

PRIVACY LEVEL AGREEMENT (PLA)  
**OPIQUAD SRL a SOCIO UNICO**  
**Servizi SaaS/laaS in CLOUD**

PANORAMICA

**Abstract**

Il cloud computing è un nuovo approccio per la fornitura di risorse IT sotto forma di servizi accessibili via rete. Il Cloud sollecita una nuova frontiera e nuove modalità di controllo e di governo nella gestione delle informazioni, nella produzione, erogazione e fruizione dei servizi IT, nonché nella gestione dei rischi. Il nuovo modello di security Governance è basato sul controllo indiretto e sulla delega delle funzioni tecniche: la sicurezza delle informazioni e in special modo dei dati personali e comuni è una delle principali preoccupazioni per i potenziali clienti Cloud. Pertanto, "la compliance alla privacy" è diventata un criterio di valutazione fondamentale tra i Cloud Service Provider.

**Opiquad**, conforme alle linee guida indicate dal Gruppo di lavoro dei garanti Europei ha provveduto ad individuare gli aspetti più critici che possono incidere sulla tutela dei dati personali e comuni nei contratti cloud e lo ha tradotto in un Privacy Level Agreement volto a disciplinare i requisiti di sicurezza e di resilienza del servizio, la compliance e la protezione dei dati, che vengono quindi stabiliti su base contrattuale definendo con trasparenza e chiarezza i livelli e le garanzie relative alla tutela e alla sicurezza dei dati personali.

**Il Regolamento generale sulla protezione dei dati e il Sistema di Gestione Opiquad**

La protezione dei dati personali richiesta dal Regolamento Generale sulla Protezione dei Dati (Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, di seguito anche "Regolamento"), entrata in vigore il 25 maggio 2018 passa per una nuova organizzazione aziendale. Opiquad si è dotata di un Sistema di Gestione "Risk based" che trova una leva nell'adozione "cooperativa" di un modello organizzativo privacy (MOP) e del Modello di Organizzazione di Gestione e Controllo (MOG). Tenendo conto del nostro contesto operativo, delle esigenze di filiera e delle aspettative dei nostri clienti, il Sistema stabilisce Leadership e impegno, attraverso la definizione dei ruoli organizzativi, delle responsabilità interne ed esterne e dell'autorità dei soggetti coinvolti. All'interno del Modello, sono stati individuati gli obiettivi di sicurezza e sono state pianificate le azioni necessarie per la loro realizzazione. Vengono inoltre garantite le risorse e le competenze necessarie al fine di un costante e continuo miglioramento del Sistema nel tempo, verificando periodicamente il suo campo di applicazione e l'allineamento con gli scopi aziendali.

**Dichiarazione di conformità**

Opiquad è conforme: (i) alle direttive sulla tutela dei dati personali e quindi della privacy dei clienti che affidano le loro informazioni al servizio in Cloud; (ii) implementa un sistema specializzato sulle tematiche peculiari della privacy referenziando gli altri standard vigenti in materia dei quali estende ed attualizza le indicazioni.

- I clienti dei servizi cloud Opiquad sanno dove sono archiviati i loro dati.
- I dati dei clienti non verranno usati per scopi di marketing o pubblicitari senza il consenso esplicito.
- I clienti Opiquad sanno cosa accade alle informazioni personali e comuni.
- Opiquad ottempera esclusivamente alle richieste di divulgazione dei dati dei clienti legalmente vincolanti.

Opiquad aderisce **alle norme UNI EN 27017:2015 e 27018:2019** che garantiscono che i servizi Cloud a disposizione dei Clienti ed in generale l'intero sistema informazionale Opiquad sono progettati per garantire la massima sicurezza nella gestione delle informazioni e per la protezione dei dati personali trattati, per la valutazione dei rischi per proteggere tali informazioni in infrastrutture informatiche distribuite.

I documenti che provano le certificazioni Opiquad per gli standard in oggetto sono disponibili presso il nostro registro. Per visualizzare le certificazioni Opiquad, consulta la pagina del sito web Opiquad – sezione "certificati".

D PRI 31

DATA DI EMISSIONE	REDDATTO DA	APPROVATO DA	ULTIMO AGGIORNAMENTO
15.04.2022	- AdS area Connect TLC – CSI - NOC - Project Manager Servizi Cloud (SaaS) - Data Protection Officer - Security Manager	Governance	15.04.2022
24.10.2022	- Security Manager	Governance	24/10/2022

**OPIQUAD SRL A SOCIO UNICO**

039 93 99 920 | [info@opiquad.it](mailto:info@opiquad.it) | [opiquad@pec.opiquad.it](mailto:opiquad@pec.opiquad.it)

Sede operativa: Via Bergamo, 60 – Merate 23807 (LC) | Sede legale: Via Pietro Paleocapa, 6 – Milano 20121 (MI)

Codice fiscale e Partiva Iva: IT 05866450967 | Codice SDI: M5UXCR1 | REA: MI – 1946731 | Capitale Sociale: € 90.000 i.v.

Società soggetta a direzione e coordinamento di **Opiquad Holding Srl**

**STRUTTURA DEL DOCUMENTO PLA**

AMBITO	CAPITOLI (S)
<b>GENERALITA'</b>	Privacy Level Agreement Applicabilità Obiettivi Validità e durata Riferimenti Termini e definizioni
<b>RUOLI E RESPONSABILITA' INFORMAZIONI SUL TRATTAMENTO</b>	Ruoli privacy Addendum sul trattamento dei dati (DPA) Modello di responsabilità condivisa della sicurezza Selezione dei servizi Termini e livelli del servizio
	Tipologia e Finalità di Trattamento Categorie di dati
<b>SICUREZZA DEI DATI E REG. EU 679/2016</b>	Misure organizzative generali Gestione dei rischi Progettazione secondo i principi "by design" & "by default" Rapporti con i soggetti coinvolti nel trattamento Categorie di dati Il ciclo di vita dei dati Misure organizzative e tecniche specifiche Garanzia di controllo (Audit) Attività di revisione e organismi di controllo
<b>POLICY SPECIFICHE</b>	Data Breach Migrazione (portabilità) Diritti degli interessati Assicurazione
<b>CONSERVAZIONE</b>	Comunicazione, diffusione e trasferimento dei dati Gestione del rapporto con le terze parti
<b>SUPERVISIONE</b>	Audit prima e seconda parte Audit di terze parti

**OPIQUAD SRL A SOCIO UNICO**

039 93 99 920 | [info@opiquad.it](mailto:info@opiquad.it) | [opiquad@pec.opiquad.it](mailto:opiquad@pec.opiquad.it)

Sede operativa: Via Bergamo, 60 – Merate 23807 (LC) | Sede legale: Via Pietro Paleocapa, 6 – Milano 20121 (MI)

Codice fiscale e Partiva Iva: IT 05866450967 | Codice SDI: M5UXCR1 | REA: MI – 1946731 | Capitale Sociale: € 90.000 i.v.

Società soggetta a direzione e coordinamento di **Opiquad Holding Srl**

## GENERALITA'

Il presente documento, denominato Privacy Level Agreement (di seguito anche "PLA") è parte integrante del Contratto di servizi e descrive il livello di protezione della privacy che manterrà il provider di servizi Opiquad SRL a socio unico (di seguito anche "Opiquad"), fornendo metriche rispetto alla privacy delle informazioni e di protezione dei dati personali e comuni che la stessa si impegna a mantenere rispetto al trattamento dei dati personali, nell'erogazione dei servizi contrattualizzati cui il medesimo si applica.

### 1. Il Privacy Level Agreement

Il presente PLA si applica a tutti i rapporti contrattuali posti in essere tra Opiquad e ciascun Cliente, anche se non incorporate nel relativo documento contrattuale. In particolare, il PLA rappresenta uno standard che consente ad Opiquad di comunicare in modo articolato ed armonizzato il livello di protezione dei dati personali offerto rispetto ai requisiti imposti dal Regolamento (UE) 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 (di seguito anche "Regolamento") nell'ambito dei servizi di Cloud Pubblico, nel caso in cui operi come Responsabile esterno del trattamento (di seguito anche "Data Processor").

### 2. Applicabilità e Ubicazione Geografica

Il modello di dispiegamento dei servizi cloud riguarda i Data Center di Opiquad in cui sono installati tali servizi:

- Data Center di Merate (Lecco)
- Data Center di Siziano (Pavia)

Il seguente PLA interessa quindi i servizi in Cloud offerti da Opiquad (SaaS, gli stessi servizi IaaS) e l'intera infrastruttura che li ospita (IaaS).

Allo Stato dell'arte il presente PLA si applica ai seguenti servizi Cloud (catalogo dei servizi):

Email Backup

bWireless

IaaS

Infrastruttura servizi IaaS

Opivoice (erogato in modalità IaaS)

Dad (Digital Asset Defender)

Le Infrastrutture Opiquad su cui vengono messe a disposizione le istanze delle macchine virtuali (risorse di calcolo cpu/ram), gli spazi di storage e gli altri spazi di archiviazione, sono accessibili al Cliente attraverso la rete Internet. Il Cliente deve disporre di una connessione Internet per connettersi all'Interfaccia di Gestione e accedere al Servizio, ed è l'unico responsabile della suddetta connessione Internet con particolare riferimento alla sua disponibilità, affidabilità e sicurezza.

### 3. Obiettivi

Opiquad, attraverso il PLA si prefigge una duplice finalità:

- fornire agli utenti del cloud uno strumento di valutazione del livello di protezione dei dati personali e comuni offerto;
- comunicare in modo articolato ed armonizzato il livello di protezione dei dati personali e comuni offerto rispetto ai requisiti imposti dal Regolamento Europeo 679/2016 sulla Protezione dei dati personali e la libera circolazione degli stessi (di seguito, "Regolamento") in ambito Cloud, da Opiquad.

Più in generale, il PLA mira ad aumentare il livello di trasparenza e responsabilità dal punto di vista della privacy e della sicurezza.

### 4. Validità, durata

Il PLA entra in vigore al momento della sottoscrizione di ciascun contratto di servizio e rimane attivo per tutta la durata dello stesso.

Opiquad si riserva di modificare anche durante l'anno il documento PLA, qualora avvengano fatti che lo rendano consigliabile o necessario.

### 5. Riferimenti

Il PLA si basa sulle disposizioni legali obbligatorie della protezione dei dati personali dell'UE applicabile e al contempo riflette la pertinente interpretazione delle autorità di vigilanza europee e le migliori pratiche correlate e sviluppate dalle agenzie competenti.

- Riflette i requisiti del Regolamento EU 679/2016 rilevanti per il dominio cloud e, seguendo la "portata territoriale", si estende oltre l'UE;
- Linee guida del gruppo di lavoro sulla protezione dei dati sul diritto ai dati Portabilità10 (A.29WP242/16),
- Linee guida sui responsabili della protezione dei dati (A.29WP243/16),
- Linee guida su Valutazione dell'impatto sulla protezione dei dati (DPIA) ai fini del Regolamento 2016/679 (A.29WP248/17),

## **OPIQUAD SRL A SOCIO UNICO**

039 93 99 920 | [info@opiquad.it](mailto:info@opiquad.it) | [opiquad@pec.opiquad.it](mailto:opiquad@pec.opiquad.it)

Sede operativa: Via Bergamo, 60 – Merate 23807 (LC) | Sede legale: Via Pietro Paleocapa, 6 – Milano 20121 (MI)

Codice fiscale e Partiva Iva: IT 05866450967 | Codice SDI: M5UXCR1 | REA: MI – 1946731 | Capitale Sociale: € 90.000 i.v.

Società soggetta a direzione e coordinamento di **Opiquad Holding Srl**

- Parere 05/2012 sul Cloud Informatica (A.29WP05/2012)
- ENISA Linee guida tecniche per l'attuazione delle misure di sicurezza per i fornitori di servizi digitali (Linee guida ENISA 16.02.2017).
- Eusec (European Security Certification Framework): Privacy code of conduct draft.
- CSA (CSA Code of Conduct for GDPR\_V4).

## 6. Termini e Definizioni

TERMINI	DEFINIZIONI
<b>Cloud Service Provider (CSP)</b>	È il soggetto responsabile di rendere il servizio utilizzabile alle parti terze interessate. Il cloud provider acquisisce e gestisce le infrastrutture elaborative necessarie a fornire i servizi, assicura l'esecuzione dei programmi che consentono i servizi, e le infrastrutture per erogare i servizi attraverso la rete. Le attività del CSP coprono cinque aree principali che riguardano l'erogazione del servizio, l'orchestrazione del servizio, la gestione dei servizi cloud, la sicurezza e la privacy. <b>Ruolo privacy: Responsabile esterno del trattamento.</b> È la persona giuridica, che tratta dati personali per conto del Cliente, secondo quanto concordato tra le parti nel contratto di trattamento e richiamato nel presente PLA. Il Responsabile del Trattamento, salvo quanto diversamente specificato, è Opiquad SRL
<b>Il Cliente</b>	È colui che configura i servizi offerti dal cloud provider e svolge una funzione di interfaccia tra quest'ultimo e il cliente finale. Rappresenta la persona o l'organizzazione che ha sottoscritto un contratto con un cloud provider. <b>Ruolo privacy: Data Controller.</b> 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 e gli strumenti adottati, ivi comprese le misure di sicurezza relative al funzionamento ed alla fruizione dei servizi Cloud. Il titolare del Trattamento, salvo quanto diversamente specificato è il Cliente.
<b>Cloud consumer CSC</b>	È "l'utente finale", l' utilizzatore del servizio. È il principale soggetto che utilizza i servizi di cloud computing. L'individuo che utilizza i servizi Cloud di Opiquad coincide con l'Interessato, ovvero la persona fisica cui si riferiscono i Dati Personali.
<b>Data Processing Agreement (DPA)</b>	L'Accordo sul trattamento dei dati, o DPA in breve, è un contratto legalmente vincolante tra un'azienda e un responsabile del trattamento di dati di terze parti, inteso a regolamentare la privacy dei dati in relazione alla conformità al Regolamento. Il Data Processing Agreement descrive le condizioni e le modalità di trattamento dei dati personali: il suo contenuto minimo dettato dal Regolamento è sempre necessario, è lo strumento formale di compliance per il rispetto del principio di accountability.
<b>Modello organizzativo privacy (MOP)</b>	Definizione e adozione di un modello organizzativo per la gestione degli adempimenti in materia di protezione dei dati e degli interessati, avendo come riferimento il Regolamento UE 2016/679 sulla protezione dei dati personali che permetta di regolare e definire la struttura aziendale, nonché inserire la gestione dei dati personali in adempimenti automatizzati (privacy by design) che a loro volta attivano correttivi (privacy by default) in caso di necessità (data breach e data security).
<b>Il Servizio Cloud</b>	Il Servizio Cloud fornito da Opiquad così come definito nei relativi termini (se presenti) su questo sito/applicazione. servizi forniti tramite cloud computing, ossia un modello che consente l'accesso in rete diffuso, pratico e su richiesta a un gruppo condiviso di risorse elettroniche configurabili (ad esempio, reti, server, memorie, applicazioni e servizi), che possono essere forniti e messi a disposizione rapidamente con un minimo di impegno gestionale o di interazione con il fornitore del servizio.
<b>Software As A Service - SaaS -</b>	Software Opiquad o Non Opiquad attraverso la rete Internet con accesso autenticato ai server gestiti dalla Opiquad, tramite Credenziali di accesso fornite da Opiquad. Il Servizio SAAS non prevede la fornitura della strumentazione necessaria per poter usufruire del Servizio (quali ad esempio computer, modem/router, connessione Internet, ecc.) e che rimane in capo al Cliente.
<b>Infrastructure As A Service - IaaS -</b>	Alloggiamento presso server virtuale di risorse multimediali (es. core CPU, memoria RAM, storage, indirizzi IP, banda) nella disponibilità e sotto il controllo del Cliente, limitandosi Opiquad alla fornitura del solo spazio virtuale. Virtual Private Server: spazio virtuale presso i data center di Opiquad, accessibile tramite Internet, nel quale è possibile configurare una computer virtuale in base alle esigenze del Cliente, svincolando l'utilizzatore dalla necessità di acquistare componenti hardware, ove è possibile installare qualunque software.
<b>Valutazione d'impatto PIA</b>	PIA sta per "(Data) Privacy Impact Assessment" o "Valutazione d'Impatto sulla Privacy" ed è il primo documento che dovrebbe fare un'Azienda (quale titolare del trattamento dei dati) per valutare il livello di "impatto" delle proprie attività sulla gestione dei dati personali. In base a questo documento di "autovalutazione" verranno fatte una serie di considerazioni successive ed impostata la propria politica sulla privacy e la gestione dei dati personali.
<b>Disaster recovery (DR)</b>	L'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare, indisponibilità prolungate;

## OPIQUAD SRL A SOCIO UNICO

039 93 99 920 | [info@opiquad.it](mailto:info@opiquad.it) | [opiquad@pec.opiquad.it](mailto:opiquad@pec.opiquad.it)

Sede operativa: Via Bergamo, 60 – Merate 23807 (LC) | Sede legale: Via Pietro Paleocapa, 6 – Milano 20121 (MI)

Codice fiscale e Partiva Iva: IT 05866450967 | Codice SDI: M5UXCR1 | REA: MI – 1946731 | Capitale Sociale: € 90.000 i.v.

Società soggetta a direzione e coordinamento di **Opiquad Holding Srl**

documento pubblico

**OPIQUAD.IT**

## RUOLI E RESPONSABILITA' e INFORMAZIONI SUL TRATTAMENTO

### 7. Ruoli privacy

Opiquad è il Responsabile del Trattamento rispetto all'azienda o al soggetto che deposita i dati nel cloud ("il Cliente") che è il Titolare del trattamento. Il Cliente può agire come Data Controller o come Data Processor in relazione ai dati personali, fermo restando che il Fornitore agirà sempre come Responsabile.

RUOLI PRIVACY	NOMINATIVO
TITOLARE DEL TRATTAMENTO (Data Controller)	IL CLIENTE
RESPONSABILE O SUB RESPONSABILE DEL TRATTAMENTO (Data Processor)	OPIQUAD SRL A SOCIO UNICO <a href="mailto:privacy@opiquad.it">privacy@opiquad.it</a>

Opiquad, agisce in qualità di Responsabile o Sub Responsabile del trattamento, come previsto dall'articolo 28 del Regolamento, per la gestione dei dati di terzi presenti nei sistemi per l'erogazione dei servizi, sia nel caso in cui il Cliente sia il Titolare del trattamento sia che sia a sua volta un Responsabile del trattamento. Come "responsabile del trattamento" elabora le informazioni per conto dei titolari, non prendono decisioni su come usare le informazioni o sugli scopi dell'elaborazione. Opiquad, all'interno della sua struttura tratta i dati attraverso:

RUOLI PRIVACY	NOMINATIVO
<b>Amministratori di sistema (AdS)</b> Sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali.	Responsabile area NOC Responsabile area CONNECT CSI Responsabile area CONNECT TLC
<b>Autorizzati</b> Autorizzati che concorrono al trattamento dei dati per le finalità predefinite.	Dipendenti
<b>Responsabile della protezione dei dati o Data Protection Officer</b> Opiquad Holding SRL ha nominato un Responsabile della Protezione dei dati personali, incaricato di garantire il rispetto delle norme per la tutela della Privacy per questioni inerenti al trattamento dei dati personali.	Il Data Protection Officer <a href="mailto:dpo@opiquad.it">dpo@opiquad.it</a>
<b>Responsabile della sicurezza delle informazioni.</b> Implementa, mantiene e aggiorna i sistemi e le infrastrutture informatiche dell'azienda: Responsabile della sicurezza delle informazioni nell'ambito del sistema integrato SIGSI.	Senior System Engineer & Risk Manager <a href="mailto:support-csi@opiquad.it">support-csi@opiquad.it</a>

### 8. Addendum sul trattamento dei dati (DPA)

Opiquad offre un Addendum sul trattamento dei dati conforme al Regolamento, che consente di soddisfare gli obblighi contrattuali ivi stabiliti. L'Addendum di Opiquad al Regolamento è integrato nei CGC di Opiquad e viene applicato indistintamente e automaticamente a tutti i clienti: è quindi in tal senso che è sempre stipulato un contratto di elaborazione dati (Data Protection Agreement, o "DPA") così come previsto dall'art.31 delle CGC e dall'art. 28 del Regolamento.

### 9. Modello di responsabilità condivisa della sicurezza

La responsabilità in materia di sicurezza e conformità è condivisa tra Opiquad e il cliente. Ai sensi dell'art. 32, comma 1, lett. b), del Regolamento, il Titolare e il Responsabile del trattamento devono mettere in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio. Quando un cliente trasferisce sistemi informatici e dati nel cloud, le responsabilità di sicurezza vengono condivise tra il Cliente e il Fornitore di servizi cloud. Quando il cliente migra al cloud Opiquad, la stessa è responsabile della sicurezza

### **OPIQUAD SRL A SOCIO UNICO**

039 93 99 920 | [info@opiquad.it](mailto:info@opiquad.it) | [opiquad@pec.opiquad.it](mailto:opiquad@pec.opiquad.it)

Sede operativa: Via Bergamo, 60 – Merate 23807 (LC) | Sede legale: Via Pietro Paleocapa, 6 – Milano 20121 (MI)

Codice fiscale e Partiva Iva: IT 05866450967 | Codice SDI: M5UXCR1 | REA: MI – 1946731 | Capitale Sociale: € 90.000 i.v.

Società soggetta a direzione e coordinamento di **Opiquad Holding Srl**

dell'infrastruttura che supporta il cloud, mentre il cliente è responsabile per qualsiasi cosa venga caricata sul cloud o collegata a esso. La suddivisione delle responsabilità è generalmente indicata come "sicurezza del cloud versus sicurezza nel cloud". Il modello condiviso può aiutare a ridurre l'onere operativo a carico del cliente, fornendogli la flessibilità e il controllo necessari allo sviluppo delle infrastrutture nel cloud Opiquad. Le responsabilità sono sempre dettagliate nell' Addendum sul trattamento dei dati (DPA) dello spe

## Condizioni di utilizzo IaaS

Nell'ambito del presente contratto, il Cliente è l'unico amministratore delle sue macchine virtuali e spazi storage/archiviazione, Opiquad non interviene in nessun caso nella gestione delle istanze del Cliente. Allo stesso modo, il Cliente è l'unico responsabile dell'utilizzo dei delle sue macchine virtuali e spazi storage/archiviazione messi a sua disposizione.

Opiquad è incaricata dell'amministrazione dell'Infrastruttura (hardware, rete, Server Host, dischi) su cui sono configurate le Istanze e gli Spazi di Storage/archiviazione messi a disposizione del Cliente. Il Cliente dichiara di possedere l'insieme delle conoscenze tecniche necessarie a garantire un'amministrazione corretta delle risorse (Istanze, spazi di storage/archiviazione) messe a disposizione da Opiquad, e a effettuare un backup dei dati archiviati sulle suddette risorse. Il Cliente si impegna anche a prendere visione della documentazione messa a disposizione da Opiquad relativa al servizio.

Le operazioni di eliminazione e reinstallazione di spazi storage/archiviazione comportano la cancellazione automatica e irreversibile di tutti i dati e informazioni che vi sono salvati. Allo stesso modo, le operazioni di eliminazione e di reinstallazione di istanze comportano la cancellazione automatica e irreversibile (a) dei sistemi operativi e delle applicazioni installati, e (b) di tutti i dati e informazioni salvati sugli spazi di storage associati alle istanze eliminate o reinstallate. Il Cliente è l'unico responsabile delle operazioni (come backup, trasferimenti, snapshot, etc.) che ritiene necessario effettuare prima dell'eliminazione o della reinstallazione delle sue istanze e spazi di storage, per premunirsi contro la perdita delle sue informazioni, contenuti e dati.

### **Responsabilità Opiquad**

Opiquad si impegna a:

- Mantenere l'infrastruttura software aggiornata con le versioni dei software più stabili e sicuri rilasciate dal produttore
- Tenere sotto monitoraggio l'infrastruttura dei sistemi di virtualizzazione, hypervisor e storage al fine di garantire la continuità di servizi
- Controllare la presenza di eventuali anomalie relative alla sicurezza che si evidenzino attraverso i log o alert del sistema
- Disattivazione del servizio se a seguito di segnalazione da parte di altri service provider, il server stesse attuando dei comportamenti anomali (spam, phishing, contenuti inerenti al terrorismo, frode, sito hackerato)
- Informare il cliente in caso durante il monitoraggio o le analisi dei log dovessero essere riscontrati problemi sul server.

## **10. Selezione dei servizi**

10.1 Cliente è il solo responsabile della selezione dei Servizi assicurandosi che presentino le caratteristiche e le condizioni richieste per rispettare le attività e gli scopi del trattamento, nonché il tipo di Dati Personali da trattare all'interno dei Servizi, ivi compreso, senza tuttavia a ciò limitarsi, quando tali Servizi siano utilizzati per trattare Dati Personali soggetti a regolamenti o standard specifici.

10.2 Il Cliente è a conoscenza che Opiquad propone i Servizi con misure organizzative e di sicurezza specificatamente studiate per il trattamento di dati. Opiquad definisce preventivamente le categorie di dati autorizzate ovvero quelle che per la loro natura è fatto divieto al Cliente di trattare o conservare nel cloud.

10.3 Il Cliente ha l'obbligo di utilizzare i Servizi nel rispetto delle leggi, dei regolamenti vigenti e del Contratto. Qualsiasi uso difforme configura inadempimento del Cliente. Il Cliente non deve usufruire dei Servizi o degli Apparati in modo tale da causare danni a terzi, violazione di diritti di proprietà intellettuale di terzi, malfunzionamenti alla rete o violazione le normative vigenti. Il Cliente ha l'obbligo di attenersi ai criteri di buona fede e correttezza nell'uso dei Servizio, astenendosi dal conseguire utilità ulteriori rispetto a quelle tipiche dei Servizi. Il Cliente si obbliga ad utilizzare, in connessione ai Servizi e/o agli Apparati, eventuali dispositivi di cui lo stesso è proprietario, solo se conformi alla normativa e agli standard tecnici vigenti aventi i requisiti minimi eventualmente indicati da Opiquad ai fini della fruizione dei singoli Servizi. Sarà responsabilità del Cliente assicurare l'interoperabilità tra i suoi apparati e l'interfaccia dell'infrastruttura di rete Opiquad. Il Cliente si obbliga a non intervenire o manomettere, direttamente ovvero mediante terzi, Servizi e/o agli Apparati. Fatto salvo ogni altro rimedio di legge e ogni altra misura prevista dal presente Contratto, Opiquad si riserva la facoltà di sospendere immediatamente la fornitura dei Servizi e di risolvere il Contratto qualora il Cliente ne faccia l'uso improprio indicato nei commi precedenti, dando, se del caso, idonea comunicazione dell'illecito alle autorità competenti.

## **OPIQUAD SRL A SOCIO UNICO**

039 93 99 920 | [info@opiquad.it](mailto:info@opiquad.it) | [opiquad@pec.opiquad.it](mailto:opiquad@pec.opiquad.it)

Sede operativa: Via Bergamo, 60 – Merate 23807 (LC) | Sede legale: Via Pietro Paleocapa, 6 – Milano 20121 (MI)

Codice fiscale e Partiva Iva: IT 058866450967 | Codice SDI: M5UXCR1 | REA: MI – 1946731 | Capitale Sociale: € 90.000 i.v.

Società soggetta a direzione e coordinamento di **Opiquad Holding Srl**

**11. Termine e livelli del servizio**

11.1 Al termine del servizio, indipendentemente dalla causa (scadenza, risoluzione, eliminazione, mancato rinnovo, etc.) così come al termine della conservazione applicabile secondo i termini di legge, l'integralità dei dati (personali, non personali, e/o comuni) associati al servizio sarà automaticamente eliminata in modo irreversibile (backup incluso). Competerà pertanto al Cliente, previamente al termine del servizio o del periodo di conservazione dei dati (personali, non personali e/o comuni), salvare o trasferire eventualmente detti Dati su un ulteriore sistema, fatto salvo in presenza di una richiesta emessa da un'autorità legale o giudiziaria competente, oppure quando la normativa applicabile dell'Unione europea e di uno Stato membro dell'UE preveda diversamente. Il Cliente è l'unico responsabile di garantire la posta in essere delle operazioni necessarie sopradescritte prima della conclusione o della scadenza dei Servizi, nonché prima di avviare eventuali procedure di cancellazione, aggiornamento o reinstallazione dei Servizi.

11.2 Manutenzione, riparazioni ed aggiornamenti: la fornitura dei Servizi da parte di Opiquad potrà essere sospesa in caso di interventi programmati di manutenzione, che verranno comunicati con un preavviso di almeno 24 ore. Opiquad potrà, in ogni caso, sospendere l'erogazione dei Servizi senza preavviso in caso di guasti alle reti di comunicazione o agli Apparati. Opiquad si impegna a ripristinare gli eventuali disservizi del Servizio non imputabili direttamente o indirettamente al Cliente entro il più breve tempo possibile e comunque in accordo agli SLA eventualmente applicabili. Il Cliente prende atto ed acconsente che Opiquad potrà effettuare degli aggiornamenti tecnologici (aggiornamenti software e/o modifica delle configurazioni) alla propria rete, anche in un'ottica di sviluppo dei Servizi, nonché sugli Apparati necessari per fruire dei Servizi.

11.3 I livelli qualitativi del servizio offerto (o Service Level Agreement – SLA), cioè gli “allegati tecnici” che indicano dettagliatamente i parametri del servizio offerto sono definiti e trattati nel documento “SLA” (<https://www.opiquad.it/documentazione/>).

**12. Tipologia e Finalità di Trattamento**

Le attività di trattamento sono quelle strettamente connesse all'erogazione del servizio contrattualmente pattuito e ratificato nel DPA cui il servizio si riferisce. Il Fornitore dichiara espressamente che dati dei clienti non verranno usati per scopi di marketing o pubblicitari senza il consenso esplicito degli interessati che in ogni caso, non sarà mai una condizione necessaria per l'utilizzo del servizio cloud.

Modus Operandi	Tipologia	Finalità
ATTIVITA' ESEGUITE P/C DEL CLIENTE	RACCOLTA ORGANIZZAZIONE CONSERVAZIONE (ARCHIVIAZIONE) COMUNICAZIONE ESTRAZIONE INTERCONNESSIONE CANCELLAZIONE DISTRUZIONE	La fornitura del servizio contrattualizzato
ATTIVITA' RICHIESTA DAL CLIENTE		Configurazione del servizio Supporto tecnico Cancellazione – distruzione Configurazione dei privilegi di access
ATTIVITA' EFFETTUATE SU INIZIATIVA DEL FORNITORE		BaaS (back up as a Service) Aggiornamento (Update) Manutenzione Monitoraggio attività telematiche per la sicurezza informatica

## SICUREZZA DEI DATI E REGOLAMENTO EU 679/2016

### 13. Misure tecniche organizzative

Opiquad implementa una policy di gestione per la qualità e la sicurezza dei sistemi informativi che descrive l'insieme dei nostri provvedimenti in materia, che viene solitamente aggiornata almeno una volta all'anno, oppure in caso di modifiche importanti relative al contenuto. I nostri servizi sono a loro volta regolati da sistemi formali di gestione della sicurezza delle informazioni.

Le nostre infrastrutture e i servizi Cloud sono certificati ISO 9001, ISO/IEC 27001, 27017, 27018. Tali certificazioni garantiscono la presenza di un sistema di gestione qualitativo e nell'ambito della sicurezza dell'informazione (ISMS) per la gestione dei rischi, delle vulnerabilità e della continuità operativa, nonché di un sistema di gestione delle informazioni personali. La nostra conformità normativa ti consente di ospitare i dati personali in totale sicurezza.

**ISO 9001:** Opiquad ha conseguito la certificazione ISO 9001, che le consente di supportare direttamente i clienti che sviluppano, migrano e gestiscono i loro sistemi IT di qualità controllata nel cloud Opiquad. I clienti possono utilizzare i rapporti di compliance Opiquad come prove nei programmi ISO 9001 e nei programmi di qualità specifici del settore. I clienti Opiquad che non presentano requisiti per i sistemi di qualità trarranno comunque vantaggio dall'ulteriore garanzia e trasparenza offerte dalla certificazione ISO 9001.

La certificazione ISO 9001 può essere scaricata tramite sito web [www.opiquad.it](http://www.opiquad.it).

**ISO/IEC 27001:** Opiquad ha conseguito la certificazione ISO 27001 per il sistema ISMS (Information Security Management System) che copre l'infrastruttura, i data center e i servizi Opiquad.

La certificazione Opiquad ISO 27001 può essere scaricata tramite sito web [www.opiquad.it](http://www.opiquad.it).

**ISO/IEC 27017:** è il codice più recente sulle best practice pubblicato all'International Organization for Standardization (ISO). Fornisce indicazioni sull'implementazione dei controlli per la sicurezza delle informazioni che riguardano specificamente i servizi cloud.

La certificazione ISO 27017 può essere scaricata tramite sito web [www.opiquad.it](http://www.opiquad.it).

**ISO/IEC 27018:** è il primo codice internazionale delle best practice incentrato sulla protezione dei dati personali nel cloud. Si basa sullo standard ISO 27002 relativo alla sicurezza delle informazioni e fornisce indicazioni per l'implementazione dei controlli ISO 27002 che si applicano alle informazioni di carattere personale nel cloud pubblico. Prevede, inoltre, una serie di controlli aggiuntivi e di indicazioni associate finalizzati al soddisfacimento dei requisiti relativi alle informazioni di carattere personale nel cloud pubblico non previsti dal gruppo di controlli dello standard ISO 27002 esistente.

La certificazione ISO 27018 può essere scaricata tramite sito web [www.opiquad.it](http://www.opiquad.it).

In conclusione si impegna a: adottare un sistema di gestione sicura delle informazioni conforme ai requisiti specificati della Norma ISO/IEC 27001:2013 e delle linee guida ISO/IEC 27017 e 27018, mantenere costantemente monitorato il grado di conformità del sistema alle norme e leggi applicabili di natura cogente e volontaria, e gli obblighi contrattuali pertinenti l'ambito di applicazione del SGSI; garantire mezzi e risorse idonee al suo mantenimento e miglioramento continuo, in particolare per quanto attiene la mitigazione/riduzione dei livelli di rischio sulla sicurezza delle informazioni e l'adozione di misure idonee a prevenire situazioni anomale e di emergenza; rendere consapevoli tutte le persone che dell'organizzazione degli obblighi e delle responsabilità di ciascuno nella gestione della sicurezza delle informazioni e delle conseguenze in caso di eventi, dolosi e colposi, relativi all'utilizzazione non autorizzata, modifica o distruzione di informazioni critiche.

Almeno una volta all'anno, i servizi Cloud Opiquad vengono sottoposti a controlli di conformità a tali standard svolti da un organismo di certificazione di terze parti, che fornisce una convalida indipendente dell'implementazione e dell'efficacia dei controlli di sicurezza applicabili.

#### **14. Gestione dei rischi**

La direzione di Opiquad ha sviluppato un piano aziendale strategico che include l'identificazione del rischio e l'implementazione di controlli che limitano o gestiscono i rischi. La stessa rivaluta il piano aziendale strategico all'occorrenza o almeno ogni due anni. Questo processo richiede che la direzione identifichi i rischi che rientrano nelle sue aree di responsabilità e che implementi misure adeguate ad affrontarli. Inoltre, l'ambiente di controllo Opiquad è soggetto a diverse valutazioni del rischio sia interne sia esterne. Opiquad adotta il framework certificabile ISO/IEC 27001 sulla base dei controlli ISO/IEC 27002. Opiquad gestisce la policy di sicurezza, si occupa della formazione dei dipendenti in materia di sicurezza ed effettua verifiche sulla sicurezza dell'applicazione. Tali verifiche valutano la riservatezza, l'integrità e la disponibilità dei dati, oltre alla conformità alla policy di sicurezza delle informazioni.

In particolare sono presenti le seguenti soluzioni per gestire la sicurezza delle informazioni.

<b>Controllo</b>	<b>Dettaglio</b>
Antivirus	Viene utilizzata la scansione dei file presenti nelle aree dei software, tramite il motore ClamAv per il servizio EmailBackup.
Backup	Viene utilizzata la soluzione Veeam Backup e replica dati Ceph su più nodi.
Crittografia	I dati conservati nello storage degli oggetti e i dati necessari agli applicativi, vengono memorizzati utilizzando un sistema di crittazione a doppia chiave. La chiave con cui i dati vengono criptati è a sua volta criptata con una seconda chiave. I due dati vengono conservati in due differenti server. Le chiavi di criptatura vengono generate automaticamente e ruotate ogni mese. L'algoritmo utilizzato è SHA256 sia per la prima che per la seconda criptazione (dati e chiave).
Monitoraggio log	Viene utilizzata una soluzione proprietaria che permette di mantenere immutato il log, sia nel periodo di conservazione che di visualizzazione.
Sistemi di autenticazione	Oltre all'uso di un algoritmo univoco usato nella fase di autenticazione dei servizi, viene proposto l'utilizzo (facoltativo per l'utente e/o amministratore) di un controllo con codice "one time password".
Sicurezza dati perimetrale	Sono utilizzati apparati firewall hardware in modalità HA (alta affidabilità)

**15. Rapporti con i soggetti coinvolti nel trattamento**

Sono regolarmente gestiti e formalizzati:

<b>DPA CLIENTI</b>	Data Processing Agreement ("DPA") con i clienti che ci affidano i loro dati
<b>DPA TERZE PARTI</b>	Data Processing Agreement ("DPA") con fornitori di servizi
<b>ACCORDI NI NOMINA</b>	Vincoli di riservatezza con dipendenti e collaboratori - Incarichi e autorizzazioni ai soggetti autorizzati
<b>AdS</b>	Compliance alla normativa sugli Amministratori di sistema
<b>TRASPARENZA</b>	Informative artt. 12-13 Regolamento EU 679/2016

**16. Gestione della continuità operativa (BCP)**

Opiquad garantisce la protezione dalle potenziali criticità delle funzionalità informatiche, tenendo conto delle risorse umane, strutturali, tecnologiche riferibili all'infrastruttura informatica, stabilendo le idonee misure preventive e correttive nel rispetto dei livelli prestazionali riconosciuti e concordati. La continuità operativa delle infrastrutture (dispositivi, applicazioni e processi operativi) è garantita da diversi meccanismi:

- la continuità e la ridondanza della fornitura elettrica;
- la gestione dei dispositivi sotto la responsabilità di Opiquad;
- il supporto tecnico del servizio;
- La ridondanza dei dispositivi e dei server utilizzati per l'amministrazione dei sistemi.
- Parallelamente, altri meccanismi come il backup delle configurazioni e dei device di rete, garantiscono il ripristino in caso di incidente.

In base al servizio, Opiquad metterà a disposizione del cliente funzionalità di backup e ripristino che potrebbero essere sia incluse\* nell'offerta di base sia opzioni a pagamento. Pertanto, il perimetro di competenza comprende: (i) le applicazioni informatiche e i dati del sistema informativo indispensabili all'erogazione dei servizi e allo svolgimento delle attività (informatiche e non); (ii) le infrastrutture fisiche e logiche che ospitano sistemi di elaborazione; (iii) le componenti di connettività locale e/o remota/geografica; (iv) le misure per garantire la disponibilità dei sistemi di continuità elettrica (UPS e gruppi elettrogeni) e più in generale la continuità di funzionamento del sistema informativo.

**16.1 Disaster Recovery plan**

Opiquad conserva e ripristina l'intero sistema IT nel caso di downtime, incidenti o qualsiasi episodio possa minare la continuità di business dell'azienda predisponendo una o più repliche dell'intera infrastruttura IT. È dotata di un Disaster Recovery Plan (DRP), documento che comprende le misure tecnologiche e procedurali utili a ripristinare nel minor tempo possibile l'operatività, che a sua volta è ricompreso nel più ampio (BCP), che contempla anche gli aspetti relativi al backup. Il Disaster Recovery rappresenta la capacità di ripristinare l'operatività dei sistemi IT anche nel caso in cui il data center aziendale sperimenti un'inattività, legata a errori umani, calamità naturali (incendi, terremoti, alluvioni) o attacchi intenzionali.

**16.2 Backup**

(i) Opiquad non effettua nessun salvataggio specifico del contenuto e dei dati presenti sulle istanze, spazi storage/archiviazione. I meccanismi di replica dei dati effettuati da Opiquad nel quadro dei suddetti spazi di storage/archiviazione non costituiscono in nessun caso per il Cliente una garanzia contro la perdita del suo contenuto e dei suoi dati.

(ii) tutti i sistemi e i dati necessari alla continuità operativa, alla ricostruzione del sistema informativo o all'analisi successiva agli incidenti vengono memorizzati (file di database tecnici e amministrativi, registri delle attività, codici sorgente per applicazioni sviluppate internamente, configurazione di server, applicazioni e dispositivi, ecc.);

(iii) le frequenze, i tempi di memorizzazione e i metodi di archiviazione dei backup sono definiti in base alle esigenze di ciascuna risorsa memorizzata; la realizzazione dei backup è soggetta a un monitoraggio e a una gestione degli alert e degli errori.

Opiquad effettua i backup dei propri server secondo la più opportuna politica e con le opportune retention, inoltre effettua i backup delle macchine virtuali dei clienti in base ai piani di backup concordati commercialmente.

Opiquad implementa un sistema automatico di monitoraggio dell'esito dei job di backup con apertura automatica dei ticket in caso di problemi e garantisce la presa in carico e possibilmente la risoluzione di eventuali problemi entro il giorno lavorativo successivo.

SaaS	Frequenza	luogo	Type	Esecuzione	Ritenzione	crittografia
E-Mail Backup	Giornaliera	Data center Siziano	Full	Automatica	1 gg	attiva
DaD	Giornaliera	Data center Siziano	Full	Automatica	7 gg	attiva

**OPIQUAD SRL A SOCIO UNICO**

039 93 99 920 | [info@opiquad.it](mailto:info@opiquad.it) | [opiquad@pec.opiquad.it](mailto:opiquad@pec.opiquad.it)

Sede operativa: Via Bergamo, 60 – Merate 23807 (LC) | Sede legale: Via Pietro Paleocapa, 6 – Milano 20121 (MI)

Codice fiscale e Partiva Iva: IT 05866450967 | Codice SDI: M5UXCR1 | REA: MI – 1946731 | Capitale Sociale: € 90.000 i.v.

Società soggetta a direzione e coordinamento di **Opiquad Holding Srl**

bWireless	Giornaliera	Data Center Siziano	Full	Automatica	7 gg	attiva
Opivoice	Giornaliera	Data Center Siziano/Merat e	Full	Automatica	7 gg	attiva

I server dei sistemi oggetto di backup, oltre ai dati utente, includono: le configurazioni, i sistemi operativi, i prodotti, i file server, i server di posta e i web server. Opiquad garantisce che le tecniche di cifratura utilizzata non pregiudichino la disponibilità dei dati in caso di necessità, e che, pertanto, sia assicurata a tale scopo la compatibilità tecnologica dei supporti, dei formati di registrazione, degli strumenti crittografici e degli apparati di lettura dei dati per tutta la durata della conservazione del dato.

#### **17. Politiche di accesso IaaS**

Opiquad garantisce che ogni accesso, di tipo fisico o logico, sia autorizzato, controllato e monitorato sulla base dei seguenti criteri:

1. l'accesso è autorizzato al personale abilitato solo per le informazioni necessarie (principio della conoscenza minima o necessità di sapere);
2. l'accesso è autorizzato al personale abilitato solo per le informazioni relative alle attività specifiche (funzione di lavoro-correlati);
3. l'accesso alla struttura e ai locali è autorizzato al personale Opiquad abilitato, e al personale Cliente debitamente autorizzato.

L'accesso ai locali di Opiquad è autorizzato, controllato e monitorato in linea con la politica aziendale.

#### **18. Politiche di accesso SaaS**

Opiquad garantisce che ogni accesso, di tipo fisico o logico, sia autorizzato, controllato e monitorato sulla base dei seguenti criteri:

1. l'accesso è autorizzato al personale Opiquad abilitato solo per le informazioni necessarie (principio della conoscenza minima o necessità di sapere);
2. l'accesso è autorizzato al personale Opiquad abilitato solo per le informazioni relative alle attività specifiche (funzione di lavoro-correlati);
3. l'accesso alla struttura e ai locali è autorizzato al personale Opiquad abilitato.
4. l'accesso agli applicativi SaaS è autorizzato da parte di personale Cliente debitamente riconosciuto.

L'accesso ai locali di Opiquad è autorizzato, controllato e monitorato in linea con la politica aziendale.

#### **19. Responsabilizzazione del personale**

Opiquad si impegna che tutto il personale sia responsabilizzato all'obbligo di:

1. garantire il rispetto delle norme, leggi e regolamenti vigenti, di natura cogente, contrattuale e volontaria rese applicabili negli ambiti del SGSI;
2. proteggere la riservatezza, l'integrità e la disponibilità delle informazioni gestite da BLS, la proprietà intellettuale e il patrimonio di Opiquad o da questa affidati a terze parti;
3. aver cura dei beni materiali, i sistemi e le risorse di Opiquad;
4. salvaguardare e gestire in modo appropriato ogni informazione e dato afferenti le attività di propria competenza;
5. contattare la Direzione, il Responsabile della Sicurezza delle informazioni e/o altre autorità competenti in caso di effettive o sospette violazioni della sicurezza;
6. segnalare qualsiasi necessità di modifiche alle procedure relative alla gestione della sicurezza delle informazioni.

#### **20. Responsabilizzazione di soggetti terzi**

Opiquad si impegna nei confronti di soggetti terzi a:

1. formalizzare il proprio impegno alla riservatezza e non divulgazione delle informazioni tratte negli ambiti di competenza;
2. proteggere le risorse e le informazioni fisiche e intellettuali a cui possono accedere nella effettuazione delle attività assegnate;
3. garantire la piena osservanza ai requisiti del SGSI nei comportamenti e nell'operatività.

#### **21. Accesso ai portatili di gestione**

L'accesso ai portatili di gestione è protetto con adeguate misure di sicurezza (password, two factor authentication, indirizzo IP da cui viene effettuato l'accesso), superiori ai requisiti di legge. Vengono conservati i log degli accessi a norma di legge. I tentativi di accesso vengono identificati e segnalati immediatamente al cliente via email, gli account soggetti ad attacco vengono anche temporaneamente bloccati.

#### **22. Data breach, incidenti e non conformità**

Opiquad ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali e comuni che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente. Le violazioni potranno riguardare uno o più dei parametri di riservatezza, integrità e disponibilità. La perdita transitoria di disponibilità non costituisce una violazione di dati personali se non quando ci si trova davanti a una "interruzione significativa". Pertanto, l'impossibilità (momentanea) di accedere al servizio Cloud contrattualizzato, risolta dopo breve tempo, non potrà essere qualificata, in genere, come violazione di dati personali.

### **OPIQUAD SRL A SOCIO UNICO**

039 93 99 920 | [info@opiquad.it](mailto:info@opiquad.it) | [opiquad@pec.opiquad.it](mailto:opiquad@pec.opiquad.it)

Sede operativa: Via Bergamo, 60 – Merate 23807 (LC) | Sede legale: Via Pietro Paleocapa, 6 – Milano 20121 (MI)

Codice fiscale e Partiva Iva: IT 05866450967 | Codice SDI: M5UXCR1 | REA: MI – 1946731 | Capitale Sociale: € 90.000 i.v.

Società soggetta a direzione e coordinamento di **Opiquad Holding Srl**

22.1 Le eventuali violazioni dei dati personali (data breach) vengono comunicate secondo quanto previsto dalla normativa entro 72 ore al Garante per la protezione dei dati personali ed ai clienti interessati.

22.2 Opiquad implementa un sistema di gestione degli incidenti che prevede: segnalazione tempestiva al cliente mediante il più opportuno sistema di comunicazione (SMS o email), evidenziazione di eventuali non conformità collegate agli incidenti, adozione di opportune azioni correttive per evitare il ripetersi degli incidenti, produzione di un report ed invio al cliente, revisione periodica degli incidenti ad opera del security manager.

### **23. Documentazione tecnica di supporto**

23.1 Opiquad garantisce che i servizi offerti siano soggetti ad un processo di gestione della configurazione che consente, mediante procedure standard e relativi tool, il controllo di tutte le componenti rilevanti del servizio;

23.2 Opiquad fornisce la documentazione tecnica, le guide d'uso e/o altro materiale di supporto, ivi compresa la documentazione dettagliata delle API e delle interfacce CLI e GUI se previste dal servizio. Obiettivo Fornire gli elementi utili circa la presenza di documentazione tecnica al servizio e alle relative modalità di fruizione.

### **24. Policy specifiche**

#### **Portabilità, migrazione e transfer back dei dati**

Opiquad garantisce l'interoperabilità e la cancellazione dei dati (personali, non personali e/o comuni) attraverso un libero piano di migrazione mediante l'utilizzo di standard aperti (ad es. Open Virtualization Format) ed opportune Application Programming Interface (API).

Il Cliente avrà sempre la possibilità di poter migrare le proprie applicazioni, SaaS o IaaS, verso un altro fornitore Cloud in maniera semplice e sicura, in modo da garantire la possibilità di estrarre ed eventualmente eliminare permanentemente i propri dati in qualsiasi momento mediante opportuna interfaccia di gestione ed API.

#### **Diritti degli interessati**

Per quanto riguarda l'esercizio di diritti in materia di protezione dei dati personali Opiquad mette a disposizione degli utenti la casella [privacy@opiquad.it](mailto:privacy@opiquad.it), alla quale l'utente può fare riferimento per le diverse categorie di esercizio. Le e-mail inviate a tale indirizzo aprono automaticamente un ticket nel sistema, che viene gestito dagli operatori in base a delle categorie scelte. Anche la casella [dpo@opiquad.it](mailto:dpo@opiquad.it) è sempre disponibile per l'esercizio di tale richiesta, ma in questo caso è responsabilità diretta del Data Protection Officer (DPO) inserire il ticket nel sistema. La descrizione dei vari step operativi che compongono il workflow e la seguente:

1. Il richiedente (cliente/utente) invia una mail contenente la richiesta di esercizio dei diritti in merito alla protezione dei dati personali a [privacy@opiquad.it](mailto:privacy@opiquad.it),
2. La richiesta viene verificata dal Responsabile del Servizio.
3. Se la Richieste di Servizio (RdS) si dimostra attendibile, viene qualificata: accesso ai dati personali, richiesta di intervento sui dati, portabilità dei dati, opposizione al trattamento, o richiesta generica. Il ticket passa in stato "in elaborazione".
4. La RdS viene evasa entro un mese, in accordo a quanto previsto dalla legislazione. Nel caso non sia possibile evadere la richiesta e comunque necessario, ai sensi dell'art.12, par. 4 del GDPR fornire al richiedente i motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste, e in particolare di eventuali condizioni che impediscono al titolare di identificarlo come interessato, (art.11, par.2).
5. Al termine della corretta evasione delle RdS, il ticket viene chiuso a cura del Responsabile del Servizio. Le varie categorie di richieste per l'esercizio dei diritti in materia di protezione dei dati personali sono descritte nei paragrafi successivi

#### **Politica di conservazione**

Opiquad conserva i dati in Italia e solo su propri sistemi, non esporta quindi i dati fuori dal territorio Italiano ne cede a terzi i dati (se non su richiesta esplicita dell'autorità giudiziaria). I dati vengono conservati in locali costantemente monitorati e con accesso limitato mediante badge e con log degli accessi.

### **25. Garanzia di effettiva possibilità di controllo sul fornitore di servizi cloud**

Il Cliente, Titolare del trattamento è sempre in condizione di esercitare un effettivo potere di verifica sui trattamenti posti in essere da Opiquad con il limite dei diritti di proprietà industriale e intellettuale di costui, della protezione del know how, dei segreti industriali o di diritti privacy altrui.

### **26. Comunicazione, diffusione e trasferimento di dati**

26.1 Opiquad ottempera esclusivamente alle richieste di divulgazione dei dati dei clienti legalmente vincolanti. Se Opiquad dovesse ottemperare a una richiesta di questo tipo, ad esempio in caso di indagine penale, ne informerà sempre il cliente a meno che ciò non sia proibito per legge.

26.2 (ii) consulterà il corrispondente cliente del servizio cloud ove legalmente consentito prima di effettuare qualsiasi divulgazione di PII;

## **OPIQUAD SRL A SOCIO UNICO**

039 93 99 920 | [info@opiquad.it](mailto:info@opiquad.it) | [opiquad@pec.opiquad.it](mailto:opiquad@pec.opiquad.it)

Sede operativa: Via Bergamo, 60 – Merate 23807 (LC) | Sede legale: Via Pietro Paleocapa, 6 – Milano 20121 (MI)

Codice fiscale e Partiva Iva: IT 05866450967 | Codice SDI: M5UXCR1 | REA: MI – 1946731 | Capitale Sociale: € 90.000 i.v.

Società soggetta a direzione e coordinamento di **Opiquad Holding Srl**

26.3 (iii) accettare qualsiasi richiesta contrattualmente concordata per la divulgazione di PII autorizzata dal corrispondente cliente del servizio cloud.

26.4 Opiquad è autorizzata ad avvalersi di sub-fornitori per assisterla nella fornitura dei Servizi. Nell'ambito di tale assistenza, i sub-fornitori possono partecipare alle attività di trattamento dei dati effettuate da Opiquad su istruzione del Cliente. L'elenco dei sub-fornitori autorizzati a prendere parte alle attività di trattamento effettuate da Opiquad su istruzione del Cliente ("Sub-Responsabile(i) del trattamento"), inclusi i Servizi interessati e il luogo dal quale possono trattare i Dati Personali del Cliente ai sensi del Contratto sul Trattamento dati (DPA), è fornito (a) sul sito di Opiquad; ovvero (b) quando un Sub-Responsabile del trattamento prende parte solo ad uno specifico Servizio, nelle Condizioni Particolari di Servizio applicabili.

## **27. Supply Chain security: la gestione del rapporto con le terze parti**

L' Elenco dei subfornitori attivi è presente nel DPA attivo

<b>Email Backup</b>	<b>Assente</b>
<b>bWireless</b>	<b>Sendgrid</b>
<b>IaaS</b>	<b>Vmware Inc.</b>
<b>IaaS</b>	<b>Sangfor Technologies</b>
<b>Opivoice</b>	<b>Master Voice srl</b>
<b>DaD (Digital Asset Defender)</b>	<b>Eyeonid Group AB</b>

27.1 Opiquad si assicurerà che ogni Sub-responsabile del trattamento sia, quantomeno, in grado di rispettare gli obblighi sottoscritti da Opiquad nel Contratto di trattamento dati (DPA) all'uopo sottoscritto con il Cliente in riferimento al trattamento dei Dati Personali da parte del Sub-Responsabile del trattamento. A tale scopo, Opiquad sottoscriverà un accordo con il Sub-responsabile del trattamento, restando totalmente responsabile nei confronti del Cliente per qualsivoglia obbligo per il quale il Sub-responsabile del trattamento risulti inadempiente.

27.2 Così come previsto nel Contratto di trattamento dati (DPA) si ratifica che Opiquad è autorizzata a coinvolgere fornitori terzi (come fornitori di energia, di reti, gestori di punti di interconnessione di rete o centri dati collocati, fornitori di materiale o software, trasportatori, fornitori tecnici, società di sicurezza), ovunque si trovino, senza dover informare il Cliente del trattamento od ottenerne l'approvazione, nella misura in cui tali fornitori terzi non accedano ai dati personali del Cliente;

27.3 Prevede In ipotesi di autorizzazione generale al subappalto, l'obbligo di informare il cliente di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di propri subappaltatori, in modo tale da consentire al cliente di opporsi alla modifica;

27.4 In ipotesi di opposizione del cliente ad eventuali modifiche della filiera di fornitura la necessità di verifica, nell'ambito degli audit da parte del cliente, dei sub-fornitori effettivi.

Tale diritto di opposizione del cliente alla filiera di fornitura, nella prassi contrattuale riguardante i servizi Cloud, assume tipicamente la forma di un diritto di recesso senza costi o oneri accordato al cliente che dissenta rispetto all'utilizzo di subappaltatori diversi rispetto a quelli dichiarati e conosciuti al momento della stipulazione del contratto;

27.5 Qualora Opiquad decida di sostituire un Sub-Responsabile del trattamento o di introdurre un nuovo Sub-Responsabile del trattamento ("Sostituzione del Sub-Responsabile del trattamento"), Opiquad informerà il Cliente nel suo pannello di controllo o via e-mail (all'indirizzo e-mail registrato sul Profilo Cliente) (a) con trenta (30) giorni di anticipo se il Sub-Responsabile del trattamento è situato nell'Unione europea o in un paese che è soggetto a una Decisione di Adeguatezza, o (b) con novanta (90) giorni di anticipo in qualsiasi altro caso. Il Cliente ha il diritto di opporsi alla sostituzione di un Sub-Responsabile del trattamento come previsto dal Regolamento. L'opposizione deve essere notificata a Opiquad entro quindici (15) giorni dalla notifica della Sostituzione del Sub-Responsabile del trattamento da parte di Opiquad al Cliente e specificare il motivo della stessa. Tale opposizione dovrà essere notificata dal Cliente per iscritto al Responsabile della protezione dei dati, all'indirizzo telematico [dpd@opiquad.it](mailto:dpd@opiquad.it) . Opiquad non sarà in nessun caso obbligata a rinunciare ad una Sostituzione del Sub-Responsabile del trattamento. Se, a seguito dell'opposizione del Cliente, Opiquad non rinuncerà alla suddetta Sostituzione del Sub-Responsabile del trattamento, il Cliente avrà il diritto di interrompere i Servizi oggetto dell'opposizione.

## **28. Coperture assicurative**

Opiquad ha attiva una copertura assicurativa su eventuali incidenti che riguardano la protezione dei dati personali. L'assicurazione comprende la responsabilità civile ai sensi del D. Lgs. n. 196 del 30/6/2003 (Codice in materia di dati personali) per perdite patrimoniali cagionate a terzi, compresi i clienti e/o i dipendenti, in conseguenza dell'errato trattamento (raccolta, registrazione, elaborazione, conservazione, utilizzo, comunicazione e diffusione) dei dati personali di terzi.

## **OPIQUAD SRL A SOCIO UNICO**

039 93 99 920 | [info@opiquad.it](mailto:info@opiquad.it) | [opiquad@pec.opiquad.it](mailto:opiquad@pec.opiquad.it)

Sede operativa: Via Bergamo, 60 – Merate 23807 (LC) | Sede legale: Via Pietro Paleocapa, 6 – Milano 20121 (MI)

Codice fiscale e Partiva Iva: IT 05866450967 | Codice SDI: M5UXCR1 | REA: MI – 1946731 | Capitale Sociale: € 90.000 i.v.

Società soggetta a direzione e coordinamento di **Opiquad Holding Srl**

### **29. Attività di revisione e organismi di controllo**

29.1 Opiquad renderà disponibile al Cliente tutte le informazioni necessarie per (a) dimostrare il rispetto dei requisiti del Regolamento e (b) consentire lo svolgimento di eventuali attività di revisione. Tali informazioni potranno essere comunicate al Cliente a seguito di richiesta a Opiquad Support.

29.2 Qualora si tratti di Servizio certificato, rispettoso di un codice di condotta o soggetto a specifiche procedure di revisione, Opiquad renderà disponibili al Cliente i certificati corrispondenti o le relazioni sulle attività di revisione dietro richiesta scritta. Nel caso in cui suddette informazioni, relazioni e certificati si dimostrino insufficienti per consentire al Cliente di accertare il rispetto degli obblighi riportati nel Regolamento, Opiquad e il Cliente concorderanno quindi condizioni operative, di sicurezza e finanziarie per un'ispezione tecnica sul posto. Le condizioni di tale ispezione, tuttavia, non dovranno pregiudicare in alcun modo la sicurezza di altri clienti di Opiquad. Suddetta ispezione sul posto, nonché la comunicazione di certificati e relazioni sulla revisione, potrebbero ragionevolmente comportare una fatturazione aggiuntiva.

29.3 Qualunque informazione comunicata al Cliente nel rispetto di questa sezione e che non sia disponibile sul sito Web di Opiquad sarà considerata un'informazione riservata di Opiquad in base al Contratto. Prima di comunicare tali informazioni, il Cliente può essere tenuto a sottoscrivere uno specifico accordo di non divulgazione.

29.4 A prescindere da quanto sopra, il Cliente è autorizzato a rispondere a richieste di autorità di supervisione competenti, sempre che qualunque comunicazione di informazioni sia strettamente limitata a quanto sollecitato da suddetta autorità di supervisione. In tal caso, e salvo che non sia proibito dalla normativa vigente, il Cliente consulterà prima Opiquad in merito a tale richiesta di comunicazione di informazioni

29.5 Diritto di Audit: Opiquad riconosce al titolare il diritto di effettuare audit nei confronti dei responsabili, allo scopo di verificare e garantirsi il rispetto dei principi di protezione dei dati. Applicando tale previsione legislativa al contratto di cloud computing e dando atto che il CSP in tale contratto riveste il ruolo di responsabile ex art. 28, ne deriva che oggi il diritto di audit è automaticamente inserito nel contratto, indipendentemente dalla forza contrattuale delle parti: in sostanza oggi il titolare è, giuridicamente, posto nella condizione di effettuare un audit relativo alla protezione dei dati nei confronti del CSP.

### **30. Giurisdizione e responsabilità**

Le norme europee (regolamento CE n. 593/2008, sostitutivo della Convenzione di Roma del 19 giugno 1980, e Convenzione di Bruxelles) stabiliscono l'applicabilità al contratto di cloud computing della **legge dello Stato in cui risiede il consumatore**. Il presente Accordo sarà regolato, interpretato e applicato in conformità alle leggi italiane. Qualsiasi controversia derivante da o in relazione al presente Accordo sarà risolta, in via esclusiva, dal Tribunale di Milano.

### **31. Segnalazioni**

Per qualsiasi malfunzionamento o segnalazione, la cui responsabilità possa essere ricondotta a Opiquad, il Cliente ha la possibilità di contattare il supporto Opiquad utilizzando le coordinate presenti sul sito Opiquad.

Ogni richiesta o dichiarazione di incidente ricevuta con queste modalità dà luogo alla creazione di un ticket di supporto, inviando una email alla casella support-csi@opiquad.it. Il Cliente viene informato tramite un messaggio di posta elettronica della creazione del ticket e del numero corrispondente.

In caso di dichiarazione di un incidente, il Cliente comunica a Opiquad tutte le informazioni relative al problema riscontrato, per consentirle la corretta esecuzione della diagnostica.