Vertraulich zusammenarbeiten

NDA-Mustervorlage für die Machbarkeitsprüfung mit cleverR und ABBYY

Muster – vor Einsatz rechtlich prüfen und vervollständigen

Diese Vorlage ist ein Gestaltungsvorschlag, keine als rechtsgeprüft bestätigte Vereinbarung. Parteien, Vertretungsberechtigung, Fristen und projektspezifische Anforderungen sind vor Unterzeichnung zu prüfen und zu vervollständigen.

Partei A · Anbieter
EDV-Partner Ingenieurgesellschaft für Informationstechnologie mbH
Große Bahnstraße 33 · 22525 Hamburg
Vertreten durch · Name und Funktion

Partei B · Gegenpartei
Firma / vollständige rechtliche Bezeichnung

Adresse / vollständige Geschäftsanschrift

Vertreten durch · Name und Funktion

Partei A und Partei B werden jeweils „Partei“, gemeinsam „Parteien“ genannt. Jede Partei kann offenlegende oder empfangende Partei sein.

1 Gemeinsamer Zweck

Zweck ist die Prüfung der technischen und fachlichen Machbarkeit einer automatisierten Eingangsrechnungsverarbeitung mit cleverR und ABBYY im Rahmen eines Proof of Concept (POC) bzw. Piloten. Der Austausch kann insbesondere Testbelege, Rechnungsdaten sowie Prozessinformationen, Konfigurationen, Schnittstellen und andere technische Informationen umfassen. Ein produktiver Betrieb ist nicht Gegenstand dieser Vereinbarung.

Was vertraulich bleibt

Gegenseitiger Schutz – unabhängig von der Rolle im Informationsaustausch

2 Vertrauliche Informationen und Ausnahmen

Vertrauliche Informationen sind alle im Zusammenhang mit dem Zweck unmittelbar oder mittelbar offengelegten Informationen, die als vertraulich bezeichnet sind oder deren Vertraulichkeit nach Inhalt oder Umständen erkennbar ist. Erfasst sind schriftliche, elektronische, mündliche und visuelle Informationen, insbesondere die in Ziffer 1 genannten Daten, Geschäfts- und Betriebsgeheimnisse, Zugangsdaten, Preise, Unterlagen sowie daraus erstellte Auswertungen, Kopien und Notizen. Mündliche Angaben sind auch ohne nachträgliche Kennzeichnung geschützt, soweit ihre Vertraulichkeit erkennbar ist.

Nicht erfasst sind Informationen, soweit die empfangende Partei nachvollziehbar nachweist, dass sie (a) bereits rechtmäßig und ohne Geheimhaltungspflicht bekannt waren, (b) ohne Verstoß gegen diese Vereinbarung allgemein zugänglich sind oder werden, (c) rechtmäßig von einem hierzu befugten Dritten ohne Geheimhaltungspflicht erlangt wurden oder (d) unabhängig und ohne Nutzung vertraulicher Informationen entwickelt wurden. Eine schriftliche Freigabe der offenlegenden Partei gilt nur im ausdrücklich freigegebenen Umfang.

3 Zweckbindung und gebundene Empfänger

Die empfangende Partei verwendet vertrauliche Informationen ausschließlich für den vereinbarten Zweck. Sie gibt sie nur solchen Beschäftigten, Organmitgliedern, beruflich zur Verschwiegenheit verpflichteten Beratern oder erforderlichen Dienstleistern weiter, die sie hierfür tatsächlich benötigen (Need-to-know). Empfänger müssen vor Zugang mindestens gleichwertig vertraglich oder gesetzlich zur Vertraulichkeit und zweckgebundenen Nutzung verpflichtet sein.

Die empfangende Partei stellt die Einhaltung dieser Pflichten durch ihre eingesetzten Empfänger sicher und steht für deren Verhalten nach den gesetzlichen Vorschriften ein. Eine Weitergabe an ABBYY, weitere Technologieanbieter, Hosting-, Cloud- oder Supportdienste ist durch deren Nennung oder diese NDA allein nicht genehmigt; konkrete Empfänger und Zugriffsrollen sind vorab zwischen den Parteien abzustimmen. Ziffer 5 bleibt unberührt.

4 Angemessene Schutzmaßnahmen

Jede Partei schützt empfangene Informationen mindestens mit der Sorgfalt für eigene vergleichbar sensible Informationen, in jedem Fall mit angemessenen technischen und organisatorischen Maßnahmen. Dazu gehören insbesondere beschränkte und nachvollziehbare Zugriffe, sichere Übertragung und Speicherung, Schutz von Zugangsdaten und die Beschränkung von Kopien auf das Erforderliche. Öffentlich zugängliche Ablagen oder unfreigegebene KI- und Cloud-Dienste dürfen nicht verwendet werden.

Wird eine unbefugte Nutzung, Offenlegung oder ein Verlust bekannt, informiert die empfangende Partei die andere Partei unverzüglich, soweit rechtlich zulässig, und wirkt an angemessenen Maßnahmen zur Begrenzung der Folgen und Verhinderung weiterer Vorfälle mit. Gesetzliche Melde- und Benachrichtigungspflichten bleiben unberührt.

Klare Grenzen für Daten

Offenlegung, Modelltraining, Rückgabe und Dauer der Verpflichtungen

5 Gesetzlich zwingende Offenlegung

Ist eine Partei aufgrund zwingenden Rechts oder einer verbindlichen behördlichen oder gerichtlichen Anordnung zur Offenlegung verpflichtet, darf sie nur den rechtlich erforderlichen Umfang offenlegen. Sie informiert die andere Partei, soweit zulässig, vorab und rechtzeitig, damit Schutzmaßnahmen beantragt werden können, und unterstützt angemessene Bemühungen um eine vertrauliche Behandlung. Ist eine Vorabinformation untersagt, erfolgt sie, sobald dies rechtlich zulässig ist.

6 Kein Modelltraining ohne gesonderte Vereinbarung

Vertrauliche Informationen, insbesondere Testbelege und Rechnungsdaten, dürfen ohne gesonderte ausdrückliche Vereinbarung der Parteien weder zum Training, Nachtraining oder zur allgemeinen Verbesserung von KI-/ML-Modellen noch zur Erstellung hierfür bestimmter Trainingsdatensätze verwendet oder Dritten hierfür bereitgestellt werden. Auch ein Anbietertraining durch eingesetzte Dienste ist auszuschließen. Erforderliche projektbezogene Verarbeitung, Inferenz oder Konfiguration im POC/Pilot darf nur im abgestimmten Umfang und unter Beachtung von Ziffer 10 erfolgen; sie begründet keine Erlaubnis zum Modelltraining.

7 Rückgabe, Löschung und begrenzte Ausnahmen

Auf Verlangen der offenlegenden Partei, spätestens nach Ende des Zwecks oder der Austauschphase, gibt die empfangende Partei vertrauliche Informationen nach Wahl der offenlegenden Partei zurück oder löscht bzw. vernichtet sie einschließlich Kopien, Auszügen und Arbeitsunterlagen innerhalb von 30 Kalendertagen. Sie veranlasst dies auch bei ihren Empfängern und bestätigt die Umsetzung auf Verlangen in Textform.

Ausgenommen sind nur gesetzlich zwingend aufzubewahrende Unterlagen und technisch nicht mit vertretbarem Aufwand selektiv löschbare Sicherungskopien in regulären Backups. Die empfangende Partei dokumentiert auf Verlangen Kategorien, Grund, Zugriffsbeschränkung und Aufbewahrungs- bzw. Überschreibungsfrist dieser Restbestände. Sie bleiben geschützt, werden gesperrt bzw. nicht weiter für den Zweck genutzt und nach Wegfall der Pflicht oder im dokumentierten regulären Backup-Zyklus gelöscht. Nach einer Wiederherstellung sind betroffene Daten erneut zu löschen. Datenschutzrechtlich erforderliche kürzere Fristen oder weitergehende Pflichten gehen vor.

8 Laufzeit – ausdrücklich als Mustervorschlag

Vorgeschlagen wird eine Austauschphase von **zwei Jahren** ab Wirksamwerden. Für jede innerhalb dieser Phase offengelegte Information gelten die Schutz- und Nutzungsbeschränkungen bis **drei Jahre nach Ende der Austauschphase**. Für Geschäftsgeheimnisse gelten sie darüber hinaus, solange die Voraussetzungen des gesetzlichen Geschäftsgeheimnisschutzes bestehen. Die Parteien prüfen diese Fristen vor Unterzeichnung und passen sie bei Bedarf gemeinsam an. Ziffer 7 bleibt anwendbar.

9 Keine Rechteübertragung oder Durchführungspflicht

Alle Rechte verbleiben bei der jeweils berechtigten Partei bzw. den Rechteinhabern. Es werden nur die für den vereinbarten Zweck erforderlichen, zeitlich darauf beschränkten Nutzungsbefugnisse eingeräumt; Lizenzen oder Eigentumsrechte gehen nicht über. Keine Partei ist zur Offenlegung bestimmter Informationen, zur Durchführung eines Piloten, zur Auftragserteilung oder zum Abschluss weiterer Verträge verpflichtet.

Erst prüfen, dann starten

Vervollständigung und beiderseitige Unterzeichnung sind erforderlich

Wichtig: Diese NDA ersetzt keine AVV und keine Datenschutzprüfung

Vor dem Einsatz von Echtdaten müssen die Parteien die Rechtsgrundlage und datenschutzrechtlichen Rollen prüfen sowie eine gegebenenfalls erforderliche Auftragsverarbeitungsvereinbarung (AVV) schließen. Ebenso sind konkrete Empfänger einschließlich Unterauftragnehmern, Zugriffe und etwaige Drittlandübermittlungen, Löschfristen und ein sicherer Übertragungsweg zu vereinbaren. Bis zur Klärung sollen ausschließlich synthetische oder nachweislich anonymisierte Testdaten verwendet werden; bloß pseudonymisierte Daten bleiben personenbezogen.

10 Personenbezogene Daten

Die Parteien halten die jeweils anwendbaren Datenschutzvorschriften ein und beschränken Daten auf das erforderliche Maß. Diese Vereinbarung erlaubt für sich genommen weder eine Verarbeitung personenbezogener Daten noch einen Zugriff durch ABBYY oder andere Dritte. Erforderliche Datenschutzvereinbarungen und Freigaben sind vor Übermittlung oder Zugriff zu dokumentieren. Die Geheimhaltungspflichten bestehen daneben fort.

11 Haftung, Recht und Änderungen

Die Haftung richtet sich nach den gesetzlichen Vorschriften; eine pauschale Haftungsfreizeichnung wird nicht vereinbart. Es gilt deutsches Recht. Die Zuständigkeit der Gerichte richtet sich nach den gesetzlichen Vorschriften; ein ausschließlicher Gerichtsstand wird mit diesem Muster nicht festgelegt. Änderungen und Ergänzungen sollen zu Nachweiszwecken in Textform dokumentiert werden; zwingende gesetzliche Formerfordernisse und der Vorrang individueller Abreden bleiben unberührt.

12 Wirksamwerden und Gegenzeichnung

Diese Vereinbarung wird erst mit Unterzeichnung durch vertretungsberechtigte Personen beider Parteien wirksam; maßgeblich ist das Datum der letzten Unterschrift. Eine einseitige Unterzeichnung genügt nicht. Beide Parteien erhalten eine beiderseits unterzeichnete Ausfertigung. Eine Rückwirkung für vor Wirksamwerden ausgetauschte Informationen ist nicht vorgesehen und wäre gesondert zu vereinbaren.

Für Partei A

EDV-Partner Ingenieurgesellschaft für Informationstechnologie mbH

Ort, Datum

Name, Funktion

Unterschrift / Gegenzeichnung

Für Partei B

Gegenpartei gemäß Seite 1

Ort, Datum

Name, Funktion

Unterschrift / Gegenzeichnung