



SERVIZI CLOUD AWS PER SOGEI

CAPITOLATO TECNICO



Sommario

1. GLOSSARIO	3
2. CONTESTO	5
2.1. Strategia di evoluzione	7
3. OGGETTO E DURATA	10
3.1. Oggetto	10
3.2. Massimale e Durata	19
4. RESPONSABILE DELLA FORNITURA	20
5. MODALITÀ DI UTILIZZO DEI SERVIZI	20
5.1. Requisiti di qualificazione dei servizi e delle infrastrutture cloud	22
5.2. Requisiti DNSH	23
5.3. Piattaforma elettronica e disponibilità dei servizi	23
5.4. Livelli di servizio e Crediti di Servizio	23
5.5. Gestione delle Utenze AWS	24
5.6. Disciplina servizi	25
5.7. Aggiornamento dell'Elenco dei Servizi	25
6. NOTIFICHE	26
7. VERIFICA DI CONFORMITÀ	26
8. EXIT STRATEGY E GRACE PERIOD	27



1. GLOSSARIO

Account AWS Enterprise	Qualsiasi account AWS inserito nell'Elenco Email Account AWS Enterprise, che può essere periodicamente aggiornato, usando un indirizzo email (con un dominio di proprietà di Sogei), riportante la denominazione legale per esteso del Cliente nel campo "Denominazione Sociale" associato all'account AWS in questione, e ad una posizione geografica che corrisponde a una Parte Contraente AWS che abbia aderito al presente Contratto.
Amministrazione o Committente o Cliente	Sogei (Società Generale d'Informatica S.p.A.).
"API" (application program interface)	Indica l'interfaccia applicativa di un programma.
Assistenza	Supporto da parte di risorse professionali del fornitore, nell'ambito delle verifiche di conformità e di assistenza agli utenti nell'ordinaria erogazione dei servizi
Attività	Quota parte di un servizio contrattuale, omogenea, per tipologia, alla quale si applica una ben definita modalità di esecuzione.
Cloud	Il NIST (National Institute of Standard and Technology) definisce il cloud come un modello per abilitare, tramite la rete, l'accesso diffuso, agevole e a richiesta, ad un insieme condiviso e configurabile di risorse di elaborazione (ad esempio reti, server, memoria, applicazioni e servizi) che possono essere acquisite e rilasciate rapidamente e con minimo sforzo di gestione o di interazione con il fornitore di servizi.
Consip	La società che, in qualità di stazione appaltante della presente fornitura, affida la fornitura oggetto del presente Capitolato.
Container	Si tratta di ambienti runtime leggeri che forniscono le applicazioni con i file, le variabili e le librerie indispensabili per l'esecuzione dei servizi applicativi. Le macchine virtuali tradizionali (VM) consentono la virtualizzazione dell'infrastruttura informatica, mentre i container rendono possibile quella delle applicazioni software. A differenza delle macchine virtuali, i container utilizzano il sistema operativo (SO) dell'host, anziché fornire il proprio.
Contenuti del Cliente	I Contenuti che il Cliente o qualsiasi Utente Finale trasferiscono a AWS per finalità di trattamento, archiviazione o hosting nell'ambito dei Servizi, in relazione a un Account AWS Enterprise e qualsiasi risultato computazionale ottenuto da quanto sopra dal Cliente o da qualsiasi Utente Finale tramite l'utilizzo dei Servizi. I Contenuti del Cliente includono, per esempio, i Contenuti archiviati su Amazon Simple Storage Service dal Cliente o da qualsiasi Utente Finale. I Contenuti del



	Cliente non includono le Informazioni sull'Account.
Distributed Cloud	Offerta dei principali hyperscaler cloud per installare, sul Data Center del Cliente, le proprie soluzioni evolute di servizi cloud, sebbene con funzionalità, in genere, ridotte, (che vengono quindi erogate on-premises al cliente). A volte sono chiamate anche soluzioni @customer.
Documentazione	I manuali per gli utenti e per gli amministratori dei Servizi (in entrambi i casi esclusi i contenuti a cui si fa riferimento tramite collegamento ipertestuale), disponibili alla pagina http://aws.amazon.com/documentation (ovvero altri indirizzi subentranti o collegati indicati da AWS), come periodicamente aggiornati da AWS).
Fornitura	Il complesso dei servizi IaaS e PaaS offerti e le attività incluse nei Servizi e descritti nel presente documento tecnico.
Green Field	Area Tecnica da cui parte la costituzione di un'infrastruttura IT, senza vincoli con l'ambiente e le tecnologie preesistenti. La progettazione e la sua implementazione non risente di conseguenza di vincoli e stratificazioni tecniche esistenti e può essere fatta con principi innovativi ed usando tecnologie best of breed.
Hybrid Multicloud	Configurazione di servizi Cloud che uniscono servizi Private e Public ed in particolare quelli Public sono di diversi provider
Hyperscaler	Quelle società di dimensioni massive come Google, Microsoft, and Amazon (ma anche Oracle IBM, Facebook o Alibaba) che sostengono fortissimi investimenti non solo per dominare il mercato Public Cloud con continui sviluppi, nuove capacità, nuovi data center, ma per usare il cloud anche come strumento di espansione del loro business 'più verticale'
Impresa o Fornitore	La società affidataria della presente procedura
Private Cloud	Rappresenta un modello di deployment su cloud, on demand, in cui i servizi e l'infrastruttura di cloud computing sono in hosting in un ambiente privato (data center o rete Intranet aziendale) e utilizzano risorse proprietarie.
Public Cloud	E' un modello di deployment su cloud in cui le risorse di elaborazione sono di proprietà di un provider (che si occupa anche della gestione) e vengono condivise tra più tenant tramite Internet.
Regolamento sugli Usi Autorizzati	Il regolamento pubblicato alla pagina http://aws.amazon.com/aup (ovvero altri indirizzi subentranti o collegati indicati da AWS), come periodicamente aggiornato da AWS.
Responsabile della Fornitura	La persona individuata dall'Impresa come interlocutore di Sogei e responsabile di tutte le attività contrattuali.



Servizio	Ciascuno dei servizi resi disponibili da AWS o dalle Affiliate di quest'ultima (sempre nel rispetto del vincolo di esclusiva) e per i quali il Cliente si registra dal Sito di AWS (ovvero tramite altro canale messo a disposizione da AWS), inclusi i servizi web descritti nei Termini del Servizio. I Servizi non includono i Contenuti di Terzi.
Service Credits	Crediti maturati in favore di Sogei a fronte di disservizi verificati in sede di verifica di conformità negativa e successivamente quantificati e che possono essere compensati da Sogei secondo le modalità indicate nel Contratto.
Services Level Agreement (SLA)	Tutti i contratti sul livello di servizio offerti da AWS relativi ai Servizi e pubblicati sul Sito di AWS, come periodicamente aggiornati da AWS. Gli accordi sul livello di servizio offerti da AWS relativamente ai Servizi sono disponibili alla pagina https://aws.amazon.com/legal/service-level-agreements (ovvero altri indirizzi subentranti o collegati specificati da AWS), come periodicamente aggiornati da AWS.
Standard di Sicurezza di AWS	Gli standard di sicurezza allegati al presente Capitolato come Allegato 2.1 .
Software Defined	Si definisce Software Define un'infrastruttura costituita da risorse di elaborazione, rete e storage completamente virtualizzate e riunite in pool, in modo logico, che possono essere gestite come fossero software.
Utente Finale	Qualsiasi individuo o ente che direttamente o indirettamente tramite un altro utente (a) acceda ai, ovvero utilizzi i, Contenuti del Cliente, oppure (b) altrimenti acceda ai, ovvero utilizzi, i Servizi Offerti da un Account AWS Enterprise. Il termine "Utente Finale" non include quegli individui e quegli enti che accedono ai, ovvero utilizzano i, Servizi o altri Contenuti dal proprio account AWS personale, e non da un Account AWS Enterprise.

2. CONTESTO

Sogei ha introdotto, da diversi anni, tecnologie cloud infrastrutturali e di automazione del proprio Data Center, ma solo più recentemente ha sviluppato architetture pienamente orientate ai principali modelli, applicativi ed infrastrutturali, del cloud, quali “container” e sviluppi a “micro servizi”.

L'adozione del Public Cloud, in Sogei, si sta quindi velocemente sviluppando essendo però ancora limitata ad alcuni ambiti, anche se ha avuto una sicura accelerazione, nell'ultimo triennio, grazie soprattutto all'uso di metodologie di collaborazione in cloud, allo sviluppo di soluzioni CRM basate sul SaaS o a forme di gestione totalmente in cloud, come quella in favore della Corte dei Conti.



La recente situazione pandemica ed il supporto che Sogei dovuto dare allo sviluppo di soluzioni per fronteggiare l'emergenza (i.e. Piattaforma Gestione Emergenza Covid) hanno dimostrato come la strada intrapresa dell'uso di piattaforme integrate in cloud, sia quella corretta anche grazie al fatto di come queste rendano possibili tempi progettuali notevolmente ridotti, rispetto agli approcci tradizionali.

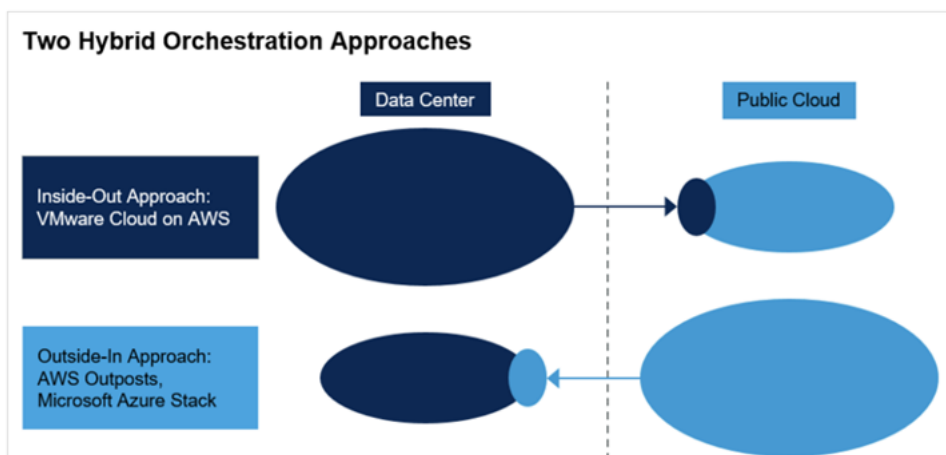
Lo scenario si completa tenendo conto che **le soluzioni di Private Cloud** in dotazione al Data Center, si stanno rapidamente evolvendo, grazie ad un approccio Green Field implementato con riferimento alle moderne tecnologie Software Defined.

La situazione, ad oggi, è pertanto quella che usualmente viene definita **Hybrid IT piuttosto che Hybrid Cloud**; questo scenario è molto frequente per quelle aziende, come Sogei, che non possono abbandonare, radicalmente e nel breve termine, le tecnologie e i sistemi esistenti, a favore di una completa migrazione al Public Cloud.

Infatti, i vincoli legati alle normative ed alla localizzazione dei dati e la necessaria integrazione con sistemi esistenti portano spesso alla equilibrata **combinazione tra architetture orientate al private-cloud e altre ispirate al paradigma del cloud pubblico**.

In questo contesto - come mostra la **Figura 1** - l'unico approccio praticabile è quello c.d. **Inside-Out** che non consente di beneficiare, a pieno, dei vantaggi dei servizi IaaS PaaS, messi a disposizione dai Cloud Providers, equivalente all'approccio c.d. **Outside-In**.

Figura 1





A tale riguardo, il precedente Piano Triennale Sogei è stato incentrato su un profondo processo di analisi e riprogettazione, finalizzato alla realizzazione di un nuovo modello di Data Center, di cui il nuovo Piano definisce le linee di sviluppo e di realizzazione operativa, per il prossimo triennio.

2.1. Strategia di evoluzione

Il piano Triennale Sogei 21-23, si propone di introdurre una profonda trasformazione dell'offerta Sogei, tesa alla realizzazione di uno scenario strategico denominato **"Digital Assets Manager"** e/o **"Platform Company"**. Sogei, oltre a continuare a fornire, **a scopo tattico**, Applicazioni per l'utente finale (APP), **come obiettivo strategico**, dovrà diventare Creatore e Gestore di Business-Specific Assets (BSA) e Business-Independent Capabilities (BIC), per conto dei Clienti.

Basilare, a tal fine, è la decisa spinta alla **trasformazione del Data Center Sogei in un Hybrid MultiCloud Data Center**.

Quattro sono i pillar su cui si deve fondare questa trasformazione:

- **creazione di un Private Cloud green field**, come base dell'evoluzione di tutti i servizi erogati nel Data Center Sogei ed abilitato da tecnologie Software Defined, studiate e sperimentate nel precedente piano industriale;
- **messa a disposizione di soluzioni di "Distributed Public Cloud" dei principali Cloud Service Provider (CSP)**, come acceleratore dello sviluppo di servizi a valore aggiunto, anche in attesa di valutare i requisiti sulla strategicità di ciascun servizio e della necessità di dover mantenere o meno i dati presso un Data Center della Pubblica Amministrazione;
- **messa a disposizione di "Contratti di Public Cloud", possibilmente, stipulati direttamente con i soggetti erogatori**, stante la strategicità dei servizi richiesti da Sogei (ed erogati ai propri clienti) che, indubbiamente, richiedono particolari SLA, oltre alla necessità di avere rapporti diretti con i laboratori di sviluppo, anche al fine di poter condividere strategie evolutive sui servizi dei provider e per evitare tutte le limitazioni indotte dagli accordi tra alcuni cloud provider ed i propri partner.
- **estensione e completamento dell'automazione per le modalità di release management Dev/ops** basate su Container che si appoggiano appunto completamente su un'infrastruttura cloud ibrida.

Questi pillar rappresentano i fondamenti di un utilizzo efficace delle tecnologie Cloud allo scopo di:

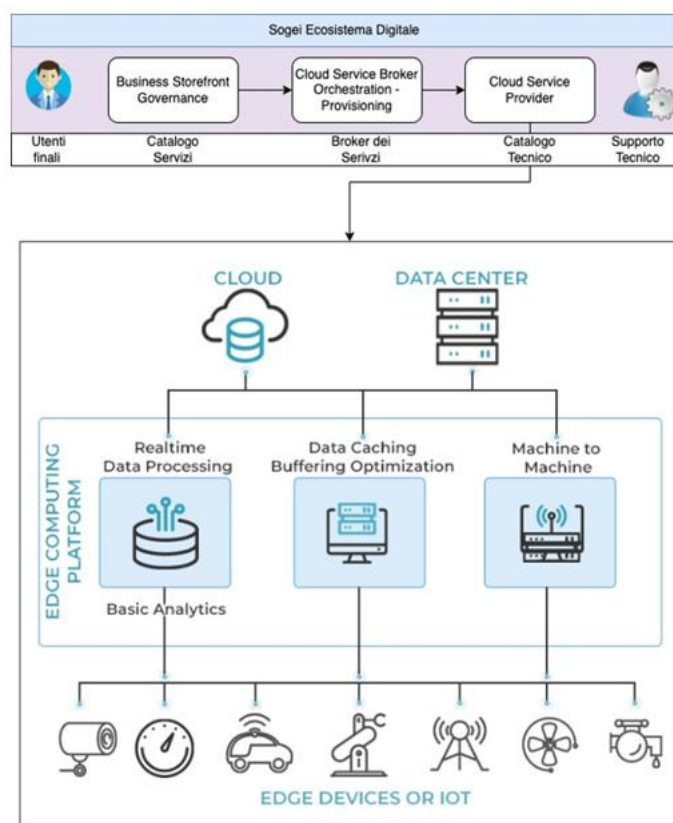
1. Aumentare automazione ed efficienza operativa nell'attuale Data Center Sogei;
2. Velocizzare il "time to market" nello sviluppo di nuove soluzioni per i clienti;



3. Perseguire un obiettivo di economia di scala e di “riuso” degli investimenti tecnologici su scenari di applicazione differenti.

Il punto di arrivo dovrà quindi essere **un ecosistema digitale** – vedi **Figura 2** - dove la domanda interna (Sogei) ed esterna (Clienti) di soluzioni tecnologiche possa essere soddisfatta velocemente con soluzioni comuni declinate al meglio, a seconda dello scenario di applicazione.

FIGURA 2



Il modello strategico ibrido cui tenderà Sogei potrà percorrere, a fronte della disponibilità di soluzioni tecnologiche on-prem o on-cloud, tutte le varie possibilità presenti nello spettro dell’offerta, da privato a pubblico:

- private IaaS;
- private IaaS/PaaS (container);
- modello inside out (es. vmware on AWS);



- distributed cloud (es. AWS outposts);
- edge computing (es. per requisiti di specifici settori)
- public cloud encrypted (o Secure Public Cloud);
- (public cloud region gov) in funzione di eventuali accordi strategici;
- public cloud generico.

Attualmente Sogei utilizza i servizi AWS per alcuni obiettivi di sviluppo della Corte dei conti (DataLake) e della Presidenza del Consiglio dei Ministri (Transizione Digitale e PNRR). I servizi configurati per la Presidenza del Consiglio dei Ministri utilizzano infrastrutture nel Cloud Amazon AWS per la connettività (Virtual Network, VPN Gateway, Ip Pubblici, Network Security Group), per il calcolo (Virtual Machine per Application Server e DB) e per la logica applicativa (API Gateway, Elastic Beanstalk, SQL Managed Instance). Per la Corte dei conti, invece, il focus è orientato su API Mgmt e MongoDB. Pertanto, il cloud AWS costituisce l'ambiente di riferimento per l'esecuzione di importanti interventi di trasformazione di alcune Amministrazioni e la cui continuità dei servizi costituisce un requisito fondamentale per lo sviluppo e per il raggiungimento degli obiettivi della transizione, compatibilmente alla pianificazione stabilita. Risulta quindi indispensabile garantire la continuità di tali servizi oppure pianificarne l'eventuale sostituzione, nell'ambito dello scenario multicloud ipotizzato.

Gli articoli che, nell'ambito della presente iniziativa, saranno oggetto di acquisto verranno pertanto definiti e selezionati, **primariamente, in base agli specifici criteri del contesto tecnologico di riferimento** (Transizione al Digitale della Presidenza del Consiglio dei Ministri, DataLake di Corte dei conti), e, **successivamente, in funzione dell'eventuale migrazione di altri Workload nel Cloud AWS**, in coerenza con le strategie di transizione verso un Hybrid Multicloud Data center, che Sogei, di volta in volta, adotterà.



3. OGGETTO E DURATA

3.1. Oggetto

Nel presente Capitolato verranno descritte le modalità di acquisizione e di delivery dei servizi erogati nel cloud AWS, in maniera funzionale alla strategia Sogei, tesa a portare avanti, progressivamente, il suo progetto di Hybrid Multicloud Data center, assicurando – fino a che sia ritenuto necessario - il suo mantenimento del dato on-prem, e semplificando, pertanto, la scelta della tipologia di cloud e di servizio da utilizzare, potendola basare su mere considerazioni tecniche. Inoltre, la previsione di un listino, sottoposto a periodici aggiornamenti tecnologici, consentirà a Sogei di non vincolarsi a soluzioni che, ad un certo momento della vita contrattuale, non risultino più ‘attuali’, rispetto alla rapidissima evoluzione dell’offerta, nel mercato cloud computing.

La selezione del catalogo dei servizi IaaS e PaaS (dei listini AWS), incluse nella presente iniziativa, è stata effettuata in conseguenza di una preliminare classificazione delle **MACROCATEGORIE di servizi potenzialmente utilizzabili, nel contesto Sogei**, come indicate, nella **Tabella 1**.

TABELLA 1 - CATALOGO DEI SERVIZI	
Macrocategorie	Descrizione
Compute	<i>Istanze di macchine virtuali, servizi gestiti per l'orchestrazione di container e container registry. Servizi di "Function As A Service" di cloud ibrido e servizi gestiti per il deployment di applicazioni con orchestrazione dell'infrastruttura sottostante. HW/SW per la realizzazione di infrastrutture ibride per l'erogazione di servizi con vincoli di sovranità, residenza dei dati a riposo, bassa latenza del trasferimento dei dati e prossimità con device mobili connessi con reti 4G/5G.</i>
Storage	<i>Servizi gestiti di object storage, block storage e file storage con supporto di protocolli SMB e NFS. Servizi per la creazione e automazione di Disaster Recovery per workload on-premises e in cloud.</i>
Database	<i>Servizi gestiti di database relazionali con engine commerciali ed Open Source. Servizi gestiti di Database NoSQL almeno di tipo Key Value e Document. Servizi di Data Warehouse gestito.</i>
Security, Identity & Compliance	<i>Servizi gestiti di Identity e Access Management, single sign-on, auditing, threat detection, Network e Web Application firewall, encryption dei dati con custodia offline delle chiavi private, PKI/HSM, Gestione dei certificati SSL</i>



TABELLA 1 - CATALOGO DEI SERVIZI	
Macrocategorie	Descrizione
AI & Machine Learning	<i>Servizi gestiti per il riconoscimento di immagini, text to speech, speech to text, traduzione, chatbot, gestione del ciclo di vita dei modelli di ML.</i>
Management & Governance	<i>Servizi per il deployment di landing zone, infrastructure as code, monitoring e gestione dei log, servizi centralizzati di system management.</i>
Developer Tools	<i>Servizi per la gestione del ciclo del software in modalità DevOps e toolkit SDK per l'integrazione del proprio software con i servizi cloud, monitoring a livello applicativo</i>
Migration & Transfer	<i>Servizi per il discovery di workload applicativi e servizi e tool di migrazione per virtual machine, file storage e database</i>
Networking & Content Delivery	<i>Servizi gestiti per la creazione e la gestione di API. Servizi gestiti di network e application load balancer, DNS, VPN e connettività dedicata.</i>
Media Services	<i>Servizi gestiti per il trasporto, la conversione, il packaging e il delivery di contenuti video.</i>
Internet of Things (IoT)	<i>Servizi per la gestione centralizzata e la protezione di dispositivi IoT ed il collezionamento dei dati.</i>
Front-End Web & Mobile	<i>Servizi per lo sviluppo e il deployment di Applicazioni Web e Mobile che si avvalgono di servizi cloud. Servizi gestiti per l'invio e la ricezione di notifiche destinate a device mobili. Servizi per la sincronizzazione dei dati tra sorgenti multiple di App per dispositivi mobili</i>
Analytics	<i>Servizi gestiti per l'Analisi dei dati e la creazione e gestione di data lake, ETL, DWH e business intelligence.</i>
Application Integration	<i>Servizi gestiti per l'integrazione e il disaccoppiamento di workload applicativi quali la gestione di code di messaggi, notifiche, workflow, bus di eventi. (dovrebbe essere la categoria Integration di Microsoft ad esempio).</i>
Customer Enablement Services	<i>Sono i servizi, presenti a listino e di supporto.</i>

A ciò ha fatto seguito la concreta individuazione, nell'ambito dei cataloghi AWS, dei servizi che Sogei ha ritenuto di specifico interesse, in maniera indicativa, ma non esaustiva, con riferimento ai pattern di sviluppo attualmente in essere e a quelli di futura, probabile, adozione:

TABELLA 2 - CATALOGO DEI SERVIZI RIFERITO AD AWS	
Macrocategorie	Servizi AWS
Compute	Amazon EC2



TABELLA 2 - CATALOGO DEI SERVIZI RIFERITO AD AWS	
Macrocategorie	Servizi AWS
	AWS App Runner
	AWS Batch*
	AWS Elastic Beanstalk
	Amazon EC2 Image Builder*
	AWS End-of-Support Migration Program (EMP) for Windows Server*
	AWS Lambda
	Amazon Lightsail
	AWS Outposts
	AWS ParallelCluster*
	AWS Serverless Application Model (AWS SAM)*
	AWS Serverless Application Repository*
	AWS Wavelength
	Amazon ECR
	Amazon ECS
	Amazon EKS
	AWS App2Container*
	ROSA on AWS
Storage	Amazon S3
	AWS Backup
	Amazon EBS
	Amazon EFS
	AWS Elastic Disaster Recovery
	AmazonFSx
	Amazon S3 Glacier
	AWS Snow Family
	AWS Storage Gateway
Database	Amazon Aurora
	Amazon DocumentDB
	Amazon DynamoDB
	Amazon ElastiCache
	Amazon Keyspaces
	Amazon MemoryDB



TABELLA 2 - CATALOGO DEI SERVIZI RIFERITO AD AWS	
Macrocategorie	Servizi AWS
	Amazon Neptune
	Amazon QLDB
	Amazon RDS
	Amazon Redshift
	Amazon Timestream
Security, Identity & Compliance	AWS Identity & Access Management (IAM)
	AWS Artifact*
	AWS Audit Manager
	Amazon Cognito
	Amazon Detective
	AWS Directory Service
	AWS Firewall Manager
	Amazon Cloud Directory
	Amazon GuardDuty
	Amazon Inspector
	Amazon Macie
	AWS Network Firewall
	AWS Resource Access Manager (AWS RAM)*
	AWS Secrets Manager
	AWS Security Hub
	AWS Shield
	AWS IAM Identity Center*
	AWS WAF
	Amazon Managed Blockchain
	AWS CloudHSM
	AWS Key Management Service (AWS KMS)
	AWS Certificate Manager
	AWS Certificate Manager Private Certificate Authority
	AWS Signer*
AI & Machine Learning	Amazon SageMaker
	Amazon Augmented AI (A2I)
	Amazon CodeGuru



TABELLA 2 - CATALOGO DEI SERVIZI RIFERITO AD AWS

Macrocategorie	Servizi AWS
	Amazon Comprehend
	Amazon Comprehend Medical
	Amazon DevOps Guru
	Amazon Elastic Inference
	Amazon Forecast
	Amazon Fraud Detector
	Amazon HealthLake
	Amazon Kendra
	Amazon Lex
	Amazon Lookout for Equipment
	Amazon Lookout for Metrics
	Amazon Lookout for Vision
	Amazon Monitron
	AWS Panorama
	Amazon Personalize
	Amazon Polly
	Amazon Rekognition
	Amazon Textract
	Amazon Translate
	Amazon Transcribe
	AWS Deep Learning AMIs*
	AWS Deep Learning Containers
	AWS DeepComposer
	AWS DeepLens
	AWS DeepRacer
	AWS Apache MXNet*
Management & Governance	AWS Account Management*
	AWS AppConfig
	AWS Auto Scaling*
	AWS Backint Agent*
	AWS Chatbot*
	AWS CloudFormation



TABELLA 2 - CATALOGO DEI SERVIZI RIFERITO AD AWS	
Macrocategorie	Servizi AWS
	AWS CloudTrail
	Amazon CloudWatch
	AWS Command Line Interface (AWS CLI)*
	AWS Compute Optimizer
	AWS Config
	AWS Console Mobile Application*
	AWS Control Tower
	Amazon Data Lifecycle Manager
	AWS Health*
	AWSLaunch Wizard*
	AWS License Manager
	Amazon Managed Grafana
	Amazon Managed Service for Prometheus
	AWS Management Console*
	AWS OpsWorks
	AWS Organizations*
	AWS Proton*
	AWS Resilience Hub
	AWS Resource Groups*
	AWS Service Catalog
	AWS Service Quotas*
	AWS Systems Manager
	AWS Tag Editor*
	AWS Tools for PowerShell*
	AWS Trusted Advisor*
	AWS Well-Architected Tool*
Developer Tools	AWS Cloud9
	AWS Cloud Control API*
	AWS CloudShell*
	AWS CodeArtifact
	AWS CodeBuild
	AWS CodeCommit



TABELLA 2 - CATALOGO DEI SERVIZI RIFERITO AD AWS	
Macrocategorie	Servizi AWS
	AWS CodeDeploy
	AWS CodePipeline
	AWS CodeStar
	AWS Fault Injection Simulator
	AWS Microservice Extractor for .NET*
	Porting Assistant for .NET*
	AWS Tools & SDKs*
	AWS X-Ray
Migration & Transfer	AWS Application Discovery Service*
	AWS Application Migration Service
	AWS Database Migration Service
	AWS DataSync
	AWS Mainframe Modernization (Preview)
	AWS Migration Hub
	AWS Schema Conversion Tool
	AWS Transfer Family
Networking & Content Delivery	Amazon API Gateway
	AWS App Mesh
	AWS Cloud Map
	Amazon CloudFront
	AWS Direct Connect
	Elastic Load Balancing
	AWS Global Accelerator
	Amazon Route 53
	Amazon VPC
	AWS VPN
Media Services	Amazon Elastic Transcoder
	Amazon Interactive Video Service
	Amazon Nimble Studio
Internet of Things (IoT)	AWS IoT Core
	FreeRTOS*
	AWS IoT Analytics



TABELLA 2 - CATALOGO DEI SERVIZI RIFERITO AD AWS	
Macrocategorie	Servizi AWS
	AWS IoT Device Defender
	AWS IoT Device Management
	AWS IoT Events
	AWS IoT ExpressLink (Preview)
	AWS IoT FleetWise (Preview)
	AWS IoT Greengrass
	AWS IoT RoboRunner (Preview)
	AWS IoT SiteWise
	AWS IoT Things Graph
	AWS IoT TwinMaker
	AWS IoT 1-Click
Front-End Web & Mobile	AWS Amplify
	Amplify Android (AWS Mobile SDK for Android)
	Amplify iOS (AWS Mobile SDK for iOS)
	AWS AppSync
	AWS Device Farm
	Amazon Location Service
	AWS Mobile SDK for Unity*
	AWS Mobile SDK for .NET and Xamarin*
	Amazon Pinpoint
	Amazon SNS
Analytics	Amazon AppFlow
	Amazon Athena
	Amazon CloudSearch
	AWS Data Exchange
	AWS Data Pipeline
	Amazon OpenSearch Service
	Amazon EMR
	Amazon FinSpace
	AWS Glue
	Amazon Kinesis
	AWS Lake Formation



TABELLA 2 - CATALOGO DEI SERVIZI RIFERITO AD AWS	
Macrocategorie	Servizi AWS
	Amazon MSK
	Amazon QuickSight
	Amazon Redshift
Application Integration	Amazon EventBridge
	Amazon Managed Workflows for Apache Airflow
	Amazon MQ
	Amazon SNS
	Amazon SQS
	AWS Step Functions
	Amazon SWF
Customer Enablement Services	AWS Managed Services
	AWS Support
	Amazon Connect

*Consiste in una funzionalità accessoria gratuita non suscettibile di qualificazione.

Servizi AWS “Trasversali” per cui è richiesta una configurazione speciale

Stante la particolare strategicità delle attività svolte da Sogei, è richiesta ad AWS, oltre alla possibilità di beneficiare di rapporti diretti con i laboratori di sviluppo, al fine di poter condividere strategie evolutive sui servizi, la disponibilità, su alcuni servizi denominati ‘trasversali’ (in quanto interagiscono con tutti gli altri, valorizzandoli), di una configurazione speciale, superiore a quella standard, come illustrato nella seguente tabella.

TABELLA 3 - CATALOGO DEI SERVIZI TRASVERSALI			
Nome Servizio	Configurazione speciale	Valore Standard	Valore richiesto da Sogei
AWS Key Management Service (KMS)	Numero Massimo di Customer managed keys per AWS account e Region	10.000	500.000
	Ciascun customer managed key può avere fino a un massimo di 50,000 grants	50.000	100.000



TABELLA 3 - CATALOGO DEI SERVIZI TRASVERSALI			
Nome Servizio	Configurazione speciale	Valore Standard	Valore richiesto da Sogei
AWS Outposts	SLA per la disponibilità del servizio AWS Outposts	N/A	99.99%
Amazon CloudWatch	Numero massimo di richieste, applicabili a Custom Metrics e PutMetricData API Calls, che possono essere effettuate al secondo per AWS account e Region	500	5.000
	Accesso anticipato (Beta e Preview) a tutti i servizi di tipo "Observability"	Accesso solo a servizi GA	Accesso Anticipato
AWS Enterprise Support*	Numero massimo di operazioni AWS Support API per secondo	5	20
	Numero massimo di operazioni AWS Trusted Advisory API per secondo. Il servizio AWS Support abilita la scrittura di applicazioni che interagiscono con AWS Trusted Advisor	100	150
	Numero massimo di AWS Support case che possono essere creati (per ora)	10	20

*Consiste in una funzionalità accessoria gratuita non suscettibile di qualificazione.

3.2. Massimale e Durata

L'ammontare massimo dei servizi acquisibili, nel corso della durata contrattuale, è pari a **20.000.000,00€**.

La durata contrattuale prevista è di **36 mesi**, a partire dalla stipula.

Si precisa che tale dimensionamento massimo è stimato al meglio delle conoscenze attuali, e che si intende pertanto non vincolante, riservandosi Sogei di:

- 1) non attivare i servizi;
- 2) attivare i servizi in misura minore rispetto a quanto riportato.

secondo i limiti e le condizioni previste nello Schema di Contratto.



4. RESPONSABILE DELLA FORNITURA

Prima della stipula, l'Impresa dovrà comunicare il nominativo del proprio rappresentante designato quale **Responsabile della fornitura** (o Responsabile del Fornitore per le attività contrattuali). In particolare, tale responsabile sarà, per gli aspetti amministrativi e contrattuali, l'interlocutore unico di Sogei.

Sarà cura del Responsabile della fornitura verificare il rispetto di tutti gli adempimenti contrattuali. Tale referente non dovrà comportare alcun onere aggiuntivo per la Committente.

Il Responsabile della fornitura dovrà essere reperibile telefonicamente e partecipare alle riunioni su richiesta della Committente con un preavviso massimo di **3 giorni lavorativi**.

Il Responsabile della fornitura non farà parte di alcuno dei gruppi di lavoro relativi ai servizi oggetto della fornitura.

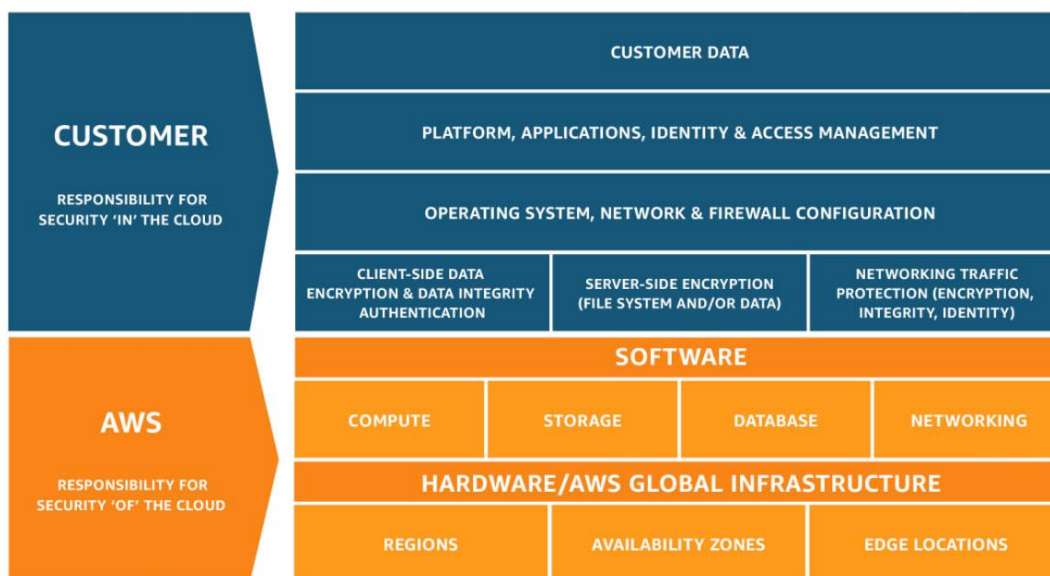
5. MODALITA' DEI SERVIZI

La sicurezza e la conformità dei servizi offerti sono una responsabilità condivisa tra AWS e Sogei, ciascuno secondo la propria competenza e nel rispetto dei ruoli di fornitore e cliente.

AWS si impegna ad azionare, gestire e controllare i componenti dal sistema operativo host e il livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui il servizio opera. AWS si occupa di proteggere l'infrastruttura globale su cui vengono eseguiti tutti i servizi offerti nel cloud AWS. L'infrastruttura è formata dai componenti hardware e software, le reti e le strutture che eseguono i servizi Cloud AWS.

Sogei si assume la responsabilità e la gestione del sistema operativo guest (inclusi gli aggiornamenti e le patch di sicurezza), di altro software applicativo nonché della configurazione del firewall del gruppo di sicurezza fornito da AWS. La responsabilità di Sogei verrà determinata dai servizi Cloud AWS scelti. Questo determina l'entità del lavoro di configurazione che Sogei deve eseguire come parte delle proprie responsabilità di sicurezza.

Come illustrato nel grafico che segue, questa differenziazione della responsabilità viene comunemente detta sicurezza "del" cloud rispetto a sicurezza "nel" cloud.



Sogei avrà a propria disposizione varie opzioni rispetto alla configurazione dei propri account e, per quanto concerne tutti i contenuti di natura sensibile o di valore, sarà sua cura adottare misure di sicurezza e di ridondanza efficaci, quali controlli relativi all'accesso, crittografia e backup.

Sarà sotto la responsabilità di Sogei la corretta configurazione e il corretto utilizzo dei servizi offerti, in modo da garantire la sicurezza e la ridondanza dei propri Account AWS Enterprise e dei propri contenuti, inclusi, ad esempio, l'impiego di controlli d'accesso rafforzati tesi ad impedire accessi non autorizzati agli Account AWS Enterprise o ai Contenuti di Sogei, l'impiego di sistemi di crittografia per impedire accessi non autorizzati ai propri contenuti, e garantendo l'implementazione di un adeguato livello di backup per prevenire la perdita degli stessi.

AWS dovrà garantire la disponibilità di un programma per la sicurezza informatica sviluppato per accordare un livello di protezione non inferiore a quello attestato alla Data di Efficacia del contratto: al momento il sistema ISMS (Information Security Management System) di AWS dispone di certificazione ISO 27001.

Su richiesta di Sogei, e a condizione che le parti abbiano siglato un Accordo di Riservatezza, AWS fornirà al Cliente una copia del report AWS Controlli di Sistema e Organizzazione 1, Tipo 2, o in alternativa report o certificazioni analoghi rappresentanti lo standard del settore e che siano ragionevolmente considerati



da AWS come sostanzialmente equivalenti. AWS renderà disponibile a Sogei tale documentazione tramite AWS Artifact (o tramite un canale alternativo accessibile dal Sito di AWS) e tale documentazione verrà trattata come Informazione Riservata di AWS ai sensi dell'Accordo di Riservatezza.

Inoltre AWS implementerà adeguate e ragionevoli misure di sicurezza per il Network di AWS (come stabilito da AWS), sviluppate per aiutare Sogei a difendere i propri contenuti da accessi, perdite o divulgazioni accidentali o illeciti (di seguito definiti "**Obiettivi di Sicurezza**"), in conformità con gli Standard di Sicurezza di AWS descritti nell'**Allegato 2.1** al presente Capitolato Tecnico. AWS ha la facoltà di modificare periodicamente i propri standard di sicurezza, ma continuerà a fornire un livello di sicurezza non inferiore a quello descritto nell'**Allegato 2.1**.

Eventuali componenti e/o dispositivi/apparati necessari all'erogazione dei servizi richiesti e resi disponibili nell'ambito dei listini AWS, dovranno essere messi a disposizione dal fornitore, senza ulteriori oneri per Sogei e, con il rispetto dei livelli di servizio previsti per la categoria di appartenenza.

5.1. Requisiti di qualificazione dei servizi e delle infrastrutture cloud

I servizi cloud oggetto della presente iniziativa dovranno essere erogati nel rispetto dei requisiti descritti dall'ACN, in tema di qualificazione dei servizi e delle infrastrutture cloud. Si applica pertanto quanto previsto dal decreto direttoriale n. 29 del 2 gennaio 2023 e dalla precedente determina n. 307 del 18 gennaio 2022 (e i relativi atti ivi richiamati).

La qualificazione del CSP è condizione essenziale ai fini della stipula del contratto e dovrà essere mantenuta per tutta la durata contrattuale.

Di conseguenza, in conformità a quanto previsto dal decreto direttoriale n. 29 del 2 gennaio 2023 e della precedente determina n. 307 del 18 gennaio 2022 dell'ACN in tema di qualificazione di servizi Cloud per le PA, nell'ambito del regime transitorio in essere, il livello di qualificazione minimo da possedere per i servizi oggetto della presente acquisizione è il QC1; il livello di qualifica nonchè lo stato inerente gli altri livelli di qualificazione dei servizi oggetto del contratto è dichiarato da AWS all'interno della sua Dichiarazione d'Offerta Economica (Tabella "Qualificazione servizi"); lo stesso dovrà essere aggiornato da parte del Fornitore, a fronte di eventuali successivi eventi. La Sogei – in corso di contratto - potrà utilizzare lo stesso per servizi da erogarsi per dati rientranti nella classificazione ordinaria, critica e strategica purchè i relativi servizi siano preliminarmente qualificati in accordo con la classificazione del dato.

Resta inteso che troveranno applicazione, ove possibile, le disposizioni eventualmente introdotte a



seguito dell'entrata in vigore del regime ordinario di qualificazione dei servizi cloud, la cui adozione da parte di ACN è prevista entro il 31 luglio 2023.

In caso di revoca della qualificazione o di scadenza della validità della qualificazione ai sensi della normativa vigente, si applica quanto previsto in materia dallo Schema di Contratto.

5.2. Requisiti DNSH

I servizi indicati nel paragrafo 3.1 dovranno essere conformi ai requisiti tecnici e ambientali previsti dalla normativa europea e nazionale in ottemperanza al principio di non arrecare un danno significativo all'ambiente, "Do No Significant Harm" (DNSH), Scheda n. 6, della Circolare RGS n. 33/2022, qualora debbano essere acquisiti tramite fondi PNRR.

I partecipanti dovranno completare la Scheda 6 "Servizi informatici di hosting e cloud", della Circolare RGS n. 33/2022 presente nell'**Allegato 12**, secondo la dichiarazione redatta ai sensi e per gli effetti degli art. 47 e art. 76 del DPR 445/2000 e fornire la documentazione e/o dichiarazioni necessarie per la verifica di tali requisiti, la cui sussistenza sarà accertata, in fase esecutiva. Coerentemente con quanto previsto dalla Circolare RGS n. 33/2022, la Committente si riserva di verificare l'applicabilità di ulteriori schede al momento non segnalate.

5.3. Piattaforma elettronica e disponibilità dei servizi

La disponibilità dei servizi dovrà essere assicurata **h 24/7, 365 giorni l'anno** ed in modalità continuativa. Sogei potrà specificare le aree geografiche AWS in cui dovranno essere archiviati i propri contenuti, anche in accordo a quanto previsto nell'**Allegato 10 "DPA"** (Data Processing Addendum). In particolare i servizi dovranno essere fruibili da almeno 2 distinti siti geografici di localizzazione delle risorse, su territorio europeo e con distanza adeguata alla realizzazione di soluzioni di disaster recovery.

5.4. Livelli di servizio e Crediti di Servizio

Gli SLA di AWS associati ai singoli servizi sono riportati nella pagina <https://aws.amazon.com/it/legal/service-level-agreements/>. Nel caso di mancato rispetto di detti livelli di servizio, Sogei potrà avviare la richiesta di un **Credito di Servizio** e, a tal fine, AWS metterà a disposizione di Sogei degli strumenti di monitoraggio dei servizi e delle API che si possono integrare con gli strumenti scelti da Sogei.

La determinazione dei Crediti di Servizio, i tempi relativi alla richiesta ed eventuali pagamenti sono



indicati nella pagina relativa allo SLA di ciascun servizio.

Per ricevere i Crediti di Servizio, Sogei dovrà aprire un ticket presso AWS Support Center, seguendo la procedura prevista all'interno di ciascun servizio.

A titolo esemplificativo, l'apertura di un ticket di richiesta credito, deve includere:

- la data del downtime, la Region e le risorse interessate;
- i log che documentano gli errori e confermano l'interruzione dichiarata (qualsiasi informazione riservata o sensibile in questi log deve essere rimossa o sostituita con asterischi);
- ogni altra informazione, così come indicata nella pagina relativa allo SLA del servizio.

Una volta preso in carico il ticket aperto, AWS analizzerà la richiesta di credito e se l'inadempimento relativo agli SLA sarà confermato, provvederà a riconoscere il credito richiesto da Sogei, nella prima fatturazione utile.

Per quanto riguarda i servizi “trasversali”, i Livelli di Servizio richiesti dovranno essere quelli garantiti di cui alla Tabella 3 del presente Capitolato.

Fatto salvo l'obbligo di mantenere i requisiti previsti al paragrafo 5.1, AWS può modificare i LdS dei servizi, inviando una notifica con 90 giorni di preavviso, fermo restando che tali modifiche non dovranno essere peggiorative rispetto a quanto definito, al momento della stipula del contratto; si precisa tuttavia che, per quanto i servizi ‘trasversali’ i relativi LdS si intendono come requisiti minimi, immodificabili in peius.

5.5. Gestione delle Utenze AWS

Una volta creato un Account AWS Enterprise Sogei sarà responsabile della gestione dei dati (incluse le opzioni di crittografia), della classificazione degli asset e dell'utilizzo degli strumenti di Identity and Access Management (IAM), per applicare le autorizzazioni appropriate.

Il controllo dei contenuti resterà sotto la responsabilità di Sogei che potrà:

- scegliere dove memorizzare i propri contenuti, selezionando anche il tipo di archiviazione e l'area geografica in cui conservarli;
- scegliere lo stato di sicurezza dei propri contenuti, utilizzando funzionalità di crittografia leader del



settore offerte da AWS per proteggere i contenuti in transito e inattivi, insieme alla possibilità di gestire le chiavi di crittografia;

- gestire l'accesso ai propri contenuti e ai servizi e risorse di AWS, utilizzando configurazioni specifiche con utenti, gruppi, autorizzazioni e credenziali controllate da Sogei.

Le credenziali di accesso di AWS e le chiavi private generate dai servizi sono esclusivamente a uso interno e non potranno essere cedute a qualsiasi titolo ad altri enti/persone. Sogei ha, tuttavia, la facoltà di comunicare la sua chiave privata ai propri agenti e collaboratori che operano per suo conto. Fatto salvo quanto causato da inadempimenti da parte di AWS, per quanto concerne il rapporto tra le parti, Sogei è responsabile per tutte le attività poste in essere dal suo Account AWS Enterprise, come la creazione di nuovi account, la gestione delle identità e l'autorizzazione degli accessi a servizi e dati.

La presente disciplina regola tutti gli Account AWS Enterprise con esclusione di ogni altra regolamentazione con essa incompatibile.

5.6. Disciplina servizi

Si precisa che solo Sogei sarà responsabile per l'utilizzo, da parte dei eventuali Utenti Finali (amministrazioni clienti), per i contenuti ed i servizi offerti, in ogni caso gli Utenti Finali dovranno operare in conformità con qualsiasi obbligo di Sogei, ai sensi del presente Capitolato e del Contratto. AWS non presterà servizi o assistenza agli Utenti Finali, questa laddove necessaria dovrà essere prestata da Sogei.

In particolare, a Sogei e a qualsiasi Utente Finale si fa espresso divieto di fare quanto segue:

- a) effettuare operazioni di reverse engineering, scomposizione, o decompilazione, sui servizi o sui contenuti AWS, ovvero applicare processi o procedure di altro tipo per ricavare il codice sorgente di qualsiasi software incluso nei servizi o nei Contenuti AWS;
- b) accedere o utilizzare i servizi o i contenuti di AWS in un modo teso ad eludere le commissioni da corrispondere o a superare i limiti o le soglie di utilizzo previsti;
- c) rivendere i servizi o i contenuti AWS.

5.7. Aggiornamento dell'Elenco dei Servizi

L'Elenco dei servizi, di cui al paragrafo 3.1, è frutto della recente analisi svolta da Sogei, ed è riferito all'offerta complessiva di AWS d'interesse di Sogei che, al momento, ha individuato tali servizi come



propedeutici alla realizzazione delle sue attività progettuali.

Il soprarichiamato Elenco dei servizi sarà, in ogni caso, suscettibile di integrazioni, sotto forma di evoluzione tecnologica che ampliano e personalizzano altri già in uso, ovvero con l'inclusione di ulteriori servizi funzionalmente collegati, e appartenenti all'ambito delle macrocategorie contrattualmente previste (Tabella 1), necessari a supportare la Sogei nella realizzazione dei suoi futuri progetti. Resta inteso che, nelle integrazioni, potranno essere inclusi esclusivamente i servizi del listino pubblico del CSP, compatibilmente con requisiti di cui al precedente paragrafo 5.1 e 5.2 e nel rispetto delle condizioni economiche previste dal contratto; tali modifiche saranno effettuate, previo accordo tra Sogei ed AWS, durante tutto il corso del contratto.

In tutti i casi in cui si verifichi un aumento dei prezzi di listino dei servizi, AWS invierà una Notifica a Sogei con almeno 60 giorni di preavviso; in ogni caso, Sogei ha la facoltà di recedere dai servizi, secondo le modalità previste nel contratto.

In tutti i casi di aggiornamento dell'Allegato Elenco dei Servizi saranno applicabili le condizioni economiche previste nel Contratto. La percentuale di sconto, così come praticata in sede di offerta, sarà applicata anche agli aggiornamenti.

6. NOTIFICHE

Tutte le comunicazioni dovranno essere effettuate inviando una notifica al Responsabile di Sogei indicato nel Contratto (o a qualsiasi altro referente successivamente designato) a condizione che i suoi riferimenti di contatto (es. indirizzo email) siano associati all'Account AWS Enterprise del Cliente.

7. VERIFICHE DI CONFORMITA'

Entro il termine di **5 giorni lavorativi** dalla scadenza di ciascun mese di riferimento, Sogei effettuerà le verifiche di conformità sui servizi attivati, volte a certificare che le prestazioni contrattuali siano eseguite a regola d'arte sotto il profilo tecnico-funzionale; le verifiche saranno eseguite in conformità a quanto previsto nel presente Capitolato e nel Contratto.

In particolare, le verifiche saranno effettuate controllando, mediante la piattaforma elettronica messa a disposizione da AWS, la regolare disponibilità ed erogazione dei servizi.



Nel caso di particolari caratteristiche dei servizi oggetto di acquisizione che non consentono la verifica di conformità per la totalità delle prestazioni, Sogei si riserva la possibilità di effettuare controlli a campione o in forma semplificata con modalità comunque idonee a garantire la verifica dell'esecuzione contrattuale.

Nel caso di esito positivo delle verifiche di conformità, la data di ogni verbale verrà considerata quale **“Data di accettazione del Servizio”**, relativamente alle attività verificate da parte di Sogei; nel caso in cui, dalle verifiche di conformità, emerga che, nel periodo di riferimento, si sono verificati dei disservizi, all'interno del relativo verbale si darà atto degli elementi necessari ai dell'attivazione della conseguente procedura di quantificazione e richiesta dei **“Service Credit”** maturati.

Nel caso di esito negativo della verifica di conformità, verrà emesso un verbale con la certificazione dei disservizi verificati, ai fini dell'applicazione delle penali e della conseguente quantificazione dei **“Service Credit”** maturati.

8. EXIT STRATEGY E GRACE PERIOD

Il Fornitore si obbliga a prestare supporto a Sogei nella fase di Exit Strategy che consiste nel processo di individuazione e migrazione dei dati presenti sulle infrastrutture AWS.

L'Exit Strategy dovrà concludersi entro novanta giorni decorrenti dalla scadenza naturale del contratto ovvero dalla data di efficacia del recesso/risoluzione del contratto stesso.

Inoltre 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 di Sogei 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 da parte di Sogei e volta a richiedere tale recupero o cancellazione.

Entro e non oltre il termine di tale periodo di 90 giorni il Cliente dovrà chiudere tutti gli account AWS contenenti Dati del Cliente.

Al momento della scadenza naturale del contratto, il Fornitore non avrà più titolo per emettere fatture, in quanto deve intendersi attivato il Grace period, per un periodo massimo di 30 giorni, durante il quale



la Committente si riserva di procedere al rinnovo del contratto, anche con altro cloud service provider ovvero alla migrazione dei servizi (Exit strategy) senza alcun onere aggiuntivo per la Committente, che dovrà avvenire entro il Grace period.

In caso di recesso da un singolo servizio, si applica, in quanto compatibile, la summenzionata disciplina relativa all'Exit Strategy e al Grace Period.