APOSTROPH GROUP

The Language Intelligence Company

Security White Paper

Bei Apostroph stehen Sicherheit und Vertraulichkeit an erster Stelle

Security White Paper

Sicherheit und Vertraulichkeit bei der Systemwahl und bei Entscheidungen im IT-Bereich haben bei Apostroph oberste Priorität. Dies gilt auch für die Wahl der Tools, die wir unseren Mitarbeitenden und Freelancern zur Verfügung stellen. Weiter werden unsere Mitarbeitenden gemäss der Verordnung über die Personensicherheit des Bundes regelmässig überprüft. Wir sind zertifiziert nach ISO 27001.

Die IT-Security basiert bei der Apostroph Group auf fünf Grundpfeilern:

- Physikalische Sicherheit
- Sicherheit auf Systemebene
- Sicherheit auf Applikationsebene
- Netzwerksicherheit
- Regelmässige Schulung der User

Die IT-Umgebung von Apostroph entspricht dem Bankenstandard. Interne User wie auch Freelancer arbeiten ausschliesslich mit einem persönlichen User-Account, eine Multifaktor-Authentifizierung unterstützt die bereits hohen Sicherheitsstandards mit einem komplexen Passwort zusätzlich. Weiter bestätigen sämtliche Freelancer vor Beginn der Zusammenarbeit durch die Unterzeichnung der Allgemeinen Geschäftsbedingungen, dass sie sich an die darin detailliert beschriebenen Vorgaben halten.

Alle Mitarbeitenden unterzeichnen beim Ein- wie auch beim Austritt eine umfangreiche Verschwiegenheitserklärung und haben vor dem Stellenantritt einen Strafregisterauszug einzureichen, der nicht älter als ein Monat sein darf. Viele unserer Mitarbeitenden wurden zusätzlich nach Art. 11 der Verordnung über die Personensicherheitsprüfung PSPV überprüft und freigegeben.

Bei der Zustellung Ihrer Dokumente an uns, während der Übersetzung und auch nach der Ablieferung bleiben Ihre vertraulichen Texte vertraulich. Zwei verschiedene Vertraulichkeitsstufen für die Auftragserteilung bestimmen das Mass an Sicherheit, das bei der Bearbeitung angewendet wird:

Unternehmen

1994 gegründet
160 Mitarbeitende
100 Sprachen
> 2000 Sprachprofis
> 5000 Kundinnen

Vorteile

- Interne Sprachprofis
- Internes Entwickler-Team
- Neueste Übersetzungstechnologien
- Individuelle Unternehmenslösungen
- Kompetente Beratung

Sicherheit

100 % Diskretion und höchste Sicherheit Ihrer vertraulichen Daten dank Datenhoheit Schweiz und ISO-27001-zertifizierter Prozesse.

Vertraulichkeitsstufen			
Level	**Beschreibung/Einstufung des zu übersetzenden Dokuments**	**Sicherheitsanforderung**	**Sicherheitsmassnahmen**
1	Normal – allgemein zugängliche Information	Keine	Allgemeiner Zugang in elektronischer Form, Schutz gegen unerlaubten Zugriff
2	Vertraulich	Hoch	Zugang nur für eine beschränkte Zahl von Anwendern oder internen Mitarbeitenden

Physikalische Sicherheit

IT-Infrastruktur

Die Server von Apostroph befinden sich in der Schweiz mit Datenhosting in der Schweiz. Die Serverumgebung ist komplett redundant aufgebaut. Täglich wird ein Daten-Back-up erstellt, das extern an einem sicheren Ort aufbewahrt wird. Sämtliche Clients sperren sich automatisch bei Inaktivität. Die Mitarbeitenden sind gemäss Clear Desk Policy angehalten, die Computer zu sperren oder herunterzufahren, sobald sie ihren Arbeitsplatz verlassen. Dies wird kontrolliert; Verstösse werden vom direkten Vorgesetzten mit schriftlichem Vermerk im Personaldossier geahndet.

Sicherheit

Alle Dokumente werden grundsätzlich nur digital bearbeitet. Falls eine Bearbeitung auf Papier (aufgrund der gewünschten Dienstleistung) notwendig ist, werden diese ausschliesslich unter Verschluss aufbewahrt. Die Clear Desk Policy wird durchgesetzt. Alle Printdokumente werden zur Vernichtung in einem abschliessbaren Behälter aufbewahrt und dann durch ein zertifiziertes Aktenvernichtungsunternehmen fachgerecht entsorgt. Besucherinnen und Besucher müssen sich anmelden und dürfen sich nur unter Aufsicht in den für sie vorgesehenen Bereichen der Geschäftsräumlichkeiten aufhalten. Die Dokumentation der Besuche erfolgt nach ISO 27001.

Sicherheit auf Systemebene

Prozesse/Systeme
Apostroph nutzt APOS (Apostroph Order System) für die Auftragsabwicklung. Alle Arbeitsprozesse werden via APOS verteilt, überwacht und abgeschlossen. APOS wird ausserdem für die Verwaltung von Zugriffsrechten auf die verschiedenen Datenbanken genutzt.

Zugriffe auf vertrauliche Daten werden mit Passwörtern geregelt, die einzig der jeweils zuständigen Benutzergruppe zur Verfügung stehen. Die Zugänge können nur von den Administratoren vergeben werden. So stellt Apostroph sicher, dass jeder Kundenauftrag jederzeit in einem kontrollierten, sicheren Umfeld abgewickelt wird.

Zugriff
Das E-Mail-System ist ebenfalls mit einem Passwort geschützt. Die Passwörter müssen bestimmte Sicherheitskriterien erfüllen und alle drei Monate geändert werden. Eine entsprechende System-aufforderung ist automatisiert und nicht umgehbar.

Vertraulichkeit
Die Vertraulichkeitsstufe wird vom Kunden in myAPOSTROPH bei der Auftragsvergabe festgelegt. Als vertraulich markierte Aufträge können nur von der entsprechenden erfassenden Person und einem intern definierten Superuser eingesehen werden.

Verschlüsselung
Bei Apostroph werden die Daten mittels SSL verschlüsselt.

Weitere spezifische Verschlüsselungen werden eingesetzt, wenn Apostroph direkten Zugang zu den Kundensystemen (z. B. CMS-Tools) erhält.

Sicherheit auf Applikationsebene

Verwendete Applikationen
Die von Kunden, Übersetzerinnen und Apostroph hauptsächlich genutzten Applikationen sind:

- Verschlüsselte Microsoft-Access-Applikationen
- Verschlüsselte Trados Translation Memories und Terminologie-datenbanken
- Verschlüsselte Web-Applikationen
- B2B HTTPS & FTP Web Services

Microsoft Access

APOS ist eine Eigenentwicklung von Apostroph, die auf Microsoft .NET und Vue.js basiert und über eine professionelle SQL-Datenbank verfügt. Die webbasierten Applikationen myFREELANCE (auf Übersetzerseite) respektive myAPOSTROPH (auf Kundenseite) werden für den Datenaustausch eingesetzt und sind SSL-verschlüsselt. Sie basieren ebenfalls auf .NET und Vue.js. APOS stellt den gesamten Prozess sowie dessen Rückverfolgbarkeit sicher: Welcher Freelancer und welche Freelancerin welche Services ausführt, wer am Projekt beteiligt und wofür sie oder er zuständig ist, welche Textart das zu bearbeitende Dokument aufweist, in welche Sprachen übersetzt wird, welche Vertraulichkeitsstufe der Auftrag hat, welche Termine fixiert sind etc. sind Informationen, die für jeden Auftrag eingepflegt werden.

Trados Studio

Für die Übersetzung wird Trados Studio oder auf Kundenwunsch ein anderes CAT-Tool benutzt. Dabei wird das Dokument in sogenannte Segmente (in der Regel Sätze) unterteilt, die in einer Translation Memory gespeichert und bei neu zu übersetzenden Dokumenten wieder aufgerufen werden können. Dies garantiert Konsistenz, kürzere Liefertermine sowie tiefere Kosten.

Der Zugriff auf die Translation Memory- und Terminologiedatenbanken wird von Fall zu Fall pro Kundin und Freelancer freigeschaltet. Er erfolgt mit persönlichem Usernamen und Passwort mittels SSL-Verschlüsselung.

B2B Services

Verschiedene Services stehen für den automatisierten Datenaustausch zur Verfügung:

- Kundenportal myAPOSTROPH (HTTPS) für Up- und Download von Auftragsdateien
- Apostroph REST API für System-zu-System-Anbindungen
- CMS-Connector (z. B. für Drupal)
- Hotfolder-Integrationen entweder in der Kunden- oder in der Apostroph Umgebung

HTTPS-basierte Lösung (myAPOSTROPH)

Sämtliche Methoden sind mittels HTTP Basic Authentication geschützt. Bei jedem Serviceaufruf müssen Username und Passwort mitgeliefert werden.

Kundinnen und Kunden können in myAPOSTROPH den Status ihrer Aufträge einsehen (in Bearbeitung, geliefert, verrechnet). Übersetzungen können dort auch nachträglich heruntergeladen werden. Weiter können sie Reports zu ihren Aufträgen generieren (CSV-Format – lässt sich in Excel öffnen und bearbeiten).

Netzwerksicherheit

Set-up

Alle Mitarbeitenden arbeiten mittels Citrix Server. Dadurch werden alle Anwendungen und Ressourcen zentral gehostet und lassen sich remote abrufen. So ist auch sichergestellt, dass die Mitarbeitenden in Krisenzeiten (Umweltkatastrophen, Epidemien) auf die Arbeitsumgebung zugreifen und den Betrieb aufrechterhalten können. Hosting und Aktualisierung der Software werden einheitlich gehandhabt und zentral kontrolliert. Der Datenaustausch findet ausschliesslich verschlüsselt statt. Die Benutzung wird permanent kontrolliert.

Notfallpläne existieren. Übungen dazu finden regelmässig statt.

Schutz

Die Firewalls von Apostroph werden laufend bezüglich neuester Technologien und Softwarestände aktualisiert. Auf den Arbeitsgeräten von Apostroph und den Servern werden immer die aktuellsten Sicherheitspatches von Microsoft eingespielt. Ausserdem sind Anti-Virus- und Anti-Spam-Softwares installiert und E-Mails werden gescannt. Alle Mitarbeitenden werden regelmässig für die Gefahren und das Verhalten bei Phishing-, Viren- und Hackerangriffen geschult. Gewisse Websites sind aus Sicherheitsgründen grundsätzlich gesperrt.

Es finden regelmässige Pen-Tests und simulierte Phishing-Attacken statt.

Unternehmen

Die Apostroph Group ist die führende Sprachdienstleisterin in der DACH-Region. Zur Gruppe gehören 10 Standorte in der Schweiz und in Deutschland. Heute vertrauen über 5000 Unternehmen und Institutionen auf die Expertise von Apostroph. Mit 160 Mitarbeitenden, darunter 40 Linguistinnen und Linguisten, und über 2000 geprüften Fachübersetzerinnen und Fachübersetzern bietet Apostroph Sprachservices in allen Disziplinen und in 100 Sprachen an und bedient dabei alle Branchen, jeweils massgeschneidert für die lokalen Märkte. Langjährige Erfahrung in der Sprachtechnologie und Prozessdigitalisierung sowie das gezielte Zusammenspiel von Mensch und Maschine bilden dabei die Kernbausteine für die Qualität und Effizienz der Apostroph Dienstleistungen.