SPENDENBEGÜNSTIGUNG UND DATENSCHUTZ IM SPENDENWESEN

Vorgaben und Best Practices

Jasmin Preuer
Mario Neubauer
Barbara Fahringer-Postl

15.04.2024

BDO

ANSPRECH-PERSONEN

Barbara Fahringer-Postl
Partnerin

+43 5 70 375 - 1381
+43 664 60 375 - 1381
barbara.fahringer-postl@bdo.at

Jasmin Preuer
Managerin

+43 5 70 375 - 4825
+43 664 60 375 - 4825
jasmin.preuer@bdo.at

Mario Neubauer
Senior Manager

+43 5 70 375 – 4253
+43 664 60 375 - 4253
mario.neubauer@bdo.at

AGENDA

01 Antrag auf Zuerkennung der Spendenbegünstigung

02 Datenübermittlungsverpflichtung - Meldung Sonderausgaben

03 keine Datenübermittlungsverpflichtung- Spenden aus dem Betriebsvermögen

04 Datenschutz

05 Informationssicherheit

01

ANTRAG AUF ZUERKENNUNG DER SPENDEN-BEGÜNSTIGUNG

Checkliste

ANTRAG ZUERKENNUNG SPENDENBEGÜNSTIGUNG

CHECKLISTE FÜR ORGANISATIONEN DIE EINEN ANTRAG STELLEN MÜSSEN

- Steuerberater:in oder Wirtschaftsprüfer:in beauftragen
- gesetzlichen Voraussetzungen prüfen
  - Sitz im Inland oder EU-Mitgliedstaat
  - gemäß Rechtsgrundlage und tatsächlicher Geschäftsführung ausschließliche und unmittelbare Verfolgung gemeinnütziger, mildtätiger Zwecke
  - Organisation muss seit einem mindestens 12 Monate umfassenden Wirtschaftsjahr begünstigten Zweck dienen
  - Maßnahmen zur Erfüllung der Datenübermittlungsverpflichtung müssen getroffen werden
  - Verwaltungskosten iZm der der Spendenverwendung höchsten 10% der Spendeneinnahmen
  - Wirtschaftsprüferbestätigung wenn Organisation einer gesetzlichen oder satzungsgemäßen Abschlussprüfung unterliegt
- Statuten kontrollieren und gegebenenfalls anpassen, insbesondere in den Punkten
  - begünstigte Zwecke
  - ideelle und materielle Mittel
  - Gewinnausschluss
  - Auflösungsbestimmung
- Mitgliederversammlung, Meldung an Vereinsbehörde

ANTRAG ZUERKENNUNG SPENDENBEGÜNSTIGUNG

CHECKLISTE FÜR ORGANISATIONEN DIE EINEN ANTRAG STELLEN MÜSSEN

- Steuernummer beantragen, sofern noch keine vorhanden
  - Verf15a-Spend – neues Formular
  - vereinfachte Angaben (wenn Steuernummer nur für die Spendenbegünstigung benötigt wird)

- FinanzOnline Zugang beantragen, falls Organisation Spenderdaten selbst an das Finanzamt melden möchte

- Zuerkennung Spendenbegünstigung beim Finanzamt beantragen durch Steuerberater:in, Wirtschaftsprüfer:in
  - nur Steuerberater:in und Wirtschaftsprüfer:in haben Zugriff auf das Formular
  - nur in FinanzOnline möglich
  - jährliche Verlängerungsmeldung durch Steuerberater:in, Wirtschaftsprüfer:in für die Aufrechterhaltung der Spendenbegünstigung
  - Rechtsgrundlage ist bei Antragstellung in FinanzOnline im Format OCR pdf/a textinterpretierbar hochzuladen

- Datenübermittlungsverpflichtung beachten
  - FinanzOnline-Zugang nötig, wenn Datenübermittlung durch Organisation selbst vorgenommen werden soll
  - Datenübermittlung kann auch durch Dienstleister oder eine gemeinsame Datenübermittlungsstelle erfolgen

ANTRAG ZUERKENNUNG SPENDENBEGÜNSTIGUNG

ANTRAG STEUERNUMMER SOFERN "NUR" FÜR DIE SPENDENBEGÜNSTIGUNG NOTWENDIG FORMULAR VERF 15A-SPEND

Antrag auf Vergabe einer Steuernummer für Vereine

Für die Beantragung einer Spendenbegünstigung nach § 4a Einkommensteuergesetz 1988 [1)]

FRAGEBOGEN

Wie lautet die genaue Bezeichnung des Vereins? (Bitte auch eine allfällige Kurz- oder Schlagwortbezeichnung anführen)			
Wo befindet sich die Vereinsleitung? Adresse des Vereins lt. Zentralem Vereinsregister (ZVR)			
ZVR-Zahl (falls bekannt):	Wann ist die Eintragung ins Zentrale Vereinsregister erfolgt? Datum:		
Obfrau/Obmann des Vereines ist: Zu- und Vorname		Sozialver-sicherungs-nummer	Geburtsdatum (TTMMJJ)
Adresse	PLZ	Ort	
Tel. erreichbar unter:			

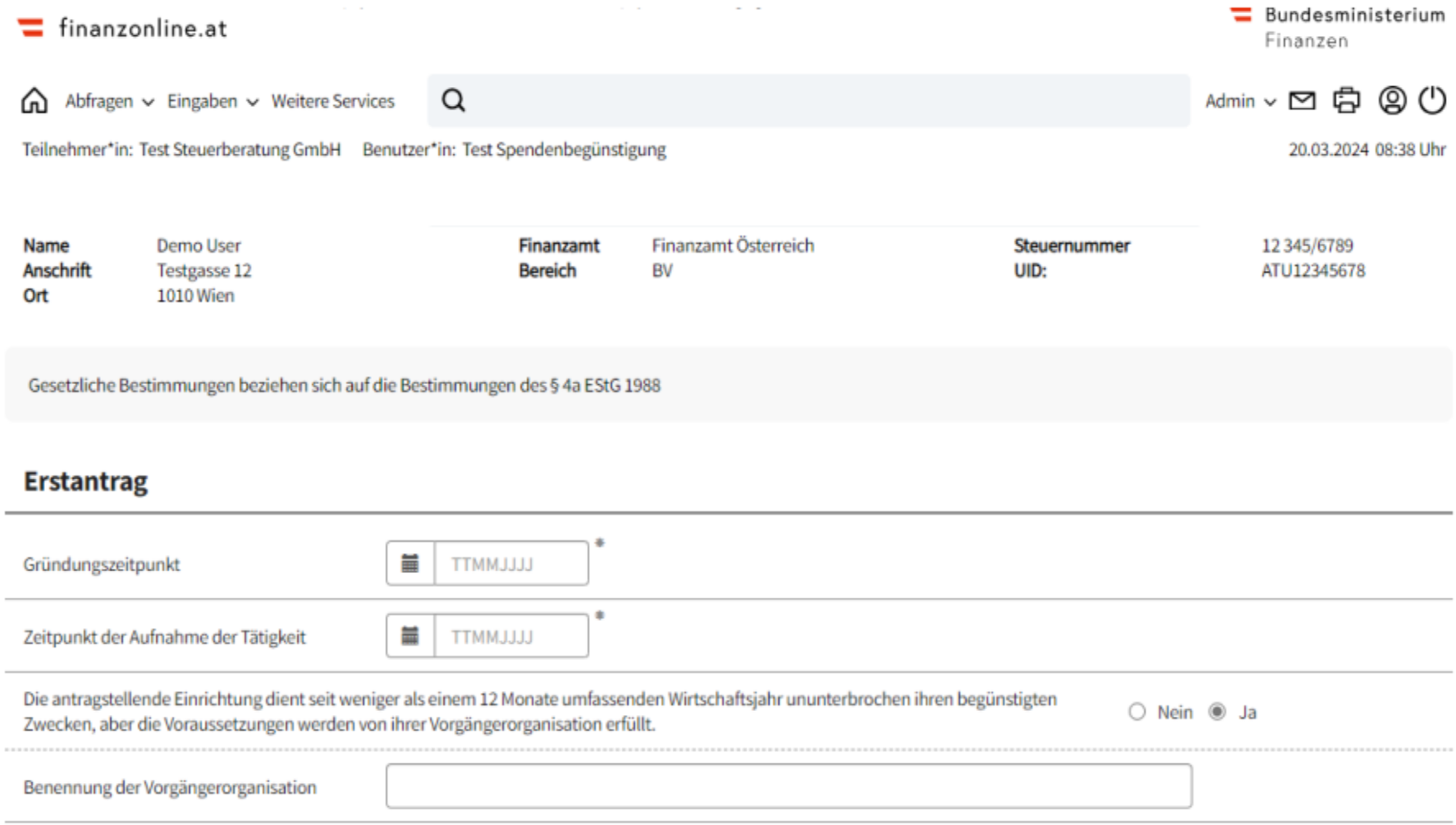
Ich (wir) nehme(n) zur Kenntnis, dass alle Umstände, die zum Entstehen oder Erlöschen einer Abgabenpflicht führen, sowie alle weiteren Umstände, die für die Abgabenerhebung bedeutsam sind (z.B. Adressänderung, Wechsel vertretungsbefugter Personen, etc.) innerhalb eines Monats dem Finanzamt bekanntzugeben sind (§§ 120 ff Bundesabgabenordnung).

Ich (Wir) versichere(n), dass die vorstehenden Angaben nach bestem Wissen und Gewissen vollständig und wahrheitsgemäß gemacht wurden.

ANTRAG NUR DURCH STEUERBERATER:IN, WIRTSCHAFTSPRÜFER:IN

Eingabemaske Finanzonline

2.2. Eingabeseite der erstmaligen Meldung



ANTRAG NUR DURCH STEUERBERATER:IN, WIRTSCHAFTSPRÜFER:IN

Eingabemaske Finanzonline

2.4. Eingabeseite der gemeinsamen Felder

Diese Felder sind sowohl bei der erstmaligen Meldung als auch bei der Verlängerung auszufüllen.

Daten der antragstellenden Einrichtung

Region(en) der Tätigkeit

- Österreich ☐
- EU/EWR ☐
- Sonstiges ☐

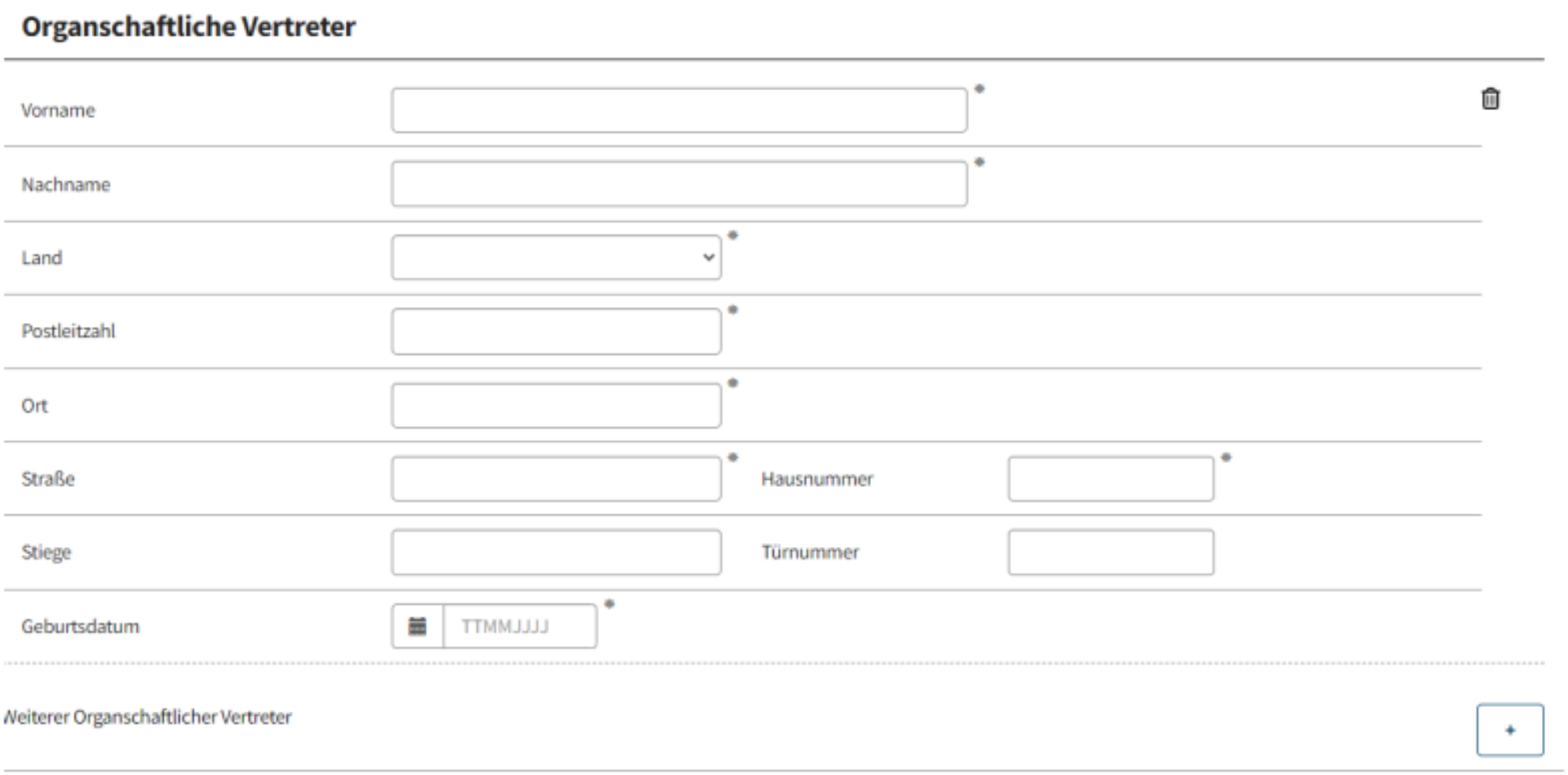
Ende des Rechnungsjahres/Wirtschaftsjahres oder Abschlussstichtag: TTMMJJJJ *

Besteht eine Pflicht zur gesetzlichen oder satzungsmäßigen Abschlussprüfung? ◉ Nein ○ Ja

Hinweis: Die Übermittlung der Bestätigung des Wirtschaftsprüfers gemäß § 4a EStG 1988 betreffend das letzte abgeschlossene Rechnungsjahr/Wirtschaftsjahr ist erforderlich.

ANTRAG NUR DURCH STEUERBERATER:IN, WIRTSCHAFTSPRÜFER:IN

Eingabemaske Finanzonline



ANTRAG NUR DURCH STEUERBERATER:IN, WIRTSCHAFTSPRÜFER:IN

Eingabemaske Finanzonline

Finanzen

Letztes abgeschlossenes Jahr vor Antragstellung *

Gesamteinnahmen *

Davon Spenden *

Davon Mitgliedsbeiträge bzw. Schulgeld *

Subventionen lt. Transparenzdatenbank

Hinweis: Wenn keine Förderung vorliegt, dann ist der Wert 0 einzutragen. Wenn eine Förderung erhalten wurde, dann ist unabhängig von der Höhe der Wert 1 einzutragen. *

Gesamtausgaben *

Weiteres Jahr +

Zwecke, Tätigkeiten und Mittel der antragstellenden Einrichtung

In der Rechtsgrundlage ist ausgeschlossen, dass die Einrichtung auf Gewinn gerichtet ist. ◉ Nein ○ Ja

Welcher Zweck wird erfüllt?

gemeinnützig ☐

mildtätig ☐

ANTRAG NUR DURCH STEUERBERATER:IN, WIRTSCHAFTSPRÜFER:IN

Eingabemaske Finanzonline

Welcher Zweck wird als Hauptzweck gefördert?

- ☐ Bekämpfung von Elementarschäden, Katstrophenhilfe, - schutz, Zivilschutz
- ☐ Berufsausbildung
- ☐ Denkmalpflege und Denkmalschutz
- ☐ Entwicklungszusammenarbeit
- ☐ Fürsorge für alte, kranke oder mit körperlichen Gebrechen behaftete Personen
- ☐ Gesundheitspflege
- ☐ Heimatkunde und Heimatpflege
- ☐ Körpersport und Denksport
- ☐ Kinder-, Jugend- und Familienfürsorge, Studentenbetreuung
- ☐ Kunst und Kultur, Musik
- ☐ Leistungen im Rahmen der Erfüllung hoheitlicher Tätigkeiten
- ☐ Menschenrechte, Konsumentenschutz, Bürgerinitiativen, Friedensbewegungen, Völkerverständigung, demokratisches Staatswesen, ethische Vereinigungen
- ☐ Mildtätige Zwecke
- ☐ Natur-, Umwelt-, Tier- und Höhlenschutz, Landschaftsschutz, Betrieb eines Tierheimes
- ☐ Schulbildung, Erziehung
- ☐ Unterstützung von hilfsbedürftigen Personen bzw. Personen mit Einschränkungen/Behinderungen, Beschäftigung, Resozialisierung, Suchtbekämpfung, Selbsthilfe
- ☐ Volksbildung und Erwachsenenbildung
- ☐ Volkswohnungswesen
- ☐ Wissenschaft und Forschung

ANTRAG NUR DURCH STEUERBERATER:IN, WIRTSCHAFTSPRÜFER:IN

Eingabemaske Finanzonline

Werden nicht begünstigte Nebenzwecke verfolgt?	(•) Nein ( ) Ja
Wirtschaftliche Betätigungen (zB Vereinsfeste, Vereinslokal/Kantine, Flohmarkt, Benefizveranstaltungen, Shop)	500 Zeichen frei
Wenn begünstigungsschädliche Betriebe vorhanden sind, liegen Ausnahmegenehmigungen für alle Betriebe vor?	( ) ja, nach dem Gesetz (§ 45a BAO) ( ) ja, Ausnahmegenehmigungen nach § 44 Abs. 2 BAO für alle Betriebe vorhanden ( ) nein ( ) Es liegen keine begünstigungsschädlichen Betriebe vor.

ANTRAG NUR DURCH STEUERBERATER:IN, WIRTSCHAFTSPRÜFER:IN

Eingabemaske Finanzonline

Bestätigung des vertretungsberechtigten Leitungsorgans liegt dem Wirtschaftstreuhänder vor

Bestätigung

Das vertretungsberechtigte Leitungsorgan bestätigt, dass die obigen Angaben korrekt sind. ☐

Das vertretungsberechtigte Leitungsorgan bestätigt, dass folgende Voraussetzungen für die Spendenbegünstigung vorliegen: ☐

- Die tatsächliche Geschäftsführung stimmt mit der Rechtsgrundlage überein.
- Es wurden Maßnahmen zur Erfüllung der Datenübermittlungspflicht gemäß § 18 Abs. 8 EStG 1988 getroffen.
- Die in Zusammenhang mit der Verwendung der Spenden stehenden Verwaltungskosten betragen ohne Berücksichtigung der für die Erfüllung der Übermittlungsverpflichtung anfallenden Kosten höchstens 10% der Spendeneinnahmen.
- Gegen die Körperschaft, deren Entscheidungsträger oder deren Mitarbeiter wurden innerhalb der letzten 2 Jahre auf Grund von gerichtlich strafbaren Handlungen oder vorsätzlich begangener Finanzvergehen (ausgenommen Finanzordnungswidrigkeiten) keine Verbandgeldbußen oder Strafen rechtskräftig verhängt, wenn die strafbare Handlung innerhalb der letzten 5 Kalenderjahre begangen wurde.
- Die Körperschaft fördert nicht systematisch die vorsätzliche Begehung von in ihrem Interesse methodisch begangenen strafbaren Handlungen.
- Es wurden keine Personen (Mitglieder, Gesellschafter, diesen nahestehende Personen, Dritte) durch zweckfremde Verwaltungsausgaben bzw. durch unverhältnismäßig oder unangemessen hohe Vergütungen (überhöhte Gehälter, überhöhte Vergütungen usw.) begünstigt.

Alle Angaben erfolgen wahrheitsgemäß und nach bestem Wissen und Gewissen. ☐

ANTRAG NUR DURCH STEUERBERATER:IN, WIRTSCHAFTSPRÜFER:IN

Eingabemaske Finanzonline

02

DATENÜBERMITTLUNGS-VERPFLICHTUNG

Meldung Sonderausgaben

DATENÜBERMITTLUNGSVERPFLICHTUNG

ZULASSUNG ZUR DATENÜBERMITTLUNG

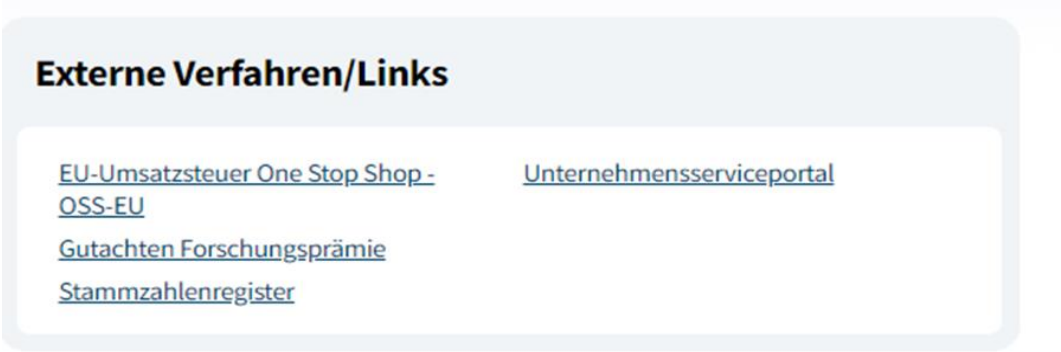
- Datenübermittlungsverpflichtung
  - Meldung der Daten (Spender und Höhe der Spende) bis Ende Februar des Folgejahres an das Finanzamt über FinanzOnline
    - Vorname und Zuname des Spenders (Schreibweise des Namens lt Meldezettel!)
    - Geburtsdatum des Spenders
    - Höhe der Spende
  - verschlüsseltes bereichsspezifische Personenkennzeichne für Steuern und Abgaben (vbPK SA) nötig zur Identifikation des Spenders – in Übereinstimmung mit Datenschutzrecht, wird auf Basis Namen und Geb.Dat. ermittelt
  - Zugriff (vbPK SA) kann in Finanz-Online beantragt werden.
  - Ermittlung des verschlüsselten Personenkennzeichens, zwei Verfahren stehen zur Auswahl:
    - Datenstromverfahren
    - Dialogverfahren

- Spende wird vom Finanzamt automatisch als Sonderausgabe in der Steuererklärung des Spenders berücksichtigt
- Für Spenden, die vom automatischen Datenaustausch betroffen sind, besteht für die Organisation keine Verpflichtung zur Ausstellung einer Spendenbestätigung (EStR Rz 1341)

DATENÜBERMITTLUNGSVERPFLICHTUNG

VERSCHLÜSSELTE, BEREICHSSPEZIFISCHE PERSONENKENNZEICHEN FÜR STEUERN UND ABGABEN VBPK SA

- Spendenbegünstigte Organisation muss auf Grundlage der bekanntgegebenen Daten des Spenders das verschlüsselte, bereichsspezifische Personenkennzeichen für Steuern und Abgaben (vbPK SA) ermitteln.
- Vergabe des vbPK SA erfolgt auf Basis einer Anfrage an das Stammzahlenregister in FinanzOnline



- Vor- und Zuname sowie Geb.Datum werden mit dem im ZMR gespeicherten Vor- und Zunamen sowie Geb.Datum verglichen
  - vbPK SA wird vergeben.
  - FinanzOnline Zugang notwendig, wenn Datenübermittlung von Organisation selbst vorgenommen wird

- Übermittlung kann auch durch einen Dienstleiter erfolgen (zB Steuerberater:in, Spend2 Formular)

DATENÜBERMITTLUNGSVERPFLICHTUNG

3 MÖGLICHKEITEN DER ERFASSUNG DER SONDERAUSGABEN

1. Buchung der Spenden über ein Buchungsprogramm (zB BMD)
   - der Spender ist als Kunde anzulegen
   - Übermittlung mittels eigener Programmfunktion im Datenstromverfahren

DATENÜBERMITTLUNGSVERPFLICHTUNG

3 MÖGLICHKEITEN DER ERFASSUNG DER SONDERAUSGABEN

2. Import der Spendenliste mittels CSV-File (Datenstromverfahren)
   - Ermittlung des vbPK mittels File-upload
     - Erstellung einer CSV-Datei aus der Spenderliste

D8

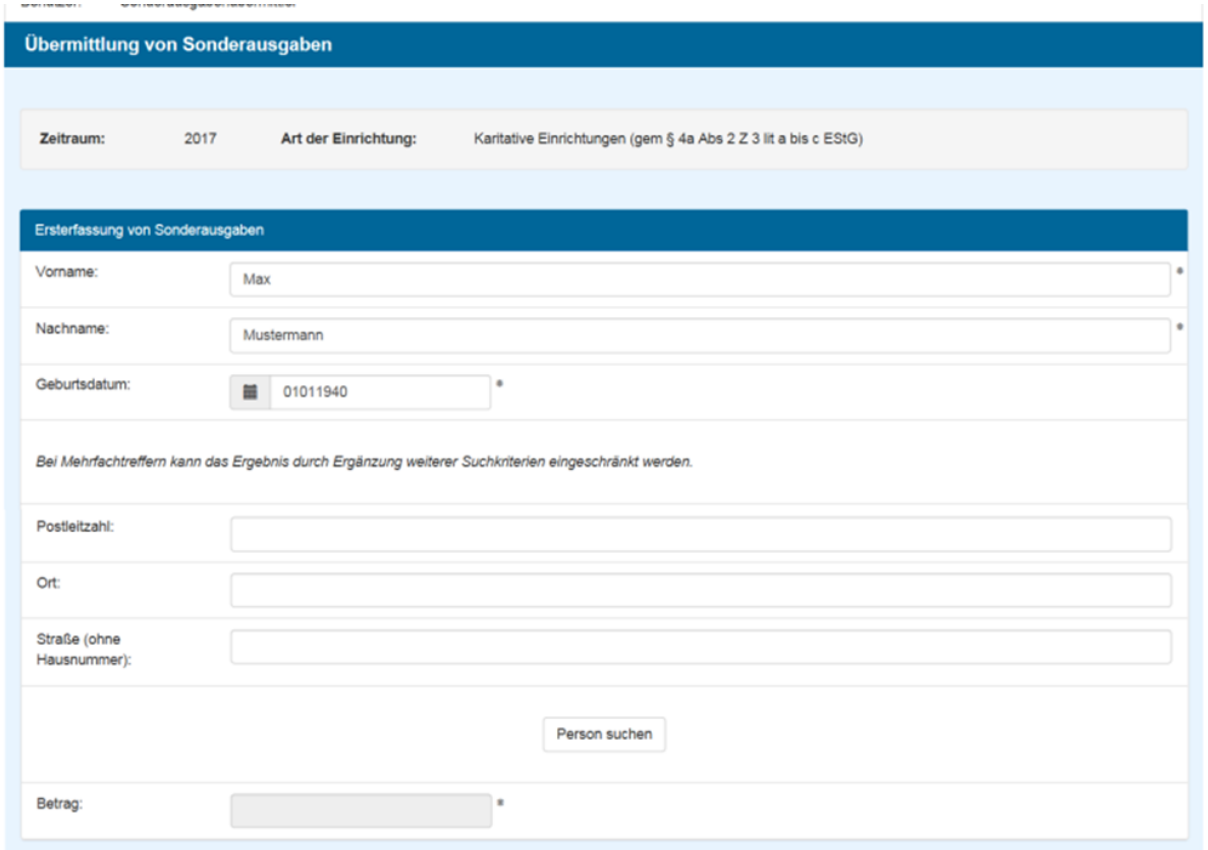
	A	B	C	D	E	F	G	H	I
1	Datum	Betrag	Nachname	Vorname	Geburtsdatum	Straße	Postleitzahl	Ort	Land
2	17.09.2017	50	Muster	Josef	12.12.1975	Wickistraße 4	4020	Linz	1
3									

     - Hochladen des CSV-Datei über FinanzOnline
     - Retourerhalt einer ZIP-Datei der Spender:in mit den vbPK-Nummer, welche wiederum importiert werden muss
     - Übermittlung kann durch die Organisation selbst erfolgen oder einen Dienstleister (zB Steuerberater:in, Spend2 Formular)
     - Erstellung der XML-Datei
     - Übermittlung der XML-Datei via FA-Online oder WebService

DATENÜBERMITTLUNGSVERPFLICHTUNG

3 MÖGLICHKEITEN DER ERFASSUNG DER SONDERAUSGABEN

3. manuelle Eingabe über Eingabemaske in FinanzOnline (Dialogverfahren)
   - Eingabe für jede Person einzeln



DATENÜBERMITTLUNGSVERPFLICHTUNG

SANKTION BEI NICHTERFÜLLUNG

- Finanzamt kann:
  - die Spendenbegünstigung widerrufen
  - der spendenbegünstigten Organisation einen Zuschlag zur Körperschaftssteuer in Höhe von 20% der zugewendeten Beträge vorschreiben

03

KEINE DATENÜBERMITTLUNGS-VERPFLICHTUNG

Spenden aus dem Betriebsvermögen

KEINE DATENÜBERMITTLUNG AN FINANZAMT

SPENDEN AUS DEM BETRIEBSVERMÖGEN

- keine Datenübermittlung an das Finanzamt bei Spenden aus dem Betriebsvermögen
  - Spender:in darf seine persönlichen Daten nicht bekanntgeben (sonst Annahme Spende aus Privatvermögen)

- Spenden sind vom Spender:in in der Steuererklärung als Betriebsausgabe anzugeben
  - auf Verlangen des Finanzamtes ist die Spende vom Spender durch Beleg (zB Quittung, Erlagschein, Kontoauszug) nachzuweisen

- auf Verlangen des Spenders ist von der empfangenden Organisation eine Spendenbestätigung auszustellen:
  - Name und die Anschrift des Spenders
  - der Name des Spendenempfängers
  - Höhe der Geldzuwendung
  - genaue Bezeichnung der Sachzuwendung das
  - Datum der Zuwendung
  - Verwendungszweck der Spende
  - die Registrierungsnummer unter der der Spendenempfänger in der Liste der begünstigten Spendenempfänger eingetragen ist
  - ordnungsgemäße Unterfertigung der empfangenden Organisation

KEINE DATENÜBERMITTLUNG AN FINANZAMT

SACHSPENDEN AUS DEM BETRIEBSVERMÖGEN - SPENDENBESTÄTIGUNG

- Sachspenden sind beim Spender nur steuerlich abzugsfähig wenn diese aus dem Betriebsvermögen geleistet werden

- Spendenbestätigung muss enthalten (EStR Rz 1341):
  - genaue Bezeichnung der Sachzuwendung
  - Die Beschreibung der Sachzuwendung muss gewährleisten, dass der gespendete Gegenstand eindeutig identifizierbar ist. Es sind die Kriterien der Beschreibung der Art und des Umfanges der Leistung in einer Rechnung im Sinne des § 11 UStG 1994 zu beachten. Bloße Sammelbezeichnungen (zB Speisen, Getränke, Lebensmittel) sind nicht ausreichend.
  - Sachzuwendungen sind im Rahmen der Spendenbestätigung durch den Spendenempfänger nicht zu bewerten
  - die Bewertung hat durch den Spender zu erfolgen.

04

DATENSCHUTZ

Rechtsgrundlagen und Grundsätze im Datenschutz
sowie Datenschutzverletzungen

PERSONENBEZOGENE DATEN

Definition und Kategorien von personenbezogenen Daten 1/2

DEFINITION „PERSONENBEZOGENE DATEN“

- Alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** (im Folgenden „betroffene Person“) beziehen;
- "Personenbezogene Daten” umfassen
  - alle Information, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen;
  - Informationen oder eine Kombination von Informationen, welche die Identifizierung einer natürlichen Person ermöglichen.

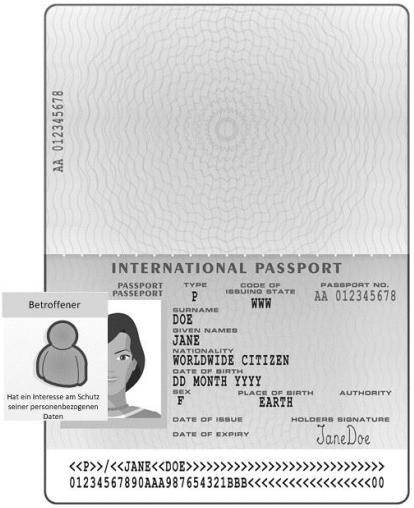
- <u>Beispiele:</u>
  - Persönliche Daten (z.B. Vorname, Nachname, Geburtsdatum, akademischer Titel)
  - Kontaktdaten (z.B. Adresse, Telefonnummer, E-Mail Adresse)
  - Sozialdaten (z.B. Beziehungsstatus (verheiratet, geschieden, verwitwet, Kinder..))
  - Finanzdaten (z.B. Kontoverbindung, Kreditkartennummer, Bonität)
  - Spendendaten (z.B: Spendenbetrag, Kommunikations- und Spendenhistorie, Spendenhöhe, Häufigkeit)

PERSONENBEZOGENE DATEN

Definition und Kategorien von personenbezogenen Daten 2/2

Besondere Kategorien personenbezogener Daten

- Personenbezogene Daten, aus denen die "rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person".*



Strafrechtsbezogene Daten

- Strafrechtliche Verurteilungen, Straftaten und
  - Auch Verwaltungsstrafrecht!

Verfahren

*Vgl. Artikel 9 DSGVO.

WAS IST VERARBEITUNG?

Definition von Verarbeitung und Beispiele

DEFINITION „VERARBEITUNG“

- Verarbeitung ist ,,jede mit oder ohne Hilfe automatisierte Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“

- Beispiele für Verarbeitung sind:
  - Versenden und Empfangen von E-Mails, die personenbezogene Daten beinhalten
  - Analyse historischer Spendendaten
  - Übermittlung von Spendendaten z.B. an das Finanzamt
  - Löschen von personenbezogenen Daten
  - Kontaktaufnahme zur Spendenwerbung
  - Systematische Ablage von personenbezogenen Daten in einem Aktensystem (Karteisystem)

DATENSCHUTZ IM ÜBERBLICK

*Wesentliche Pflichten der DSGVO**

UNTERBAU

Technische und organisatorische Maßnahmen (TOM) / IT-Sicherheit (Artikel 32 DSGVO)

Datenschutzbeauftragter (Artikel 37-39 DSGVO)

***Übersicht stellt einen Auszug einiger relevanten Pflichten nach der DSGVO dar.**
Bei Verstößen: Geldbußen bis zu 20 000 000 EUR oder bis zu 4 % des weltweit erzielten Jahresumsatzes.

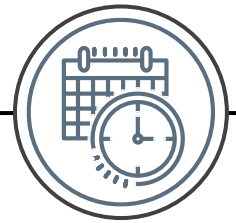
IMMER EINZUHALTEN

Grundsätze (Artikel 5 DSGVO)

Rechtsgrundlagen (Artikel 6, 9 und 10 DSGVO)

Informationspflichten (Artikel 12 bis 14 DSGVO)

Verzeichnis von Verarbeitungstätigkeiten (Artikel 30 DSGVO)



ANLASSBEZOGEN

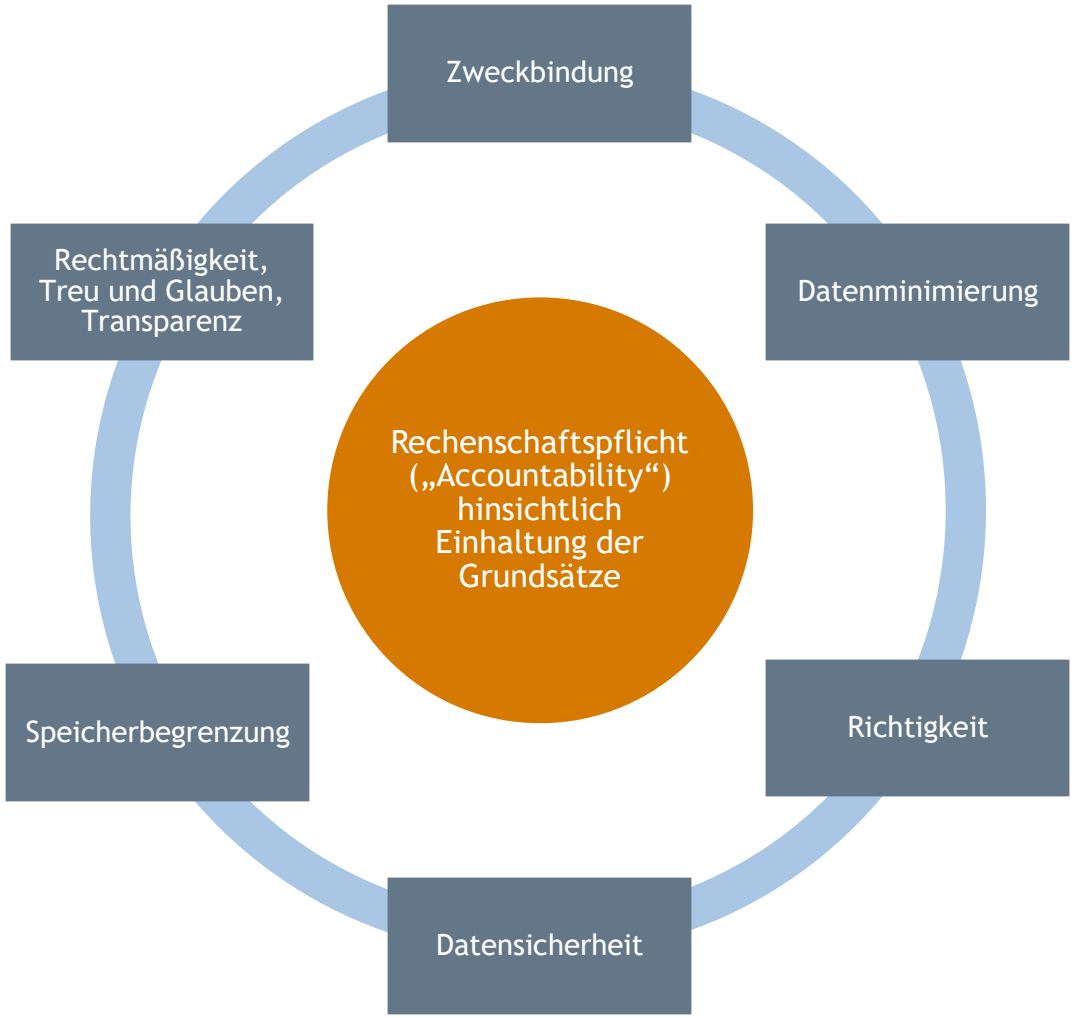
Auftragsverarbeiter (Artikel 28 DSGVO)

Betroffenenanfragen (Artikel 15 bis 18 und 20 DSGVO)

Datenschutzverletzungen (Artikel 33 und 34 DSGVO)

GRUNDSÄTZE IM DATENSCHUTZ

Grundsätze für die Verarbeitung personenbezogener Daten



GRUNDSÄTZE IM DATENSCHUTZ

Grundsätze für die Verarbeitung personenbezogener Daten

- **Rechtmäßigkeit, Treu und Glauben, Transparenz**
  Personenbezogene Daten müssen rechtmäßig, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

- **Zweckbindung**
  Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

- **Datenminimierung**
  Personenbezogene Daten müssen im Hinblick auf den jeweiligen Zweck angemessen und erheblich sowie auf das für die Verarbeitungszwecke unbedingt notwendige Ausmaß beschränkt sein.

- **Richtigkeit**
  Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die hinsichtlich der Verarbeitungszwecke unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

GRUNDSÄTZE IM DATENSCHUTZ

Grundsätze für die Verarbeitung personenbezogener Daten

- **Speicherbegrenzung**
  Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Personenbezogene Daten sind sohin zu löschen bzw. zu anonymisieren, sobald der jeweilige Verarbeitungszweck erfüllt ist.

- **Integrität und Vertraulichkeit**
  Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Zum Schutz personenbezogener Daten vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung sind geeignete technische und organisatorische Maßnahmen umzusetzen.

- **Rechenschaftspflicht**
  Der **Verantwortliche** ist für die Einhaltung der Grundsätze verantwortlich und muss deren Einhaltung nachweisen können.

Die meisten Pflichten iZm der DSGVO sind vom sogenannten Verantwortlichen zu erfüllen. Dieser hat sicherzustellen, dass personenbezogene Daten gemäß den DSGVO Grundprinzipien verarbeitet werden, dass Dokumentationserfordernisse erfüllt und angemessene technische und organisatorische Maßnahmen umgesetzt und laufend aktualisiert werden. Der Verantwortliche ist für die Behandlung der Betroffenenrechte und die Gewährleistung allgemeiner DSGVO Compliance verantwortlich.

RECHTSGRUNDLAGEN

Rechtmäßigkeit – Rechtsgrundlagen für die Verarbeitung personenbezogener Daten

Wann dürfen Daten verarbeitet werden?

- Die DSGVO verbietet grundsätzlich die Verarbeitung von personenbezogenen Daten, außer es liegt eine Rechtsgrundlage für die Verarbeitung vor (Verbot mit Erlaubnisvorbehalt)
- Es ist zu unterscheiden zwischen Rechtsgrundlagen für:
  - Nicht sensible personenbezogene Daten (Art 6 DSGVO)
  - Sensible personenbezogene Daten (Art 9 DSGVO)
  - Strafrechtsbezogene Daten (Art 10 DSGVO)
- Auch wenn eine Rechtsgrundlage vorliegt muss das Verhältnismäßigkeitsprinzip beachtet werden. D.h. es dürfen nur diejenigen personenbezogenen Daten verarbeitet werden die notwendig sind, um den Zweck zu erreichen.
- Sie dürfen, des Weiteren nur für die Dauer verarbeitet werden, für die sie notwendig sind, um den Zweck zu erreichen. Falls der Zweck ohne die Verarbeitung von personenbezogenen Daten möglich ist, muss die Verarbeitung personenbezogener Daten unterbleiben.

Die Verarbeitung von personenbezogenen Daten ist nur aufgrund einer Rechtsgrundlange zulässig!

RECHTSGRUNDLAGEN

Rechtmäßigkeit – Rechtsgrundlagen für die Verarbeitung personenbezogener Daten

Personenbezogene Daten

Grundsätzliches Verbot der Datenverarbeitung

Verhältnismäßigkeitsprinzip
Gelindestes Mittel!

Nicht-sensible Daten (Art 6)	Besondere Kategorien personenbezogener Daten (Art 9)	Strafrechtsbezogene Daten (Art 10)
Vor allem: ▶ Vertragserfüllung (Kundenverträge, Dienstverträge) ▶ Rechtliche Verpflichtung (Geldwäschebekämpfung, SV Meldungen, Aufbewahrungspflichten) ▶ Berechtigtes überwiegendes Interesse ▶ Einwilligung (z.B. Newsletter, Cookies)	Vor allem: ▶ Ausdrückliche Einwilligung ▶ Ausübung/Erfüllung von Rechten/Pflichten aus dem Arbeits- bzw. Sozialrecht ▶ Lebenswichtige Interessen des Betroffenen oder einer anderen natürlichen Person ▶ Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen ▶ Offensichtlich vom Betroffenen selbst öffentlich gemachte Daten ▶ Rechtsgrundlage in Unionsrecht oder nationalem Recht	Nur unter behördlicher Aufsicht oder gemäß nationalen Recht. In Österreich: ▶ Ausdrückliche rechtliche Ermächtigung bzw. Verpflichtung ▶ Gesetzliche Sorgfaltspflichten ▶ Berechtigtes überwiegendes Interesse

VERARBEITUNG VON (SPENDEN-)DATEN

Informationspflichten

Über was muss informiert werden?

Der Verantwortliche hat betroffenen Personen gemäß Artikel 13 und 14 DSGVO vor Beginn der Verarbeitung der personenbezogenen Daten bzw. innerhalb normierter Fristen bestimmte Informationen zu erteilen. Dazu gehören:

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Zwecke und Rechtsgrundlagen der Verarbeitung
- Wenn relevant: Beschreibung der berechtigten Interessen
- (Kategorien der) Empfänger, an die die Daten offengelegt werden sollen sowie Angabe „geeigneter“ bzw. „angemessener Garantien“ (bei Drittländern)
- Angaben zur Speicherdauer hinsichtlich der Daten
- Hinweis auf die Betroffenenrechte
- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde
- Ggf. Bestehen automatisierter Entscheidungsfindung bzw. Profiling mit Beschreibung der Logik und Tragweite der Auswirkungen für die betroffene Person
- Herkunft der Daten, wenn die personenbezogenen Daten nicht bei der betroffenen Person selbst erhoben wurden

Dieses Recht ist ohne Antrag der betroffenen Person zu erfüllen -> Datenschutzerklärungen!

VERARBEITUNG VON (SPENDEN-)DATEN

Nutzung der Daten für Spendenaufrufe und Werbung

Sind Spenden-aufrufe und Werbungen zulässig?

- Mitglieder- und Spendenwerbung ist zulässig, da regelmäßig ein erhebliches Interesse an der Mitglieder- und Spendenwerbung besteht, um einen ausreichenden Mitgliederbestand und genügend finanzielle Mittel sicherzustellen. Die Daten dürfen nur für Spendenaufrufe und für Werbung zur Erreichung der eigenen Ziele des Vereins genutzt werden (Art. 6 Abs. 1 lit. b) DS-GVO).
- Spendenwerbung ist aufgrund des berechtigten Interesses über die Verwendung der getätigten Spende und über neue Spendenaktionen zu informieren, zulässig wenn bereits Spende getätigt wurde (Art. 6 Abs. 1 lit. f) DSGVO). Achtung Widerspruchsrecht!
- Bisher keine Spendentätigkeit: Spendenaufruf-Newsletter zulässig mit Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO).

Für die Zulässigkeit der Spendenaufrufe und Werbung muss eine Rechtsgrundlage vorliegen!

VERARBEITUNG VON (SPENDEN-)DATEN

Aufbewahrungsfristen und Löschung

Wann müssen Daten gelöscht werden?

- Abhängig vom Verarbeitungszweck, Art der Daten und Rechtsgrundlage!
- Personenbezogene Daten sind nach Artikel 17 DSGVO jedenfalls zu löschen wenn:
  - der Zweck erloschen ist, also die Daten also nicht mehr benötigt werden. Die zweckentfremdete Nutzung ist grundsätzlich unzulässig.
  - eine der Erhebung zugrunde liegende Einwilligung durch den Betroffenen widerrufen wurde. (Ausnahme: Datenverarbeitung ist nicht allein von der Einwilligungserklärung des Betroffenen abhängig)
  - Die Betroffene Person vom Recht auf Löschung Gebrauch gemacht hat, sofern diesem Verlangen keine triftigen Gründe entgegenstehen.
  - eine andere Löschfrist berührt wird.
- Aufgrund Spendenabsetzbarkeit können bestimmte Daten nach Art. 132 Abs. 1 BAO jedenfalls 7 Jahre gespeichert werden. Darüberhinausgehend solange sie für die Abgabenbehörde in einem anhängigen Verfahren von Bedeutung sind.

Die Aufbewahrungsfristen unterscheiden sich abhängig vom Zweck und der Art der personenbezogenen Daten!

VERARBEITUNG VON (SPENDEN-)DATEN

Datenweitergabe an Dritte

Wann dürfen Daten weiter-gegeben werden?

- Die Übermittlung von (Spenden-)Daten an Dritte ist nur aufgrund einer Rechtsgrundlage zulässig.
- Grundsatz der Datenminimierung
  - Frage: Wer muss wann was wissen?
- Beispiele:
  - Übermittlung von personenbezogenen Daten an das Finanzamt zur Spendenabsetzbarkeit
  - Weitergabe von personenbezogenen Daten an den Rechnungshof (Parteienkontrolle)
  - Aushang der Mitgliederliste im Verein, wenn die Herausgabe der Mitgliederliste dem Erreichen des Vereinsziels dient (z.B. Selbsthilfevereine zum Informationsaustausch)
  - Weitergabe von Daten zur postalischen und telefonischen Spendenkommunikation an Dienstleister

Bei der Übermittlung von personenbezogenen Daten ist unbedingt auf das Prinzip der Datenminimierung zu achten!

DATENSCHUTZVERLETZUNGEN

Überblick

- Eine „Verletzung des Schutzes personenbezogener Daten“ (auch „Datenschutzverletzung“ oder „Data Breach“) ist definiert als „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.“
- Beeinträchtigung
  - der Vertraulichkeit, Integrität bzw. Verfügbarkeit von personenbezogenen Daten

- In welchen Fällen liegt eine Datenschutzverletzung vor?
  Beispiele:
  - Erteilung von Zugriffsrechten an unbefugte Personen (fehlerhafte Zugriffsberechtigungen)
  - Übermittlung Spendendaten an falsche Empfänger
  - Unrechtmäßige Zugriffe auf Spendenlisten durch unbefugte Personen (Hacking, Leaks)
  - Verlust von personenbezogenen Daten durch Software-/Hardware-Fehler
  - Unerwünschte Veränderung von personenbezogenen Daten im Rahmen von Datenübermittlungen, -exporten bzw. -importen
  - Unbeabsichtigte Veröffentlichung personenbezogener Daten im Internet

- Formular zur Meldung einer Verletzung des Schutzes personenbezogener Daten

DATENSCHUTZVERLETZUNGEN

Was ist bei einer Datenschutzverletzung zu tun?

Kein Risiko für die Betroffenen

- Interne Dokumentation

Risiko für die Betroffenen

- Unverzügliche Meldung (möglichst binnen 72 Stunden) an die Datenschutzbehörde

Hohes Risiko für die Betroffenen

- Unverzügliche Meldung (möglichst binnen 72 Stunden) an die Datenschutzbehörde
- Unverzügliche Benachrichtigung der betroffenen Personen(en)

IM FALL EINER VERLETZUNG DES SCHUTZES PERSONENBEZOGENER IST DIESE UNVERZÜGLICH UND MÖGLICHST BINNEN 72 STUNDEN NACH KENNTNISNAHME AN DIE DATENSCHUTZBEHÖRDE ZU MELDEN!

DATENSCHUTZVERLETZUNGEN

Welche Informationen sind bei einer Einmeldung hilfreich?

- Wann ist es zur Datenschutzverletzung gekommen?
  - Zeitpunkt der Handlung die zur Datenschutzverletzung geführt hat (z.B. Zeitpunkt der Falschversendung, Zeitpunkt der Vergabe von inkorrekten Zugriffsrechten)
- Wann wurde die Datenschutzverletzung festgestellt?
- Wie wurde die Datenschutzverletzung festgestellt? (z.B. Falschempfänger wies von sich aus darauf hin)
- Wie ist es zur Datenschutzverletzung gekommen?
  - Was war die Ursache? (z.B. menschlicher Fehler (falschen Empfänger eingefügt), technischer Fehler)
- Wessen Daten sind betroffen?
  - z.B. Mitarbeiter, Spender, Kontaktpartner
- Welche Daten sind betroffen?
  - z.B. Vor- Nachname, Kontaktdaten, Spender
- Falls die Daten an einen unberechtigten Dritten offengelegt worden sind:
  - Wer ist der Dritte? (z.B. andere Organisation, anderer Verein, keine Verbindung)
  - An wie viele Dritte wurden die Daten offengelegt?

05

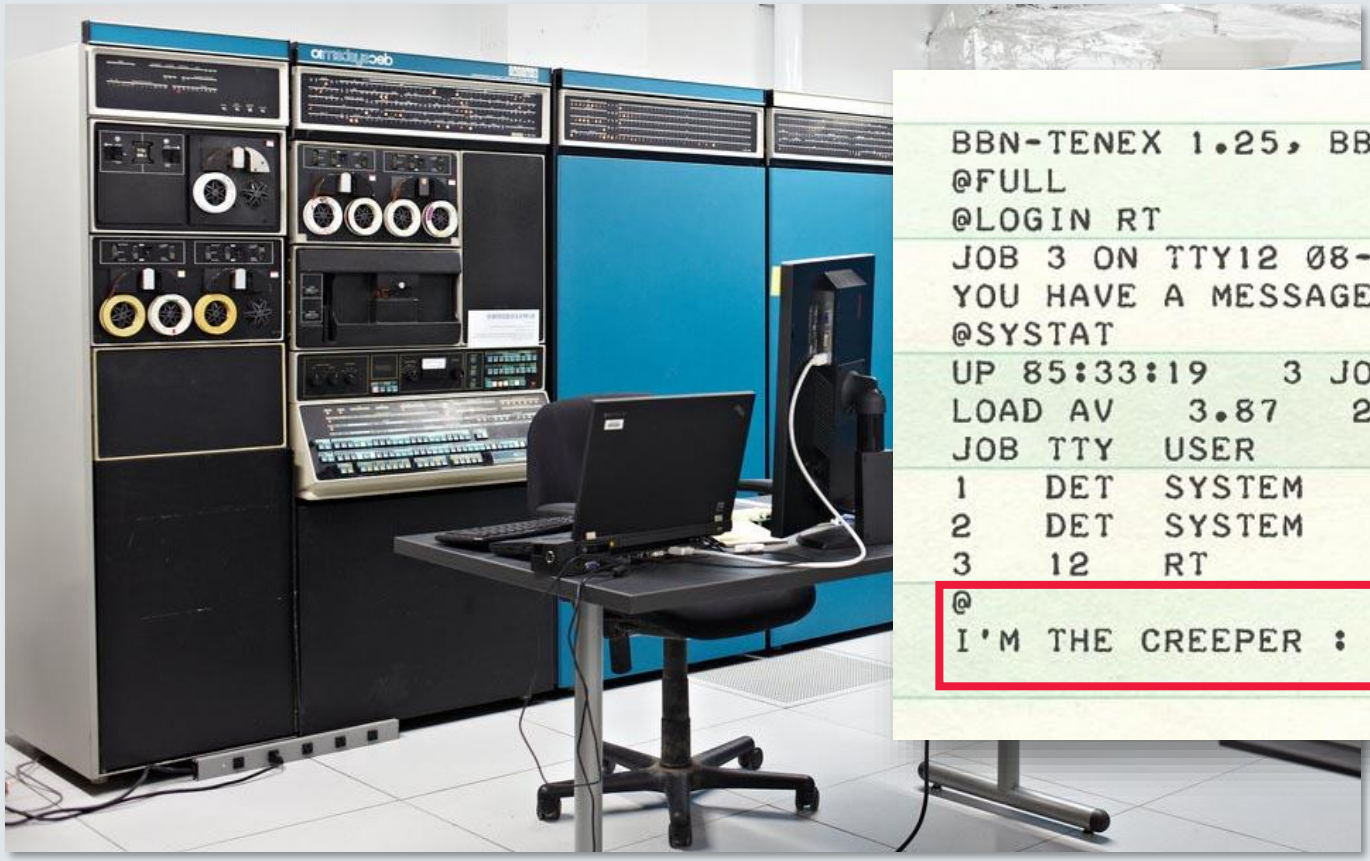
INFORMATIONS-SICHERHEIT

Der Schutz von Informationen
unabhängig von ihrer Darstellungsform
(elektronisch, schriftlich, bildhaft oder gesprochen)

https://www.pexels.com/de-de/foto/autos-strasse-verkehr-wasser-163945/

WIE ALLES BEGANN - 1971

Cyber Crime und seine Auswirkungen



```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19   3 JOBS
LOAD AV   3.87   2.95   2.14
JOB TTY  USER      SUBSYS
1   DET  SYSTEM    NETSER
2   DET  SYSTEM    TIPSER
3   12   RT        EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

https://corewar.co.uk/creeper.htm

https://www.livingcomputers.org/Computer-Collection/Vintage-Computers/Mainframes/DEC-PDP-10-KI-10-(DECsystem-10).aspx

CYBER SECURITY RISIKEN

Cyber Crime und seine Auswirkungen

REPUTATIONSVERLUST

Website Defacement
Fake News
Datenlecks

DATENDIEBSTAHL

Hacking von Webseiten und IT-Netzwerken über Schwachstellen

ERPRESSUNG

Denial-of-Service Angriffe
Ransomware

AUSNUTZUNG VON RESSOURCEN

Crypto-Mining
Botnetze

SPIONAGE

Social Engineering
Phishing

BETRUG

CEO – Fraud
Fake President Angriffe

SABOTAGE

Lahmlegen des Unternehmens
Ransomware

WER SIND DIE PROFITEURE VON CYBER CRIME?

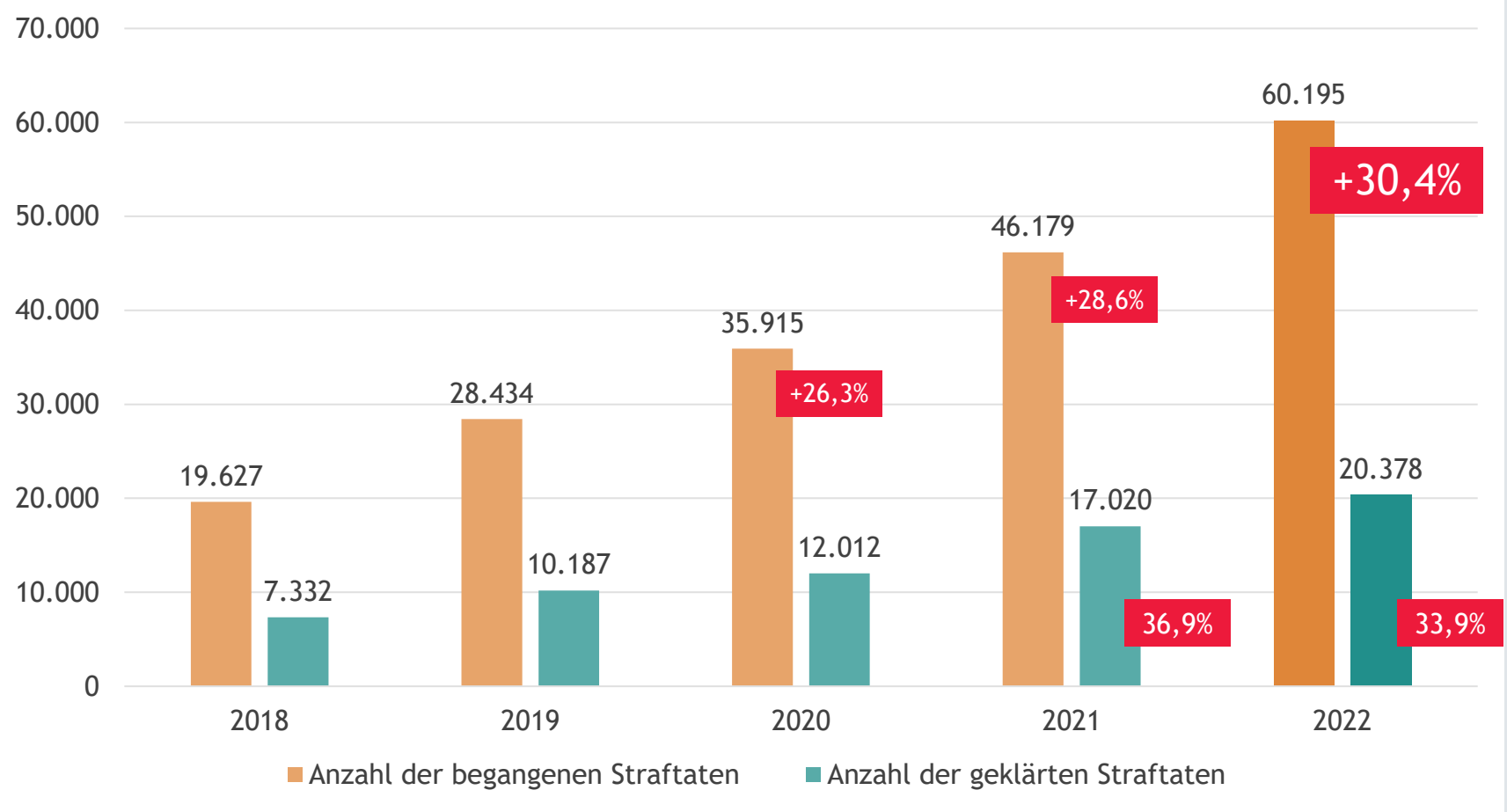
Cyber Crime und seine Auswirkungen

Hacker Group REvil

https://www.interpol.int/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring
https://www.bbc.com/news/technology-59297187

CYBER CRIME IN ÖSTERREICH

Straftaten vs. geklärte Straftaten - Report 2022



https://bundeskriminalamt.at/306/files/Cybecrime_2022_V20230517_webBF.pdf

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

DI Walter Stephan (CEO) aus dem Vorstand der FACC AG mit sofortiger Wirkung abberufen

Der Aufsichtsrat hat in seiner Sitzung vom 24. Mai 2016 Herrn DI Walter Stephan als Vorsitzenden des Vorstandes der FACC AG mit sofortiger Wirkung aus wichtigem Grund abberufen. Der Aufsichtsrat ist zum Schluss gekommen, dass Herr DI Walter Stephan seine Pflichten schwerwiegend verletzt hat, insbesondere im Zusammenhang mit dem "Fake President" Vorfall.

Hr. Robert Machtlinger wurde vorübergehend als CEO der FACC AG bestellt.

25/05/2016 | Ad-Hoc

*FACC war Anfang 2016 Opfer eines "Fake President Fraud" geworden. Betrüger hatten sich gegenüber der Buchhaltung des Unternehmens als Firmenchefs ausgegeben und in mehr als 92 "streng vertraulichen" Mails die Überweisung von **54 Millionen Euro** auf ausländische Konten gefordert. Die Buchhaltung kam der vermeintlichen Weisung des Vorstands nach.*

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

Hackerangriff *Daten von FMA geklaut*

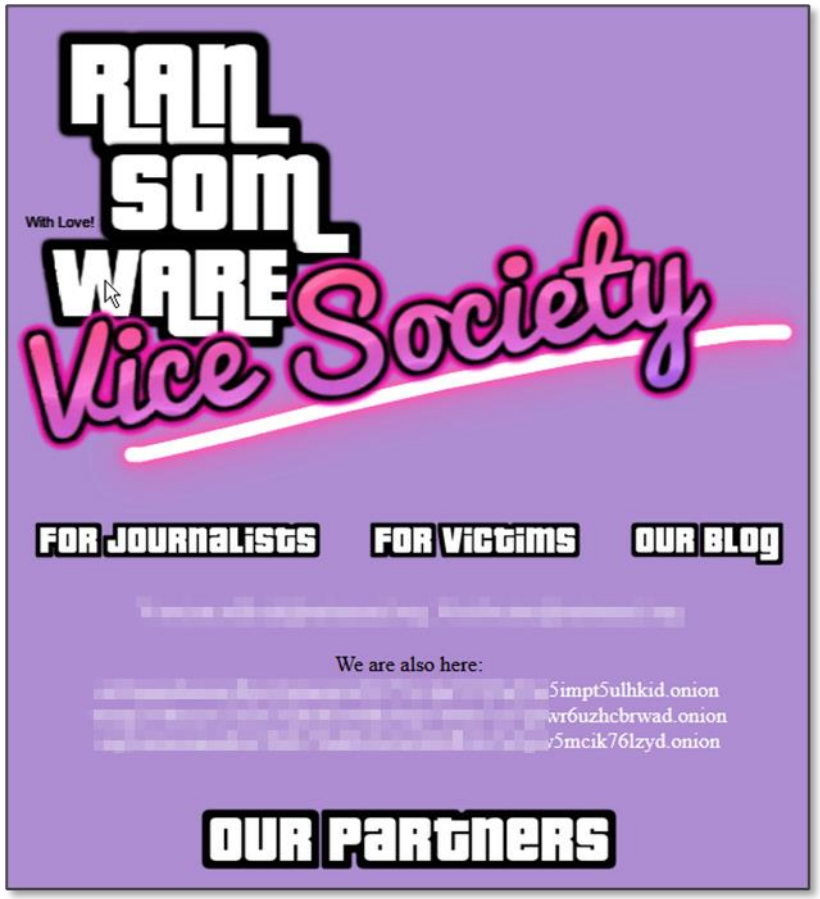
Bei der Finanzmarktaufsicht (FMA) ist eine virtuelle Diebesbande eingefallen. Wie gerade bekannt wurde, haben sich Hacker über eine Sicherheitslücke in die Progress-Software gehackt und dabei Datensätze kopiert und gestohlen. Die Qualität der Daten ist sehr heterogen, erklärte mir FMA-Sprecher Klaus (Grubelnik), da sie zum Transfer bereitstanden.

Betroffen sind etwa Gehaltsdaten und Ähnliches von rund 400 FMA-Mitarbeitern sowie noch ein paar Dutzend unterschiedliche Datensätze anderer. Klaus erzählt, dass die Betroffenen bereits informiert wurden und das Sicherheitsleck geschlossen sei. Die gestohlenen Daten konnten allesamt wiederhergestellt werden. Die Lücke im System entstand übrigens über die bislang als relativ sicher geltende Software

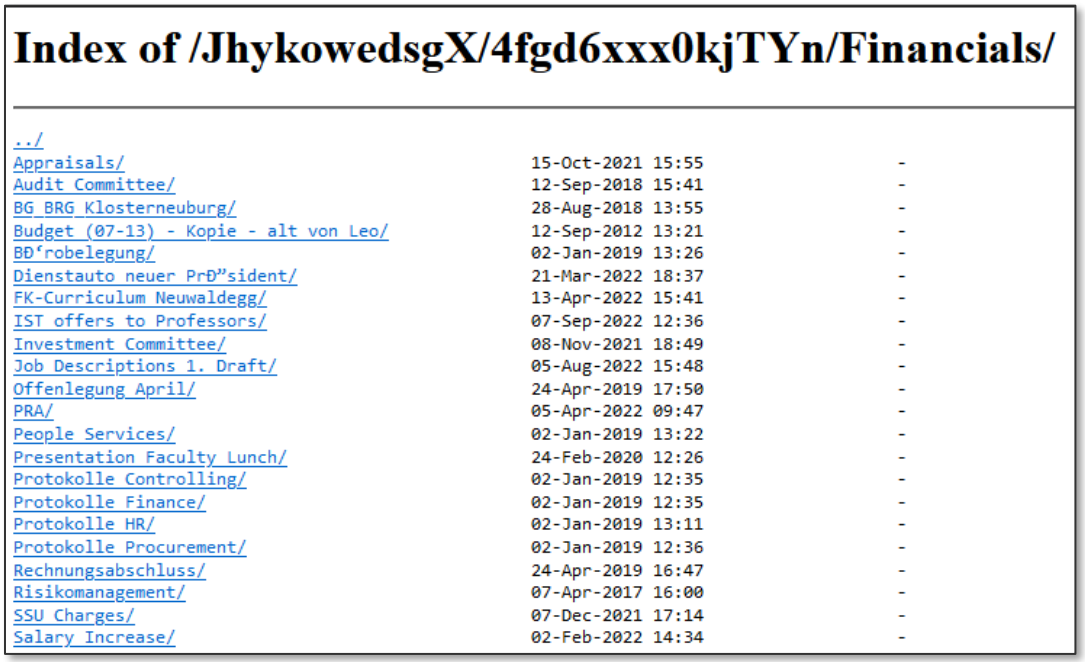
Die Finanzmarktaufsicht wurde Mitte 2023 Ziel einer Cyberangriffskampagne. Die Täter erlangten bei dem Angriff verschiedene Daten, darunter auch Gehaltsdaten von ca. 400 Mitarbeitern der Finanzmarktaufsichtsbehörde.
https://www.derboersianer.com/2023/06/hackerangriff-daten-von-fma-geklaut/

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft



*Quelle: Onion Service



Index of /JhykowedsgX/4fgd6xxx0kjTYn/Financials/

../		
Appraisals/	15-Oct-2021 15:55	-
Audit Committee/	12-Sep-2018 15:41	-
BG BRG Klosterneuburg/	28-Aug-2018 13:55	-
Budget (07-13) - Kopie - alt von Leo/	12-Sep-2012 13:21	-
BĐ‘robelegung/	02-Jan-2019 13:26	-
Dienstauto neuer PrĐ”sident/	21-Mar-2022 18:37	-
FK-Curriculum Neuwaldegg/	13-Apr-2022 15:41	-
IST offers to Professors/	07-Sep-2022 12:36	-
Investment Committee/	08-Nov-2021 18:49	-
Job Descriptions 1. Draft/	05-Aug-2022 15:48	-
Offenlegung April/	24-Apr-2019 17:50	-
PRA/	05-Apr-2022 09:47	-
People Services/	02-Jan-2019 13:22	-
Presentation Faculty Lunch/	24-Feb-2020 12:26	-
Protokolle Controlling/	02-Jan-2019 12:35	-
Protokolle Finance/	02-Jan-2019 12:35	-
Protokolle HR/	02-Jan-2019 13:11	-
Protokolle Procurement/	02-Jan-2019 12:36	-
Rechnungsabschluss/	24-Apr-2019 16:47	-
Risikomanagement/	07-Apr-2017 16:00	-
SSU Charges/	07-Dec-2021 17:14	-
Salary Increase/	02-Feb-2022 14:34	-

RISIKOANALYSE – KENNE DEINE RISIKEN

Created by AI (DALL-E 3)

ZIELE DER RISIKOANALYSE

Risikoanalyse

Früherkennung

- Erkennung potenzieller Risiken im Frühstadium
- Behebung von Kontrollschwächen
- Minimierung möglicher Folgekosten

Schutz der Assets

- Abwehr potenzieller Bedrohungen
- Effektiver Schutz von Vermögenswerten wie Daten oder Systemen
- Gewährleistung der Geschäftsfortführung

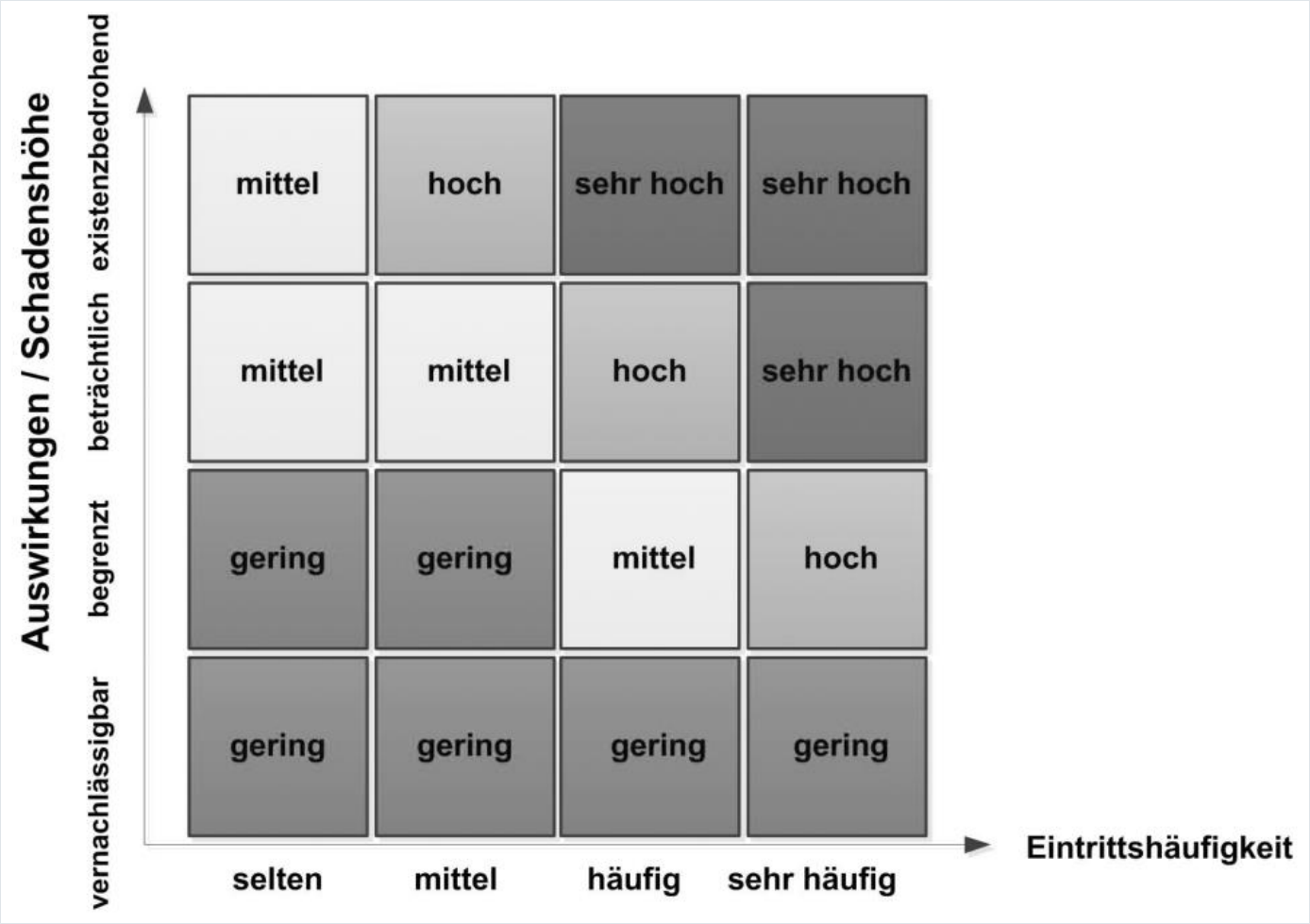
Kostenoptimierung

- Besseres Verständnis der Geschäftsprozesse
- Kosteneinsparungen durch bewussten Einsatz von Firmenressourcen
- Vermeidung von Fehlentscheidungen

DIE RISIKOANALYSE IST DAS FUNDAMENT ALLER (CYBER SECURITY) ENTSCHEIDUNGEN!

RISIKOBEWERTUNGSMATRIX

Risikoanalyse



Quelle: BSI Standard 200-3

VORBEREITUNG AUF DEN ERNSTFALL

Risikoanalyse

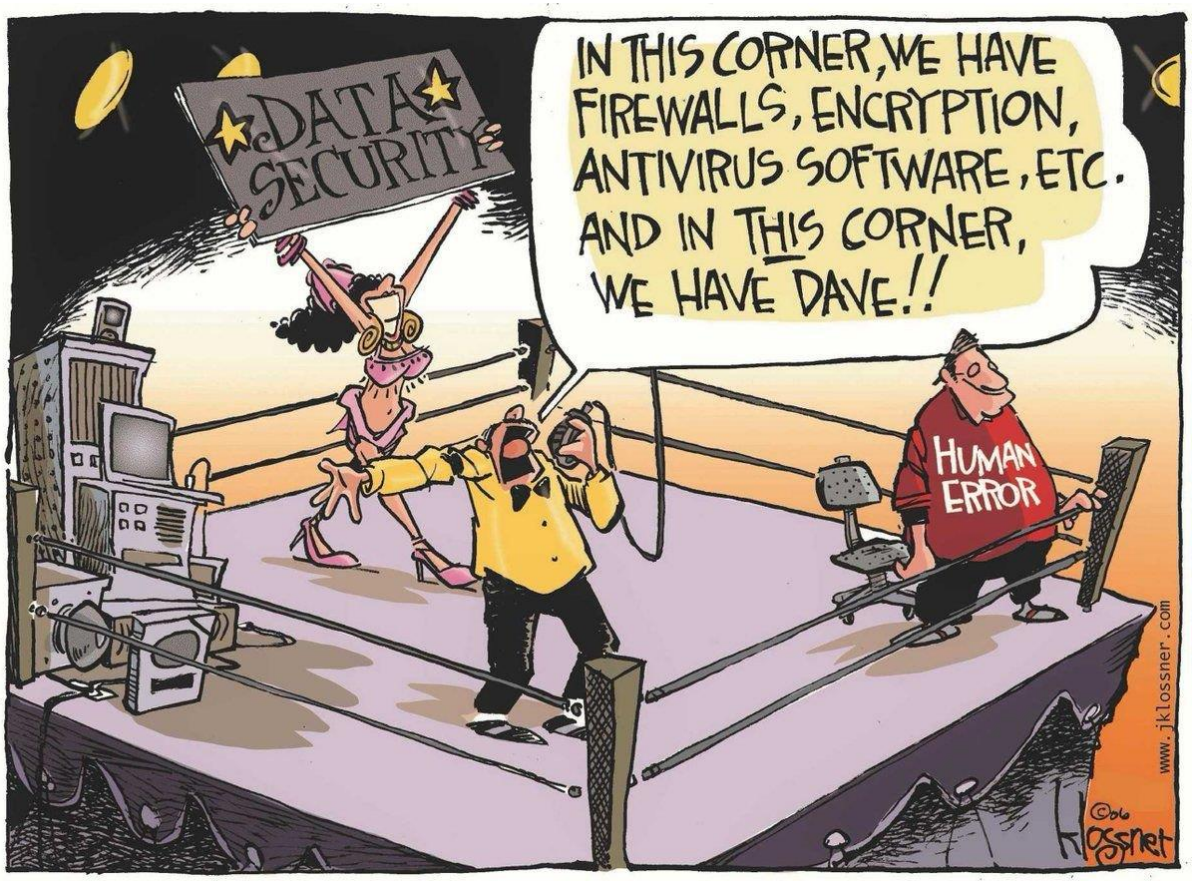
Empfehlungen!

- **Risikomanagement:** Identifizieren Sie die Risiken, bewerten Sie diese und definieren Sie Maßnahmen!

- Kennen Sie Ihre schützenswerten Daten (Business Impact Analyse) und schützen Sie diese!
  - Zugriffsberechtigungen einschränken
  - Regelmäßige Backups
  - Backups vor Veränderung sichern
  - Offline Backups anlegen

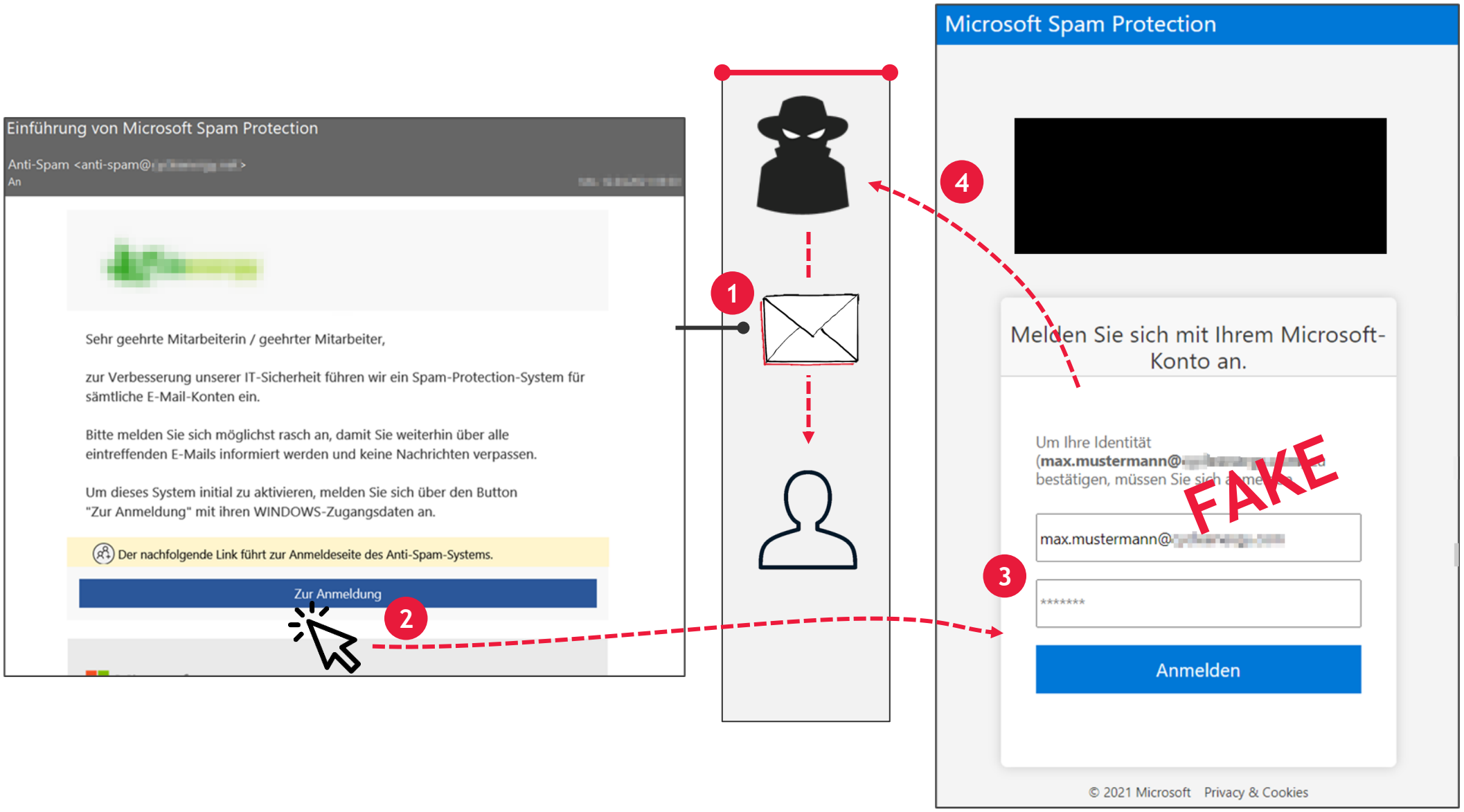
- Ziehen Sie professionellen Rat hinzu!

DER ANGRIFF AUF DIE MITARBEITER



PHISHING – DER ANGRIFF

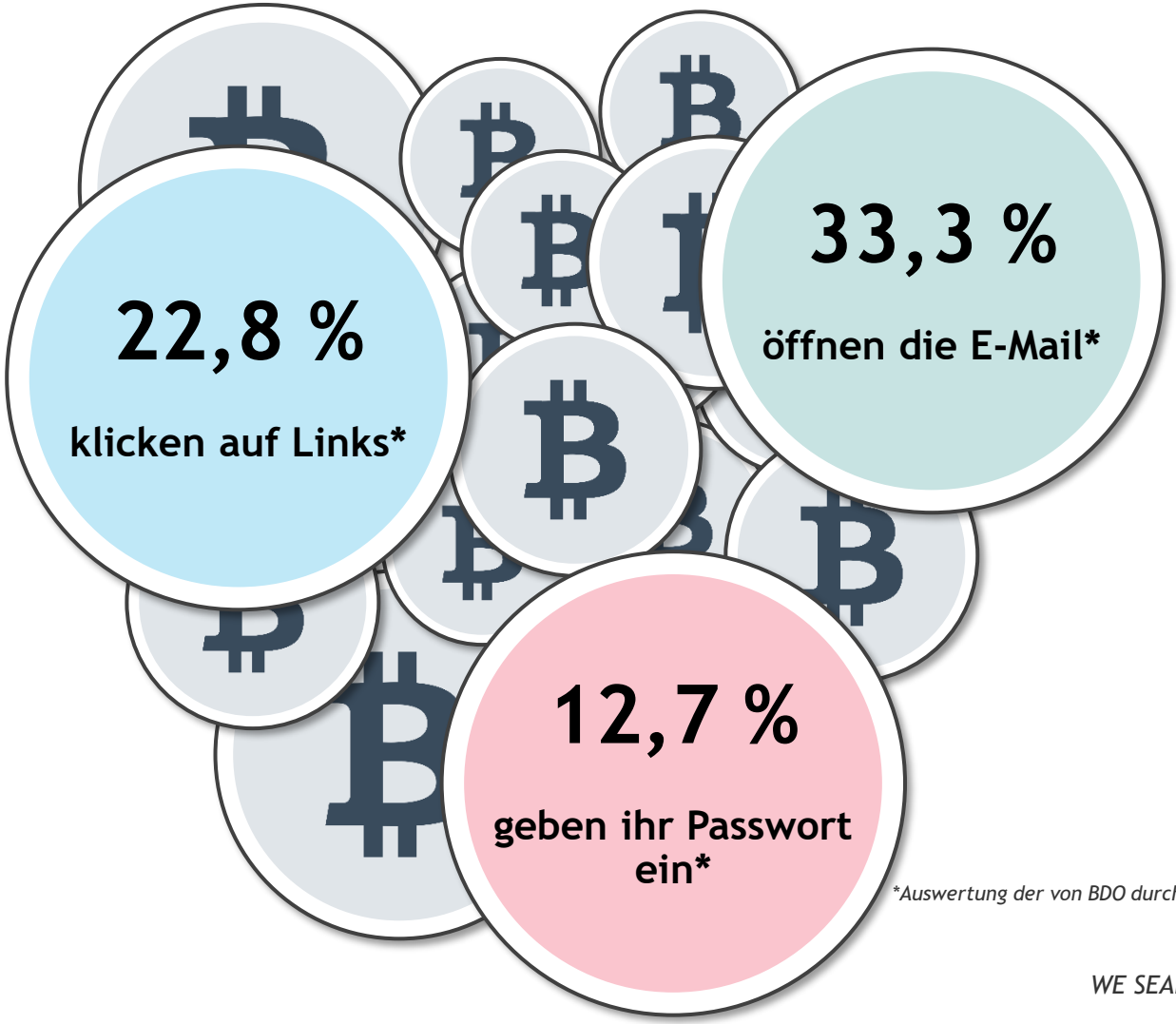
Der Angriff auf die Mitarbeiter



PHISHING – ALLTÄGLICHE GEFAHR

Der Angriff auf die Mitarbeiter

Phishing-E-Mails sind aktuelle die häufigste Angriffsart auf Unternehmen!



**Auswertung der von BDO durchgeführten Phishing-Simulationen (n=17.300 E-Mails)*

MITARBEITER REGELMÄßIG SCHULEN!

Der Angriff auf die Mitarbeiter

Empfehlungen!

- Schulen Sie Ihre Mitarbeiter zu Cyber Security Themen!

  Erklären Sie dabei, wie man verdächtige E-Mails erkennt und wohin diese gemeldet werden sollen!

- Überprüfen Sie den Lernerfolg mithilfe von simulierten Phishing-Kampagnen. Dadurch machen Sie die KPI Mensch messbar!

PASSWORTHYGIENE BETREIBEN!

Der Angriff auf die Mitarbeiter

- Überprüfen Sie, ob Sie von den Data Breaches betroffen sind!

  Ändern Sie Ihre Passwörter, sofern Sie von einem Data Breach betroffen sind!

- Verwenden Sie einzigartige und sichere Passwörter für jeden Dienst! -> Passwortmanager

- Verwenden Sie Mehrfaktorauthentifizierung und/oder Biometrie!

Empfehlungen!

Have I been pwned?
https://haveibeenpwned.com/

HPI Identity Leak Checker
https://sec.hpi.de/ilc/

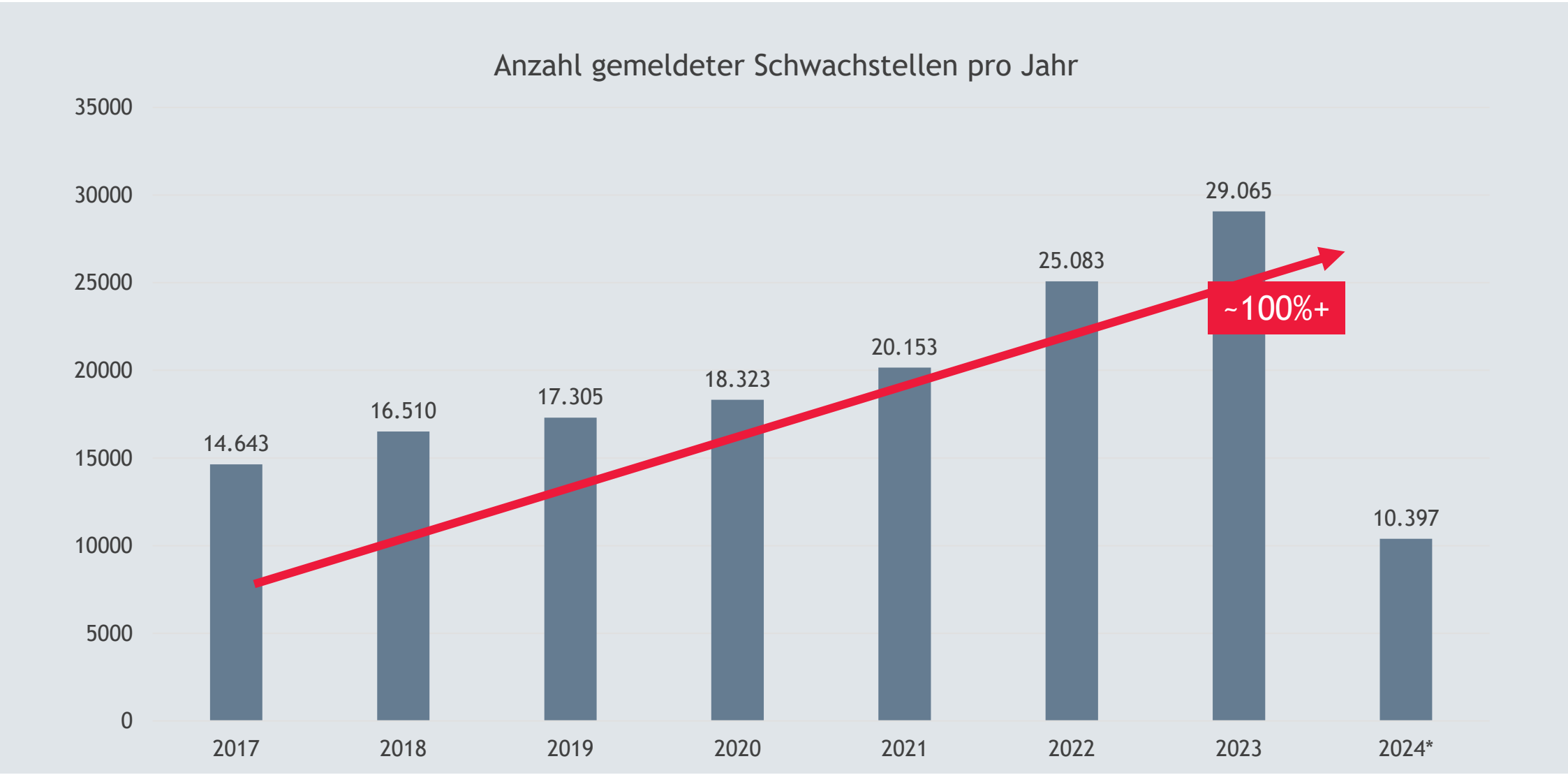
Keepass / Bitwarden
https://keepass.info/
https://bitwarden.com/

TECHNISCHE IT-SECURITY

Created by AI (DALL-E 3)

SCHWACHSTELLEN IN SOFTWARE

Technische IT-Security



* laufendes Jahr
https://www.cvedetails.com/browse-by-date.php

STAND DER TECHNIK BEACHTEN!

Technische IT-Security

Empfehlungen!

- Aktuelle Sicherheitshardware und -software verwenden (z.B. Firewalls, Spam-Filter)!
- Ausführbare Inhalte (Makros) in Dateien blockieren (.pdf, .docm, .xlsm, .bat, .ps1, …)
- Einschränkung der externen Angriffsfläche (VPN, IP- / Geolocation-Filter, alte Services deaktivieren)
- Setzen Sie auf flächendeckende Zwei-Faktor-Authentifizierung

Makro Security

https://learn.microsoft.com/de-de/microsoft-365/security/intelligence/macro-malware?view=o365-worldwide

IT-SYSTEME LAUFEND AKTUELL HALTEN

Technische IT-Security

Empfehlungen!

- Führen Sie einen Update- und Patch-Management-Prozess ein!
- Informieren Sie sich laufend zu neuen Sicherheitslücken und Angriffen!
- Führen Sie regelmäßig (zumindest jährlich) Schwachstellenscans durch!

CERT AT
https://cert.at/

Microsoft Security Advisory
https://learn.microsoft.com/en-us/security-updates/

DANKE FÜR IHRE AUFMERKSAMKEIT!

Barbara Fahringer-Postl
Partnerin

+43 5 70 375 - 1381
+43 664 60 375 - 1381
barbara.fahringer-postl@bdo.at

Jasmin Preuer
Managerin

+43 5 70 375 - 4825
+43 664 60 375 - 4825
jasmin.preuer@bdo.at

Mario Neubauer
Senior Manager

+43 5 70 375 – 4253
+43 664 60 375 - 4253
mario.neubauer@bdo.at


WE SEARCH FOR
GREATNESS.
BDO