VISCHER

Datenschutz-Compliance.
Herausforderung ihrer Überprüfung

David Rosenthal, Partner, VISCHER AG
3. Oktober 2023

Einen Mythos beerdigen wir gleich …

Sehr geehrter [redacted]

gerne kann ich Ihnen bestätigen, dass die [redacted] alle aktuellen Vorgaben der EU-Datenschutzgrundverordnung sowie der entsprechenden deutschen Normen einhält. Die vorliegenden Dokumente erfüllen, soweit hier ersichtlich, auch die Anforderungen an den Datenschutz in der Schweiz.

Für weitere Fragen stehe ich Ihnen gerne zur Verfügung.

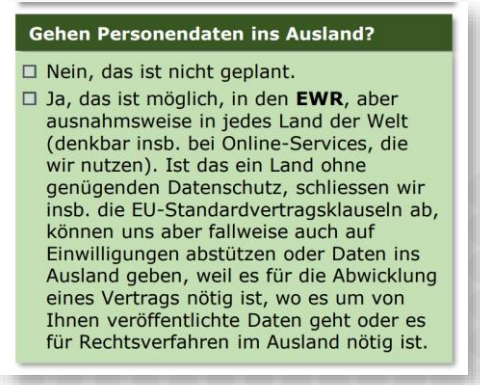
Mit freundlichen Grüße

Dr. [redacted]
Geschäftsführer

Quelle: LinkedIn

Warum ist das so?

- Beispiel **Informationspflichten**
  - Transparenzgrundsatz
  - Pflicht zur Datenschutzerklärung
  - Bei jeder Beschaffung von Personendaten
  - Wachsende Anforderungen der Aufsichtsbehörden
- Kennen Sie **jeden Fall**, in welchem Ihr Unternehmen planmässig an Personendaten gelangt?
- Gelingt es Ihnen, die Informationen darüber allen betroffenen Personen, deren Adresse Sie kennen, **mitzuteilen**?
- Wissen Sie, wie **detailliert** die Information erfolgen muss?
- Werden z.B. die **Aufbewahrungsfristen** eingehalten?


Gehen Personendaten ins Ausland?

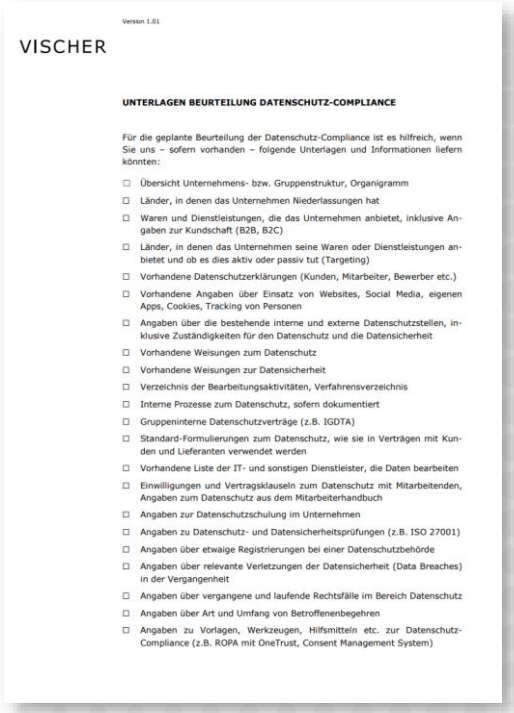
☐ Nein, das ist nicht geplant.

☐ Ja, das ist möglich, in den **EWR**, aber ausnahmsweise in jedes Land der Welt (denkbar insb. bei Online-Services, die wir nutzen). Ist das ein Land ohne genügenden Datenschutz, schliessen wir insb. die EU-Standardvertragsklauseln ab, können uns aber fallweise auch auf Einwilligungen abstützen oder Daten ins Ausland geben, weil es für die Abwicklung eines Vertrags nötig ist, wo es um von Ihnen veröffentlichte Daten geht oder es für Rechtsverfahren im Ausland nötig ist.

https://www.rosenthal.ch/downloads/VISCHER-DSE-XS-KMU.pdf

Wo hinschauen?

- **Organisation** und Regelung des Datenschutzes
- **Bearbeitungsverantwortliche** Personen
- Wissen, welche Daten **wo bearbeitet** werden
- **Lifecycle**-Management von Daten
- Prozesse für **neue/geänderte** Datenbearbeitungen
- Prozesse für Datenaustausch mit **Dritten**, Verträge
- Informationen und **Bearbeitungszwecke**
- Wissen um **Sicherheit** und Data Breaches im Alltag
- **Reporting**



Version 1.01

VISCHER

UNTERLAGEN BEURTEILUNG DATENSCHUTZ-COMPLIANCE

Für die geplante Beurteilung der Datenschutz-Compliance ist es hilfreich, wenn Sie uns – sofern vorhanden – folgende Unterlagen und Informationen liefern könnten:

- ☐ Übersicht Unternehmens- bzw. Gruppenstruktur, Organigramm
- ☐ Länder, in denen das Unternehmen Niederlassungen hat
- ☐ Waren und Dienstleistungen, die das Unternehmen anbietet, inklusive Angaben zur Kundschaft (B2B, B2C)
- ☐ Länder, in denen das Unternehmen seine Waren oder Dienstleistungen anbietet und ob es dies aktiv oder passiv tut (Targeting)
- ☐ Vorhandene Datenschutzerklärungen (Kunden, Mitarbeiter, Bewerber etc.)
- ☐ Vorhandene Angaben über Einsatz von Websites, Social Media, eigenen Apps, Cookies, Tracking von Personen
- ☐ Angaben über die bestehende interne und externe Datenschutzstellen, inklusive Zuständigkeiten für den Datenschutz und die Datensicherheit
- ☐ Vorhandene Weisungen zum Datenschutz
- ☐ Vorhandene Weisungen zur Datensicherheit
- ☐ Verzeichnis der Bearbeitungsaktivitäten, Verfahrensverzeichnis
- ☐ Interne Prozesse zum Datenschutz, sofern dokumentiert
- ☐ Gruppeninterne Datenschutzverträge (z.B. IGDTA)
- ☐ Standard-Formulierungen zum Datenschutz, wie sie in Verträgen mit Kunden und Lieferanten verwendet werden
- ☐ Vorhandene Liste der IT- und sonstigen Dienstleister, die Daten bearbeiten
- ☐ Einwilligungen und Vertragsklauseln zum Datenschutz mit Mitarbeitenden, Angaben zum Datenschutz aus dem Mitarbeiterhandbuch
- ☐ Angaben zur Datenschutzschulung im Unternehmen
- ☐ Angaben zu Datenschutz- und Datensicherheitsprüfungen (z.B. ISO 27001)
- ☐ Angaben über etwaige Registrierungen bei einer Datenschutzbehörde
- ☐ Angaben über relevante Verletzungen der Datensicherheit (Data Breaches) in der Vergangenheit
- ☐ Angaben über vergangene und laufende Rechtsfälle im Bereich Datenschutz
- ☐ Angaben über Art und Umfang von Betroffenenbegehren
- ☐ Angaben zu Vorlagen, Werkzeugen, Hilfsmitteln etc. zur Datenschutz-Compliance (z.B. ROPA mit OneTrust, Consent Management System)

https://www.rosenthal.ch/downloads/VISCHER-compliance-check-request-list-DE.pdf (auch auf Englisch verfügbar)

Wo hinschauen?

Falls Sie Audit-Erfolge brauchen …

- Datenschutzerklärung deckt **nur Website bzw. Online** ab
- **Unvollständige** Angaben in der Datenschutzerklärung
- **Pflichtangaben** fehlen (z.B. Auslandsexporte)
- Angegebene **Aufbewahrungsfristen** werden nicht eingehalten
- Es **fehlen** Aufbewahrungsfristen (und werden nicht befolgt)
- Fehlende Möglichkeit zur **vorzeitigen Löschung** von Daten
- Es fehlt eine Datenschutzerklärung für **HR-Daten**
- Keine klare/korrekte Zuordnung der **Controller** in Gruppen
- **Bearbeitungsverzeichnisse** nicht vollständig oder aktuell

Falls Sie Audit-Erfolge brauchen …

- Dienstleister nicht nach ihrer **datenschutzrechtlichen Rolle** klassifiziert (Controller, Processor, Joint-Controller)
- Ungenügende oder unpassende **Verträge** (AVV, JCA, C-C)
- Keine oder ungenügende **Provider-Prüfung**, mangelhaftes Vendor Cyber Risk Management, fehlende Vorgaben
- Fehlendes Wissen über **internationale Datentransfers**
- Fehlende **Regelung** von internationalen Datentransfers
- Fehlender Schweizer Zusatz zu Verträgen mit den **EU SCC**
- Fehlende **Transfer Impact Assessments**
- Fehlende Regelung gruppeninterner Datenflüsse (**IGDTA**)

Falls Sie Audit-Erfolge brauchen …

- **Newsletter** und andere Mailings ohne Opt-in oder Soft-Opt-in
- Fehlende oder nicht funktionierende **Sperrlisten** für Marketing
- Unzulässige "**Cookie-Banner**" (auch wo es keine bräuchte)
- Fehlende Angaben zu Joint-Controllern (Website, **Social Media**)
- Fehlende interne Zuweisung der **Compliance-Verantwortung**
- Fehlendes Reporting bzw. **Überwachung** durch Leitung
- Fehlende Dokumentation der **Compliance**
- Fehlende **Weisungen**
- Fehlende **Schulungen**

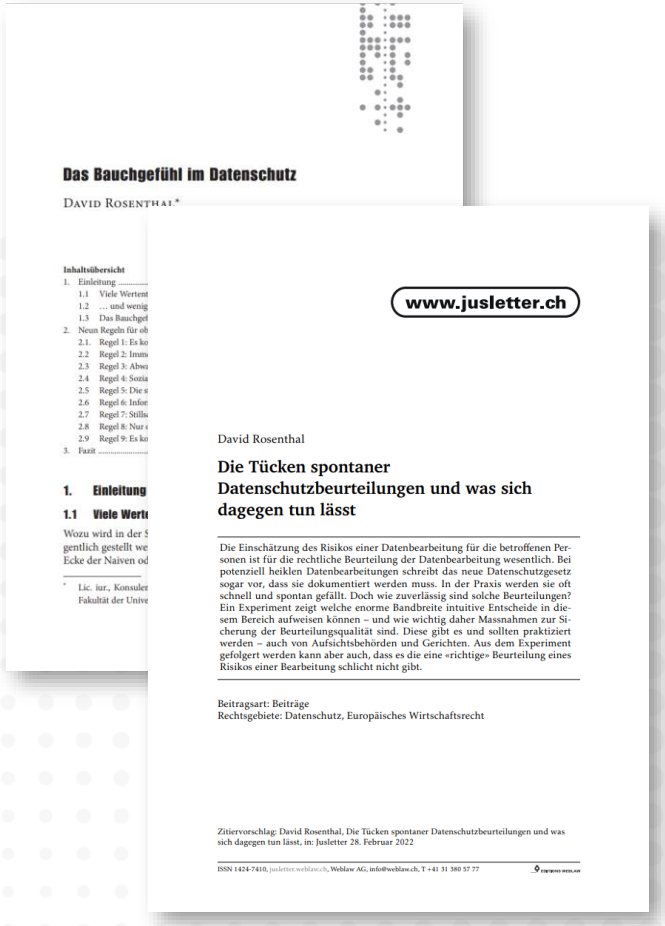
Falls Sie Audit-Erfolge brauchen …

- Fehlende **Protokollierungen** in den Computersystemen
- Mangelhafte **Datensicherheit** (inkl. BCM und Notfallplanung)
- **Data Breaches** intern nicht gemeldet und dokumentiert
- Fehlende Prozesse und Know-how für **Betroffenenbegehren**
- Ungeprüfte **neue Datenbearbeitungen** (inkl. Secondary Use)
- Ungeprüfte **Änderungen** bestehender Datenbearbeitungen
- Bestehende Datenbearbeitung nicht auf **Konformität** geprüft
- Unkontrollierter Einsatz von **Online-Tools** (ChatGPT …)
- Verletzung der allgemeinen **beruflichen Schweigepflicht**

Risikobeurteilungen im Datenschutz?

- Sie sind möglich aber oftmals **zufällig**
- Das **"Bauchgefühl"** spielt im Datenschutz eine zentrale Rolle
- Abgrenzen zwischen gesetzlicher Compliance und **ethischen Erwartungen**
- **Aufsichtsbehörden** unterscheiden oft nicht
- Wesentlich ist, dass Risikobeurteilungen **strukturiert** gemacht werden – der Weg ist das Ziel

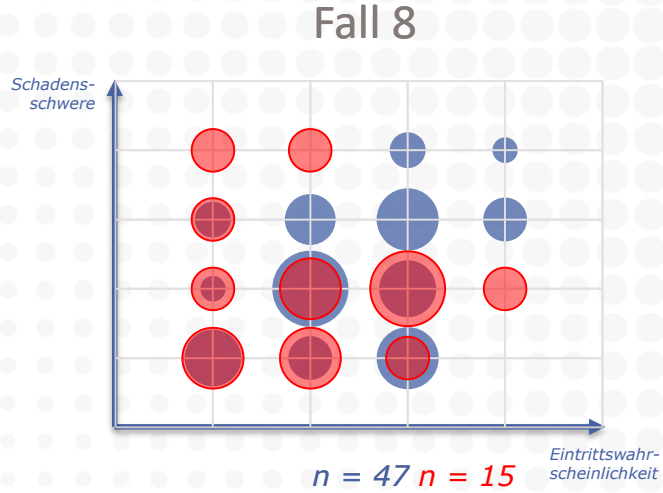
https://bit.ly/3ZCIWDw



https://bit.ly/3qbFMpL

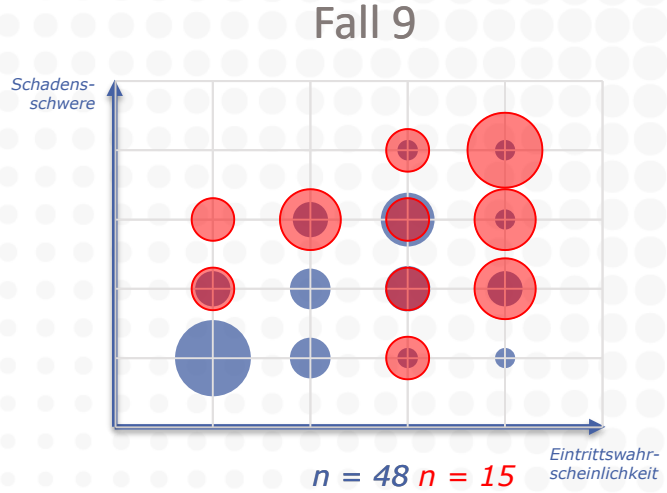
Fall 8

"Eine Beraterfirma will ein Computerprogramm verwenden, das von jeder Stellenbewerbung eines Beraters einen "Erfolgsscore" aufgrund seines bisherigen Werdegangs und seiner Noten berechnet. Der Score basiert auf den bisherigen Erfahrungen des Unternehmens mit vergangenen Einstellungen. Der Score dient nur der Information des Hiring-Partners. Es wird niemand automatisch aussortiert."



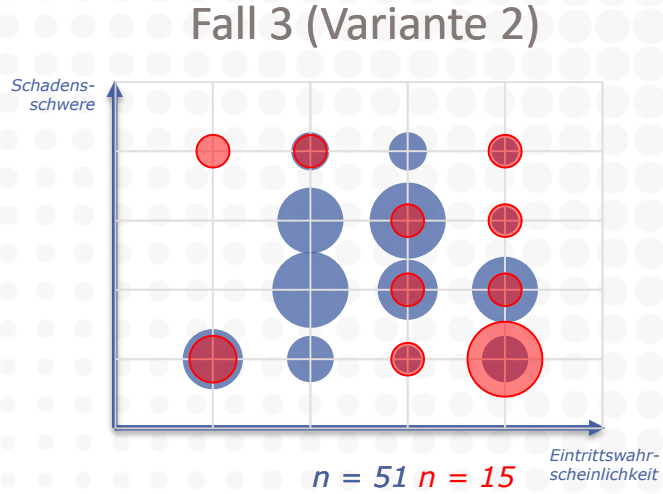
Fall 9

"Eine private Forschergruppe hat ein Computerprogramm entwickelt, dass die Attraktivität von Gesichtern beurteilen kann. Jeder kann auf der Website beliebige Bilder hochladen, die daraufhin vom Computer beurteilt werden. Die Bilder werden zudem genutzt, um das Computerprogramm noch besser zu machen. Hierzu werden sie Testteilnehmern zur menschlichen Beurteilung vorgelegt und danach gelöscht."



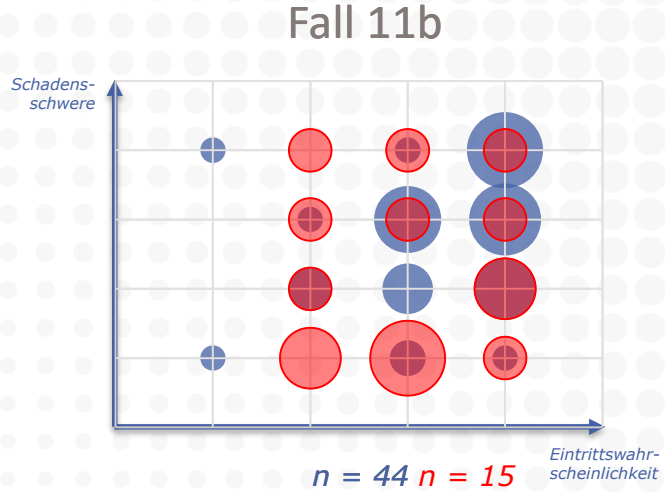
Fall 3 (Variante 2)

"Ein Unternehmen erhebt beim Verkauf von Waren in einem Online-Shop Kontaktdaten und Angaben über Warenkäufe. Es kann aufgrund dieser Angaben Vorlieben seiner Kunden ermitteln. Es will dieses Wissen verwenden, um den einzelnen Kunden auf ihre jeweiligen Vorlieben zugeschnittene Angebote zukommen zu lassen. Er hat keine Einwilligung der Kunden und informiert sie nicht."



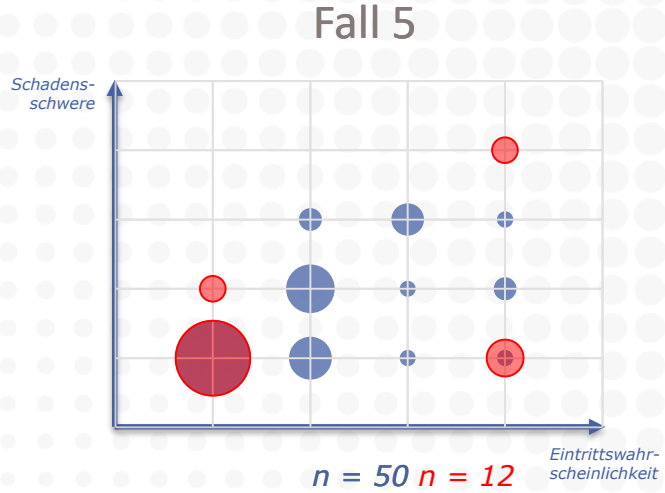
Fall 11b

"Der Betreiber eines Online-Shops will Zahlungsausfälle besser bekämpfen. Er hat festgestellt, dass es Korrelationen zwischen Nationalität, Wohnort, Alter, Geschlecht und bestimmter bestellter Ware und Zahlungsausfällen gibt. Statt auf traditionelle Kreditwürdigkeitsdaten abzustellen, berechnet er sich aufgrund dieser Angaben seinen eigenen Score, auf dessen Basis er über die Option zum Kreditkauf entscheidet."

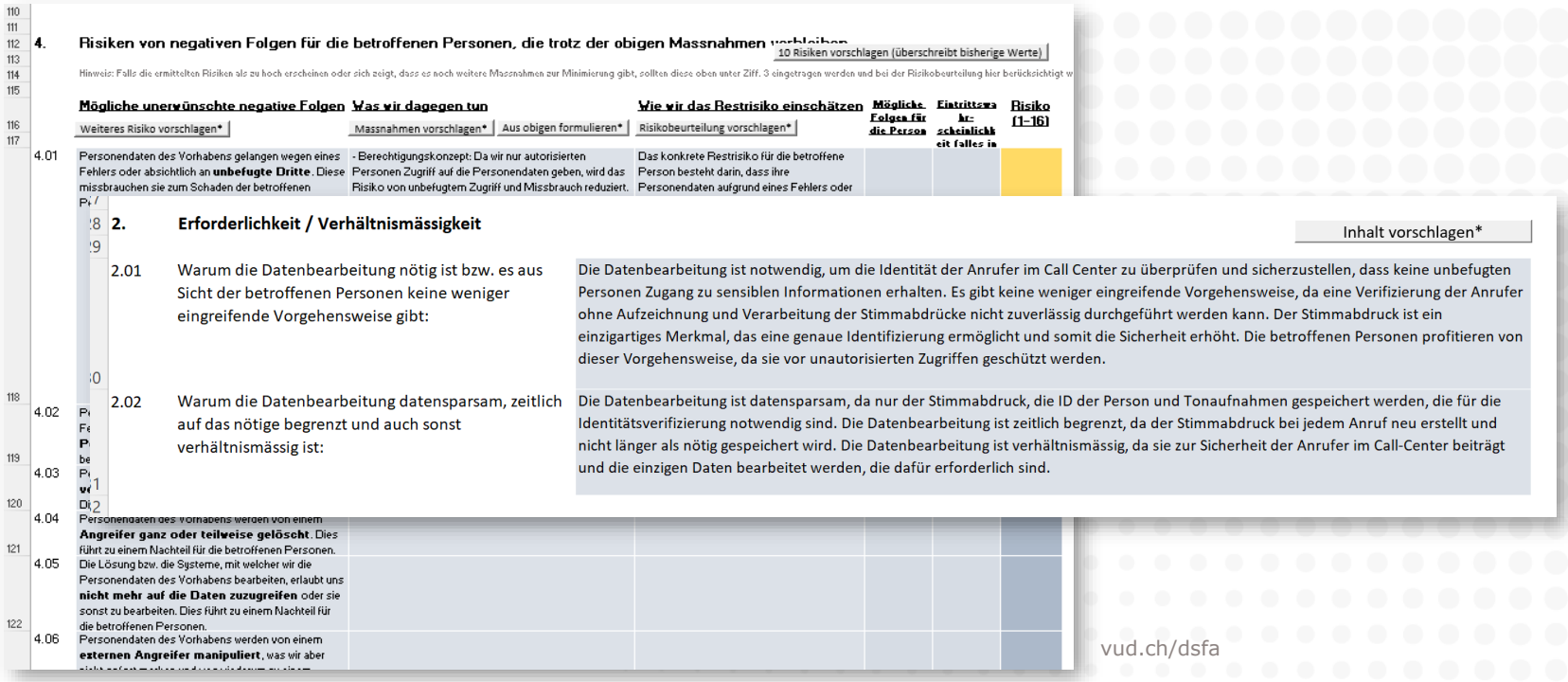


Fall 5

"Eine Aufzugswartungsfirma stellt ihren Aussendienstlern Wagen zur Verfügung, die diese auch privat nutzen dürfen. Eingebaut ist ein Tracker, der Standort und Fahrweise aufzeichnet. Das dient der Einsatzplanung und präventiven Wartung (aus der Fahrweise lässt sich die Abnutzung ermitteln). Zugang haben der Fahrer, die Einsatzplanung und die Fuhrparktechniker. Für private Fahrten können die Mitarbeiter das Tracking abschalten."



Risikobeurteilungen …



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 w

	Mögliche unerwünschte negative Folgen	Was wir dagegen tun		Wie wir das Restrisiko einschätzen	Mögliche Folgen für die Person	Eintrittswahrscheinlichkeit falles in	Risiko (1–16)
	Weiteres Risiko vorschlagen*	Massnahmen vorschlagen*	Aus obigen formulieren*	Risikobeurteilung vorschlagen*			
4.01	Personendaten des Vorhabens gelangen wegen eines Fehlers oder absichtlich an **unbefugte Dritte**. Diese missbrauchen sie zum Schaden der betroffenen P…	- Berechtigungskonzept: Da wir nur autorisierten Personen Zugriff auf die Personendaten geben, wird das Risiko von unbefugtem Zugriff und Missbrauch reduziert.		Das konkrete Restrisiko für die betroffene Person besteht darin, dass ihre Personendaten aufgrund eines Fehlers oder			
4.02	P… Fe… **P**… be…						
4.03	P… **w**… Di…						
4.04	Personendaten des Vorhabens werden von einem **Angreifer ganz oder teilweise gelöscht**. Dies führt zu einem Nachteil für die betroffenen Personen.						
4.05	Die Lösung bzw. die Systeme, mit welcher wir die Personendaten des Vorhabens bearbeiten, erlaubt uns **nicht mehr auf die Daten zuzugreifen** oder sie sonst zu bearbeiten. Dies führt zu einem Nachteil für die betroffenen Personen.						
4.06	Personendaten des Vorhabens werden von einem **externen Angreifer manipuliert**, was wir aber						

2. Erforderlichkeit / Verhältnismässigkeit

Inhalt vorschlagen*

2.01	Warum die Datenbearbeitung nötig ist bzw. es aus Sicht der betroffenen Personen keine weniger eingreifende Vorgehensweise gibt:	Die Datenbearbeitung ist notwendig, um die Identität der Anrufer im Call Center zu überprüfen und sicherzustellen, dass keine unbefugten Personen Zugang zu sensiblen Informationen erhalten. Es gibt keine weniger eingreifende Vorgehensweise, da eine Verifizierung der Anrufer ohne Aufzeichnung und Verarbeitung der Stimmabdrücke nicht zuverlässig durchgeführt werden kann. Der Stimmabdruck ist ein einzigartiges Merkmal, das eine genaue Identifizierung ermöglicht und somit die Sicherheit erhöht. Die betroffenen Personen profitieren von dieser Vorgehensweise, da sie vor unautorisierten Zugriffen geschützt werden.
2.02	Warum die Datenbearbeitung datensparsam, zeitlich auf das nötige begrenzt und auch sonst verhältnismässig ist:	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

Privacyscore.ch

Online kostenlos und anonym

VPS Detailbeurteilung. VPS Kleinbetriebe.

60 20

Minuten

VPS Detailbeurteilung eignet sich für Unternehmen mit über
Mitarbeitenden, mit risikoträchtigen Datenbearbeitungen od
in denen eine ausführlichere Beurteilung gewünscht ist.

VPS DSG

VPS DSGVO

VPS Cloud-P

VPS Cloud-Projekt err
(ohne Berufsgeheimni

7. Unsere DSE deckt im Bereich des DSG auch die Bearbeitung von Mitarbeitendendaten ab, jedenfalls soweit wir solche planmässig (und i spontan oder zufällig) erheben.

- ◯ Wir haben keine DSE für Mitarbeitende.
- ◯ Weiss nicht.

die Anforderungen des Datenschutzrechts zu erfüllen. Nötigenfalls ist die Höhe jeder Zeile von Excel automatisch anpassen
m die für dieses Thema nötigen Dokumente vermerkt; sie sind diesfalls oben mit den entsprechenden Abkürzungen
ch DSG bzw. nach DSGVO erforderlich ist oder nicht. Am Ende jeder Zeile ist festgehalten, wieviele Reifegradpunkte (max. 5)
ng: Wird Prüfgegenstand, Prüfprogramm bzw. das anwendbare Recht oder Sprache nachträglich angepasst, stimmen bereits

Bitte nur hier die am besten passende Antwort wählen

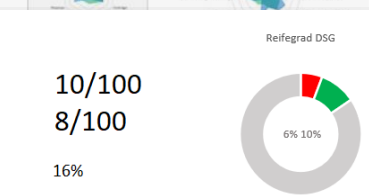
Status	Empfehlung	Dokumente	DSG	DSGVO	Reifegrad DSG	Reifegrad DSGVO	(nicht benutzt)	Strafbarkeit DSG	Bussen DSGVO	Reputationsrisiko
Nein. / Weiss nicht.	Eine DSE ist zwingend und das Fehlen bemerkt jeder. Lassen Sie sich raschmöglichst eine erstellen.	DSE	Nötig	Nötig	0	0	0	3	3	0
Das wissen wir nicht, aber wir haben eine Vorlage benutzt.	Vorlagen können tückisch sein. Prüfen Sie, ob die DSE gesetzlich vorgeschriebenen Pflichtinhalte aufweist.	DSE	Nötig	Nötig	2	2	0	2	2	2
Ja, ausser, dass wir sie nicht in allen Sprachen haben, in denen wir kommunizieren.	Ist die DSE auf einer Website, sollte sie mind. in den Sprachen der Website verfügbar sein. Nötigenfalls lassen Sie sie übersetzen.	DSE	Nötig	Nötig	3	3	0	1	2	1
Die DSE ist auf der Front unserer Website abrufbar, aber wir weisen nicht darauf hin und den Personen ist auch nicht unbedingt klar, dass	Das hilft etwas, aber erreicht nur jene Personen, die wissen, dass Sie Daten über Sie erheben. Sorgen Sie so gut wie möglich dafür, dass sie davon erfahren.	HDSE	Nötig	Nötig	4	4	0	1	2	1

genen Daten unserer

VISCHER Privacy Score:

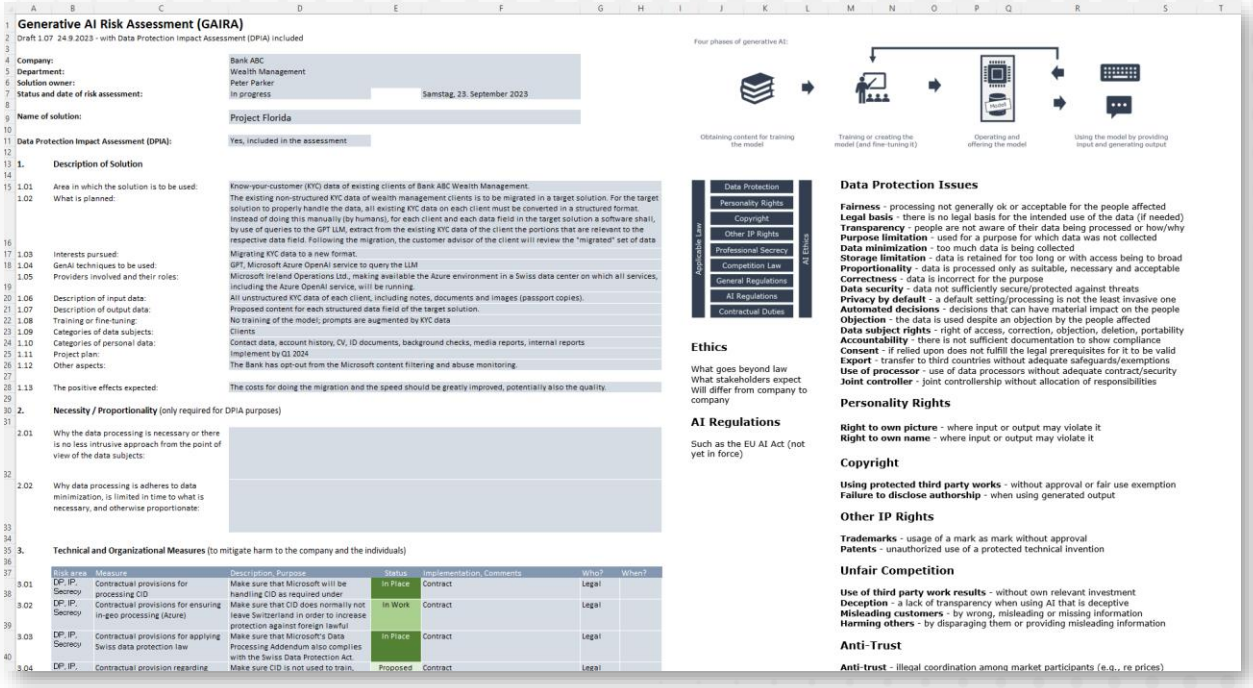
DSG	10/100
DSGVO	8/100
Beurteilt:	16%

Reifegrad DSG



VISCHER

Die rechtlichen Fragen gehen uns nicht aus …



Generative AI Risk Assessment (GAIRA)

Draft 1.07 24.9.2023 - with Data Protection Impact Assessment (DPIA) included

Company:	Bank ABC	
Department:	Wealth Management	
Solution owner:	Peter Parker	
Status and date of risk assessment:	In progress	Samstag, 23. September 2023
Name of solution:	Project Florida	
Data Protection Impact Assessment (DPIA):	Yes, included in the assessment	

1. Description of Solution

1.01	Area in which the solution is to be used:	Know-your-customer (KYC) data of existing clients of Bank ABC Wealth Management.
1.02	What is planned:	The existing non-structured KYC data of wealth management clients is to be migrated in a target solution. For the target solution to properly handle the data, all existing KYC data on each client must be converted in a structured format. Instead of doing this manually (by humans), for each client and each data field in the target solution a software shall, by use of queries to the GPT LLM, extract from the existing KYC data of the client the portions that are relevant to the respective data field. Following the migration, the customer advisor of the client will review the "migrated" set of data
1.03	Interests pursued:	Migrating KYC data to a new format.
1.04	GenAI techniques to be used:	GPT, Microsoft Azure OpenAI service to query the LLM
1.05	Providers involved and their roles:	Microsoft Ireland Operations Ltd., making available the Azure environment in a Swiss data center on which all services, including the Azure OpenAI service, will be running.
1.06	Description of input data:	All unstructured KYC data of each client, including notes, documents and images (passport copies).
1.07	Description of output data:	Proposed content for each structured data field of the target solution.
1.08	Training or fine-tuning:	No training of the model; prompts are augmented by KYC data
1.09	Categories of data subjects:	Clients
1.10	Categories of personal data:	Contact data, account history, CV, ID documents, background checks, media reports, internal reports
1.11	Project plan:	Implement by Q1 2024
1.12	Other aspects:	The Bank has opt-out from the Microsoft content filtering and abuse monitoring.
1.13	The positive effects expected:	The costs for doing the migration and the speed should be greatly improved, potentially also the quality.

2. Necessity / Proportionality (only required for DPIA purposes)

2.01	Why the data processing is necessary or there is no less intrusive approach from the point of view of the data subjects:	
2.02	Why data processing is adheres to data minimization, is limited in time to what is necessary, and otherwise proportionate:	

3. Technical and Organizational Measures (to mitigate harm to the company and the individuals)

	Risk area	Measure	Description, Purpose	Status	Implementation, Comments	Who?	When?
3.01	DP, IP, Secrecy	Contractual provisions for processing CID	Make sure that Microsoft will be handling CID as required under	In Place	Contract	Legal	
3.02	DP, IP, Secrecy	Contractual provisions for ensuring in-geo processing (Azure)	Make sure that CID does normally not leave Switzerland in order to increase protection against foreign lawful	In Work	Contract	Legal	
3.03	DP, IP, Secrecy	Contractual provisions for applying Swiss data protection law	Make sure that Microsoft's Data Processing Addendum also complies with the Swiss Data Protection Act.	In Place	Contract	Legal	
3.04	DP, IP,	Contractual provision regarding	Make sure CID is not used to train,	Proposed	Contract	Legal	

Four phases of generative AI:

Obtaining content for training the model

Training or creating the model (and fine-tuning it)

Operating and offering the model

Using the model by providing input and generating output

Applicable Law: Data Protection; Personality Rights; Copyright; Other IP Rights; Professional Secrecy; Competition Law; General Regulations; AI Regulations; Contractual Duties

AI Ethics

Ethics

What goes beyond law
What stakeholders expect
Will differ from company to company

AI Regulations

Such as the EU AI Act (not yet in force)

Data Protection Issues

Fairness - processing not generally ok or acceptable for the people affected
Legal basis - there is no legal basis for the intended use of the data (if needed)
Transparency - people are not aware of their data being processed or how/why
Purpose limitation - used for a purpose for which data was not collected
Data minimization - too much data is being collected
Storage limitation - data is retained for too long or with access being to broad
Proportionality - data is processed only as suitable, necessary and acceptable
Correctness - data is incorrect for the purpose
Data security - data not sufficiently secure/protected against threats
Privacy by default - a default setting/processing is not the least invasive one
Automated decisions - decisions that can have material impact on the people
Objection - the data is used despite an objection by the people affected
Data subject rights - right of access, correction, objection, deletion, portability
Accountability - there is not sufficient documentation to show compliance
Consent - if relied upon does not fulfill the legal prerequisites for it to be valid
Export - transfer to third countries without adequate safeguards/exemptions
Use of processor - use of data processors without adequate contract/security
Joint controller - joint controllership without allocation of responsibilities

Personality Rights

Right to own picture - where input or output may violate it
Right to own name - where input or output may violate it

Copyright

Using protected third party works - without approval or fair use exemption
Failure to disclose authorship - when using generated output

Other IP Rights

Trademarks - usage of a mark as mark without approval
Patents - unauthorized use of a protected technical invention

Unfair Competition

Use of third party work results - without own relevant investment
Deception - a lack of transparency when using AI that is deceptive
Misleading customers - by wrong, misleading or missing information
Harming others - by disparaging them or providing misleading information

Anti-Trust

Anti-trust - illegal coordination among market participants (e.g., re prices)

Mit dem Einsatz generativer KI kommen weitere Ebenen hinzu

Generative AI Risk Assessment (GAIRA)

VISCHER

Danke für Ihre Aufmerksamkeit!

drosenthal@vischer.com

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