

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

Beurteilung ausländische Behördenzugriffe

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

Step 5: Overall assessment			
d)	Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)		6.25%
e)	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)		
		80%	20%
		disclosure of the data at issue (in our experience, this is not the case for most p other hand, we can assume that at least the Swiss-based employees who are comply with Swiss law and prevent the production of the data (Swiss law principl	

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>

Datenschutz-Compliance für KMU

revDSG – was zu tun ist. Umgang mit: Neu ab 19.2023

Zehn Gebote zum Umgang mit Personendaten nach DSG!

- Wir **sagen** der Person vorher, was wir mit ihren Daten wozu tun.
- Wir **halten uns daran** und setzen Daten nicht zweckwidrig ein.
- Wir **üben uns in Datensparsamkeit** und "need-to-know".
- Wir **löschen rasch**, was wir nicht mehr brauchen.
- Wir **erlauben** einer Person auch "Nein" zu sagen.
- Wir tun nur das, was wir bei uns selbst **akzeptabel** finden.
- Wir **prüfen** unsere Daten auf **problematische Fehler** und Lücken.
- Wir geben **sensitive Daten** nicht für Zwecke Dritter weiter.
- Wir treffen **Massnahmen**, damit die Daten bei uns **sicher** sind.
- Wir **beschaffen** Daten auf **legale Weise** und aus **legalen Quellen**.
- Ausnahmen sind (nur) bei "besseren" Grund möglich.**

Wir gestalten Jede Datenbearbeitung nach diesen Geboten!

Wenn Daten ins Ausland gehen

Problemlos: EWR, UK, angemessene Länder!
Alle anderen Staaten u.a. erlaubt falls:
 • Export zur Abwicklung eines Vertrages mit oder für die betroffene Person nötig
 • Expliziter Verzicht auf Schutz im Ausland
 • Abschluss der "Standardvertragsklauseln" der EU* mit CH-Anpassung und keinen Grund zur Annahme haben, dass es zu problematischen Beeinträchtigungen kommt ("JA machen")
Wir prüfen unsere Verträge daraufhin!

Die Daten sind sicher, sonst melden wir

Technisch: Zugang nur "need-to-know" und mit persönlichem Konto, "MFA" bei externem Zugriff, Audit-Trails (ggf. Pflicht bei sensiblen Daten), 1 Jahr* Passwortspeicherung, Firewalls, Antimalware-Software, Backups (auch offline).
Organisatorisch: Weisungen (z.B. dieses Blatt dazu verwenden), Schulungen, Prüfung der Logs, Prüfung der Massnahmen, bei vielen sensiblen Daten: Bearbeitungsregime!
Meldepflicht: Ist die Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten verletzt und das Risiko negativer Folgen für einzelne Personen hoch (nicht bloss selbst) → EDOB melden (Formular auf <https://esdob.admin.ch>) und für 2 Jahre dokumentieren; können sich Personen selbst vor Folgen schützen → Meldung auch an sie.
Jeder ist für Sicherheit mitverantwortlich!

Datenschutzerklärung
 Jede planmässige, gesetzlich nicht erforderliche Beschaffung von Personendaten ist in der Datenschutzerklärung ("DSF"). Wir weisen die Personen auf die DSE hin (AGB, Formulare, Apps etc.). Sie ist auf unserer Website.
Pflichtinhalt: Wer wir sind (mit Kontaktangaben), wozu wir die Daten beschaffen, welche Daten, wem wir sie geben (Namen nicht nötig), in welche Länder oder Regionen sie gehen können und worauf wir uns rechtlich stützen.*

Inventar der Bearbeitungen
 Wir führen ein Verzeichnis unserer Aktivitäten, bei denen Personendaten bearbeitet werden (z.B. Verwaltung der Kundendaten, Buchhaltung, Personalverwaltung, Onlineshop). Aufgeführt ist der Inhalt gemäss Art. 12 revDSG, u.a. Bearbeitungs- und Aufbewahrungsdauer. Diese **Pflicht gilt nur**, falls wir 250+ Mitarbeiter (Köpfe) haben oder sensitive Daten* in grossem Umfang bearbeiten oder Hochrisiko-Profilung betreiben.

Auftragsbearbeiter
 Falls wir einem IT-Provider oder sonst jemandem die Bearbeitung unserer Daten anvertrauen, schliessen wir einen "ADV" ab, d.h. einen Vertrag, der uns erlaubt ihn zu steuern und zu kontrollieren und den Bezug von Dritten vorab zu genehmigen* (oder ihn zu widersprechen). Er hält auch die **Sicherheitsmassnahmen** (sog. TOMS) fest. Diese prüfen wir (ggf. inkl. Audit-Berichte). Ein ADV nach Art. 28 DSGVO genügt, falls er ebenso auf das DSG verweist. Der Auftragsbearbeiter darf nur tun, was wir auch tun dürfen (z.B. i.d.R. keine Datennutzung für sich). Wir prüfen die heutigen/neuen ADV auf Konformität.

Datenschutz-Folgenabschätzung (DSFA)
 Bei Vorhaben, die punkto Datenbearbeitung für Betroffene **risikoreicher** sein könnten, machen wir eine DSFA. Darin dokumentieren wir das Vorhaben und die Massnahmen zu ihrem Schutz und prüfen, ob trotzdem hohe Risiken unerwünschter **negativer Folgen** für sie bleiben (falls ja: Hilfe holen). Wir **beharren** sie auf.

Privacy by Default
 Wo wir in Apps, auf Websites etc. **Einstellungen** zum Datenschutz haben, sind diese auf das **Minimum** voreingestellt. Die Entwickler achten darauf.

Kleines Berufsgeheimnis
 Uns **anvertraute**, beruflich nötige Personendaten halten wir geheim oder nur **stiller** weitergeben. **Wir haben eine Stelle, die weiss was zu tun ist, wenn**
 ... eine Person ihre Daten sehen/haben oder diese gelöscht oder korrigiert haben will oder sie sonst ein sie betreffendes Datenschutzanliegen hat;
 ... wir ein neues oder geändertes Vorhaben haben, das auch Daten von Personen betrifft und daher der Datenschutz (ggf. mit DSFA) geprüft werden muss;
 ... Daten von Personen verloren gehen, in falsche Hände gelangen, manipuliert wurden, dies passiert sein könnte oder es Sicherheitsprobleme gibt:
Jeder von uns meldet solche Vorkommnisse dieser Stelle umgehend!

Fragen? VPS auf privacy@vps.ch oder www.vps.ch
Extern: privacy@vps.ch
Interim: privacy@vps.ch
Info: www.vps.ch
 *Vgl. DSGVO/DSG: <https://www.vps.ch/glossar/gesetzliche-grundlagen>
 *Vgl. Art. 17 DSGVO (Recht auf Vergessenwerden)
 *Vgl. Art. 18 DSGVO (Recht auf Einschränkung der Verarbeitung)
 *Vgl. Art. 19 DSGVO (Recht auf Berichtigung)
 *Vgl. Art. 20 DSGVO (Recht auf Datenportabilität)
 *Vgl. Art. 21 DSGVO (Recht auf Widerspruch gegen die Verarbeitung)
 *Vgl. Art. 22 DSGVO (Recht auf automatische Entscheidung und Profiling)
 *Vgl. Art. 23 DSGVO (Recht auf Einschränkung der Verarbeitung)
 *Vgl. Art. 24 DSGVO (Recht auf Löschung und Einschränkung der Verarbeitung)
 *Vgl. Art. 25 DSGVO (Datenschutz durch Design und durch Default)
 *Vgl. Art. 26 DSGVO (Rechenschaftspflicht)
 *Vgl. Art. 27 DSGVO (Datenschutzbeauftragter und Datenschutzberater)
 *Vgl. Art. 28 DSGVO (Auftragsverhältnisse)
 *Vgl. Art. 29 DSGVO (Datenschutz Impact Assessment)
 *Vgl. Art. 30 DSGVO (Aufzeichnungspflichten)
 *Vgl. Art. 31 DSGVO (Kontrollmechanismen)
 *Vgl. Art. 32 DSGVO (Sicherheit der Verarbeitung)
 *Vgl. Art. 33 DSGVO (Meldung von Datenschutzverletzungen)
 *Vgl. Art. 34 DSGVO (Meldung von Datenschutzverletzungen)
 *Vgl. Art. 35 DSGVO (Datenschutz Impact Assessment)
 *Vgl. Art. 36 DSGVO (Ansprüche der Betroffenen)
 *Vgl. Art. 37 DSGVO (Aufsichtsbehörden)
 *Vgl. Art. 38 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 39 DSGVO (Aufgaben der Aufsichtsbehörden)
 *Vgl. Art. 40 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 41 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 42 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 43 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 44 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 45 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 46 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 47 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 48 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 49 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 50 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 51 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 52 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 53 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 54 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 55 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 56 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 57 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 58 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 59 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 60 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 61 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 62 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 63 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 64 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 65 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 66 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 67 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 68 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 69 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 70 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 71 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 72 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 73 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 74 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 75 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 76 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 77 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 78 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 79 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 80 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 81 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 82 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 83 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 84 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 85 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 86 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 87 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 88 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 89 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 90 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 91 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 92 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 93 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 94 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 95 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 96 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 97 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 98 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 99 DSGVO (Ansprüche der Aufsichtsbehörden)
 *Vgl. Art. 100 DSGVO (Ansprüche der Aufsichtsbehörden)

VISCHER Privacy Score (für private Betriebe)

60 Minuten

20 Minuten

VPS Detailbearbeitung eignet sich für Unternehmen mit über 50 Mitarbeitern, mit risikoreichen Datenbearbeitungen oder in Fällen, in denen eine ausführlichere Beurteilung gerechtfertigt ist.

VPS Kleinbetriebe ist eine einfache und generische Beurteilung für Unternehmen bis etwa 50 Mitarbeitern ohne risikoreiche Datenbearbeitungen. Sie gibt einen ersten Eindruck.

VPS DSGVO

VPS DSGVO & DSGVO

VPS DSGVO & DSGVO

VPS DSGVO & DSGVO

VPS Kleinbetriebe DSGVO

VPS Kleinbetriebe DSGVO

VPS Kleinbetriebe DSGVO & DSGVO

VPS Kleinbetriebe DSGVO & DSGVO

VPS Cloud-Projekt.

VPS Datensicherheit.

25

20

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

<https://privacyscore.ch>

Tool für ein GenAI Risk Assessment (GAIRA)

The screenshot displays the GAIRA tool interface, which includes a header section with project details, a central risk radar chart, and a detailed compliance checklist. The risk radar chart shows a red area indicating a high-risk level. The checklist contains 25 items related to data processing and privacy, with columns for 'Answer', 'Reason', 'Assessment', '2nd Line Comment', 'By whom?', and 'Risk Handle'.

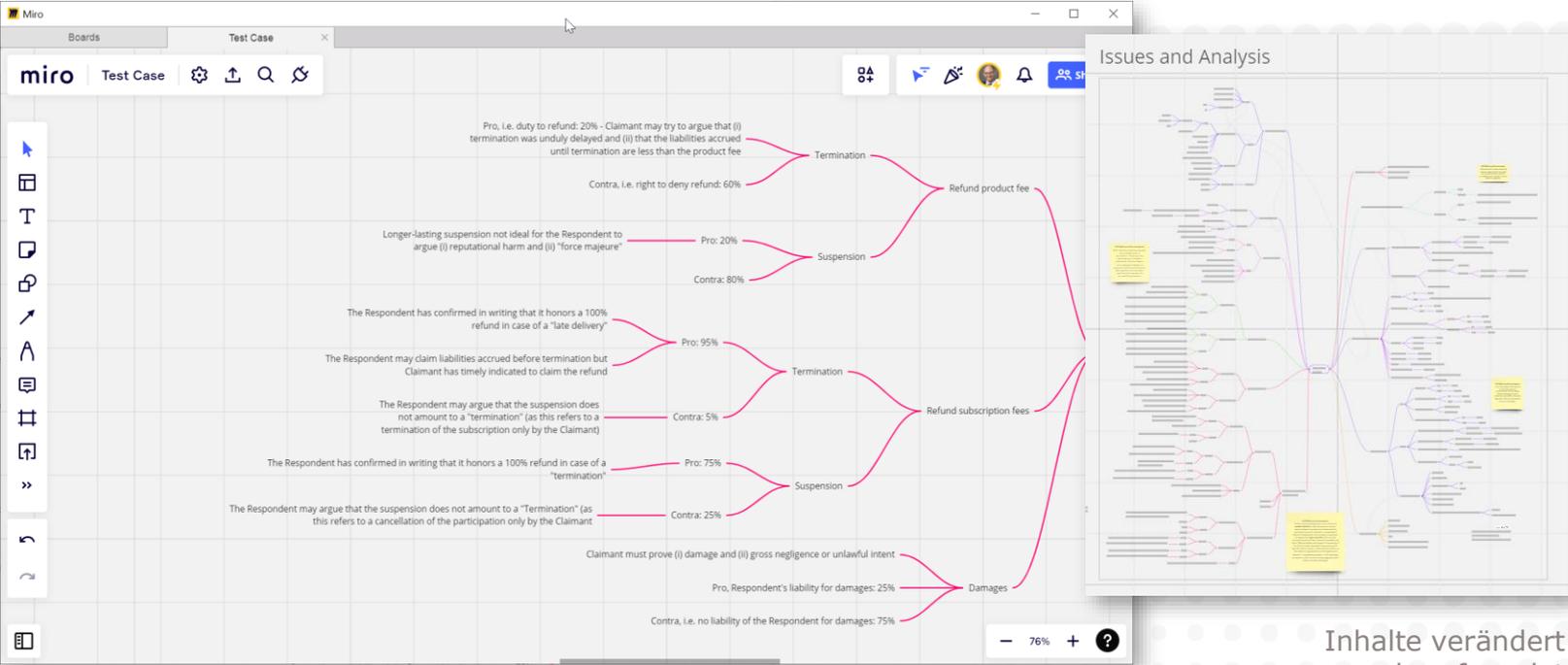
Answer	Reason	Assessment	2nd Line Comment	By whom?	Risk Handle
Yes		OK			
Yes	Yes, we have the EU SCC in place with a TIA.	OK			
Yes	Are our provider(s) approved for use with official/professional secrecy data (where necessary)? ⁽⁶⁾	OK			
Yes	Do our provider(s) contracts protect the confidential or legally protected data we may be using? ⁽⁶⁾	Warning!			
No	Have we performed a DPIA insofar necessary (with no high risks for data subjects)? ⁽⁷⁾	OK	DPO	Accepted	
Yes	Have we amended the privacy notice (where necessary)? ⁽⁸⁾	OK			
Yes	Have we amended the records of processing activities (where necessary)? ⁽⁹⁾	OK			

- 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>



Mindmap eines Falls



Inhalte verändert
und verfremdet

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/DSG	
Hinweis: Eine Anleitung zum Ausfüllen dieser DSFA und zur KI-gestützten Ausfüllhilfe (optional, nur in der Version des Exceils mit Makros) findet sich am Ende dieses Arbeitsblatts	
Unternehmen (Verantwortlicher): Musterfirma AG	
Abteilung: 1	
Verantwortlich intern:	2 4.
Status der DSFA:	3
Name des Vorhabens:	4
Aktivität gemäß Bearbeiter:	5
1. Beschreibung der	6
1.01 In welchem Bereich bzw. welcher Gesc	7
1.02 Was vorgesehen i	4.01
1.03 Welche Interessar	
1.04 Welche Mittel uns	
1.05 Welche Dritten an	
1.06 Welche Daten bes	
1.07 Wessen Daten bez	
1.08 Wo überall Daten	
1.09 Wann die Datenb	
1.10 Weitere Besonder	
2. Erforderlichkeit	
2.01 Warum die Daten	4.02
2.02 Sicht der betroffe	
2.03 Warum die Datenbearbeitung datensparsam, zeitlich auf das nötige begrenzt und auch sonst verhältnismässig ist:	

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

10 Risiken vorschlagen (überschreibe 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

Was wir dagegen tun

Wie wir das Restrisiko einschätzen

Mögliche Folgen für die Person

Eintrittswahrscheinlichkeit (alles in allem)

Risiko (1-16)

Weiteres Risiko vorschlagen*

Massnahmen vorschlagen* | Aus obigen formulieren*

Risikobeurteilung vorschlagen*

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)

Personendaten des Vorhabens gelangen wegen eines Fehlers oder absichtlich an eine **unbefugte interne Person**.

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.

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

Problemlösungen mit KI vermitteln

Künstliche Intelligenz

In der Arbeit
sicher, sinnvoll
und erlaubt
nutzen



Diana Perry

VISCHER
SWISS LAW AND TAX

Darf frei verteilt werden.
Individuelle Fassungen
sind einfach zu erstellen.



vischerlnk.com/ki-intro

VISCHER

Danke für Ihre Aufmerksamkeit!

Fragen: drosenthal@vischer.com

Zürich

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

www.vischer.com

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

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