DATA PROCESSING AGREEMENT GEMÄSS ARTIKEL 28 DER VERORDNUNG (EU) 2016/679 (DS-GVO)

Zwischen:

_____, mit Sitz in _____ Hausnr. ____, PLZ _____ Stadt _____, USt-Nr._____, vertreten durch _____

(„Kunde", „Data Controller" oder **„Datenverantwortlicher"),**

und

ACS Data Systems AG mit Sitz in Via Luigi Negrelli 6, 39100 Bozen, USt-Nr. 00701430217, vertreten durch den jeweiligen gesetzlichen Vertreter,

(„ACS", „Data Processor" oder **„Auftragsverarbeiter"),**

hier nachstehend auch einzeln als „Partei" bzw. gemeinsam als „Parteien" bezeichnet.

Prämisse

1. Zwischen den Parteien besteht mindestens eine Geschäftsvereinbarung über einen oder mehrere IT-Dienste, die ACS für den Kunden erbringt.
2. Bei der Erbringung der vorgenannten Leistungen verarbeitet ACS personenbezogene Daten im Auftrag des Kunden, welcher die Rolle des Datenverantwortlichen innehat.
3. Gemäß den geltenden Rechtsvorschriften zur Verarbeitung und zum Schutz personenbezogener Daten, insbesondere der Verordnung (EU) 2016/679 vom 27. April 2016 (im Folgenden „DS-GVO" oder „Verordnung"), ergibt sich die Notwendigkeit, die Beziehungen zwischen dem Kunden als dem Datenverantwortlichen einerseits und ACS als Auftragsverarbeiter andererseits in Bezug auf die durchgeführte Datenverarbeitung, die im Rahmen der Erbringung vertragsgegenständlichen Dienstleistungen in Auftrag gegeben werden, zu regeln. Diesbezüglich ist der Datenverantwortliche der Auffassung, dass der Auftragsverarbeiter über ausreichend Erfahrung, Professionalität, Kompetenzen, technische Fähigkeiten und Zuverlässigkeit verfügen, um für das Risiko angemessenen Schutz bietende technisch-organisatorische Maßnahmen umzusetzen.
4. Mit diesem Vertrag wollen die Parteien die hier gegenständliche Beziehung regeln.

Dies vorausgeschickt treffen die Parteien folgende Vereinbarungen

1. Die Prämisse bildet einen wesentlichen Bestandteil des vorliegenden Vertrags.

2. Beauftragung zum Auftragsverarbeiter

2.1. Gemäß und kraft Artikel 28 der Verordnung, beauftragt hiermit der Datenverantwortliche (im Folgenden „der Data Controller") in seiner Eigenschaft als die Partei, die über die Zwecke und Vorgehensweisen der Verarbeitung personenbezogener Daten zu entscheiden hat, das Unternehmen ACS Data Systems S.p.A. als Auftragsverarbeiter (im Folgenden „Data Processor").

3. Dauer und Ort der Datenverarbeitung

3.1. Die Dauer der Datenverarbeitung entspricht der Laufzeit der Dienste, die Gegenstand des Vertrags oder der Geschäftsvereinbarungen zwischen den Parteien sind. Sollten eine oder

mehrere geschäftliche Verträge aus welchem Grund auch immer enden, endet automatisch auch der Auftrag zur Verarbeitung der Daten, die dem/den beendeten Vertrag/Verträgen zugrunde liegen. Vorbehalten bleiben spezifische gesetzliche Pflichten, die aufgrund ihres Wesens weiter bestehen bleiben.

3.2. Die Verarbeitung der personenbezogenen Daten durch den Data Processor im Auftrag des Data Controller erfolgt überwiegend auf elektronischem Weg und auf jeden Fall innerhalb eines Mitgliedsstaats der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) bzw. in einem Land außerhalb der EU oder des EWR, für dessen Datenschutzsystem ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Artikel 45 DS-GVO vorliegt. In jedem anderen Fall erfolgt die Übermittlung personenbezogener Daten an einen Staat, der nicht Mitglied der EU oder des EWR ist, nur auf dokumentierte Anweisung des Kunden und nur dann, wenn die spezifischen Bedingungen in Artikel 44 ff. DS-GVO erfüllt sind.

4. Art und Zwecke der Verarbeitung

4.1. Die Datenverarbeitung, mit der der Data Controller den Data Processor beauftragt hat, ist für die Erbringung der Dienstleistungen und die Ausübung der Tätigkeiten, die Gegenstand der zwischen den Parteien bestehenden geschäftlichen Verträge sind, erforderlich.

5. Kategorien der verarbeiteten personenbezogenen Daten

5.1. Zum Zwecke der Erbringung der in den zwischen den Parteien geschlossenen Handelsverträgen vorgesehenen Dienstleistungen verarbeitet der Data Processor vom Data Controller bereitgestellte, gespeicherte, übermittelte oder erstellte Daten und unter der ausschließlichen Verantwortung des letzteren. Die Verarbeitung kann verschiedene Kategorien von Daten umfassen, wie z. B. personenbezogene Daten und Identifizierungsdaten (z. B. Vorname, Nachname, Steuernummer, IP-Adressen, Geolokalisierungsdaten usw.), Kontaktdaten, Daten über Löhne und Gehälter, An- und Abwesenheit, multimediale Inhalte (z. B. Audiodateien, Fotos, Videos, Unternehmenspräsentationen usw.), Protokolldaten über den Zugang zu Systemen und Anwendungen sowie sonstige von dem Data Controller bereitgestellte Daten.

6. Kategorien der betroffenen Personen

6.1. Die personenbezogenen Daten, deren Verarbeitung der Data Controller dem Data Processor anvertraut, können verschiedenen Kategorien von betroffenen Personen angehören, wie z.B. Angestellten, Mitarbeitern, dem Vorstand und/oder ihm gleichgestellten Personen, Kunden, Lieferanten sowie allen anderen Personen, die nicht den vorgenannten Kategorien angehören. Zu diesem Zweck erklärt der Data Controller, dass er alle ihm als Datenverantwortlicher obliegenden Pflichten erfüllt hat, insbesondere die Pflichten im Zusammenhang mit der Bereitstellung der Datenschutzrichtlinien und, soweit erforderlich, mit der Einholung aller erforderlichen Zustimmungen und Genehmigungen der betroffenen Personen, damit der Data Processor die Tätigkeiten im Rahmen dieser Vereinbarung durchführen kann.

7. Pflichten des Data Controller und Erklärungen

7.1. Der Data Controller entscheidet allein über den Zweck und die Art der Verarbeitung von personenbezogenen Daten. Er verpflichtet sich daher, den Data Processor in der mit dieser Beauftragung festgelegten Art und Weise über alle Änderungen zu informieren, die bei den Verfahren zur Verarbeitung der o.g. Daten erforderlich werden. Es wird davon ausgegangen, dass im Falle einer wesentlichen Änderung der delegierten Verarbeitungen oder wenn die delegierte Verarbeitungen gegen die geltenden Rechtsvorschriften und/oder die Anordnungen der zuständigen Aufsichtsbehörden, einschließlich des EDPB, verstoßen, der Data Processor diese Vereinbarung durch schriftliche Mitteilung an den Data Controller fristlos kündigen kann.

7.2. Unbeschadet der Pflichten des Data Processor im Sinne dieses Auftrags, trägt der Data Controller die allgemeine Haftung für jede Verarbeitung personenbezogener Daten, die durch ihn selbst direkt oder durch Dritte in seinem Namen erfolgt ist. Daher ist er gehalten, geeignete und wirksame Maßnahmen zu treffen, und muss nachweisen können, dass die Verarbeitungstätigkeiten den Bestimmungen der DS-GVO entsprechen, und dass die Maßnahmen wirksam sind. Diese müssen dem Wesen, dem Rahmen der Anwendung, dem Kontext und den Zwecken der Verarbeitung entsprechen und auch dem Risiko für die Rechte und Freiheiten natürlicher Personen Rechnung tragen. Rein beispielhaft und nicht abschließend muss der Data Controller folgenden Pflichten nachkommen: ein Datenschutzsystem konzipieren und umsetzen, das der DS-GVO und den einschlägigen Rechtsvorschriften entspricht, wofür er unter anderem angemessene technische und organisatorische Maßnahmen ergreifen und diesbezüglich eine Angmessenheitsbeurteilung vornehmen muss; die personenbezogenen Daten rechtmäßig erfassen und den betroffenen Personen die Informationen gemäß Artikel 13 und 14 zukommen lassen; in den in Artikel 33 vorgesehenen Fällen und vorbehaltlich einer Beurteilung die Meldung an die Aufsichts¬behörde erstatten; den Schutz der Rechte der betroffenen Personen und die daraus resultierende Bearbeitung und Beantwortung der Anträge solcher Personen gewährleisten; gemäß Artikel 34 DS-GVO und vorbehaltlich einer gesonderten Beurteilung im Fall einer Verletzung des Datenschutzes (im folgenden auch „Data Breach“) die betroffenen Personen in Kenntnis setzen.

7.3. Der Data Controller erklärt, dass die dem Data Processor delegierten Tätigkeiten die Grundsätze der Rechtmäßigkeit, der fairen Verarbeitung, der Transparenz, der Datenverringerung, der Genauigkeit, der Einschränkung der Verarbeitung, der Integrität des Speicherplatzes und der Vertraulichkeit einhalten. Er erklärt des Weiteren, dass es sich bei den personenbezogenen Daten, die aufgrund der Vertragsdurchführung oder der mit dem Data Processor geschlossenen Serviceverträge verarbeitet werden, um maßgebliche Daten handelt, und dass diese nicht über die Zwecke, für die sie erfasst und anschließend verarbeitet wurden, hinausgehen. Er erklärt zudem, dass er die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der betroffenen Personen korrekt identifiziert hat.

7.4. Der Data Controller erklärt, dass die personenbezogenen Daten und/oder etwaige Sonderkategorien von personenbezogenen Daten, die Gegenstand der dem Data Processor anvertrauten Verarbeitungsprozesse sind, in Übereinstimmung mit sämtlichen Vorgaben der geltenden Rechtsvorschriften erfasst und übermittelt wurden, einschließlich der Pflichten des Datenverantwortlichen in Bezug auf die Information und gegebenenfalls die Einholung einer gültigen Einwilligung der betroffenen Personen.

7.5. Der Data Controller erklärt, dass ausschließlich er für die Verfahren und Mittel zur Übermittlung der personenbezogenen Daten verantwortlich bleibt, sofern diese Verfahren auf Anwendungsprozessen basieren, die nach seinen Regeln und/oder mittels seiner eigenen IT- oder Telekommunikationsinstrumente entwickelt wurden. Falls solche Daten also aus irgendeinem nicht dem Data Processor zuzuschreibenden Grund nicht übermittelt werden, kann er nicht für die Verarbeitung der oben genannten Daten haftbar gemacht werden.

7.6. Wo vorgesehen, ist der Data Controller gemäß Artikel 30 DS-GVO verpflichtet, das Verzeichnis der Verarbeitungstätigkeiten zu führen und fortzuschreiben.

7.7. Der Data Controller befolgt und erfüllt die in dieser Beauftragung festgelegten Anforderungen mit Bezugnahme insbesondere auf die Kontroll- und Überprüfungsaktivitäten gegenüber dem Data Processor sowie in Bezug auf jede an den Data Processor gesendete Anforderung von Informationen und Unterstützung. Dies erfolgt stets im Rahmen der Pflichten, die zulasten des Letztgenannten festgelegt wurden.

7.8. Alle weiteren durch die einschlägigen Vorschriften vorgeschriebenen gesetzlichen Pflichten bleiben unbeschadet

8. Pflichten des Data Processor

8.1. Der Data Processor verpflichtet sich, die Daten ausschließlich gemäß den dokumentierten Anweisungen des Data Controller zu verarbeiten. Dies gilt auch im Falle der Übermittlung

von personenbezogenen Daten an ein Drittland oder eine internationale Organisation, es sei denn, dies ist nach EU- oder nationalem Recht erforderlich.

8.2. Der Data Processor gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

8.3. Gemäß Artikel 32 DS-VO ergreift der Data Processor, bei der Verarbeitung der hier auftragsgegenständlichen personenbezogenen Daten alle geeigneten technischen und organisatorischen Maßnahmen gemäß Anhang 2, welche der Data Controller für vollständig ausreichend erklärt und deren Angemessenheit er ausdrücklich bestätigt, dies unter Berücksichtigung des Stands der Technik und der Umsetzungskosten sowie der Art, des Gegenstands, des Kontextes und der Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen mit der jeweiligen Eintrittswahrscheinlichkeit und Schwere.

8.4. Unter Berücksichtigung der Art der Verarbeitung unterstützt der Data Processor den Data Controller nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Bearbeitung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person nachzukommen. Es besteht Einigkeit darüber, dass der Data Processor den Data Controller nur im Einklang mit dokumentierten Anweisungen unterstützt, und dass der Data Controller als Anlaufstelle für die betroffenen Personen bleibt.

8.5. Der Data Processor unterstützt den Data Controller bei der Einhaltung der in Artikel 32 bis 36 DS-GVO festgelegten Pflichten unter Berücksichtigung der Art der Verarbeitung und der dem Data Processor bereitgestellten Informationen. Es besteht Einigkeit darüber, dass die Unterstützung u.a. auf die Rolle des Data Processor und auf die Laufzeit und den Umfang der Tätigkeiten dieser Beauftragung beschränkt ist. Ausgeschlossen sind beispielsweise Tätigkeiten der Rechts- und IT-Beratung sowie auch die typischen Leistungen anderer Berater wie z. B. des Datenschutzberaters oder des Datenschutzbeauftragten.

8.6. Nach Abschluss der Erbringung der hier auftragsgegenständlichen Verarbeitungsleistungen wird der Data Processor nach Wahl des Data Controller alle personenbezogenen Daten löschen oder zurückgeben und alle bestehenden Kopien löschen, es sei denn, auf Ebene des Gemeinschaftsrechts oder des Recht der Mitgliedstaaten besteht eine Pflicht zur Speicherung der personenbezogenen Daten.

8.7. Der Data Processor liefert dem Data Controller auf dessen präzise, schriftliche Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung aller in dieser Beauftragung festgelegten Pflichten.

8.8. Der Data Processor informiert den Data Controller unverzüglich, falls eine Anweisung seiner Meinung nach gegen die DS-GVO oder andere nationale oder EU-Bestimmungen zum Schutz personenbezogener Daten verstößt.

8.9. Im Fall eines „Data Breach" wird der Data Processor gemäß Artikel 33 DS-GVO den Data Controller unverzüglich nach Kenntnisnahme hierüber unterrichten

9. Spezifische Pflichten im Zusammenhang mit der Funktion des Systemadministrators

9.1. Gemäß der Verordnung vom 27.11.2008 und nachfolgenden Änderungen, die von der Datenschutzbehörde (im Folgenden die "Verordnung der Datenschutzbehörde") erlassen wurde und mit der Verordnung vereinbar ist, wenn ACS bei der Erbringung der im vorstehenden Punkt genannten Dienstleistungen personenbezogene Daten im Auftrag des Kunden mit den typischen Aufgaben und Zuständigkeiten des Systemadministrators verarbeitet, muss der Data Processor innerhalb seiner Organisation die Personen bestimmen, die aufgrund ihrer fachlichen und beruflichen Fähigkeiten, ihrer Erfahrung und Zuverlässigkeit die Tätigkeiten eines Systemadministrators ausüben können und diesbezüglich den gesetzlichen sowie den in diesem Auftrag festgelegten Pflichten unterliegen. Der Data Processor muss außerdem eine Liste der Systemadministratoren führen und fortschreiben.

9.2. Auf schriftliche Anfrage des Data Controller, muss der Data Processor diesem die Liste der Systemadministratoren mit den identifizierenden Eckdaten und den diesen zugewiesenen Aufgabenbereichen zur Verfügung stellen

9.3. Der Systemadministrator oder die Systemadministratoren setzen Verfahren ein, die geeignet, die logischen Zugriffe auf die IT-Systeme aufzuzeichnen (Authentifizierung oder Access Log). Diese Aufzeichnungen müssen vollständig und unveränderbar sein und geeignete Möglichkeiten einer Integritätsüberprüfung hinsichtlich der Erreichung des Zwecks, für den sie erforderlich sind, bieten. Die Aufzeichnungen müssen die Zeitangaben und eine zusammenfassende Beschreibung des Ereignisses enthalten, das sie ausgelöst hat, und sind für einen Zeitraum von mindestens 6 (sechs) Monaten aufzubewahren. Sofern der oder die Systemadministratoren direkt auf dem IT-System des Data Controller arbeiten müssen, hT dieser, sofern nicht schon vorhanden, ein System einzusetzen, das eine Aufzeichnung der logischen Zugriffe ermöglicht

9.4. Auf schriftliche Anfrage des Data Controller stellt der Data Processor einen Auszug der im vorherigen Absatz genannten Aufzeichnungen, die sich auf den Zugriff des oder der Systemadministratoren beziehen, zur Verfügung

9.5. Um der Notwendigkeit von Prüfungen aufseiten des Data Controller gerecht zu werden, liefert der Data Processor dem Data Controller auf schriftliche Anfrage einen spezifischen Bericht über die von den Systemadministratoren vorgenommenen Tätigkeiten. Die diesbezügliche Anfrage ist mit einem angemessenen Vorlauf von mindestens 15 (fünf¬zehn) Werktagen zu übermitteln und muss sich auf die Tätigkeiten beziehen, die im Verlauf des Kalenderjahres durchgeführt wurden. Es kann nur ein Bericht pro Kalenderjahr bereitgestellt werden. Der Data Processor behält sich das Recht vor, eine Vergütung nach Maßgabe der durchgeführten Tätigkeit, des Zeitaufwands und der eingesetzten Ressourcen zu verlangen. Hierbei wird bestehenden gesetzlichen Tarifen oder geltenden Marktpreisen Rechnung getragen

10. Dateschutzbeauftragter

10.1. Unter Berücksichtigung von Artikel 37 des GDPR hat der Datenverarbeiter intern den Datenschutzbeauftragten (in Englisch auch unter dem Namen „Data Protection Officer" – Kürzel „DPO", bekannt) benannt. Die Kontaktdaten des DPO sind unter folgendem Link abrufbar: privacy.acs.it.

11.Sub Processor

11.1. Hinsichtlich der Durchführung der hier auftragsgegenständlichen Verarbeitungsvorgänge erteilt der Data Controller schon jetzt die Genehmigung, dass der Data Processor Subunternehmer (im Folgenden „Sub Processor") einsetzen darf. Bei der Beauftragung von Sub Processor sichert der Data Processor durch einen Vertrag oder einen anderen Rechtsakt zu, dass diese denselben Pflichten und Bedingungen unterliegen, die in dieser Beauftragung enthalten sind, und dass sie ausreichende Gewährleistungen bieten, angemessene technische und organisatorische Maßnahmen umsetzen zu können. Der Data Controller kann vom Data Processor die Bereitstellung einer aktuellen Liste der beauftragten Sub Processor verlangen.

11.2. Wird ein zusätzlicher Sub Processor beauftragt oder ein bestehender ersetzt, teilt der Data Processor diese Änderungen dem Data Controller unverzüglich mit, sodass dieser die Möglichkeit hat, den Änderungen zu widersprechen. Sofern der Data Controller 5 (fünf) Tage nach Eingang der Mitteilung keinen Widerspruch zum Ausdruck gebracht hat, kann der Data Processor die Änderungen als angenommen betrachten.

12.Inspektionen und Kontrollen

12.1. Der Data Processor erteilt im Rahmen der im Auftrag des Data Controller durchgeführten Verarbeitung die Genehmigung zur Durchführung von Prüfungen – einschließlich Inspektionen – durch den Data Controller oder durch einen von diesem ordnungsgemäß ernannten Dritten.

12.2. Wird die Prüfung durch einen Dritten vorgenommen, kann der Data Processor, falls es sich dabei um einen Wettbewerber handelt, oder ein Interessenkonflikt besteht, die Durchführung der Prüfungstätigkeiten durch den beauftragten Dritten verweigern.

12.3. Bei Kontrollen oder sonstigen Prüfmaßnahmen jeglicher Art, und vor allem bei solchen, die in den Räumlichkeiten des Data Processor stattfinden, um die Betriebsabläufe beim Data Processor so wenig wie möglich zu stören und dafür zu sorgen, dass dieser seinen Geschäftstätigkeiten effizient und gewinnbringend nachgehen kann, verpflichtet sich der Data Controller, die Prüfung oder Überprüfung oder Inspektion mit einem Vorlauf von mindestens 15 (fünfzehn) Tage im Voraus schriftlich anzukündigen und vor Beginn der Tätigkeiten die Bedingungen für diese Überprüfung (Beginn und Dauer), die Art des Kontrollen und den Gegenstand des Überprüfung zu vereinbaren, wobei der Data Controller nicht mehr als 1 (ein) Audit pro Jahr durchführen darf, außer im Falle einer Datenschutzverletzung. In Anbetracht der Art, der Vorgehensweise und des Gegenstands dieser im vorangehenden Absatz genannten Tätigkeiten kann der Data Processor für deren Durchführung verlangen, dass der Data Controller eine Geheimhaltungsvereinbarung (ein sogenanntes „NDA") unterzeichnet.

12.4. Im Falle von Inspektionen, Kontrollen und Prüfungen behält sich der Data Processor das Recht vor, von dem Data Controller eine angemessene Vergütung für die vorgenommenen Tätigkeiten und die Anzahl der Sitzungen sowie die eingesetzten Ressourcen zu verlangen. Dies erfolgt unter Berücksichtigung der zum Zeitpunkt der Verarbeitung geltenden Stundensätze und unter der Vorgabe, keinen Anfragen nachzukommen, bei denen die Prüfungsaktivitäten die in dieser Beauftragung festgelegten Pflichten und Grenzen überschreiten. Für alle Prüfungen, Inspektionen oder Kontrollen, die außerhalb der normalen Arbeitszeit in den Räumlichkeiten des Data Processor durchgeführt werden, ist immer eine Vergütung erforderlich. In jedem Fall trägt der Data Controller alle Kosten für die Prüfungs- und Kontrolltätigkeiten.

13.Haftung

13.1. Gemäß Artikel 82 DS-GVO haftet der Data Controller für materielle oder immaterielle Schäden, die durch die dem Data Processor anvertraute Datenverarbeitung verursacht wurden, sofern der Schaden aus der Verletzung der ihm durch die Datenschutzgesetze und die in dieser Beauftragung auferlegten Pflichten resultiert.

13.2. Gemäß Artikel 82 DS-GVO haftet der Data Processor für materielle oder immaterielle Schäden infolge der ihm anvertrauten Verarbeitung nur dann, wenn er den spezifischen Pflichten als Data Processor aus den datenschutzrechtlichen Vorschriften und der vorliegenden Beauftragung nicht nachgekommen ist oder die rechtmäßig erteilten Anweisungen des Data Controller nicht befolgt oder entgegen diesen Anweisungen gehandelt hat.

13.3. Der Data Processor ist in jedem Fall von jeglicher Haftung für die ihm anvertraute Verarbeitung befreit, wenn er nachweist, dass er in keiner Weise für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist, bzw. dass sich dieser aus Anweisungen ableitet, die durch den Data Controller unrechtmäßig trotz Hinweis gemäß Punkt 8.8 erteilt wurden. Auch der Data Controller ist von jeglicher Haftung befreit, wenn er nachweist, dass er in keiner Weise für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

14.Schlussbestimmungen

14.1. Diese Beauftragung unterliegt ausschließlich dem Recht der Italienischen Republik und entspricht im Übrigen auch den europäischen Rechtsvorschriften über die Verarbeitung personenbezogener Daten. Als offizielle Version dieser Beauftragung gilt der auf Italienisch abgefasste Text. Bei Unstimmigkeiten und/oder Abweichungen zwischen der italienischen Version und den Fassungen in anderen Sprachen ist die italienische Version maßgeblich und verbindlich.

14.2. Sofern in dieser Beauftragung Begriffe oder Begriffsbestimmungen verwendet werden, denen gemäß der Verordnung und des Datenschutzgesetzes eine bestimmte Bedeutung zukommt, werden diese Begriffe mit dieser spezifischen Bedeutung verwendet.

14.3. Diese Beauftragung stellt eine Ergänzung zu den vertraglichen Vereinbarungen zwischen den Vertragsparteien dar. Sie ersetzt alle vorangehenden, auch mündlichen, Vereinbarungen und stellt somit die einzige rechtsgültige und wirksame Vereinbarung in Bezug auf die in ihr geregelten Angelegenheiten dar. Die Bestimmungen dieser Beauftragung gelten auch für alle künftigen Datenverarbeitungen, die der Data Processor im Auftrag des Data Controller zukünftig durchführt. Etwaige Ergänzungen, die gemäß Artikel 14.6 vorzunehmen sind, bleiben vorbehalten.

14.4. Bei Anfragen zu Tätigkeiten und Leistungen, die über die Bestimmungen dieser Ernennung hinausgehen, behält sich der Data Processor das Recht vor, dem Data Controller eine Gebühr auf der Grundlage der in den Handelsverträgen zwischen den Parteien vereinbarten Tarife oder alternativ auf der Grundlage der geltenden gesetzlichen oder marktüblichen Tarife zu berechnen oder die Anfrage nicht zu bearbeiten.

14.5. Eine etwaige Duldung von Vertragsverletzungen der Gegenpartei kann in keiner Weise als Verzicht auf die Rechte aus dieser Vereinbarung gewertet werden.

14.6. Sollte eine Bestimmung dieser Beauftragung ganz oder teilweise ungültig oder nicht anwendbar sein oder werden, bleiben die übrigen Bestimmungen in jedem Fall gültig und wirksam. Entsprechendes gilt im Fall einer vertraglichen Lücke. Die Vertragsparteien ersetzen die ungültige oder nicht anwendbare Bestimmung bzw. füllen die Lücke durch eine gültige und anwendbare Bestimmung, die dem Wesen und Zweck dieser Vereinbarung so nahe wie möglich kommt. Etwaige Änderungen oder Ergänzungen im Sinn des vorherigen Absatzes sind durch schriftliche Vereinbarung zwischen den Vertragsparteien als Ergänzung zu dieser Beauftragung zu treffen.

14.7. Die Vertragsparteien erklären, die vorliegende Beauftragung Klausel für Klausel ausgehandelt zu haben. Bei Streitigkeiten über die Gültigkeit, Auslegung, Ausführung und Beendigung dieser Vereinbarung oder der damit verbundenen Anlagen oder Dokumente verpflichten sich die Vertragsparteien, eine faire und gütliche Beilegung anzustreben. Kann keine gütliche Beilegung erreicht werden, ist ausschließlich die Justizbehörde Bozen zuständig.

14.8. Im Rahmen der Erfüllung der in dieser Beauftragung genannten Pflichten sind alle Mitteilungen und Anträge der Vertragsparteien ausschließlich an die im Anhang 1 angegebenen Adressen zu richten.

Ort und Datum

_____, __/__/____

Zur Bestätigung

Data Controller

Data Processor

_____

ACS Data Systems AG

_____

_____

ANHANG 1: SPEZIFISCHE ANWEISUNGEN DES DATA CONTROLLERS*

* Dieser Anhang muss von den Parteien vor jeglicher Art der Datenverarbeitung ausgefüllt und unterzeichnet werden.

PERSONEN	
Data Controller	
Name des gesetzlichen Vertreters (oder einer anderen Person, die befugt ist, im Namen des Data Controllers zu handeln)	_____
Data Processor	
Name des gesetzlichen Vertreters (oder einer anderen Person, die befugt ist, im Namen des Data Processors zu handeln)	Luis Plunger, CFO und gesetzlicher Vertreter
DPO und Kontaktangaben (falls vorhanden)*	
Für den Data Controller	
Name	_____
Email	_____
PEC	_____
Anschrift	_____
Für den Data Processor	
Name	Dr. Manuel Mattia
Email	privacy@acs.it
PEC	info@pec.acs.it
Anschrift	Luigi Negrelli Straße 6, 39100 - Bozen

* Geben Sie die entsprechenden Kontaktdaten an, sofern gesetzlich vorgeschrieben und sofern eine oder beide Parteien einen *Data Protection Officer* ernannt haben. Jede Änderung der Daten muss der anderen Partei unverzüglich mitgeteilt werden.

KATEGORIEN VON PERSONENBEZOGENEN DATEN
Allgemeine Daten
☐ persönliche Daten (z. B. Vorname, Nachname, Steuernummer, Telefonnummer, E-Mail usw.)
☐ Kontaktdaten (z. B. E-Mail, PEC, Telefonnummer, Wohnadressen usw.)
☐ Konten für IT-Hardware und -Dienste (z. B. Zugangsdaten für Arbeitsplätze, E-Mail, Portale usw.)
☐ IT Erkennungsmerkmale (z. B. IP-Adressen, Zugriffsprotokolle, Geolokalisierungsdaten usw.)
☐ multimediale Inhalte (z. B. Audio, Fotos, Video usw.)
☐ Arbeits- und/oder Berufsinformationen (z. B. Lebenslauf, Gehaltsabrechnungen, Ausbildungsnachweise, Referenzschreiben usw.)
☐ Sonstiges (bitte angeben) _____

KATEGORIEN VON INTERESSENTEN
☐ Der Verwaltungsrat und ihm gleichgestellte Personen
☐ Eigene Angestellte und Mitarbeiter
☐ Angestellte und Mitarbeiter von Geschäftspartnern (z. B. Händler, Lieferanten usw.)
☐ Kunden und potenzielle Kunden
☐ Sonstiges (bitte angeben) _____

KONTAKTE *	
Für den Data Controller	
Kontaktperson	_____
Email	_____
PEC	_____
Für den Data Processor	
Kontaktperson	Dr. Manuel Mattia
Email	privacy@acs.it
PEC	info@pec.acs.it

***Jede Änderung der Kontakte ist der anderen Partei unverzüglich mitzuteilen.

ANHANG 2: TECHNISCH-ORGANISATORISCHE MAßNAHMEN ZUR EINHALTUNG DES DATENSCHUTZES (ART. 32 DSGVO)

Überblick

Dieses Dokument enthält die technisch-organisatorischen Maßnahmen für die Sicherheit der ACS IT-Infrastrukturen, sowohl für die eigene IT als auch für die ACS.Cloud, in Bezug auf Artikel 32 der Datenschutzgrundverordnung (EU) 2016/679, die von ACS zum Schutz der personenbezogenen Daten ergriffen wurden.

Die hier enthaltenen Sicherheitsmaßnahmen beziehen sich sowohl auf die ACS-Standorte als auch auf das Datacenter in Bozen. Sie gelten als Veranschaulichung der von ACS ergriffenen Sicherheitsmaßnahmen in allen Datacenterstandorten und gelten auch als Standard für zukünftige Datacenterstandorte.

Alle Datacenterstandorte befinden sich in Italien.

Das Dokument enthält folgende Sektionen:

1. **Vertraulichkeit (Art. 32(1) (b) GDPR)**
    a. Zutrittskontrolle
    b. Zugriffskontrolle
    c. Datentrennung von Kunden
    d. Verschlüsselung
2. **Integrität (Art. 32 (1)(b) GDPR)**
    a. Sicherheit beim Datentransfer
    b. Sicherheit der Datenverarbeitung
    c. Sicherheit der IT-Systeme
3. **Verfügbarkeit und Belastbarkeit (Art. 32(1)(b) GDPR)**
    a. Verfügbarkeitskontrolle
4. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)**
    a. Auftragskontrolle
    b. Organisationssysteme

1. Vertraulichkeit (Art. 32(1) (b) GDPR)

a. Zutrittskontrolle

Maßnahmen zur physischen Sicherheit und zum Schutz vor nicht autorisiertem Zugang zu den Datenverarbeitungssystemen.

Schutzmaßnahmen am Gebäude (Datacenter)

a) Sicherheitszone Datacenter mit Personenschleuse
b) Verriegelbare Fenster
c) Alarmanlagen
d) Kontrollen durch den Sicherheitsdienst
e) Zugang nur für autorisierte Personen (mit persönlichem Badge)
f) Permanente Videoüberwachung der Eingangsbereiche
g) Alarmgesicherte Notausgänge
h) Mit Schlüssel verriegelbare Rackschränke

Schutzmaßnahmen am Gebäude (ACS Data Systems Büros)

a) Videoüberwachung der Eingangsbereiche in Bozen, Venedig
b) Alarmanlage in allen Niederlassungen
c) Regelung zur Aufsicht und Begleitung betriebsexterner Personen innerhalb der Bürogebäude

Organisatorische Sicherheitsmaßnahmen

a) Kontrollen durch einen Überwachungsdienst außerhalb der Öffnungszeiten
b) Zugangsregelung zu den Betriebssitzen
c) Regelung für den Austritt von Mitarbeitern aus dem Unternehmen

Regelungen für den physischen Zugang (Datacenter)

a) Regelung für den Zugang einzelner Mitarbeiter zum Datacenter
b) Regelung des Zugangs im Datacenter für Kunden/Interessierte und Mitarbeiter
c) Regelung und Steuerung von notwendigen Arbeiten im Datacenter
d) Möglichkeit zur Erteilung, Änderung oder Sperrung von Zugängen zum Datacenter

b. Zugriffskontrolle

Maßnahmen zum Schutz vor unbefugtem Zugriff auf Systeme und Anwendungen sowie Maßnahmen zum Schutz vor unbefugtem Lesen, Ändern oder Löschen von personenbezogenen Daten.

Kontrolle der Zugriffe

a) Regelung zur Verwaltung von Benutzerrechten
b) Regelung der Verwaltung von Benutzerrechten und der Systemverwaltung
c) Regelmäßige Kontrollen der Benutzerrechte
d) Autorisierte Personen identifizieren sich mit individuellem Benutzername und Passwort
e) Passwortmanagement von administrativen Accounts (root, Administrator)
f) Passwortrichtlinien: Komplexes Passwort mit 8 Zeichen, mindestens Groß-und Kleinbuchstaben, Zahlen und Sonderzeichen
g) Regelung für den Eintritt/Austritt von Mitarbeitern

h) Zeitlich befristete Sperrung von Benutzeraccounts bei wiederholter Falscheingabe von Passwörtern
i) Sperrung der Computer bei mehr als 10 Minuten Inaktivität

Netzwerksicherheit

a) Einsatz von Firewall und Antivirus
b) Einsatz von Intrusion Detection Systemen (IDS)
c) Regelung für die sichere Konfiguration von Client und Servern
d) Regelung für den Einsatz neuer Geräte
e) Einsatz von Network Access Control Systemen (802.1X) für den Zugang zum ACS Netzwerk

Maßnahmen zur Sicherheit von externen Zugriffen

a) Regelung für den externen Zugriff auf die Datenverarbeitungssysteme
b) Externer Zugriff ausschließlich mit 2 Faktor Authentifizierung für den Zugang zum ACS Netzwerk
c) Regelung für die externe Systemverwaltung der IT-Systeme
d) Regelung für die Vergabe von Benutzerrechten an externe Personen und Business Partner
e) Sperrung von unautorisierten Zugriffen auf das Netzwerk über das Internet

Zusätzliche Maßnahmen zur Sicherheit (Datacenter)

a) Einsatz von virtuellen Maschinen
b) Zuweisung von individuellen administrativen Benutzer-Accounts
c) Regelung für die Zuweisung von administrativen Rechten an die Administratoren
d) Individuelle Ernennung der Administratoren und Passwortadministatoren
e) Geschütztes Logging der Zugriffe von administrativen Accounts
f) Regelung des Transportes und der Kopien von Daten mit externen Datenträgern
g) Regelung für die Vernichtung von Festplatten

Logging der Zugriffe

a) Geschütztes Logging der Zugriffe administrativer Accounts
b) Log der nicht autorisierten Zugriffe auf das Netzwerk (Firewall)

Weitere Schutzmaßnahmen für Dokumente und Daten in Papierform

a) Einsatz von Aktenvernichtern
b) Mit Schlüssel gesperrte Archive und Verwaltung der Schlüssel
c) Mit Schlüssel gesperrte Aktenschränke
d) Automatisches Schließen der HR- und Verwaltungsbüros

c. Datentrennung von Kunden

Trennung der Daten, die für unterschiedliche Verarbeitungszwecke erfasst wurden.

a) Getrennte Serversysteme und Datenspeicher
b) Mandantenfähigkeit der eingesetzen Software
c) Regelung für die Einrichtung von neuen Kunden und neuen Benutzern der Kunden in der Cloud Umgebung.

d. Verschlüsselung

Verschlüsselung der Daten zur Verhinderung des nicht autorisierten Lesens von Informationen durch nicht befugte Personen oder Dritte.

a) Verschlüsselte Passworte
b) Verschlüsselung des Backup-to-Disk
c) Dateiverschlüsselung (individuell durch die (Datacenter-)Beauftragten)

2. Integrität (Art. 32 (1)(b) GDPR)

a. Sicherheit beim Datentransfer

Schutz der Verbindung vor unerlaubtem Lesen, Ändern oder Löschen von personenbezogenen Daten während der Verbindung oder des Transports von Daten.

a) Einsatz von geeigneten Protokollen für den Zugriff auf die IT-Systeme (Citrix, RDP, VPN, SSH, SSL/TLS)
b) Einsatz von PEC-Email
c) Feststellen von autorisierten Personen durch ein Autorisierungskonzept

b. Sicherheit der Datenverarbeitung

Technische und organisatorische Maßnahmen zur Bestimmung, wer Daten in Datenverarbeitungssysteme eingeben, ändern oder löschen darf.

a) Definition von Verantwortlichkeiten für die Eingabe von Daten (sowie Stellvertreter)
b) Logging der Eingabe, Änderung und Löschung von personenbezogenen Daten im ERP System
c) Konfiguration unterschiedlicher Benutzerberechtigungen (z.B. lesen, schreiben, ändern, löschen) im ERP-System

c. Sicherheit der IT-Systeme

a) Whitelisting von erlaubten Applikationen (ACS.Public Cloud)
b) Antivirus auf allen Systemen (Server und Client)
c) Antispam Lösung auf Anfrage des Kunden
d) Verschlüsselung der Festplatten von Notebooks von ACS Mitarbeitern

3. Verfügbarkeit und Belastbarkeit (Art. 32(1)(b) GDPR)

a. Verfügbarkeitskontrolle

Backups

a) Regelung des Backups von Daten
b) Definition der Datenaufbewahrungsrichtlinien
c) Aufbewahrung der Backupkassetten in geschützten Zonen
d) Regelmäßiges Backup von Dateien, virtuellen Servern und Datenbanken
e) Namenskonvention für Backupkassetten
f) Beschriftung von Backupkassetten
g) Inventar aller Backups und Backupkassetten

Backups (Datacenter)

a) Regelung des Backups von Daten in der ACS.Cloud
b) Definition der Datenschutzrichtlinien
c) Aufbewahrung der Backupkassetten in einem feuerfesten Tresor
d) Aufbewahrung der Backups an zwei unterschiedlichen Standorten
e) Regelmäßiges Backup von Dateien, virtuellen Servern und Datenbanken
f) Namenskonvention für Backupkassetten
g) Beschriftung von Backupkassetten
h) Inventar aller Backups und Backupkassetten

Maßnahmen zur Sicherstellung der Systemverfügbarkeit

a) Notstromversorgung durch UPS-Systeme
b) Redundante Klimaanlagen, mit abwechselndem Betrieb
c) Überwachung der Temperatur
d) Monitoring mit automatischem Meldesystem der IT-Systeme
e) Trennung der einzelnen Abteilungen und dem internen IT Team
f) Zentrale Beschaffung von Hardware und Software
g) Guidelines zur Prozessdokumentation
h) Regelmäßige Fort- und Weiterbildung der Mitarbeiter

Maßnahmen zur Sicherstellung der Systemverfügbarkeit (Datacenter)

a) Notstromversorgung durch UPS-Systeme
b) Notstromaggregat
c) Automatische Brandmeldeanlagen
d) Redundante Klimaanlagen
e) Überwachung der Temperatur
f) Monitoring der IT-Systeme mit automatischem Meldesystem
g) Notfallpläne (inkl. Verantwortlichkeiten, Wiederherstellungsrichtlinie, alternative Datacenterstandorte)
h) Redundante Auslegung kritischer Systeme (Firewall, Switch, Server)
i) Disaster Recovery Policy
j) Trennung der einzelnen Abteilungen und dem ACS.Cloud Team
k) Zentrale Beschaffung von Hardware und Software
l) Richtlinien zur Prozessdokumentation
m) Richtlinien für den Zugang zum Datacenter sowie für das Verhalten im Datacenter
n) Regelmäßige Fort- und Weiterbildung der Mitarbeiter

Organisatorische Maßnahmen

a) Monatliche Bewertung der Informationssicherheit (Penetration Test)
b) Regelung der Verantwortlichkeiten für die Aktualisierung der IT-Systeme

4. Verfahren zum regelmäßigen Testen, Prüfen und Bewerten der Maßnahmenwirksamkeit (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

a. Auftragskontrolle

Es werden keine personenbezogenen Daten von ACS verarbeitet ohne Anweisung, gemäß Artikel 28 Absatz 3 a) der DSGVO EU 2016/679, durch den Verantwortlichen für die Datenverarbeitung.

Vereinbarungen

a) Der Verantwortliche der Datenverarbeitung kommuniziert die Auftragserteilung über ein schriftliches oder digitales Dokument an den Auftragsverarbeiter.
b) Anweisungen des Verantwortlichen für die Datenverarbeitung erfolgen in schriftlicher Form; Mündlichen Anweisungen werden in Schriftform bestätigt.

Unterauftragnehmer

a) Maßnahmen zur Sicherstellung der Einhaltung geltender Datenschutzbestimmungen durch die Unterauftragnehmer können vom Verantwortlichen der Datenverarbeitung überprüft werden.

b. Organisationssysteme

a) Dezidierte Kontaktperson zur Beantwortung von Datenschutzfragen
b) Schriftliche Ernennung von Mitarbeitern als autorisiertes Personal zur Verarbeitung personenbezogener Daten
c) Jährliches Privacy-Audit durch externe Berater
d) Zertifizierung ISO 9001:2015
e) Leitlinien für befugtes Personal zur Gewährleistung der Sicherheit bei der Verarbeitung personenbezogener Daten
f) Regelung zum Umgang mit Datenschutzanfragen