# Informationssicherheit in Übersetzungsprozessen

Unternehmen tun viel, damit die auf dem Server befindlichen Daten sicher sind. Dazu gehören Back-up-Routinen, Firewalls und auch deklarierte Prozesse und Regularien. Sobald Dokumente jedoch zur Übersetzung an externe Dienstleister geschickt werden und das Haus verlassen, ist ohne entsprechende Maßnahmen die Informationssicherheit nicht mehr gewährleistet. Das damit verbundene Risiko wird oft unterschätzt. Dieses White Paper beschreibt, wie Unternehmen Informationen vor Manipulation, Diebstahl, Verlust und unerwünschter Weitergabe an Unbefugte schützen können.

# Inhalt

# Informationssicherheit in Übersetzungsprozessen

Grundsätzlich sind Informationen wie Produktideen, Visionspapiere, anzumeldende Patente, Marketing-Kampagnen oder Geschäftsberichte für Unternehmen sehr wertvoll und können einen Wettbewerbsvorteil darstellen oder vor Schaden bewahren. Um sie vor Verlust, Diebstahl, unerwünschter Weitergabe und Manipulation zu schützen, ist für deren Erstellung, Aufbewahrung, Verarbeitung und Weitergabe ein verantwortungsvoller Umgang erforderlich. Diese Informationssicherheit hat die ISO/IEC 20000 definiert: „Informationssicherheit ist das Ergebnis eines Systems von Strategien und Verfahren zur Identifizierung, Kontrolle und zum Schutz von Informationen und Geräten, die im Zusammenhang mit ihrer Speicherung, Übermittlung und Verarbeitung genutzt werden."

**Auf Basis dieser Definition lassen sich drei Ziele ableiten, die über verschiedene Maßnahmen erreicht werden können:**

- **Verfügbarkeit:**
  Hardware, Software, Daten
- **Integrität:**
  Unerwünschte Änderungen von Daten verhindern
- **Vertraulichkeit:**
  Sensitive Daten vor nicht autorisiertem Zugriff schützen

**Als mögliche Bedrohungen kommen folgende Kategorien in Betracht:**

- **Höhere Gewalt:**
  Feuer, Wasserschaden, Blitzschlag
- **Organisatorische Mängel:**
  Fehlende Verantwortlichkeiten, unzureichende Zugriffskontrolle
- **Fehlerhafte Handlungen durch den Menschen:**
  Benutzerfehler, Verwechslung von Daten
- **Technisches Versagen:**
  Stromausfall, Festplattenfehler
- **Vorsätzliche Handlungen:**
  Diebstahl, Manipulation, Computerviren

Im eigenen Unternehmen sind üblicherweise in einem Compliance-Management entsprechende Maßnahmen hinterlegt, die vor diesen Bedrohungen schützen. Bei der Übersetzung von Dokumenten bestehen hinsichtlich solcher Maßnahmen besondere Herausforderungen. Dennoch wird der Informationssicherheit bei der Zusammenarbeit mit Sprachdienstleistern häufig noch zu wenig Beachtung geschenkt.

## Risikolücken in Übersetzungsprozessen

Übersetzungsprozesse sind verteilte Prozesse mit zahlreichen Akteuren, die dem Auftraggeber nicht unbedingt bekannt sind. In der Regel beauftragen Unternehmen Sprachdienstleister oder Freelancer mit der Lokalisierung. Der Sprachdienstleis-

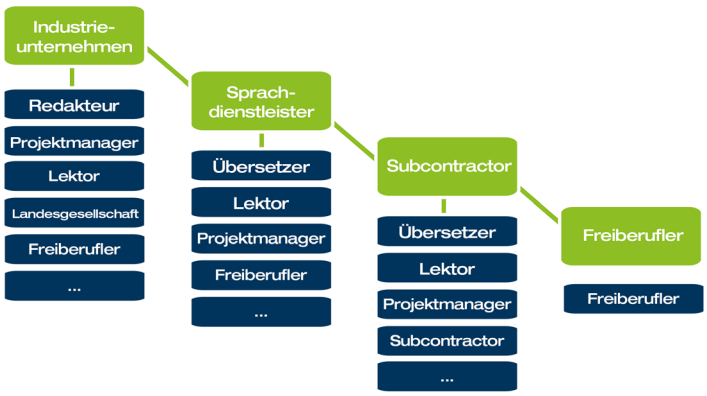


**Abb. 1: Übersetzungsprozesse sind verteilte Prozesse**

ter wiederum vergibt die Aufträge an Subkontraktoren oder ebenfalls an Freelancer. Die Datenübertragung erfolgt häufig über E-Mail oder FTP-Server und ist daher nicht nur für den eigentlichen Empfänger zugänglich. Je nach Übersetzungsvolumen verlängert sich die Lieferkette zu weiteren Subsubkontraktoren oder weiteren Dienstleistern. Sie alle verfügen über unterschiedliche Infrastrukturen und haben ein unterschiedliches Verständnis von Informationssicherheit. Darüber hinaus ist die Integrität der Daten in offenen Systemen kaum zu gewährleisten. Dennoch trägt das Industrieunternehmen die alleinige Verantwortung dafür, dass die Informationen integer, vertraulich und verfügbar sind.

Für Unternehmen besteht somit die Gefahr, dass Informationen ungeplant an die Öffentlichkeit gelangen. Während der Entwicklung einer Produktinnovation werden dazugehörige Informationen wie Anleitungen oder Beschreibungen häufig bereits in einem frühen Entwicklungsstadium übersetzt, um so die Time-to-Market möglichst kurz zu halten. Dieses Vorgehen kann gefährlich werden, wenn ein Wettbewerber auf Grund unzureichender Sicherheitsmaßnahmen an diese Informationen gelangt und beispielsweise mit einer Produktneuheit früher präsentiert. Eine Urheberrechtsverletzung kann nicht geltend gemacht werden, denn der Eigentümer hat für eine sichere Lieferkette Sorge zu tragen. Ebenso ist z. B. bei der Übersetzung von Börsenberichten Vorsicht geboten, um Insiderhandel vorzubeugen. Selbst in der Pharmaindustrie und der Finanzwirtschaft werden vertrauliche Inhalte oftmals in offenen Dokumentenformaten und in unkontrollierbaren Prozessen an eine Vielzahl von Übersetzern herausgegeben.

Diese in der Praxis üblichen Prozesse setzen Informationen unnötigen Risiken aus. Eine Vertraulichkeitsvereinbarung als gängige Maßnahme greift dabei zu kurz und kann keine vollständige Sicherheit für den Umgang mit den Daten garantieren. Der Auftraggeber sollte also nicht nur innerhalb seines direkten Einflussbereichs Risiken identifizieren und Maßnahmen dagegen ergreifen, sondern auch sicherstellen, dass bei jedem einzelnen Projektbeteiligten und bei jeder Datenübergabe Compliance-konforme Prozesse ablaufen. Mit einer Kombination aus Compliance-Richtlinien und passenden Technologien lassen sich die Risiken verringern.

## Organisatorische Maßnahmen treffen

Um die Verfügbarkeit der Daten zu gewährleisten, sollte der externe Sprachdienstleister vorgegebene technische Voraussetzungen erfüllen. So kann beispielsweise vertraglich festgehalten werden, dass er Daten durch ausgelagerte Sicherungskopien vor Zerstörung schützen und eine unterbrechungsfreie Stromversorgung gewährleisten muss.

Ein anderer Ansatz ist die zentrale Datenhaltung beim Auftraggeber selbst. Damit die Datenintegrität sichergestellt ist, sollte in der Übersetzungsumgebung eine Authentifizierungspflicht nicht autorisierte Änderungen verhindern. Außerdem ist über eine Historienverfolgung jederzeit nachvollziehbar, wer zu welchem Zeitpunkt welche Inhalte geändert hat. Darüber hinaus sollten interne und externe Mitarbeiter regelmäßige Schulungen für die eingesetzten Systeme absolvieren und die erworbenen Kompetenzen nachweisen können. Dies stellt die richtige Anwendung der verfügbaren technischen Funktionen sicher.

Sobald sensible Daten für die Übersetzung das eigene Haus verlassen, muss dafür gesorgt werden, dass sie nach der Bearbeitung durch den externen Übersetzer nicht auf dessen Rechner verbleiben. Dies gilt nicht nur für die Ausgangstexte und Übersetzungen, sondern ebenso für das Translation Memory und die Firmenterminologie. Schließlich lassen sich aus all diesen Daten leicht Rückschlüsse auf Firmeninterna ziehen. Zusätzlich geschützt werden Informationen, wenn sie nur einem beschränkten Empfängerkreis zur Verfügung stehen und eine vertragliche Vereinbarung mit dem beauftragten Sprachdienstleister verhindert, dass sie an weitere Sublieferanten oder Freelancer weitergegeben werden.

## Risiken minimieren

Da organisatorische Maßnahmen in verteilten Übersetzungsprozessen die Sicherheit der Informationen nicht hinreichend gewährleisten können, sind Prozesse und Werkzeuge erforderlich, die den Missbrauch verhindern. Dazu zählen vor allen Dingen Übersetzungsmanagementsysteme mit den zentralen Komponenten Translation Memory, Terminologiesystem sowie Werkzeugen zur Projekt- und Workflowsteuerung. Als

***Translation Memory:***
***Datenbank, in der Übersetzungseinheiten (Satzpaare) gespeichert werden. Dabei wird jedem quellsprachlichen Segment das entsprechende zielsprachliche Segment zugeordnet.***

***Terminologiesystem:***
***Verwaltung und Pflege des gesamten Firmenwortschatzes inklusive Verwendungshinweisen für Autoren und Übersetzer***

geschlossene integrierte Arbeits- und Systemumgebung für alle Sprachressourcen und Übersetzungsprozesse, in der alle Beteiligten auf gemeinsamer Datenbasis und idealerweise mit unterschiedlichen Zugriffsrechten kooperieren, stellen sie sicher, dass alle Prozesse nachvollziehbar bleiben und Daten nicht unkontrolliert auf lokalen Rechnern gespeichert werden oder das geschützte System verlassen. Die Datenhoheit und so auch die Verantwortung für informationstechnologische Sicherungsmaßnahmen liegen damit beim Unternehmen selbst. Einige Systeme bieten bereits die Möglichkeit, bestimmte Prozessschritte zu automatisieren und dadurch mögliche Fehlerquellen gar nicht erst entstehen zu lassen. Beispielsweise verringern eine automatische Aufgabenzuweisung und unterschiedlich definierte Zugriffsrechte für die einzelnen Bearbeiter das Risiko, dass Übersetzungsdaten versehentlich an einen unbefugten Empfängerkreis gesandt werden. Darüber hinaus können mit Hilfe des Translation Memory und der Terminologiedatenbank Daten zweckgebunden bzw. zeitlich limitiert bereitgestellt werden.

## Informationssicherheit mit einem TMS

Zu den führenden Translation-Management-Systemen (TMS) gehört der Across Language Server. Er verfügt über ein Translation Memory und ein Terminologiesystem. Darüber hinaus ist er mit weiteren Werkzeugen ausgestattet, die die beschriebenen Sicherheitsrisiken minimieren sowie Projekte und Prozesse steuern.

- Das Translation-Management-System verfolgt einen **geschlossenen Ansatz** und ist nur per Login zugänglich. Das integrierte Rechtesystem definiert die Bearbeitungsmöglichkeiten für jeden Nutzer.

- Texte können nur nach Auftragszuweisung editiert werden. Im Translation Memory und Terminologiesystem **vorgenommene Änderungen** sind in der Historie jederzeit **nachvollziehbar**.

- Der Auftraggeber kann **Regeln für den Übersetzungsprozess definieren**, die in der gesamten Lieferkette zu beachten sind und nicht verändert werden können.

- **Daten werden** nach Abschluss der Aufgaben oder gemäß Verfallsdatum in der Lieferkette **gelöscht**.

## Fazit

Damit Unternehmen sich bei Übersetzungen von sensitiven Informationen durch externe Dienstleister nicht unnötigen Risiken aussetzen, wird ihnen empfohlen, zunächst die damit verbundenen Prozesse zu dokumentieren und die Anfor-

derungen an die Informationssicherheit zu definieren – falls nötig mit der Unterstützung externer Berater. Über einfach umzusetzende Maßnahmen wie Schulungen können dann erste Sicherheitslücken geschlossen werden. Des Weiteren empfiehlt sich der Einsatz einer geschlossenen Umgebung, wie sie der Across Language Server bietet. Damit bleibt die Datenhoheit beim Auftraggeber, alle Prozessbeteiligten sind nahtlos über einen Browserzugriff angebunden, die Prozesse sind integriert und nachvollziehbar und ein granulares Rechtesystem schützt sensitive Daten vor nicht autorisiertem Zugriff oder unkontrollierter Speicherung.

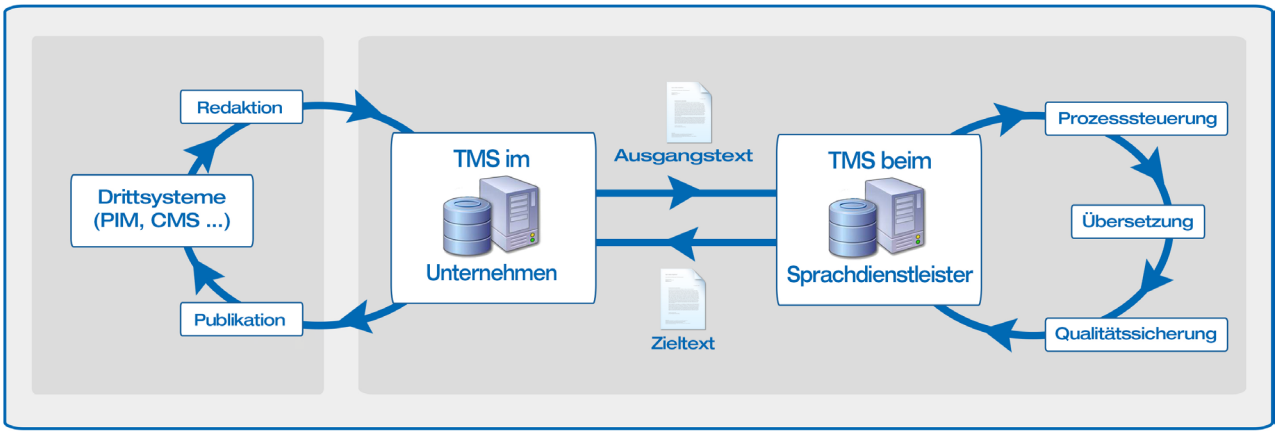


**Abb. 2: Ein geschlossenes System gewährleistet sichere Übersetzungsprozesse**


Tel. +49 7248 925 425
www.across.net
info@across.net

across
Language Technology for a Globalized World.