ANLAGE III

VERARBEITUNGSBLATT

Besondere Bedingungen zum Allgemeinen Auftragsverarbeitungsvertrag

Art. 28 Verordnung (EU) 2016/679 („**DSGVO**")

Zwischen

dem **Verantwortlichen**, wie im Auftragsverarbeitungsvertrag bestimmt, vertreten durch seinen mit den erforderlichen Befugnissen ausgestatteten gesetzlichen Vertreter,

und

dem **Auftragsverarbeiter**, wie im Auftragsverarbeitungsvertrag bestimmt, vertreten durch seinen mit den erforderlichen Befugnissen ausgestatteten gesetzlichen Vertreter,

Der Verantwortliche und der Auftragsverarbeiter können im Folgenden gemeinsam als „**Parteien"** und einzeln als „**Partei"** bezeichnet werden.

VORBEMERKUNGEN

I. die Parteien haben den Allgemeinen Auftragsverarbeitungsvertrag („Auftragsverarbeitungsvertrag") unterzeichnet, der die Bedingungen und Modalitäten der Verarbeitung personenbezogener Daten regelt, die der Auftragsverarbeiter im Rahmen der Bereitstellung der den Gegenstand des Vertrags bildenden Dienste durchführt;

II. gemäß dem vorgenannten Auftragsverarbeitungsvertrag wird die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung bestimmter Dienste durch Verarbeitungsblätter geregelt, die deren operative Merkmale, die Kategorien der verarbeiteten Daten, die Zwecke, die angewandten Sicherheitsmaßnahmen sowie die etwaige Einbeziehung von Unterauftragsverarbeitern festlegen;

III. dieses Verarbeitungsblatt legt die Einzelheiten des Dienstes im Einklang mit dem Auftragsverarbeitungsvertrag fest. Es ergänzt und vervollständigt die allgemeinen Bestimmungen des Auftragsverarbeitungsvertrags und bildet einen integralen und für die Parteien verbindlichen Bestandteil derselben;

IV. im Falle eines Widerspruchs zwischen den Bestimmungen dieses Verarbeitungsblatts und denjenigen des Auftragsverarbeitungsvertrags gehen die Bestimmungen des Auftragsverarbeitungsvertrags vor, sofern das Verarbeitungsblatt nicht ausdrücklich zwischen den Parteien vereinbarte Abweichungen vorsieht;

V. soweit darin nicht ausdrücklich etwas anderes vorgesehen ist, gelten die Bestimmungen und Definitionen des Auftragsverarbeitungsvertrags und des Vertrags, auf die hiermit vollumfänglich Bezug genommen wird.

Dies vorausgeschickt, führen die Parteien in der nachstehenden Tabelle die Einzelheiten der Verarbeitung personenbezogener Daten in Bezug auf den Dienst auf, einschließlich Angaben zu den Zwecken, den Kategorien der verarbeiteten Daten, den angewandten Sicherheitsmaßnahmen und allen sonstigen für die Zwecke des Auftragsverarbeitungsvertrags relevanten Einzelheiten.

	BESCHREIBUNG
DIENST	*eSignAnyWhere* (eSAW) – *Namirial Sign Enterprise* (NSE)
ERBRINGENDES UNTERNEHMEN	**Namirial S.p.A.** Sofern das Erbringende Unternehmen nicht mit dem im Kommerziellen Angebot bestimmten Anbieter identisch ist, handelt es als Konzerninterner Unterauftragsverarbeiter im Auftrag des

	Anbieters auf der Grundlage bereits bestehender, mit Artikel 28 DSGVO konformer konzerninterner Vereinbarungen zwischen den Gesellschaften der Namirial-Gruppe.
ART DER VERARBEITUNG	Der Auftragsverarbeiter darf die Personenbezogenen Daten des Verantwortlichen im Rahmen der Bereitstellung des Dienstes verarbeiten, soweit dies für die Erbringung der vertraglichen Leistungen unbedingt erforderlich ist, und zwar in Form von: Erheben, Erfassen, Organisieren oder Ordnen, Abfragen, Verarbeiten, Auswählen, Auslesen, Abgleichen, Verwenden, Offenlegen, Löschen oder Vernichten.
ZWECK DER VERARBEITUNG	Abschluss des Vertrags und Erbringung der den Gegenstand des Vertrags bildenden Leistungen.
BEREITSTELLUNGSMODELL	*SaaS (Shared/Private)*
KATEGORIEN BETROFFENER PERSONEN	• Endkunden; • Nutzer des Dienstes; • Mitarbeiter.
KATEGORIEN VERARBEITETER PERSONENBEZOGENER DATEN	Die vom Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeiteten Personenbezogenen Daten gehören zu den folgenden Kategorien. **ALLGEMEINE DATEN:** • **Stammdaten** (Vorname, Nachname, E-Mail, Geburtsdatum, Geburtsort, Land, Geschlecht, Steuernummer, Wohnsitz-/Aufenthaltsanschrift); • **Kontaktdaten** (E-Mail, Telefonnummer); • **Navigationsdaten** (IP-Adresse); • **Sonstige etwaige Daten**: Daten, die in den auf die Signaturplattform hochgeladenen Dokumenten enthalten sind. **BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN:** • **Sonstige etwaige Daten**: besondere Kategorien von Daten, die in den auf die Signaturplattform hochgeladenen Dokumenten enthalten sind.
ORT DER DATENSPEICHERUNG	Die Daten werden auf Servern des Auftragsverarbeiters und/oder der Unterauftragsverarbeiter innerhalb der Europäischen Union/des EWR gespeichert.
DAUER DER VERARBEITUNG PERSONENBEZOGENER DATEN	Die Verarbeitung der Personenbezogenen Daten zum Zwecke der Bereitstellung der Dienste hat folgende Dauer: die gesamte Laufzeit des Vertrags mit dem Verantwortlichen; die gesamte Laufzeit des Auftragsverarbeitungsvertrags mit dem Verantwortlichen, sofern dieser, aus welchem Grund auch immer, länger als die Laufzeit des Vertrags ist. Nach Ablauf der vorgenannten Zeiträume ist dem Auftragsverarbeiter eine weitere Speicherung der Personenbezogenen Daten gestattet, soweit dies der Erfüllung besonderer gesetzlicher Pflichten oder Anordnungen der zuständigen Behörden dient.

	Die Speicherung der Personenbezogenen Daten ist ferner ausschließlich gestattet, soweit diese Personenbezogenen Daten für den Auftragsverarbeiter zum Nachweis, zur Geltendmachung oder zur Verteidigung eigener Rechte erforderlich sind, und zwar für einen Zeitraum von höchstens 10 Jahren.
SICHERHEITSMASSNAHMEN	Siehe **Anlage III A - TECHNISCHE UND ORGANISATORISCHE SICHERHEITSMASSNAHMEN**
UNTERAUFTRAGSVERARBEITER	Das Erbringende Unternehmen des Dienstes (in der vorstehenden Zeile bestimmt) bedient sich für die Erbringung des Dienstes anderer Gesellschaften der Namirial-Gruppe sowie ausgewählter Dritter, die Garantien für die Vertraulichkeit der Daten bieten. Die aktuelle Liste ist in Anlage III B enthalten und gegliedert in **Tabelle A** (an der Erbringung des Dienstes beteiligte Gesellschaften der Namirial-Gruppe, die auf der Grundlage bereits bestehender, mit Artikel 28 DSGVO konformer und von diesem Auftragsverarbeitungsvertrag gesonderter konzerninterner Vereinbarungen tätig werden) und **Tabelle B** (dritte Unterauftragsverarbeiter). Einige dieser Dritten können auch außerhalb des Europäischen Wirtschaftsraums (EWR), einschließlich der Vereinigten Staaten, tätig sein. Um die Einhaltung der DSGVO (Art. 44-49) und der Vorschriften zum Schutz personenbezogener Daten sicherzustellen, kann der Anbieter geeignete Mechanismen für die Datenübermittlung einsetzen. Diese Dritten werden im Einklang mit den Bestimmungen des Auftragsverarbeitungsvertrags ausgewählt, erhalten genaue Weisungen zur Datenverarbeitung und führen ausschließlich die erforderlichen Tätigkeiten unter Beachtung der erteilten Vorgaben durch. Die aktuelle Liste dieser Dritten ist in Anlage III B dieses Dokuments enthalten.

ANLAGE III - A

TECHNISCHE UND ORGANISATORISCHE SICHERHEITSMASSNAHMEN

Die in dieser Anlage beschriebenen Sicherheitsmaßnahmen gelten zusätzlich zu den im Auftragsverarbeitungsvertrag vorgesehenen Maßnahmen und stellen ein zusätzliches Schutzniveau für die durch das Verarbeitungsblatt, dem sie beigefügt sind, geregelten Verarbeitungen dar. Sie werden angewandt von und sind anwendbar auf das Erbringende Unternehmen des vertraglichen Dienstes, das mit dem Auftragsverarbeiter identisch sein kann oder nicht.

1. TECHNISCHE SICHERHEITSMASSNAHMEN

ART DER MASSNAHME	BESCHREIBUNG
Maßnahmen zur dauerhaften Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung	Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten übermittelt werden. Insbesondere setzt das Erbringende Unternehmen die folgenden technischen und organisatorischen Maßnahmen um: • Nutzung von VPN; • Protokollierung der Zugriffe und der relevanten Vorgänge; • Bereitstellung des Dienstes über verschlüsselte Verbindungen wie sftp, https und secure cloudstores; • Einsatz von Signaturverfahren (je nach gewählter Signaturstufe); Erfassung der Vorgänge zum Abruf und zur Übermittlung der Daten; • Übermittlung in anonymisierter oder pseudonymisierter Form; • sorgfältige Auswahl des Personals und der Transportmittel für Dokumente; kodiertes Übergabeverfahren. Weitere Maßnahmen sind in den folgenden internen Richtlinien festgelegt: SCS-P01 Group Information Security Policy; SCS-P14 Group Privacy and Personal Data Protection Policy.
Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	Maßnahmen, mit denen die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können. Insbesondere setzt das Erbringende Unternehmen die folgenden technischen und organisatorischen Maßnahmen um: • Überwachung und Meldung der Backups; • Wiederherstellung mittels Automatisierungswerkzeugen; • Backup-Konzept und Recovery-Prozess entsprechend den spezifischen Kritikalitäten und den Anforderungen des Kunden; • Kontrolle des Backup-Prozesses • regelmäßiger Test des Datenwiederherstellungsprozesses und Dokumentation der Ergebnisse; • Aufbewahrung der Backup-Datenträger an einem sicheren Ort außerhalb des Serverraums. Weitere Maßnahmen sind in den folgenden internen Richtlinien festgelegt: Notfallplan; SCS-P01 Group Information Security Policy; Work instruction operational security.

Maßnahmen zum Schutz der Daten während der Speicherung	Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten vor zufälliger Zerstörung oder zufälligem Verlust (USV, Klimatisierung, Brandschutz, Datensicherung, sichere Aufbewahrung von Datenträgern, Virenschutz, RAID-Systeme, Festplattenspiegelung usw.). **Technische Maßnahmen** • Brandmeldesysteme; • Feuerlöscher im Serverraum; • Überwachung der Temperatur und der Luftfeuchtigkeit im Serverraum; • Kontrolle der Belüftung des Serverraums; USV-System und Notstrom-Dieselgeneratoren; • RAID-System / Festplattenspiegelung; • Videoüberwachung des Serverraums; • Alarmmeldung bei unbefugtem Zutritt zum Serverraum. **Organisatorische Maßnahmen** • Backup-Dienst; • keine Wasserleitungen im Serverraum; • Aufbewahrung der Backup-Datenträger an einem sicheren Ort außerhalb des Serverraums; • getrennte Partitionen für Betriebssysteme und Daten, soweit erforderlich. Weitere Maßnahmen sind in den folgenden internen Richtlinien festgelegt: Notfallplan; SCS-P01 Group Information Security Policy; Work instruction operational security.
Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen	**Vom Auftragsverarbeiter getroffene organisatorische Maßnahmen**: • dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenschutzverletzungen (siehe SCS-P04 Group Incident Management & Reporting Policy); • formalisiertes Verfahren für die Behandlung von Sicherheitsvorfällen (siehe SCS-P04 Group Incident Management & Reporting Policy); • Einbindung des DSB und des CISO bei Sicherheitsvorfällen und Datenschutzverletzungen; Dokumentation der Sicherheitsvorfälle und Datenschutzverletzungen über das Ticketsystem (mittels des Tools „Jira“); • formaler Prozess zur Nachverfolgung von Sicherheitsvorfällen und Datenschutzverletzungen (siehe SCS-P04 Group Incident Management & Reporting Policy). Weitere Maßnahmen sind in den folgenden internen Richtlinien festgelegt: SCS-P01 Group Information Security Policy; SCS-P14 Group Privacy and Personal Data Protection Policy; Work instruction operational security; Work instruction IT user regulations.
Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration	Der Auftragsverarbeiter setzt die folgenden Maßnahmen zur Gewährleistung der Systemintegrität um: Einsatz einer regelmäßig aktualisierten Firewall; Einsatz eines regelmäßig aktualisierten Spamfilters; Einsatz eines regelmäßig aktualisierten Virenscanners; Intrusion-Detection-System (IDS) für die Systeme des Kunden; Intrusion-Prevention-System (IPS) für die Systeme des Kunden.

Maßnahmen der internen IT sowie des Managements und der Governance der IT-Sicherheit	Das System ist nach ISO/IEC 27001 zertifiziert.
Maßnahmen zur Gewährleistung einer begrenzten Datenspeicherung	Es werden die Sicherheitskontrollen nach OWASP Secure Mobile Development durchgeführt (siehe SCS-P08 Group Secure Coding Policy). Analyse des Perimeters der Webanwendungen.
Maßnahmen zur Gewährleistung der Rechenschaftspflicht	Die Mitarbeiter des Auftragsverarbeiters werden fortlaufend über den Datenschutz informiert und geschult und sind vertraglich zur Verschwiegenheit und zur Vertraulichkeit der Daten verpflichtet. Dritte, die im Rahmen ihrer Tätigkeit für das Erbringende Unternehmen mit personenbezogenen Daten in Berührung kommen können, werden vor Beginn ihrer Tätigkeit durch ein NDA (Non-Disclosure Agreement) zur Verschwiegenheit und Vertraulichkeit verpflichtet, um den Datenschutz und das Datengeheimnis zu wahren. Die an der Erbringung des Dienstes beteiligten Gesellschaften der Namirial-Gruppe handeln auf der Grundlage bereits bestehender konzerninterner Vereinbarungen zwischen den Gesellschaften der Namirial-Gruppe, die mit Artikel 28 DSGVO konform und von diesem Auftragsverarbeitungsvertrag getrennt sind.
Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung	Der Auftragsverarbeiter sieht Maßnahmen vor, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

ANLAGE III - B

UNTERAUFTRAGSVERARBEITER

Diese Anlage enthält die Liste der zum Zeitpunkt der Unterzeichnung des betreffenden Verarbeitungsblatts genehmigten Unterauftragsverarbeiter gemäß des Auftragsverarbeitungsvertrags.

Die aufgeführten Stellen wurden nach Kriterien der Erfahrung, Zuverlässigkeit und der Garantien für die Einhaltung der anwendbaren Vorschriften ausgewählt, insbesondere der Bestimmungen von Art. 28 der Verordnung (EU) 2016/679.

Sie handeln unter der Weisungsbefugnis des Auftragsverarbeiters, halten sich an die erhaltenen Weisungen und treffen angemessene Sicherheitsmaßnahmen zum Schutz der verarbeiteten Personenbezogenen Daten.

Die Liste der Unterauftragsverarbeiter kann im Laufe der Zeit nach Maßgabe der Bestimmungen des Auftragsverarbeitungsvertrags aktualisiert werden.

TABELLE A

AN DER ERBRINGUNG DES DIENSTES BETEILIGTE GESELLSCHAFTEN DER NAMIRIAL-GRUPPE

FIRMA	ANSCHRIFT	ORT DER VERARBEITUNG	TÄTIGKEITSBEREICH
Namirial SPA	Via Caduti sul Lavoro 4 – Senigallia (AN) Italia	EEA	Anbieter des Dienstes
Namirial GmbH	Seilerstatte 16/Tur 14, 1010 Vienna, Austria	EEA	IT

TABELLE B

DRITTE UNTERAUFTRAGSVERARBEITER

FIRMA	ANSCHRIFT	ORT DER VERARBEITUNG	TÄTIGKEITSBEREICH
AWS EMEA SARL	Luxembourg, 38 Avenue John F. Kennedy L-1855	EEA	Cloud-Dienste
Zendesk Inc.	989 Market St, San Francisco, CA 94103	EEA	Verwaltung der Support-Tickets
Atlassian B.V.	Amsterdam Singel 236 1016 AB Amsterdam, Netherlands	EEA	Verwaltung der Support-Tickets
Exalate NV	Roderveldlaan 2 bus 3, 2600 Berchem, Belgium	EEA	Synchronisierung der Support-Tickets
Var Group S.p.A. (Yarix)	Via della Piovola, 138 – 50053, Empoli FI	EEA	SOC (Security Operation Center) und MOC (Monitoring Operation Center)

Fastweb S.p.A.	Milano (MI) Piazza Adriano Olivetti 1	EEA	SMS Provider
Orange Espagne, S.A.U.	Paseo Club Deportivo 1, 28223 Pozuelo de Alarcón	EEA	SMS Provider
Twilio Ireland Ltd.	25-28 North Wall Quay, Dublino, Irlanda	EEA/USA	SMS/E-mail Provider
Link Mobility Italia S.r.l.	Via Paolo Da Cannobio 37 - 20122 - Milano (Mi), Italia	EEA	SMS Provider
MailJet SAS	43, Rue de Dunkerque , Paris, France 75010	EEA	E-Mail Provider
Vonage B.V.	Radarweg 29A 12, Office 10.42, 1043 NX Amsterdam, The Netherlands	EEA	SMS Provider
Mitto AG	Bahnhofstrasse 21, Zug CH-6300, Switzerland	EEA	SMS Provider
Dynatrace S.r.l.	Viale Enrico Forlanini, 23 20134 Milano (MI) Italia	EEA	Log monitoring