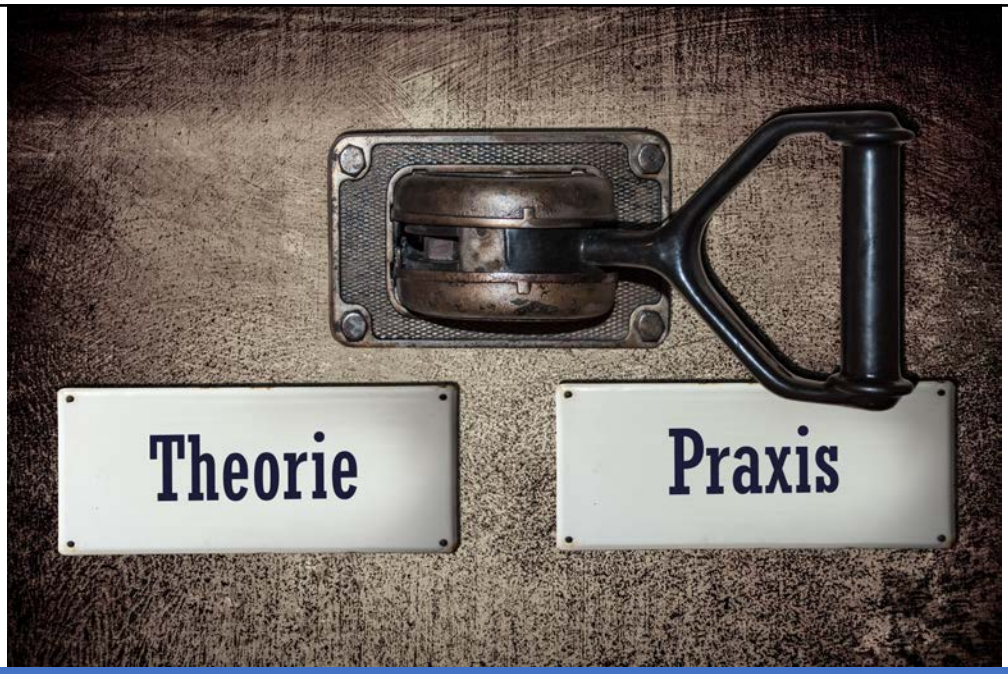
Verfasser: Gerald Kortschak

Thema: DSGVO/DSG – Maßnahmen für Buchhaltungsberufe – TEIL 2

Dipl.-Ing. Gerald Kortschak, BSc, CMC

- Selbständig seit 2001
- IT-Systeme & Unternehmensberatung
- Zertifizierungen: CMC, CDISE, CDC, geprüfter Datenschutzexperte
- IT-Security ExpertGroup, Spr. Ö
- FH-Lektor: FH St. Pölten
- DSGVO-Vorträge & Workshops
- DSGVO-Begleitung (0-2400 MA)

www.sevian7.com/ www.dsgvo2018.at / www.digital-coaches.at / derschenner.at



Fakten für BH

✓ Sie sind Verantwortliche

✓ Sie sind Verarbeiter

Die DSGVO gilt für alle EU-Mitgliedstaaten. Alle Unternehmen sind von den umfangreichen Neuerungen betroffen – von Ein-Personen-Unternehmen bis zum Großbetrieb.

www.sevian7.com/ www.dsgvo2018.at / www.digital-coaches.at / derschenner.at

Pflichten für Buchhaltungsberufe

WEGFALL des Datenverarbeitungsregisters!!!

- Verfahrensverzeichnis als Verantwortliche
- Verarbeitervertrag mit Auftraggeber (Vollmacht reicht nicht)
- Verarbeiter - Verfahrensverzeichnis
- geeignete TOMs

Pflichten für Buchhaltungsberufe

- Datenschutzfolgeabschätzung
- Warnpflicht bei Weisungen die gegen Datenschutzrecht verstoßen!
- Belehrung der Mitarbeiter zu Datengeheimnis
- Verarbeitung nur auf Weisung Auftraggeber (außer gesetzliche Verpflichtung)

Folgen

- **für Einsetzung von Sub-Auftragsverarbeitern ist Zustimmung des Verantwortlichen erforderlich (theoretisch auch Cloud-Dienste)**
- **zwischen Auftragsverarbeiter und Sub- Auftragsverarbeiter ist ein Vertrag abzuschließen**
- **Vereinbarung, dass Auftragsverarbeiter nach Beendigung seiner Tätigkeit alle personenbezogenen Daten löscht oder zurückgibt**

Schriftliche Vereinbarungen mit Auftragsverarbeitern mit den in Artikel 28 geforderten Inhalten

- Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen (inkl Informationspflicht bei abweichender rechtlicher Verpflichtung)
- Vertraulichkeitserklärung/Verschwiegenheitspflicht des Personals
- Sicherstellung von technischen und organisatorischen Datenschutzmaßnahmen
- Zustimmungsrechte oder Informationspflicht mit Einspruchsrecht bei Subauftragsverarbeitern und Überbindung aller eigenen Verpflichtungen
- Verpflichtung zur Unterstützung des Verantwortlichen hinsichtlich Datensicherheit und Betroffenenrechte
- Pflicht zur Datenlöschung/-rückgabe nach Beendigung der Tätigkeit
- Nachweis- und Inspektionsrechte

Vereinbarung mit Auftragsverarbeiter

- Vollmacht des Klienten ersetzt die Vereinbarung nicht

Verfahrensverzeichnis

- Stammdatenblatt
- Data-Breach-Notification
- Logbuch
- Antworttexte Begehren
- TOMs
- Verträge

www.sevian7.com/ www.dsgvo2018.at / www.digital-coaches.at / derschenner.at

Prüf-Fragen / Die 8 Ws!

WER	• (wer als Verantwortlicher benannt wird)
WAS	• (welche Daten-Kategorien erfasst werden)
WO	• (Daten gespeichert und verarbeitet werden – betroffene Systeme,)
WARUM	• (was ist der Rechtsgrund der zur Anwendung kommt)
WOZU	• (Zweck der jeweiligen Datenverarbeitung)
WOHIN	• (wenn Daten weitergegeben werden - an wen werden die Daten übergeben, auch ob innerhalb der EU oder Drittland)
WIE LANGE	• (werden Daten gespeichert – welche Löschfristen kommen zur Anwendung)
WIE SICHER	• (welche Datensicherheitsmaßnahmen werden ergriffen).

Erfassungshilfe

Verarbeiter

Dritte

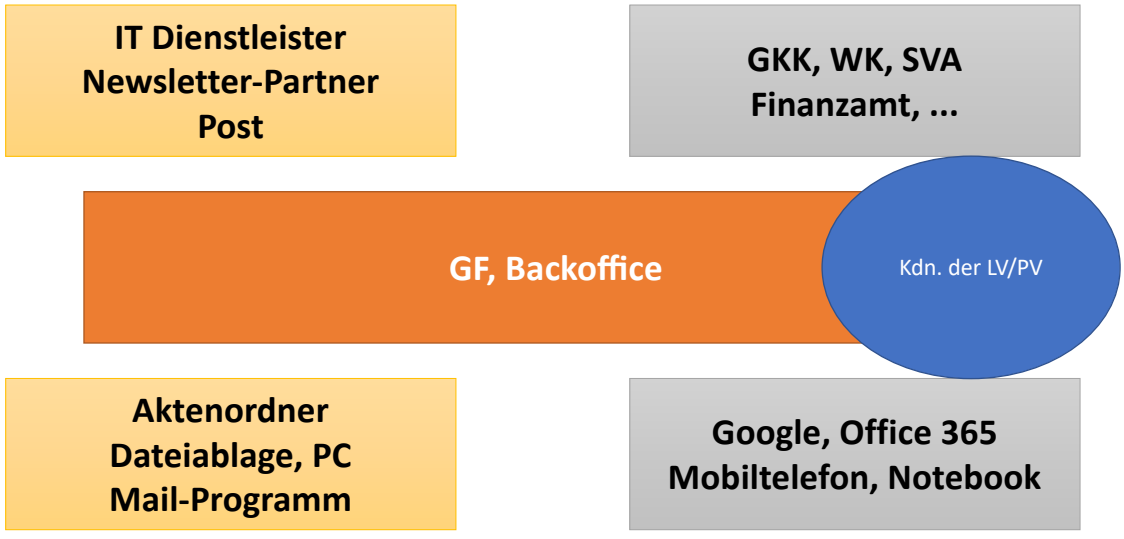
Mein Unternehmen

für wen verarbeite ich?

Systeme intern

Systeme extern oder extern nutzbar

Erfassungshilfe



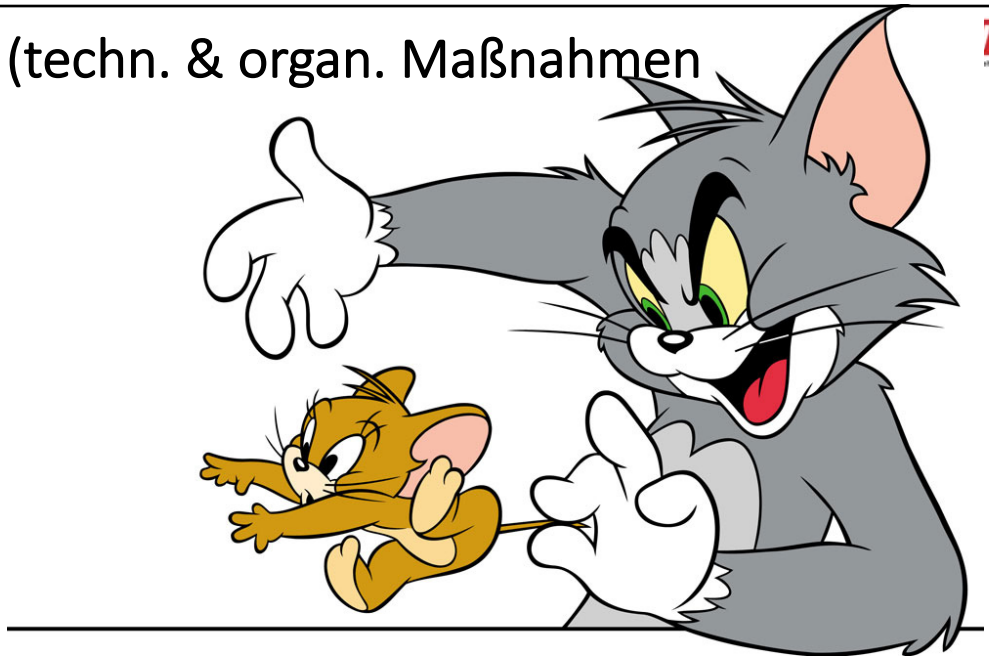
personenbezogene Daten Beispiele

Allgemeine personenbezogene Daten	besondere personenbezogene Daten (Art 9)
Vorname, Nachname, Anschrift	Sozialversicherungsnummer
KFZ-Kennzeichen	AUVA-Meldungen
Geburtsdatum, Geschlecht	Gesundheitsdaten, Religion
	Exekutionsdaten / Straftaten (Art. 10)

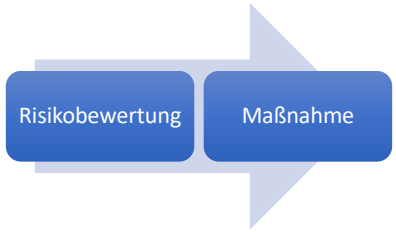
Einwilligung vs Information

Informationspflicht	Einwilligung
Daten der Vertragserfüllung	Foto auf Website / Print
Erfüllung gesetzlicher Regelungen	Newsletter
Berechtigtes Interesse	Verlängerte Aufbewahrungsfristen
Aufbewahrung nach gesetzlicher Frist	Autom. Verarbeitung Daten von Kindern (< 14 Jahre)
Lohnverrechnung => Mitarbeiterdaten	

TOMs (techn. & organ. Maßnahmen



Datensicherheitsmaßnahmen (§54 DSG [für Behörden])



STAND DER TECHNIK

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übertragungskontrolle
- Eingabekontrolle
- Transportkontrolle
- Wiederherstellung
- stabiles System: Zuverlässigkeit / Datenintegrität

"geeignete" TOM – techn. und org. Maßnahmen

Unter Berücksichtigung

- des Stands der Technik,
- der Implementierungskosten und
- der Art,
- des Umfangs,
- der Umstände und
- der Zwecke der Verarbeitung sowie der
- unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

organisatorische Maßnahmen

Mitarbeiter

- Geheimhaltungsvereinbarung
- Verbot privater Nutzung
- kein WhatsApp

Dokumente

- versperrbare Kästen
- Dritten keine Einsicht geben
- Aktenvernichter

organisatorische Maßnahmen

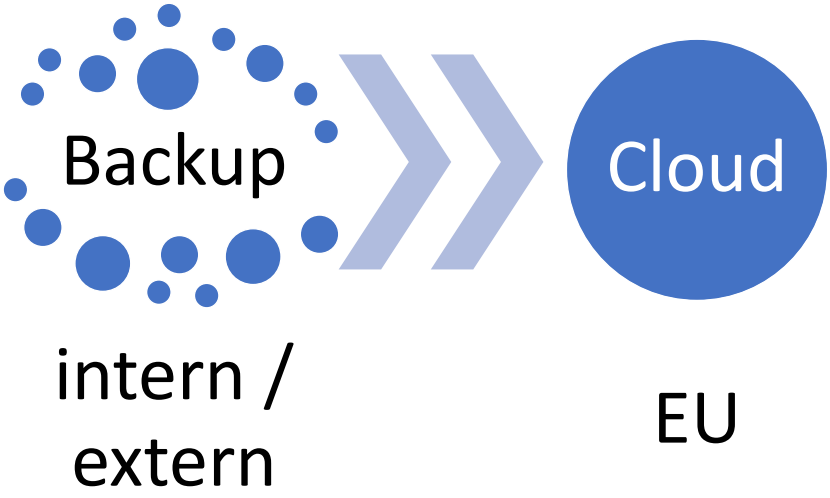
löschen

- Speicher sicher entsorgen
- Backupzyklus (Überschreiben)
- keine Wiedereinspielung

Regelwerk

- Post – Verarbeitervertrag
- Website – Datenschutzerklärung
- Website - Informationspflichten

Technische Maßnahmen



intern / extern

EU

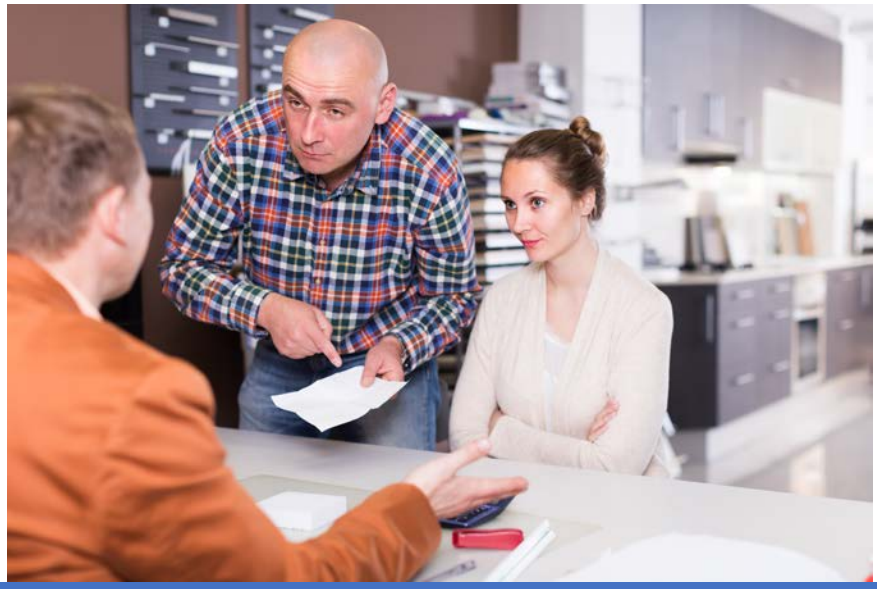
Technische Maßnahmen

verschlüsseln vs. offen

Vereinbarung!

Passwortschutz

Rechte der Betroffenen



DSGVO – Rechte der betroffenen Personen

- Auskunftsrecht (Art. 15)
- Berichtigung (Art. 16)
- Löschung (Art. 17) – Recht auf Vergessenwerden
- Widerspruch (Art. 21)
- Einschränkung der Verarbeitung (Art. 18)
- Recht auf Datenübertragbarkeit (Art. 20)

Recht auf Löschung

Dem Verlangen ist grundsätzlich Folge zu leisten, es sei denn spezielle Ablehnungsgründe liegen vor. Der wichtigste Ablehnungsgrund sind die gesetzlichen Aufbewahrungsfristen.

Daten, die nur aufgrund einer Einwilligung länger als die gesetzlichen Fristen gespeichert wurden, sind auf Verlangen des Betroffenen umgehend zu löschen. Im Verarbeitungsverzeichnis sind die Aufbewahrungsfristen, wenn möglich, ebenfalls anzuführen.

Aufbewahrungsfristen (Beispiele)

Rechnungswesen, Steuer- und Zollrecht:

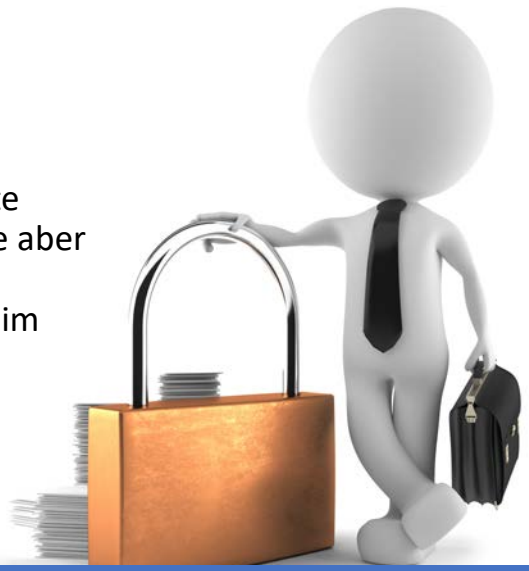
1. Steuerrechtliche Aufbewahrungspflicht nach § 132 Abs 1 BAO: 7 Jahre darüberhinausgehend solange sie für die Abgabenbehörde in einem anhängigen Verfahren von Bedeutung sind)
2. Unternehmensrechtliche Aufbewahrungspflicht nach §§ 190, 212 UGB: 7 Jahre
3. Umsatzsteuerrechtliche Aufbewahrungspflichten nach § 18 Abs 10 UStG (Spezialbestimmung für Grundstücke): 22 Jahre
4. Umsatzsteuerrechtliche Aufbewahrungspflicht nach § 18 Abs 2 3. Unterabsatz: 7 Jahre
5. Aufzeichnungen nach § 23 Abs. 2 Zollrechts-Durchführungsgesetz: 5 Jahre

Recht auf Datenübertragbarkeit

- **Beispiel:** Ein Kunde möchte den Buchhalter wechseln und seine Daten mitnehmen. Um die Pflicht zu erfüllen reicht es aus, ihm die Daten in einem gängigen Format (Word, Excel,… elektronisch (E-Mail, USB-Stick,…) zukommen zu lassen.
- PDFs sollten hierfür nicht verwendet werden
- Voraussetzung:
  - automatisierte Verarbeitung
  - gilt nicht für Papier

Datenschutzbeauftrager

- Es ist zum jetzigen Stand nicht davon auszugehen, dass Personalverrechner standardmäßig Datenschutzbeauftragte benötigen werden. Im Einzelfall könnte aber dennoch die Bestellung eines solchen notwendig werden (zB Spezialisierung im Unternehmen,…).



- Sie müssen Risikoanalysen der Datenanwendungen durchführen und den Verantwortlichen bei Erfüllung seiner Pflichten nach der DSGVO unterstützen.

AUSSER:

- Wenn bestehende Verarbeitungsvorgänge vor dem 25. Mai 2018 bereits von der Datenschutzbehörde geprüft worden sind (etwa im Rahmen einer Vorabkontrolle nach dem Datenschutzgesetz 2000) und die Verarbeitungsvorgänge sich seit dieser Prüfung nicht geändert haben.

DSFA - Umfang

- laufend, kein einmaliger Prozess
- Bewertung und Beschreibung der Vorgänge
- Risikobewertung
- Abhilfemaßnahmen
- Erneute Risikobewertung unter Berücksichtigung getroffener Maßnahmen

https://www.privacyofficers.at/Privacyofficers_DSFA-Umsetzung_DSGVO_v1.0.pdf
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-datenschutz-grundverordnung-datenschutz-folgenabschaetzu.html

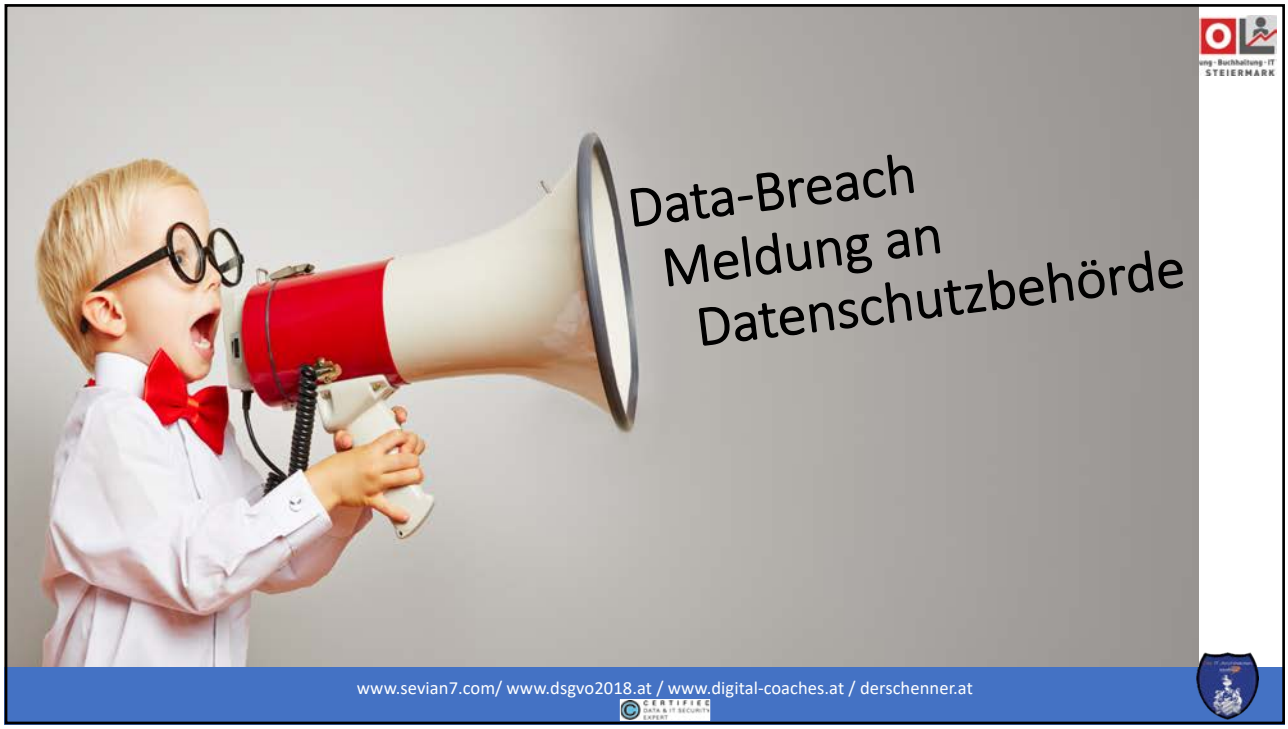
Auswirkungen - Beispiel

	Vernachlässigbar	Eingeschränkt	Signifikant	Maximal
Beispiele für physische Auswirkungen	Vorübergehende Kopfschmerzen	Leichte körperliche Beschwerden (z. B. leichte Krankheiten aufgrund unberücksichtigter medizinischer Kontraindikationen)	Veränderung der körperlichen Unversehrtheit z. B. nach einem Angriff, einem Unfall zu Hause oder auf der Arbeit etc.	Tod (z. B. Mord, Selbstmord, tödlicher Unfall)
Beispiele für materielle Auswirkungen	Empfang unerwünschter E-Mails (z. B. Spam)	Unrichtiges oder unangebrachtes Profiling	Verbot der Führung von Bankkonten	Erhebliche Schulden
Beispiele für moralische Auswirkungen	Angst, die Kontrolle über die eigenen Daten zu verlieren	Einschüchterung in sozialen Netzwerken	Cyber-Mobbing und Belästigung	Strafrechtliche Verurteilung

Tabelle 3: Beispiele für die Einschätzung der Auswirkungen gemäß Bitkom-Leitfaden für "Risk Assessment & Datenschutz-Folgenabschätzung" *[3, p. 51f.]*

Behandlung von Risiko / Restrisiko?

- **Eliminieren**
  - Systemwechsel
  - Prozessänderung
- **Reduzieren**
  - Abwehrmaßnahmen
  - Gegenmaßnahmen (Firewall, IPS, IDS, ...)
- **Akzeptieren**
  - "is so"
  - Entscheidung der GF
- **Transferieren**
  - Risiko abwälzen (Versicherung)
  - Risiko auslagern (Rechenzentrum)



Meldung von Datenschutzverletzungen

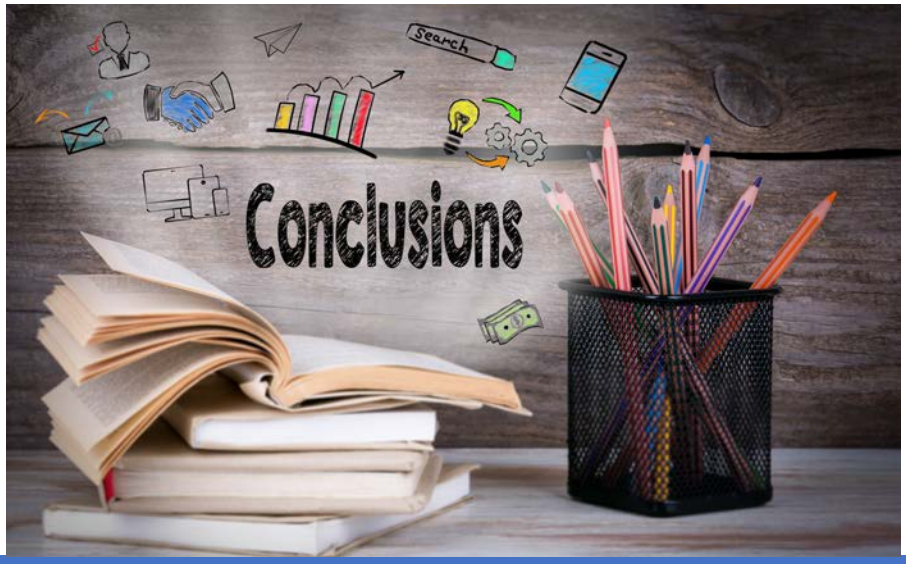
- 72h nach Entdecken

Inhalte dieser Meldung sind:

- Beischreibung des Vorfalles
- Auflistung der betroffenen Daten
- Beschreibung der Auswirkung auf die betroffenen Daten
- Beschreibung der geplanten/eingeleiteten Maßnahmen zur Beendigung des Vorfalls und der Wiederherstellung der Daten
- Beschreibung der Maßnahmen zur Minimierung des Schadens
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen

www.sevian7.com/ www.dsgvo2018.at / www.digital-coaches.at / derschenner.at

FAZIT



Checkliste zur DSGVO

- Feststellung IST-Zustand
- Bestellung Datenschutzbeauftragter ja/nein
- Dokumentation der Verarbeitungsvorgänge
- Datenschutz-Folgenabschätzung
- Meldung von Verstößen
- Verträge mit Auftragsverarbeitern
- Formulare prüfen und anpassen
- Informationspflichten / Betroffenenrechte
- Sicherheitsmaßnahmen
- Mitarbeiterschulungen

WK hilft

Förderung für:
WIFI-Kurse
Beratungen (Fokus C) von Certified Data & IT Security Expert
50% bis max. € 1.000,--
Potential-Analyse zu 100% gefördert (Certified Digital Consultant)

Online Hilfestellungen und Tipps:

- **wko.at/datenschutz**
- **https://www.wko.at/branchen/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/buchhaltung/leitfaden-dsgvo-bilanz-buchhalter-personalverrechner.html**

Mit Rat und Tat:
Rechtsservice WK-STMK
0316 / 601 - 601

Ihre Fachgruppe

Die IT-Architekten

DER SCHENNER Consulting & Training

sevian e pluribus unum >> www.sevian7.com

Ing. DI(FH) Harald SCHENNER, CMC und DI Gerald Kortschak, BSc, CMC
www.derSchenner.at | www.sevian7.com
www.dsgvo2018.at

CERTIFIED DATA & IT SECURITY EXPERT

CERTIFIED DIGITAL CONSULTANT

Geprüfte Datenschutz-Experten

www.sevian7.com/ www.dsgvo2018.at / www.digital-coaches.at / derschenner.at

Wir weisen ausdrücklich darauf hin, dass es sich bei den vorliegenden Unterlagen um ein unentgeltliches Service der Autoren handelt und die Informationen keine Unternehmensberatung darstellen. Jegliche Haftung für die Aktualität, Richtigkeit und Vollständigkeit der dargestellten Informationen wird ausgeschlossen.

Die für Schulen und Hochschulen vorgesehene freie Werknutzung „Vervielfältigung zum eigenen Schulgebrauch“ gilt für dieses Werk nicht, weil es seiner Beschaffenheit und Bezeichnung nach nicht zum Unterrichtsgebrauch bestimmt ist.