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

ACS Spa, mit Rechtssitz in der Negrellistraße 6 – 39100 Bozen (BZ), MwSt.-Nr. 03320800216, Telefon 0471063063, E-Mail info@acs.spa, PEC info@pec.acs.it (nachfolgend auch „**Auftragsverarbeiter**").

Vorausgeschickt, dass:

- zwischen dem Verantwortlichen und ACS Spa ein oder mehrere Vertragsverhältnisse bestehen, die eine oder mehrere von ACS Spa erbrachte IT-Dienstleistungen zum Gegenstand haben (nachfolgend auch „Hauptvertrag");
- ACS Spa bei der Erbringung dieser Dienstleistungen personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten kann;
- das Personal von ACS Spa im Zusammenhang mit den übertragenen Tätigkeiten Funktionen ausüben könnte, die der Rolle des 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, die einen – auch zufälligen – Zugriff auf personenbezogene Daten ermöglichen;

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 der Grundlage der vom Verantwortlichen erteilten dokumentierten Weisungen, dieses Vertrags sowie etwaiger späterer Weisungen oder Vereinbarungen verarbeiten darf;
- die Übertragung der Funktionen des Systemadministrators nach vorheriger Bewertung der Erfahrung, Fähigkeiten und Zuverlässigkeit der benannten Person erfolgen muss;

Dies vorausgeschickt, vereinbaren und beschließen die Parteien, die sich zur Einhaltung der geltenden Datenschutzvorschriften und insbesondere der Verordnung (EU) 2016/679 („DSGVO") sowie des ital. Gesetzesvertretenden Dekrets Nr. 196/2003 verpflichten, Folgendes:

1. Bestellung des Auftragsverarbeiters

Der Kunde bestellt als Verantwortlicher für die Verarbeitung der im Rahmen seiner Tätigkeit verwalteten personenbezogenen Daten ACS Spa gemäß Art. 28 DSGVO zum Auftragsverarbeiter und ermächtigt diesen, alle – und ausschließlich – die Datenverarbeitungen vorzunehmen, die zur Erbringung der Dienstleistungen gemäß „Hauptvertrag" erforderlich sind.

Der Auftragsverarbeiter bestätigt, über Fachwissen, Zuverlässigkeit sowie wirtschaftliche, organisatorische und betriebliche Ressourcen – auch im Hinblick auf das mit den Verarbeitungstätigkeiten betraute 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 ACS Spa die Rolle des Systemadministrators („SysAdmin") einnehmen. ACS Spa 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;
- die namentliche Liste der natürlichen Personen, die mit Funktionen eines Systemadministrators betraut sind, unter Angabe mindestens von Vor- und Nachname, Rolle/Funktion, Tätigkeitsbereich, betroffenen Systemen oder Diensten und Berechtigungszeitraum stets aktuell zu halten und sie dem Verantwortlichen auf Anfrage mit angemessener Vorankündigung von mindestens 15 (fünfzehn) Arbeitstagen zur Verfügung zu stellen. Die Liste ist bei neuen Benennungen, Beendigungen oder Änderungen der Tätigkeitsbereiche unverzüglich zu aktualisieren;
- regelmäßige Kontrollen der Tätigkeit der benannten Systemadministratoren sowie der von ihnen vorgenommenen logischen Zugriffe auf Datenverarbeitungssysteme und elektronische Archive gemäß den Bestimmungen der Maßnahme der Datenschutzbehörde durchzuführen;
- die Protokollierung administrativer Zugriffe, soweit technisch anwendbar, sicherzustellen und die Protokolle (Logs) nach 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 einen Zeitraum von mindestens sechs Monaten aufbewahrt, sofern vom Verantwortlichen keine andere Frist angegeben oder von den geltenden Vorschriften vorgesehen ist.

In Bezug auf diese Bestellung legt der Verantwortliche als Tätigkeitsbereiche der Systemadministratoren jene fest, die im Dokument „Tätigkeitsbereiche der Systemadministratoren“ in der jeweils gültigen Fassung beschrieben sind, beschränkt auf die tatsächlich an ACS Spa übertragenen Dienstleistungen.

Die aktualisierten Einzelheiten sind im Dokument „Tätigkeitsbereiche SysAdmin“ enthalten, das auf Anfrage übermittelt wird.

Bei der Ausübung der genannten Funktionen könnte ACS Spa Zugang zu personenbezogenen Daten des Verantwortlichen erhalten und ist berechtigt, diese ausschließlich in dem Umfang zu verarbeiten, der zur Erfüllung der übertragenen Aufgaben und Tätigkeiten erforderlich ist. Weitere Verarbeitungsvorgänge außerhalb der mit diesem Vertrag oder mit weiteren förmlichen Weisungen des Verantwortlichen vereinbarten 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 unwirksam werden oder die Dienstleistung des Hauptvertrags nicht mehr erbracht werden, endet auch dieser Vertrag automatisch, unbeschadet jener Pflichten, die ihrer Natur nach fortbestehen.

4. Allgemeine Pflichten des Auftragsverarbeiters

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

1. die Daten nur für die oben genannten Zwecke und zur Erbringung der angegebenen vertraglichen Leistungen oder gemäß weiteren schriftlichen Weisungen des Verantwortlichen 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 dieses 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 Weisungen zur Art und Weise der Verarbeitung zu erteilen und sie auch über die Beendigung des Verhältnisses hinaus zur Vertraulichkeit zu verpflichten;
6. die Identifikationsdaten der natürlichen Personen, die gegebenenfalls als Systemadministratoren eingesetzt sind, unmittelbar und gesondert aufzubewahren und sie dem Verantwortlichen auf Anfrage mit angemessener Vorankündigung von mindestens 15 (fünfzehn) Arbeitstagen unverzüglich 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 länger auf eigenen Datenträgern zu speichern, als dies für die Erbringung der Dienstleistung erforderlich oder gesetzlich vorgeschrieben ist, und dabei in jedem Fall angemessene Sicherheitsmaßnahmen zu ergreifen.

5. Weitere Auftragsverarbeiter („Unterauftragsverarbeiter")

Der Verantwortliche ermächtigt den Auftragsverarbeiter bereits jetzt allgemein und im Voraus, einen oder mehrere Unterauftragsverarbeiter zur Durchführung der Tätigkeiten dieses Vertrags heranzuziehen. Der Auftragsverarbeiter gewährleistet, dass jeder Unterauftragsverarbeiter hinreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen im Sinne der geltenden Datenschutzvorschriften bietet, und verpflichtet sich, diesen durch Vertrag oder ein anderes Rechtsinstrument zur Einhaltung von Datenschutzpflichten zu verpflichten, die im Wesentlichen denen dieses Vertrags entsprechen. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen für die Erfüllung der Pflichten der Unterauftragsverarbeiter im Rahmen der geltenden Vorschriften. 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 zu ergreifen und in jedem Fall 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 wurden;
- eine nicht zulässige oder nicht den Zwecken der Verarbeitungsvorgänge entsprechende Datenverarbeitung.

Der Auftragsverarbeiter erklärt ferner, sich bewusst zu sein, dass sich die 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 etwaige erforderliche Anpassungen bewerten kann.

Der Auftragsverarbeiter darf die im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten nicht für Zwecke des Trainings, der Entwicklung oder Verbesserung von Systemen künstlicher Intelligenz, für Analytics, Profiling, Benchmarking, Datenanreicherung oder eigene Zwecke verwenden, es sei denn, es liegt 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 den Verantwortlichen innerhalb von 5 Tagen nach Eingang unverzüglich schriftlich, vorzugsweise per PEC, unter Beifügung einer Kopie des Antrags zu informieren und ihn mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen, um die Beantwortung zu ermöglichen.

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 dem Verantwortlichen sowie gegebenenfalls den zuständigen Behörden die umfassendste Unterstützung zu leisten, um die Pflichten nach 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 erforderlichenfalls der Aufsichtsbehörde melden und/oder den betroffenen Personen mitteilen kann.

Die Meldung muss mindestens:

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

Können die Informationen nicht zur gleichen Zeit bereitgestellt werden, so 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 einer Datenschutz-Folgenabschätzung (DSFA) und der vorherigen Konsultation der Aufsichtsbehörde. Sollten die vom Verantwortlichen angeforderten Unterstützungsleistungen, die über die nach den geltenden Vorschriften oder 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 geltenden ACS-Preislisten ermittelte Entgelt. Der Auftragsverarbeiter legt den geschätzten Aufwand vorab dar und erstellt nach Abschluss der Tätigkeiten einen geeigneten Leistungsnachweis. Die Tätigkeiten werden nach Annahme des entsprechenden Kostenvoranschlags durch den Verantwortlichen durchgeführt.

11. Datenschutzbeauftragter

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

12. Verzeichnis der 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 vorgesehenen 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 in Form von Dokumentenanforderungen, Fragebögen, Zertifizierungen, unabhängigen Auditberichten oder Fernprüfungen durchgeführt werden. Etwaige Inspektionen an den Standorten des Auftragsverarbeiters erfolgen mit angemessener Vorankündigung von mindestens 15 (fünfzehn) 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 jede sonstige im Zusammenhang mit der Verarbeitung personenbezogener Daten relevante Information unverzüglich mitzuteilen. Werden Audit-, Prüf- oder Kontrolltätigkeiten an einen Dritten übertragen und wird zwischen diesem und dem Auftragsverarbeiter ein Wettbewerbsverhältnis oder ein Interessenkonflikt festgestellt, kann der Auftragsverarbeiter die Durchführung dieser 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 in der DSGVO vorgesehenen Pflichten durch den Auftragsverarbeiter.

Dieser Vertrag gilt ausschließlich für Verarbeitungen, die der Auftragsverarbeiter im Auftrag des Verantwortlichen und auf der Grundlage von dessen dokumentierten Weisungen durchführt. Verarbeitet der Auftragsverarbeiter im Rahmen des Vertragsverhältnisses personenbezogene Daten für eigene Zwecke oder in Erfüllung eigener gesetzlicher Pflichten, ist diese Verarbeitung gesondert einzustufen und unterliegt nicht diesem Vertrag, sofern zwischen den Parteien nichts anderes schriftlich vereinbart ist.

15. Rückgabe oder Löschung der Daten nach Abschluss 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 anderslautender 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 geltenden ACS-Preislisten gesondert angeboten werden. Der Auftragsverarbeiter darf die personenbezogenen Daten nach Beendigung der Dienstleistung in dem Umfang und für die Dauer aufbewahren, die nach den geltenden Vorschriften erforderlich sind oder soweit dies zur Feststellung, Ausübung oder Verteidigung eigener Rechte notwendig ist. Auf Anfrage des Verantwortlichen stellt der Auftragsverarbeiter eine Erklärung über die erfolgte Löschung der personenbezogenen Daten aus, unbeschadet gesetzlicher Aufbewahrungspflichten.

16. Vergütungen, Entschädigungen oder Kostenerstattungen

Die Bestellung zum Auftragsverarbeiter begründet für sich allein keine Vergütungen, Entschädigungen oder Kostenerstattungen über die im Hauptvertrag vorgesehenen hinaus. Die Parteien vereinbaren, dass etwaige vom Verantwortlichen angeforderte Tätigkeiten, die nicht ausdrücklich in den Dienstleistungen des Hauptvertrags enthalten sind – darunter beispielsweise und nicht abschließend Unterstützungsleistungen im Zusammenhang mit der Ausübung der Rechte betroffener Personen, Audits, Prüfungen, Inspektionen, Anfragen der zuständigen Behörden, Folgenabschätzungen oder sonstige Tätigkeiten, die einen erheblichen Ressourceneinsatz des Auftragsverarbeiters erfordern –, auf Grundlage der zum Zeitpunkt der Anfrage geltenden Tarife des Auftragsverarbeiters oder nach anderweitiger Vereinbarung zwischen den Parteien gesondert vergütet werden können.

17. Widerruf und Ersetzung früherer Vereinbarungen

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

_____	ACS Spa
Verantwortlicher	Auftragsverarbeiter
_____	_____
Ort und Datum: _____	Ort und Datum: _____

**Die vorliegende deutsche Übersetzung wurde mithilfe eines KI-gestützten Übersetzungstools erstellt und dient ausschließlich Informationszwecken. Rechtlich verbindlich ist ausschließlich die italienische Fassung des Dokuments, die unter folgendem Link verfügbar ist:* DPA

Anlage 1 - VERZEICHNIS DER TECHNISCHEN UND ORGANISATORISCHEN SICHERHEITSMASSNAHMEN

VERZEICHNIS DER TECHNISCHEN UND ORGANISATORISCHEN SICHERHEITSMASSNAHMEN	**Referenz ISO/IEC 27001 (Controls Anhang A)**	
Übergeordnete Richtlinie (High-Level-Policy) zu Cybersecurity / Informationssicherheit / IT-Sicherheit.	5.2	Mit Zielen und Grundsätzen
		Von der obersten Leitung genehmigt
		Allen relevanten internen und externen Parteien zugänglich gemacht
		Mindestens jährlich aktualisiert
Mit der übergeordneten Richtlinie verbundene spezifische Richtlinien und Verfahren.	A.5.1	Zur Regelung des Incident-Managements
		Zur Regelung der physischen Zugangskontrolle
		Zur Regelung der logischen Zugangskontrolle
		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 der Systeme
		Zur Regelung der Informationsklassifizierung
		Zur Regelung des Log-Managements
		Zur Regelung des Datenlebenszyklus
		Zur Regelung des Lieferantenmanagements
Plan für das Business Continuity Management.	A.5.30	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
Notfallplan für die Kontinuität der IKT-Systeme.	A.5.30	Mit so bemessener Ressourcenzuweisung, dass die Verfügbarkeit stets gewährleistet ist
		Mit lokaler Redundanz aller kritischen Systeme durch hochverfügbare Lösungen
		Mit geografischer Redundanz aller kritischen Systeme an einem entfernten Standort, mehr als 50 km vom Primärstandort entfernt
Formalisierung der Verantwortlichkeiten für Cybersecurity / Informationssicherheit / IT-Sicherheit	A.5.2	Zugewiesen an einen Informationssicherheits- / Cybersecurity-Beauftragten oder CISO, der an den IT-Leiter oder höher berichtet
		Zugewiesen an diejenigen, die Informationssysteme verwalten, um deren Schutz zu gewährleisten
		Zugewiesen an das gesamte Personal, damit Informationen und Informationssysteme korrekt genutzt werden
		Zugewiesen an Dritte, die beim Schutz der Informationen eine Rolle spielen
		Zugewiesen an diejenigen, die im Notfall oder bei einem Vorfall bestimmte Maßnahmen ergreifen müssen
		Dokumentiert und aktuell gehalten
Formalisierung der Verantwortlichkeiten für den Schutz personenbezogener Daten	A.6.1.1.	Gegenüber den zur Verarbeitung befugten Personen
		Gegenüber den Systemadministratoren (intern und extern)
		Gegenüber den Auftragsverarbeitern
		Gegenüber den Gesellschaften bei Verarbeitungstätigkeiten als Auftragsverarbeiter
		Dokumentiert und aktuell gehalten
		Unterstützt durch einen Datenschutzbeauftragten (DPO)
Schulungsmaßnahmen zur Stärkung der Kompetenz des Personals in den Bereichen Informationssicherheit und Schutz personenbezogener Daten	7.3 A.6.3	Mindestens jährlich
		Für das gesamte Personal
		Bei der Einstellung und bei besonderem Bedarf

VERZEICHNIS DER TECHNISCHEN UND ORGANISATORISCHEN SICHERHEITSMASSNAHMEN	Referenz ISO/IEC 27001 (Controls Anhang A)	
Verzeichnis der für die Informationsverarbeitung genutzten Unternehmenswerte	A.5.9	Eingesetzte Software und Hardwarekomponenten sind inventarisiert
		In Anspruch genommene und erbrachte Dienste sind inventarisiert
		Einschließlich der verarbeiteten Daten
		Einschließlich der Verantwortlichen für diese Werte
		Laufend oder in festen Abständen aktualisiert
Regelung der Beziehungen zu Dritten durch Vertragsklauseln	A.5.20	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
		Geheimhaltungsklauseln
		Klauseln zu den einzuhaltenden Sicherheitsmaßnahmen
		Klauseln zum Business Continuity Management
Risikobewertung in Bezug auf Cybersecurity / Informationssicherheit des Unternehmens	6.1.2	Mindestens jährlich neu bewertet
		Unter Verwendung verbreiteter oder marktüblicher Methoden
		Durch einen formalen und dokumentierten Prozess, der die Festlegung eines akzeptablen Risikos vorsieht
		Unter Identifizierung und Dokumentation von Bedrohungen, Schwachstellen und Auswirkungen
Überwachung des Konformitätsniveaus des Managements von Cybersecurity / Informationssicherheit / IT-Sicherheit	9.2 A.5.35	Auf Grundlage eines formalisierten Programms
		Durch eine interne Auditfunktion oder einen unabhängigen externen Dienstleister
		Durch Personal mit angemessener beruflicher Qualifikation
		Mindestens jährlich
Protokolle für die sichere Softwareentwicklung, umgesetzt von angemessen geschulten Entwicklern	A.8.25	Kontinuierlich entlang der gesamten Entwicklungs- und Testkette angewendet
		Formale Sicherheitstests vor den wichtigsten Produktivsetzungen durchgeführt
		Nutzung einer von der Produktionsumgebung getrennten Umgebung
Zuweisung eines Budgets für Cybersecurity / Informationssicherheit / IT-Sicherheit / Datensicherheit	7.1	Jährlich festgelegt und zugewiesen
Sorgfältige Auswahl der Auswirkungen der eingesetzten Cloud-Computing-Dienste	A.5.23	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 Anbieter formal aufgeteilt
Bewertung des Fachpersonals nach vordefinierten Kriterien	A.6.1	Informationen zur erhaltenen Ausbildung werden angefordert
		Informationen zu früheren Beschäftigungen werden angefordert
		Die angeforderten Informationen werden unter Beachtung der gesetzlichen Vorgaben überprüft
Zertifizierte Verfahren	-	ISO/IEC 27001:2022, ISO/IEC 20000-1, ISO 9001:2015
Vorhandensein und Konfiguration von Firewalls zum Internet, zum Schutz der Unternehmensserver und zu jeder Verbindung mit Dritten	A.8.20	Ja, und es sind DMZs konfiguriert, in denen die von außen erreichbaren Systeme untergebracht sind
		Ja, und es werden VLANs mit konfigurierten ACLs eingerichtet, die das Netzwerk nach den erforderlichen Funktionen segmentieren
Nutzung von WLAN-Netzen	A.8.22	Geschützt durch Verschlüsselungsmechanismen WPA oder höher; die kryptografischen Schlüssel werden regelmäßig ausgetauscht
Durchführung von Backups der Unternehmensinformationen	A.8.13	Nach festgelegten Verfahren
		Verschlüsselt
		Regelmäßigen Wiederherstellungstests unterzogen (höchstens alle zwei Jahre)

VERZEICHNIS DER TECHNISCHEN UND ORGANISATORISCHEN SICHERHEITSMASSNAHMEN	Referenz ISO/IEC 27001 (Controls Anhang A)	
		Wiederherstellungstests in der Produktionsumgebung unterzogen
		Mindestens wöchentlich
		Mit der Möglichkeit, Daten bis (höchstens) 24 Stunden vor der Kompromittierung des Systems wiederherzustellen.
Geregeltes Management der logischen Zugriffe aus dem internen Netzwerk auf die Systeme und die wichtigsten Unternehmensanwendungen	A.5.16	Über persönliche Benutzerkonten und niemals über Gruppen- oder gemeinsam genutzte Konten
	A.5.17	Über eine Mehrfaktor-Authentifizierung (Passwort und Token oder biometrisch)
		Mittels Passwörtern mit mindestens 8 Zeichen
		Mittels Passwörtern mit einer Gültigkeit von höchstens 90 Tagen
		Unter Anwendung strengerer Zugangskriterien als für die Benutzer
Geregeltes Management der Fernzugriffe auf die Unternehmenssysteme	A.6.7	Über ein VPN oder ein gleichwertiges Instrument, 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
Geregeltes Benutzermanagement auf Betriebssystemebene und, soweit anwendbar, auf Ebene der Anwendungssoftware	A.5.18	Zentral
		Mit Berechtigungen, die auf das für die Tätigkeit unbedingt Notwendige beschränkt sind; Administratoren sind auf einen kleinen Personenkreis beschränkt
		Zeitnahe Anpassung bei Neueinstellungen, Rollenwechseln und Kündigungen
		Systematische Überprüfung der Berechtigungen mindestens halbjährlich
Kontrolle der von den Herstellern veröffentlichten Sicherheitspatches	A.8.8	Laufend kontrolliert und auf Anwendbarkeit geprüft
		Soweit anwendbar, vor der Freigabe umfassend auf Testsystemen getestet
		Nach Kritikalität klassifiziert und entsprechend ausgerollt
Vulnerability Assessment	A.8.8 A.8.16	Auf allen internen Informationssystemen halbjährlich oder häufiger
		Unter Klassifizierung der festgestellten Schwachstellen nach Kritikalität und deren entsprechender Behebung
		Unter Einsatz qualifizierter Tools und qualifizierten Personals
		Auf Infrastrukturebene
		Auf Anwendungsebene
Penetrationstest	A.8.8.	Auf allen exponierten Informationssystemen jährlich oder häufiger
		Unter Klassifizierung der festgestellten Schwachstellen nach Kritikalität und deren entsprechender Behebung
		Auf Infrastrukturebene
		Auf Anwendungsebene
Protokollierung (Logging) auf den Systemen	A.8.15	Ja, mit Kontrollen ihrer Integrität
		Mit regelmäßiger Überprüfung
		Mit einem oder mehreren zentralen Systemen
		Unter Verwendung einer Zeitreferenz, die mit einer zuverlässigen externen Quelle synchronisiert ist
Maßnahmen zum Schutz der auf den Systemen gespeicherten Daten (data at rest)	A.8.24	Durch Anwendung starker Festplattenverschlüsselung auf allen Systemen
	A.8.21	Durch Implementierung von Application Firewalls, die Datenbankanfragen filtern
	A.8.3	Durch Implementierung granularer Zugriffskontrollstrategien

VERZEICHNIS DER TECHNISCHEN UND ORGANISATORISCHEN SICHERHEITSMASSNAHMEN	Referenz ISO/IEC 27001 (Controls Anhang A)	
Maßnahmen zum Schutz der über das Internet mit den Systemen ausgetauschten Daten (data in transit) und für den administrativen Zugriff (einschließlich Zugangsdaten, Session-Token und sonstiger vergleichbarer Elemente)	A.8.20 A.8.21	Durch ausschließliche Verwendung sicherer Kommunikationsprotokolle mit starker Datenverschlüsselung
		Durch Maßnahmen zur Authentifizierung von Quelle oder Empfänger
Schutz der Unternehmens-Endgeräte (Laptops, Smartphones, Tablets)	A.8.1	Durch BIOS-Passwort oder Gleichwertiges
		Durch Festplattenverschlüsselung oder Gleichwertiges
		Durch Benutzername und Passwort des Betriebssystems
		Durch über eine MDM-Plattform (Mobile Device Management) festgelegte Sicherheitsrichtlinien
Konfiguration und Aktivierung grundlegender Schutzsysteme	A.8.7	Anti-Malware mit automatischer oder mindestens täglicher Aktualisierung der Signaturen
		EDR (Endpoint Detection and Response)
		Antispam
		Proxy-Firewall mit Anti-Malware-Funktion
	A.8.16	IDS (Intrusion Detection System) oder IPS (Intrusion Prevention System)
	A.8.3	DRM (Digital Rights Management)
	A.8.7	Anti-APT (Advanced Persistent Threat)
	A.8.15	SIEM (Security Incident and Event Management)
	A.8.23	File Integrity Monitoring
	A.5.14	DNS-Einträge DMARC, DKIM und SPF
Regelung der Nutzung privater Endgeräte (einschließlich Tablets und Smartphones)	A.8.1	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	A.5.24 A.5.25 A.5.26 A.5.27	Erfassung, Analyse, Klassifizierung, Maßnahmen und Behebung
		Regelung einer etwaigen Weitergabe an Dritte gemäß den Vorgaben
		Unterstützung durch 24/7 verfügbares Fachpersonal oder ein externes SOC
		Detaillierter, regelmäßig aktualisierter Incident-Response-Plan
		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 Incidents und Data Breaches	A.5.26	Einbeziehung verschiedener Funktionen in die Analyse
		Gemeinsame Nutzung der Bewertungen
Sichere Datenlöschung	A.8.10	Durch logisches Überschreiben oder physische Vernichtung aller Datenträger, die das Unternehmen verlassen oder neu zugewiesen werden, sodass die Daten nicht wiederherstellbar sind
		Durch die Verpflichtung der Systemwartungsdienstleister, die sichere Löschung der von ihnen ersetzten oder ausgemusterten Datenträger sicherzustellen
Richtlinie zur Datenaufbewahrung (Data Retention Policy)	A.5.33	Auch automatische Löschung nach Ablauf der vorgesehenen Aufbewahrungsfristen
		Regelmäßige Überprüfung der Aufbewahrungsfristen
Regelung von Änderungen an Informationssystemen und Software	A.8.32	So erfasst, dass Informationen über den Antragsteller, die erwarteten Auswirkungen und die Art der Änderung enthalten sind
		Vor ihrer Durchführung von einer anderen Person als dem Antragsteller genehmigt
		Vor der Produktivsetzung getestet

VERZEICHNIS DER TECHNISCHEN UND ORGANISATORISCHEN SICHERHEITSMASSNAHMEN	Referenz ISO/IEC 27001 (Controls Anhang A)	
Regelung der Konfiguration der Betriebssysteme und der wichtigsten auf den Informationssystemen installierten Software	A.8.9	Durch Änderung der Standardkonfigurationen gemäß festgelegten Hardening-Verfahren
		Auf Grundlage von Branchen-Best-Practices für das Hardening von Informationssystemen
		Zentral über Konfigurationsmanagementsysteme oder -mechanismen gesteuert
		Mindestens jährlich aktualisiert
		Konform mit dem Prinzip der minimal notwendigen Funktionalität
		Regelmäßig auf unbefugte Änderungen überprüft
Einsatz von Monitoring-Systemen	A.8.6 A.8.16	Zur Erkennung und Erfassung der Nichtverfügbarkeit eines Systems
		Zur Überprüfung des Netzwerkverkehrs
		Zur Überprüfung der Ressourcennutzung
		Zur Überprüfung der Funktion der Sicherheitssysteme
		Zum Versand von Echtzeitalarmen bei Anomalien oder Störungen
Formalisierung der relevanten Anwendungsarchitektur	A.8.27	Dokument mit einer Gesamtbeschreibung der Anwendungsarchitektur
		Dokument mit einer Beschreibung der Anwendungsschichten (z. B. Datenbankserver, Anwendungsserver, Webserver, …)
		Dokument, das die Kommunikationsschnittstellen der Anwendung auflistet und beschreibt (Protokolle, verwendete Ports usw.)
Kontrollen des Zugangs zum Perimeter der Organisation	A.7.4	Videoüberwachungsmaßnahmen
		Einbruchmeldeanlagen außerhalb der Bürozeiten
	A.7.2	Erfolgt über einen Empfang an jedem Zugangspunkt
Regelung des Zugangs zu den Serverräumen	A.7.2	Externes Personal erhält nur in Begleitung Zutritt
		Erfolgt über physische Schlüssel, die dem internen Personal zugewiesen sind
		Wird detailliert protokolliert; die erfassten Informationen werden mindestens 3 Monate aufbewahrt
	A.7.4	Einbruchmeldesysteme
Temperatur- und Feuchtigkeitskontrolle in den Serverräumen	A.7.5	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	A.7.11	Über USV
		Ja, mit regelmäßigen Funktionstests der USV und/oder Notstromaggregate
Brandschutzsysteme in den Serverräumen	A.7.5	Mit einer Alarmanlage verbundene Rauchmelder
		Handfeuerlöscher
Schutz der wichtigsten Papierarchive	A.7.2	Außerhalb der Arbeitszeiten verschlossen gehalten