Hinweisgeber und sichere Kommunikation

Data-Hosting in CH, Anwaltsprivileg, KI-gestützte Compliance

Prof. Dr. Patrick Krauskopf

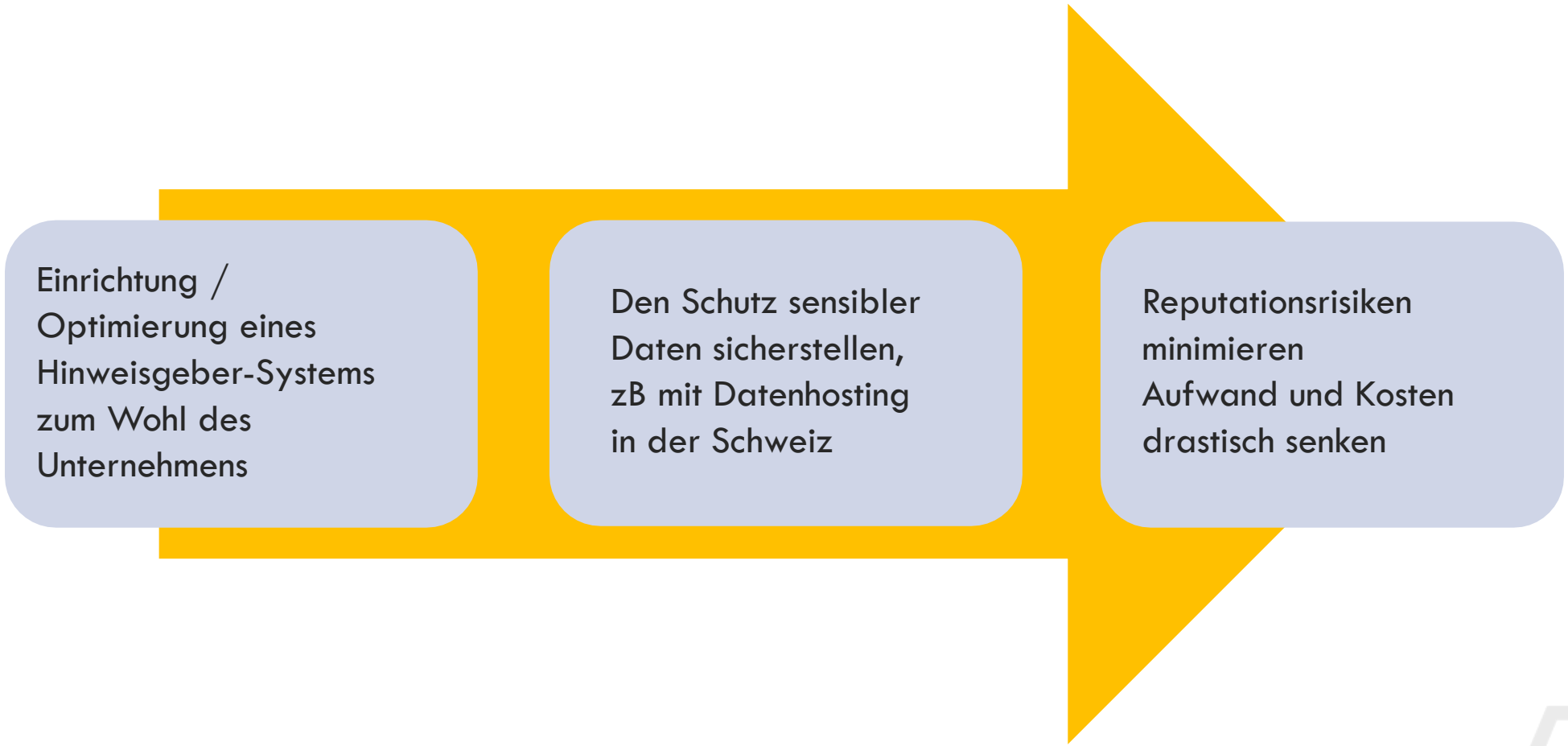
Mona Fahmy

Tobias Gurtner

Agenda

I. Begrüssung und Einführung
II. Case Study
III. Digitale Souveränität
IV. Legal Privilege
V. AGON Hinweisgeber Hotline
V. 80% Aufwand- und Kostenreduktion mit KI
VI. Wichtige Links

I. Begrüssung und Einführung



II. Case Study

- Mögliche Betrugsaspekte bei der RUAG MRO Holding AG im Zusammenhang mit Geschäften mit den Kampfpanzern Leopard 1 und 2
- Die Eidg. Finanzkommission EFK kommt in ihrem Bericht zum Schluss, dass es ausreichend Hinweise auf Betrug gebe, insbesondere durch ein ehemaliges Kadermitglied mit Doppelfunktion in der Schweiz und Deutschland.
- Ende August 2019 schrieb ein Hinweisgeber eine „sehr gezielte“ Meldung and die Vorsteherin VBS und den VR der RUAG.
- In der Meldung wurden Transaktionen, Geschäftspartner und Modus Operandi konkret beschrieben.

II. Case Study – der Fall RUAG

- Meldung wurde ans Kader weitergeleitet, u.a. an den Vorgesetzen des Beschuldigten.
- Dieser leitet die Meldung dem Beschuldigten weiter zur Stellungnahme.
- Beschuldigter gab Entwarnung – GL, VR und VBS gaben sich zufrieden.
- Mutmasslicher Betrug ging über Jahre weiter.
- Eine Prüfung der Meldung fand **nicht** statt!
- Keine Weiterverfolgung der Meldung laut EFK „unverständlich“

II. Case Study – der Fall RUAG

Aus dem EFK-Bericht:

- Für die EFK ist es unverständlich, dass weder der Verwaltungsrat noch weitere informierte Personen der Geschäftsleitung und des Managements die Stellungnahme nachweislich kritisch hinterfragten. …..
- Die zeitliche Abfolge und Qualität der Stellungnahme lässt darauf schliessen, dass eine seriöse und unabhängige Aufarbeitung nicht im Vordergrund stand…..
- Diese konkrete Whistleblowing-Meldung hätte der RUAG eine unabhängige Untersuchung ermöglicht. Dass dies nicht erfolgt ist, ist unverständlich.
- Der Umstand, dass die Meldung RUAG-intern an das verdächtigte Kadermitglied weitergeleitet wurde , obwohl aus der Meldung implizit zu vermuten war, dass die Vorwürfe ihre Zuständigkeit betreffen, ist nicht nachvollziehbar. Damit besteht auch das Risiko, dass wichtige Dokumente zur Klärung vernichtet wurden.

II. Case Study – Lessons learned

Fazit:

- Die Meldung von 2019 wurde zwar empfangen, aber nicht wirksam behandelt.
- Es bestand weder eine unabhängige Prüfung, noch wurde sie der zuständigen externen Stelle gemeldet.
- Der Umgang offenbart grundlegende Mängel im Compliance-Management, sowohl strukturell als auch kulturell.

→ **Ein KI-gestütztes, rechtssicheres Hinweisgebersystem hätte entscheidende Schwächen im Umgang mit Hinweisgebermeldungen wirksam adressieren können.**

II. Case Study – Lessons learned

1 Unabhängigkeit und Vertraulichkeit

Problem: WB-Meldung an Beschuldigten weitergeleitet / Interessenkonflikt

KI-gestützte Lösung: System stellt interne und externe Trennung sicher. Vertraulichkeit des Hinweisgebers wird durch technische und organisatorische Massnahmen garantiert.

2 Automatisierte Risikoanalyse und Priorisierung

Problem: Keine vertiefte Untersuchung. Beschuldigter kommentiert Vorwürfe.

KI-gestützte Lösung: Automatische Analyse der Hinweise, Identifikation relevanter Risiken, objektive Priorisierung. Schwerwiegende Hinweise gehen nicht unter und werden nicht bagatellisiert.

II. Case Study – Lessons learned

3 Transparente und dokumentierte Prozesse

Problem: Keine externe Meldung an EFK, keine Prüfung, keine Dokumentation

KI-gestützte Lösung: Jede Phase des Hinweisbearbeitungsprozesses wird automatisch dokumentiert.

4 Rechtssicherheit

Problem: Gesetzlich geschützter Meldeweg nicht genutzt, interne Regeln verletzt.

KI-gestützte Lösung: gesetzeskonforme Meldekanäle, Leitung und Schutz der Hinweisgeber.

III. Digitale Souveränität

Geopolitische Relevanz

- Strategische Priorität Europas: Reduktion technologischer Abhängigkeit.
- Herausforderung: Dominanz US-amerikanischer Cloud-Anbieter hinterfragt.

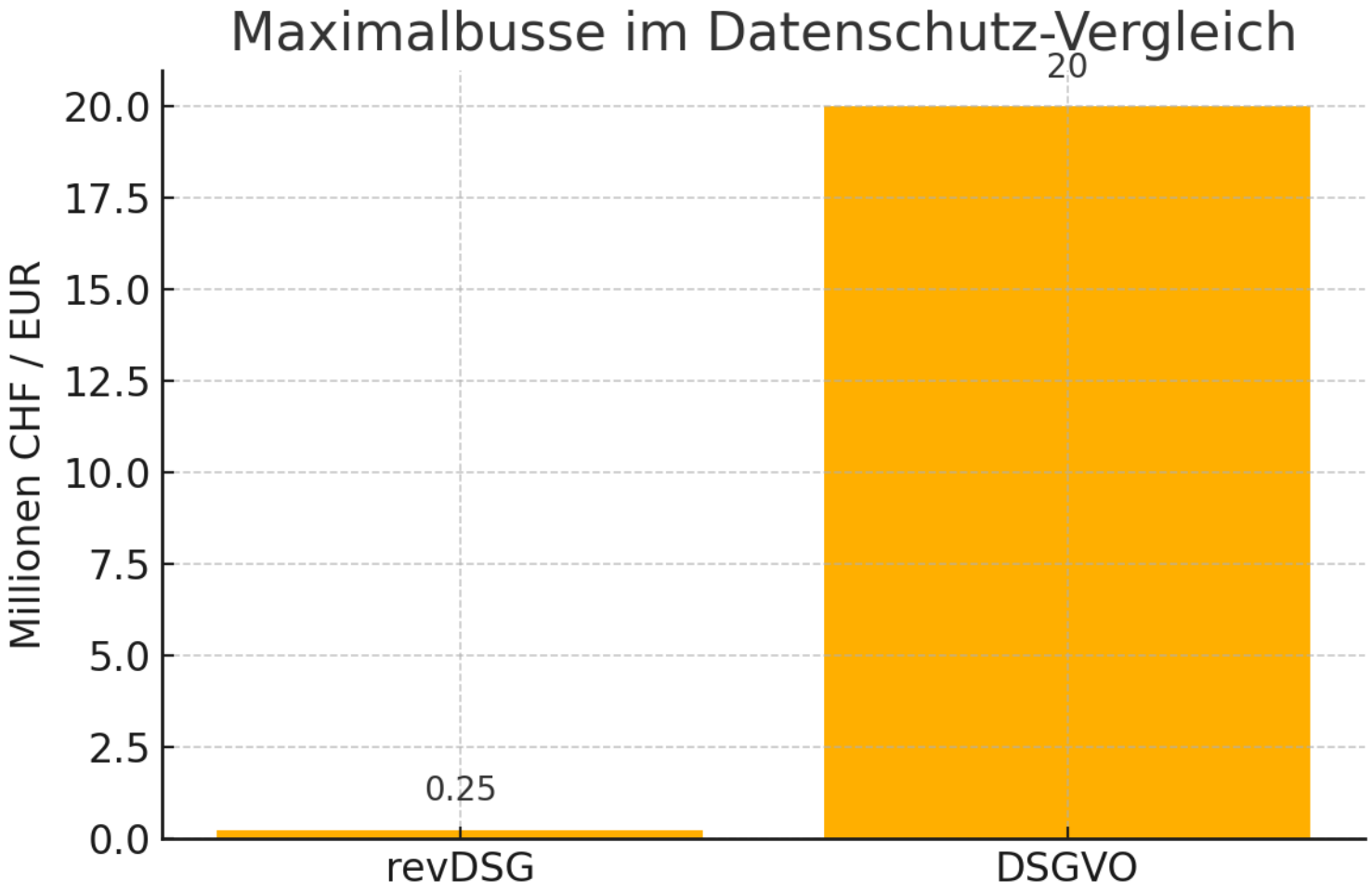
Lokales Datenhosting (CH/EU)

- Schweizer Rechenzentren: Lokale Kontrolle & strenger Datenschutz (revDSG, ähnlich DSGVO).
- US CLOUD Act: Kein direkter Zugriff auf CH-gehostete Daten (formelles Rechtshilfeverfahren nötig).

revDSG vs. DSGVO – Kernvorteile

- Moderner Datenschutzstandard, weniger bürokratisch, dennoch EU-konform.
- Bussgeld max. CHF 250’000 (statt DSGVO: bis 4 % Umsatz).
- Datenschutzbeauftragter empfohlen, nicht zwingend.
- Einwilligungspflicht enger gefasst (nur hohes Profiling-Risiko).

III. Digitale Souveränität



III. Digitale Souveränität

Compliance & Rechtssicherheit

- Lokales Hosting minimiert transatlantische Rechtsrisiken (US CLOUD Act vs. DSGVO).
- Klarheit bei Drittland-Transfers nach Privacy-Shield-Ende.
- Unabhängige Schweizer Aufsicht (EDÖB) stärkt Compliance.

Adressierung von Pain Points

- Misstrauen gegenüber US-Clouds (CLOUD Act, FISA, Datenschutz-Verstösse).
- Lokale Datenhaltung schafft Vertrauen, klare Rechtslage, Schutz vor unberechtigtem Zugriff.

IV. Legal Privilege

Legal Privilege bezeichnet das Recht auf Vertraulichkeit rechtlicher Kommunikation zwischen einem Klienten und einem Rechtsanwalt.

In der Schweiz spricht man vom «**Anwaltsgeheimnis**» (Art. 321 StGB).

Ziel: **Schutz** der Kommunikation mit unabhängigen, zugelassenen RechtsanwältInnen gegenüber Dritten, Behörden, Gerichten.

Grundsatz: Ohne Entbindung dürfen Anwälte keine Informationen offenlegen.

IV. Legal Privilege

Wer ist geschützt?

Nur selbständige AnwältInnen **mit Eintrag** im Anwaltsregister

➡ InhouseJuristInnen und Unternehmensberater sind **nicht** geschützt

Was ist geschützt?

- Kommunikation zur rechtlichen Beratung
- Dokumente, Memos, Gutachten, Notizen
- Elektronische Kommunikation, wenn eindeutig anwaltschaftlich und vertraulich

IV. Legal Privilege

Was ist nicht geschützt?

- Inhouse-Juristen: gelten laut Bundesgericht nicht als unabhängig
- Nicht-rechtliche Beratung, zB Business-Strategie, PR
- Straftaten oder Missbrauch des Privilege

Gerichte prüfen im Streitfall **inhaltlich**, ob die Kommunikation dem anwaltlichen Berufsgeheimnis unterliegt.

IV. Legal Privilege

Wann greift das Anwaltsgeheimnis **beim Whistleblowing**?

1. Die Kommunikation erfolgt mit unabhängigen, zugelassenen AnwältInnen

- Nicht geschützt ist Kommunikation mit Inhouse-JuristInnen– auch wenn sie über Anwaltspatent verfügen.

2. Der Inhalt betrifft die rechtliche Beratung oder Beurteilung, zB

- rechtliche Risiken für den Arbeitgeber
- Schutz des Whistleblowers
- Vorbereitung interner Untersuchungen

IV. Legal Privilege

Wann greift das Anwaltsgeheimnis **beim Whistleblowing**?

3. Die Kommunikation ist klar vertraulich

- Keine Veröffentlichung
- Kein Weiterleiten ohne Zustimmung
- Dokumente sind „vertraulich“ o.ä. gekennzeichnet

IV. Legal Privilege

Wann greift das Anwaltsgeheimnis beim Whistleblowing **nicht**?

- Wenn der Hinweisgeber ohne anwaltliche Beratung an eine interne Meldestelle geht
- Wenn der WB anonym mit Medien oder Behörden kommuniziert
- Wenn der Anwalt andere Rollen einnimmt (zB HR)

IV. Legal Privilege

Relevanz für Unternehmen:

- Vertraulicher Rechtsrahmen für Risikoanalysen
  - Interne Abklärungen zu Haftung, Compliance, Steuerfragen
- Schutz bei Behördenanfragen und Verfahren
  - zB Verfahren der FINMA, Weko, Staatsanwaltschaft
- Keine unfreiwillige Datenfreigabe an Behörden oder weitere Dritte
  - Besonders wichtig bei Durchsuchungen (Art. 264 ff. stopp)

CH Server + Legal Privilege = doppelte Absicherung!

V. AGON Hinweisgeber Hotline

HINWEIS PER POST KUMMERKASTEN

- \+ Kostengünstig
- – Nicht dialogbasiert
- – Zeitliche Verzögerung
- – Dokumentation

DIALOG UND VERFÜGBARKEIT EINGESCHRÄNKT

TELEFON HOTLINE

- \+ Direktes Feedback vom Gesprächspartner
- – Sprachbarriere
- – Kostenintensiv

DIALOG NUR BEDINGT GEWÄHRLEISTET

E-MAIL-SYSTEM

- \+ Hohe Bekanntheit
- – Keine anonyme Kommunikation
- – Tracking von Email

ANONYMITÄT NUR BEDINGT GEWÄHRLEISTET

AGON Hinweisgeber Hotline

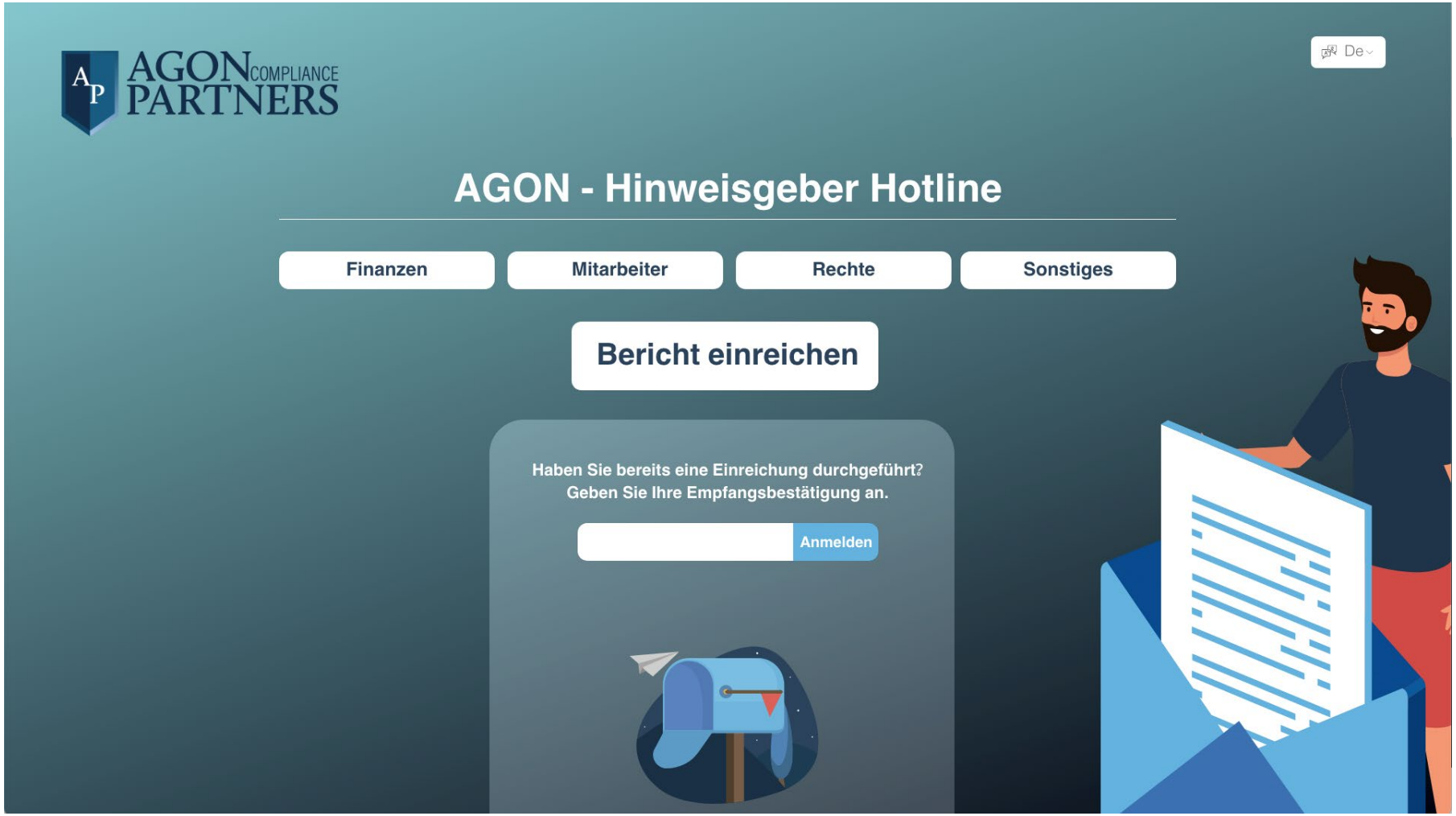
- \+ Weltweite 24/7 Falleingabe und -bearbeitung
- \+ Höchste Verschlüsselung
- \+ Dialogfähige Kommunikation
- \+ Zeit- und Geldersparnis
- \+ Video und Telefon mit Anonymisierung

GEWÄHRLEISTUNG VOLLER KONFORMITÄT

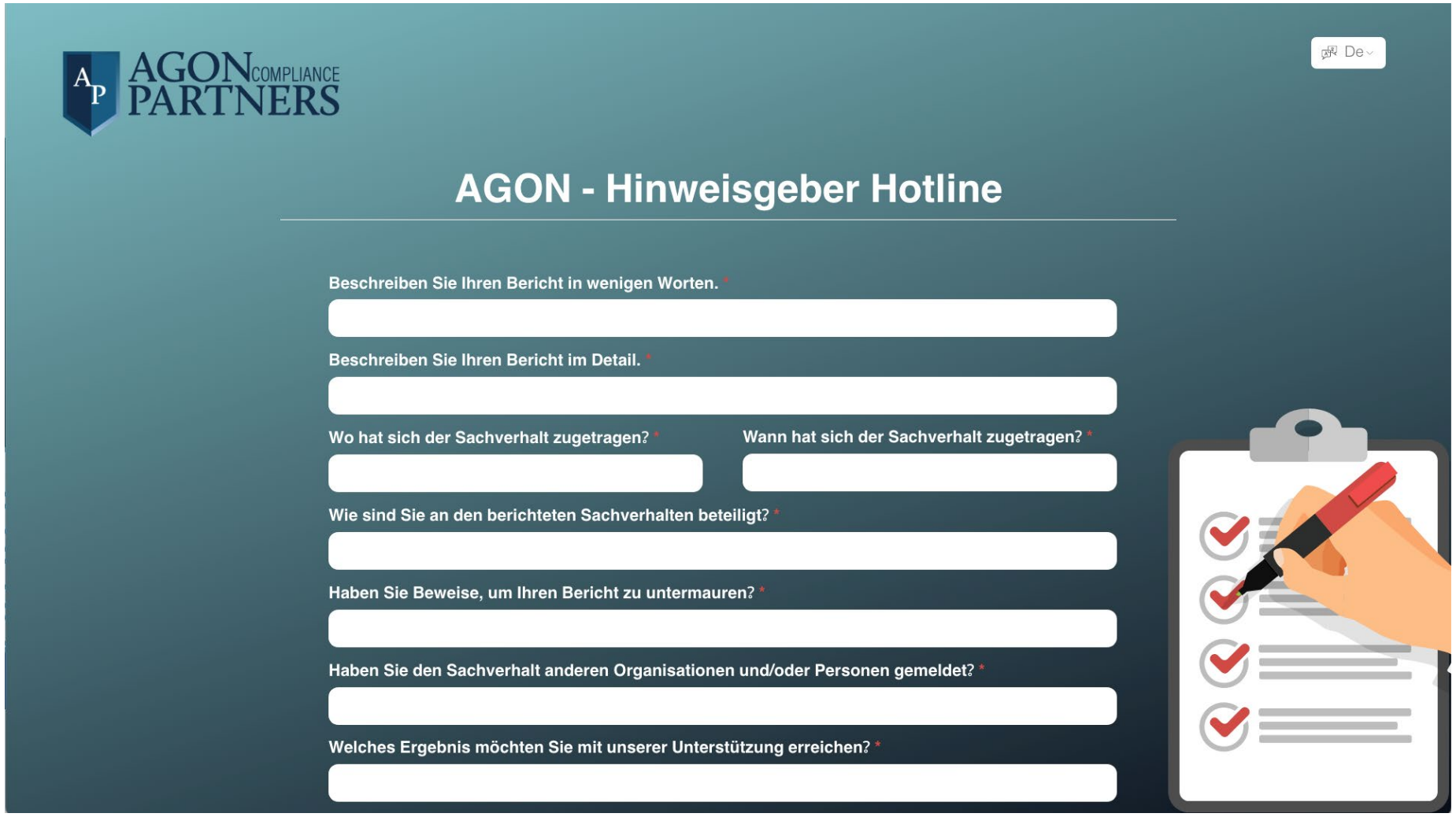
V. AGON Hinweisgeber Hotline

- Unterstützung für **mehr als 90 Sprachen**
- Unterstützung bei der Zuweisung und Erstellung von Case-Management-Status
- Anpassbares Erscheinungsbild (Logo, Farbe, Stile, Schriftart, Text)
- Verwalten Sie mehrere Whistleblowing-Websites über ein einziges Dashboard
- Überlassen Sie es den Hinweisgebern, ob und wann sie ihre Identität vertraulich preisgeben
- Sicherheits-Chat mit dem Hinweisgeber zur Erläuterung des Hinweises
- Einfache Empfängerschnittstelle zum Empfangen und Analysieren von Berichten
- Unterstützung für die Hinweisgebersuche von Berichten
- **Weltneuheit** .. Hochsichere Video und Telefon-Konfererenz mit Anonymisierung und Verschlüsselung und Transkription.

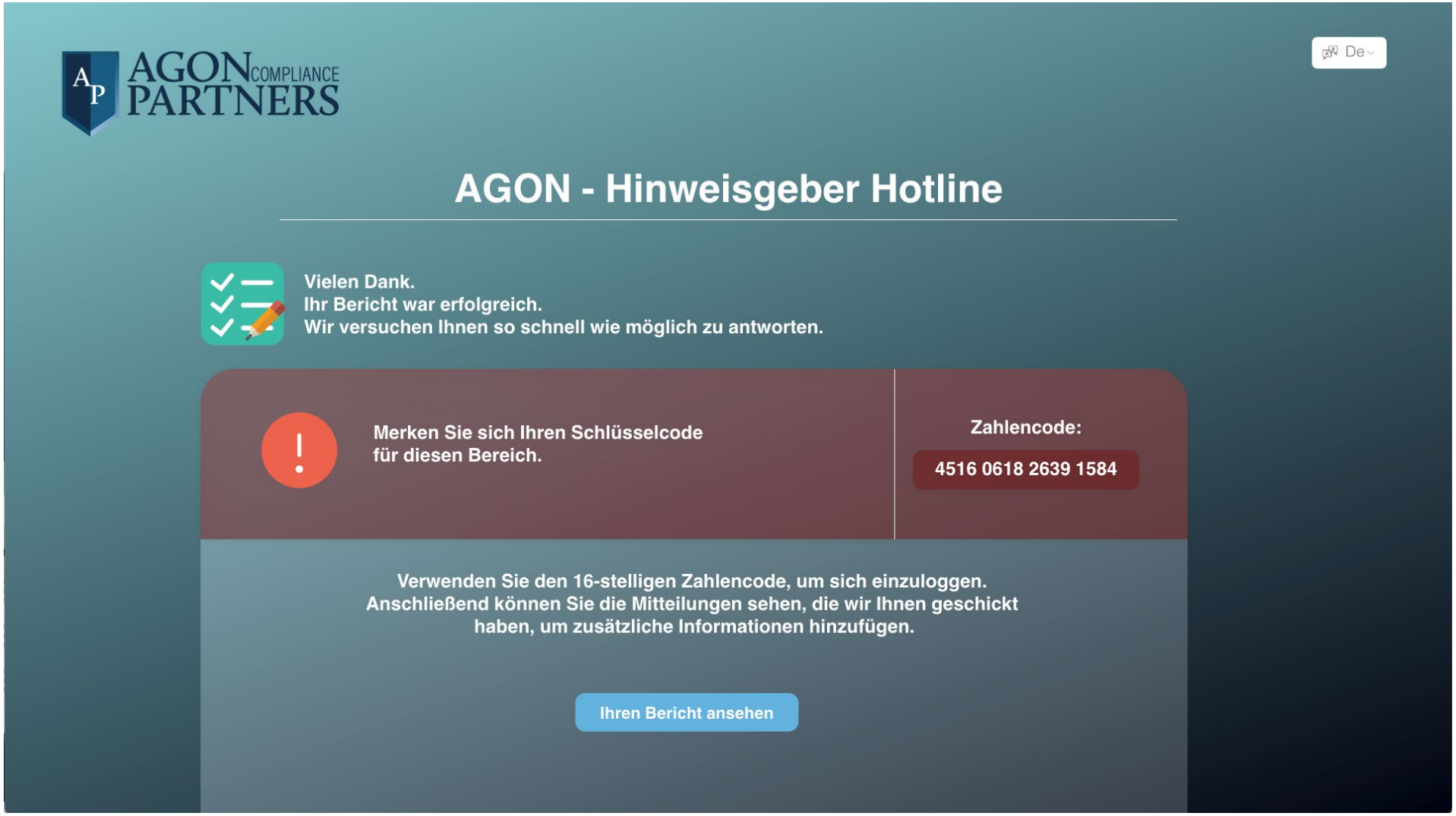
V. AGON Hinweisgeber Hotline



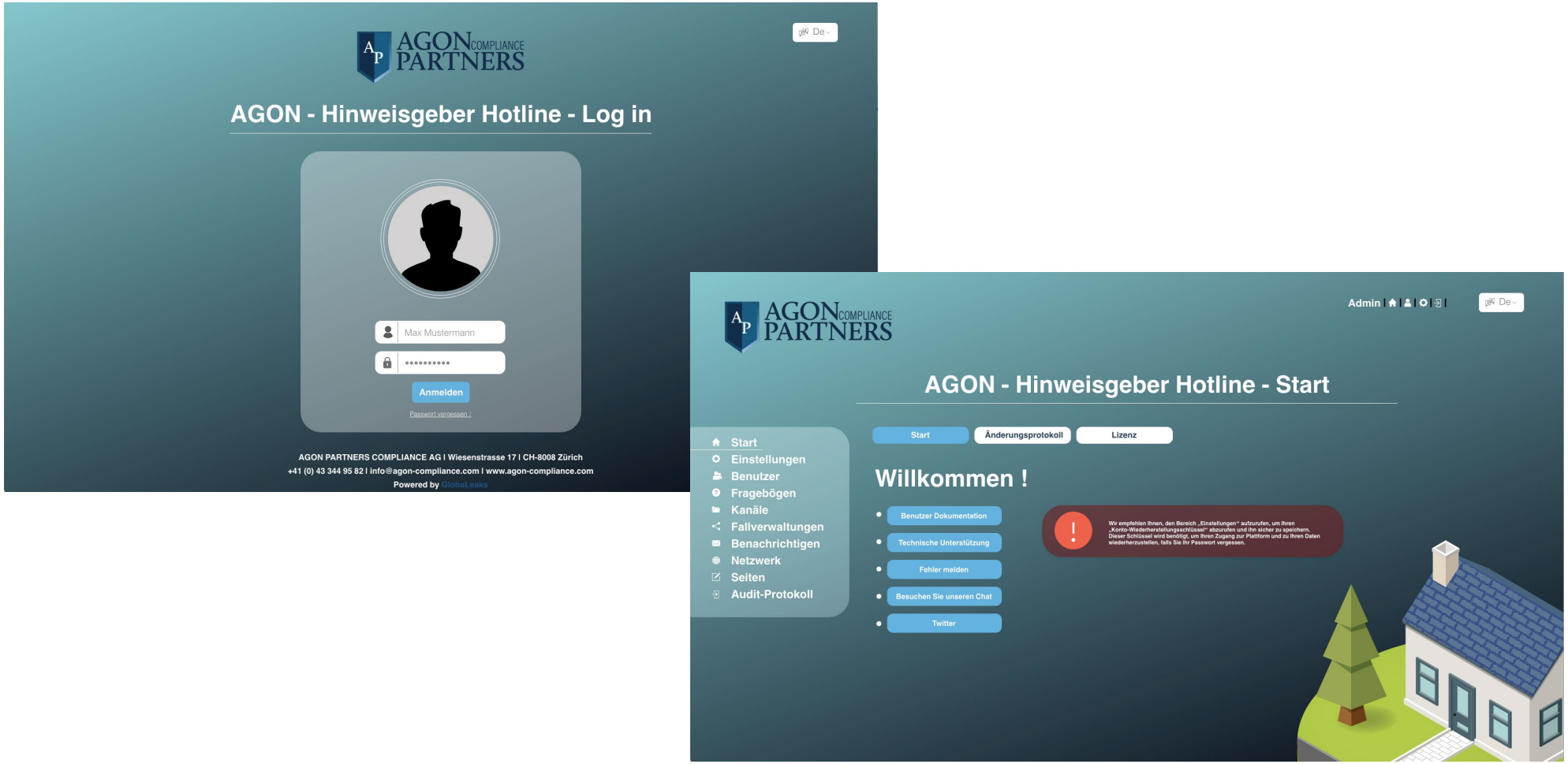
V. AGON Hinweisgeber Hotline



V. AGON Hinweisgeber Hotline



V. AGON Hinweisgeber Hotline



VI. 80% Aufwand- und Kostenreduktion mit KI

Whistleblowing-Prozess mit KI:

- Automatische Vorqualifizierung eingehender Meldungen
- Chatbots und Web-Formulare erfassen und anonymisieren Hinweise
- NLP analysiert Inhalte und priorisiert Risikostufen, Reduktion manuellen Aufwands

Automatisierte Risikoerkennung:

- KI erkennt Muster und Anomalien in grossen Datenmengen
- ML-Modelle bündeln ähnliche Vorfälle und bewerten deren Glaubwürdigkeit
- Echtzeitanalyse von Transaktionen identifiziert Betrug frühzeitig, schnell und objektiv

V. 80% Aufwand- und Kostenreduktion mit KI

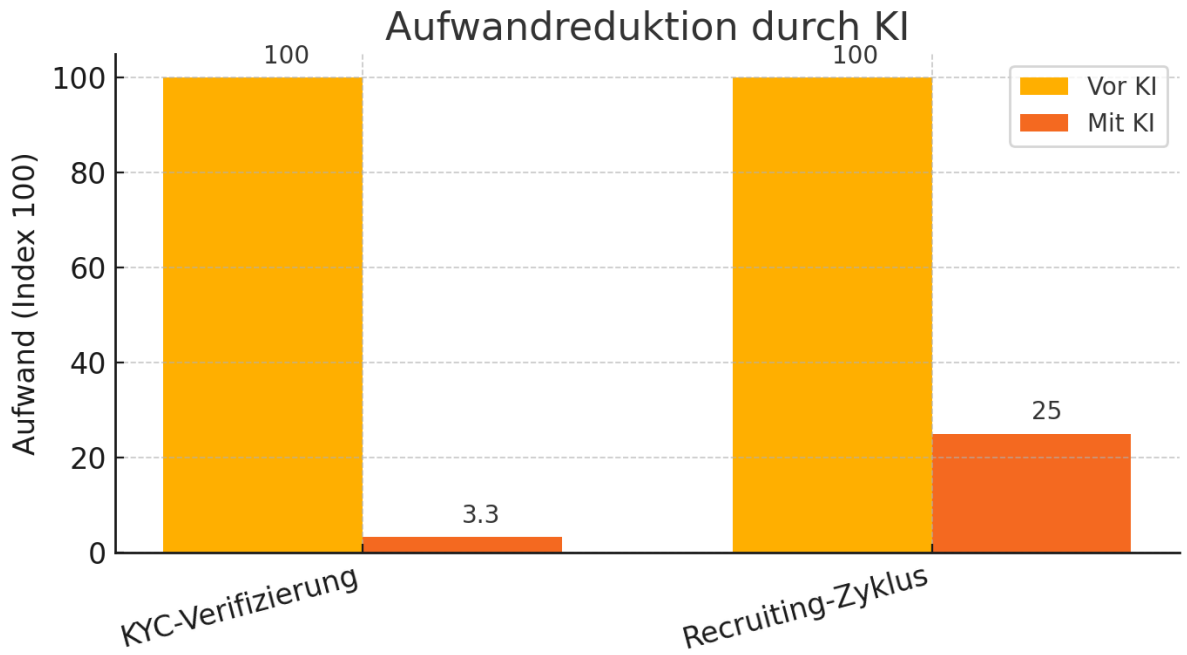
Automatisierte Dokumentation & Reporting:

- KI-basierte Dokumentation aller Bearbeitungsschritte lückenlos
- Automatische Erstellung von Berichten und Fallzusammenfassungen für Management und Aufsichtsbehörden
- Reduktion manueller Fehlerquellen, vereinfachte Audits

Effizienzsteigerung um bis zu 80 %:

- KI automatisiert repetitive Aufgaben (Beispiel: KYC-Prozess verkürzt von 2 Stunden auf 30 Sekunden)
- Ermöglicht Fokus auf kritische und komplexe Compliance-Aufgaben

V. 80% Aufwand- und Kostenreduktion mit KI



Prozess	Aufwand vor KI	Aufwand mit KI	Zeitersparnis
KYC-Verifizierung	18 min	0,6 min	-97 %
Recruiting	100 %	25 %	-75 %

V. 80% Aufwand- und Kostenreduktion mit KI

- **Branchenübergreifende Use Cases:**
  - **HR:** KI-gesteuertes Bewerber-Screening reduziert Einstellungsdauer (z.B. 75 % Zeitersparnis bei Unilever)
  - **Legal:** KI-basierte Vertragsprüfung spart 50 % Zeit, reduziert Fehlerquote
  - **Finance:** KI erkennt Transaktions-Anomalien in Echtzeit, verbessert Betrugsprävention und Risikomanagement drastisch

VI. Wichtige Links

AGON COMPLIANCE
https://agon-compliance.com/

AGON PARTNERS EVENTS
https://agon-partners.com/academics-events

AGON SOLUTIONS
https://agon-solution.ch/de/

Hinweisgeger Hotline Safe2 Whistle ->
https://agon-solution.ch/de/produkte/hinweisgeberhotline

Vielen Dank für Ihre Aufmerksamkeit!