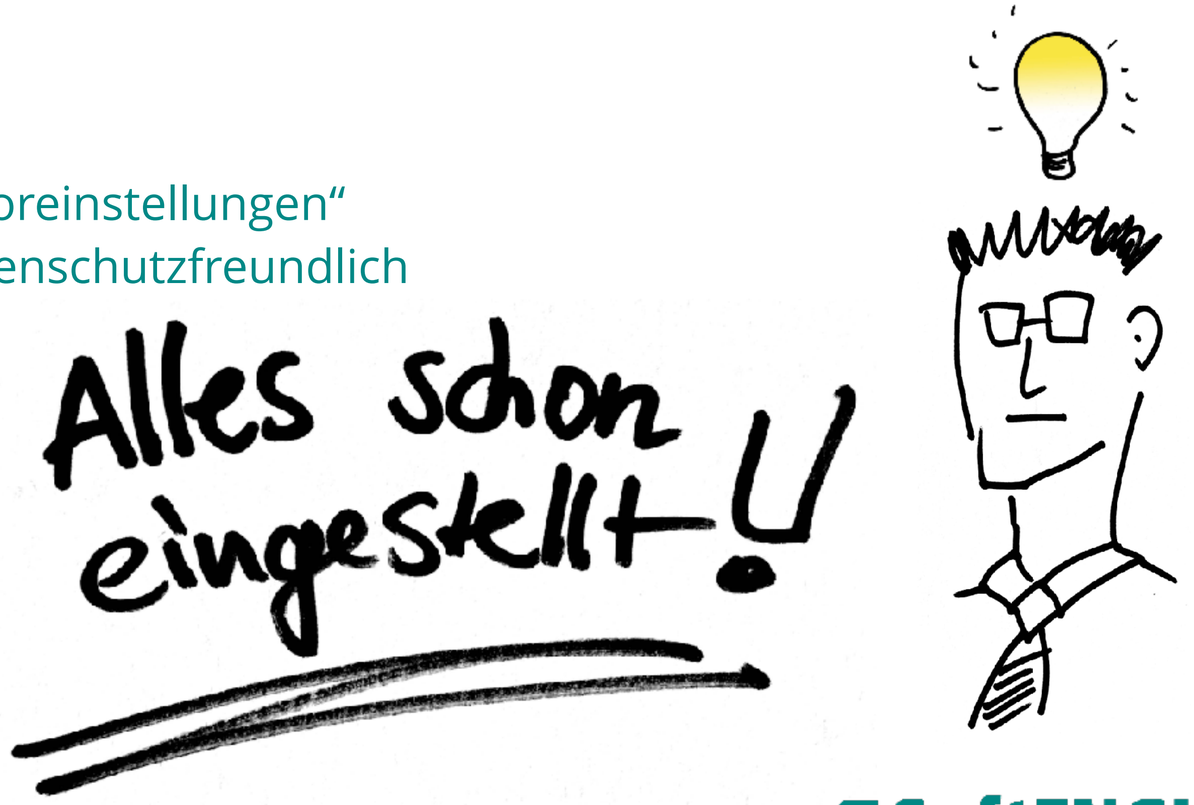
Übersetzt heißt Privacy by Design
„Datenschutz durch Technikgestaltung“
und greift den Grundgedanken auf,
dass sich der Datenschutz am besten
einhalten lässt, wenn er bereits bei Erarbeitung
eines Datenverarbeitungsvorgangs technisch
integriert ist.



Klares Vorgehen! Begriffe kennen

Was ist das?„Privacy by Default“

Privacy by Default heißt sinngemäß übersetzt
„Datenschutz durch datenschutzfreundliche Voreinstellungen“
und bedeutet, dass die Werkeinstellungen datenschutzfreundlich
auszugestalten sind.



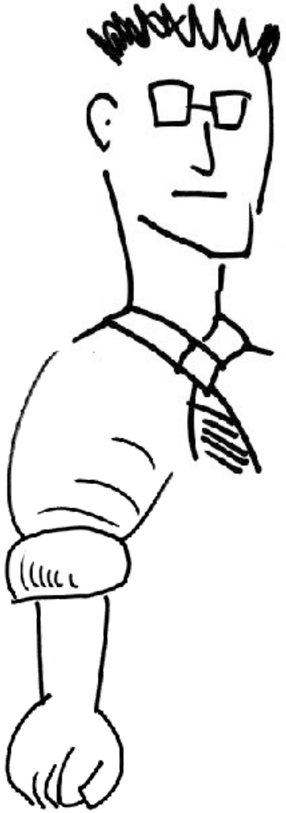
Klares Vorgehen! Was muss ich noch wissen...

Was ist noch geregelt:

- **Unabhängige Aufsicht**
  - jeder Mitgliedsstaat hat eine oder mehrere Aufsichtsbehörden einzurichten.
- **Effektive Durchsetzung**
  - umfangreiche Befugnisse für die Behörden werden festgelegt. Hohe Bußgelder.
- **Marktortprinzip**
- **Einheitliche Rechtsanwendung in der EU**
- **Meldungen von Datenschutzverletzungen** - Meldepflicht innerhalb 72 Stunden
- **Datenschutz-Folgenabschätzung**
- **Pflicht zur Bestellung eines Datenschutzbeauftragten**

Los geht's!

Was ist konkret zu tun...

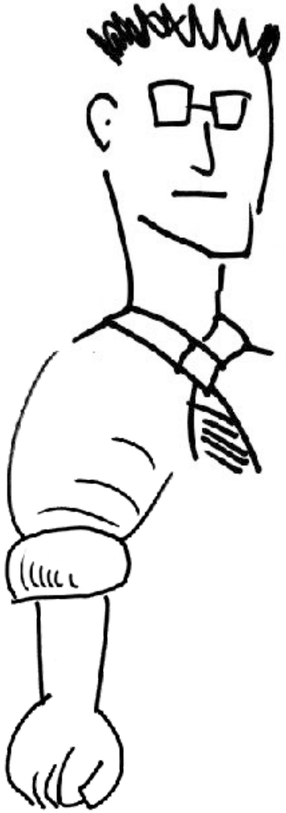


Los geht's! Was ist konkret zu tun...

- **Vor einer Datenerhebung ist der Nutzer zu informieren, welche Daten zu welchem Zweck gespeichert und verarbeitet werden, wie die Verarbeitung erfolgt und wie lange die Daten gespeichert/verarbeitet werden.**

Das betrifft beispielsweise gedruckte und Web-Formulare
ebenso, wie APPs, Internetshops und telefonische Abfragen,
außerdem sind die Datenschutzbestimmungen anzupassen (WEB!)

Prüfen + überarbeiten



Los geht's! Was ist konkret zu tun...

- **Der Verbraucher muss seine Einwilligung für jede Nutzungsart aktiv erteilen (Einwilligung in die Datenverarbeitung).**

Es darf keine vorausgefüllten Checkboxen mehr geben.
Jede Nutzung der Daten muss einzeln bestätigt werden.

Prüfen + überarbeiten

Los geht's! Was ist konkret zu tun...

- **Die DSGVO fordert (Art. 30), dass Verantwortliche ein Verzeichniss über alle Verarbeitungstätigkeiten führen, die im Unternehmen ausgeführt werden.**

Inhalt:
Verantwortlicher, Datenschutzbeauftragter, Abteilung
Bezeichnung der Verarbeitungstätigkeit
Beschreibung der Kategorien betroffener Personen
Beschreibung der Datenkategorien
Kategorien der Empfänger
Datenübermittlung an Dritte
Nennung der konkreten Datenempfänger
Fristen für Löschung
Technisch Organisatorische Maßnahmen (TOM)

„Überblick verschaffen
dokumentieren
verwalten
aktualisieren

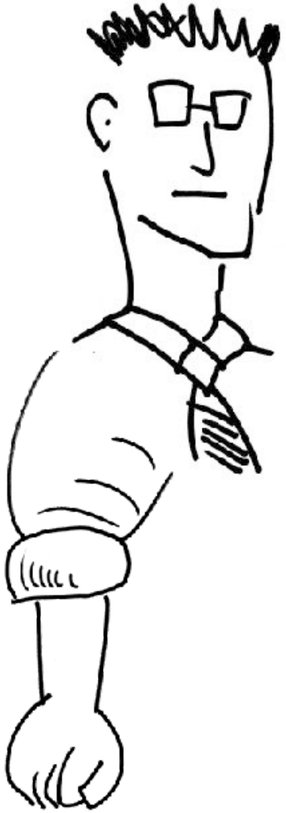
Los geht's! Was ist konkret zu tun...

- Unternehmen mit mehr als 250 Mitarbeitern müssen einen Datenschutzbeauftragten (DSB) ernennen und weiterbilden.
  Unternehmen ab 10 Mitarbeitern benötigen einen DSB, wenn sie sich regelmäßig mit automatisierter Datenerhebung, - Verarbeitung oder - Nutzung beschäftigen.
  Der DSB kann dann auch ein externer (qualifizierter) Dienstleister sein.

Los geht's! Was ist konkret zu tun...

- **Auftragsverarbeitung liegt vor, wenn eine natürliche oder juristische Person... personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.**

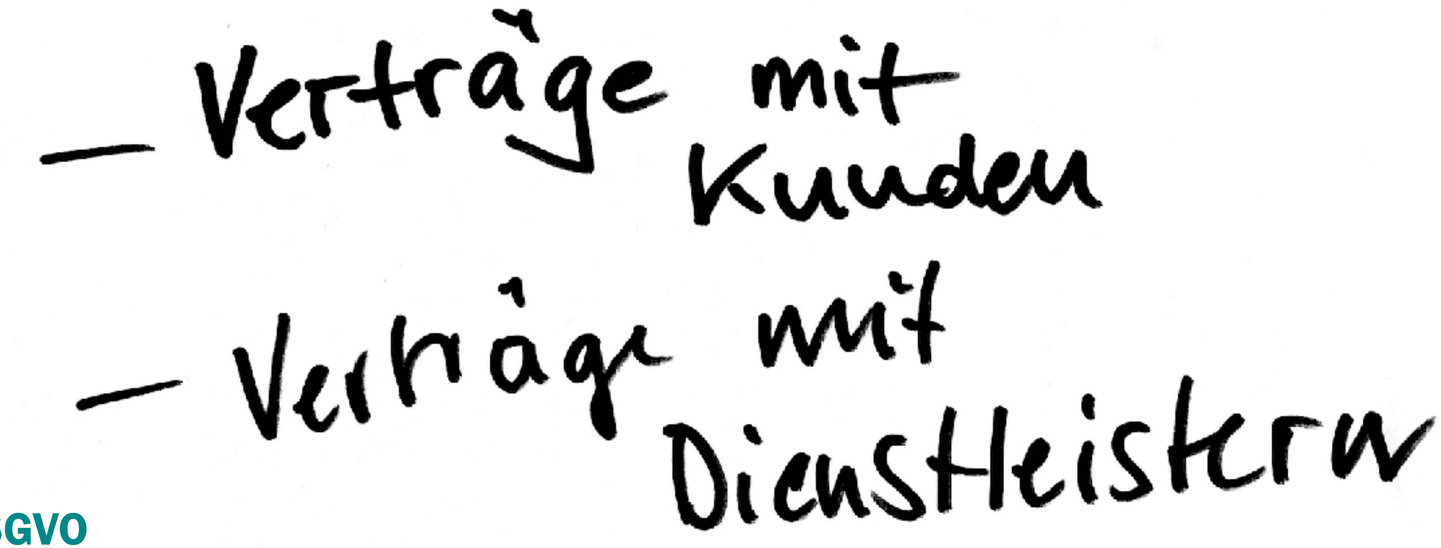
Vertragliche Regelung mit klarer Abgrenzung der Arbeiten
und Kontrollrechten ist nötig.
Bei sogenannten „weisungsfreien Branchen“ (z.B. Anwälte, Steuerberater)
muss kein Vertrag abgeschlossen werden.

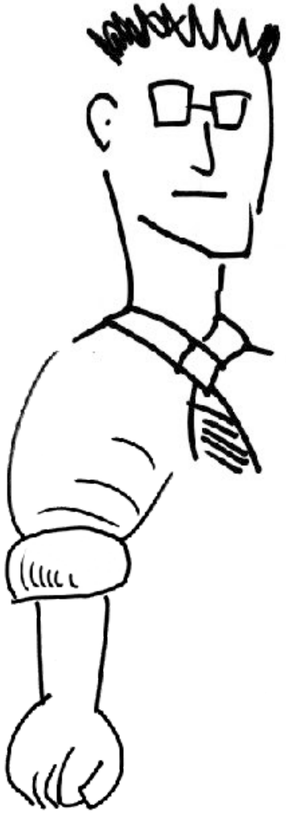


Los geht's! Was ist konkret zu tun...

- **Auftragsverarbeitung liegt vor, wenn eine natürliche oder juristische Person... personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.**

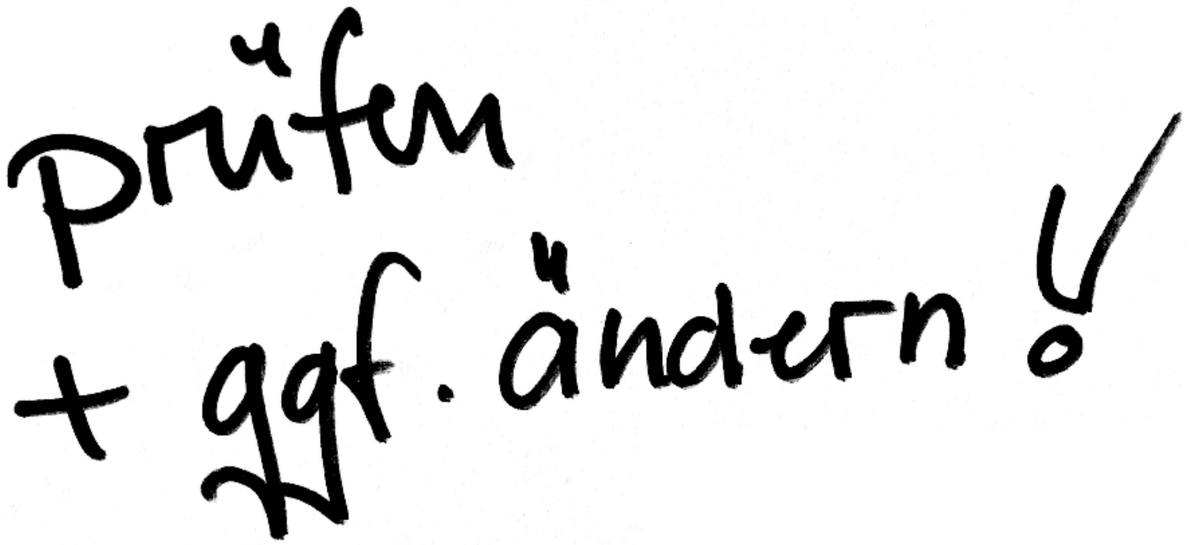
Vertragliche Regelung mit klarer Abgrenzung der Arbeiten und Kontrollrechten ist nötig.

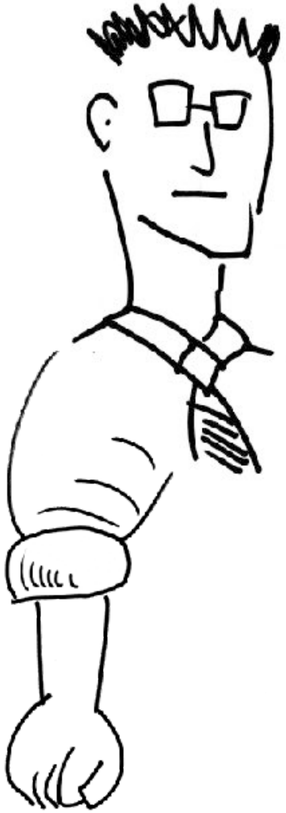




Los geht's! Was ist konkret zu tun...

- **Datenschutz mit Zweckbindung.**
  Die Daten dürfen nur für den Zweck genutzt/verarbeitet werden, für den sie erhoben wurden.



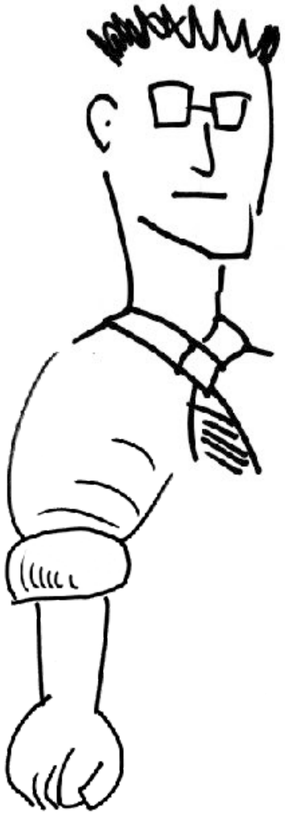


Los geht's! Was ist konkret zu tun...

- **Meldepflicht bei Datenschutzverletzungen.**

  Organisatorische Festlegungen treffen, wie Datenschutzverletzungen erkannt, protokolliert und gemeldet werden können.

Wichtig: Regelungen treffen + dokumentieren



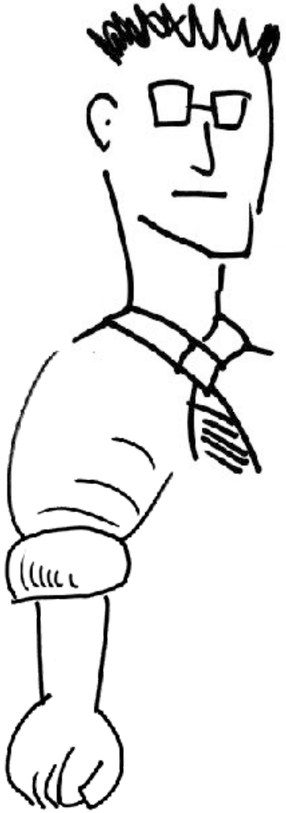
Los geht's! Was ist konkret zu tun...

- **Recht an den Daten / Recht auf Vergessenwerden - auf Verlangen müssen dem Verbraucher die gespeicherten Daten mitgeteilt werden bzw. auf entsprechende Aufforderung sind diese zu löschen.**

Prüfen, ob Daten gelöscht werden können bzw. ob diesem Ansinnen andere gesetzliche Regelungen (z.B. Aufbewahrungspflichten aus dem Steuerrecht) entgegenstehen.

Los geht's! Was ist konkret zu tun...

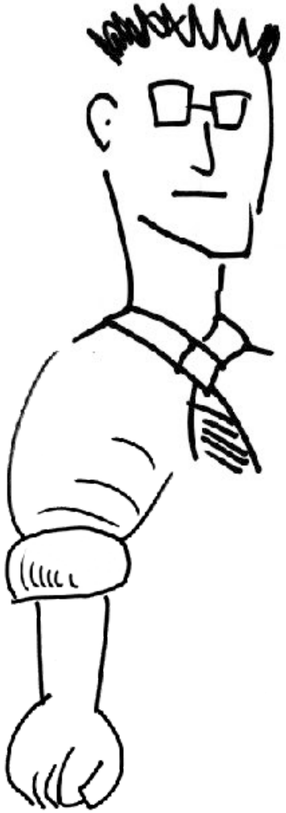
SoftENGINE



Los geht's! Was ist konkret zu tun...

- **Dateninhaber können die Übergabe ihrer Daten an einen anderen Dienstleister beauftragen.**

Prüfen, ob eine Ausgabe der Daten
in einer für andere lesbaren Form möglich
und sinnvoll ist.

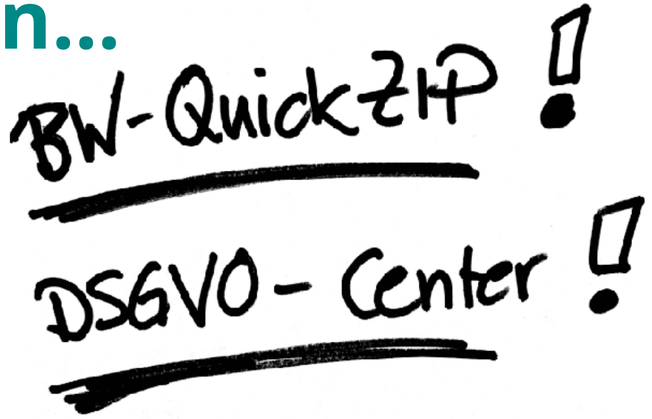


Los geht's! Was ist konkret zu tun...

Sicherheit der Verarbeitung garantieren

Zitat: „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**."

Los geht's! Was ist konkret zu tun...



- **Sicherheit der Verarbeitung garantieren**

Wichtige Maßnahmen hier können sein:

- Pseudonymisierung und Verschlüsselung von Daten
- Sicherstellung der Verfügbarkeit und Belastbarkeit von Systemen
- Datensicherungen und Wiederherstellbarkeit von Daten nach einem Zwischenfall
- Entwicklung von Test-/Prüfverfahren zur Beurteilung von Systemen

Konkrete Ansatzpunkte für **SoftENGINE und Partner und Kunden** (1)**:**

- **Verarbeitungstätigkeiten beschreiben**
- **Datensicherungen erstellen/verschlüsseln/sichern**
- **Dienstleistungen/Fehlersuchen/Unterstützung mit pseudonymisierten Daten ausführen**
- **unautorisierte Weitergabe von Daten verhindern (z.B. Übergaben von Datensätzen/-beständen an Drucker, Zwischenablage usw.)**
- **unautorisierten Zugriff auf Datenbestände verhindern**
- **unbeabsichtigtes „Zeigen“ von Daten verhindern (Bildschirm)**

Konkrete Ansatzpunkte für **SoftENGINE und Partner und Kunden** (2)**:**

- **gesicherte Kommunikation beispielsweise durch Zertifikate und Signaturen/Verschlüsselung**
- **Abläufe/Prozesse im Unternehmen auf Vereinbarkeit mit der EU-DSGVO prüfen (z.B. Arbeit mit Datensicherungen, Zugriff auf Fremde Systeme)**
- **Datenschutzmaßnahmen dokumentieren**
- **Datenschutzerklärung und Einwilligungen/Formulare überprüfen**
- **Verträge und Vertrags-/Geschäftsbedingungen überprüfen**

Keine