Vereinbarung

über eine

Auftragsverarbeitung nach Art. 28 DSGVO

Der Verantwortliche:

Der Auftragsverarbeiter:

Testify GmbH
Peter-Behrens-Platz 10
4020 Linz
Österreich

(im Folgenden Auftraggeber)

(im Folgenden Auftragnehmer / Provider)

1. GELTUNGSBEREICH

1. Im Rahmen der Leistungserbringung durch den Auftragnehmer ist es erforderlich, dass dieser personenbezogene Daten des Auftraggebers verarbeitet, für die der Auftraggeber als datenschutzrechtlich Verantwortlicher fungiert („Auftraggeber-Daten"). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien bei der Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer.
2. Im Falle von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

2. GEGENSTAND UND UMFANG DER VERARBEITUNG VON PERSONENBEZOGENEN DATEN IM AUFTRAG

1. Der Auftraggeber nutzt die Software „Testify" zur Digitalisierung von Unternehmensprozessen.
2. Der Auftragnehmer verarbeitet die Auftraggeber-Daten ausschließlich im Auftrag und auf Weisung des Auftraggebers im Sinne von Art. 28 Abs. 1 DSGVO (Verarbeitung im Auftrag). Der Auftraggeber bleibt im datenschutzrechtlichen Sinn Verantwortlicher und ist gegenüber Dritten und den Betroffenen für die Rechtmäßigkeit der auftragsgemäßen Verarbeitung der personenbezogenen Daten verantwortlich.
3. In Anlage 1b zu diesem Vertrag ist abschließend festgelegt, welche Arten von Auftraggeber-Daten der Auftragnehmer auf welche Arten und für welche Zwecke verarbeiten darf und auf welche Kategorien betroffener Personen sich die Auftraggeber-Daten beziehen. Der Auftragnehmer darf die Auftraggeber-Daten ausschließlich entsprechend diesen Vorgaben verarbeiten.
4. Der Zugriff des Auftragnehmers auf Daten des Auftraggebers erschließt sich während der Implementierungsphase der Software, im laufenden Betrieb der Software und in möglichen Supportfällen.
   Folgende Aufgaben werden vom Auftragnehmer durchgeführt:
   - Einrichtung Software as a Service (SaaS) in Testify Cloud Infrastruktur (Microsoft Azure).
     - Hosting der Software as a Service-Lösung (SaaS) auf Microsoft Azure
     - Bereitstellung integrierter Dashboards über die in der Software erfassten Daten
     - Gegebenenfalls initialer Import von Stammdaten in der Implementierungsphase der Software
     - Gegebenenfalls Erbringung von Analyse-, Diagnose- und Supportleistungen gegenüber dem Auftraggeber unter Berücksichtigung von Stammdaten und Transaktionsdaten
5. Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: Stammdaten & -Transaktionsdaten

3. DAUER DER VEREINBARUNG

(1) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags.
(2) Eine Kündigung des Hauptvertrages bewirkt automatisch die Kündigung dieses Vertrages. Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen.

4. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1a zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer weist darauf hin, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO errichtet hat.

(6) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht eingeräumt, maximal ein Mal im Kalenderjahr Einsichtnahme und Kontrolle, sei es auch durch von ihm beauftragte Dritte, der Datenverarbeitungseinrichtungen vorzunehmen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(7) Der Auftragnehmer unterstützt den Auftraggeber soweit erforderlich bei der Durchführung von Datenschutz-Folgenabschätzungen und Konsultationsverfahren gemäß Art. 35 f. DSGVO.

5. RECHTE DER BETROFFENEN PERSONEN

(1) Für die Beantwortung von Anträgen auf Wahrnehmung der nach den Art. 12 ff. DSGVO bestehenden Rechte der betroffenen Personen („Betroffenenrechte“) ist der Auftraggeber zuständig. Die betroffenen Personen wenden sich hinsichtlich Informationsauskunft, Widerruf oder Löschung an den Auftraggeber.

(2) Sofern eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Wahrnehmung der ihr zustehenden Betroffenenrechte (z.B. Löschung der Daten) wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

6. RÜCKGABE UND LÖSCHUNG VON AUFTRAGGEBER-DATEN

(1) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten zu vernichten/löschen. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er nach schriftlicher Aufforderung verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

(2) Der Auftragnehmer verpflichtet sich, die Auftraggeber-Daten nach Beendigung des Vertrages nicht aktiv zu verarbeiten.

(3) Der Auftragnehmer verpflichtet sich, sämtliche ihm vom Auftraggeber überlassenen sowie sämtliche ergänzend hinzugewonnenen Auftraggeber-Daten einschließlich aller Kopien nach Abschluss der Erbringung der Verarbeitungsleistung nach Wahl des Auftraggebers datenschutzgerecht zu löschen.

(4) Mit Abschluss der Erbringung der Verarbeitungsleistungen, verpflichtet sich der Auftragnehmer den Auftraggeber unter Angabe der betroffenen Daten schriftlich über die Datenlöschung zu informieren.

(5) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeber-Daten dienen, darf der Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren.

(6) Eine vollumfängliche Datenlöschung ist nach Beendigung des Vertrages und darin vereinbarter Behaltefristen möglich. Einzelne Datensätze können laufend durch den Admin User des Auftraggebers abhängig von den Revisionserfordernissen selbstständig deaktiviert bzw. gelöscht werden.

7. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Ausschließliche Durchführung innerhalb der EU/des EWR

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt. Details dazu können dem Testify Security Dossier entnommen werden.

8. SUB-AUFTRAGSVERARBEITER

(1) **Zulässigkeit der Hinzuziehung eines bestimmten Sub-Auftragsverarbeiters** Der Auftragnehmer ist befugt Unternehmen als Sub-Auftragsverarbeiter hinzuzuziehen. Die aktuelle Liste der Sub-Auftragsverarbeiter, welche mit Unterzeichnung dieses Vertrages durch den Auftraggeber genehmigt werden, befindet sich im Benutzerhandbuch unter Datenschutz sowie in den Datenschutzbestimmungen. Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig über die Release Notes bekannt zu geben, dass er dies allenfalls untersagen kann.

(2) Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

(3) Der Auftragnehmer ist nach eigenem Ermessen berechtigt, zukünftig Dritte zur Sicherstellung der vertraglichen Leistungen zu beauftragen. Die beteiligten Partner werden dem Auftraggeber gegenüber vor Durchführung offengelegt.

9. MELDUNGEN UND SONSTIGE UNTERSTÜTZUNGSPFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn ihm eine Verletzung des Schutzes der Auftraggeber-Daten im Sinne von Art. 4 Nr. 12 DSGVO bekannt wird. Der Auftragnehmer wird dem Auftraggeber, soweit möglich, die gemäß Art. 33, 34 DSGVO erforderlichen Informationen erteilen.

(2) Der Auftragnehmer darf ohne Wissen und Zustimmung des Auftraggebers keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen. Hiervon ausgenommen sind Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind (Backup-Strategie), sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Anlagenverzeichnis:

Anlage ./1a	Technisch-Organisatorische Maßnahmen
Anlage ./1b	Arten von Auftraggeber-Daten gem. Auftragsverarbeitung nach Art 28 DSGVO

Unterschriftenseite folgt.

....., am .....

Für den Auftraggeber:

.....
[*Name samt Funktion*]

Linz

Für den Auftragnehmer:

.....
Sebastian Spindler (CEO)

ANLAGE ./1A

TECHNISCH-ORGANISATORISCHE MASSNAHMEN

A. VERTRAULICHKEIT

- **Zutrittskontrolle**: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:
    - Magnet- oder Chipkarte
    - Elektrische Türöffner
    - Portier
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung durch:
    - Kennwörter (einschließlich entsprechender Policy)
    - Automatische Sperrmechanismen
    - Zwei-Faktor-Authentifizierung
    - Verschlüsselung von Datenträgern und Zugangsdaten
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:
    - Standard-Berechtigungsprofile auf „need to know-Basis“
    - Standardprozess für Berechtigungsvergabe
    - Protokollierung von Zugriffen
    - Sichere Aufbewahrung von Speichermedien
    - Periodische Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten
    - Datenschutzgerechte Wiederverwendung von Datenträgern
    - Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger
    - Clear-Desk/Clear-Screen Policy

B. DATENINTEGRITÄT

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:
    - Verschlüsselung von Datenträgern
    - Verschlüsselung von Dateien
- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:
    - Protokollierung
    - Dokumentenmanagement

C. VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:
    - Backup-Strategie (online/offline; on-site/off-site)
    - Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat)
    - Virenschutz
    - Firewall
    - Meldewege und Notfallpläne
    - Security Checks auf Infrastruktur- und Applikationsebene
    - Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum (Backup-Strategie)
    - Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern

- Rasche **Wiederherstellbarkeit (Business Recovery Plan)**

D. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- **Datenschutz-Management**, einschließlich regelmäßiger Mitarbeiter-Schulungen
- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen (Berechtigungskonzept)**
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers durch:
    - Eindeutige Vertragsgestaltung
    - Formalisiertes Auftragsmanagement

ANLAGE ./1B:
ARTEN VON AUFTRAGGEBER-DATEN GEM. AUFTRAGSVERARBEITUNG NACH ART 28 DSGVO

Die folgenden personenbezogenen Daten können vom Auftragnehmer verarbeitet werden:

Stammdaten
Vor- und Nachname
E-Mail-Adresse
Sprache
Abteilung/Kostenstelle
Rolle/Rechte
Transaktionsdaten

Weiters unterliegen sämtliche personenbezogene Daten ("Auftraggeber-Daten"), die der Auftraggeber in der Software "Testify" speichert bzw. verarbeitet, der vertragsgegenständlichen Verarbeitung durch den Auftragnehmer.