NIEDERER KRAFT FREY

ITSENSE

Datensicherheit und Recht – wer trägt die Verantwortung?

Clara-Ann Gordon

Aarau, 21. September 2023

Inhalt

1. Einleitende Bemerkungen
2. Kurzübersicht neues Datenschutzrecht
3. Fokus: Datensicherheit - neue Bestimmungen
4. IAM - eine wichtige Datensicherheitsmassnahme
5. Neu: Meldepflicht bei Datensicherheitsverletzungen
6. Verantwortlicher und Datenbearbeiter
7. Herausforderungen bei der Compliance
8. Bussen – Wer haftet?
9. Fazit

Einleitende Bemerkungen

Einleitende Bemerkungen

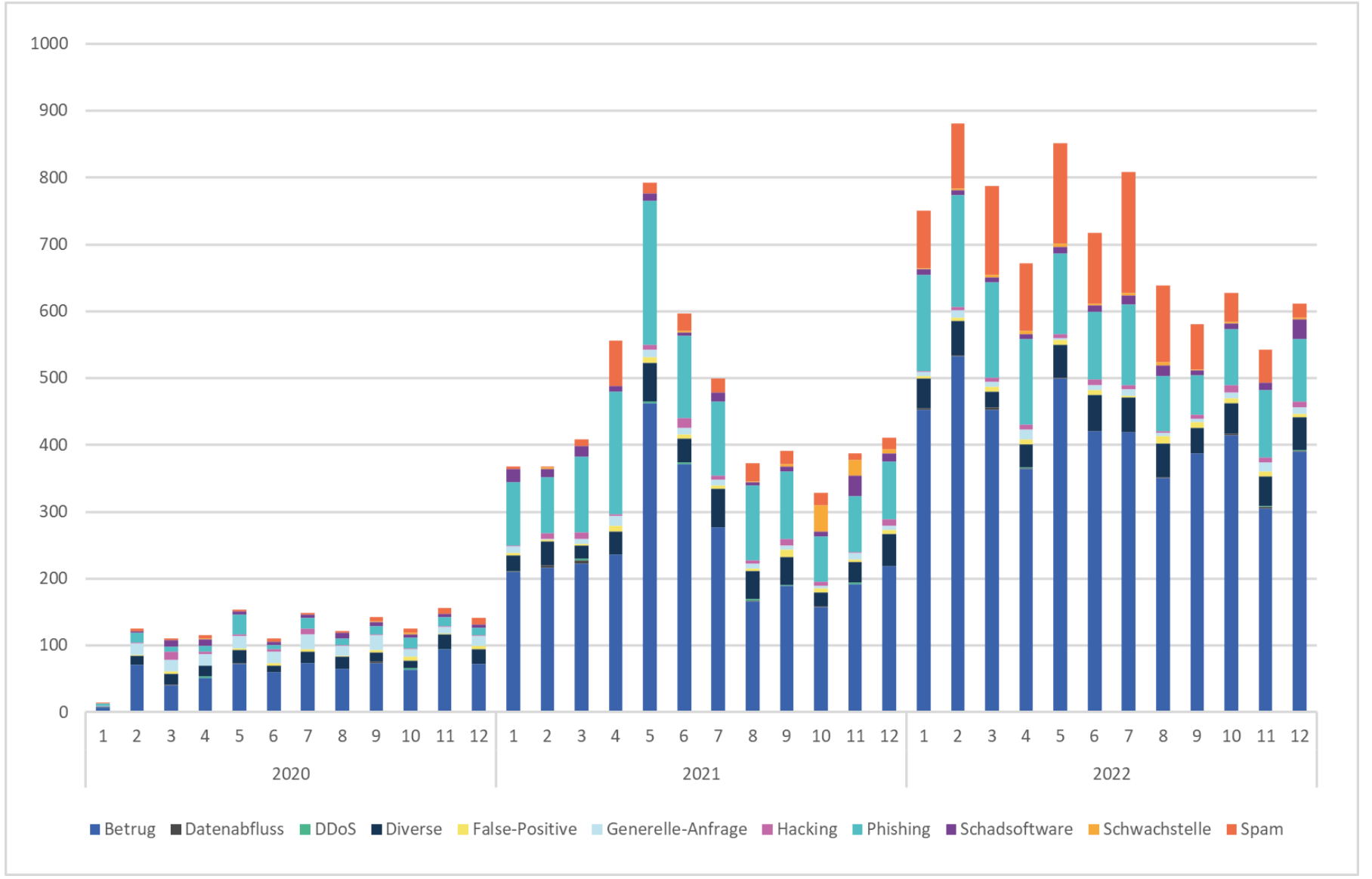
- Datenschutz wird immer wichtiger:
  - 60% nutzen eine Cloud, um Daten und Fotos zu sichern

    2022: 34'527 Meldungen von Bevölkerung und Unternehmen zu Cybervorfällen beim nationalen Zentrum für Cybersicherheit
- Potenziell weitreichende Konsequenzen von Cyber-Angriffen:

→ Arbeitsausfälle und -verzögerungen bis hin zu Schadenersatzklagen

- Neues Datenschutzrecht seit dem 1. September 2023 in Kraft: strengere Bestimmungen in Bezug auf die Datensicherheit mit Bussenfolge!

Verdreifachung der Cyber-Angriffe in CH seit 2020



Quelle: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-95071.html

Cyber-Angriffe 2022

Cyber-Angriffe auf Schweizer Unternehmen um 61% gestiegen seit 2021

Country	Industry	Rank	Avg. Weekly Attacks Per Organization in 2022	Change from 2021
Switzerland	Manufacturing	1	752	-24 %
Switzerland	Finance/Banking	2	623	+120 %
Switzerland	Government/Military	3	569	+52 %
Switzerland	Healthcare	4	455	+78 %
Switzerland	Communications	5	397	+200 %

Quelle: https://www.safety-security.ch/cyberangriffe-schweiz-2022-um-61-prozent/

NKF

Schweiz mit über 13'000 Cyber-Angriffen in 2023

Öffentlich bekannte Cyber-Attacken in 2023 in der Schweiz z.B.:

NZZ

BERNINA

SBB CFF FFS

Erziehungsdepartement des Kantons Basel-Stadt

ch media

- National Cyber Security Center (NCSC) berichtet über 13'000 Cyber-Angriffe auf Schweizer Unternehmen
- Dies ist mehr als gesamthaft im Jahre 2020

NKF

Quelle: https://www.iamexpat.ch/expat-info/swiss-expat-news/switzerland-hit-over-13000-cyber-attacks-2023-so-far

Hauptgrund: menschliches Versagen und mangelnde Datensicherheit

Kurzübersicht über das neue Datenschutzrecht

Allgemeine Bestimmungen des neuen DSG

- Das totalrevidierte DSG gilt seit dem **1. September 2023** – keine Übergangsfrist
- Geltungsbereich: Ist Ihr Unternehmen betroffen?

  Bearbeitung von Personendaten in der Schweiz oder ausserhalb der Schweiz aber mit Wirkung in der Schweiz

  → neu: extraterritoriale Wirkung
- Schutzziele: Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit
- Schutzbedarfsanalyse → je höher der Schutzbedarf, desto strenger sind die Anforderungen an die Massnahmen
- Viele Regelungen der DSGVO werden übernommen, es gibt aber auch ein paar Unterschiede (sog. "Swiss Finishes")

Was sind die wichtigsten Änderungen im neuen DSG?

- **Ausweitung der Informationspflicht** → gilt neu für jede Beschaffung von Personendaten
- Personendaten juristischer Personen sind nicht länger erfasst
- Die Grundsätze "Privacy by Design" und "Privacy by Default" werden eingeführt
- Genetische und biometrische Daten werden explizit als besonders schützenswert qualifiziert
- Hohes Risiko für die Persönlichkeit / Grundrechte bei einer Datenbearbeitung? → DSFAs (Datenschutz-Folgenabschätzungen) müssen durchgeführt werden
- Obligatorisches Verzeichnis der Bearbeitungstätigkeiten → **Ausnahme für KMU**, bei deren Datenverarbeitung nur ein geringes Risiko von Datenschutzverletzungen besteht
- Schnelle **Meldung an den EDÖB**, wenn die Datensicherheit verletzt wurde
- "Profiling" wurde in das Gesetz mitaufgenommen (entspricht aber weitgehend dem bisherigen "Persönlichkeitsprofil")

Fokus: Datensicherheit

Allgemeine Bestimmungen DSV

- Allgemeine Massnahmen zur Gewährung der Datensicherheit
  - Anonymisierung, Pseudonymisierung und Verschlüsselung von Personendaten
  - Verfahren zur Identifikation, Bewertung und Evaluierung der Risiken und Überprüfung der Angemessenheit der getroffenen Massnahmen
  - Schulung und Beratung

- Risikobasierter Ansatz, d.h. keine starren Mindestanforderungen, sondern es muss im Einzelfall der Schutzbedarf festgelegt und Massnahmen anhand des Risikos definiert werden

→ DSV ist inhaltlich ähnlich, aber weniger detailliert als die DSGVO (dafür technologieneutral)

TOMs – Allgemeine Grundsätze (I)

- Leitplanke (Art. 8 Abs. 1 und 2 DSG): Der Verantwortliche **und** der Auftragsbearbeiter gewährleisten durch geeignete technische **und** organisatorische Massnahme eine dem Risiko angemessene Datensicherheit. Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit **zu vermeiden**
- Technische Massnahmen sind Massnahmen, die technisch implementiert werden (z.B. ein Passwortschutz, Zugangssperren oder eine Transportverschlüsselung)
- Organisatorische Massnahmen setzen beim Menschen an (z.B. durch ein Vieraugenprinzip, Kontrollen oder Schulungen)

→ Technische Massnahmen gelten tendenziell als stärker.

- Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg zu überprüfen und nötigenfalls anzupassen (Art. 1 Abs. 5 DSV). **Je höher das Risiko, desto häufiger ist eine Überprüfung notwendig.**

→ In der DSGVO wird ein Verfahren zur regelmässigen Überprüfung verlangt.

TOMs – Allgemeine Grundsätze (II)

- Massnahmen müssen dem Schutzbedarf entsprechen (vgl. Ziele Art. 2 revDSV)

- Kriterien zur Festlegung (Art. 1 Abs. 4 DSV):
  - Stand der Technik (lit. a): es ist ausreichend Massnahmen zu haben, die sich bereits bewährt haben;
  - Implementierungskosten (lit. b): "Kosten" ist weit zu verstehen und meint (personelle, finanzielle und zeitliche) Ressourcen

- Strafnorm: mit Busse bis zu 250'000 wird bestraft, wer die Mindestanforderungen an die Datensicherheit vorsätzlich nicht einhält (Art. 61 lit. c DSG)

- In der DSGVO wird bezüglich TOMs dasselbe Datenschutzniveau verlangt

TOMs – Vertraulichkeit

- **Zugriffskontrolle**: die Zugriffsberechtigungen und die Art wie auch der Umfang des Zugriffs wird bestimmt
  - z.B. individuelle Vergabe von Nutzungsrechten, Passwortabfrage nach Inaktivität
- **Zugangskontrolle**: kein Zugang für unbefugte Personen zu den Räumlichkeiten bzw. Anlagen
  - z.B. ständig verschlossene Türen/Fenster, Codeschlösser an Türen, Sicherheitspersonal
- **Benutzerkontrolle**: die Daten sollen nicht in unbefugter Weise benutzt oder weitergegeben werden
  - z.B. regelmässige Kontrollen von Berechtigungen (Sperrung bei Personalwechsel), "Spyware" (insoweit zulässig), Virenschutz/Firewall

TOMs – Verfügbarkeit und Integrität (I)

- **Datenträgerkontrolle**: unbefugten Personen das Lesen, Kopieren, Verändern, Verschieben, Löschen oder Vernichten von Datenträgern verunmöglichen; verhindern, dass Personendaten unkontrolliert auf Datenträger übertragen werden können
  - z.B. Verschlüsselung oder Vernichtung von Daten, gesicherte Speicherung von Datenträgern
- **Speicherkontrolle**: verunmöglichen, dass unbefugte Personen auf den Inhalt des Datenspeichers Zugriff haben, diesen einsehen, verändern oder löschen können
  - z.B. differenzierte Zugriffsberechtigung für Daten, Protokollierung von Zugriffen
- **Transportkontrolle**: designierter Empfänger muss Daten in ihrer ursprünglichen Form erhalten und keine Dritte sollen die Daten unbefugt abfangen können
  - z.B. Verschlüsselung, sichere Transportbehälter bei physischen Transporten

TOMs – Verfügbarkeit und Integrität (II)

- **Data Recovery**: Möglichkeit der Wiederherstellung der Verfügbarkeit der Daten und des Zugangs zu den Daten nach einem Zwischenfall
  - z.B. Backup-Konzept, Sicherungs- und Wiederherstellungssysteme (wie RAID)

- **Zuverlässigkeit**: Gewährleistung der Stabilität der Systeme; Fehlfunktion soll das System selber melden; gespeicherte Personendaten sollen nicht durch Fehlfunktionen des Systems beschädigt werden
  - z.B. VPN-Tunnel, Firewall, Erkennung von Feuer und Rauch

- **Systemsicherheit**: Prozess für die Aktualisierung von Systemen bzw. proaktive Behebung von Schwachstellen
  - z.B. Aktivierung von verfügbaren Software- und Firmware-Updates

TOMs – Nachvollziehbarkeit

- **Eingabekontrolle**: nachträglich muss überprüft werden können, welche Daten zu welcher Zeit von welcher Person eingegeben oder verändert wurden
  - z.B. Protokollierung
- **Bekanntgabekontrolle**: Identifizierung von Datenempfänger
  - z.B. Protokollierung
- **Erkennung/Beseitigung**: reaktive Massnahme, dass Verletzungen rasch erkannt werden und Massnahmen zur Minderung bzw. Beseitigung der Folgen ergriffen werden können

IAM – eine wichtige Datensicherheitsmassnahme

Was ist Identity- und Accessmanagement (IAM)?

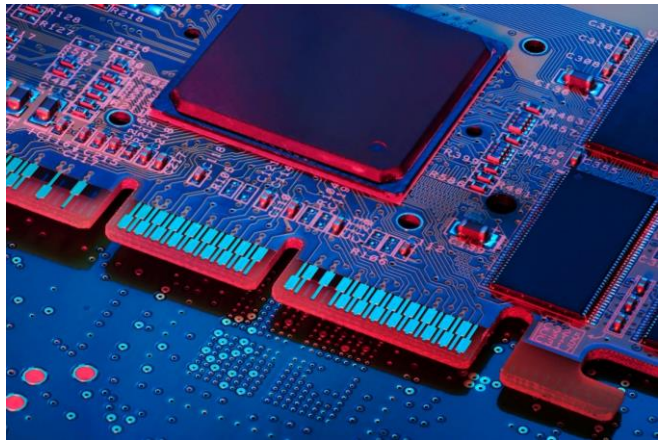
- **Identity- und Accessmanagement (kurz "IAM")** werden alle Aufgaben rund um die Verwaltung von digitalen Identitäten (Identity) und den damit verknüpften Zugriffsrechten (Access) genannt
- **Identity Management (IdM)**: Befasst sich mit Erstellung, Anpassung und Löschung von Konten im Rahmen des User Lifecycles
- **Access Management**: Verwaltung der genauen Berechtigungen der jeweiligen Accounts, inkl. Zugriff auf unstrukturierte Daten (FileServer, SharePoint, etc.)

Datensicherheit mit IAM

- IAM als verbindende Brücke zwischen Datenschutz und Datensicherheit sowie Nutzungskomfort
  1. Schritt: Authentifizierung des Nutzers
     - Durch Single-Sign-On (SSO): Einmalige Anmeldung bei einem Identity-Provider; Login für alle Geräte, auf denen der User berechtigt ist
     - Multi-Faktor-Authentifizierung (MFA): Verifizierung über mehrstufiges Verfahren, bspw. Anmeldung mit SMS-Code oder biometrischen Daten
  2. Schritt: Erteilung des Zugriffs
- Ausserdem: Verschiedene Benutzerprofile haben verschiedene und unterschiedlich viele Befugnisse und Zugriffe, wodurch die Daten besser geschützt sind

Beispiel für IAM Produkte – ITSENSE

- **Business-Modell:** Angebot von IAM-Lösungen für Unternehmen und Organisationen
- **Enterprise IAM (EIAM):** automatisierte zentrale Verwaltung der Identitäten und Zugriffs-berechtigungen für das gesamte Unternehmen; Berücksichtigung von Compliance, etc.
- **Customer IAM (CIAM):** Multi-Faktor-Authentisierung (MFA), Skalierung und User-Self-Management
- **Single Sign-On (SSO):** Anmeldeprozesse und Zugriffsberechtigungen für autorisierte Nutzer



Neu: Meldepflicht bei Datensicherheitsverletzungen

Meldung Datensicherheitsverletzung (I)

- Der Verantwortliche meldet dem EDÖB (und der Auftragsbearbeiter dem Verantwortlichen) so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt (Art. 24 Abs. 1 und 3 DSG)

- Eine Verletzung der Datensicherheit liegt vor, wenn Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden (Art. 5 lit. h DSG)

- Bezüglich dem hohen Risiko erfolgt eine Einzelfallbeurteilung
  - Ist eine schwere negative Folge mindestens wahrscheinlich oder eine mittelmässige negative Folge sehr wahrscheinlich, ist das Risiko hoch
  - Methodik der Risikoberechnung = Eintrittswahrscheinlichkeit x Schadenshöhe

Meldung Datensicherheitsverletzung (II)

- Der Verantwortliche muss die Verletzungen dokumentieren
- Die Dokumentation muss die mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Massnahmen enthalten (Art. 15 Abs. 4 DSV)
- Die Dokumentation ist ab dem Zeitpunkt der Meldung mindestens zwei Jahre aufzubewahren (Art. 15 Abs. 4 DSV)
- Der EDÖB arbeitet derzeit an der Entwicklung einer webbasierten Meldeoberfläche, voraussichtlich in Form eines **interaktiven Formulars**

Neue Meldeportale des EDÖB

Databreach-Portal (https://databreach.edoeb.admin.ch/)

– Verletzungen der Datensicherheit müssen mit dem Inkrafttreten des neuen Datenschutzgesetzes (DSG) ab dem 1. September 2023 dem EDÖB gemeldet werden

DPO-Portal (http://www.dpo-reg.edoeb.admin.ch/)

– Meldung von Datenschutzberaterinnen oder -beratern an den EDÖB gemäss Art. 10 Abs. 3 DSG für Private und Art. 10 Abs. 4 DSG für Bundesorgane

Datareg-Portal (https://datareg.edoeb.admin.ch/search)

– Das Register der Verzeichniseinträge der Bundesorgane → Hier können Sie sich über die Datenbearbeitungen der Bundesorgane informieren

Verantwortlicher und Datenbearbeiter

Wann bin ich Verantwortlicher?

- Abzustellen ist darauf, wie die Daten bearbeitet werden
- Entscheider ist grds. Verantwortlicher → Wer nicht Verantwortlicher sein will, darf keine Entscheidungsmacht haben
- Massgebend ist die Entscheidungsmacht über die Zwecke und die Mittel der Datenbearbeitung
- Entscheidungsmacht: Bestimmen, ob und warum die Datenbearbeitung stattfindet und was sie erreichen soll

Wann bin ich Datenbearbeiter?

- Wer Personendaten im Auftrag des Verantwortlichen bearbeitet, ist grds. Datenbearbeiter
- Datenbearbeiter ist an die Vorgaben des Verantwortlichen gebunden:

  → Zweck, Bearbeitungsmodalitäten (z.B. Ort der Datenbearbeitung)
- Die Anweisungen des Verantwortlichen an den Datenbearbeiter werden in einem Auftragsdatenbearbeitungsvertrag (ADV) festgehalten
- Ein AVV wird i.d.R. nicht individuell verhandelt, sondern es gibt ein Template vom Verantwortlichen, dass jeweils zugeschnitten auf alle seine Datenbearbeiter Anwendung finden kann

Bussen – wer haftet?

Bussen und Strafverfolgung

Strafbare Handlungen unter dem DSG werden in Art. 60 bis 63 DSG bestimmt:

- Informations-, Auskunfts- und Mitwirkungspflicht (Art. 60 DSG)
- Sorgfaltspflicht (Art. 61 DSG)
- Berufliche Schweigepflicht (Art. 62 DSG)
- Missachten einer Verfügung des EDÖB (Art. 63 DSG)

Diese Artikel haben drei gemeinsame Merkmale:

- Es geht nur um vorsätzlich begangene strafbare Handlungen
- Es werden in erster Linie natürliche Personen bestraft
- Die Höchststrafe beträgt CHF 250'000

Strafbestimmungen ausserhalb des DSG: V.a. Art. 179novies und 179decies StGB

Wer haftet? Die Führungskraft oder jeder Mitarbeiter?

- DSGVO (das Unternehmen haftet) vs. DSG (die natürliche Person haftet)
- Die Strafe wird gegen die natürliche Person, also die private Person verhängt
- Ausnahme: Bei einer Busse von nicht mehr als CHF 50'000 und einem unverhältnismässigen Ermittlungsaufwand kann anstelle der verantwortlichen Person das Unternehmen gebüsst werden (Art. 64 DSG)
- Nach der Botschaft zum DSG (BBl 2017, 7100) soll die Leitungsperson diejenige sein, die mit den Bussen-Vorschriften in den Blick genommen wird und haftet
- Einzelne ausführende Mitarbeiter, die faktisch entscheiden, könnten ggf. dennoch strafrechtlich belangt werden

Fazit

Fazit

- Erhöhte Anforderungen an die Datensicherheit, weil:
  - Zugriff durch unterschiedliche Anwender- und Nutzergruppen auf besonders schützenswerte und kritischen Daten
  - Verwendung verschiedener Endgeräte, von unterschiedlichen Lokationen zu unterschiedlichen Zeiten auf hybride IT-Infrastrukturen (Rechenzentrum, SaaS, Cloud Data Center, etc.)
  - Anwender haben traditionellen sicheren Perimeter verlassen und bewegen sich frei in der digitalisierten Welt
- Daher: zero-trust und Zugriff erst nach erfolgreicher Identifikation, Authentisierung und Autorisierung
- Bei fehlender Datensicherheit drohen persönliche Bussen beim Verantwortlichen

Vielen Dank für Ihre Aufmerksamkeit! Fragen?

Clara-Ann Gordon
clara-ann.gordon@nkf.ch
+41 58 800 84 26

Niederer Kraft Frey Ltd

Zurich: Bahnhofstrasse 53 CH-8001 Zurich T +41 58 800 80 00

Geneva: Place de l'Université 8 CH-1205 Geneva T +41 58 800 85 00 nkf.ch