FH | JOANNEUM
University of Applied Sciences

Interreg AUSTRIA-HUNGARY

Co-funded by the European Union

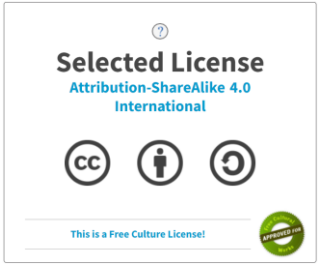
Trendig Plus
AN INTEGRATED BORDER REGION

Cybersecurity mit Fokus auf Datenschutz
Cybersecurity focusing on privacy

Sabine Proßnegg
Fachhochschule JOANNEUM Kapfenberg
University of Applied Sciences in Kapfenberg

30. April 2025

Bildquellen: Pexels / Pixabay



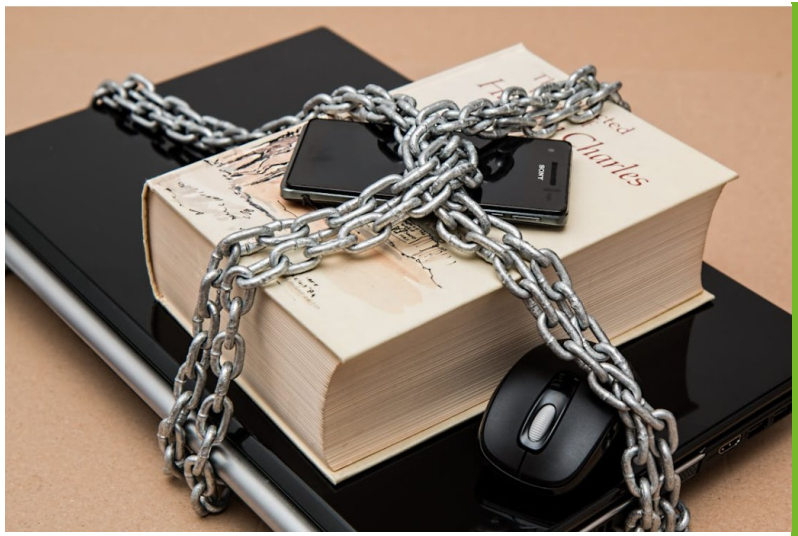
1

Interreg AUSTRIA-HUNGARY
Co-funded by the European Union
Trendig Plus AN INTEGRATED BORDER REGION
FH JOANNEUM University of Applied Sciences

Ziel / Target

Bewusstseinsbildung in KMU/

Raising awareness in SME



Pexels.com: Pixabay

Interreg AUSTRIA–HUNGARY
Co-funded by the European Union
Trendig Plus AN INTEGRATED BORDER REGION
FH JOANNEUM University of Applied Sciences

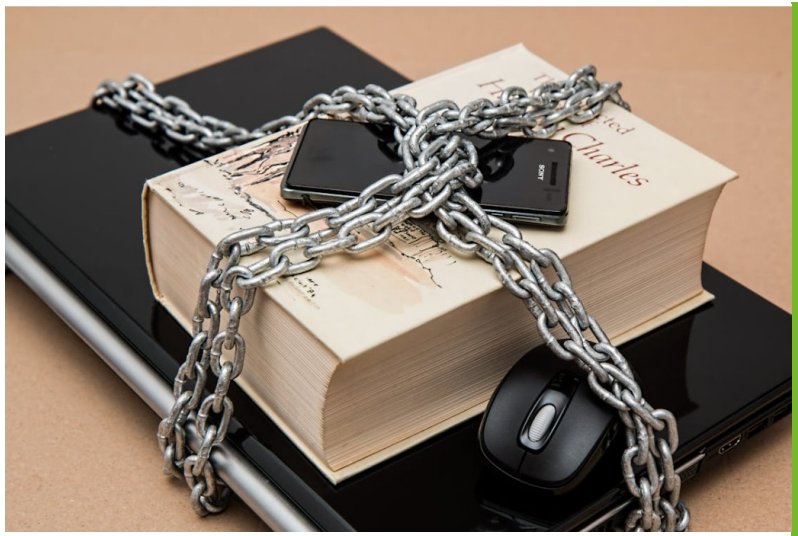
Agenda

Agenda

Warum? Why?

Wie? How?

Nächsten Schritte / Take aways



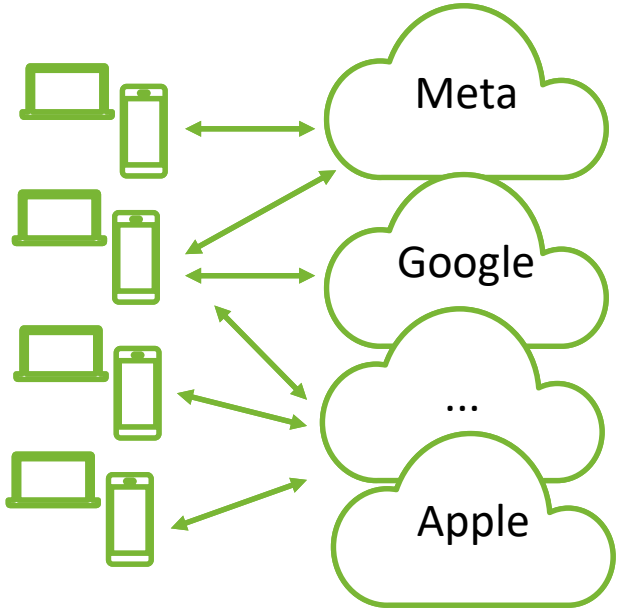
Pexels.com: Pixabay

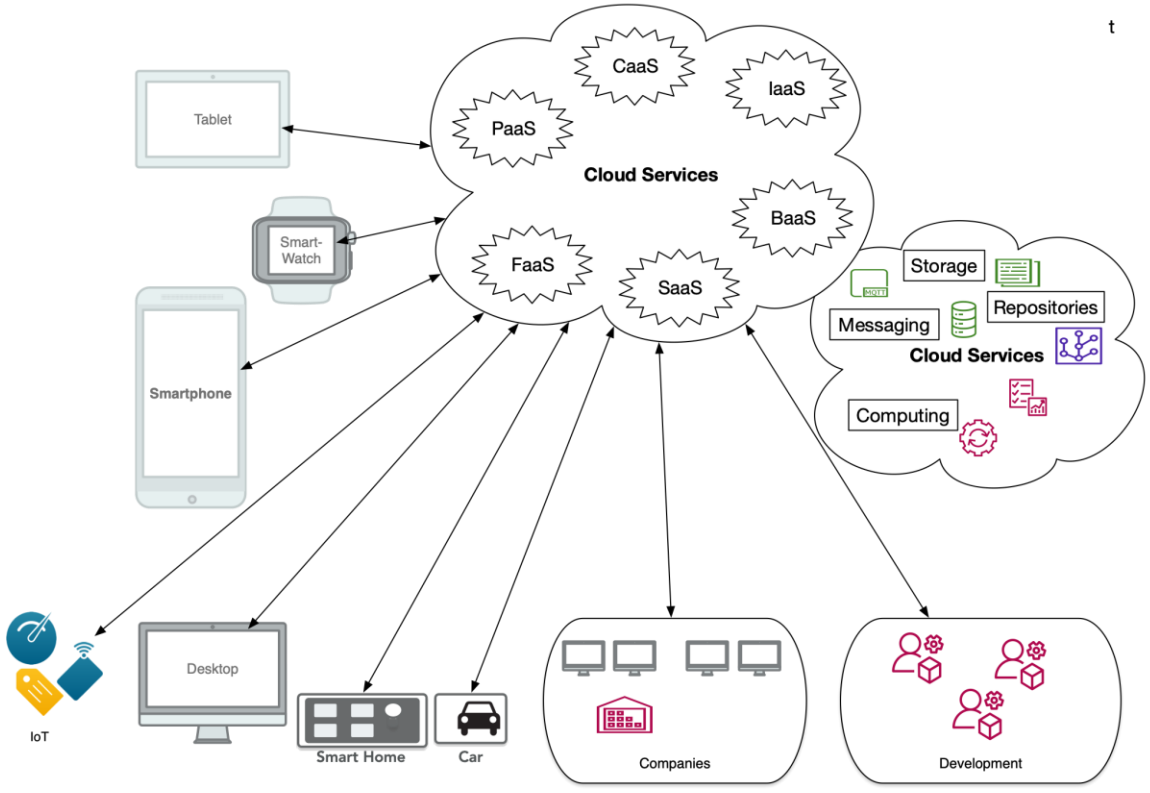
Interreg AUSTRIA-HUNGARY
Co-funded by the European Union
Trendig Plus
AN INTEGRATED BORDER REGION

Warum? / Why?

Pexels.com: Andrea Piacquadio

1. There is no Internet, but Bubbles.





2. Die Datensammler/collection of data

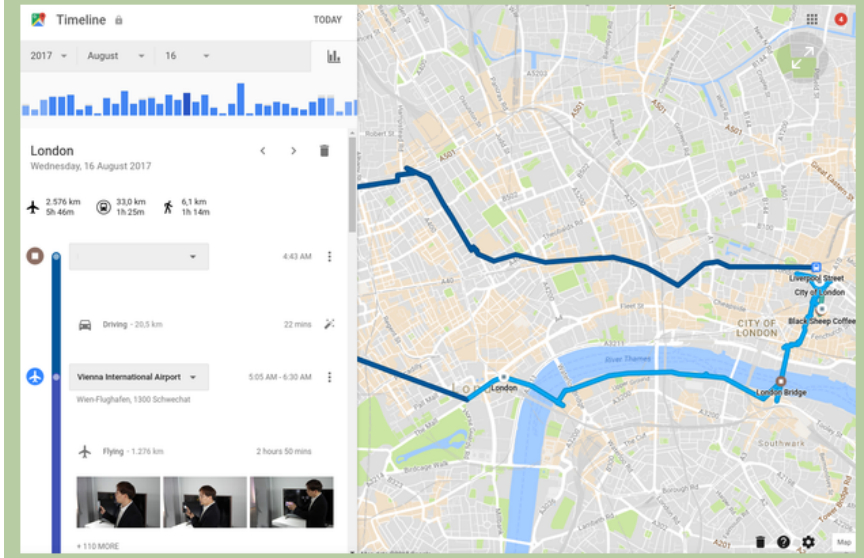
Das Kleingedruckte: Es gibt noch eine zweite Zustimmung, die Android-Nutzer üblicherweise bei der Einrichtung eines neuen Smartphones in Hinblick auf die Sammlung von Standortdaten erteilen. Mit dieser wird Google die Sammlung von Daten zum Akkustand sowie zur Qualität und Nutzungsdauer jeglicher Netzwerkverbindungen erlaubt. Google betont,

Web-, App-, und Suchnutzung

Der nächste große Bereich lässt sich g
Google-Nutzer im Internet umreißen.

Quellen: Proschofsky, **Datensammelei: Wie viel Google über uns weiß, DerStandard,** 15. April 2018

Will man einen unbedarften Google-Nutzer schocken, reicht oft der folgende Link: In der Google Maps Timeline kann jeder bis ins letzte Detail nachsehen, wo er sich die vergangenen Jahre herumgetrieben hat. Die Standorterfassung von Google ist dabei so gut, dass sie nicht nur weiß, wann man in welchem Lokal war oder wo man wie lange eingekauft hat. Auch ob man sich auf dem Weg dorthin zu Fuß, mit dem Auto, dem Rad oder öffentlichen Verkehrsmitteln bewegt hat, kann Google Maps mittlerweile ziemlich genau einschätzen.



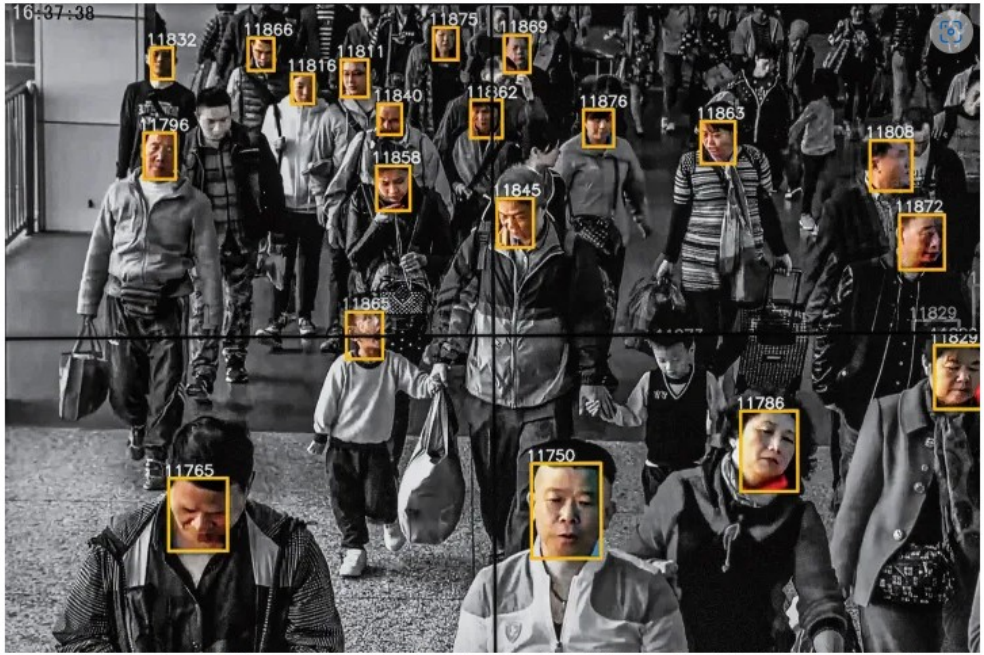
Ein Tagesausflug nach London in der Google Maps Timeline. Wird auch Google Photos genutzt, werden diese Informationen noch mit Aufnahmen angereichert.

Screenshot: Andreas Proschofsky / DER STANDARD

Welche Daten werden gesammelt? Der eigene Standort, basierend auf GPS, WLAN und Mobilfunkinformationen.

FH | JOANNEUM
University of Applied Sciences

3. „Ich habe nichts zu verbergen.“/„I‘ve got nothing to hide …“ oder: in welcher Welt wollen wir leben? What kind of future do we want?



Facial recognition is one element of China's expanding tracking efforts Photo-Illustration by TIME: Source Photo: Gilles Sabrié—The New York Times/Redux

How China Is Using “Social Credit Scores” to Reward and Punish Its Citizens

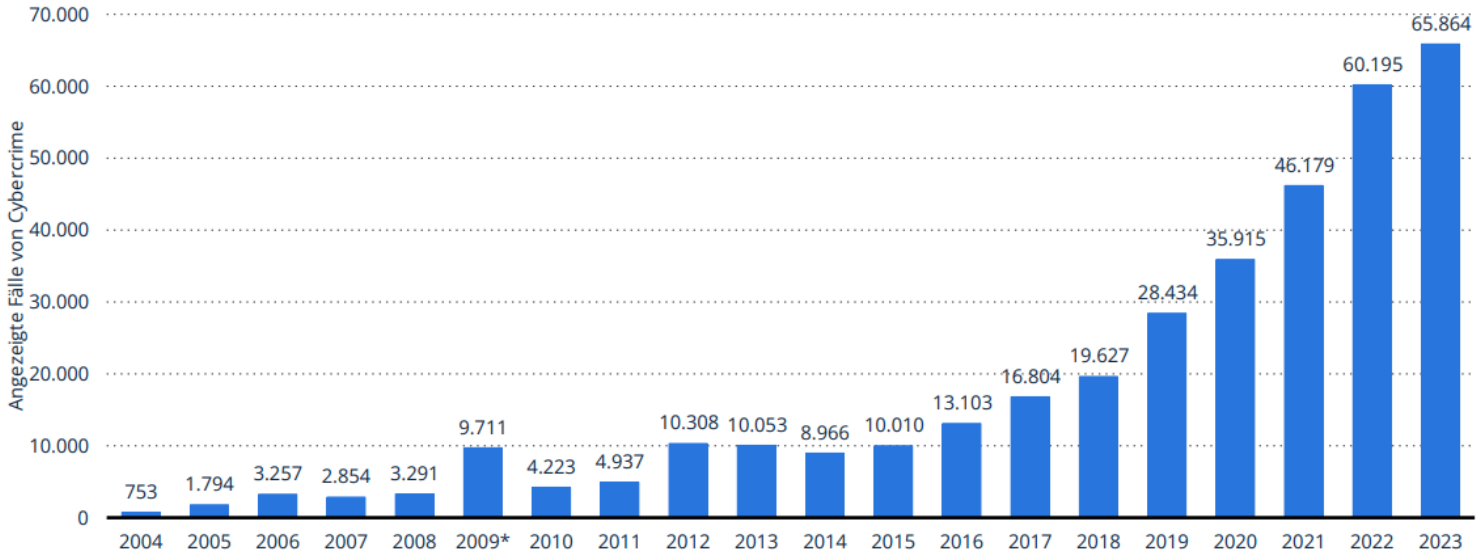
By Charlie Campbell / Chengdu

Quelle: How China Is Using Big Data to Create a Social Credit Score | Time.com, 23.4.2025.

4. Die aktuelle Bedrohungslage für Unternehmen/threads

Angezeigte Fälle von Cybercrime (gesamt) in Osterreich von 2004 bis 2023

Fälle von Cybercrime in Österreich bis 2023



Beschreibung: Die Internetkriminalität ist in Österreich auch 2023 weiter gestiegen: Mit rund 65.864 Anzeigen wurde eine Zunahme im Vergleich zum Vorjahr verzeichnet. Die zeitweise Schließungen des stationären Handels während der Corona-Pandemie und die damit verbundene Verlagerung des realen Lebens in die digitale Welt bildeten den Nährboden für Betrügerinnen und Betrüger im Internet. Mehr

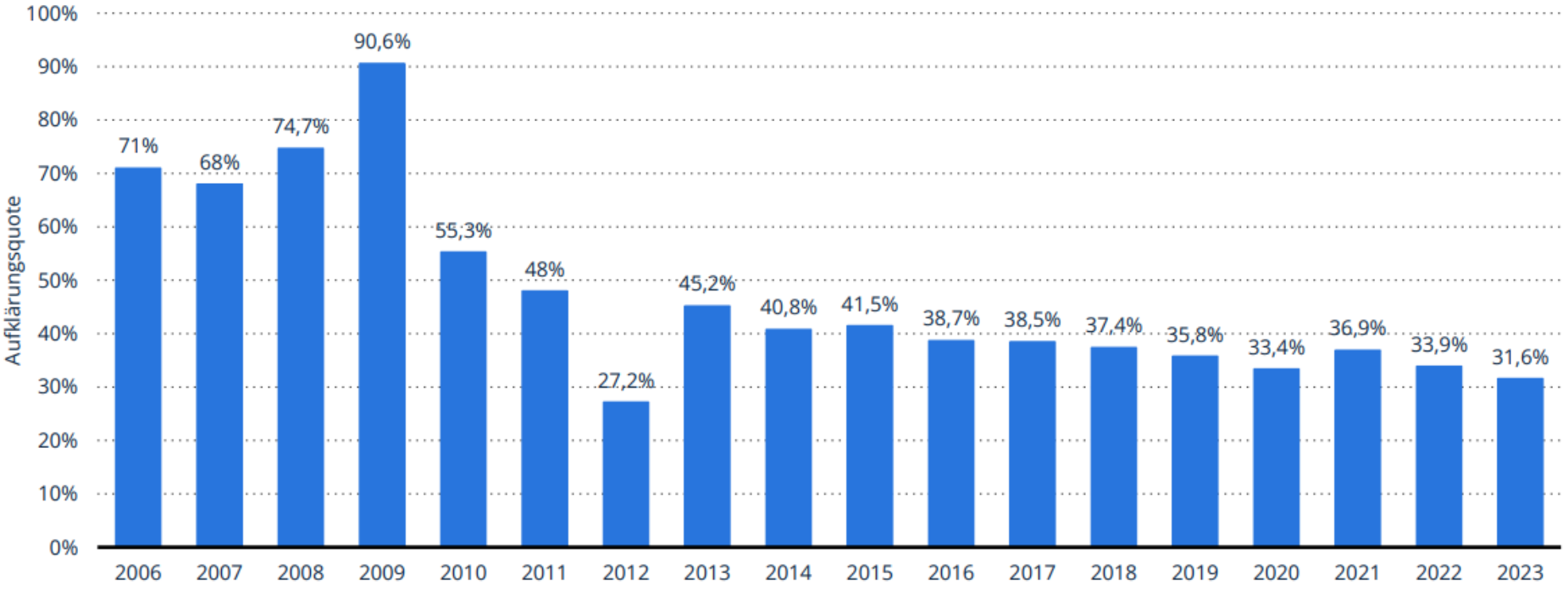
Hinweis(e): Österreich; * Das Jahr 2009 beinhaltet zwei Internetbetrugsfälle mit insgesamt 6.624 Einzeldelikten. Ältere Werte wurden teilweise entsprechenden Vorjahrespublikationen entnommen. Mehr

Quelle(n): BMI (Österreich) (Bundeskriminalamt)

statista

Entwicklung der Aufklärungsquote von Cybercrime (gesamt) in Österreich von 2006 bis 2023 /solved crimes

Aufklärungsquote von Cybercrime in Österreich bis 2023

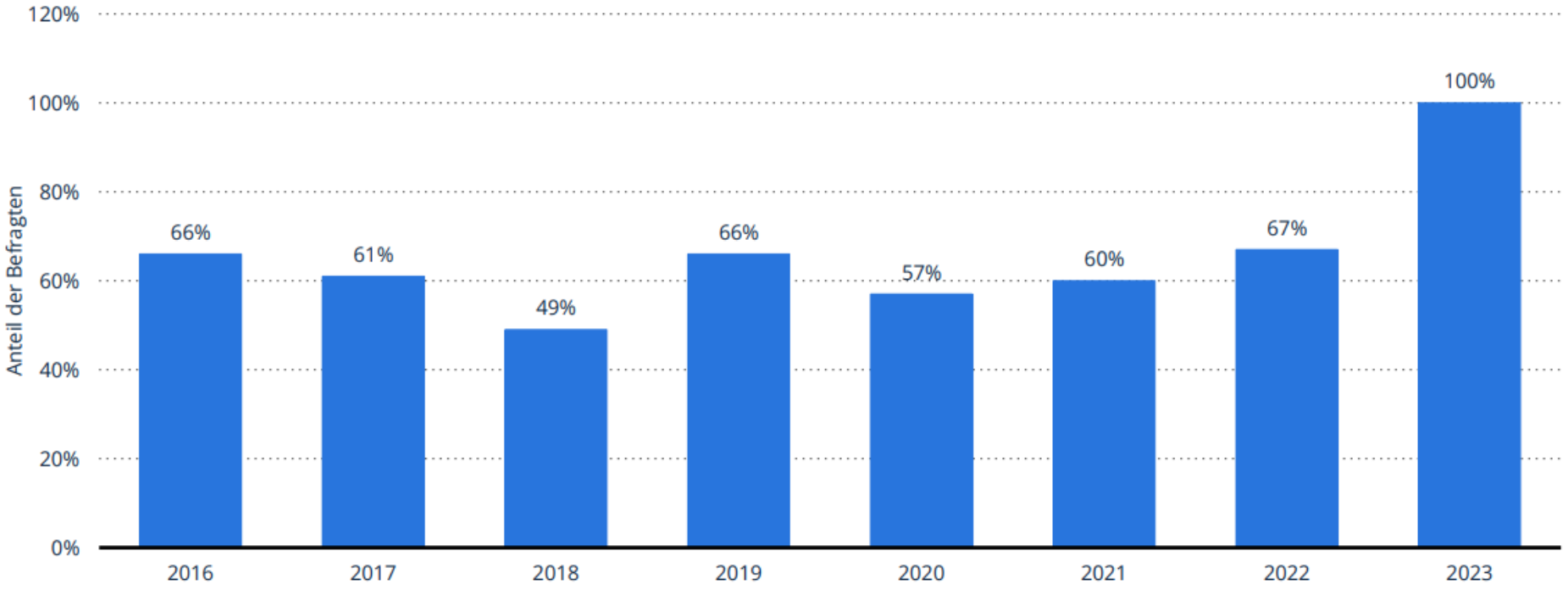


Beschreibung: Im Jahr 2023 konnten rund 31,6 Prozent der zur Anzeige gebrachten Fälle von Cybercrime in Österreich aufgeklärt werden. Die absolute Anzahl der geklärten Straftaten stieg in diesem Bereich von 17.000 im Jahr 2021 auf über 20.000 Fälle 2023. Mehr
Hinweis(e): Österreich; 2006 bis 2023; Cybercrime im engeren und im weiteren Sinn
Quelle(n): BMI (Österreich) (Bundeskriminalamt)

statista

Hat Ihr Unternehmen in den letzten 12 Monaten Versuche von Cyberangriffen festgestellt? / attackes on companies

Erfahrungen von österreichischen Unternehmen mit Cyber-Angriffen bis 2023

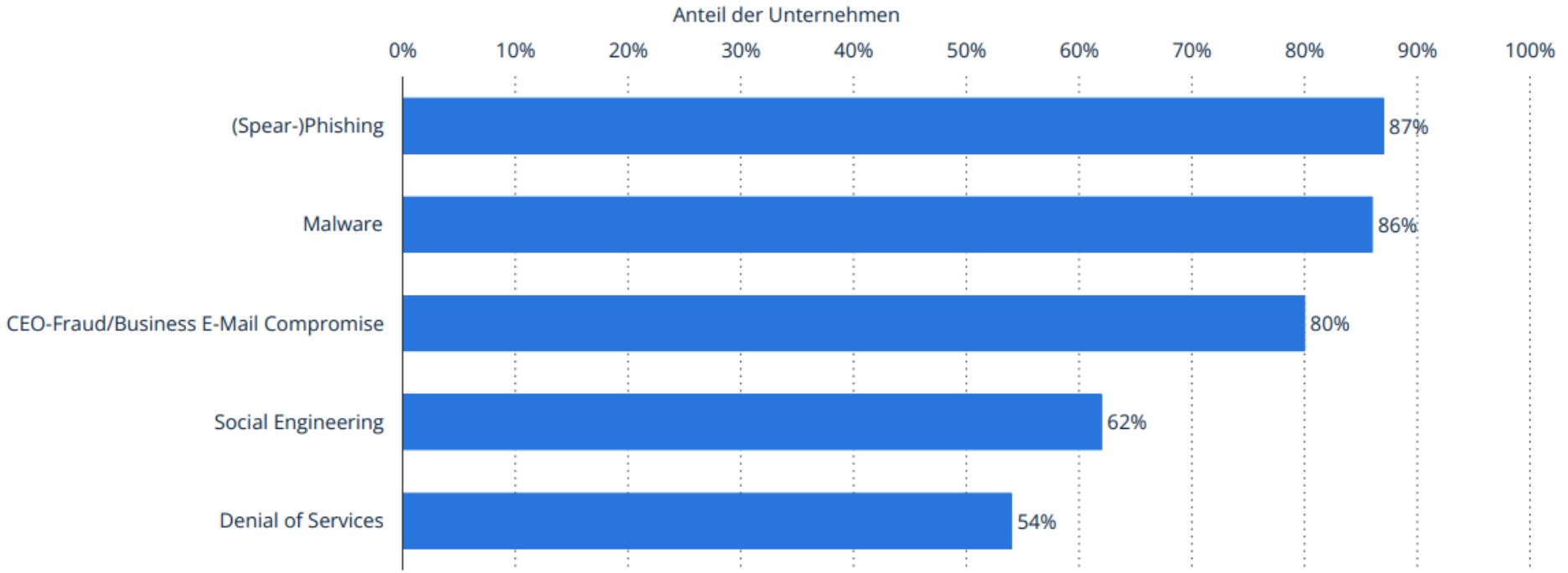


Beschreibung: Im Jahr 2023 waren alle befragten österreichischen Unternehmen in den letzten zwölf Monaten Opfer mindestens einer Cyberattacke geworden. Damit ist der Anteil im Vergleich zum Vorjahr von 67 auf 100 Prozent gestiegen. Mehr
Hinweis(e): Österreich; Februar und März 2023; 903 befragte Unternehmen
Quelle(n): KPMG

statista

Welche Arten von Cyberangriffen haben Sie in den letzten 12 Monaten in Ihrem Unternehmen identifiziert? / what kind of attackes?

Arten von Cyberangriffen auf Unternehmen in Österreich 2024

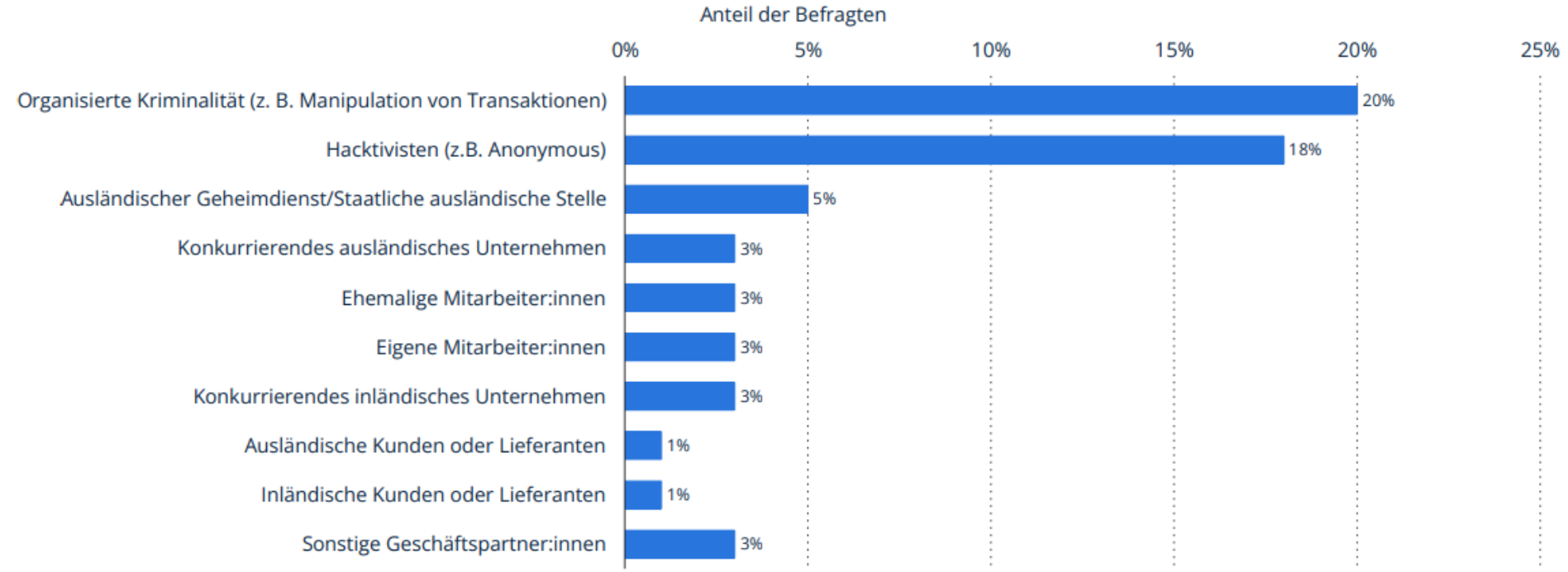


Beschreibung: Etwa 87 Prozent der befragten österreichischen Unternehmen erfuhren laut einer Umfrage 2024 im letzten Jahr Phishingattacken. Dabei handelt es sich um Versuche, über gefälschte Webseiten oder Nachrichten persönliche Daten zu erhalten oder den Nutzer zu schädlichen Aktionen zu bewegen. Beim CEO-Fraud oder Business E-Mail Compromise, dem 80 Prozent der befragten Unternehmen ausgesetzt waren, geben sich die Betrüger als Geschäftsführer oder Mitarbeiter eines [...] Mehr
Hinweis(e): Österreich; Februar und März 2024; 1.158 Befragte; Mehrfachnennungen möglich
Quelle(n): KPMG

statista

Wie bewerten Sie das Risiko, von folgenden Tätergruppen geschädigt zu werden? / what kind of attackers?

Umfrage zum Täterkreis von Cyberangriffen in Unternehmen in Österreich 2022



Beschreibung: Laut einer Umfrage unter Führungskräften österreichischer Unternehmen zum Thema Datenklau befürchten für das Jahr 2022 rund 20 Prozent der Befragten von organisierter Kriminalität wie Manipulation von Transaktionen geschädigt zu werden. Das Risiko von ausländischen oder inländischen Kunden oder Lieferanten geschädigt zu werden wurde hingegen als sehr gering eingeschätzt. Mehr

Hinweis(e): Österreich; Januar 2022; 202 Führungskräfte

Quelle(n): EY

statista

Cybercrime / Internetkriminalität

… umfasst Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IKT) /

criminal activities carried out by means of computers or the internet (ICT)

oder / or

gegen diese begangen werden / or targets ICT.

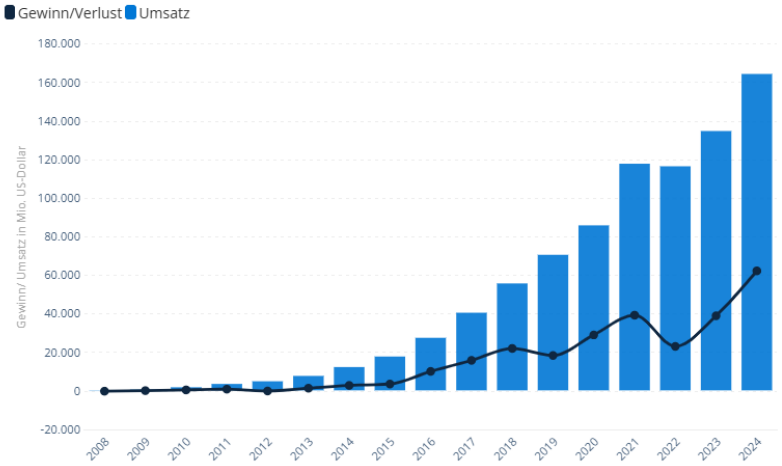
Quelle: https://bundeskriminalamt.at, 24.4.2023.

5. Die wundersame Vermehrung des Geldes/Money is growing on a tree.

"Today we are seen as a social media company, but in our DNA we are a company that builds technology to connect people, and the metaverse is the next frontier just like social networking was when we got started," Meta CEO **Mark Zuckerberg** said.

Meta-Umsatz mit neuem Rekord

Umsatz und Gewinn/ Verlust von Meta bis 2024 (in Millionen US-Dollar)



Quelle: Meta Platforms

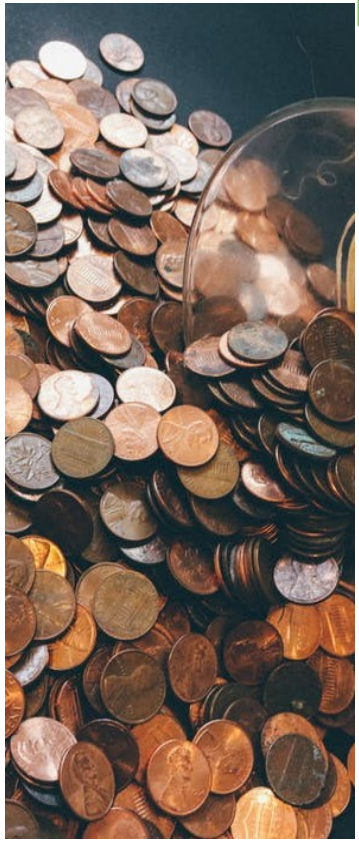
Mark Zuckerberg (2018)

Quelle: Mark Zuckerberg – Wikipedia, 27.4.2025.

6. Last but not least ...

Der Strafrahmen hat sich durch die DSGVO deutlich verändert / *Penalties according to the GDPR*

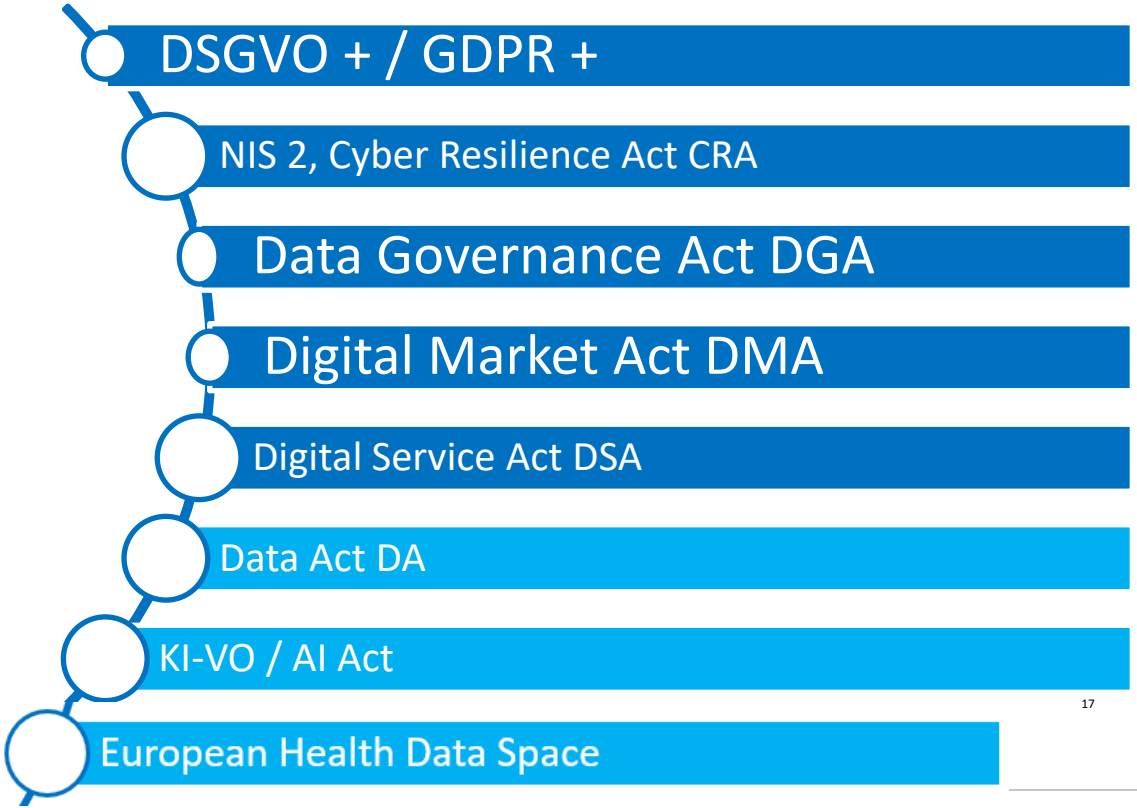
Until 2018: bis zu / *up to* € 25.000
Since 2028: bis zu /*up to* €10 Mio. / 20 Mio.
oder/*or* 2%/4% des weltweiten Umsatzes/*of the worldwide turnover*



Bildnachweis: https://www.pexels.com

FH JOANNEUM
University of Applied Sciences

7. Datenschutz ist die Basis / Privacy is the fundament



Darum: Datenschutzrecht! / That‘s why we need to be compliant

DSGVO - VO (EU) 2016/679 des EP und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, gültig seit Mai 2018.

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten
StF: BGBl. I Nr. 165/1999 DSG idF 2024

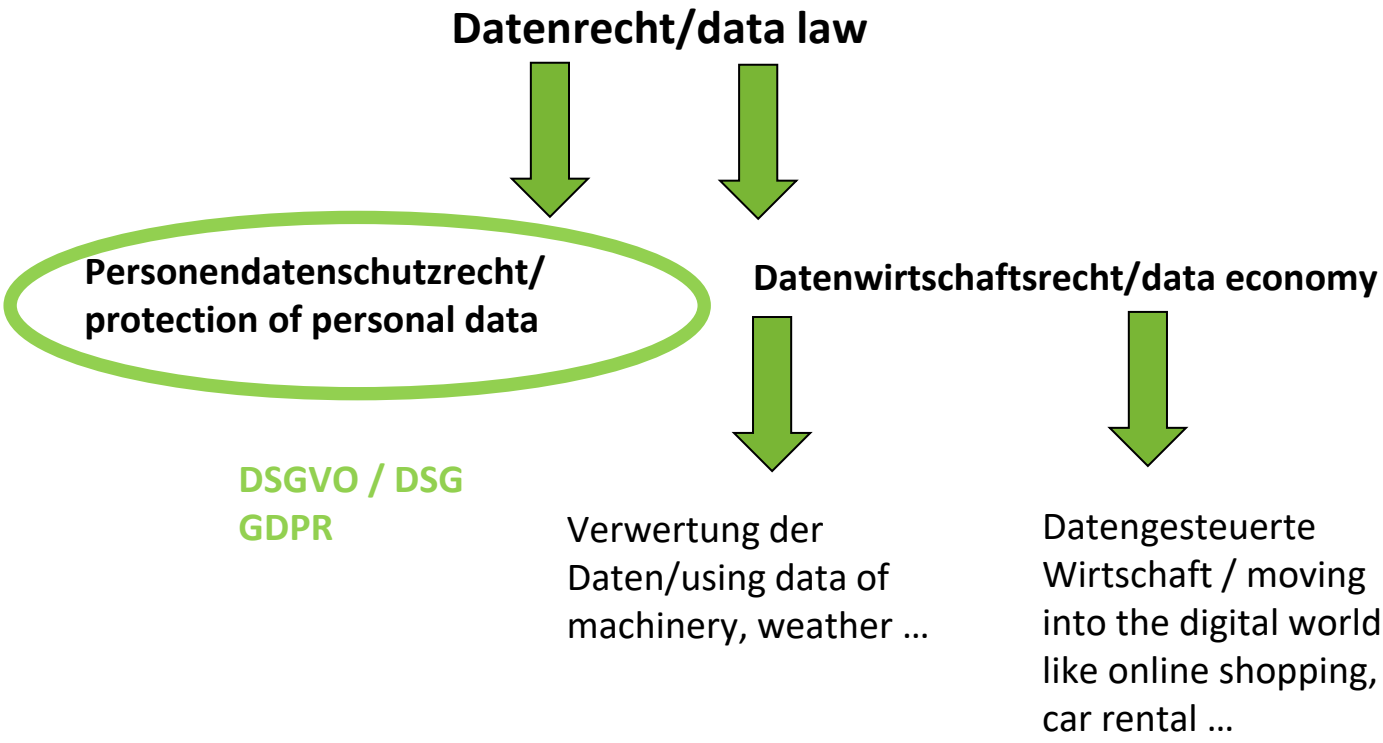
GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation)

Interreg AUSTRIA-HUNGARY
Co-funded by the European Union
Trendig Plus
AN INTEGRATED BORDER REGION

Wie? How?

Pexels.com: Andrea Piacquadio

Sachlicher Anwendungsbereich / Applicability

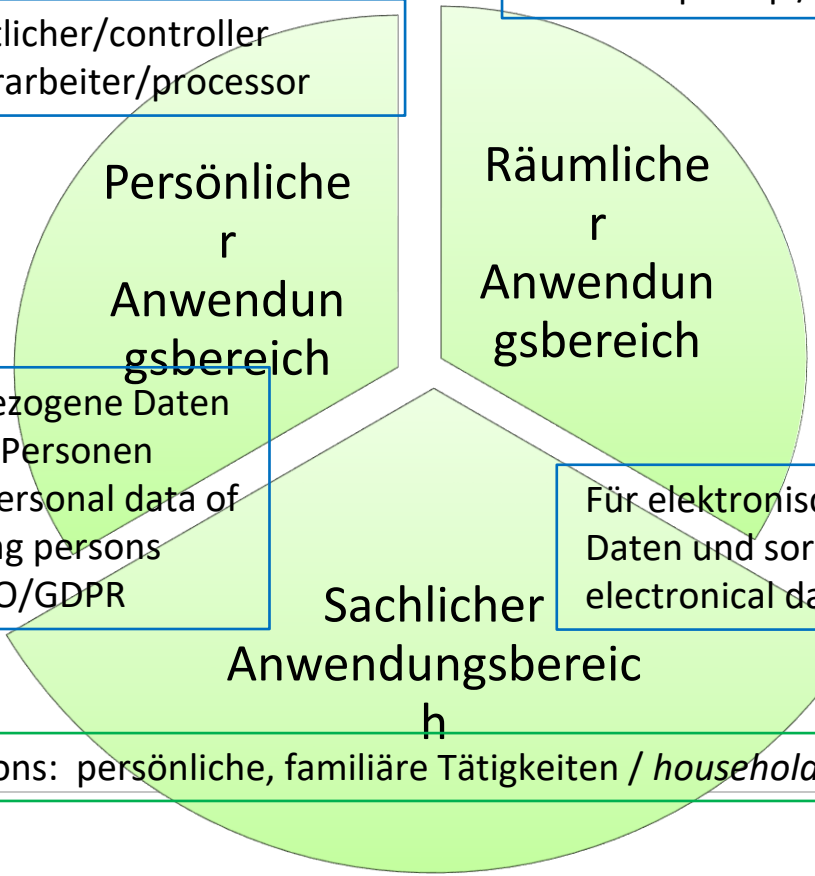


20

Anwendungsbereiche / *Scope* Art 1, 2 and 4 DSGVO/*GDPR*

Marktortprinzip / market principle

Verantwortlicher/controller
Auftragsverarbeiter/processor



personenbezogene Daten natürlicher Personen lebender/personal data of natural living persons Art 4 DSGVO/GDPR

Für elektronisch verarbeitete Daten und sortierte Papierakte / electronical data and sorted paper

Nicht erfasst/Exemptions: persönliche, familiäre Tätigkeiten / *household exemption* and anonym data

FH | JOANNEUM
University of Applied Sciences

Personenbezogene Daten /*personal data* Art 4 Z 1 DSGVO/*GDPR*

- **natürlicher lebender Personen /*natural living persons***
- **Identifiziert/*identified*:** Hans Huber, Frederike Maier ….
- **Identifizierbar/*identifiable*** (direkt oder indirekt): KFZ-Nummerntafel/*number plate*, Sozialversicherungsnummer/*social security number*, …
- **Pseudonymisierte Daten/pseudonym data:**
  - Kundenservice, Verrechnung — Marketingabteilung
  - *CRM, billing* — *marketing department*
    - Hans Huber –> Kundengruppe A
    - Frederike Maier –> Kundengruppe B

- **Räumlicher Anwendungsbereich / *spacial scope***
- Alle Daten, in der EU (Marktortprinzip) /*market*

Datenschutzrecht = Grundrecht (mit Drittwirkung) *fundamental right*

Bildnachweis: schweitzer-media.de

Personal scope

„Datendreieck“
Data triangle

Rechtsgrundlage / *legal basis*
Betroffenenrechte/ rights for data subject

Accountability / Security (TOMs)
Auftragsverarbeitervertrag / Contract with Processors

Verantwortlicher/ Data Controller
„Herr der Daten“

Betroffener / Data Subject

„natürliche Person, deren Daten verarbeitet werden“

Auftragsverarbeiter / Processor

Vgl. Dohr/Pollirer/Weiss/Knyrim, DSG Kommentar

Grundsatz der Datenverarbeitung DSGVO / *Main Principles of the GDPR*

Pixabay.com

Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten.

Verbot mit Erlaubnisvorbehalt.

It is not allowed to process personal data, but …

- ✓ **Informationelle Selbstbestimmung: wo gebe ich wem und wofür meine personenbezogenen Daten? / *data souvereignity***
- ✓ **Teil meiner Grundrechte / *fundamental rights***

24

Höhe des Schutzniveaus / *Appropriate* – Art 24 DSGVO/GDPR

category of personal data	level of protection	measures
Besondere Kategorie von Daten / *Art 9 + 10 GDPR data*	**hoch/high**	**hoch/high**
Personendaten	Schutzwürdigkeit	Angemessenheit
Öffentliche Daten /public data aggregierte oder anonyme Daten	**niedrig/low**	**niedrig/low**

Besondere Datenkategorien, sensible Personendaten Art 9 DSGVO/ *Special category of personal data according to Art 9 GDPR*

Pexels.com, Fernando Arcos

Rassische und ethnische Herkunft / *racial or ethnic origin*
Politische Meinungen / *political opinions*
Religiöse oder weltanschauliche Überzeugungen / *religious or philosophical believes*
Gewerkschaftszugehörigkeit / *trade union membership*
Genetische Daten / *genetic data*
Biometrische Daten zur eindeutigen Identifizierung / *biometric data for identification purposes*
Gesundheitsdaten / *health data*
Daten zum Sexualleben / *sex life or sexual orientation*

Eine weitere besondere Kategorie sind strafrechtsbezogene Danten / *another special category are data related to criminal convictions or offences* - Art 10 DSGVO:

FH JOANNEUM
University of Applied Sciences

Grundsätze nach Art 5 DSGVO /*Principles Art 5 GDPR*

Rechtmäßigkeit
lawful

Treu und Glaube
Bona fide

Transparenz
transparent

Zweckbindung
purpose

Datenminimierung
minimisation

Richtigkeit
accuracy

Speicherbegrenzung
Storage limitation

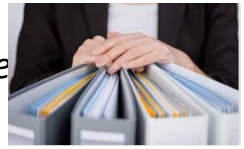
Integrität und Vertraulichkeit
Integrity, confidentiality

Rechenschaftspflicht
accountability

Betroffenenrechte
rights for data subjects

Pflichten des Verantwortlichen / *Controller Obligations*

Verzeichnisführungspflicht / *records of processing activitie*
Art 30 DSGVO



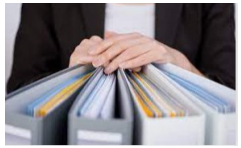
- Informationspflichten / *Information*

- Datenschutz-Folgenabschätzung / *PIA data protection impact assessment (Art 35 ff DSGVO)*
  - *TIA*

- Bestellung eines Datenschutzbeauftragten / *data protection officer (Art 37 DSGVO)*

Pflichten des Verantwortlichen/*Obligations*

- *Privacy by design / Privacy by default*

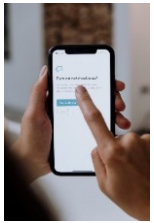


  - Datensicherheitsmaßnahmen / Security *(TOMs)*

- *Auskunftspflicht, request*

- *Daten im übertragbarem Format, data transferability*

- Meldepflicht / *Data breach notification duty*



Rechte der Betroffenen/*Rights of affected ps*

Recht auf Geheimhaltung § 1 (1) DSG, *secrecy, fundamental right*
soweit schutzwürdiges Interesse besteht

Recht auf Information Art 13 und 14 DSGVO *information*

Recht auf Auskunft Art 15 DSGVO / *right of request*

Recht auf Berichtigung Art 16 DSGVO *accuracy*

Recht auf Löschung (*Vergessenwerden*) Art 17 DSGVO *data deletion*

Recht auf Einschränkung der Verarbeitung Art 18 DSGVO
contradiction of scope, parallel zum Recht auf Widerspruch und Berichtigung mög

Widerspruchsrecht Art 21 DSGVO *contradiction*

Recht auf Datenübertragbarkeit Art 20 DSGVO *transportability*
Leitlinie der Art 29 Datenschutzgruppe vom 5.4.2016 WP 242 rev.01

Recht gegen Profiling Art 22 DSGVO, *contradiction to profiling*

Recht auf Beschwerde bei der Datenschutzbehörde /
Right to lodge a complaint with a supervisory authority

Pexels.com, cottonbro studio

Rechtmäßigkeit Art 6 Abs 1 DSGVO

Einwilligung / *Consent* Art 6 Abs 1 lit a DSGVO*/GDPR*–> jederzeitiger Widerruf möglich

Vertrag **/** *Contract* Art 6 Abs 1 lit b DSGVO*/GDPR*

rechtliche Verpflichtung **/** *legal obligation* Art 6 Abs 1 lit c DSGVO*/GDPR*

Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten
Protection of vital interests Art 6 Abs 1 lit d DSGVO*/GDPR*

Aufgabe im öffentlichen Interesse **/** *public interest* Art 6 Abs 1 lit e DSGVO*/GDPR*

überwiegend berechtigte Interessen des Verantwortlichen oder eines Dritten **/**
legitimate interest of controller or a third party Art 6 Abs 1 lit f DSGVO*/GDPR* (nicht
für die besondere Personendaten / *not for data within Art 9 or 10 GDPR*)

Einwilligung /*Consent* Art 6 Abs 1 lit a iVm Art 4 Z 11 / 7 DSGVO/*GDPR*

bestehende Einwilligung / *existing consent* (vor 2018)

freiwillig /*freely*

nicht pauschal, für einzelne /*specific* Verarbeitungsvorgänge

dh Koppelungsverbot / distinguishable

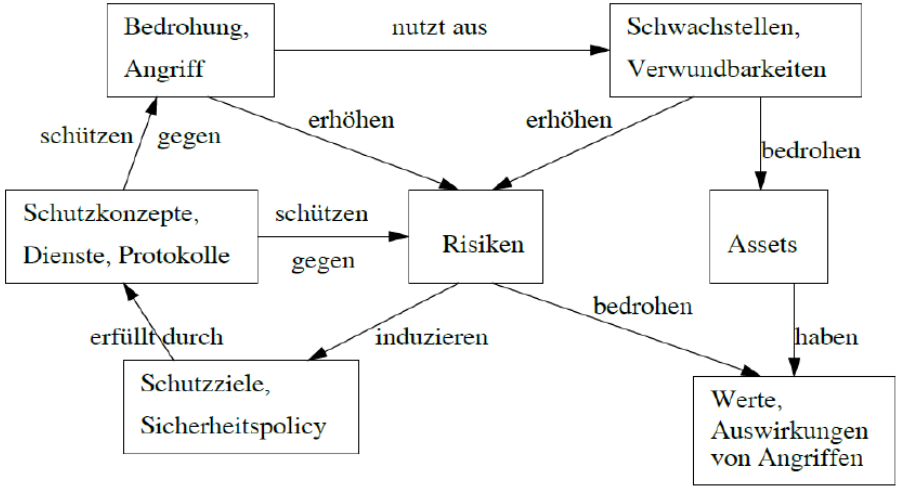
in informierter Weise / *informed*

kann Teil der AGB sein, aber klar erkennbar /*clear and unar*

https://www.pexels.com/ pixabay

Nachweispflicht für den Verantwortlichen, dh schriftlich dokumentiert, in verständlicher und leicht zugänglicher Form für die Zielgruppe formuliert (Kinder?, ältere Menschen?), von anderen Sachverhalten klar zu unterscheiden dh -> Überschrift, fett und jederzeitige Widerrufbarkeit + Hinweis darauf / d*ocumentation and right to withdraw the consent*

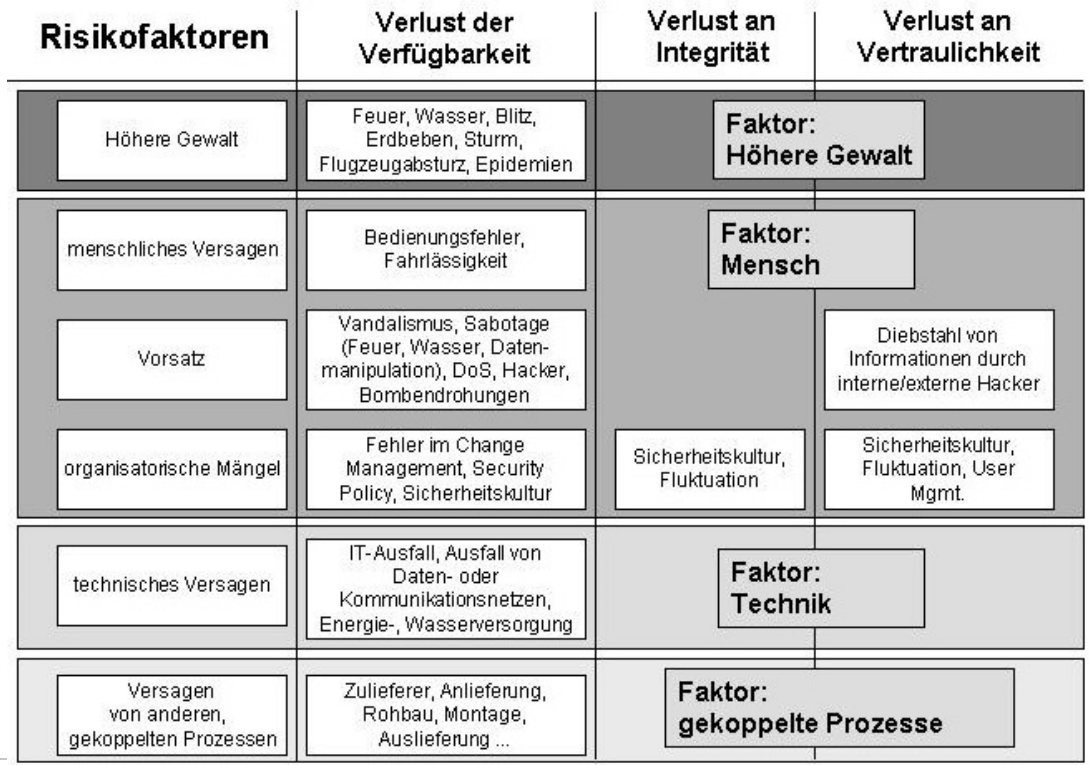
Datensicherheit und Risikoabschätzung/ *security of data and risk assessment*



Eckert, Claudia (2013). IT-Sicherheit: Konzepte - Verfahren - Protokolle. Munich: Oldenbourg Verlag München. ISBN: 978-3-486-72138-6.

Risikomanagement / Risk assessment

Risikofaktoren und Auswirkungen (www.sicherheitskultur.at)



PRIVACY & DATA PROTECTION (PDP) RISK ASSESSMENT FRAMEWORK

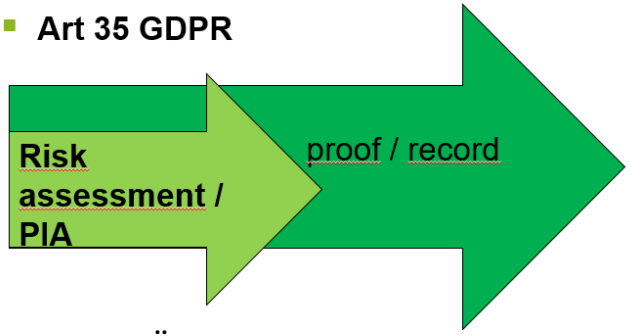
	COLLECTION	STORAGE	USAGE	DISCLOSURE	TRANSFER	ARCHIVE	DISPOSAL
HUMAN ERRORS & PROCESSES	PDP clauses included in Data collection medium? Any other potential errors from fatigue or carelessness?	Does staff know about using File-sharing features? Are files properly labelled, categorize and have Data classification?	Is staff properly trained in processing data and NDA signed? Are controls put in place to reduce human errors?	Has the disclosure been notified to data subjects? Is there contractual agreement for the disclosure?	Is due diligence conducted under the Transfer obligation with evidences of the due diligence done?	Is there a proper Password Management System puts in place so that the organisation can still retrieve the data if anything happened to the staff?	Is a proper Disposal process puts in place to ensure safe disposal with no risk of data breach? Eg. any evidence to prove a proper disposal?
MALICIOUS ACTIVITIES	What are some potential threats? • Theft • Malware • Social Engineering • Bad USB/OMG Cable • Hacking	Is the storage device properly protected? Eg. Data encrypted Is there a proper 3-2-1 Backup setup? Is Access control properly configured?	Are the applications used in processing secure with no vulnerability? Are staff properly training in Privacy & Data Protection from malicious activities?	Is the transmission channel secure? Are there danger of unauthorized access? Are the files properly secured? Eg. encrypted	Is the other entity overseas or Cloud applications have evidences demonstrating their PDP compliance?	Are the archived files/folders properly encrypted? **Note:** Ransomware can still put a layer of encryption over encrypted files	What are some technical controls put in place for disposal of Digital assets?
COMPUTER ERRORS	Is the system updated to ensure no vulnerabilities? Is there a Data subject rights procedures put in place?	Is there a Recovery Plan in place to swiftly reinstate the system if there is a major disaster (attack)?	Is there a regular monitoring on the processing to check on abnormality? Is there a Cyber & Data Breach Incident Management System put in place?	Is the other entity the data is been disclosed has been validated to comply with the PDP regulations?	Has Penetration Test conducted on the oversea entity system to ensure no vulnerability?	Is there a Retention monitoring system puts in place to ensure that the Retention Period is followed according to the Retention & Disposal Policy?	Will there be any trace of the data in other devices? Eg. mobile devices, computers, other storage, etc.

Navigating the Complexities of Risk Assessment in Privacy and Data Protection: A Comprehensive Framework | by Patrick Oh | Medium, 29.4.2025.

Risikomanagement / risk managment

Datenschutzfolgeabschätzung besteht aus 2 Teilen/ *2 parts of a privacy impact assessment (PIA)*

1. Durchführung der DSFA = *carrying out a PIA*
2. Erstellung des DSFA-Berichts = *reporting*



Inhalt:

Systematische Beschreibung der geplanten Verarbeitungsvorgänge

Zweck der Verarbeitung / Interessen

Bewertung der Notwendigkeit

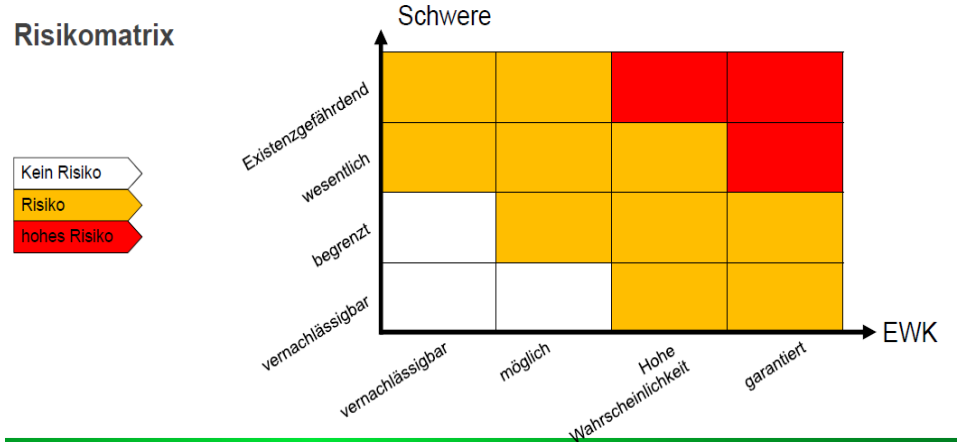
Bewertung der Verhältnismäßigkeit

Bewertung der Risiken

Abhilfemaßnahmen / Sicherheitsvorkehrungen

Risiko-Stufen sind/The GDPR requires the following:
Kein Risiko / no risk (ergibt sich zwangsläufig)
Risiko / risk (ErwGr 76)
Voraussichtlich hohes Risiko / a likely high risk (Art. 34, 35, 36)
Hohes Risiko / high risk (ErwGr 76)

Risiko Matrix / Risk matrix



Consequence					Increasing probability			
					A	B	C	D
Severity Rating	People	Assets	Environment	Reputation	Has occurred in Industry	Has occurred in operating company	Occurred several times a year in operating company	Occurred several times a year in location
0	Zero injury	Zero damage	Zero effect	Zero impact	Manage for continued improvement			
1	Slight injury	Slight damage	Slight effect	Slight impact				
2	Minor injury	Minor damage	Minor effect	Limited impact		Incorporate risk-reducing measures		
3	Major injury	Local damage	Local effect	Considerable impact				
4	Single fatality	Major damage	Major effect	Major national impact			Failed to meet screening criteria	
5	Multiple fatalities	Extensive damage	Massive effect	Major international impact				

Figure 1 – A typical Risk Assessment Matrix

[The Matrix Reloaded - our guide to the risk assessment matrix – Risktec](), 29.4.2025

Art 24 ff DSGVO/GDPR

Lucky Luke ist der Westernheld, der schneller schiesst als sein Schatten. Mitte November 2016 wird er 70 (Archiv) (Bild: Keystone/EHAPA VERLAG)

Nachweis = Dokumentation/*documentation*

Sicherstellung der „angemessenen“ technische und organisatorische Maßnahmen - *TOMs*

Quelle: https://www.luzernerzeitung.ch/panorama/comic-lucky-luke-schiesst-seit-70-jahren-schneller-als-sein-schatten-ld.116839, 23.4.2025.

Meldepflichten / data breach notification duty

Bei Verletzung des Schutzes personenbezogener Daten – Definition in Art 4 Z 12 DSGVO, besteht:

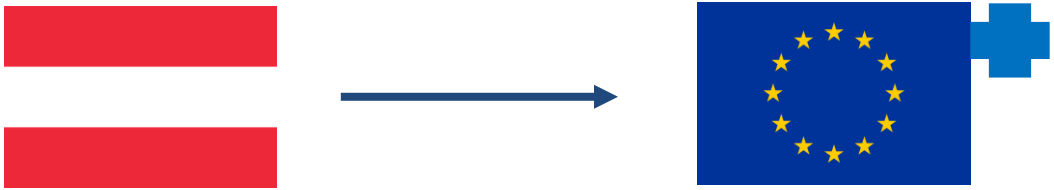
- Meldepflicht der Verletzung an die Behörde gem Art 33 DSGVO/
  binnen 72 Stunden nach Bekanntwerden, wenn spätere Meldung: Begründung
  wenn voraussichtliches Risiko für Rechte und Freiheiten natürlicher Personen
  Notification of supervisory authority withing 72 hours if there are risks for the rights and freedom of natural persons

- Wenn voraussichtlich hohes Risiko für Rechte und Freiheiten natürlicher Personen, Meldung an Behörde UND an betroffene Personen
  Notification of supervisory authority AND affected persons in case of high risks for rights and freedom of natural persons

- Dokumentationspflicht – immer / *always an obligation to document breaches*

Datentransfer innerhalb der EU+/*data transfer within the EU+*

- Grundsätzlich keine Einschränkungen/*no restriction*
- Sofern DSGVO eingehalten wird/*provided for compliant with GDPR*
- Inklusive/*including* **Norwegen, Island, Liechtenstein** (EWR)
- Rechtlich gleichgestellt mit Datentransfer im Inland = *like data transfer within the country*



Datentransfer außerhalb der EU+ / *data transfer outside the EU+*

- Sorgfalt bei der Auswahl des Auftragsverarbeiters / *due diligence*
- Sicherheitsvorkehrungen und Nachweise /*security and proof*
- Provider hat die Pflichten eines Auftragsverarbeiters

gem Art 28f DSGVO (Vertrag) / *stronger contractual oligations Art 28f GDPR*

- darf Daten nicht für eigene Zwecke verwenden / *esp no use of data for own purposes*
- muss Mindestanforderungen an Datensicherheit erfüllen

gem Art 32 DSGVO / *safety and security acc to Atr 32 GDPR*

- **Angemessenes Schutzniveau / *appropriate level of safety/securty***

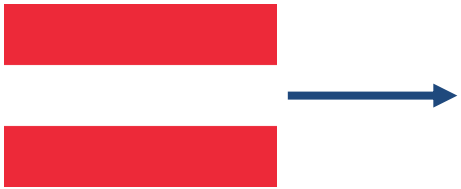
Art 44-50 DSGVO/*GDPR* -> Haftung/liability /
Betroffenenrechte/*data subjects' rights*

- **WIE?**

Datentransfer in Drittstaaten/*Data transfer to third countries*

Datenübermittlungen auf der Grundlage eines **Angemessenheitsbeschluss der Kommission (Art 45 DSGVO) / *Adequacy decision Art 45 GDPR***

- Mechanismus für eine regelmäßige Überprüfung, die mindestens alle 4 Jahre zu erfolgen hat / *assessment every 4 year*



Derzeit/currently **Andorra, Argentinien, Färöer Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada (tw), Neuseeland, Schweiz, Uruguay, Japan, Südkorea, UK, USA (tw)**

https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

FH | JOANNEUM
University of Applied Sciences

Aufsichtsbehörden / Supervisor Authority

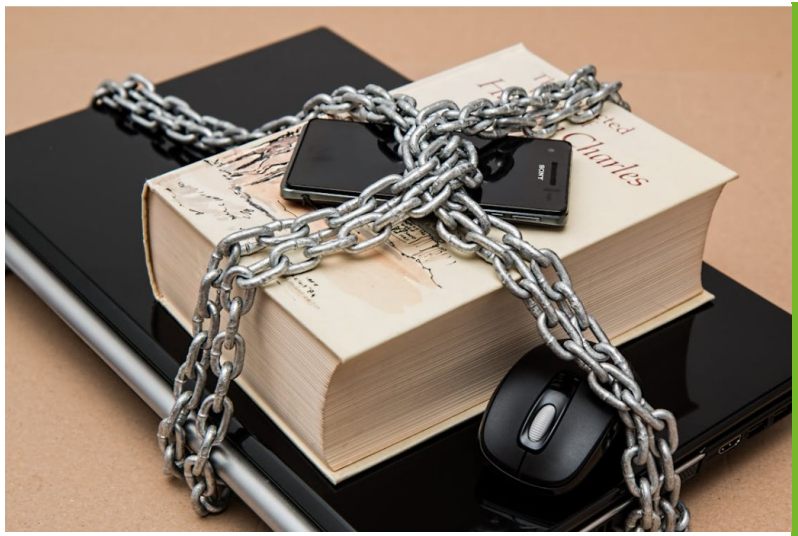
Each country has one or more data protection authorities / Österreich hat nun 2 Behörden

Europäischer Datenschutzausschuss EDSA / European Data Protection Board / EDPB

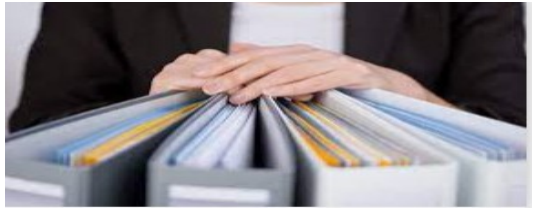
Interreg AUSTRIA–HUNGARY
Co-funded by the European Union
Trendig Plus AN INTEGRATED BORDER REGION
FH JOANNEUM University of Applied Sciences

Agenda

Nächsten Schritte / Take aways



Pexels.com: Pixabay



ToDos:

- Verarbeitungsverzeichnis erstellen /aktualisieren / *Data Processing record*
- Datenschutzerklärung erstellen / aktualisieren / *Privacy declaration*
- Risikoeinschätzung durchführen / *Risk assessment*
- *Verträge (ua Auftragsverarbeiter-, Standard Contractual Clauses …*
- *Berechtigungsmanagement ua organisatorische Maßnahmen*
- *Backups, Verschlüsselungen, updates, ua technische Maßnahmen (TOMs)*
- *Prozesse für Worst case (data breach), Auskunftsbegehren, Anfrage der Behörde …*

- *Regelmäßigkeit/regularly*

Verarbeitungsverzeichnis des Verantwortlichen / *record of activities of the controller* Art 30 DSGVO = muss/must have

Name und Kontaktdaten des Verantwortlichen bzw seines Vertreters in der EU / *name and contact details*

Name und Kontakt des etwaigen Datenschutzbeauftragten / *name, contact details of data protection officer*

Zwecke der Verarbeitung / *purpose of data processing*

eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten / *description of categories of data subjects and of their data*
(z.B. Kunden und Lieferanten; Rechnungsdaten, Adressdaten)

die Kategorien von Empfängern (z.B. Sozialversicherung, Finanzamt, Steuerberater), gegebenenfalls einschließlich Empfänger in Drittländern / *category of recipience, third countries*

wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien, Speicherdauer je D-Kategorie/ *envisaged time limits for erasure of categories of data*

wenn möglich, eine allgemeine Beschreibung der Datensicherheitsmaßnahmen TOMS/ *description of security measures*

Information – Datenschutzerklärung & Co *Privacy statement*

Informationspflicht bei Erhebung von personenbezogenen Daten/*information obligation*

Erhebung bei Betroffenen

Data from data subject

Art 13 DSGVO/*GDPR*

Erhebung nicht bei Betroffenen

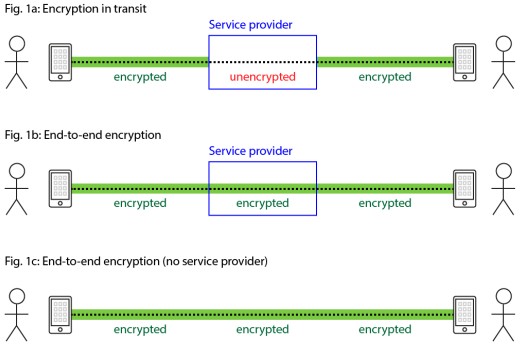
Data not from data subject

Art 14 DSGVO/*GDPR*

Datenschutzerklärung / privacy declaration

FH JOANNEUM
University of Applied Sciences

Sensible Daten schützen/protect special category data



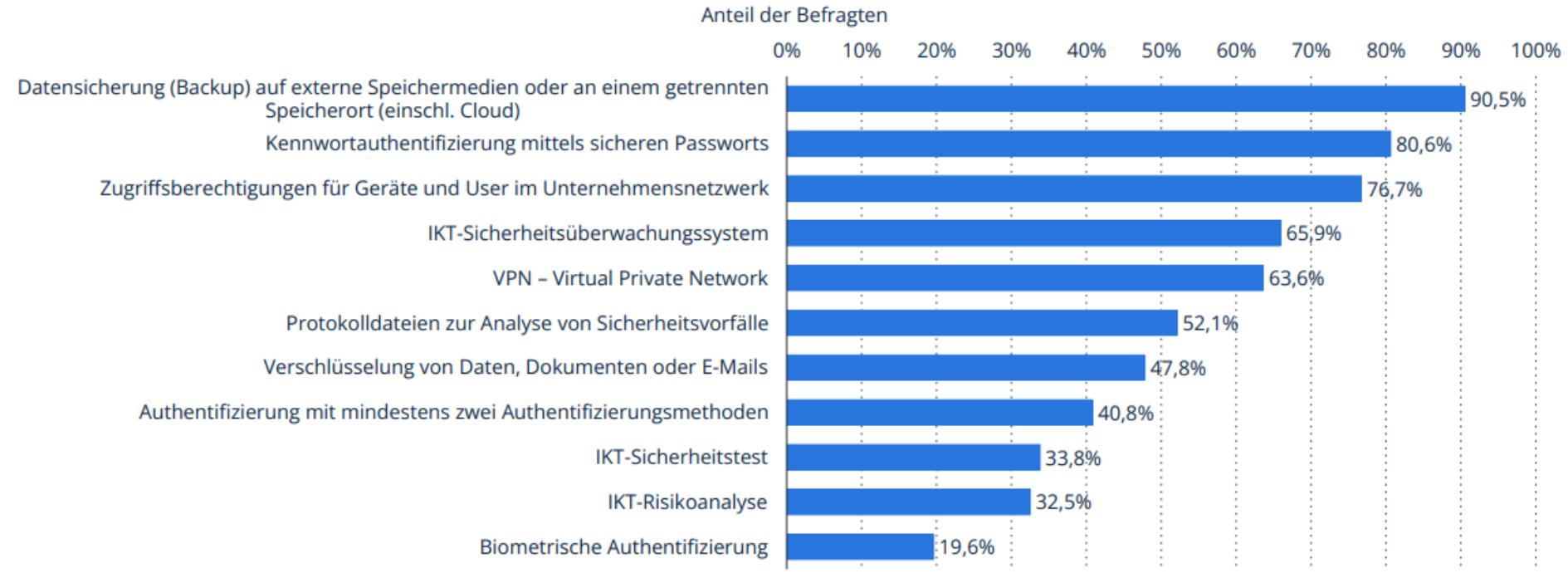
Daten, auch Backups verschlüsseln/*encryption*
Achtung/*attention*
End-To-End

Berechtigungsmanagement überlegen – wer muss worauf zugreifen können / *Access management*
Löschung (Zeitablauf, Widerruf), Richtigkeit der Daten etc – Prozesse/Abläufe im UN
Deletion (expiration, contradiction), accuracy - processes
Geräte, Daten und Datenbanken schützen (Passwörter, 2 Faktor Audentifikation)
ection of hardware, data and data basis (Password , 2 factor audentification)
bei Abwesenheit sperren / *secure PC if away from key*
rlagen versperrt aufbewahren / *secure data / information in the office (lock the office ..)*

- kritisches Auge / *critical eye*
- Österreichisches Informationssicherheitshandbuch
  https://www.sicherheitshandbuch.gv.at

Welche Maßnahmen im Bereich der IKT-Sicherheit führen Sie in Ihrem Unternehmen durch? / measures to achieve cyber security?

IKT-Sicherheitsvorkehrungen in österreichischen Unternehmen 2024



Beschreibung: Im Jahr 2024 war die häufigste Maßnahme im Bereich der IKT-Sicherheit in Unternehmen in Österreich die Datensicherung auf externen Speichermedien oder an einem getrennten Speicherort (z.B. Cloud). Rund 90,5 Prozent der befragten Unternehmen trafen diese Vorkehrung. Eine Biometrische Authentifizierung nutzten nur 19,6 Prozent der Unternehmen. Mehr
Hinweis(e): Februar bis Juli 2024; Mehrfachangaben möglich
Quelle(n): Statistik Austria

statista

Get informed …

Respective data protection authority/authorities

Austria:

DSB: www.dsb.gv.at, vierteljährl. Newsletter

Jährlicher Datenschutzbericht der DSB für Österreich

EDSA Europäischer Datenschutzausschuss /

EDPB European Data Protection Board

bzw Leitlinien der Art. 29-Gruppe

Weitere Informationen auch auf Webseiten gv.at;

Interessensvertretungen WKO /chambers of commerce …

- Kurze Artikel, Überblick / Praxistipps / Checklisten
  - (DaKo, JusIT, RdW …)

RTR – Rundfunk und Telekom Regulierungsbehörde

Get informed …

Unger, Kaja, Datenschutzrecht (2018)

Saferinternet: https://www.saferinternet.at/
Epicenter.works: https://epicenter.works/

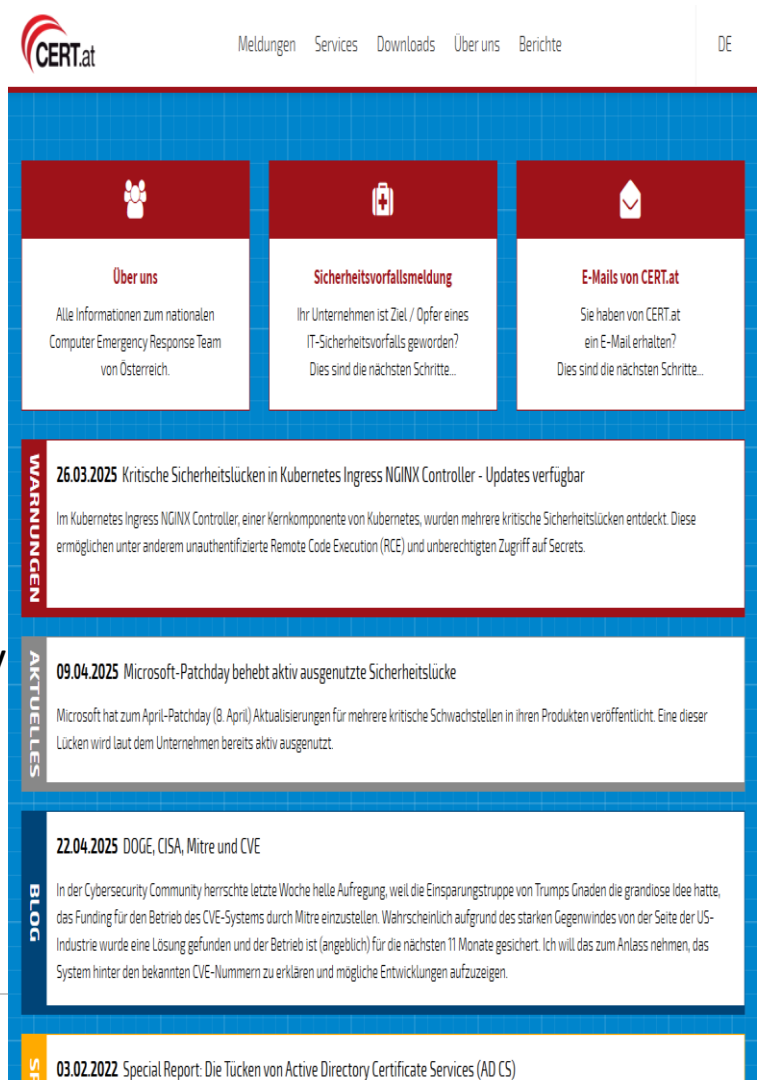
noyb.eu: https://noyb.eu/en
computer chaos club https://www.ccc.de/

Bitkom.org

National Institute of Standards and Technology, nist.gv

Österreichisches Sicherheitshandbuch

Cert.at



More Information

International:

Deutschland

- Baden-Würtemberg
- Düsseldorfer Kreis

ICO

USA

- CCPA

Interreg AUSTRIA-HUNGARY
Co-funded by the European Union
Trendig Plus
AN INTEGRATED BORDER REGION
FH JOANNEUM
University of Applied Sciences

"Technology is a useful servant, but a dangerous master."

[Christian Lous Lange]