VISCHER

Legal Innovation.

Ein Bericht aus der Praxis

David Rosenthal, Partner, VISCHER AG
10. Januar 2024

Was tun wir in der Juristerei?

- Wir drücken uns kompliziert und unklar aus?
- Wir machen **alles mühsamer**?
- Mir schaffen keine Wertschöpfung?

- Wir beschäftigen uns mit den **Regeln des Zusammenlebens**
- Wir lösen auf diese Weise Probleme und machen Dinge möglich
- Die Komplexität der Thematik nimmt zu (Beispiel KI)

- Wie können wir das **besser machen**?
- Wie können wir das effizienter tun?
- Wir können unsere Inhalte zugänglicher werden?

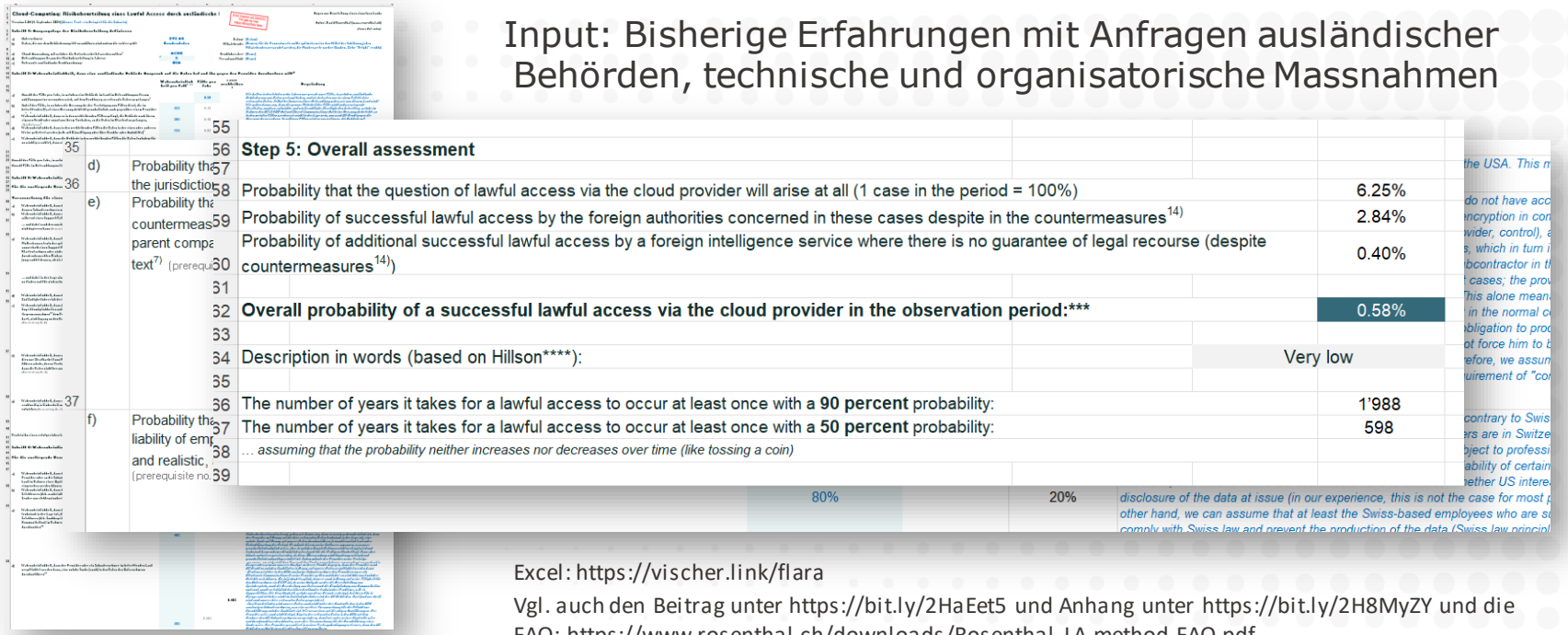
Problemlösungen strukturieren & standardisieren

- **2019: "Methode Rosenthal"**
  - Beurteilung des Risikos ausländischen Behördenzugriffe
  - Bis heute die einzige strukturierte Methode, Standard
- **2022: "Cloud Compliance & Risk Assessment" (CCRA)**
  - Für Finanzinstitute (FI) und öffentliche Organe (PS)
  - FI: Bald auch in einer Light-Version für einfachere Projekte
- **2023: Privacyscore.ch**
  - Beurteilung der Datenschutz-Compliance bzw. Maturität
- **2023: Generative AI Risk Assessment (GAIRA)**
  - Seit Januar 2024 auch als "Light" Version

Ausser CCRA-FI ist alles kostenlos erhältlich www.rosenthal.ch

VISCHER

Beurteilung ausländische Behördenzugriffe



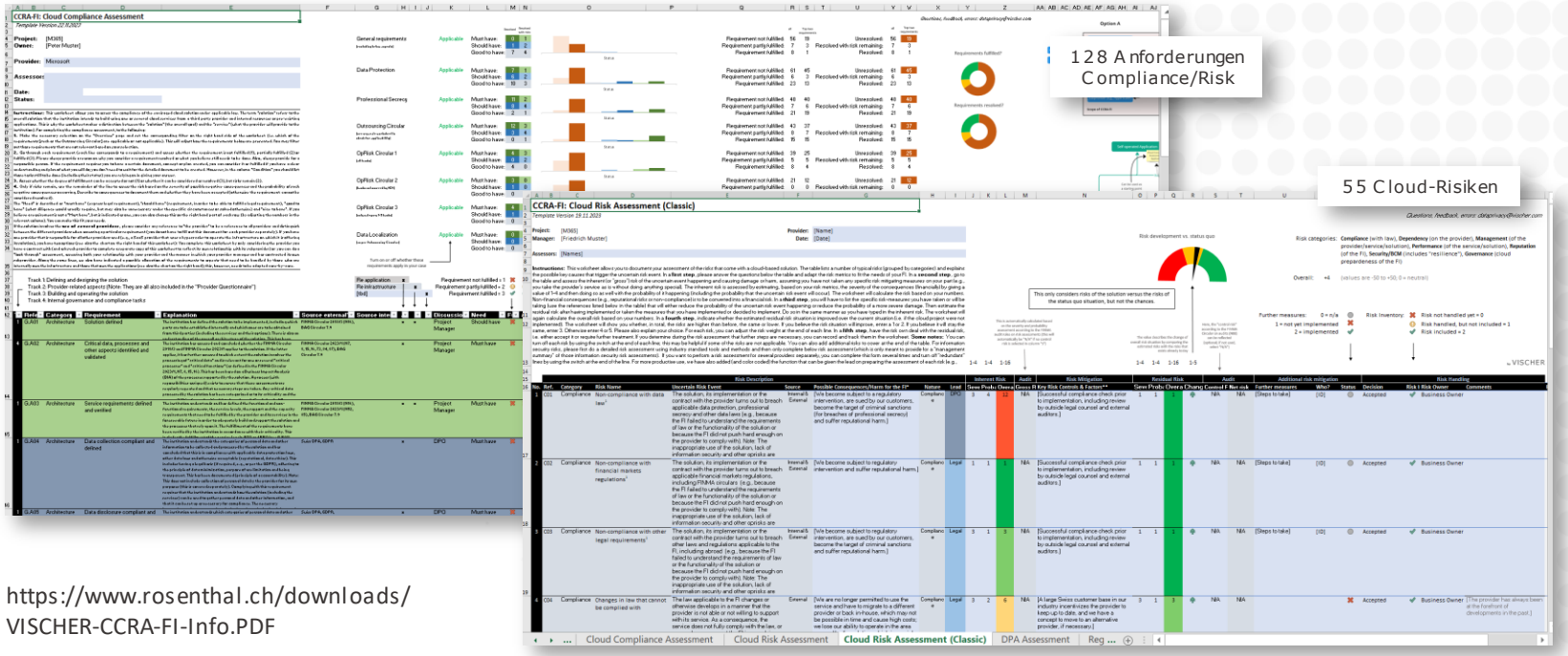
Step 5: Overall assessment		
Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)		6.25%
Probability of successful lawful access by the foreign authorities concerned in these cases despite in the countermeasures[14)]		2.84%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures[14)])		0.40%
Overall probability of a successful lawful access via the cloud provider in the observation period:* **		0.58%
Description in words (based on Hillson****):	Very low	
The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:		1'988
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:		598
… assuming that the probability neither increases nor decreases over time (like tossing a coin)		

Input: Bisherige Erfahrungen mit Anfragen ausländischer Behörden, technische und organisatorische Massnahmen

Excel: https://vischer.link/flara

Vgl. auch den Beitrag unter https://bit.ly/2HaEet5 und Anhang unter https://bit.ly/2H8MyZY und die FAQ: https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf

Cloud-Projekte in sensiblen Bereichen prüfen



https://www.rosenthal.ch/downloads/VISCHER-CCRA-FI-Info.PDF

Datenschutz-Compliance für KMU

https://www.rosenthal.ch/downloads/VISCHER-revDSG-Survival-Guide.pdf

https://privacyscore.ch

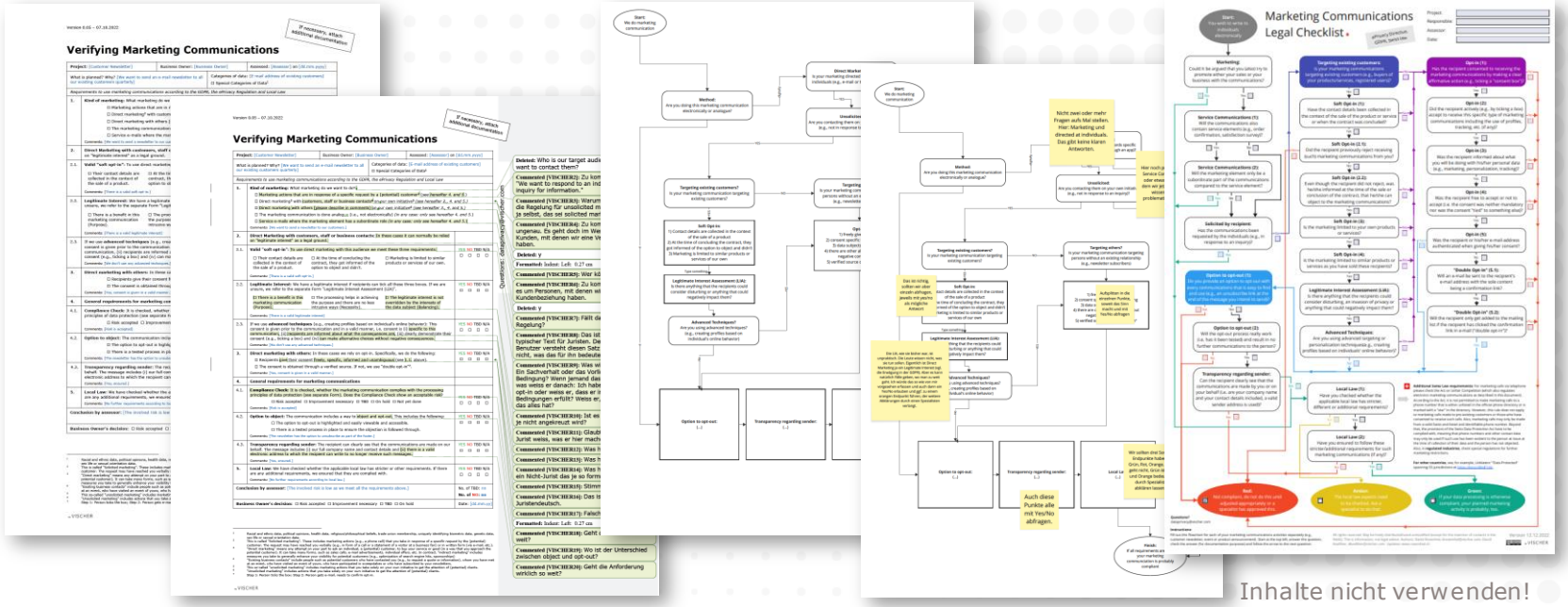
VISCHER

Tool für ein GenAI Risk Assessment (GAIRA)

- GAIRA Light & GAIRA
- Volles Risiko-Assessment inklusive Datenschutz-Folgenabschätzung (DSFA)
- Folgt hinsichtlich der Methodik dem Prinzip einer DSFA
- Separate Compliance-Checkliste
- ROAIA-Vorlage

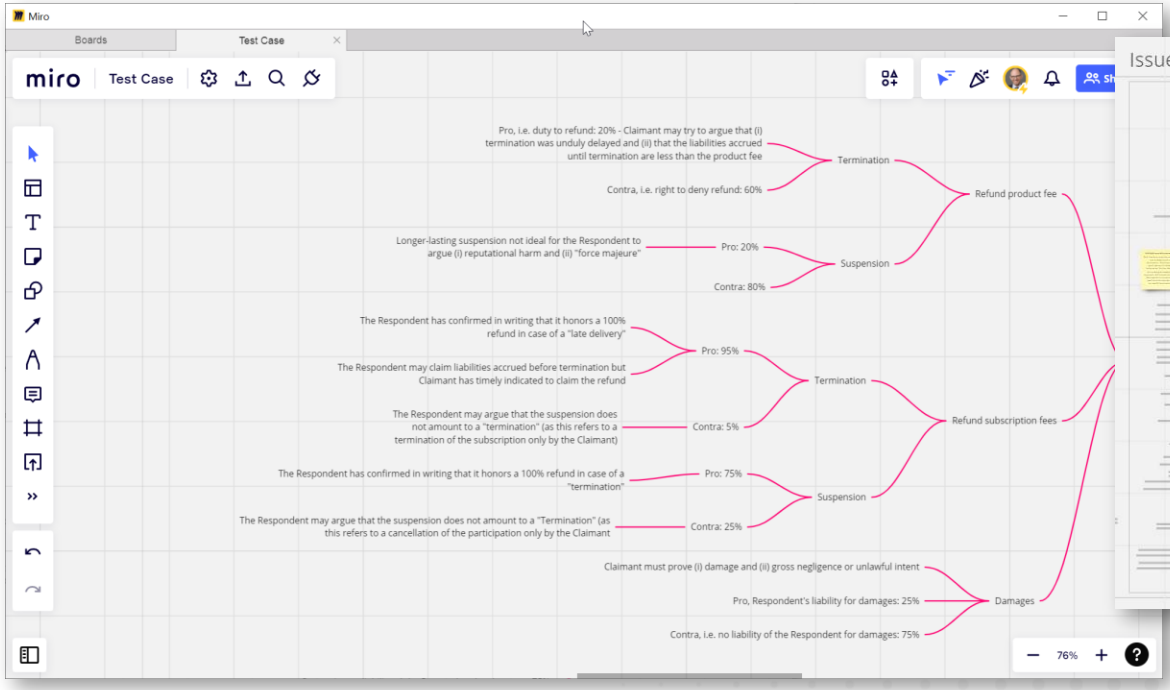
Kostenlos abrufbar unter
https://vischerlnk.com/gaira

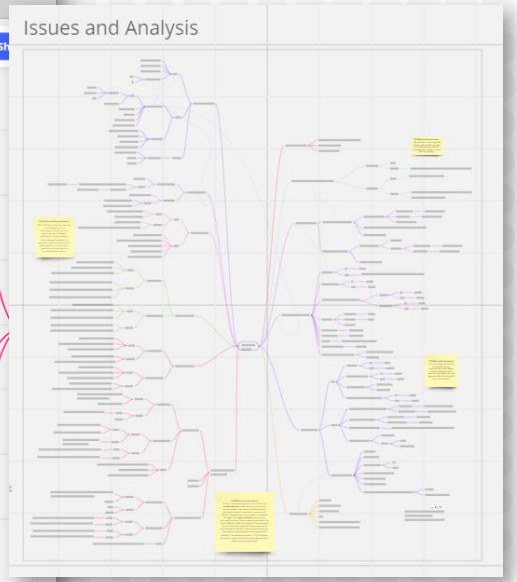
Evolution einer Checkliste



https://www.rosenthal.ch/downloads/VISCHER-Marcom-Checklist.pdf

Mindmap eines Falls





Inhalte verändert
und verfremdet

Mehr Transparenz auch in der Budgetierung

se	Task (custom specific)	Partner	Associate	Junior	Specialist	Include	Total CHF	Total EUR	Comments
1	Besprechung / Überprüfung der Liste der Datenberarbeitungen, Selektion der Datenbearbeitungen, welche einen Compliance Check brauchen	0.2	3	0	0	Yes	1'270	1'294	Liste wird durch K
1	Überprüfung Anwendbarkeit DSGVO (Liechtenstein)	0.5	2	0	0	Yes	1'085	1'105	
2	Überarbeitung Datenschutzteil IT-Richtlinie	0.2	2	0	0	Yes	890	907	
3	Überarbeitung Datenschutzteil Mitgliederverträge + Mitgliederinfos	0.5	5	0	0	Yes	2'225	2'267	Verträge bisher nic
4	~~Anpassung und Einführung Group Data Protection Policy (DE) /~~	0	2	0	0	No	-	-	Benötigt VISCHER
5	~~Überarbeitung AGBs für Weiterbildungen~~	1	4	0	0	No	-	-	
5	~~Überarbeitung Lizenzbedingungen www.time2learn.ch~~	0	0	0	0	No	-	-	Schätzung noch n
5	~~Vereinbarung zwischen Verbänden, welche www.time2learn.ch anbieten~~	0	0	0	0	No	-	-	Schätzung noch n
	Fragen und Antworten	1	5	0	0	Yes	2'550	2'598	
		0	0	0	0	Yes	-	-	
		0	0	0	0	Yes	-	-	
		0	0	0	0	Yes	-	-	
		0	0	0	0	Yes	-	-	
		0	0	0	0	Yes	-	-	
		0	0	0	0	Yes	-	-	
		0	0	0	0	Yes	-	-	
		0	0	0	0	Yes	-	-	
		0	0	0	0	Yes	-	-	
		3.4	23	0	0		8'020	8'171	

se	Task (pre-defined)	Basis	Per Item	Quantity	Adjustment	Include	Total	Total EUR	Comments
1	Creation of privacy notices (only Swiss law)	-	2'530	1	-	Yes	2'530	2'578	
2	Compliance check of processing activities (low complexity)	-	930	1	-	Yes	930	948	Requires Compliance
2	Redflag review of DPAs (excl. EU SCC)	-	730	1	-	Yes	730	744	Including reasonable
3	Redflag review of DPAs (incl. EU SCC)	-	930	1	-	Yes	930	948	Including reasonable
3	Notify EU SCC to FDPIC	1'060	-		-	Yes	1'060	1'080	
3	~~Transfer Impact Assessment (using country-specific TIA form)~~	-	3'850	1	-	No	-	-	All information is avai country-specific TIA
5	~~Creation of Data Retention Policy (no. of doc categories)~~	1'325	195	10	-	No	-	-	Requires VISCHER D excluding special rul
5	~~Customize Data Breach Policy and Process~~	1'850	-		-	No	-	-	Requires VISCHER D setup only low-comp

VISCHER Data & Privacy Budgeting Tool

Problemlösungen automatisieren

- **2023: KI-Assistent für Datenschutz-Folgenabschätzung**
  - DSFA: Beurteilung der möglichen unerwünschten negativen Folgen einer Datenbearbeitung für die betroffenen Personen
  - KI zur Formulierung von Risiken, Massnahmen und Folgen
  - Ein Projekt des Vereins Unternehmens-Datenschutz (VUD)
  - Verfügbar auf Deutsch und Englisch
  - Excel mit Makros, benötigt einen OpenAI-API-Schlüssel
- **2024: KI-Assistent für Vertragsanalyse**
  - (Vor-)Analyse von standardisierten Vertragsinhalten (z.B. TOMS, Auftragsbearbeitungsverträge)
  - KI zur Prüfung, ob die nötigen Elemente enthalten sind

DSFA mit kreativer KI-Ausfüllhilfe

Datenschutz-Folgenabschätzung (DSFA)
Version 25.9.2023 for public comment - Private CH-DSG/DSGV

Hinweis: Eine Anleitung zum Ausfüllen dieser DSFA und zur KI-gestützten Ausfüllhilfe (optional, nur in der Version des Excels mit Makros) findet sich am Ende dieses Arbeitsblatt

Unternehmen (Verantwortlicher): Musterfirma AG

Abteilung:
Verantwortlich intern:
Status der DSFA:
Name des Vorhabens:
Aktivität gemäss Bearbeitu
1. Beschreibung de
1.01 In welchem Bereic bzw. welcher Gesc
1.02 Was vorgesehen i
1.03 Welche Interesser
1.04 Welche Mittel unc
1.05 Welche Dritten an
1.06 Welche Daten bea
1.07 Wessen Daten bei
1.08 Wo überall Daten
1.09 Wann die Datenb
1.10 Weitere Besonder
2. Erforderlichkeit /
2.01 Warum die Daten Sicht der betroffer eingreifende Vorg
2.02 Warum die Datenbearbeitung datensparsam, zeitlich auf das nötige begrenzt und auch sonst verhältnismässig ist:

Zugriffen geschützt werden.
Die Datenbearbeitung ist datensparsam, da nur der Stimmabdruck, die ID der Person und Tonaufnahmen gespeichert werden, die für die Identitätsverifizierung notwendig sind. Die Datenbearbeitung ist zeitlich begrenzt, da der Stimmabdruck bei jedem Anruf neu erstellt und nicht länger als nötig gespeichert wird. Die Datenbearbeitung ist verhältnismässig, da sie zur Sicherheit der Anrufer im Call-Center beiträgt und die einzigen Daten bearbeitet werden, die dafür erforderlich sind.

4. Risiken von negativen Folgen für die betroffenen Personen, die trotz der obigen Massnahmen verbleiben

10 Risiken vorschlagen (überschreibt bisherige Werte)

Hinweis: Falls die ermittelten Risiken als zu hoch erscheinen oder sich zeigt, dass es noch weitere Massnahmen zur Minimierung gibt, sollten diese oben unter Ziff. 3 eingetragen werden und bei der Risikobeurteilung hier berücksichtigt werden.

	Mögliche unerwünschte negative Folgen Weiteres Risiko vorschlagen*	Was wir dagegen tun Massnahmen vorschlagen* / Aus obigen formulieren*	Wie wir das Restrisiko einschätzen Risikobeurteilung vorschlagen*	Mögliche Folgen für die Person	Eintrittswahrscheinlichkeit (alles in allem)	Risiko (1-16)
4.01	Personendaten des Vorhabens gelangen wegen eines Fehlers oder absichtlich an **unbefugte Dritte**. Diese missbrauchen sie zum Schaden der betroffenen Personen.	- Berechtigungskonzept: Da wir nur autorisierten Personen Zugriff auf die Personendaten geben, wird das Risiko von unbefugtem Zugriff und Missbrauch reduziert. - Schulung: Durch Schulungen stellen wir sicher, dass die Mitarbeitenden die Lösung korrekt und sicher nutzen, was das Risiko von Fehlern und Missbrauch verringert. - Zugriffskontrolle: Durch die Beschränkung des Zugriffs auf autorisierte Personen können wir Missbräuche und unbefugte Nutzung der Personendaten verhindern. - Verschlüsselung "at rest": Die Verschlüsselung der Personendaten in unserem System schützt vor unautorisiertem Zugriff, falls jemand physischen Zugriff auf die Speichermedien erhält. - Datenlöschungsfunktionen: Durch die Möglichkeit, nicht mehr benötigte Personendaten zu löschen oder zu anonymisieren, minimieren wir das Risiko eines unbefugten Zugriffs auf diese Daten.	Das konkrete Restrisiko für die betroffene Person besteht darin, dass ihre Personendaten aufgrund eines Fehlers oder absichtlich an unbefugte Dritte gelangen könnten. Diese könnten die Daten dann zum Schaden der betroffenen Person nutzen, beispielsweise für Identitätsdiebstahl oder Missbrauch in sozialen Medien. Die Wahrscheinlichkeit dieses Szenarios ist jedoch insgesamt gering, da strenge Sicherheitsmassnahmen wie Zugriffskontrollen und Verschlüsselung implementiert wurden.	Substanziell	Tief	Mittel (6)
4.02	Personendaten des Vorhabens gelangen wegen eines Fehlers oder absichtlich an eine **unbefugte interne Person**.					

vud.ch/dsfa und vud.ch/dpia (oder www.rosenthal.ch)

Problemlösungen mit KI vermitteln

…rt verteilt werden.
Individuelle Fassungen
sind einfach zu erstellen.

vischerlnk.com/ki-intro

VISCHER

Danke für Ihre Aufmerksamkeit!

Fragen: drosenthal@vischer.com

Besuchen Sie das VISCHER Legal Innovation Lab www.vischer.com/lil

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com