



Datenschutzgrundverordnung



Dr. Vohradsky & Friends
UNTERNEHMENSBERATUNG

Verein TWI Wirtschafts-Service, 19.4.2018
Überblick und ToDo's

S. 1

Agenda



- I. Ausgangssituation
- II. zentrale Themen der DSGVO
 - ❖ Beispiele dazu
- III. häufig gestellte Fragen
- IV. ToDo's bis 25.5.2018
- V. nützliche links – WKO

I. Ausgangssituation



Heute:

- jeder EU-Staat hat eigene DS-Gesetze
 - ❖ → fairer Wettbewerb?
 - ❖ Bsp.: Facebook in Irland

Zukunft (ab 25. Mai 2018):

- einheitliches DS-Gesetz in der gesamten EU
- hohe und einheitliche DS-Standards
- → Datenschutzgrundverordnung - DSGVO **MY TWI**

— Verein —

I. Ausgangssituation



Die DSGVO:

- regelt Verarbeitung von personenbezogenen Daten
- betrifft alle Unternehmen, die personenbezogene Daten von Menschen mit Aufenthalt (Wohnsitz, Urlaub,...) in der EU verarbeiten
 - ❖ Standort des Unternehmens dabei irrelevant
 - ❖ Marktteilnahme ist entscheidend

MY TWI

— Verein —

II. Zentrale Themen der DSGVO



- a) Betroffenenrechte
- b) Datensicherheit
- c) Pflichten des Verarbeitenden

- d) Verzeichnis der Verarbeitungstätigkeiten

II.a. Betroffenenrechte



- Auskunftsrecht
- Löschungsrecht, Recht auf Vergessenwerden
- Recht auf Einschränkung der Verarbeitung
- Widerspruchsrecht
- Berichtigungsrecht
- Recht auf Datenübertragbarkeit

ACHTUNG:

- Anträge innerhalb eines Monats abschließen!

Beispiel: Auskunft



- Auskunft an (ehemalige) Mitarbeiter oder Kunden
 - ❖ Verzeichnis der Verarbeitungstätigkeiten vorhanden?
 - ❖ strukturierter Prozess zur Auskunftserteilung?
 - ❖ Datenexport aus verschiedenen Quellen nötig?
 - ❖ Frist (1 Mon.) einhalten!

MY TWI
— Verein —
S. 7

Beispiel: Auskunft



- Auskunft muss enthalten:
 - ❖ Namen und Kontaktdaten des Verantwortlichen
 - ❖ ggf. Kontaktdaten des Datenschutzbeauftragten
 - ❖ Zwecke der Verarbeitung
 - ❖ Rechtsgrundlage der Verarbeitung
 - ❖ Empfänger der Daten
 - ❖ Dauer der Datenspeicherung, oder wenn unmöglich, die Kriterien für die Festlegung der Dauer
 - ❖ Belehrung über die Betroffenenrechte und Beschwerdemöglichkeiten
 - ❖ ggf. automatisierte Entscheidungsfindung (vgl. Amazon-Logik)

MY TWI
— Verein —
S. 8

Beispiel: Löschung



- Aufforderung zur Löschung inkl. nachvollziehbarem Nachweis dazu
 - ❖ Verzeichnis der Verarbeitungstätigkeiten vorhanden?
 - ❖ strukturierter Prozess zur Löschung aus allen Speicherorten?
 - inkl. Prüfungsprozess, ob Löschung erlaubt
 - ❖ strukturierter Prozess zur Dokumentation der Löschung?
 - ❖ ggf. Kommunikation mit Auftragsverarbeiter
 - ❖ Frist (1 Mon.) einhalten!

MY TWI
— Verein —
S. 9

II.b. Datensicherheit



- Vertraulichkeit
- Integrität
- Verfügbarkeit
- technische u. organisatorische Maßnahmen (TOMs)
 - ❖ = Privacy by Design + Privacy by Default

ACHTUNG:

- Dokumentationspflicht!

MY TWI
— Verein —
S. 10

II.b. Datensicherheit



- Vertraulichkeit
 - ❖ Schutz vor unbefugtem Zugriff
 - ❖ → z.B. Zutritts-/Zugangskontrollen, Zugriffsbeschränkungen, Verpflichtung zum Datengeheimnis
- Integrität
 - ❖ Schutz vor unbefugter Veränderung
 - ❖ → z.B. Zugriffsbeschränkungen, Schulungen, Logs
- Verfügbarkeit
 - ❖ Schutz vor Verlust oder Vernichtung
 - ❖ → z.B. Systeme zur Wiederherstellung, klare Prozessabläufe

MY TWI
— Verein —
S. 11

II.b. Datensicherheit



- Privacy by Design
 - ❖ Sicherstellung des Datenschutzes durch technische Maßnahmen
 - Verschlüsselung, Anonymisierung, o.ä.
 - Minimierung der DV
 - ❖ Sicherstellung des Datenschutzes durch organisatorische Maßnahmen
 - klare Zuständigkeiten
 - definierte Prozesse
 - Schulungen
 - Prüf- und Kontrollverfahren (Compliance)

MY TWI
— Verein —
S. 12

II.b. Datensicherheit



- Privacy by Default
 - ❖ datenschutzfreundliche Voreinstellungen
 - keine automatische Voreinstellung von Einwilligungen
 - Verarbeitung nur der minimal erforderlichen Daten
 - verschlüsselte Kommunikation

II.c. Pflichten des Verarbeitenden



- Rechtsgrundlagen der Datenverarbeitung
 - ❖ berechtigtes Interesse
 - Erfüllung eines Vertrags
 - vorvertragliche Maßnahmen auf eine Anfrage hin
 - Erfüllung einer rechtlichen Verpflichtung
 - Interessensabwägung
 - Schutz lebenswichtiger Interessender betroffenen Person oder einer anderen natürlichen Person
 - öffentliches Interesse oder Ausübung öffentlicher Gewalt
 - ❖ Einwilligung der betroffenen Person

II.c. Pflichten des Verarbeitenden



- Wahrung der Betroffenenrechte
- Gewährleistung der Datensicherheit
- Verzeichnis der Verarbeitungstätigkeiten
- Informationspflicht
- Meldung von Datenschutzvorfällen
 - ❖ binnen 72 Stunden
- Risikoanalysen und ggf. Datenschutz-Folgenabschätzung
 - ❖ verpflichtend, wenn ein sog. „hohes Risiko“ vorliegt

MY TWI
— Verein —
S. 15

Beispiel: Folgenabschätzung



- bei sog. „hohem Risiko“:
 - ❖ systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen
 - „Amazon-Logik“, Profiling
 - ❖ umfangreiche Verarbeitung sensibler Daten
- Folgenabschätzung = Evaluierung der DV
 - ❖ hinsichtlich Auswirkungen und Risiken auf die Rechte der Betroffenen
 - ❖ und die Folgen der Verarbeitungen für den Datenschutz
 - Dokumentation

MY TWI
— Verein —
S. 16

Sensible Daten



- = „besondere Kategorien von Daten“
 - ❖ ethnische Herkunft
 - ❖ Religionszugehörigkeit
 - ❖ politische oder weltanschauliche Einstellungen
 - ❖ sexuelle Orientierung
 - ❖ Gewerkschaftszugehörigkeit
 - ❖ Gesundheitsdaten
 - ❖ biometrische und genetische Daten
 - ❖ (SV-Nummer)

MY TWI
— Verein —
S. 17

II.d. Verzeichnis der Verarbeitungstätigkeiten



- strukturierte Auflistung alle durchgeführten Verarbeitungstätigkeiten
- zwingend zu führen, wenn
 - ❖ das Unternehmen mehr als 250 MA hat
 - ❖ eine „nicht nur gelegentliche“ Datenverarbeitung erfolgt

MY TWI
— Verein —
S. 18

II.d. Verzeichnis



- vorgeschriebener Inhalt:
 - ❖ Name und Kontaktdaten des Verantwortlichen, des Vertreters und ggf. des Datenschutzbeauftragten
 - ❖ Zweck der Verarbeitung
 - ❖ betroffene Personen, Kategorien betroffener Personen
 - ❖ relevante Empfänger, Kategorien relevanter Empfänger
 - ❖ Fristen zur Löschung der Daten
 - ❖ ggf. Informationen zu betroffenen Drittländern
 - ❖ TOMs zur sicheren Datenverarbeitung

MY TWI
— Verein —
S. 19

III. häufige gestellte Fragen



- Benötigen wir einen Datenschutzbeauftragten?
 - ❖ → ein DS-Beauftragter ist nur verpflichtend, wenn die Kerntätigkeit des Unternehmens...
 - ... in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung/Auswertung von (Daten von) betroffenen Personen erforderlich machen.
 - ... in der umfangreichen Verarbeitung sensibler Daten oder von Daten über strafrechtliche Verurteilungen oder Straftaten besteht.

MY TWI
— Verein —
S. 20

III. häufige gestellte Fragen



- Sind Überwachungskameras erlaubt?
 - ❖ → „Bildaufnahmen“ (mit/ohne Ton) sind zulässig, wenn...
 - ... ein berechtigte Interessen des Verantwortlichen besteht und die Verhältnismäßigkeit gegeben ist
 - ... sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt sind
 - ... betroffene Personen eingewilligt haben
 - ... sie im lebenswichtigen Interesse einer Person erforderlich sind.

MY TWI
— Verein —
S. 21

III. häufige gestellte Fragen



- Gibt es Geldstrafen? → Ja, insbesondere bei Verletzung...
 - ❖ ... von Betroffenenrechten (bis zu 4% oder € 20mio)
 - Informations- und Auskunftsrechte / -pflichten
 - Berichtigungsrecht
 - Recht auf Löschung („Vergessenwerden“)
 - ...
 - ❖ ... der Datensicherheit (bis zu 2% oder € 10mio)
 - Vertraulichkeit (Schutz vor Zugriff)
 - Integrität (Schutz vor Veränderung)
 - Verfügbarkeit (Schutz vor Verlust)
 - ...
 - ❖ ... der Dokumentationspflicht (bis zu 2% oder € 10mio)
 - Verarbeitungsverzeichnis

MY TWI
— Verein —
S. 22

IV. mind. ToDo's bis 25.5.2018



1. Verarbeitungsverzeichnis erstellen
(Auflistung aller personenbezogenen Daten, die im Unternehmen verarbeitet werden)
 - a) ggf. Datenschutz-Folgenabschätzungen dazu
2. Überprüfung aller Rechtsgrundlagen und ggf. Einwilligungsprozesse
3. Prozesse auf die Betroffenenrechte einrichten

MY TWI
— Verein —
S. 23

IV. mind. ToDo's bis 25.5.2018



4. Überprüfung und Anpassung aller Auftragsverarbeitungsverträge
5. Überprüfung/Anpassung sämtlicher Rechtstexte
 - ❖ Datenschutzinformationen
 - ❖ Allgemeine Geschäftsbedingungen
 - ❖ sonstige Informationstexte (online, offline) in Bezug auf die Informationspflichten
 - ❖ Einwilligungstexte

MY TWI
— Verein —
S. 24

V. nützliche links – WKO



- Überblick
 - ❖ <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html>
- Verarbeitungsverzeichnis
 - ❖ <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html>
- Betroffenenrecht „Auskunft“
 - ❖ <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-musterschreiben-auskunftserteilung.html>

MY TWI
— Verein —
S. 25

MY TWI
— Verein —



DSGVO

Viel Erfolg!



Dr. Vohradsky & Friends
UNTERNEHMENSBERATUNG

Dr. Christian Vohradsky, MBA
office@vohradsky.com