Eine Stunde Datenschutz

Datenschutz für EPU

Eine Stunde Datenschutz

- Webinar-Reihe des Arbeitskreises Datenschutz sowie des Servicezentrums, Team Rechtsservice, der Wirtschaftskammer Kärnten

- Vortragende:

  Dr. Ludwig Notsch

  Ing. Walter Wratschko

- Moderation:

  Dr. Christina Kitz-Überall

Eine Stunde Datenschutz
Datenschutz für EPU

- INTERNETJURIST.AT | Dr. iur. Ludwig Notsch I Lastenstraße 14, 9020 Klagenfurt
  Klagenfurt –Wien -Milano
  T+43 463 310 557 I E kontakt@internetjurist.at I www.internetjurist.at

- Ing. Walter Wratschko, geprüfter Datenschutzexperte
  Office Klagenfurt: Brunnplatz 5, 9020, Office Wien: Esteplatz 3, 1030
  T +43 699 1504 3860
  E walter.wratschko@datenschutz-sued.at I www.datenschutz-sued.at

- https://www.wko.at/branchen/k/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/arbeitskreis-datenschutzexperten.html

- Dr. Christina Kitz-Überall, Servicezentrum, Rechtsservice, Wirtschaftskammer Kärnten, christina.kitz-ueberall@wkk.or.at I 0590904-723

Datenschutz für EPU

Dr.iur. Ludwig Notsch & Ing. Walter Wratschko

Alle Rechte vorbehalten

Die Außenwirkung

Datenschutzerklärung auf der Homepage

- Erfüllung der Informations**pflichten** nach Art 13 und 14 DSGVO
- Personenbezogene Daten, die direkt bei der „betroffenen Person“ erhoben werden

- Zwingende Inhalte sind beispielsweise
  Name und Kontaktdaten des Verantwortlichen = jedes EPU höchstpersönlich
  Zweck der Datenverarbeitung
  Rechtsgrundlagen der Datenverarbeitung
  Dauer der Datenspeicherung bzw. Kriterien für die Dauer

Die Außenwirkung

Datenschutzerklärung auf der Homepage

- Zwingende Inhalte (Teil II) sind beispielsweise

  Empfänger/ Kategorien der erhobenen Daten

  Absicht die Daten in **Drittländer** zu übertragen (sicheres/ unsicheres Drittland)

  berechtigtes Interesse (Argumentationskette erforderlich)

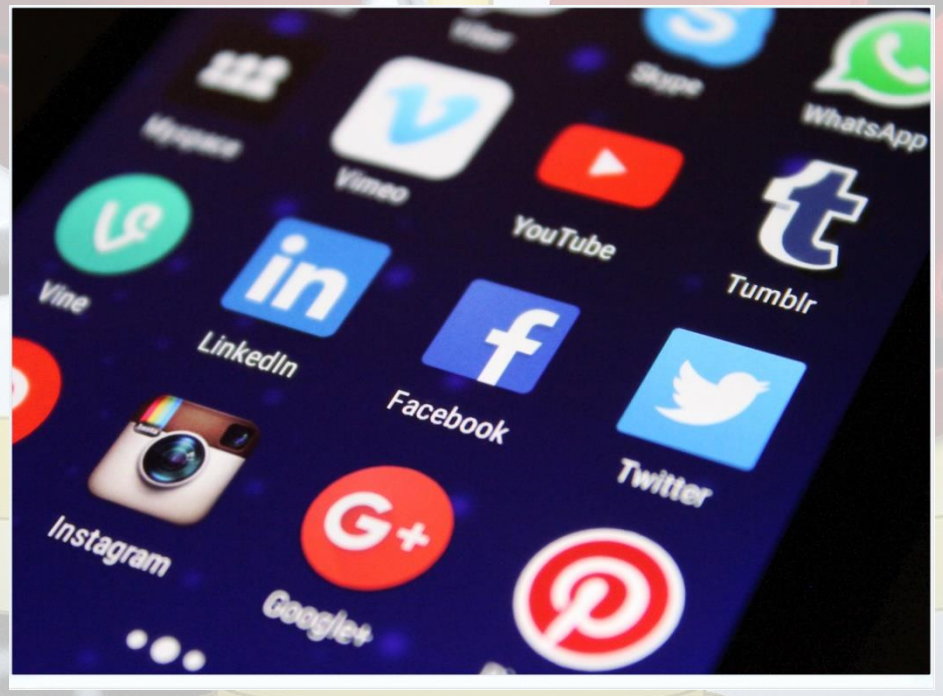
Die Außenwirkung

Warum ist die Datenschutzerklärung so wichtig?

- Für jeden unmittelbar einsehbar = **öffentlich**
- **Aktualität** sofort erkennbar
  Beispiel **EU – US Data Privacy Framework**: Steht da noch das Privacy Shield, ist die Datenschutzerklärung ziemlich ALT

- Erste **Angriffsfläche** für Wettbewerb, unzufriedene „Ex“-Mitarbeiter, Kunden, etc

Datenschutz in Social Media



Internationaler Datenverkehr

Datenschutz in Social Media

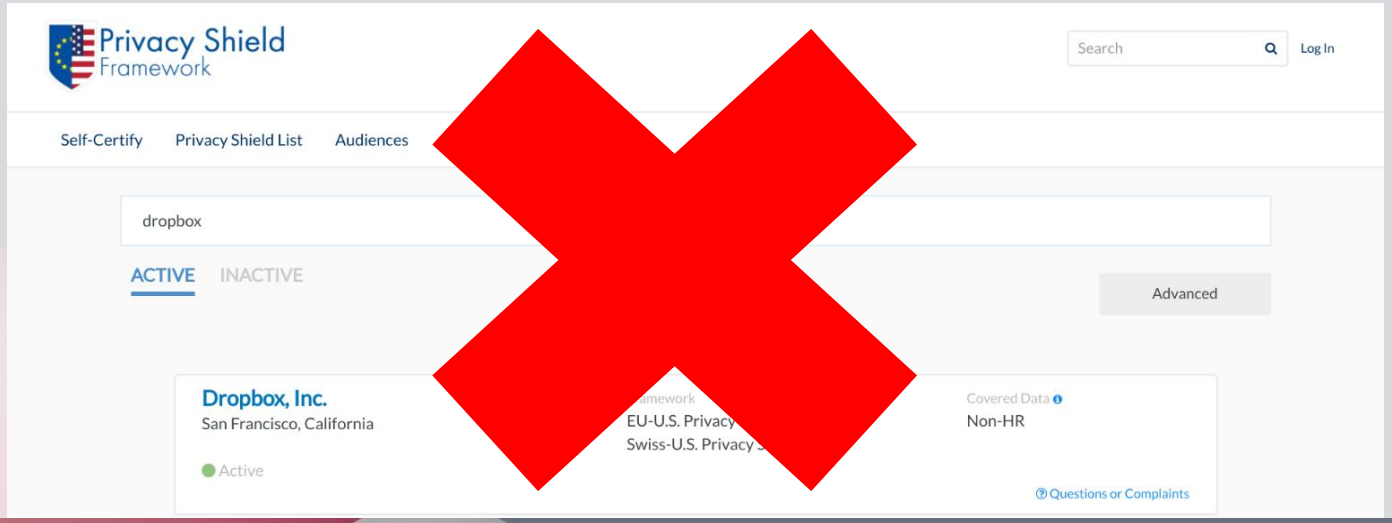
Am Beispiel Meta:
Facebook Fanpage & Instagram Businessaccount

- brauchen eine eigene Datenschutzerklärung
- Warum?
  Abgrenzung der datenschutzrechtlichen Verantwortlichkeit zw. Meta und uns als Betreiber einer Fanpage bzw. eines Insta-Businessaccounts
- verpflichtend seit EuGH Urteil in der Rechtssache C-210/16 vom **05.06.2018**

Drittstaaten-Thematik am Beispiel USA

Privacy Shield = Geschichte

ACHTUNG: Der Privacy Shield ist seit **16.7.2020** außer Kraft!
Es ist somit eine eigene AVV bei Datenübermittlung an Drittstaat USA erforderlich, um rechtskonform zu arbeiten



Drittstaaten-Thematik am Beispiel USA

NEU = E.U. – U.S. Data Privacy Framework

Angemessenheitsbeschluss der Europäischen Kommission

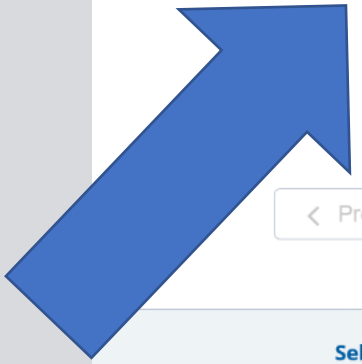
U.S. Diensteanbieter muss entsprechend als **AKTIV** gelistet sein

Auftragsdatenverarbeitungsvereinbarung muss abgeschlossen sein

Drittstaaten-Thematik am Beispiel USA

Ist mein U.S. Diensteanbieter gelistet?
ZB Microsoft, Apple, Google, etc

Direkter Check über:
https://www.dataprivacyframework.gov/s/



DATA PRIVACY FRAMEWORK PROGRAM

Search

Log in

Home | Self-Certify | Data Privacy Framework List | Audiences | About

ACTIVE | INACTIVE

Search

Advanced Search

Previous

Next

Self-Certify

Data Privacy Framework List

Audiences
U.S. Businesses
European Businesses
European Individuals
Data Protection Authorities

About
Program Overview
Framework Text
Inactive Participants
News & Events
Contact
Privacy Program

Home | **Website Feedback** | **Privacy Policy** | **Disclaimer** | **FOIA** | **USA.gov**

INTERNATIONAL TRADE ADMINISTRATION

The International Trade Administration (ITA), U.S. Department of Commerce manages this site to facilitate the Data Privacy Framework program in the United States. External links to other Internet sites should not be construed as an endorsement of the views or privacy policies contained therein. This site contains PDF documents. A PDF Reader is available from Adobe Systems Incorporated.

U.S. Department of Commerce | Data Privacy Framework Program | 1401 Constitution Avenue, N.W. | Room 11018 | Washington, D.C. 20230

DANKE!
für die
Aufmerksamkeit

und nun weiter zu den
Dokumentationspflichten!

Was ist zu tun?

Korrektes Erfüllen der

- ➢ Informationspflicht (wie gerade besprochen)
- ➢ Rechenschaftspflicht (wie in den letzten Webinaren besprochen)

- ➢ *Dokumentationspflichten*

Die Dokumentationspflichten

1. Welche regelmäßigen Verarbeitungstätigkeiten werden von mir mit welchen Mitteln durchgeführt?

2. Wie stelle ich effiziente und effektive Datenschutz- und Datensicherheitsmaßnahmen sicher?
   und in naher Zukunft:

3. Welche KI-Tools habe ich im Einsatz? (Transparenzpflicht)

Das Verarbeitungsverzeichnis (1/4)

Was muss verpflichtend angegeben werden:

1. Name und Kontaktdaten des Verantwortlichen und, falls vorhanden:
   Name und Kontaktdaten des Vertreters und/oder des Datenschutzbeauftragten
2. Zweck der Datenverarbeitung
3. Rechtsgrundlage
4. Kategorie der betroffenen Personen
5. Kategorien der personenbezogenen Daten
6. Kategorien von Empfängern
7. Löschfristen
8. Beschreibung der technischen und organisatorischen Maßnahmen

Das Verarbeitungsverzeichnis (2/4)

Zweck der Datenverarbeitung:

Angebots- und Rechnungslegung, Buchhaltung, Marketing, Newsletter, Kontakt-Management, Videoüberwachung,...

Rechtsgrundlage:

gesetzliche Verpflichtung, Erfüllung eines Vertrags, berechtigte Interessen des Verantwortlichen, Einwilligung,...

Das Verarbeitungsverzeichnis (3/4)

Kategorie der betroffenen Personen:

Kunden, Lieferanten, Interessenten, …

Kategorien der personenbezogenen Daten:

Name, Adresse, IP-Adresse, Geburtsdatum, ...

Kategorien von Empfängern:

Hosting-Anbieter, Cloud-Anbieter, Steuerberater, externe Buchhalter, Behörden, Bank,...

falls zutreffend: Übermittlung der Daten in Drittländer und an internationale Organisationen ***inklusive*** der entsprechende Garantien für die Einhaltung der DSGVO

Das Verarbeitungsverzeichnis (4/4)

Löschfristen:

Rechnung für 7 Jahre, Webseiten Interessenten 1 Jahr, versteckter Schaden 30 Jahre, Urheberrecht lebenslänglich…

Beschreibung der technischen und organisatorischen Maßnahmen:

Verschlüsselung, Pseudonymisierung, Backup, Zugriffskontrollen, ...

TOM‘s: Der gesetzliche Auftrag (Artikel 32 DSGVO)

Unter Berücksichtigung des

- Stands der Technik
- der Implementierungskosten und
- der Art, des Umfangs,
- der Umstände und der Zweck der Verarbeitung sowie
- der unterschiedlichen **Eintrittswahrscheinlichkeiten** und
- der 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.

Die technischen Mindestanforderungen

- **siehe Präsentation der zweiten Stunde Datenschutz:**
- *https://www.wko.at/ktn/wirtschaftsrecht/webinar-reihe--eine-stunde-datenschutz*

Schlaglichter zum Datenschutz im Alltag

- **Disaster Recovery für EPU**
  - Fernlöschung der nicht mehr vertrauenswürdigen Geräte sicherstellen..
  - IMEI-Nummern eruieren: *#06#
- **2-Stufen-Authentifizierung auch nutzen, wenn angeboten**
  - Biometrische Daten
  - Einmalkennwort bzw. TAN. ...
  - Kennwort per App. ...
  - ID-Austria
  - QR-Codes

Schlaglichter zum Datenschutz im Alltag

- **Wenn es schon Passwörter sein müssen..**
  - kein „Reichseinheits“-Passwort
  - das Mouse Pad ist kein Passwortkäfig…
  - der Passwort-Manager ist kein Passwort-Safe
- Laptop wegräumen im Cafe….
- Shouldersurfer verhindern im Zug
  - Bei Blickschutzfilter nicht auf den Preis schauen…
- Öffentliche Netze / WLAN im Hotel

Schlaglichter zum Datenschutz im Alltag

- **Haltbarkeit der Datenbestände**
  - USB-Stick → SSD →HDD
- **Backups oder: Was speichere ich wo?**
  - Cloud ist gut, aber…
  - besser EWR-Anbieter, wenn….
- **Wofür zahle ich eigentlich eh schon regelmäßig?**

Die Dokumentation der TOM (1/3)

- **technische Maßnahmen:** physischer und digitaler Schutz
- **organisatorische Maßnahmen:** Richtlinien und Verfahren

- Keine Formvorschriften, ausser:
- Nach **Ermittlung des Status Quo ihrer Infrastruktur** erstellen Sie einen auch zeitlich definierten **Maßnahmenplan** für die Behebung der wahrgenommenen Problemfelder.

Die Dokumentation der TOM (2/3)

- alle Maßnahmen zur Umsetzung der Zutrittskontrolle
  - Alarmanlagen, Schließsysteme,....
- alle Maßnahmen zur Umsetzung der Zugangskontrolle
  - Firewall, Verschlüsselung von Datenträgern,....
- alle Maßnahmen zur Umsetzung der Zugriffskontrolle
  - Passwortrichtlinien, Löschanweisungen,....

Die Dokumentation der TOM (2/3)

- alle Maßnahmen zur Umsetzung der Zugriffskontrolle
  - Passwortrichtlinien, Löschanweisungen,....
- alle Maßnahmen zur Umsetzung der Weitergabekontrolle
  - E-Mail Verschlüsselung, verschlüsselter USB-Stick,....
- alle Maßnahmen zur Umsetzung der Verfügbarkeitskontrolle
  - Feuer- und Rauchmelder, Plattenspiegelungen,....

Die Dokumentation der TOM (3/3)

- alle **Maßnahmen zur Umsetzung des Trennungsgebots**
  - Physische Trennung von Daten und Betriebssystem
  - Speicherung von personenbezogenen Daten je nach Zweck in unterschiedlichen Datenbanken →folglich: Excel ist **schlecht!!**

- Prüfen Sie alle Ihre **Auftragsverarbeiter**?
  - Spiegeln die dort angegeben TOMs die Realität wieder?
  - Vorabkontrolle bei dem potentiellen Auftragsverarbeiter

Die Dokumentation der TOM (3/3)

- Bestehen Verfahren zur **Wiederherstellung** der Verfügbarkeit?

  :::::::::

- Existieren Verfahren regelmäßiger Überprüfung und Evaluierung der **Wirksamkeit** der technischen und organisatorischen Maßnahmen?

Terminaviso

Nächste Folge „1 Stunde Datenschutz“ am

15.5.2024

von 09:00 bis 10:30 Uhr