INFOMINDS SPA

Sede legale ed amministrativa
BRESSANONE
Via Brennero, 72
I-39042 Bressanone (BZ)

T. +39 0472 057 700
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

VERTRAG ZWISCHEN VERANTWORTLICHEM UND AUFTRAGSVERARBEITER

GEMÄSS ART. 28 DER VERORDNUNG (EU) 2016/679

Zwischen

_____, mit Sitz in _____, MwSt.-Nr. _____, Telefon _____, E-Mail _____ und PEC: _____ als Verantwortlicher (nachfolgend auch „**Verantwortlicher**"),

und

INFOMINDS S.p.A., mit Rechtssitz in der Brennerstraße 72 – 39042 Brixen (BZ), MwSt.-Nr. 00899390215, Telefon 0472057700, E-Mail info@infominds.eu, PEC info@pec.infominds.eu (nachfolgend auch „**Auftragsverarbeiter**").

Vorausgeschickt, dass:

- zwischen dem Verantwortlichen und INFOMINDS S.P.A. ein oder mehrere Vertragsverhältnisse bestehen, die einen oder mehrere von INFOMINDS S.P.A. erbrachte IT-Dienstleistungen zum Gegenstand haben (nachfolgend auch „Hauptvertrag");
- INFOMINDS S.P.A. bei der Erbringung dieser Dienstleistungen personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten kann;
- das Personal von INFOMINDS S.P.A. im Zusammenhang mit den übertragenen Tätigkeiten Funktionen ausüben könnte, die der Rolle eines Systemadministrators im Sinne der Maßnahme der italienischen Datenschutzbehörde (Garante per la protezione dei dati personali) vom 27. November 2008 in der jeweils geltenden Fassung zuzuordnen sind, soweit es an Systemen, Datenbanken, Netzwerken, Zugangsdaten oder Geräten tätig wird, bei denen ein – auch zufälliger – Zugriff auf personenbezogene Daten möglich ist;
  Ferner vorausgeschickt, dass:

- der Auftragsverarbeiter hinreichende Garantien dafür bieten muss, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der jeweils geltenden Vorschriften erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet;
- der Auftragsverarbeiter personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen verarbeiten darf, die durch diesen Vertrag sowie durch etwaige spätere Weisungen oder Vereinbarungen erteilt wird;
- die Übertragung der Funktionen eines Systemadministrators nach vorheriger Bewertung der Erfahrung, Fähigkeiten und Zuverlässigkeit der benannten Person erfolgen muss;

Dies vorausgeschickt, vereinbaren die Parteien – unter Verpflichtung zur Einhaltung der geltenden Datenschutzvorschriften, insbesondere der Verordnung (EU) 2016/679 („DSGVO“) und des Gesetzesvertretenden Dekrets Nr. 196/2003 – Folgendes:

1. Bestellung des Auftragsverarbeiters

Der Verantwortliche für die Verarbeitung der im Rahmen seiner Tätigkeit verwalteten personenbezogenen Daten bestellt INFOMINDS S.P.A. zum Auftragsverarbeiter gemäß Art. 28 DSGVO und ermächtigt ihn, alle – und ausschließlich – die Datenverarbeitungen durchzuführen, die zur Erbringung der Dienstleistungen gemäß dem „Hauptvertrag“ erforderlich sind.

Der Auftragsverarbeiter bestätigt, über Fachwissen, Zuverlässigkeit sowie wirtschaftliche, organisatorische und betriebliche Ressourcen – auch in Bezug auf das für die Verarbeitungstätigkeiten eingesetzte Personal – zu verfügen, die die Umsetzung geeigneter technischer und organisatorischer Maßnahmen zum Schutz der im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten ermöglichen.

2. Tätigkeitsbereich als Systemadministrator

Im Zusammenhang mit den Dienstleistungen des Hauptvertrags könnte das Personal von INFOMINDS S.P.A. die Rolle eines Systemadministrators („ADS“) einnehmen.

INFOMINDS S.P.A. verpflichtet sich daher, die Pflichten aus der Maßnahme der italienischen Datenschutzbehörde vom 27. November 2008 in der jeweils geltenden Fassung zu erfüllen, und insbesondere:

- als Systemadministratoren ausschließlich Personen zu benennen, die unter Berücksichtigung ihrer Berufserfahrung sowie der bei der Ausübung ihrer Aufgaben nachgewiesenen Fähigkeiten und Zuverlässigkeit die erforderlichen Voraussetzungen erfüllen, um diese Funktion im Einklang mit den geltenden Vorschriften auszuüben;
- ein namentliches Verzeichnis der mit Systemadministratorfunktionen betrauten natürlichen Personen aktuell zu halten, das mindestens Vorname, Nachname, Rolle/Funktion, Tätigkeitsbereich, betroffene Systeme oder Dienste und Berechtigungszeitraum enthält, und es dem Verantwortlichen auf Anfrage mit angemessener Vorlaufzeit von mindestens 15 (fünfzehn) Arbeitstagen zur Verfügung zu stellen. Das Verzeichnis ist bei neuen Benennungen, Beendigungen oder Änderungen der Tätigkeitsbereiche unverzüglich zu aktualisieren;
- regelmäßige Kontrollen der Tätigkeit der benannten Systemadministratoren sowie der von ihnen durchgeführten logischen Zugriffe auf Verarbeitungssysteme und elektronische Archive gemäß den Vorgaben der Maßnahme der Datenschutzbehörde durchzuführen;
- die Protokollierung administrativer Zugriffe, soweit technisch anwendbar, sicherzustellen und die Logs gemäß den Fristen und Modalitäten aufzubewahren, die mit den Vorschriften und den Weisungen des Verantwortlichen im Einklang stehen. Die Logs werden vor unbefugten Veränderungen geschützt und für mindestens sechs Monate aufbewahrt, sofern vom Verantwortlichen oder von den geltenden Vorschriften keine abweichende Frist vorgesehen ist.

In Bezug auf diese Bestellung legt der Verantwortliche im Rahmen der tatsächlich übertragenen Dienstleistungen die folgenden zulässigen Tätigkeitsbereiche fest:

Tätigkeitsbereich	Funktionen	Beschreibung der Funktionen	Anwendbarkeit JA/NEIN
Verwaltung von Geräten und Arbeitsplätzen	Support und Wartung	Eingriffe an anvertrauter Hardware, Arbeitsplätzen und Peripheriegeräten; gegebenenfalls Austausch oder Wiederherstellung von Geräten	
Verwaltung von ERP-/Verwaltungssoftware	Installation und Aktualisierung	Wartung, Aktualisierung sowie korrektive, adaptive und evolutive Betreuung der Software	
Verwaltung von ERP-/Verwaltungssoftware	Profile und Zugangsdaten	Unterstützung bei der Verwaltung von Benutzerkonten, Zugangsdaten und Berechtigungsprofilen, sofern im Leistungsumfang vorgesehen	
Datenbanken und Anwendungsarchive	Wartung	Eingriffe in Datenbanken, Anwendungsarchive, Abfrage-, Sicherungs- und Wiederherstellungsverfahren	
Backup und Recovery	Verwaltung und Überprüfung	Durchführung, Überprüfung, Wiederherstellung und Test von Backups der anvertrauten Daten und Systeme	
Digitale/elektronische Langzeitarchivierung	Dokumentenmanagement	Erstellung, Korrektur, Signatur, Übermittlung zur Archivierung und Verwaltung der Metadaten digitaler Dokumente im Rahmen des Leistungsumfangs	
Elektronische Rechnungsstellung	Verwaltung der Datenflüsse	Unterstützung bei den Flüssen der ausgehenden und eingehenden elektronischen Rechnungen, sofern aktiviert	
Fernzugriff und Support	Technischer Support	Fernverbindungen oder Einsätze vor Ort beim Verantwortlichen für Support, Wartung und Störungsbehebung	

Logging und Monitoring	Technische Kontrollen	Überprüfung der System-/Anwendungslogs und Fehler, sofern vorgesehen und technisch anwendbar	

Bei der Ausübung der vorgenannten Funktionen könnte INFOMINDS S.P.A. Zugriff auf personenbezogene Daten des Verantwortlichen haben und ist berechtigt, diese ausschließlich in dem Umfang zu verarbeiten, der zur Ausführung der übertragenen Aufgaben und Tätigkeiten erforderlich ist. Weitere Verarbeitungsvorgänge außerhalb der in diesem Vertrag oder in weiteren förmlichen Weisungen des Verantwortlichen vereinbarten Vorgänge dürfen nicht durchgeführt werden.

3. Vertragsdauer

Dieser Vertrag tritt mit der Unterzeichnung durch beide Parteien in Kraft und hat dieselbe Laufzeit wie der Hauptvertrag. Sollte der Hauptvertrag aus irgendeinem Grund entfallen oder seine Wirksamkeit verlieren oder die Dienstleistung des Hauptvertrags nicht mehr erbracht werden, endet auch dieser Vertrag automatisch, unbeschadet der Pflichten, die ihrer Natur nach fortbestehen.

4. Allgemeine Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter ist kraft Gesetzes und dieses Vertrags für sich selbst und für die zur Verarbeitung befugten Personen, die in seiner Organisation mitarbeiten, verpflichtet:

1. die Daten nur für die oben genannten Zwecke und zur Erbringung der angegebenen oder sich aus weiteren schriftlichen Weisungen des Verantwortlichen ergebenden Vertragsleistungen zu verarbeiten, auch in Bezug auf eine etwaige Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation;
2. die Daten gemäß den dokumentierten Weisungen des Verantwortlichen zu verarbeiten; ist er der Auffassung, dass eine Weisung gegen die DSGVO oder andere geltende Datenschutzbestimmungen verstößt, den Verantwortlichen unverzüglich zu informieren;
3. den Verantwortlichen vor der Verarbeitung über eine etwaige Verpflichtung zur Übermittlung von Daten an ein Drittland oder eine internationale Organisation nach dem Recht der Union oder des Mitgliedstaats, dem er unterliegt, zu informieren, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
4. die Vertraulichkeit der im Rahmen dieses Vertrags verarbeiteten personenbezogenen Daten zu gewährleisten;
5. innerhalb seiner Organisation die zur Verarbeitung befugten natürlichen Personen zu bestimmen und zu benennen, ihnen angemessene schriftliche Anweisungen zu den Verarbeitungsmodalitäten zu erteilen und sie – auch für die Zeit nach Beendigung des Verhältnisses – zur Vertraulichkeit zu verpflichten;
6. die Identifikationsdaten der gegebenenfalls als Systemadministratoren eingesetzten natürlichen Personen unmittelbar und gesondert aufzubewahren und sie dem Verantwortlichen auf Anfrage mit angemessener Vorlaufzeit von mindestens 15 (fünfzehn) Arbeitstagen umgehend zur Verfügung zu stellen;
7. bei der Verwendung von Materialien, Produkten, Anwendungen oder Diensten die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu berücksichtigen;

8. personenbezogene Daten des Verantwortlichen nicht über das zur Erbringung der Dienstleistung erforderliche oder gesetzlich vorgeschriebene Maß hinaus auf eigenen Datenträgern zu speichern und in jedem Fall angemessene Sicherheitsmaßnahmen zu ergreifen.

5. Weitere Auftragsverarbeiter („Unterauftragsverarbeiter")

Der Verantwortliche ermächtigt den Auftragsverarbeiter bereits jetzt allgemein und im Voraus, für die Durchführung der Tätigkeiten dieses Vertrags einen oder mehrere Unterauftragsverarbeiter in Anspruch zu nehmen.

Der Auftragsverarbeiter gewährleistet, dass jeder Unterauftragsverarbeiter hinreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen gemäß den geltenden Datenschutzvorschriften bietet, und verpflichtet sich, ihn durch Vertrag oder ein anderes Rechtsinstrument zur Einhaltung von Datenschutzpflichten zu verpflichten, die den in diesem Vertrag vorgesehenen im Wesentlichen gleichwertig sind.

Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen im Rahmen der geltenden Vorschriften für die Erfüllung der Pflichten der Unterauftragsverarbeiter.

Die aktuelle Liste der Unterauftragsverarbeiter wird vom Auftragsverarbeiter auf Anfrage des Verantwortlichen zur Verfügung gestellt.

6. Sicherheitsmaßnahmen

Der Auftragsverarbeiter ist verpflichtet, die in Anlage 1 aufgeführten Sicherheitsmaßnahmen umzusetzen und darüber hinaus weitere dem Risiko angemessene technische und organisatorische Maßnahmen vorzusehen und umzusetzen, unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Der Auftragsverarbeiter muss ein dem Risiko angemessenes Schutzniveau gewährleisten, insbesondere gegen:

- die – unbeabsichtigte oder unrechtmäßige – Vernichtung, den Verlust, die Veränderung, die unbefugte Offenlegung von bzw. den unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden;
- die unzulässige oder nicht mit den Zwecken der Verarbeitungsvorgänge übereinstimmende Verarbeitung der Daten.

Der Auftragsverarbeiter erklärt ferner, sich bewusst zu sein, dass sich die vom Verantwortlichen geforderten Sicherheitsmaßnahmen gemäß Anlage 1 zur Gewährleistung ihrer Angemessenheit gegenüber den Risiken infolge einer regelmäßigen Überprüfung im Laufe der Zeit ändern können; hierüber wird der Auftragsverarbeiter vom Verantwortlichen ordnungsgemäß informiert, damit er etwa erforderliche Anpassungen prüfen kann.

Der Auftragsverarbeiter darf die im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten nicht für das Training, die Entwicklung oder Verbesserung von Systemen künstlicher Intelligenz, für Analytics, Profiling, Benchmarking, Datenanreicherung oder eigene Zwecke verwenden, es sei denn, es liegen eine vorherige schriftliche Genehmigung des Verantwortlichen und eine geeignete Rechtsgrundlage vor.

7. Information der betroffenen Personen

Es obliegt dem Verantwortlichen, den betroffenen Personen die nach den geltenden Vorschriften vorgesehenen Informationen über die durchgeführten Verarbeitungen personenbezogener Daten zu erteilen.

8. Ausübung der Rechte der betroffenen Personen

Im Rahmen seiner Zuständigkeit unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen auf Ausübung der Rechte der betroffenen Personen, einschließlich des Rechts auf Auskunft, Berichtigung, Löschung, Widerspruch, Einschränkung der Verarbeitung, Datenübertragbarkeit sowie des Rechts, nicht einer automatisierten Entscheidung unterworfen zu werden, soweit anwendbar.

Erhält der Auftragsverarbeiter Anträge von betroffenen Personen, hat er dies dem Verantwortlichen unverzüglich schriftlich, vorzugsweise per PEC, unter Beifügung einer Kopie des Antrags innerhalb von 5 Tagen nach Eingang mitzuteilen und den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung zu unterstützen.

9. Meldung von Verletzungen des Schutzes personenbezogener Daten (Data Breach)

Sobald dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, verpflichtet er sich, den Verantwortlichen zu informieren und mit dem Verantwortlichen sowie gegebenenfalls mit den zuständigen Behörden umfassend zusammenzuarbeiten, um die Pflichten aus den geltenden Vorschriften zu erfüllen.

Insbesondere meldet der Auftragsverarbeiter dem Verantwortlichen per PEC jede Verletzung oder vermutete Verletzung des Schutzes personenbezogener Daten innerhalb von höchstens 48 Stunden nach Kenntnisnahme und fügt alle zweckdienlichen Unterlagen bei, damit der Verantwortliche die Verletzung bewerten und sie gegebenenfalls der Aufsichtsbehörde melden und/oder den betroffenen Personen mitteilen kann.

Die Meldung muss mindestens:

- die Art der Verletzung des Schutzes personenbezogener Daten beschreiben, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der betroffenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen mitteilen;
- die wahrscheinlichen Folgen der Verletzung beschreiben;
- die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Abmilderung ihrer möglichen nachteiligen Auswirkungen beschreiben.

Wenn die Informationen nicht zur gleichen Zeit bereitgestellt werden können, können sie ohne unangemessene weitere Verzögerung schrittweise zur Verfügung gestellt werden.

10. Unterstützung bei der Datenschutz-Folgenabschätzung und der vorherigen Konsultation

Der Auftragsverarbeiter leistet dem Verantwortlichen in dem nach Art. 28 DSGVO erforderlichen Umfang und unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen angemessene

Unterstützung bei der gegebenenfalls erforderlichen Erstellung der Datenschutz-Folgenabschätzung (DSFA) und der vorherigen Konsultation der Aufsichtsbehörde.

Sofern die vom Verantwortlichen angeforderten Unterstützungsleistungen, die über die in den geltenden Vorschriften oder in diesem Vertrag vorgesehenen Unterstützungspflichten hinausgehen, einen Ressourceneinsatz des Auftragsverarbeiters von mehr als einem (1) Arbeitstag erfordern, vergütet der Verantwortliche dem Auftragsverarbeiter das auf Grundlage der jeweils geltenden Preislisten von INFOMINDS S.P.A. ermittelte Entgelt. Der Auftragsverarbeiter legt den geschätzten Aufwand im Voraus dar und erstellt nach Abschluss der Tätigkeiten eine geeignete Abrechnung der erbrachten Leistungen. Die Tätigkeiten werden nach Annahme des entsprechenden Angebots durch den Verantwortlichen ausgeführt.

11. Datenschutzbeauftragter

Der Auftragsverarbeiter hat einen eigenen Datenschutzbeauftragten benannt, der unter folgender E-Mail-Adresse erreichbar ist: dpo@acsgroup.it.

12. Verzeichnis aller Kategorien von Verarbeitungstätigkeiten

Der Auftragsverarbeiter erklärt, soweit nach den geltenden Vorschriften vorgesehen, ein schriftliches Verzeichnis aller Kategorien von im Auftrag des Verantwortlichen durchgeführten Verarbeitungstätigkeiten zu führen, das die nach Art. 30 Abs. 2 DSGVO erforderlichen Angaben enthält.

13. Dokumentation, Audits und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag und in den geltenden Vorschriften festgelegten Pflichten zur Verfügung und ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu diesen bei.

Audits können auch durch Anforderung von Unterlagen, Fragebögen, Zertifizierungen, unabhängige Auditberichte oder Remote-Prüfungen durchgeführt werden. Etwaige Inspektionen an den Standorten des Auftragsverarbeiters erfolgen mit angemessener Vorankündigung von mindestens 15 Arbeitstagen während der üblichen Geschäftszeiten und unter Beachtung der Sicherheits- und Vertraulichkeitsmaßnahmen des Auftragsverarbeiters. Werden wesentliche Nichtkonformitäten festgestellt, hat der Auftragsverarbeiter innerhalb angemessener, mit dem Verantwortlichen vereinbarter Fristen einen Maßnahmenplan (Remediation-Plan) zu erstellen und umzusetzen.

Der Auftragsverarbeiter ist ferner verpflichtet, dem Verantwortlichen Anträge betroffener Personen, Beanstandungen, Inspektionen oder Anfragen der Aufsichtsbehörde oder der Justizbehörden sowie alle sonstigen relevanten Informationen im Zusammenhang mit der Verarbeitung personenbezogener Daten unverzüglich mitzuteilen.

Werden Audit-, Prüf- oder Überprüfungstätigkeiten an einen Dritten delegiert und wird zwischen diesem und dem Auftragsverarbeiter ein Wettbewerbsverhältnis oder ein Interessenkonflikt festgestellt, kann der Auftragsverarbeiter die Durchführung der genannten Tätigkeiten durch den beauftragten Dritten ablehnen.

14. Pflichten des Verantwortlichen

Der Verantwortliche:

- erklärt, dass die an den Auftragsverarbeiter übermittelten personenbezogenen Daten im Einklang mit den geltenden Vorschriften erhoben und verwaltet wurden, wobei die Bestimmung der Rechtsgrundlage der Verarbeitung dem Verantwortlichen obliegt;
- verpflichtet sich, dem Auftragsverarbeiter jede erforderliche Änderung der Datenverarbeitungsvorgänge offiziell mitzuteilen;
- verpflichtet sich, etwaige zusätzliche Weisungen zur Datenverarbeitung durch den Auftragsverarbeiter schriftlich zu dokumentieren;
- überwacht während der gesamten Dauer der Verarbeitung die Einhaltung der Pflichten aus der DSGVO durch den Auftragsverarbeiter.

Dieser Vertrag gilt ausschließlich für Verarbeitungen, die der Auftragsverarbeiter im Auftrag des Verantwortlichen und auf Grundlage von dessen dokumentierten Weisungen durchführt. Verarbeitet der Auftragsverarbeiter im Rahmen des Vertragsverhältnisses personenbezogene Daten für eigene Zwecke oder zur Erfüllung eigener rechtlicher Pflichten, ist diese Verarbeitung gesondert einzuordnen und wird – vorbehaltlich einer abweichenden schriftlichen Vereinbarung der Parteien – nicht durch diesen Vertrag geregelt.

15. Rückgabe oder Löschung der Daten nach Beendigung der Leistungen

Bei Beendigung der Dienstleistungen dieses Vertrags – gleich aus welchem Grund – ist der Verantwortliche berechtigt, seine personenbezogenen Daten innerhalb von fünfzehn (15) Tagen ab dem Datum der Beendigung der Dienstleistung abzurufen und zu migrieren.

Nach Ablauf dieser Frist und vorbehaltlich abweichender Bestimmungen der geltenden Vorschriften kann der Auftragsverarbeiter die im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten ohne weitere Mitteilung löschen.

Es gilt als vereinbart, dass der Verantwortliche für die Extraktion und Migration seiner Daten innerhalb der genannten Frist verantwortlich ist. Auf Anfrage des Verantwortlichen kann der Auftragsverarbeiter Unterstützungsleistungen bei der Migration erbringen, die auf Grundlage der jeweils geltenden Preislisten von INFOMINDS S.P.A. gesondert angeboten werden.

Der Auftragsverarbeiter kann die personenbezogenen Daten nach Beendigung der Dienstleistung in dem Umfang und für die Dauer aufbewahren, die nach den geltenden Vorschriften erforderlich sind, oder wenn dies zur Geltendmachung, Ausübung oder Verteidigung eigener Rechtsansprüche erforderlich ist.

Auf Anfrage des Verantwortlichen stellt der Auftragsverarbeiter eine Bestätigung über die erfolgte Löschung der personenbezogenen Daten aus, unbeschadet gesetzlicher Aufbewahrungspflichten.

16. Vergütungen, Entschädigungen oder Erstattungen

Die Bestellung zum Auftragsverarbeiter begründet für sich genommen keine Vergütungen, Entschädigungen oder Erstattungen über die im Hauptvertrag vorgesehenen hinaus.

Die Parteien vereinbaren, dass etwaige vom Verantwortlichen angeforderte und nicht ausdrücklich in den Dienstleistungen des Hauptvertrags enthaltene Tätigkeiten – einschließlich, beispielhaft und nicht abschließend, Unterstützungsleistungen im Zusammenhang mit der Ausübung der Rechte betroffener Personen, Audits, Prüfungen, Inspektionen, Anfragen der zuständigen Behörden, Folgenabschätzungen oder sonstiger Tätigkeiten, die einen erheblichen Ressourceneinsatz des Auftragsverarbeiters erfordern – gesondert auf Grundlage der zum Zeitpunkt der Anfrage geltenden Tarife des Auftragsverarbeiters oder gemäß einer abweichenden Vereinbarung der Parteien vergütet werden können.

17. Widerruf und Ersetzung früherer Vereinbarungen

Mit diesem Vertrag werden alle sonstigen Akte, Bestellungen, Verträge oder Vereinbarungen zwischen den Parteien betreffend die Verarbeitung personenbezogener Daten ausdrücklich widerrufen und ersetzt, soweit sie dieselben Dienstleistungen des Hauptvertrags betreffen.

Ort und Datum: _____

_____ Verantwortlicher _____	INFOMINDS S.P.A. Auftragsverarbeiter _____

Anlage 1 - VERZEICHNIS DER TECHNISCHEN UND ORGANISATORISCHEN SICHERHEITSMASSNAHMEN

VERZEICHNIS DER TECHNISCHEN UND ORGANISATORISCHEN SICHERHEITSMASSNAHMEN	
Übergeordnete Richtlinie zu Cybersecurity / Informationssicherheit / IT-Sicherheit.	Einschließlich Zielen und Grundsätzen
	Von der obersten Leitung genehmigt
	Allen relevanten internen und externen Stellen zugänglich gemacht
	Mindestens jährlich aktualisiert
Themenspezifische Richtlinien und Verfahren, die mit der übergeordneten Richtlinie verknüpft sind.	Zur Regelung des Vorfallmanagements
	Zur Regelung der physischen Zutrittskontrolle
	Zur Regelung der logischen Zugriffskontrolle
	Zur Regelung der zulässigen Nutzung von IT-Ressourcen
	Zur Regelung des Update-Managements
	Zur Regelung des Change-Managements
	Zur Regelung der sicheren Softwareentwicklung
	Zur Regelung des Lebenszyklusmanagements von Systemen
	Zur Regelung der Klassifizierung von Informationen
	Zur Regelung des Log-Managements
	Zur Regelung des Datenlebenszyklus
	Zur Regelung des Lieferantenmanagements
Plan für das Business Continuity Management.	Der mindestens jährlich getestet wird
	Der den IT-Bereich mit einer zugehörigen Business Impact Analysis umfasst
	Der einen Disaster-Recovery-Plan für kritische Dienste vorsieht
	Der mindestens jährlich aktualisiert wird
Kontinuitätsplan für IKT-Systeme.	Mit so bemessener Ressourcenzuweisung, dass die Verfügbarkeit stets gewährleistet ist
	Mit lokaler Redundanz aller kritischen Systeme durch Hochverfügbarkeitslösungen

	Mit geografischer Redundanz aller kritischen Systeme an einem entfernten Standort, der mehr als 50 km vom Primärstandort entfernt liegt
Formalisierung der Verantwortlichkeiten für Cybersecurity / Informationssicherheit / IT-Sicherheit	Sie sind einem Informationssicherheits- / Cybersecurity-Beauftragten oder CISO zugewiesen, der an die IT-Leitung oder eine höhere Ebene berichtet
	Sie sind den Verantwortlichen für Informationssysteme zugewiesen, um deren Schutz zu gewährleisten
	Sie sind dem gesamten Personal zugewiesen, damit Informationen und Informationssysteme ordnungsgemäß genutzt werden
	Sie sind Dritten zugewiesen, die eine Rolle beim Schutz der Informationen spielen
	Sie sind denjenigen zugewiesen, die im Notfall oder bei Vorfällen spezifische Maßnahmen ergreifen müssen
	Sie sind dokumentiert und werden aktuell gehalten
Formalisierung der Verantwortlichkeiten für den Schutz personenbezogener Daten	Gegenüber den zur Verarbeitung befugten Personen
	Gegenüber den Systemadministratoren (intern und extern)
	Gegenüber den Auftragsverarbeitern
	Gegenüber den Gesellschaften bei Verarbeitungstätigkeiten als Auftragsverarbeiter
	Sie sind dokumentiert und werden aktuell gehalten
	Sie werden durch einen Datenschutzbeauftragten (DPO) unterstützt
Schulungsmaßnahmen zur Stärkung der Kompetenz des Personals in Bezug auf Informationssicherheit und Schutz personenbezogener Daten	Mindestens jährlich
	Für das gesamte Personal
	Bei der Einstellung und bei spezifischem Bedarf
Verzeichnis der für die Informationsverarbeitung genutzten Unternehmenswerte	Die eingesetzte Software und Hardwarekomponenten sind inventarisiert
	Die bezogenen und erbrachten Dienste sind inventarisiert
	Sie umfassen die verarbeiteten Daten
	Sie umfassen die Verantwortlichen für diese Werte
	Sie werden laufend oder in festen Abständen aktualisiert

Regelung der Beziehungen zu Dritten durch Vertragsklauseln	Standard-Sicherheitsklauseln, die an jeden Vertrag angepasst und unter Berücksichtigung der Anforderungen der eigenen Kunden entwickelt werden
	Klauseln, die die Weitergabe der Sicherheitsanforderungen entlang der gesamten Lieferkette verlangen
	Klauseln zur Geheimhaltung von Informationen
	Klauseln zu den einzuhaltenden Sicherheitsmaßnahmen
	Klauseln zum Business Continuity Management
Risikobewertung in Bezug auf Cybersecurity / betriebliche Informationssicherheit	Mindestens jährlich neu bewertet
	Unter Verwendung verbreiteter oder marktüblicher Methoden
	Durch einen formalen und dokumentierten Prozess, der die Festlegung eines akzeptablen Risikos vorsieht
	Durch Identifizierung und Dokumentation von Bedrohungen, Schwachstellen und Auswirkungen
Überwachung des Konformitätsniveaus des Managements von Cybersecurity / Informationssicherheit / IT-Sicherheit	Auf Grundlage eines formalisierten Programms
	Durch eine interne Auditfunktion oder einen unabhängigen externen Anbieter
	Durch Personal mit angemessener beruflicher Qualifikation
	Mindestens jährlich
Protokolle für die sichere Softwareentwicklung, umgesetzt durch angemessen geschulte Entwickler	Kontinuierlich in der gesamten Entwicklungs- und Testkette angewendet
	Formale Sicherheitstests vor wesentlichen Produktivsetzungen
	Nutzung einer von der Produktion getrennten Umgebung
Zuweisung eines Budgets für Cybersecurity / Informationssicherheit / IT-Sicherheit / Datensicherheit	Jährlich festgelegt und zugewiesen
Sorgfältige Auswahl unter Berücksichtigung der Auswirkungen der eingesetzten Cloud-Computing-Dienste	Alle Daten befinden sich innerhalb der EU
	Alle sind nach ISO/IEC 27001, 27017, 27018 oder gleichwertig zertifiziert
	Bei allen sind die Sicherheitsverantwortlichkeiten mit dem jeweiligen Anbieter formal aufgeteilt

Bewertung des Fachpersonals nach vordefinierten Kriterien	Einholung von Informationen zur Ausbildung
	Einholung von Informationen zu früheren Beschäftigungen
	Überprüfung der eingeholten Informationen unter Beachtung der gesetzlichen Vorgaben
Vorhandensein und Konfiguration von Firewalls zum Internet, zum Schutz der Unternehmensserver und zu jeder Verbindung mit Dritten	Ja, und es sind DMZs konfiguriert, in denen die von außen erreichbaren Systeme betrieben werden
	Ja, und es werden VLANs mit konfigurierten ACLs eingerichtet, die das Netzwerk nach den erforderlichen Funktionen segmentieren
Nutzung von WLAN-Netzen	Geschützt durch Verschlüsselung mit WPA oder höher; die kryptografischen Schlüssel werden regelmäßig ersetzt
Durchführung von Backups der Unternehmensinformationen	Nach festgelegten Verfahren
	Verschlüsselt
	Regelmäßigen Wiederherstellungstests unterzogen (mindestens alle zwei Jahre)
	Wiederherstellungstests in der Produktionsumgebung unterzogen
	Mindestens wöchentlich
	Mit der Möglichkeit, Daten bis (höchstens) 24 Stunden vor der Kompromittierung des Systems wiederherzustellen.
Geregelte Verwaltung der logischen Zugriffe aus dem internen Netzwerk auf die Systeme und die wichtigsten Unternehmensanwendungen	Über persönliche Benutzerkonten und niemals über Gruppen- oder gemeinsam genutzte Konten
	Über eine Multi-Faktor-Authentifizierung (Passwort und Token oder biometrisch)
	Mittels Passwörtern mit mindestens 8 Zeichen
	Mittels Passwörtern, die spätestens alle 90 Tage ablaufen
	Unter Anwendung strengerer Zugriffskriterien als für normale Benutzer
Geregelte Verwaltung der logischen Fernzugriffe auf die Unternehmenssysteme	Über ein VPN oder ein gleichwertiges Tool, das die Vertraulichkeit des Netzwerkverkehrs schützt
	Mittels einer Authentifizierung mit mehreren Faktoren (Passwort und Token oder Zertifikat oder biometrisch)

	Mittels einer Authentifizierung, die ein individuelles Benutzerkonto erfordert
	Nur bei ausdrücklicher Genehmigung und regelmäßiger Bestätigung
Geregelte Benutzerverwaltung auf Betriebssystemebene und, sofern zutreffend, auf Ebene der Anwendungssoftware	Zentral
	Mit Berechtigungen, die auf das für die Tätigkeit unbedingt Notwendige beschränkt sind; Administratoren sind auf einen kleinen Personenkreis begrenzt
	Zeitnahe Anpassung bei Neueinstellungen, Rollenwechseln und Austritten
	Systematische Überprüfung der Berechtigungen mindestens halbjährlich
Kontrolle der von den Herstellern veröffentlichten Sicherheitspatches	Laufend kontrolliert, mit Prüfung der Anwendbarkeit
	Sofern anwendbar, werden sie vor der Freigabe umfassend auf Testsystemen getestet
	Sie werden nach ihrer Kritikalität klassifiziert und entsprechend ausgerollt
Vulnerability Assessment	Auf allen internen Informationssystemen mindestens halbjährlich
	Mit Klassifizierung der festgestellten Schwachstellen nach Kritikalität und entsprechender Behebung
	Unter Einsatz qualifizierter Tools und qualifizierten Personals
	Auf Infrastrukturebene
	Auf Anwendungsebene
Penetrationstest	Auf allen exponierten Informationssystemen mindestens jährlich
	Mit Klassifizierung der festgestellten Schwachstellen nach Kritikalität und entsprechender Behebung
	Auf Infrastrukturebene
	Auf Anwendungsebene
Protokollierung (Logs) auf den Systemen	Ja, mit Kontrollen ihrer Integrität
	Mit regelmäßiger Überprüfung
	Mit einem oder mehreren zentralen Systemen

	Unter Verwendung einer mit einer zuverlässigen externen Quelle synchronisierten Zeitreferenz
Schutzmaßnahmen für auf den Systemen gespeicherte Daten (Data at Rest)	Durch starke Festplattenverschlüsselung auf allen Systemen
	Durch Implementierung von Application Firewalls, die Datenbankanfragen filtern
	Durch Implementierung granularer Zugriffskontrollstrategien
Schutzmaßnahmen für über das Internet mit den Systemen ausgetauschte Daten (Data in Transit) und für den administrativen Zugriff (einschließlich Zugangsdaten, Session-Tokens und sonstiger vergleichbarer Elemente)	Durch ausschließliche Verwendung sicherer Kommunikationsprotokolle mit starker Datenverschlüsselung
	Durch Maßnahmen zur Authentifizierung von Absender oder Empfänger
Schutz der Unternehmensendgeräte (Laptops, Smartphones, Tablets)	Durch BIOS-Passwort oder Gleichwertiges
	Durch Festplattenverschlüsselung oder Gleichwertiges
	Durch Benutzername und Passwort des Betriebssystems
	Durch Sicherheitsrichtlinien, die über eine MDM-Plattform (Mobile Device Management) festgelegt werden
Konfiguration und Aktivierung grundlegender Schutzsysteme	Anti-Malware mit automatischer oder mindestens täglicher Aktualisierung der Signaturen
	EDR (Endpoint Detection and Response)
	Antispam
	Proxy-Firewall mit Anti-Malware-Funktionen
	IDS (Intrusion Detection System) oder IPS (Intrusion Prevention System)
	DRM (Digital Rights Management)
	Anti-APT (Advanced Persistent Threat)
	SIEM (Security Incident and Event Management)
	File integrity monitoring
	DNS-Einträge DMARC, DKIM und SPF
Regelung der Nutzung privater Geräte (einschließlich Tablets und Smartphones)	Nur zum Surfen im Internet und über getrennte Gastnetzwerke

	Mit der Verpflichtung, Unternehmensdaten ausschließlich verschlüsselt zu speichern und zu übertragen
Regelung des Managements von Vorfällen in Bezug auf Informationssicherheit / Cybersecurity / personenbezogene Daten	Erfassung, Analyse, Klassifizierung, Maßnahmen und Behebung
	Regelung einer etwaigen Weitergabe an Dritte gemäß den Vorgaben
	Unterstützung durch rund um die Uhr (24/7) verfügbares Fachpersonal oder ein externes SOC
	Detaillierter Incident-Response-Plan, der regelmäßig aktualisiert wird
	Ursachenanalyse jedes Vorfalls, die auch zur Aktualisierung des Reaktionsplans genutzt wird
	Regelmäßige Tests der Reaktion auf Vorfälle
	Forensische Analysen bei Bedarf
Regelung der Meldung und Mitteilung von Vorfällen und Datenschutzverletzungen	Einbeziehung verschiedener Funktionen in die Analyse
	Austausch der Bewertungen
Sichere Datenlöschung	Durch logisches Überschreiben oder physische Vernichtung aller Datenträger, die das Unternehmen verlassen oder neu zugewiesen werden, sodass die Daten nicht wiederherstellbar sind
	Indem von den Systemwartungsdienstleistern die sichere Löschung der von ihnen ersetzten oder ausgemusterten Datenträger verlangt wird
Richtlinie zur Datenaufbewahrung (Data Retention)	Löschung – auch automatisch – nach Ablauf der vorgesehenen Aufbewahrungsfristen
	Regelmäßige Überprüfung der Aufbewahrungsfristen
Regelung von Änderungen an Informationssystemen und Software	So erfasst, dass sie Angaben zum Antragsteller, zu den erwarteten Auswirkungen und zur Art der Änderung enthalten
	Vor ihrer Durchführung von einer anderen Person als dem Antragsteller genehmigt
	Vor der Freigabe in die Produktion getestet
Regelung der Konfiguration der Betriebssysteme und der wichtigsten auf den Informationssystemen installierten Software	Durch Änderung der Standardkonfigurationen gemäß festgelegten Hardening-Verfahren
	Basierend auf branchenüblichen Best Practices für das Hardening von Informationssystemen

	Zentral über Konfigurationsmanagementsysteme oder -mechanismen gesteuert
	Mindestens jährlich aktualisiert
	Im Einklang mit dem Prinzip der minimal notwendigen Funktionalität
	Regelmäßig auf unbefugte Änderungen überprüft
Einsatz von Überwachungssystemen	Zur Erkennung und Erfassung der Nichtverfügbarkeit eines Systems
	Zur Überprüfung des Netzwerkverkehrs
	Zur Überprüfung der Ressourcennutzung
	Zur Überprüfung der Funktionsfähigkeit der Sicherheitssysteme
	Zum Versand von Echtzeitalarmen bei Anomalien oder Störungen
Formalisierung der relevanten Anwendungsarchitektur	Dokument mit einer Gesamtbeschreibung der Anwendungsarchitektur
	Dokument mit einer Beschreibung der Anwendungsschichten (z. B. Datenbankserver, Applikationsserver, Webserver, …)
	Dokument, das die Kommunikationsschnittstellen der Anwendung auflistet und beschreibt (Protokolle, verwendete Ports usw.)
Kontrollen des Zutritts zum Perimeter der Organisation	Videoüberwachungsmaßnahmen
	Einbruchmeldeanlagen außerhalb der Bürozeiten
	Erfolgt über einen Empfang an jedem Zugangspunkt
Regelung des Zutritts zu den Serverräumen	Externes Personal hat nur in Begleitung Zutritt
	Erfolgt über physische Schlüssel, die internem Personal zugewiesen sind
	Wird detailliert protokolliert; die erfassten Informationen werden mindestens 3 Monate aufbewahrt
	Einbruchmeldesysteme
Überwachung von Temperatur und Luftfeuchtigkeit in den Serverräumen	Die Temperatur wird überwacht; bei Überschreitung festgelegter Schwellenwerte werden Alarme ausgelöst
	Die Luftfeuchtigkeit wird überwacht; bei Überschreitung festgelegter Schwellenwerte werden Alarme ausgelöst

	Es sind redundante Klimaanlagen vorhanden
Redundante Stromversorgungssysteme in den Serverräumen	Über USV
	Ja, mit regelmäßigen Funktionstests der USV und/oder Notstromaggregate
Brandschutzsysteme in den Serverräumen	Rauchmelder, die an eine Alarmanlage angeschlossen sind
	Handfeuerlöscher
Schutz der wichtigsten Papierarchive	Außerhalb der Arbeitszeiten verschlossen gehalten

Die vorliegende deutsche Übersetzung wurde mithilfe eines KI-gestützten Übersetzungstools erstellt und dient ausschließlich Informationszwecken. Rechtlich verbindlich ist ausschließlich die italienische Fassung des Dokuments.