

|  |  |
|--|--|
| <p style="text-align: center;"><b>AWS GDPR DATA PROCESSING ADDENDUM</b></p> <p>This Data Processing Addendum (“<b>DPA</b>”) supplements the Customer Agreement signed between AWS and the Customer, as updated from time to time, or other agreement between Customer and AWS governing Customer’s use of the Service Offerings (the “<b>Agreement</b>”) when the GDPR applies to your use of the AWS Services to process Customer Data. This DPA is an agreement between the Customer (“<b>Customer</b>”) and Amazon Web Services, Inc. and the AWS Contracting Party or AWS Contracting Parties (as applicable) under the Agreement (together “<b>AWS</b>”), jointly referred to as the “<b>Parties</b>”). Unless otherwise defined in this DPA or in the Agreement, all capitalised terms used in this DPA will have the meanings given to them in Section 17 of this DPA.</p> <p><b>1. Data Processing.</b></p> <p><b>1.1 Scope and Roles.</b> This DPA applies when Customer Data is processed by AWS for the performance of the services covered by the Agreement. In this context, AWS will act as a data processor for the Customer where the Customer acts as a Data Controller, or as Other-Processor in case Customer acts as Data processor on behalf of the Client Administration.</p> <p><b>1.2 Customer Controls.</b> Customer can use the Service Controls to assist it with its obligations under the GDPR, including its obligations to respond to requests from data subjects. Considering the nature of the processing, if AWS becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. AWS will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.</p> <p><b>1.3 Details of Data Processing.</b></p> <p><b>1.3.1 Subject matter.</b> The subject matter of the data processing under this DPA is Customer Data.</p> <p><b>1.3.2 Duration.</b> As between AWS and Customer, the duration of the data processing under this DPA is determined by the duration of the Agreement signed between the Customer and AWS and any extensions thereto, unless the Customer first terminates the Agreement.</p> | <p><b>ADDENDUM SUL TRATTAMENTO DEI DATI DA PARTE DI AWS AI SENSI DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (GDPR)</b></p> <p>Il presente Addendum sul Trattamento dei Dati (“<b>DPA</b>”) integra il Contratto tra il Cliente e AWS, come di volta in volta aggiornato, o altro accordo tra le medesime parti che regoli l'uso, da parte del Cliente, delle Offerte di Servizi (il “<b>Contratto</b>”) quando il Regolamento Generale Sulla Protezione Dei Dati si applica all'uso dei Servizi AWS da parte dell’utente ai fini del trattamento dei Dati del Cliente. Il presente DPA costituisce un accordo tra il Cliente (il “<b>Cliente</b>”) e Amazon Web Services, Inc. e la Parte contraente o le Parti contraenti AWS (a seconda dei casi) ai sensi del Contratto (congiuntamente “<b>AWS</b>”), congiuntamente indicate come le “<b>Parti</b>”. Salvo ove diversamente stabilito nel presente DPA o nel Contratto, tutti i termini in maiuscolo nel presente DPA avranno il significato ad essi attribuito all’Articolo 17 del presente DPA.</p> <p><b>1. Trattamento dei dati.</b></p> <p><b>1.1 Ambito di applicabilità e funzioni.</b> Il presente DPA si applica quando i Dati del Cliente vengono trattati da AWS per l’esecuzione dei servizi oggetto del Contratto. In questo contesto, AWS agirà in qualità di responsabile del trattamento per il Cliente, laddove il Cliente rivesta il ruolo di Titolare del trattamento, ovvero in qualità di Altro-Responsabile nel caso in cui il Cliente agisca in qualità di Responsabile del trattamento dei dati per conto dell’Amministrazione Cliente.</p> <p><b>1.2 Sistemi di Controllo a disposizione del Cliente.</b> Il Cliente potrà valutare se utilizzare i Sistemi di Controllo del Servizio che agevolano l’adempimento degli obblighi previsti a suo carico dal Regolamento Generale sulla Protezione dei Dati, ivi compresi gli obblighi di rispondere alle richieste degli interessati. Tenendo conto della natura del trattamento, AWS informerà tempestivamente il Cliente qualora venga a conoscenza che i Dati del Cliente trasferiti ai sensi delle Clausole Contrattuali Standard risultino inesatti o obsoleti. AWS collaborerà con il Cliente al fine di cancellare o rettificare i Dati del Cliente inesatti o obsoleti trasferiti ai sensi delle Clausole Contrattuali Standard, mettendo a disposizione i Sistemi di Controllo del Servizio che il Cliente potrà utilizzare per cancellare o rettificare i Dati del Cliente.</p> <p><b>1.3 Elementi essenziali del trattamento.</b></p> <p><b>1.3.1 Oggetto.</b> L'oggetto del trattamento dei dati ai sensi del presente DPA sono i Dati del Cliente.</p> <p><b>1.3.2 Durata.</b> Per quanto riguarda AWS e il Cliente, la durata del trattamento dei dati ai sensi del presente DPA coincide con la durata del Contratto sottoscritto fra il Cliente e AWS e delle sue</p> |
|--|--|

|  |   |
|--|---|
| <p><b>1.3.3 Purpose.</b> The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.</p> <p><b>1.3.4 Nature of the processing.</b> Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time which may include processing in connection with the use of the Services by Customer or Customer's Client Administrations.</p> <p><b>1.3.5 Type of Customer Data.</b> Customer Data uploaded to the Services under Customer's AWS accounts.</p> <p><b>1.3.6 Categories of data subjects.</b> The data subjects could include Customer's customers, employees, suppliers and employees of Customer's Client Administrations.</p> <p><b>1.3.7 Changes to essential elements of processing.</b> The essential elements of processing communicated by the Customer before the start of the processing may be subject to integration, variation or modification with a suitable communication that the Customer can send to AWS during the execution of the Contract, in compliance with the provisions of this DPA.</p> <p><b>1.4 Compliance with Laws.</b> Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.</p> <p><b>2. Customer Instructions.</b> The parties agree that this DPA and the Agreement (including Customer providing instructions via configuration tools such as the AWS management console and APIs made available by AWS for the Services) constitute Customer's documented instructions regarding AWS's processing of Customer Data ("<b>Documented Instructions</b>"). AWS will process Customer Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Customer is entitled to terminate this DPA and the Agreement if AWS declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Considering the nature of the processing, AWS will promptly inform the Customer if it will become aware that the Documented Instructions given to it by the Customer in the manner provided for in this DPA are or may be contrary to the Rules in Subject matter of Personal Data Protection.</p> | <p>eventuali proroghe, salvo che il Cliente non receda previamente dal Contratto.</p> <p><b>1.3.3 Finalità.</b> Lo scopo del trattamento dei dati ai sensi del presente DPA è la fornitura dei Servizi di volta in volta avviati dal Cliente.</p> <p><b>1.3.4 Natura del trattamento.</b> L'elaborazione, conservazione e altri Servizi di cui alla Documentazione di volta in volta intrapresi dal Cliente che possono includere anche il trattamento connesso all'uso dei Servizi da parte del Cliente o delle Amministrazioni Clienti.</p> <p><b>1.3.5 Tipologia dei Dati del Cliente.</b> I Dati del Cliente caricati nei Servizi nell'ambito degli account AWS del Cliente.</p> <p><b>1.3.6 Categorie degli interessati.</b> Gli interessati possono essere i clienti, i dipendenti, i fornitori del Cliente, i dipendenti delle Amministrazioni Clienti.</p> <p><b>1.3.7 Modifiche degli elementi essenziali del trattamento.</b> Gli elementi essenziali del trattamento comunicati dal Cliente prima dell'avvio delle attività di trattamento potranno essere oggetto di integrazione, variazione o modifica con idonea comunicazione che il Cliente potrà inviare ad AWS nel corso dell'esecuzione del Contratto, nel rispetto di quanto previsto nel presente DPA.</p> <p><b>1.4 Conformità.</b> Ciascuna Parte rispetterà tutte le Norme in materia di Protezione dei Dati Personali ad essa applicabili e vincolanti nell'esecuzione del presente DPA, ivi compreso il Regolamento Generale sulla Protezione dei Dati.</p> <p><b>2. Istruzioni del Cliente.</b> Le Parti convengono che il presente DPA e il Contratto (ivi comprese le ulteriori istruzioni fornite dal Cliente tramite strumenti di configurazione quali la console di gestione AWS e le API messe a disposizione da AWS per i Servizi) costituiscono le istruzioni documentate del Cliente in relazione al trattamento dei Dati del Cliente da parte di AWS ("<b>Istruzioni Documentate</b>"). AWS tratterà i Dati del Cliente unicamente in conformità alle Istruzioni Documentate (che, ove il Cliente agisca in qualità di Responsabile del trattamento, potrebbero essere basate sulle istruzioni dei rispettivi titolari del trattamento). Il Cliente ha il diritto di risolvere il presente DPA e il Contratto nel caso in cui AWS rifiuti di seguire eventuali istruzioni fornite dal Cliente che esulano dall'ambito di applicabilità o diverse rispetto a quelle impartite o concordate nel presente DPA. Tenendo conto della natura del trattamento, AWS informerà prontamente il Cliente nel caso in cui venga a conoscenza che le Istruzioni Documentate impartitegli dal Cliente attraverso le modalità previste nel presente DPA siano o possano essere contrarie alle Norme in materia di Protezione dei Dati Personali. Resta inteso che il Cliente riconosce ed accetta di essere l'unico responsabile della conformità delle</p> |
|--|---|

|  |   |
|--|---|
| <p>It is understood that the Customer acknowledges and accepts that he is solely responsible for compliance with the instructions given to the Rules on the Protection of Personal Data.</p> <p><b>3. Confidentiality of Customer Data.</b> AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends AWS a demand for Customer Data, AWS will do its best to redirect the governmental body to request that data directly from Customer. As part of this effort, AWS may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then AWS will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so.</p> <p><b>4. Confidentiality Obligations of AWS Personnel.</b> AWS is committed to preventing its personnel from processing Customer Data without authorization by AWS as described in the AWS Security Standards. AWS ensures that its staff has been authorized and instructed to process Customer Data in compliance with GDPR and with the commitments that AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.</p> <p><b>5. Security of Data Processing</b></p> <p>5.1 Pursuant to Article 32 of the GDPR AWS has implemented and will maintain the technical and organizational measures for the AWS Network which allow to ensure a security level appropriate for the risk, as described in the AWS Security Standards and this Section. In particular, AWS has implemented and will maintain the following technical and organizational measures:</p> <ul style="list-style-type: none"> <li>(a) security of the AWS Network as set out in Section 1.1 of the AWS Security Standards;</li> <li>(b) physical security of the facilities as set out in Section 1.2 of the AWS Security Standards;</li> <li>(c) measures to control access rights for AWS employees and contractors to the AWS Network as set out in Section 1.1 of the AWS Security Standards; and</li> </ul> | <p>istruzioni impartite alle Norme in materia di Protezione dei Dati Personali.</p> <p><b>3. Riservatezza dei Dati del Cliente.</b> AWS non accederà ai Dati del Cliente, non li utilizzerà e non li divulgherà a terzi, salvo comunque ove ciò dovesse rendersi necessario ai fini del mantenimento in essere o della fornitura dei Servizi, o ai fini della conformità alle disposizioni di legge o all'ordine valido e vincolante di un ente governativo (quali una citazione in giudizio o un ordine del tribunale). Qualora un ente governativo richieda ad AWS i Dati del Cliente, AWS farà quanto nelle proprie possibilità per far sì che l'ente governativo richieda tali dati direttamente al Cliente. A tal proposito, AWS potrà fornire all'ente governativo le informazioni di contatto di base del Cliente. Ove sia costretta a divulgare i Dati del Cliente a un ente governativo, AWS invierà al Cliente un preavviso ragionevole onde consentirgli di richiedere un ordine di protezione o altro rimedio appropriato, salvo ove AWS non abbia facoltà di farlo.</p> <p><b>4. Obblighi di riservatezza del personale AWS.</b> AWS si impegna ad impedire al proprio personale di trattare i Dati del Cliente in assenza dell'autorizzazione di AWS, come specificato negli Standard di Sicurezza AWS. AWS garantisce che il proprio personale sia stato autorizzato ed istruito a trattare i Dati del Cliente in conformità al GDPR e a specifici obblighi contrattuali che AWS impone al proprio personale, ivi compresi quelli relativi alla riservatezza, alla protezione e alla sicurezza dei dati.</p> <p><b>5. Sicurezza del Trattamento dei Dati</b></p> <p>Ai sensi dell'Articolo 32 del GDPR, AWS ha implementato e manterrà in essere le misure tecniche e organizzative per la Rete AWS che consentono di garantire un livello di sicurezza adeguato al rischio, come descritte negli Standard di Sicurezza AWS e nel presente Articolo. In particolare, AWS ha implementato e manterrà in essere le seguenti misure tecniche e organizzative:</p> <ul style="list-style-type: none"> <li>(a) sicurezza della Rete AWS come indicato all'Articolo 1.1 degli Standard di Sicurezza AWS;</li> <li>(b) sicurezza fisica delle strutture, come stabilito all'Articolo 1.2 degli Standard di Sicurezza AWS;</li> <li>(c) misure di controllo dei diritti di accesso dei dipendenti di AWS e dei rispettivi appaltatori alla Rete AWS, come specificato all'Articolo 1.1 degli Standard di Sicurezza AWS; e</li> </ul> |
|--|---|

|  |  |
|--|--|
| <p>(d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by AWS as described in Section 2 of the AWS Security Standards.</p> <p>5.2 Customer can elect to implement technical and organizational measures to protect Customer Data. Such technical and organizational measures include the following which can be obtained by Customer from AWS as described in the Documentation, or directly from a third-party supplier:</p> <ul style="list-style-type: none"> <li>(a) pseudonymization and encryption to ensure an appropriate level of security;</li> <li>(b) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer;</li> <li>(c) measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and</li> <li>(d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.</li> </ul> <p><b>6. Sub-processing.</b></p> <p><b>6.1 Authorized Sub-processors.</b> Customer provides general authorization to AWS's use of sub-processors to provide processing activities on Customer Data on behalf of Customer in accordance with this Section. The AWS website (currently posted at <a href="https://aws.amazon.com/compliance/sub-processors/">https://aws.amazon.com/compliance/sub-processors/</a>) lists Sub-processors that are currently engaged by AWS as of the date of the signature of the Contract, containing the name and company name of the Sub-processors, appropriately listed in Annex 2 to this DPA. For each Sub-Processor authorized pursuant to the provisions of this article, the possible location in a non-EU country is also indicated, with respect to which the provisions contained in art. 12 of this DPA. Furthermore, AWS undertakes to inform the Customer or, if required, the Client Administration (in the event that the latter is the Data Controller) - upon notification request by the latter activated through the automatic notification system made available by AWS - of any additions or replacements by Sub-Processors during the term of the Agreement in order to enable Customer or Client Administration to object to such additions or replacements within 30 calendar days after such notice is received. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; (ii) cease using the Service for which AWS has engaged the Sub-processor; or</p> | <p>(d) procedure per testare, verificare e valutare su base regolare l'efficacia delle misure tecniche e organizzative adottate da AWS, come descritto all'Articolo 2 degli Standard di Sicurezza AWS.</p> <p>5.2 Il Cliente potrà scegliere di adottare misure tecniche e organizzative ai fini della protezione dei Dati del Cliente. Tali misure tecniche e organizzative comprendono le seguenti, che il Cliente potrà ricevere da AWS come descritto nella Documentazione, o direttamente da un fornitore terzo:</p> <ul style="list-style-type: none"> <li>(a) pseudonimizzazione e crittografia per garantire un livello di sicurezza adeguato;</li> <li>(b) misure atte a garantire la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento gestiti dal Cliente;</li> <li>(c) misure che consentano al Cliente di eseguire il backup e l'archiviazione in modo adeguato onde ripristinare tempestivamente la disponibilità dei Dati del Cliente e l'accesso ai medesimi in caso di incidente fisico o tecnico; e</li> <li>(d) procedure per testare, verificare e valutare su base regolare l'efficacia delle misure tecniche e organizzative adottate dal Cliente.</li> </ul> <p><b>6. Trattamento da parte di Sub-Responsabili</b></p> <p><b>6.1 Sub-Responsabili del trattamento.</b> Il Cliente autorizza AWS a ricorrere a Sub-Responsabili per svolgere specifiche attività di trattamento dei Dati del Cliente per conto del Cliente in conformità al presente Articolo. Sul sito web di AWS (attualmente all'indirizzo <a href="https://aws.amazon.com/compliance/sub-processors/">https://aws.amazon.com/compliance/sub-processors/</a>) è presente una lista dei Sub-Responsabili di cui intende avvalersi AWS alla data di sottoscrizione del Contratto, contenente denominazione e ragione sociale dei Sub-responsabili, opportunamente riportata nell'Allegato 2 al presente DPA. Per ciascun Sub-Responsabile autorizzato ai sensi di quanto previsto nel presente articolo, è indicata anche l'eventuale collocazione in un Paese extra-UE, rispetto al quale trovano applicazione le previsioni contenute nell'art. 12 del presente DPA. Inoltre, AWS si impegna ad informare il Cliente o, se richiesto, l'Amministrazione Cliente (nel caso in cui quest'ultima sia il Titolare) – previa richiesta di notifica da parte di queste ultime attivata attraverso il sistema di notifica automatica messo a disposizione da AWS – di eventuali aggiunte o sostituzioni dei Sub-Responsabili nel corso della durata del Contratto al fine di consentire al Cliente o all'Amministrazione Cliente di opporsi a tali aggiunte o sostituzioni entro 30 giorni di calendario dal momento in cui avviene la suddetta comunicazione. Al fine di opporsi all'inserimento di un Sub Responsabile, il Cliente potrà: (i) risolvere il Contratto in base ai rispettivi termini; (ii) cessare di</p> |
|--|--|

|  |  |
|--|--|
| <p>(iii) move the relevant Customer Data to another AWS Region where AWS has not engaged the Sub-processor.</p> <p><b>6.2 Sub-processor Obligations.</b> Where AWS authorizes a Sub-processor as described in Section 6.1:</p> <ul style="list-style-type: none"> <li>(i) AWS will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and AWS will prohibit the Sub-processor from accessing Customer Data for any other purpose;</li> <li>(ii) AWS will enter into a written agreement with the Sub-processor with appropriate obligations in light of the role of such sub-processor with respect to the provisions of this DPA and the agreement to the extent that the Sub-processor performs specific Customer data processing activities, pursuant to this DPA, including the same obligations regarding the protection of personal data set forth in the Agreement and in this DPA, where applicable. In particular, AWS ensures that the Sub-Processor ensures the adoption of all Security Measures and in compliance with the provisions of the Agreement, this DPA and the Personal Data Protection Regulations and any further instructions given by the Customer; and</li> <li>(iii) AWS will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause AWS to breach any of AWS's obligations under this DPA or personal data protection provisions by AWS.</li> </ul> <p><b>7. AWS Assistance with Data Subject Requests.</b> Considering the nature of the processing, the Service Controls are the technical and organizational measures by which AWS will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under the GDPR. If AWS receives complaints and/or the Data Subjects exercise their rights by transmitting the related request directly to AWS, the latter, after having ascertained that it is a Customer's data subject, must forward it promptly and in any case without unjustified delay to the Customer through the certified e-mail address indicated in the Customer's Account.</p> <p>In fact, AWS will be required to check the requests of the data subjects only if it has been authorized by the Customer and/or by the Client Administration (in the event that the latter is the Data Controller).</p> | <p>utilizzare il Servizio per il quale AWS ha incaricato il Sub Responsabile; o (iii) spostare i Dati del Cliente rilevanti in un'altra regione AWS in cui AWS non abbia conferito l'incarico a tale Sub Responsabile.</p> <p><b>6.2 Obblighi del Sub-Responsabile del trattamento.</b> Nel caso in cui AWS si avvalga di un Sub-Responsabile autorizzato dal Cliente ai sensi dell'Articolo 6.1:</p> <ul style="list-style-type: none"> <li>(i) il Sub-Responsabile potrà accedere ai Dati del Cliente unicamente nella misura necessaria a fornire o mantenere in essere i Servizi in conformità alla Documentazione, e AWS proibirà al Sub-Responsabile di accedere ai Dati del Cliente per qualsiasi altra finalità;</li> <li>(ii) AWS stipulerà un accordo scritto con il Sub-Responsabile con obbligazioni appropriate al ruolo di quest'ultimo con riferimento a quanto previsto nel presente DPA e nel contratto nella misura in cui il Sub-Responsabile esegua specifiche attività di trattamento dei dati del Cliente, ai sensi del presente DPA, includendo gli stessi obblighi in materia di protezione dei dati personali previsti nel Contratto e nel presente DPA, ove applicabili. In particolare, AWS garantisce che il Sub-Responsabile del trattamento assicuri l'adozione di tutte le Misure di Sicurezza a in conformità a quanto previsto nel Contratto, nel presente DPA e nelle Norme in materia di Protezione dei Dati Personali e alle eventuali ulteriori istruzioni impartite dal Cliente;</li> <li>(iii) AWS rimarrà responsabile della conformità agli obblighi previsti dal presente DPA e per ogni azione o omissione posta in essere dai Sub-Responsabili tale da determinare una violazione del presente DPA o delle disposizioni in materia di protezione dei dati personali da parte di AWS.</li> </ul> <p><b>7. Assistenza di AWS in relazione alle Richieste degli Interessati.</b> Tenuto conto della natura del trattamento, i Sistemi di Controllo del Servizio rappresentano le misure tecniche e organizzative con cui AWS assiste il Cliente nell'adempimento dei propri obblighi di risposta alle richieste degli interessati previsti dal Regolamento Generale sulla Protezione dei Dati. Qualora AWS riceva reclami e/o gli Interessati esercitino i propri diritti trasmettendo la relativa richiesta direttamente ad AWS, quest'ultima, dopo aver accertato che si tratti di un interessato del Cliente, deve inoltrarla tempestivamente e comunque senza ingiustificato ritardo al Cliente attraverso l'indirizzo di posta elettronica certificata indicata nell'Account del Cliente.</p> <p>AWS, infatti, sarà tenuta a riscontrare le istanze degli Interessati solo qualora sia stata autorizzata dal Cliente e/o</p> |
|--|--|

Where required, AWS will lend its support to the Customer and/or the Administration, who are required to provide feedback to the requests of the data subjects and to their requests for exercising the rights provided for by the articles 15-22 of the Regulations, exclusively through the provision of Service Control Systems which fall within the technical and organizational measures of the Services with which AWS assists the Customer in fulfilling its obligations to respond to requests from data subjects.

**8. Records of Processing activities.** AWS is obliged to prepare, keep, also in electronic format, and update Records of all the Processing activities carried out in the capacity of Data Processor or Sub-processor (hereinafter "**Register**"), in accordance with the provisions of article 30, par. 2, of the Regulation. At the request of the Supervisory Authority, AWS will make the Registry available to the Authority itself, at the same time informing the Customer. AWS, where requested, undertakes to support the Customer in the census of the Processing Activities related to the Contract, also in order to ensure the consistency of the respective Records of Processing activities.

#### **9. Data breach Notification.**

**9.1 Personal Data Breaches.** . AWS will (a) document Personal Data Breaches related to Processing activities delegated by Customer; (b) notify Customer of any Personal Data Breach immediately and, in any case, without undue delay after AWS or its Sub-Processor becomes aware of it and (b) adopt, after sharing with Customer, suitable measures to address the Violation of personal data, including measures aimed at mitigating any damage or harmful consequence for the rights and freedoms of the data subjects, deriving from this Violation.

**9.2 AWS Assistance.** To enable Customer to notify a Personal Data Breach to supervisory authorities or data subjects (as applicable), AWS will cooperate with and assist Customer by including in the notification under Section 9.1(a) and (b) such information about the Personal Data Breach that AWS is able to disclose to Customer, considering the nature of the processing, the information available to AWS, and any restrictions on disclosing the information, such as confidentiality. Furthermore, considering the nature of the processing and the information available to AWS, AWS will assist the Customer in complying with its obligations pursuant to Articles 33 and 34 of the GDPR by fulfilling its obligations under this Section 9.

dall'Amministrazione Cliente (nel caso in cui quest'ultima sia il Titolare del trattamento).

Ove richiesto, AWS presterà il proprio supporto al Cliente e/o all'Amministrazione, che sono tenuti a fornire riscontro alle richieste degli Interessati e alle istanze degli stessi per l'esercizio dei diritti previsti dagli artt. 15-22 del Regolamento, esclusivamente mediante la messa a disposizione di Sistemi di Controllo del Servizio che rientrano tra le misure tecniche e organizzative dei Servizi con cui AWS assiste il Cliente nell'adempimento dei propri obblighi di risposta alle richieste degli interessati.

**8. Registro dei trattamenti.** AWS è obbligato a predisporre, conservare, anche in formato elettronico, e aggiornare un registro di tutte le attività di Trattamento svolte in qualità di Responsabile o di Sub-Responsabile del trattamento (di seguito "**Registro**"), conformemente a quanto previsto dall'art. 30, par. 2, del Regolamento. Su richiesta dell'Autorità di controllo, AWS metterà a disposizione il Registro all'Autorità stessa dandone al contempo informazione al Cliente. AWS, ove richiesto, si impegna a supportare il Cliente nelle attività di censimento dei Trattamenti inerenti al Contratto, anche al fine di assicurare la coerenza dei rispettivi Registri del trattamento.

#### **9. Comunicazione in caso di data breach.**

**9.1 Violazioni di dati personali.** AWS (a) documenterà le Violazioni di dati personali riferibili ai Trattamenti delegati dal Cliente; (b) comunicherà al Cliente ogni Violazione di dati personali immediatamente e, in ogni caso, senza ingiustificato ritardo da quando AWS o un suo Sub-Responsabile ne ha avuto conoscenza e (b) adotterà, previa condivisione con il Cliente, misure idonee ad affrontare la Violazione dei dati personali, ivi comprese misure volte a mitigare qualsivoglia danno o conseguenza lesiva per i diritti e delle libertà degli Interessati, derivanti da tale Violazione.

**9.2 Assistenza AWS.** Al fine di consentire al Cliente di comunicare la Violazione dei dati personali alle autorità di controllo o agli interessati (a seconda dei casi), AWS collaborerà con il Cliente e lo assisterà includendo nella comunicazione di cui all'Articolo 9.1(a) e (b) le informazioni riguardanti la Violazione dei dati personali che AWS è in grado di riferire al Cliente, tenendo conto della natura del trattamento, delle informazioni disponibili ad AWS e di eventuali restrizioni alla divulgazione delle informazioni, quali gli obblighi di riservatezza. Inoltre, tenendo conto della natura del trattamento e delle informazioni a disposizione di AWS, AWS assisterà il Cliente nel rispettare i propri obblighi ai sensi degli articoli 33 e 34 del Regolamento adempiendo ai propri obblighi ai sensi della presente Sezione 9.

|  |  |
|--|--|
| <p><b>9.3 Communication.</b> Notification(s) of any personal data breaches, if any, will be sent to the Customer, immediately and, in any case, without undue delay, via the email address indicated in the Account, together with all the necessary documentation held by AWS taking into account of the nature of the processing activities, to allow the Data Controller (the Customer or the Client Administration) to notify, possibly in a preliminary way, said Violation to the competent Supervisory Authority within the terms of the law.</p> <p><b>10. AWS Certifications and Audits.</b></p> <p><b>10.1 AWS ISO-Certification and SOC Reports.</b> In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information:</p> <ul style="list-style-type: none"> <li>(i) the certificates issued for the ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification, and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and</li> <li>(ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).</li> </ul> <p><b>10.2 AWS Audits.</b> AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third-party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("<b>Report</b>"), which will be AWS's Confidential Information.</p> <p><b>10.3 Audit Reports.</b> At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this DPA. Customer may share the Report with its own customers who (i) are controllers under the GDPR in relation to personal data which forms part of Customer Data</p> | <p><b>9.3 Comunicazioni.</b> Le comunicazioni di eventuali Violazioni di dati personali saranno inviate immediatamente e, in ogni caso, senza ingiustificato ritardo e saranno trasmesse al Cliente attraverso l'indirizzo di posta elettronica indicata nell'Account, insieme a tutta la documentazione necessaria e in possesso di AWS tenendo conto della natura del trattamento, per consentire al Titolare (il Cliente o l'Amministrazione Cliente) di notificare, eventualmente in via preliminare, detta Violazione all'Autorità di controllo competente entro i termini di legge</p> <p><b>10. Certificazioni e verifiche AWS.</b></p> <p><b>10.1 Certificazioni ISO e Relazioni SOC AWS.</b> In aggiunta alle informazioni di cui al presente DPA, su richiesta del Cliente e a condizione che tra le parti sia in essere un NDA valido, AWS metterà a disposizione i documenti e le informazioni qui di seguito indicati:</p> <ul style="list-style-type: none"> <li>(iii) i certificati emessi per la certificazione ISO 27001, la certificazione ISO 27017, la certificazione ISO 27018 e la certificazione ISO 27701 (ovvero le certificazioni o altra documentazione che attestino la conformità a standard alternativi sostanzialmente equivalenti a ISO 27001, ISO 27017, ISO 27018, e ISO 27701); e</li> <li>(iv) la Relazione sui Controlli di Sistema e Organizzazione (SOC) 1, la Relazione sui Controlli di Sistema e Organizzazione (SOC) 2 e la Relazione sui Controlli di Sistema e Organizzazione (SOC) 3 (ovvero le relazioni o altra documentazione che illustri i controlli sostitutivi o equivalenti adottati da AWS rispetto a SOC 1, SOC 2 e SOC 3).</li> </ul> <p><b>10.2 Verifiche AWS.</b> AWS si avvale di revisori esterni al fine di verificare l'adeguatezza delle proprie misure di sicurezza, ivi compresa la sicurezza dei centri dati fisici dai quali AWS fornisce i Servizi. Tale verifica: (a) verrà effettuata con una frequenza minima annuale; (b) verrà effettuata in conformità agli standard ISO 27001 o standard alternativi diversi che siano sostanzialmente equivalenti a ISO 27001; (c) verrà effettuata da un professionista della sicurezza terzo indipendente, selezionato a cura e a spese di AWS; e (d) si concluderà con la predisposizione di una relazione di verifica ("<b>Relazione</b>"), che sarà ricompresa tra le Informazioni Riservate di AWS.</p> <p><b>10.3 Relazioni di Verifica.</b> Su richiesta scritta del Cliente, e a condizione che tra le parti sia in essere un NDA valido, AWS fornirà al Cliente copia della Relazione, in modo tale che lo stesso possa ragionevolmente verificare l'ottemperanza da parte di AWS agli obblighi alla stessa spettanti ai sensi del presente DPA. Il Cliente può condividere il Rapporto con i propri clienti che (i) sono titolari del trattamento ai sensi del GDPR in</p> |
|--|--|

and (ii) have a valid non-disclosure agreement in place with AWS.

**10.4 Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the processing and the information available to AWS, AWS will assist Customer, or the Client Administration (in the event that the latter is the Data Controller) through the Customer, both at a technical and organizational level in carrying out of the impact assessment on the protection of personal data, as regulated by art. 35 of the Regulation, in all cases in which the Processing provides for, requires or imposes the conduct and/or updating of the same. AWS will assist in the prior consultation activity of the Supervisory Authority pursuant to art. 35 of the Regulation, providing the information in its availability necessary for this purpose.

**11. Customer Audits.** AWS undertakes to transmit all information and documentation that the Customer may reasonably request during the execution of the Contract, to verify the compliance, by AWS or its Sub-Processors, with the provisions of this DPA and with the Rules regarding the protection of personal data and the instructions received. If the Customer intends to carry out, at AWS or its Sub-processors, control and evaluation activities, including any inspections, it can do so by instructing AWS to carry out the audit described in Section 10. Considering the nature of the treatment and the aforementioned methods of audit, AWS will, without any delay and/or omission, make available to the Customer all necessary information in its possession to demonstrate its compliance with the aforementioned obligations. In the event that, as a result of these checks, the Security Measures are found to be inadequate and/or unsuitable to ensure the application of the Personal Data Protection Regulations, the Customer will warn AWS to adopt the necessary measures within a reasonable period which will be fixed if necessary (taking into account the nature, scope, context and purposes of the Processing, the type of data and the category of data subjects involved as well as the level of risk of violation and/or the seriousness of the violation that occurred ), without prejudice to the remedies available under the Contract and/or the law.

Furthermore, AWS shall immediately inform and assist the Customer and/or the Client Administration (in the event that the latter is the Data Controller) in the event of inspections, any measures taken against it or in the event of proceedings before to the National and European personal data protection authorities and/or to the Judicial Authority in relation to the Processing entrusted to them, except in the case in which such communication is prohibited by the order or by the law, by a binding judicial or governmental provision or from any restrictions on the disclosure of confidential information.

In such circumstances, unless prohibited by law, AWS must: i) inform the Customer promptly and without unjustified delay, and in any case no later than 24 hours from receipt of the ostension request; ii) collaborate with the Customer and/or with the Client Administration (where the latter is the Data Controller), in the event that they intend to legally oppose such communication; iii) guarantee the confidential treatment of such information.

relazione ai dati personali che fanno parte dei Dati del cliente e (ii) hanno stipulato un accordo di riservatezza valido con AWS.

**10.4 Valutazione d'impatto sulla protezione dei dati personali e consultazione preventiva.** In considerazione della natura del trattamento e delle informazioni a disposizione di AWS, AWS fornirà assistenza al Cliente o all'Amministrazione Cliente (nel caso in cui quest'ultima sia Titolare del trattamento) per il tramite del Cliente sia a livello tecnico che organizzativo nello svolgimento della valutazione di impatto sulla protezione dei dati personali, così come disciplinata all'art. 35 del Regolamento, in tutte le ipotesi in cui il Trattamento preveda, necessiti o imponga la conduzione e/o l'aggiornamento della stessa. AWS presterà la propria assistenza nell'attività di consultazione preventiva dell'Autorità di controllo ai sensi dell'art. 35 del Regolamento, fornendo le informazioni nella propria disponibilità all'uopo necessarie.

**11. Attività di controllo da parte del Cliente ed ulteriori obblighi di AWS.** AWS si impegna a trasmettere tutte le informazioni e la documentazione che il Cliente potrà ragionevolmente richiederli durante l'esecuzione del Contratto, per verificare il rispetto, da parte di AWS o dei suoi Sub-Responsabili del trattamento, delle previsioni del presente DPA e delle Norme in materia di Protezione dei Dati Personali e delle istruzioni ricevute. Qualora il Cliente intenda effettuare, presso AWS o i suoi Sub-Responsabili, attività di controllo e valutazione, ivi comprese eventuali ispezioni, potrà farlo istruendo AWS a effettuare l'audit descritto nella Sezione 10. Tenuto conto della natura del trattamento e delle predette modalità di audit, AWS metterà, senza alcun ritardo e/o omissione, a disposizione del Cliente tutte le informazioni necessarie in suo possesso per dimostrare la sua conformità con i suddetti obblighi. Nel caso in cui all'esito di detti controlli, le Misure di Sicurezza risultino inadeguate e/o inidonee ad assicurare l'applicazione delle Norme in materia di Protezione dei Dati Personali, il Cliente diffiderà AWS ad adottare le misure necessarie entro un termine congruo che sarà all'occorrenza fissato (tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del Trattamento, della tipologia dei dati e della categoria dei soggetti Interessati coinvolti nonché del livello di rischio violazione e/o della gravità della violazione verificatasi), fatti salvi i rimedi esperibili ai sensi del Contratto e/o della legge.

Inoltre, AWS dovrà rendere immediatamente edotto e coadiuvare il Cliente e/o l'Amministrazione Cliente (nel caso in cui quest'ultima sia il Titolare del trattamento) in caso di ispezioni, di eventuali misure adottate nei suoi confronti o in

caso di procedure dinanzi alle Autorità per la protezione dei dati personali, nazionali ed europee, e/o all'Autorità Giudiziaria in relazione ai Trattamenti mandatigli e salvo il caso in cui tale comunicazione non sia vietata dal provvedimento o dalla legge, da un provvedimento giudiziario o governativo vincolante o da eventuali restrizioni alla divulgazione di informazioni riservate.

In simili circostanze, salvo divieti pervisti dalla legge, AWS deve: i) informare il Cliente tempestivamente e senza ingiustificato ritardo e comunque entro e non oltre 24 ore dal ricevimento della richiesta di ostensione; ii) collaborare con il Cliente e/o con l'Amministrazione Cliente (ove quest'ultima sia il Titolare del trattamento) nell'eventualità in cui gli stessi intendano opporsi legalmente a tale comunicazione; iii) garantire il trattamento riservato di tali informazioni.



## 12. Transfers of Personal Data.

**12.1 Regions.** Customer can specify the location(s) where Customer Data will be processed within the AWS Network (each a "Region"), including Regions in the EEA. Once Customer has made its choice, AWS shall ensure that Customer Data will be processed within the Region(s) selected by Customer and that no transfer of the same to a Third Country will take place or a Region other than the one(s) selected by the Customer, with the exception of the countries/territories/organisations covered by an adequacy decision made by the European Commission pursuant to art. 45 Regulation or by other adequate guarantees referred to in articles 46 et seq. of the Regulation itself (e.g. use of the standard contractual clauses adopted by the European Commission pursuant to Article 46, paragraph 2, letter c) of the Regulation, use of the Binding Corporate Rules - BCR), without prejudice to the need assessed in advance by the Parties to adopt any additional measures to ensure the effectiveness of these guarantees. Apart from the aforementioned exceptions, AWS will have to ensure that any platforms/servers on which the aforementioned data transit are based in the EU and that any replication of the data is not transmitted outside the EU or the European Economic Area. In the event that the Customer chooses to receive some of the services made available by AWS which provide for remote assistance/maintenance services, the performance of which in any case involves the transfer outside the EU of data plots connected to the service itself, the Customer may use AWS services to encrypt such Personal Data contained in the data plot. In the event that the transfer is necessary to fulfill a specific requirement under European Union or Italian law to which AWS is subject, the latter is required to inform the Customer about this legal obligation, prior to the Processing, unless that this is prohibited by law or to comply with a mandatory judicial or governmental order.

Should non-EU data transfers result in the absence of the adequate guarantees mentioned above, AWS will be warned to immediately stop the unauthorized data transfer, without prejudice to the remedies provided by law and/or by the Contract.

## 12. Trasferimento dei dati personali.

**12.1 Regioni.** Il Cliente potrà indicare il luogo (o i luoghi) in cui i Dati del Cliente verranno trattati nell'ambito della Rete AWS (singolarmente la "**Regione**"), ivi comprese Regioni all'interno del SEE. Dopo che il Cliente avrà operato la propria scelta, AWS dovrà garantire che i Dati del Cliente verranno trattati all'interno della(e) Regione(i) selezionata(e) dal Cliente e che non sarà effettuato alcun trasferimento degli stessi verso un Paese Terzo o una Regione diversa da quella(e) selezionata(e) dal Cliente, fatta eccezione dei paesi/territori/organizzazioni coperti da una decisione di adeguatezza resa dalla Commissione europea ai sensi dell'art. 45 Regolamento o da altre garanzie adeguate di cui agli artt. 46 e ss. del Regolamento stesso (es. utilizzo delle clausole contrattuali tipo adottate dalla Commissione europea ai sensi dell'art. 46, par. 2, lett. c) del Regolamento, utilizzo delle norme vincolanti d'impresa Binding Corporate Rules - BCR), fatta salva la necessità valutata preventivamente tra le Parti di adottare eventuali misure supplementari per garantire l'efficacia di tali garanzie. Al di fuori delle predette eccezioni, AWS dovrà garantire che le eventuali piattaforme/server su cui transitino i suddetti dati abbiano sede nell'UE e che qualunque replica dei dati non sia trasmessa al di fuori della UE o dello Spazio Economico Europeo. Nel caso in cui il Cliente scelga di ricevere alcuni dei servizi resi disponibili da AWS che prevedono di servizi di assistenza/manutenzione da remoto il cui espletamento implichi comunque il trasferimento al di fuori dell'UE di tracciati di dati connessi al servizio stesso, il Cliente potrà utilizzare i servizi di AWS per criptare tali Dati Personali contenuti nel tracciato. Nel caso in cui il trasferimento si renda necessario per adempiere a un requisito specifico a norma del diritto dell'Unione Europea o italiano cui è soggetto AWS, quest'ultimo è tenuto ad informare il Cliente circa tale obbligo giuridico, prima del Trattamento, a meno che ciò sia vietato per legge o per adempiere ad un provvedimento giudiziario o governativo vincolante.

Qualora dovessero risultare trasferimenti di dati extra-UE in assenza delle adeguate garanzie di cui sopra, AWS verrà diffidato all'immediata interruzione del trasferimento di dati non autorizzato, fatti salvi i rimedi previsti dalla legge e/o dal Contratto

|   |   |
|---|---|
| <p><b>12.2 Application of Standard Contractual Clauses.</b> Subject to Section 12.3, the Standard Contractual Clauses will only apply to Customer Data that is transferred, either directly or via onward transfer, to any Third Country, (each a “<b>Data Transfer</b>”).</p> <p>12.2.1 When Customer is acting as a controller, the Controller- to-Processor Clauses will apply to a Data Transfer.</p> <p>12.2.2 When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Considering the nature of the processing, Customer agrees that it is unlikely that AWS will know the identity of Customer’s controllers because AWS has no direct relationship with Customer’s controllers.</p> <p><b>12.3 Alternative Transfer Mechanism.</b> The Standard Contractual Clauses will not apply to a Data Transfer if AWS has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Data Transfers.</p> <p><b>13. Termination of the DPA.</b> This DPA will continue in force until the termination of the Agreement (the “<b>Termination Date</b>”).</p> | <p><b>12.2 Applicazione delle Clausole Contrattuali Tipo.</b> Fatto salvo quanto stabilito all’Articolo 12.3, le Condizioni Contrattuali Tipo troveranno applicazione unicamente ai Dati del Cliente che siano trasferiti, direttamente o mediante inoltrato, a un Paese Terzo (singolarmente il “<b>Trasferimento dei Dati</b>”).</p> <p>12.2.1. Ove il Cliente agisca in qualità di titolare del trattamento, il Trasferimento dei Dati sarà soggetto alle Clausole relative al rapporto Titolare-Responsabile.</p> <p>12.2.2 Ove il Cliente agisca in qualità di responsabile del trattamento, il Trasferimento dei Dati sarà soggetto alle Clausole relative al rapporto tra Responsabili. In considerazione della natura del trattamento, il Cliente dà atto che verosimilmente AWS non conosce l’identità dei titolari del trattamento del Cliente, poiché AWS non ha alcun rapporto diretto con gli stessi.</p> <p><b>12.3 Meccanismo di trasferimento alternativo.</b> Le Clausole Contrattuali Tipo non troveranno applicazione al Trasferimento dei Dati qualora AWS abbia adottato le Regole Aziendali Vincolanti per i Responsabili del trattamento o uno standard di compliance alternativo riconosciuto ai fini del legittimo Trasferimento dei Dati.</p> <p><b>13. Risoluzione dell’DPA.</b> Il presente DPA rimarrà in vigore fino alla risoluzione del Contratto e delle sue eventuali proroghe (la “<b>Data di Risoluzione</b>”).</p> |
|---|---|

|   |   |
|---|---|
| <p><b>14. Return or Deletion of Customer Data.</b> At any time up to the Termination Date, and for 90 days following the Termination Date, AWS undertakes, for itself and also for its Sub- Processors, to allow the recovery of the Customer Data or to delete the Customer Data which it has come into possession in execution of the Contract and, subsequently, to delete all existing copies from any IT support, online and offline, used for the management and conservation of the same, following the request of the Customer activated through the Service Controls and aimed at requesting such recovery or cancellation as better described in the Technical Specifications.</p> <p>No later than the end of such 90 days period, Customer must close all AWS accounts containing Customer Data.</p> <p><b>15. Duties to Inform.</b> Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by AWS, AWS will inform Customer without undue delay. AWS will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer’s property and area of responsibility and that Customer Data is at Customer’s sole disposition.</p> | <p><b>14. Recupero o cancellazione dei Dati del Cliente.</b> In qualsiasi momento fino alla Data di Risoluzione ed entro i 90 giorni successivi alla stessa, AWS si impegna, per sé e anche per i propri Sub-Responsabili, a consentire il recupero dei Dati al Cliente o a cancellare i Dati del Cliente di cui sia venuto in possesso in esecuzione del Contratto e, successivamente, a cancellarne tutte le copie esistenti da qualsivoglia supporto informatico, online e offline, utilizzato per la gestione e conservazione degli stessi, a seguito della richiesta del Cliente attivata mediante i Controlli di Servizio e volta a richiedere tale recupero o cancellazione come meglio descritto nel Capitolato Tecnico.</p> <p>Entro e non oltre il termine di tale periodo di 90 giorni il Cliente dovrà chiudere tutti gli account AWS contenenti Dati del Cliente.</p> <p><b>15. Obblighi informativi.</b> Qualora i Dati del Cliente vengano confiscati nell’ambito di una procedura fallimentare o concorsuale, ovvero misure analoghe adottate da soggetti terzi durante il trattamento degli stessi da parte di AWS, quest’ultima informerà il Cliente senza indugio. AWS informerà prontamente tutte le parti coinvolte in tali procedimenti (ad esempio i creditori, il curatore fallimentare) in merito al fatto che i Dati del Cliente oggetto di tali procedimenti sono di proprietà del Cliente e responsabilità dello stesso, e che il Cliente può decidere in merito a tali Dati a sua totale ed esclusiva discrezione.</p> |
|---|---|

**16. Entire Agreement; Conflict.** This DPA incorporates the Standard Contractual Clauses by reference. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA. Nothing in this document varies or modifies the Standard Contractual Clauses. In case of conflict between the English version and the Italian version of this DPA, the Italian version shall prevail.

**17. Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:

**16. Intero accordo; Discrepanze.** Le Clausole Contrattuali Tipo (*Standard Contractual Clauses*) sono ricomprese nel presente DPA in virtù del richiamo operato alle stesse. Salvo ove modificato dal presente DPA, il Contratto rimarrà pienamente in vigore. Qualora emergano discrepanze tra il Contratto e il presente DPA, i termini di cui al presente DPA prevarranno, fatta eccezione per le Condizioni di Servizio, che prevarranno rispetto al presente DPA. Nessuna delle disposizioni di cui al presente documento altera o modifica le Clausole Contrattuali Tipo. Le Parti prendono atto che in caso di conflitto tra la versione inglese e la versione italiana di questo DPA, prevarrà la versione italiana.

**17. Definizioni.** Salvo ove diversamente definiti nel Contratto, tutti i termini con l'iniziale maiuscola utilizzati nel presente DPA avranno il significato agli stessi qui di seguito attribuito:

|   |  |
|---|--|
| <p><b>"Client Administrations"</b> the Administrations and/or other entities or legal entities receiving the services provided by Sogei, also through the Contract, and who could be qualified as Data Controllers.</p> <p><b>"AWS Network"</b> means AWS's data center facilities, servers, networking equipment, and host software systems (for example, virtual firewalls) that are within AWS's control and are used to provide the Services.</p> <p><b>"AWS Security Standards"</b> means the security standards attached to the Agreement, or if none are attached to the Agreement, attached to this DPA as Annex 1.</p> <p><b>"Controller"</b> means the natural or legal person, public authority, service or other body which, individually or together with others, determines the purposes and means of processing personal data, i.e. the Customer or the Client Administration.</p> <p><b>"Controller-to-Processor Clauses"</b> means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at <a href="https://d1.awsstatic.com/Controller_to_Processor_SCCs.pdf">https://d1.awsstatic.com/Controller to Processor SCCs.pdf</a>.</p> <p><b>"Customer Data"</b> means the "personal data" (as defined in the GDPR) that is uploaded to the Services under Customer's AWS accounts.</p> <p><b>"EEA"</b> means the European Economic Area.</p> <p><b>"GDPR"</b> means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).</p> <p><b>"Personal Data Protection Rules"</b>: the laws, regulations, and, in general, national and European rules, including soft law, applicable in relation to the processing and/or protection and security of personal data, as well as as amended from time to time, including, by way of example and not limited to, the GDPR, Legislative Decree 196/2003 as amended by the Italian adaptation legislation referred to in Legislative Decree 101/2018, circulars, opinions and directives of the national and community Supervisory Authorities as well as any other laws, rules or regulations applicable to each of the parties regarding the Protection of Personal Data.</p> <p><b>"Processing"</b> has the meaning given to it in the GDPR i.e. means any operation or set of operations performed with or without the aid of automated processes and applied to personal data or sets of personal data, such as the collection, registration, organisation, the structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, diffusion or any other form made available, comparison or interconnection, limitation, alignment or combination, cancellation or destruction and "process", "processes" and "processed" will be interpreted accordingly.</p> <p><b>"Processor"</b> means the natural or legal person, public authority, service or other body that processes personal data on behalf of the Data Controller.</p> <p><b>"Sub-Processor" or "Other Processor"</b>: the natural or legal person or other public or private body that processes personal data pursuant to a written agreement with the Data Processor. Sub-Processor may indicate AWS when the Customer acts as a</p> | <p><b>"Amministrazioni Clienti"</b> sono le Amministrazioni e/o altri enti o persone giuridiche destinatarie dei servizi erogati dal Cliente, anche attraverso il Contratto, e che potrebbero rivestire la qualifica di Titolari del Trattamento.</p> <p><b>"Rete AWS"</b> indica le strutture dati, i server, le attrezzature di rete, e i sistemi software per l'hosting (ad esempio firewall virtuali) che sono sotto il controllo di AWS e vengono utilizzati per fornire i Servizi.</p> <p><b>"Standard di Sicurezza AWS"</b> indica gli standard di sicurezza allegati al Contratto ovvero, qualora al Contratto non sia allegato nessuno standard di sicurezza, gli standard di sicurezza allegati al presente DPA <i>sub</i> Allegato 1.</p> <p><b>"Titolare del trattamento"</b> o <b>"Titolare"</b> indica la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali ovvero sia il Cliente o l'Amministrazione Cliente.</p> <p><b>"Clausole Titolare-Responsabile"</b> indica le clausole contrattuali tipo tra i titolari e i responsabili del trattamento in merito ai Trasferimenti dei Dati, approvate dalla Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021, e attualmente disponibili all'indirizzo <a href="https://d1.awsstatic.com/Controller_to_Processor_SCCs.pdf">https://d1.awsstatic.com/Controller to Processor SCCs.pdf</a>.</p> <p><b>"Dati del Cliente"</b> indica i "dati personali" (come definiti nel GDPR) caricati sui Servizi all'interno degli account AWS del Cliente.</p> <p><b>"EEA"</b> indica lo Spazio Economico Europeo.</p> <p><b>"GDPR" o "Regolamento"</b> indica il Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati).</p> <p><b>"Norme in materia di Protezione dei Dati Personali"</b>: le leggi, regolamenti, e, in generale, le norme nazionali ed europee, anche di soft law, applicabili in relazione al trattamento e/o alla protezione e alla sicurezza dei dati personali, così come modificate di volta in volta, ivi incluso, a titolo esemplificativo e non esaustivo, il GDPR, il D.Lgs. 196/2003 come novellato dalla normativa di adeguamento italiana di cui al D.Lgs. 101/2018, circolari, pareri e direttive dell'Autorità di Controllo nazionali e comunitarie nonché eventuali altre leggi, norme o regolamenti applicabili a ciascuna delle parti in materia di Protezione dei Dati Personali.</p> <p><b>"Trattamento"</b> ha il significato attribuito a tale termine nel GDPR, cioè indica qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o, qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, allineamento o combinazione, la cancellazione o la distruzione e "trattare", "tratta" e "trattato" saranno interpretati in maniera corrispondente.</p> <p><b>"Responsabile del trattamento" o "Responsabile"</b> indica la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.</p> <p><b>"Sub-Responsabile del trattamento" o "Sub-Responsabile" o "Altro Responsabile"</b>: la persona fisica o giuridica o altro organismo pubblico o privato che tratta dati personali in forza di un accordo scritto con il Responsabile del trattamento. Sub-Responsabile del trattamento può indicare AWS quando il</p> |
|---|--|

|  |  |
|--|--|
| <p>Data Processor on behalf of the Client Administration, i.e. the entity to whom AWS, when authorized by the Customer, has delegated the execution of specific Processing operations.</p> <p><b>“Processor-to-Processor Clauses”</b> means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at <a href="https://d1.awsstatic.com/Processor%20to%20Processor%20SCCs.pdf">https://d1.awsstatic.com/Processor to Processor SCCs.pdf</a>.</p> <p><b>“Data Breach”</b> means a breach of AWS security resulting in the accidental or unlawful destruction, loss, modification, unauthorized disclosure of, or unauthorized access to, Customer Data to the same.</p> <p><b>“Service Controls”</b> means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.</p> <p><b>“Standard Contractual Clauses”</b> means (i) the Controller-to-Processor Clauses, or (ii) the Processor-to-Processor Clauses, as applicable in accordance with Sections 12.2.1 and 12.2.2.</p> <p><b>“Third Country”</b> means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).</p> | <p>Cliente agisce in qualità di Responsabile del trattamento per conto dell'Amministrazione Cliente, ovvero il soggetto a cui il AWS, autorizzato dal Cliente, abbia delegato l'esecuzione di specifiche attività di Trattamento.</p> <p><b>“Clausole tra Responsabili”</b> indica le clausole contrattuali tipo tra i responsabili del trattamento in merito ai Trasferimenti dei Dati, approvate dalla Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021, e attualmente disponibili all'indirizzo <a href="https://d1.awsstatic.com/Processor%20to%20Processor%20SCCs.pdf">https://d1.awsstatic.com/Processor to Processor SCCs.pdf</a>.</p> <p><b>“Violazioni di dati personali” (o “data breach”)</b> indica una violazione della sicurezza di AWS che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei Dati del Cliente ovvero l'accesso non autorizzato agli stessi.</p> <p><b>“Controlli di Servizio”</b> indica i controlli, ivi comprese le caratteristiche e le funzionalità di sicurezza, fornite dai Servizi, secondo quanto illustrato nella Documentazione.</p> <p><b>“Clausole Contrattuali Tipo”</b> indica (i) le Clausole Titolare-Responsabile ovvero (ii) le Clausole tra Responsabili, ove applicabile in conformità agli Articoli 12.2.1 e 12.2.2.</p> <p><b>“Paese Terzo”</b> indica un paese non appartenente al SEE che, secondo la Commissione Europea, non offre un livello adeguato di protezione dei dati personali (come illustrato nel GDPR).</p> |
|--|--|

| <p><b>Annex 1</b></p> <p><b>AWS Security Standards</b></p>   | <p><b>Allegato 1</b></p> <p><b>Standard di Sicurezza di AWS</b></p>   |
|--|---|
| <p>Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.</p>   | <p>I termini con lettera iniziale maiuscola non altrimenti definiti nel presente documento hanno il significato loro attribuito nel Contratto.</p>  |
| <p><b>1. Information Security Program.</b> AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:</p> | <p><b>1. Programma per la sicurezza informatica.</b> AWS manterrà un programma per la sicurezza informatica (comprensivo di adozione e applicazione di regolamenti e procedure interni) sviluppato per (a) aiutare il Cliente al fine di garantire che non si verifichino perdite, accessi o divulgazioni accidentali o fraudolente dei Dati del Cliente, (b) identificare rischi interni ragionevolmente prevedibili rispetto a sicurezza e accessi non autorizzati al Network di AWS, e (c) contenere i rischi rispetto alla sicurezza, anche con test e valutazione del rischio periodici. AWS designerà uno o più dipendenti che coordineranno, ovvero saranno responsabili per, il programma per la sicurezza informatica. Il programma per la sicurezza informatica includerà le seguenti misure:</p> |
| <p><b>1.1 Network Security.</b> The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.</p>   | <p><b>1.1 Sicurezza del Network.</b> Il Network di AWS sarà elettronicamente accessibile ai dipendenti, appaltatori, ovvero a chiunque ne abbia bisogno per prestare i Servizi. AWS manterrà controlli e regolamenti relativi all'accesso per gestire gli accessi autorizzati al Network di AWS di ciascun utente e di ciascuna connessione al network, anche per quanto riguarda l'utilizzo di firewall e sistemi e procedure di autenticazione funzionalmente equivalenti. AWS implementerà interventi correttivi e piani di <i>incident response</i> per risolvere possibili minacce alla sicurezza.</p>   |
| <p><b>1.2 Physical Security</b></p> <p><b>1.2.1 Physical Access Controls.</b> Physical components of the AWS Network are housed in nondescript facilities (the “Facilities”). Physical barrier controls are used to prevent unauthorised entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (for example, card access systems, etc.) or validation by</p>  | <p><b>1.2 Sicurezza fisica</b></p> <p><b>1.2.1 Controlli degli Accessi Fisici.</b> Le componenti tangibili del Network di AWS sono ospitate presso strutture prive di contrassegni particolari (di seguito “Strutture”). Sono stati implementati punti di controllo con barriere fisiche per impedire accessi non autorizzati alle Strutture, sia per quanto riguarda il perimetro esterno sia per quanto riguarda i punti di accesso a ciascun edificio. Per superare le barriere fisiche delle Strutture</p>  |

|   |  |
|---|--|
| <p>human security personnel (for example, contract or in-house security guard service, receptionist, etc.). Employees and certain contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorised employees or contractors while visiting the Facilities.</p>  | <p>è necessaria un'autenticazione elettronica all'ingresso (ad esempio sistemi di accesso tramite scheda elettronica, ecc.) o un'autenticazione da parte dello staff addetto alla sicurezza (ad esempio custodi o addetti alla reception in-house o a contratto, ecc.). Ai dipendenti e a determinati appaltatori verrà consegnato un cartellino identificativo munito di foto che gli stessi dovranno indossare quando si trovano all'interno di qualsiasi Struttura. I visitatori e i gli altri appaltatori dovranno essere registrati dal personale incaricato, dovranno presentare documenti di identità adeguati e riceveranno un cartellino identificativo per i visitatori, che dovranno indossare per tutto il tempo in cui si trovano presso qualsiasi Struttura, e durante la visita alla Struttura saranno costantemente accompagnati dai dipendenti o appaltatori autorizzati.</p>                                       |
| <p><b>1.2.2 Limited Employee and Contractor Access.</b> AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates</p>  | <p><b>1.2.2 Accesso Limitato dei Dipendenti e degli Appaltatori.</b> AWS permette l'accesso alle Strutture a quei dipendenti e appaltatori che abbiano una legittima necessità aziendale per tali privilegi di accesso. Nel momento in cui un dato dipendente o appaltatore cessa di avere una necessità aziendale per i privilegi di accesso che gli erano stati accordati, gli stessi privilegi verranno immediatamente revocati, anche nel caso in cui il dipendente o appaltatore continui ad essere impiegato da AWS o dalle affiliate di quest'ultima.</p>   |
| <p><b>1.2.3 Physical Security Protections.</b> All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorised access to the Facilities, including monitoring points of vulnerability (for example, primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.</p> | <p><b>1.2.3 Protezioni di Sicurezza Fisica.</b> Tutti i punti di accesso (escluse le porte principali) vengono tenuti chiusi (a chiave). I punti di accesso alle Strutture sono monitorati da telecamere di videosorveglianza volte a registrare tutti gli individui che accedono alle Strutture. AWS ha inoltre implementato sistemi per la rilevazione di intrusi che sono tesi a individuare accessi non autorizzati alle Strutture, inclusi il monitoraggio dei punti vulnerabili (ad esempio porte principali, uscite di emergenza, botole del tetto, portelloni di attracco e scarico dei veicoli, ecc.) con contatti sulla porta, sensori di vetri infranti, rilevamento movimenti interni, e altri dispositivi progettati per rilevare tentativi di accesso alle Strutture. Tutti gli accessi fisici alle Strutture da parte dei dipendenti e degli appaltatori vengono registrati e regolarmente sottoposti a verifica.</p> |
| <p><b>2. Continued Evaluation.</b> AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.</p>   | <p><b>2. Valutazione continua.</b> AWS sottoporrà periodicamente a revisione la sicurezza del Network di AWS e l'adeguatezza del proprio programma per la sicurezza informatica, confrontandoli con gli standard di sicurezza del settore e i propri regolamenti e procedure. AWS valuterà costantemente la sicurezza del Network di AWS e dei Servizi collegati, al fine di stabilire se si rendano necessarie ulteriori o diverse misure di sicurezza per rispondere a nuovi rischi o circostanze rilevati nel corso delle verifiche periodiche.</p>   |

---



---



---



---



---