

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

Cloud-Competing Risikoanalyse eines Lawful Access durch ausländische Behörden		Step 5: Overall assessment	
35	d) Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)		6.25%
36	e) Probability that the parent company text ⁷⁾ (prerequisite)	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
37	f) Probability that the liability of em and realistic, (prerequisite no	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 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>

Cloud-Projekte in sensiblen Bereichen prüfen

CCRA-FI Cloud Compliance Assessment

Project: (M3H) (Pilot/Matrix) | General requirements: Apply/Good/Not Good

Provider: Microsoft | Data Protection: Apply/Good/Not Good

Assessor: | Professional Services: Apply/Good/Not Good

Date: | Deteriorating/Change: Apply/Good/Not Good

Status: | OYRisk Circle 1: Apply/Good/Not Good

| OYRisk Circle 2: Apply/Good/Not Good

| OYRisk Circle 3: Apply/Good/Not Good

| Dislocation: Apply/Good/Not Good

128 Anforderungen/Risk

55 Cloud-Risiken

CCRA-FI Cloud Risk Assessment (Classic)

Template version 22.12.2023 | Risk development vs. status quo

Ref.	Control	Risk Name	Observed Risk Event	Source	Possible Consequences/Reasons for the CP	Nature	Level	Prevalence	Complexity	Impact	Key Risk (Control & Factors)	Core Profile (Check & Change)	Control	Impact	Control	Impact	Control	Impact	Control	Impact
R001	Compliance	Non-compliance with data law	The solution does not comply with the data protection requirements and other data laws (e.g. because the FI failed to understand the requirements of the data protection laws or because the FI did not have enough resources to comply with them. The implementation of the solution, lack of professional security and other specific security measures.	External	Our services do not comply with data protection and other data laws (e.g. because the FI failed to understand the requirements of the data protection laws or because the FI did not have enough resources to comply with them. The implementation of the solution, lack of professional security and other specific security measures.	Compliance	Level 3	4	NA	Business critical compliance check prior to implementation, including measures to audit legal counsel and external auditors.	1	1	NA	NA	[Steps to take]	[OK]	Accepted	Business Owner		
R002	Compliance	Non-compliance with financial regulations	The solution is not compliant with financial regulations and other financial laws (e.g. because the FI failed to understand the requirements of the financial regulations or because the FI did not have enough resources to comply with them. The implementation of the solution, lack of professional security and other specific security measures.	Internal	Our services do not comply with financial regulations and other financial laws (e.g. because the FI failed to understand the requirements of the financial regulations or because the FI did not have enough resources to comply with them. The implementation of the solution, lack of professional security and other specific security measures.	Compliance	Level 2	1	NA	Business critical compliance check prior to implementation, including measures to audit legal counsel and external auditors.	1	1	NA	NA	[Steps to take]	[OK]	Accepted	Business Owner		
R003	Compliance	Non-compliance with other legal requirements	The solution is not compliant with other legal requirements and other legal laws (e.g. because the FI failed to understand the requirements of the other legal requirements or because the FI did not have enough resources to comply with them. The implementation of the solution, lack of professional security and other specific security measures.	External	Our services do not comply with other legal requirements and other legal laws (e.g. because the FI failed to understand the requirements of the other legal requirements or because the FI did not have enough resources to comply with them. The implementation of the solution, lack of professional security and other specific security measures.	Compliance	Level 3	1	NA	Business critical compliance check prior to implementation, including measures to audit legal counsel and external auditors.	1	1	NA	NA	[Steps to take]	[OK]	Accepted	Business Owner		
R004	Compliance	Changes in law cannot be complied with	The solution is not compliant with changes in law and other legal laws (e.g. because the FI failed to understand the requirements of the changes in law or because the FI did not have enough resources to comply with them. The implementation of the solution, lack of professional security and other specific security measures.	External	Our services do not comply with changes in law and other legal laws (e.g. because the FI failed to understand the requirements of the changes in law or because the FI did not have enough resources to comply with them. The implementation of the solution, lack of professional security and other specific security measures.	Compliance	Level 3	2	NA	Business critical compliance check prior to implementation, including measures to audit legal counsel and external auditors.	1	1	NA	NA	[Steps to take]	[OK]	Accepted	Business Owner		

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

Datenschutz-Compliance für KMU

revDSG – was zu tun ist Umgangstext: **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 "besserem" Grund möglich. Wir gestalten Jede Datenbearbeitung nach diesen Geboten!

Wenn Daten ins Ausland gehen

Problemas: 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 keinem Grund zur Annahme haben, dass es zu problematischen Behördenzweifeln kommt (→ "TIA machen")
Wir prüfen unsere Verträge daraufhin!

Die Daten sind sicher, sonst melden wir!
Technisch: Zugang nur "need-to-know" und mit persönlichem Konto, "MFA" mit externem Zugriff, Audit-Trails (ggf. Pflicht bei sensiblen Daten), 1 Jahr? Pseudonymisierung, 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: Verantwortung **herausgeben**.
Meldepflicht: Ist die Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten verletzt und das Risiko negativer Folgen für einzelne Personen hoch (nicht bloss lästig) → EDOB melden (Formular auf <https://edob.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 wozu 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-zwecke, Kategorien von Personen, Daten und Empfänger, Aufbewahrungsdauer. Diese **Pflicht gilt nur**, falls wir 250+ Mitarbeiter (Köpfe) haben oder sensitive Daten* in grossem Umfang bearbeiten oder Hochrisiko-Profilierung 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 ihm zu widensprechen). 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 das 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 **wahren sie auf**.

Kleines Berufsgeheimnis
Uns **anvertraut**, bezüglich nötige Personendaten halten wir geheim oder **low-profile** stellen wir klar, dass wir die Daten nicht geheim halten werden.

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? faq@privacyscore.ch / <https://www.privacyscore.ch>
Extern: www.privacyscore.ch
Interim: www.privacyscore.ch
Intern: www.privacyscore.ch

Autoren: David Rosenthal, drosenthal@vischer.com. Alle Rechte vorbehalten. Darf (ausser in den Feldern) unverändert frei weitergegeben/benutzt werden. Dies ist Information, keine Rechtsberatung. VISCHER

VISCHER Privacy Score (für private Betriebe)

Neu ab 1.1.2023 bis 31.12.2023

DSG 48/100
DSGVO 45/100

60 Minuten
20 Minuten

VPS Detailbearbeitung eignet sich für Unternehmen mit über 80 Mitarbeiter:innen, mit risikostreichen Datenbearbeitungen oder in Fällen, in denen eine aufwändige Beurteilung gerechtfertigt ist.

VPS Kleinbetriebe ist eine einfache und generische Beurteilung für Unternehmen bis etwa 50 Mitarbeiter:innen ohne risikostreiche Datenbearbeitungen. Sie gibt einen ersten Eindruck.

VPS DSGVO
VPS DSGVO & DSGVO
VPS Kleinbetriebe DSGVO
VPS Kleinbetriebe 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)

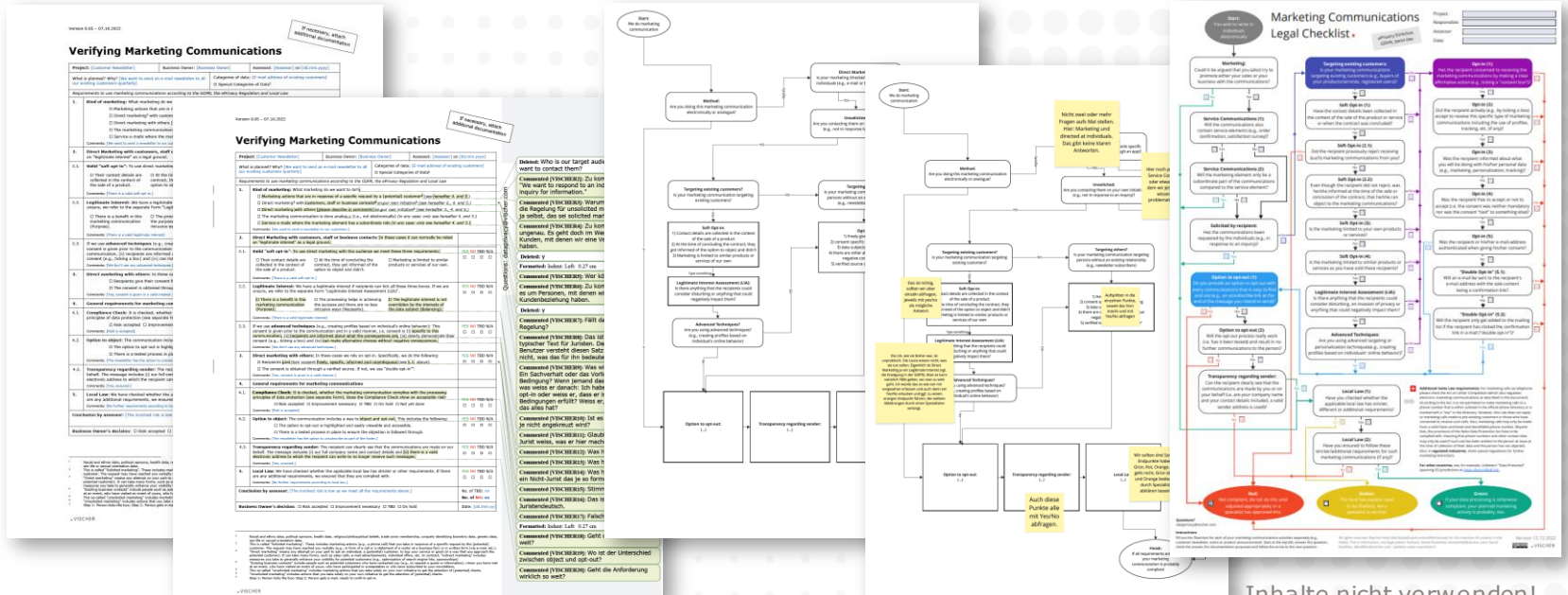
The screenshot displays the GAIRA tool interface, which includes a form for entering application details, a Risk Radar chart, and a compliance checklist. The form contains fields for company name, department, application owner, and status. The Risk Radar chart shows a red dot indicating a high-risk level. The compliance checklist consists of 25 questions related to data processing, privacy, and security, with columns for 'Answer', 'Reason/Incl. measures taken/absent', 'Assessment', '2nd Line Comment', 'By whom?', and 'Risk Handle'.

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

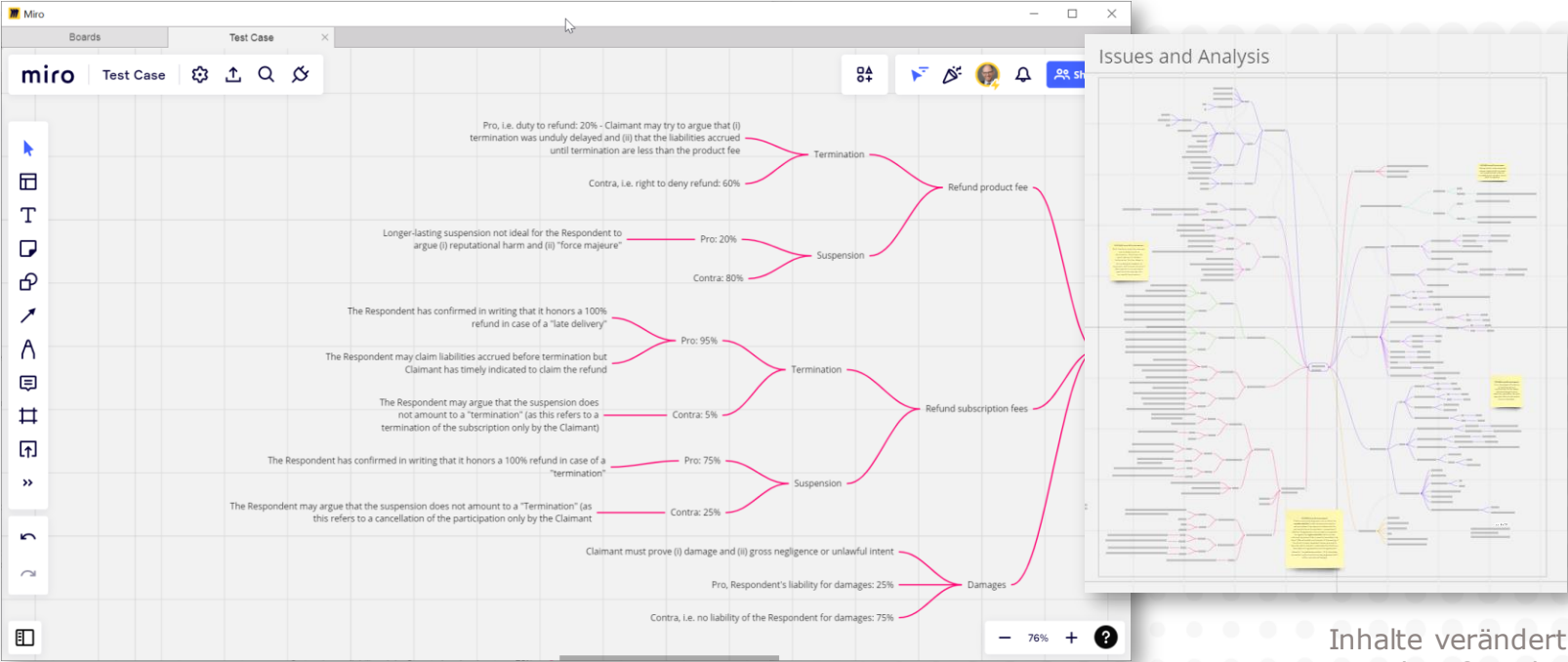
Kostenlos abrufbar unter <https://vischerlnk.com/gaira>



Evolution einer Checkliste



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 Datenbearbeitungen, 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 Datenschutzeil IT-Richtlinie	0.2	2	0	0	Yes	890	907	
3	Überarbeitung Datenschutzeil Mitgliederverträge + Mitgliederinfos	0.5	5	0	0	Yes	2'225	2'267	Verträge bisher nicht
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 nicht
5	Vereinbarung zwischen Verbänden, welche www.time2learn.ch anbieten	0	0	0	0	No	-	-	Schätzung noch nicht
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	-	-	
		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 available through country-specific TIA
5	Creation of Data Retention Policy (no. of doc-categories)	1'325	195	10	-	No	-	-	Requires VISCHER D excluding special rule
5	Customize Data Breach Policy and Process	1'850	-	-	-	No	-	-	Requires VISCHER D set up only follow 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/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

Status der DSFA: 3

Name des Vorhabens: 4

Aktivität gemäß Bearbeiter: 7

1. Beschreibung der Aktivität

1.01 In welchem Bereich bzw. welcher Gesc

1.02 Was vorgesehen i

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 Daten b

1.10 Weitere Besonder

2. Erforderlichkeit

2.01 Warum die Daten

2.02 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. 9 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)
<p>Weiteres Risiko vorschlagen*</p> <p>4.01 Personendaten des Vorhabens gelangen wegen eines Fehlers oder absichtlich an unbefugte Dritte. Diese missbrauchen sie zum Schaden der betroffenen Personen.</p>	<p>Massnahmen vorschlagen* Aus obigen formulieren*</p> <ul style="list-style-type: none"> - 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. 	<p>Risikobeurteilung vorschlagen*</p> <p>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.</p>	Substanziell	Tief	Mittel (6)
<p>4.02 Personendaten des Vorhabens gelangen wegen eines Fehlers oder absichtlich an eine unbefugte interne Person.</p>					



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

Problemlösungen mit KI vermitteln

Noch nicht released!

3.1.24

VISCHER
SWISS LAW AND TAX



... 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