

VISCHER

Neues Datenschutzgesetz.

Erfahrungen und Praxishinweise für den
Personalbereich

David Rosenthal, Partner, VISCHER AG
25. Januar 2024



Von unserer "Meet me in prison"-Party am 31. August 2023

Foto: Matthias Glatthaar, VUD

Worum geht es?

- Seit dem 1. September 2023 ein neues **Datenschutzgesetz**
 - <https://www.fedlex.admin.ch/eli/oc/2022/491/de>
- Ähnlich wie die **EU DSGVO**, aber pragmatischer sowie weniger kompliziert und formalistisch, fast nirgends strenger
 - Was bisher erlaubt war, bleibt meistens weiterhin erlaubt
 - Für Arbeit sorgten vor allem die flankierenden Massnahmen (wie Datenschutzerklärung, Verzeichnis der Bearbeitungstätigkeiten, neue Prozesse, Verträge mit Providern, IGDTAs, Weisungen)
 - Für Diskussion sorgten vor allem die neuen, schärferen Bussen
- Die **Einführung** klappte vergleichsweise gut
 - Gute "Boardroom-Attention", wenig Interesse seitens Betroffener

Was änderte sich? Was ist neu?

Ausführliche kostenlose
Kommentierung:
<https://bit.ly/3kUfzqu>

1. Ausgebaute Pflicht zur **Datenschutzerklärung***
2. Pflicht für ein **Verzeichnis der Datenbearbeitungen**
3. Leicht strengere Vorgaben für **Auftragsbearbeitungen***
4. Pflicht zur **Datenschutz-Folgenabschätzung** in heiklen Fällen
5. Pflicht zur **Meldung von Sicherheitsverstößen** an EDÖB
6. Anpassung des **Auskunfts-* und Korrekturrechts**
7. Neues Recht auf **Datenportabilität** für Kunden
8. Regelung zu **automatisierten Einzelentscheiden***
9. Anpassung diverser **Begrifflichkeiten**
10. Aufsichtsinstrumente und ***Strafbarkeit ausgebaut**

Die Grundsätze
veränderten
sich nicht!

Die wichtigsten Massnahmen

- **Datenschutzerklärung** ("DSE") verfassen und publizieren
 - Alle planmässigen Datenerhebungen gehören rein
- **Bearbeitungsverzeichnis** ("ROPA") erstellen
 - Bearbeitungsaktivitäten nicht zu detailliert darlegen
- **Auftragsbearbeitungen** identifizieren & vertraglich regeln
 - Mit jedem Auftragsbearbeiter ist ein sog. AVV abzuschliessen
- **Weisung zum Datenschutz** erlassen und schulen
 - Verantwortlichkeiten und Prozesse intern festlegen und etablieren
- **Bearbeitungsreglement** verfassen, soweit vorgeschrieben
- **Datenschutz & Sicherheit einzelner Bearbeitungen** prüfen



Auch wo Personendaten von Mitarbeitenden erhoben werden

revDSG – was zu tun ist.

Für KMU
Umgesetzt: ☒
Neu ab 1.9.2023

10 Gebote zum Umgang mit Personendaten nach DSG¹

1. Wir **sagen** der Person vorher, was wir mit ihren Daten wozu tun.
2. Wir **halten uns daran** und setzen Daten nicht zweckwidrig ein.
3. Wir üben uns in **Datensparsamkeit** und "need-to-know".
4. Wir **löschen rasch**, was wir nicht mehr brauchen.
5. Wir erlauben einer Person auch **"Nein"** zu sagen.
6. Wir tun nur das, was wir bei uns selbst **akzeptabel** finden.
7. Wir prüfen unsere Daten auf problematische **Fehler** und Lücken.
8. Wir geben **sensitive Daten**² nicht für Zwecke Dritter weiter.
9. Wir treffen Massnahmen, damit die Daten bei uns **sicher** sind.
10. Wir beschaffen Daten auf **legale Weise** und aus legalen Quellen.

**Ausnahmen sind (nur) bei "besserem" Grund möglich.
Wir gestalten jede Datenbearbeitung nach diesen Geboten!**

2 Wenn Daten ins Ausland gehen

Problemlos: EWR, UK, angemessene Länder⁵

- 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 EU⁶ mit CH-Anpassung und keinen Grund zur Annahme haben, dass es zu problematischen Behördenzugriffen kommt (→ TIA machen!)⁷

Wir prüfen unsere Verträge daraufhin!

4 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)⁸, 1 Jahr⁹ 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 Daten² Bearbeitungsregeln.¹⁰

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://edobeb.admin.ch>) und für 2 Jahre dokumentieren; können sich Personen selbst vor Folgen schützen → Meldung auch an sie.

Jeder ist für Sicherheit mitverantwortlich!

2 Datenschutzerklärung "DSE"

Jede planmässige, gesetzliche nicht erforderliche Beschaffung von Personendaten ist in der Datenschutzerklärung ("DSE"). 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.³

1 Inventar der Bearbeitungen

Wir führen ein Verzeichnis unserer Aktivitäten, bei denen Personendaten bearbeitet werden (z.B. Verwaltung der Kundendaten, Buchhaltung, Personalhaltung, Personalrecherche). Aufgeführt ist der Inhalt gemäss Art. 12 revDSG, u.a. Bearbeitungszwecke, Kategorien von Personen, Daten und Empfänger, Aufbewahrungsdauer.⁴ Diese **Pflicht gilt nur**, falls wir 250+ Mitarbeiter (Köpfe) haben oder sensitive Daten² in grossem Umfang bearbeiten oder Hochrisiko-Profilung betreiben.

1 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 genehmigen¹¹ (oder ihm 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 Datenutzung für sich). Wir prüfen die heutigen/neuen ADV auf Konformität.

2 Wir gewähren Betroffenen ihre Rechte

Wir **identifizieren** die Person vorgängig richtig.

Wir geben einer Person **Auskunft** über ihre eigenen Personendaten (nicht Dokumente) und auf Wunsch bestimmte weitere Infos (i.d.R. gratis innert 30 Tagen). Wir vermeiden den Eindruck, es seien alle Daten gegeben (falsche oder unvollständige Auskunft ist strafbar). Wir können zuerst nur gängige Daten liefern. Die Person muss beim Finden mitwirken. Datenschutzfremde Zwecke sind nicht geschützt. Wir schützen Daten Dritter und eigene Geschäftsgeheimnisse.

Jede Person kann **Datenkorrektur** verlangen. Ist die Wahrheit umstritten, vermerken wird dies.

Jede Person kann **Löschung** ihrer Daten verlangen oder sonst wollen, dass wir unsere Bearbeitung stoppen oder ändern. Wir können weitermachen, falls wir einen besseren Grund dafür haben.

Trifft bei uns ein **Computer** Ermessensentscheide mit wichtigen negativen Folgen, sagen wir das den Betroffenen und bieten menschliches Gehör an.¹² In bestimmten Fällen müssen wir Personendaten, die wir erhalten und als Historie haben, den Personen zugesetzt Weiterverwendung **herausgeben**.

Wir stellen sicher, dass wir das können!

2 Wir verlassen uns nicht auf Einwilligungen

Wir stützen uns grundsätzlich nicht auf Einwilligungen. Falls doch, müssen sie **informiert** und **freiwillig** erfolgen, bei sensiblen Daten² und Hochrisiko-Profilung explizit.

2 Datenschutz Folgenabschätzung (DSFA)¹³

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 bewahren sie auf.

2 Kleines Berufsgeheimnis

Uns **anvertraute**, beruflich nötige Personendaten halten wir geheim oder wir stellen vorab 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!

¹ revDSG/DSV: <https://datenrecht.ch/gesetze/revdsg>

² Besonders schützenswerte Daten: Art. 5 Bst. c revDSG

³ Vgl. Musterdatenschutzerklärung auf <https://dsat.ch>

⁴ Vorlagen: <https://dsat.ch>, <https://bit.ly/3agp0lb>

⁵ Vgl. Anhang I der DSV (<https://bit.ly/3dm3d9n>)

⁶ Vgl. FAQ (mit Bezugsquellen): <https://bit.ly/3agv6z5>

⁷ Vgl. TIA: <https://bit.ly/3l3mxy0> (mit Verweis auf FAQ)

Fragen? (FAQ auf <https://bit.ly/3M6G6t1> und mehr auf <https://bit.ly/38Cm2qQ>)

Intern:

Extern:

Legende: ☒ Auftragsbearbeiter ☒ Verantwortlicher ☒ Prior. Umsetzung ☒ Umgesetzt

© VISCHER



Machen
Sie den Test auf
<https://privacyscore.ch>

Alles auf
einer Seite

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

Fokus 1: Auskunftsrecht

- **Ausgebaut:** Mehr Dinge, über die Auskunft erteilt werden muss
 - Generalklausel in Art. 25(2) DSGVO; nicht nur Datensammlungen
- **Eingeschränkt:** Einschränkungsmöglichkeiten
 - Neu: Begehren "offensichtlich unbegründet, namentlich *wenn es einen datenschutzwidrigen Zweck verfolgt*" (Art. 26(1)(c) DSGVO)
 - Neu: "Personendaten *als solche*"
- **Praxis:** Oft zur Beweismittelbeschaffung, für Vergleichsdruck
 - "Nachdem diese Zielsetzung offenkundig nicht mit derjenigen des DSGVO übereinstimmt" keine Berufung auf das Auskunftsrecht (Urteil 8C_723/2022, E 5.3 betr. Sozialversicherungsanspruch)
 - Indizien für eine datenschutzfremde, rechtsmissbräuchliche Berufung auf das Auskunftsrecht?

Indizien für datenschutzwidrige Zwecke

- Einsprache wegen Kündigung kombiniert mit Auskunftersuchen
- Auskunftsbegehren zu Leistungsbeurteilungen als Reaktion auf leistungsbedingte Kündigung oder schlechtes Zeugnis
- Auskunftsbegehren im Nachgang zu einer ordentlichen oder fristlosen Arbeitgeberkündigung
- Anwaltsvollmacht für datenschutzfremde Zwecke
- Übermässig weit gefasste Auskunftsbegehren, die im Schreiben des Anwalts zur Geltendmachung arbeitsrechtlicher Ansprüche noch als Zusatz ohne weitere Begründung angehängt sind
- Wenn konkrete "Unterlagen" (z.B. Performance Review) verlangt werden statt "Personendaten" als solche

<https://vischerlnk.com/3HozjAi>

Fokus 2: Sonderregeln für PKs

- Wer mit einer **öffentlichen Aufgabe** betraut ist, wird zum Bundesorgan und unterliegt strengeren Vorgaben gemäss DSG
- Pensionskassen, FAK, Freizügigkeitsstiftungen

Im Lichte dieser Ausführungen gilt es unseres Erachtens festzustellen, dass die Aufgabe einer Freizügigkeitseinrichtung des Erhalts des Vorsorgekapitals des BVG-Obligatoriums – obgleich zeitlich beschränkt – einen Teil der Durchführung der obligatorischen Versicherung und somit eine **Bundesaufgabe** darstellt. Die Freizügigkeitseinrichtung **muss für die Erfüllung dieser Bundesaufgabe Personendaten bearbeiten** (insb. muss sie die Versichertendaten speichern, damit sie diese der neuen Vorsorgeeinrichtung zu gegebener Zeit mitsamt der Austrittsleistung weiterleiten kann). Folglich handelt eine Freizügigkeitseinrichtung nach unserer Auffassung im Rahmen ihrer gesetzlichen Aufgaben als **Bundesorgan** i.S.v. [Art. 2 Abs. 1 lit. b](#) i.V.m. [Art. 5 lit. i DSG](#), vorbehältlich eines anderslautenden gerichtlichen Entscheids in der Zukunft.



<http://bit.ly/46XkMGF>

Auskunft des EDÖB

- Erfordernis gesetzliche Grundlage, **Bearbeitungsverzeichnis** (melden), Ernennung eines **Datenschutzberaters** (melden), **Bearbeitungsreglement**, DSFA, Meldung von Projekten an EDÖB, Protokollierung – und Ausnahme von Strafbestimmungen

Fokus 3: Strafbarkeit

"Mit Busse bis zu 250'000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich ..."

Strafrechtliche Verantwortlichkeit

- Auskunftsrecht
- Informationspflicht
- Pflicht zum AVV
- Bekanntgabe ins Ausland
- Datensicherheit
- Weisungen des EDÖB
- Berufsgeheimnis (tw.)

"Bei Widerhandlungen in Geschäftsbetrieben ... sind die Strafbestimmungen auf diejenigen natürlichen Personen anwendbar ..."

Durch Handeln

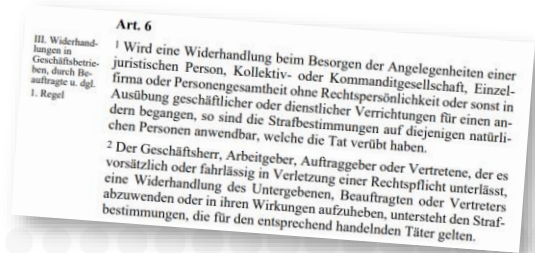
Jeder, der handelt

Durch Unterlassen

Wer eine
Garantenstellung hat

1. Person muss Pflicht haben, Rechtsverletzungen zu verhindern und die dafür nötigen Befugnisse
2. Sie kommt ihrer Pflicht zur sorgfältigen Auswahl, Instruktion und Überwachung nicht nach

VStrR



Beispiele:

- Wer in Kauf nimmt, eine falsche Auskunft an einen Betroffenen zu erteilen
- Wer entscheidet, die Datenschutz-Erklärung nicht wie erforderlich nachzuführen
- Wer als GL-Mitglied nicht dafür sorgt, dass Auskunftersuchen richtig behandelt werden
- Wer als leitender Inhaber einer Bearbeitung keine korrekte DSE in Auftrag gibt
- Der untätige VR, weil er keinen Bericht will

Die richtige Rollenverteilung

<https://vischerInk.com/425uANc>

- **Verwaltungsrat**
 - Oberaufsicht über die Einhaltung des Datenschutzes
 - Delegiert die Umsetzung an die GL
- **Geschäftsleitung**
 - Trifft die nötigen Massnahmen zur Umsetzung im Betrieb
 - Trifft die nötigen Entscheide zur Bearbeitung
- **Datenschutzstelle**
 - Erarbeitung der Vorgaben, Beratung in deren Umsetzung, Überprüfung deren Umsetzung, Inhaber Datenschutzprozesse
- **Inhaber der Datenbearbeitungen**
 - Treffen die nötigen Entscheide und sorgen für deren Umsetzung

Nicht nur Weisungen erteilen, sondern auch Reporting sicherstellen

Nur beraten, nicht entscheiden

Fokus 4: Datenschutz-Folgenabschätzung

- Wenn Aktivitäten zur Bearbeitung von Personendaten ein **hohes Risiko** für betroffene Personen mit sich bringen können, d.h. wenn es um eine "heikle" Anwendung geht (Art. 22 DSGVO)
 - Gesetzliche Fälle, namentlich bei umfangreicher Bearbeitung besonders schützenswerter Personendaten
 - Sonst: Schwellenwert-Prüfung (leider ohne klare Vorgaben)
 - Gilt an sich auch für bisherige Bearbeitungen, die weiterlaufen
- Eine Vorab-**Risiko-Beurteilung** aus Sicht der Betroffenen
 - Beschreibung der Aktivität, geplante/getroffene Massnahmen zur Mitigierung, Risikobeurteilung betr. mögliche negative Folgen
- **Meldung an den EDÖB**, falls ein "hohes" Restrisiko bleibt
 - Kommt in der Praxis nie vor

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 Arbeitsblattes.

Unternehmen (Verantwortlicher): Musterfirma AG

Abteilung: 1

Verantwortlich intern: 2

Status der DSFA: 3

Name des Vorhabens: 4

Aktivität gemäß Bearbeiter: 5

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 und... 1.05 Welche Dritten an... 1.06 Welche Daten bes... 1.07 Wessen Daten bes... 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:

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

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.

10 Risiken vorschlagen (überschreibe bisherige Werte)

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)
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 .	- 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.				

2.02 Warum die Datenbearbeitung datensparsam, zeitlich auf das nötige begrenzt und auch sonst verhältnismässig ist:

Zugriff 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)

Der Blick nach vorne ...

- Viele Unternehmen **experimentieren** mit GenKI
 - Auch Schweizer Finanzinstitute (mit CID)
 - Legal & Compliance tendenziell noch überfordert, wird sich legen
- **Datenschutzkonformer Einsatz** ist grundsätzlich möglich
 - Hauptthemen bei Klienten sind Richtigkeit, CID, Data Leakage, Verträge mit Providern, Betroffenenrechte, Transparenz
 - Die meisten GenKI-Projekte sind auch Cloud-Projekte
 - Bestehende Regelungen lassen sich gut anwenden; das neue DSG regelt zudem bereits "automatisierte Einzelentscheide"
 - Herausforderung: Überblick, Legal Bottleneck, Risiko-Beurteilung
- Nicht verwechseln mit **ethischen** Vorgaben bzw. Erwartungen



www.vud.ch

Ein Beispiel

Lebenslauf	
	
Persönliche Daten:	
Name:	Mustermann
Vorname:	Stephan
Adresse:	Musterstrasse 23, 3000 Musterstadt
Telefon:	077 XX XXX XX
E-Mail:	stephan.mustermann@musterstadt.ch
Geburtsdatum:	03.06.1978
Zivilstand:	ledig, keine Kinder
Berufliche Erfahrungen:	
02/2004 – heute	Muster AG, Bern: Marketingkoordinator, Betreuung von Print- und Offlinekampagnen, Organisation der Messeauftritte, Vorbereitung und Durchführung von Kundenevents
02/2000 – 01/2004	Marketing Verlag Basel: Marketingfachmann, Anzeigenerstellung und -schaltung, Erstellen von Produktflyern und Prospekten, Direktwerbung
07/1998 – 01/2000	Marketing Zeitung Olten: Marketingassistent, Vorbereiten von Statistiken, Unterstützung bei der Marketingplanung und -umsetzung
Ausbildung:	
05/1999 – 05/2000	HSO Schulen Thun Bern AG: «Abschluss als Marketingplaner»
08/1994 – 08/1997	Wirtschafts- und Kaderschule KV Bern: «Abschluss als Kaufmann E-Profil»

Sprachen:	
Deutsch:	Muttersprache
Englisch:	schriftlich und mündlich sehr gut
Französisch:	schriftlich und mündlich gut
Spezielle Fähigkeiten:	
	• Erstellen von 3D-Animationen • Erfahrung im Umgang mit Adobe Photoshop • selbständige und strukturierte Arbeitsweise
Freizeit:	
	Asiatische Küche, Tennis, Basketball, Städtereisen
Referenzen:	
	Auf Anfrage

Was sagt die KI dazu?

Prompt: "Du bist der weltbeste Personalchef und hast ein feines Gespür für Warnsignale in Lebensläufen von Bewerbern. Schau Dir folgenden Lebenslauf sehr genau an und erkläre mir, welche Punkte auf mögliche Probleme bei diesem Kandidaten hinweisen:"

Quelle:

https://www.jobscout24.ch/download/vorlagen/Lebenslauf_Marketing.pdf

Das ist ihre Antwort ...



"Es gibt keine Hinweise auf kontinuierliche Weiterbildung oder berufsbegleitende Schulungen oder Kurse, die Marketingplaner absolviert w... schnell verändernden Feld w... könnte dies bedeuten, dass auf aktuelle Trends und Tech... neuesten Stand ist."

Müsste einer Person gesagt werden, dass ihr CV vor dem Interview auf diese Weise geprüft wird?

und Adobe Photoshop Fähigkeiten nicht direkt in Verbindung zu... dass der Kandidat... at oder dass er über... Kommunikationen verfügt, die er möglicherweise nicht vollständig nutzen konnte."

"Wenn jemand über einen längeren Zeitraum bei demselben...
Rechtlich: Nein, da nichts getan wird, was Unternehmen sonst nicht auch tun und erwartet wird, aber die Richtigkeit der Antwort muss hinterfragt werden seiner Karriere voranzukommen."

"Stephan Mustermann ist seit über 19 Jahren bei...
Ethisch: Bewerber warnen? Ihnen die Wahl lassen?
Veränderungen hat oder in seiner Entwicklung stagniert. Es könnte auch bedeuten, dass er wenig Anpassungsfähigkeit oder Motivation zur persönlichen Weiterentwicklung zeigt."

GenKI: Zehn Fragen für die Praxis

1. Wo wird der **Input** ("Prompts") hingesandt und bearbeitet?
2. Besteht mit dem Provider ein **Auftragsdatenbearbeitungsvertrag**?
3. Ist die **Datensicherheit** (und das Berufsgeheimnis) gewährleistet?
4. Wird der Input für das **Provider-Training des Modells** benutzt?
5. Welche **Inhalte** dürfen Mitarbeitende an die KI übermitteln?
6. Wird der Output vom Provider **geprüft** (z.B. "Abuse Monitoring")?
7. Wie gehen wir mit **fehlerhaftem/ungewolltem Output** um?
8. Muss und kann "**Data Leakage**" vermieden werden?
9. Müssen oder wollen wir auf die KI-Verwendung **hinweisen**?
10. Welches Konzept besteht die Erfüllung von **Betroffenenrechten**?



Doing a risk assessment with GAIRA Light

To assess your AI application project using GAIRA Light, you need to take the following steps:

- Identify the AI application
- Describe the AI application
- Check for prohibited activities
- Check for need for a consent
- Answer questions to non-compliance housekeeping
- Answer questions regarding compliance housekeeping
- Answer 14-23 risk questions
- Decide on implementation
- Get the GDPR impact form or other checklist

Step 4: Conclusion

Instruction: Once you have come to step 4, you are almost done. The first time below will give you a recommendation based on the above responses you have made. Let the 2nd line functions and other stakeholders (e.g., other business functions with whom you have discussed your risk assessment) add any comments they wish and consider them. At the end, you are asked to assess the overall risk level of your application (low, medium, high, very high) in terms of the risk for the organization. The value can then be used for the Records of AI Activities (ROIAs). Finally, record your decision as how you wish to proceed and provide any comments you deem fit for the record (don't forget to update the status and date in the top section of the form).

Assess	Reason Ind. measures taken/planned	Assessment	2nd Line Comment	By whom?	Risk level
Yes		OK			
Yes	We have the EU SCC in place with a TIA.	OK			
Yes		OK			
No		Warning!	DPO	Accepted	
Yes	No amendment is necessary.	OK			
Yes		OK			

Assess	Reason Ind. measures taken/planned	Assessment	2nd Line Comment	By whom?	Risk level
Yes		OK			
Yes		OK			
Yes	We have opted out.	OK			
Yes		OK			

Recommendation: Your application does not appear to have any unacceptable risks. You can proceed, subject to any other objections or changes to your answers above.

Comments or objections by 2nd Line: No comments.

Comments or objections by others:

Overall risk level: Low (to be assessed by the application owner; please include this in the ROIAs)

Decision on how to proceed: Implementation (to be taken by the application owner)

Comments by application owner:

Video für Mitarbeitende zum Einsatz von KI



Das Video darf im Betrieb frei verteilt werden; individuelle Fassungen sind möglich

Es existiert in D, E und F



vischerlnk.com/ki-intro

[http://www.youtube.com/@VISCHERLegalInnovationLab](https://www.youtube.com/@VISCHERLegalInnovationLab)

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



AIgen

Abonnieren Sie unsere
Blog-Serie zum Thema KI
auf vischer.com/ki