

Allegato tecnico dei servizi SaaS de Il Dato Srl

Revisione	Data Revisione	Descrizione	Redatto	Approvato	Classificazione
01	29.07.2025	Prima Emissione	W. Persico	A. Chiesa	Usò Esterno
02	22.10.2025	Revisione	A. Chiesa	A. Chiesa	Usò Esterno

Sommario

1.	Nota di lettura	4
2.	Descrizione del servizio	4
2.1.	Definizioni e acronimi	4
2.2.	Descrizione generale	5
2.3.	Regole di ingaggio e Fruizione del servizio	6
2.4.	Licenze software	9
2.5.	Localizzazione del servizio e residenza dei dati	9
2.6.	Backup dei dati applicativi	9
2.7.	Logging e Monitoring	11
2.7.1.	Logging	11
2.7.2.	Monitoring	12
2.8.	Continuità operativa e Disaster Recovery	12
2.9.	Aggiornamenti software e manutenzioni programmate	13
2.10.	Evoluzione del servizio	14
2.11.	Gestione malfunzionamenti, incidenti di sicurezza e data breach	14
2.12.	Altre misure di sicurezza delle informazioni e compliance	15
3.	Attivazione del servizio	18
3.1.	Prerequisiti	18
3.2.	Richiesta di attivazione	19
3.3.	Tempistiche di attivazione	19
3.4.	Onboarding e configurazioni iniziali	19
3.5.	Decorrenza contrattuale	20
4.	Esercizio del servizio	20
4.1.	Ambito di responsabilità della Società	20
4.2.	Ambito di responsabilità del Cliente	20
4.3.	Continuità operativa	21

4.4.	Aggiornamenti e nuove versioni	21
4.5.	Audit e verifiche.....	21
5.	Gestione e Monitoraggio	22
5.1.	Livelli di servizio (SLA).....	22
5.2.	Monitoraggio del servizio	22
5.3.	Reportistica periodica	23
5.4.	Cessazione del servizio	23
6.	Servizio di Assistenza	23
6.1.	Canali di supporto	23
6.2.	Orari di disponibilità	23
6.3.	Classificazione delle richieste.....	24
6.4.	Flusso di gestione ticket	24

1. Nota di lettura

Il Dato S.r.l. si riserva la facoltà di aggiornare le misure tecniche e organizzative descritte nel presente allegato per garantire l'adeguamento a norme, linee guida e best practice di sicurezza. Eventuali modifiche non peggiorative degli impegni contrattuali potranno essere applicate senza preavviso; le variazioni che impattano la fruizione del servizio saranno comunicate con adeguato anticipo.

2. Descrizione del servizio

2.1. Definizioni e acronimi

- **SaaS (Software as a Service):** modello di erogazione in cui il software è fornito come servizio erogato via Internet, senza installazioni locali a carico del Cliente.
- **Servizio / Piattaforma:** l'applicazione cloud denominata Gestione Ospiti erogata da IL Dato S.r.l.
- **Tenant / Organizzazione:** l'ambiente logico assegnato al Cliente, isolato rispetto ad altri Clienti, identificato come Tenant/dominio.
- **Utente:** persona fisica abilitata ad accedere al servizio con credenziali personali.
- **Amministratore di Organizzazione:** utente del Cliente con privilegi di gestione (utenti, ruoli, configurazioni).
- **SLA (Service Level Agreement):** parametri e soglie che descrivono i livelli minimi di qualità del servizio (es. disponibilità, tempi di risposta).
- **Disponibilità/Uptime:** percentuale di tempo in cui il servizio è operativo e accessibile, al netto delle manutenzioni programmate.
- **Finestra di manutenzione:** intervallo temporale riservato agli interventi programmati.
- **Incidente:** evento che impatta disponibilità, integrità o riservatezza del servizio/dati.
- **Manutenzione correttiva/evolutiva/adattativa:** interventi per rimuovere difetti, introdurre funzionalità, adeguare ad ambienti/standard.
- **RPO/RTO:** obiettivi di perdita massima di dati (Recovery Point Objective) e tempo massimo di ripristino (Recovery Time Objective).

2.2. Descrizione generale

Le applicazioni costituenti la gamma di servizi Cloud che Il Dato distribuisce ed eroga in modalità SaaS, sono:

- Nome servizio (definito anche a listino o nei contratti) + breve descrizione
- idem

Attraverso la piattaforma SaaS vengono erogati i seguenti servizi:

- Gestione Ospiti
- GEV – Guardie Ecologiche ambientali
- Gestione articoli – DPI
- Gestione Impianti Sportivi
- SIG
- GAP
- Orti
- SUMO

L'eterogeneità di fruizione di tutti questi servizi Cloud permette ai sistemi che stanno alla base, di supportare multi-processi, gestire specificità ad hoc e dotarsi di un'architettura che fa della flessibilità e dell'integrabilità la sua stessa natura e ragione d'essere, con la possibilità di interfacciarsi con soggetti terzi tramite semplici configurazioni o implementazioni non invasive.

Tutti gli applicativi sopra riportati sono stati concepiti e sviluppati tramite l'ausilio di un Framework per lo sviluppo sicuro e rapido (RAD) implementato e adottato in azienda, in grado di fornire "out of the box" tutti gli strumenti necessari per sviluppare applicazioni moderne e sicure:

- In grado di assicurare alta disponibilità, scalabilità in modo dinamico;
- Progettati secondo i principi cardine della sicurezza by design e by Default;
- Accessibili via web con tecniche di accesso sicure e robuste
- Pensati per minimizzare l'onere gestionale del Cliente (nessuna gestione di sistemi operativi, DB o middleware);
- Sottoposti a cicli di aggiornamento continuo con rilascio controllato di patch e nuove funzioni;
- Concepiuti con Portali base in grado di supportare sistemi di autenticazione integrabile con gli più diffusi strumenti enterprise e protocolli per implementare il SSO (Windows AD, etc.);
- Utilizzo di componenti web standard (tabelle, input, combobox, grafici...) utilizzabili standalone o in componenti custom complessi;
- Dotati di Sistema di gestione di rotte e menu;

- Dotati di Sistema di gestione di diritti e profilazioni:
- In grado di assicurare protezione dei dati e conformità alle normative applicabili (es. GDPR)
- Predisposti per poter essere interfacciati con sistemi terzi esterni (del cliente, di altro provider di servizi cloud, etc.).

Tutti i prodotti proposti in modalità Cloud SaaS (vedi elenco), consentono al cliente di gestire e operare in autonomia su uno o più ambienti o istanze logiche dedicati (cosiddetto Tenant), all'interno di un pool di risorse virtuali ad esso assegnate. Si tratta pertanto di servizi Cloud per i quali Il Dato (in quanto Provider) rende disponibile e gestisce l'infrastruttura IT sulla quale vengono eseguiti i software che consentono al Cliente (Tenant) la creazione di una propria istanza logica in ambiente cloud, segregata da quella di ogni altro Cliente e da quella de Il Dato stesso, e rispetto alla quale il Tenant ha il totale controllo in autonomia delle risorse e funzionalità assegnate.

Al cliente per ogni applicativo viene assegnato un pool di risorse definite in termini di:

- GB di Storage (disco)
- Istanza DB
- Utenze per la gestione dell'ambiente (tenant anzitutto)

2.3. Regole di ingaggio e Fruizione del servizio

I vari servizi Cloud offerti da Il Dato, possono essere fruiti a seguito della stipula di un contratto tra Il Dato (Cloud Service Provider) e il Cliente, di cui il presente documento costituisce l'allegato tecnico. All'atto della adesione al servizio, il presente documento entra a far parte del contratto formale tra Il Dato e il Cliente e obbliga entrambe le parti a quanto di seguito indicato, nel rispetto dei reciproci ruoli e responsabilità.

Il Dato fornisce in seguito le modalità a cui si attiene nell'erogazione del/dei servizio/servizi contrattualizzati, unitamente ad un riepilogo in quanto cliente, degli adempimenti in capo allo stesso, e a quelli che Il Dato adotta e si impegna a garantire in qualità di fornitore di servizi cloud, in ottemperanza ai requisiti della norma tecnica ISO/IEC 27017.

Anzitutto il Cliente è tenuto a comunicare a Il Dato i riferimenti del proprio Referente Tecnico cui verrà assegnato il ruolo di amministratore del Tenant. Il Cliente dovrà comunicare eventuali variazioni nel tempo del proprio referente.

Il Dato srl è certificata ISO/IEC 27001:2022, ha un'adeguata allocazione dei ruoli e delle responsabilità in materia di sicurezza delle informazioni. Su esplicita richiesta del cliente Il Dato condividerà la versione più recente del documento "Il Dato - Ruoli e Responsabilità". Assicura che

è nelle condizioni di adempiere ai propri doveri in materia di presidio della sicurezza e protezione dei dati. A tal fine, sono condotte periodiche rivalutazioni dell'analisi dei rischi, eseguiti appropriati audit, anche tecnici (es. vulnerability assessment & Penetration test sui sistemi e applicativi di pertinenza) e dei riesami periodici che includono anche l'analisi e la valutazione delle performance, oltre che la qualità dell'erogazione.

Il Cliente che ritiene di modificare e/o integrare le prassi di controllo de Il Dato è tenuto a definire tali aspetti preventivamente, in uno specifico accordo tra le parti.

Il Dato ha identificato nel Garante della Privacy (GPDP), ACN (precedentemente Agid) e nella Polizia Postale le Autorità rilevanti per la protezione dei dati.

Salvo espressamente vietato dalla legge, se una Autorità Giudiziaria dovesse richiedere dati o informazioni del Cliente a Il Dato, quest'ultima si impegna a dare comunicazione al Cliente circa i dati/informazioni comunicati attraverso i contatti forniti (tipicamente mediante PEC) entro 2 giorni, salvo diverse disposizioni da parte dell'Autorità Giudiziaria.

I dati memorizzati nell'ambiente di cloud computing relativi ai diversi software proposti possono essere soggetti all'accesso e alla gestione da parte di Il Dato in qualità di Cloud Provider, ad esempio per gli accertamenti richiesti dall'autorità giudiziaria; a tutela del Cliente Il Dato adotta l'applicazione di metodi e processi certificati da enti terzi accreditati in ambito ISO 9001, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018.

Per ottemperare ai requisiti richiesti da regolamenti e dispositivi legislativi in materia di trattamento e protezione dei dati personali dei clienti (GDPR), Il Dato definisce e fa sottoscrivere degli accordi per il trattamento dei suddetti dati (il cui titolare è tipicamente il cliente), in qualità di Responsabile. I dati personali del cliente che venissero raccolti per l'erogazione del servizio non vengono in alcun modo trattati per finalità di marketing.

Rispetto ai vari prodotti proposti in modalità Cloud, l'accesso reso disponibile avviene via web. Per dettagli su come avviene l'accesso a ciascun prodotto si rimanda alla scheda prodotto specifica, allegata al presente documento.

La raggiungibilità di tali servizi è garantita attraverso link (url) pubblici (internet)-

L'accesso alle console web del singolo Tenant è possibile con procedura di autenticazione a più fattori (MFA). Tale accesso può essere integrato con un Identity provider a disposizione del cliente compatibile con le modalità previste dai singoli applicativi (vedi caratteristiche del singolo prodotto, sulla scheda prodotto allegata).

All'interno delle risorse assegnate (vedi punto precedente) il Cliente ha autonomia, attraverso il proprio Tenant (sempre via web), nel configurare il proprio ambiente cloud di lavoro, e per creare

utenze sotto il proprio controllo, e profilarle (assegnare diritti, anche differenziati per funzione) come meglio crede rispetto alle varie funzioni offerte dalle singole applicazioni della suite, attraverso il proprio utente amministratore (il Tenant).

A tal fine, Il Dato, per i vari applicativi cloud proposti, adotta diversi profili:

- Utenti “Superadmin”, ad uso esclusivo de Il Dato, per la gestione e la manutenzione dell’ambiente di cloud computing e della piattaforma applicativa interessata.
- Utenti “Admin” (del Tenant), ad uso esclusivo del Cliente, hanno accesso privilegiato con facoltà di modifica o variazione ad ogni livello e funzione.
- Utenti “User” standard ad uso del Cliente, possono eseguire un sottoinsieme di funzioni e/o operazioni stabilite dall’utenza Admin del tenant (es. le operazioni di gestione ordinaria come caricamento di pratiche, compilazione di documenti e elaborazione di report , etc..)
- Utenti “Visual” ad uso del Cliente, possono accedere al servizio in sola visualizzazione.
- Utenti di servizio che non possono fare login interattivo ma possono eseguire delle attività di manutenzione dei dati o di import/export su tabelle specifiche

Per ogni tipologia di utenza, viene adottata una policy password che prevede il cambio che può essere stabilito dal cliente e che comunque non può essere superiore a 6 mesi (password aging), pena la sospensione a tempo indeterminato; l’inibizione dell’utilizzo delle precedenti password (fino a 3 precedenti), definizione della stessa password con almeno 8 caratteri alfanumerici aventi al proprio interno almeno una lettera maiuscola, una minuscola, un carattere numerico e speciale (es. Punto esclamativo).

Si ricorda che il Cliente deve sempre utilizzare tecniche di autenticazione sufficientemente sicure per autenticare i profili ed eventuali servizi personalizzati riportati precedentemente; a tale scopo, opportune policy adottate da Il Dato per accedere ai propri servizi Cloud SaaS impediscono di usare credenziali deboli o inadatte allo scopo, oppure adottare tecnologie in grado di supportare tecniche crittografiche e protocolli più recenti e aggiornati; in ogni caso il cliente è tenuto a comunicare tempestivamente qualsiasi variazione degli utenti autorizzati e del loro ruolo.

Si invita il Cliente a verificare e garantire che l'accesso alle informazioni nel servizio cloud SaaS possa essere limitato in conformità con la sua politica di controllo degli accessi e che tali restrizioni siano realizzate.

Ciò include:

- La limitazione dell'accesso ai servizi cloud SaaS;
- Alle funzioni del servizio cloud SaaS;
- Ai dati dei clienti gestiti dal servizio cloud SaaS.

Per ciascun applicativo della gamma dei servizi cloud, Il Dato mette a disposizione dei Clienti documenti di supporto, guide o manuali per l'utilizzo della console di gestione (Vedi schede prodotto allegate).

Nel caso in cui il Cliente ritenga necessario lo svolgimento di un audit o ispezione presso Il Dato per verificare il rispetto degli adempimenti contrattuali in termini di sicurezza, occorre che la richiesta venga formalizzata tramite canali ufficiali (PEC o equivalente) e trasmessa con congruo anticipo (almeno 30 giorni solari) per consentire la pianificazione dell'attività, che non potrà comunque durare più di 8 ore.

2.4. Licenze software

Sono a carico de IL Dato (di cui detiene regolare possesso) tutte le licenze per il software e le librerie installate nell'ambiente Cloud utilizzato per l'erogazione del servizi cloud SaaS.

2.5. Localizzazione del servizio e residenza dei dati

Il Dato, nell'ambito dell'erogazione dei propri servizi Cloud, colloca i dati dei Clienti sempre e solo su sistemi di cloud computing posti all'interno dell'Unione Europea, nello specifico nei siti di erogazione del servizio ubicati presso il Data Center a Ponte San Pietro (BG) presso i locali di Aruba (provider di servizi di colocation), ed eventuali repliche o backup o disaster recovery presso "EL Storage" un rivenditore del servizio cloud storage "Wasabi", nel Datacenter di Amsterdam EU-Central-1.

Dunque, i dati sono trattati in Italia e archiviati all'interno della UE presso i 2 data center sopracitati. All'attivazione dell'erogazione del servizio viene selezionato il sito (Data center) di riferimento e contestualmente comunicato al cliente.

Il Dato si impegna a comunicare al Cliente, con adeguato preavviso, ogni variazione all'ubicazione dei siti in cui vengono mantenuti i propri dati.

2.6. Backup dei dati applicativi

Il Dato mantiene resiliente l'ambiente cloud dove eroga i propri servizi Cloud, eseguendo regolari Backup sui dati dei Clienti gestiti e mantenuti (vedi policy di default).

Tale funzionalità viene fornita nei confronti dei clienti, come parte integrante del servizio offerto.

Di seguito vengono elencati i vari aspetti e caratteristiche della policy adottata (da considerare la policy di default valida per tutti i servizi cloud offerti):

1. Prima modalità locale

- **frequenza:** durante l'orario lavorativo (dalle 8 alle 18 lun. – ven. e dalle 8 alle 13 sab.) ogni 2 ore con tecnologia di replica Veeam
- **Ambito:** backup dei **dati applicativi e configurazioni di Tenant**; non è previsto backup di asset non gestiti dal servizio.
- RPO: N ore 2
- RTO: 10 minuti
- Periodo di retention: 8 punti di ripristino pari a 1,5 giorni
- Destinazione: storage locale secondario

Seconda modalità locale

- frequenza: 1 volta al giorno, con tecnologia Backup Veeam
- Ambito: backup dei dati applicativi e configurazioni di Tenant; non è previsto backup di asset non gestiti dal servizio.
- RPO: N ore 24
- RTO: fino ad 1 ora
- Periodo di retention: 7 punti di ripristino pari a 7 giorni
- Destinazione: storage locale secondario

Modalità Cloud

- **frequenza:** 1 volta al giorno, con tecnologia Backup Veeam
- **Ambito:** backup dei **dati applicativi e configurazioni di Tenant**; non è previsto backup di asset non gestiti dal servizio.
- RPO: N ore 24
- RTO: fino ad 12 ore
- Periodo di retention: gli ultimi 7 giorni, le ultime 2 settimane, l'ultimo mese
- Destinazione: storage cloud

Qualora il cliente ravvisasse ulteriori o diverse necessità differenti rispetto la policy di default, queste andranno analizzate ed eventualmente preventivate separatamente come servizi aggiuntivi a parte. Le copie di backup vetuste vengono cancellate automaticamente da Il Dato al termine del periodo di conservazione stabilito (1 mese).

Su base periodica o a campione, Il Dato effettua test di restore sui backup eseguiti, al fine di verificare la loro disponibilità ed integrità in caso di scenario avverso. I backup prevedono accesso limitato al personale tecnico de Il Dato.

A fronte di una richiesta di ripristino, Il Dato si impegna a prenderla in carico entro [8 ore lavorative], di avviare la procedura di restore entro 8 ore lavorative, sulla base di un RPO pari a 24 ore.

Il Cliente in ogni caso può richiedere a Il Dato di effettuare fino a 2 test di restore annuali per verificarne l'efficacia. In tali casi Il Dato si impegna ad eseguire il test entro 2 giorni lavorativi, e a trasmettere al Cliente i report dei test eseguiti.

Il servizio viene presidiato da personale dedicato che controlla il corretto svolgimento della schedulazione, intervenendo tempestivamente in caso di problemi.

Il restore in caso di perdita di dati non immutabili a Il Dato, non può essere eseguito in autonomia dal Cliente, ma deve essere richiesto dal Referente Tecnico del Cliente tramite i canali messi a disposizione da Il Dato per il supporto tecnico (vedi sezione dedicata nel § 6).

Per nessun motivo Il Dato farà restore di Istanza DB del Cliente, se non a fronte di una richiesta ricevuta dal Cliente.

2.7. Logging e Monitoring

Attraverso il portale di accesso al servizio, è anche possibile visualizzare/reperire le informazioni di:

- Logging: tracciamento degli eventi rilevanti sulla gestione delle applicazioni in Cloud SaaS
- Monitoring: stato dei servizi e risorse del software cloud SaaS

2.7.1. Logging

Si tratta dei log rilevanti rispetto alla gestione degli applicativi erogati in cloud SaaS, ossia dell'attività di tracciamento e conservazione degli accessi logici, operazioni amministrative, eventi applicativi rilevanti ed eventi di sicurezza.

Ciò non toglie che il Cliente possa verificare se tale set di log sia sufficiente per le proprie esigenze, e in linea con le proprie politiche; diversamente, dovrà definire con Il Dato i requisiti per la registrazione degli eventi e verificare che il servizio cloud soddisfi tali requisiti.

Tali log per ciascun tenant vengono mantenuti disponibili per almeno 12 mesi.

La policy di logging prevede di default anche l'utilizzo di time-sync NTP su fonte affidabile. Come per il set di log, anche la retention è modificabile sulla base delle esigenze manifestate dal cliente. Il cliente che intende disporre e visualizzare i propri log generati, dovrà inoltrare una richiesta di assistenza tecnica, tramite gli opportuni canali predisposti (vedi § 5, più sotto).

Prossimamente verrà resa disponibile una Modalità alternativa di accesso e consultazione ai log, rappresentata da una funzione di esportazione [in formato CSV/JSON/Syslog] con filtro e

mascheramento ove necessario. Tale funzione sarà accessibile soltanto dagli utenti con ruolo Admin.

2.7.2. Monitoring

Il cliente al fine di poter assicurarsi la capacità di erogazione e continuità operativa ottimale ha accesso a funzionalità per verificare il corretto funzionamento e relative prestazioni del servizio cloud SaaS.

Il Dato infatti mette a disposizione adeguati strumenti. Da uno strumento terzo (Dashboard) sempre in gestione a Il Dato, infatti, è possibile eseguire il monitoraggio in tempo reale della disponibilità del servizio cloud e l'utilizzo delle risorse. Tutta la gestione e monitoraggio del servizio è affidata a Il Dato, che garantisce tempestiva segnalazione via email in merito ad anomalie di funzionamento o livelli critici di occupazione delle risorse computazionali assegnate, tramite il proprio sistema di monitoraggio.

Il cliente può chiedere report in merito allo stato delle risorse assegnate o in merito ad anomalie di funzionamento del servizio o di sicurezza, inoltrando una richiesta di assistenza o supporto tramite il servizio di ticketing (vedi allegato tecnico al § 6).

2.8. Continuità operativa e Disaster Recovery

Il Dato non adotta veri e propri sistemi di disaster recovery per la parte dei dati e/o informazioni, e per la parte di software e dei sistemi che ospitano l'ambiente Cloud. Per garantire una sorta di continuità operativa, esegue verifiche periodica delle copie dei dati archiviati (backup) in siti alternativi, avvalendosi della presenza e disponibilità di un sito secondario (ubicato presso "EL Storage" un rivenditore del servizio cloud storage "Wasabi"), oltre al principale, nel quale è ubicata l'infrastruttura IT che costituisce l'ambiente Cloud, vale a dire nel Datacenter primario di Aruba in Ponte San Pietro (BG).

La policy di continuità operativa adottata di default per i servizi Cloud offerti permette di ottenere le seguenti prestazioni:

- RTO: 4h in orario lavorativo (*);
- RPO: 4h (*).

Qualora il cliente ravvisasse ulteriori o diverse necessità differenti rispetto la policy di default, queste andranno analizzate ed eventualmente preventivate separatamente come servizi aggiuntivi.

Il Dato fornisce tali funzionalità e misure di resilienza del proprio servizio Cloud SaaS come parte integrante del servizio erogato per il cliente.

In ogni caso, la soluzione di resilienza adottata può solo essere attivata da parte de Il Dato, in caso di occorrenza di un evento disastroso al sito primario (DC) di produzione; Il Dato si impegna a informare tempestivamente il Cliente in tal caso.

IL Dato manterrà comunque costantemente aggiornato il Cliente sull'evoluzione della situazione fino alla conclusione dell'emergenza.

(*). Al di fuori dell'orario lavorativo il parametro diventa 24h.

2.9. Aggiornamenti software e manutenzioni programmate

Il Dato si riserva una finestra temporale per effettuare gli aggiornamenti software e le manutenzioni programmate del proprio ambiente cloud (comprese le installazioni di patch di sicurezza). Tipicamente tali interventi interessano i sistemi informativi alla base dell'erogazione dei servizi Cloud SaaS offerti (es: portale web di accesso, moduli software, sistemi di monitoraggio e raccolta metriche, etc..) e non impattano la funzionalità dei servizi Cloud e del relativo Tenant del cliente.

L'interruzione del servizio pur essendo solitamente breve, avviene solitamente in orario notturno e comunque al di fuori degli orari di punta (9-18) e, salvo casi eccezionali, viene notificata preventivamente al Cliente.

Eventuali manutenzioni di componenti infrastrutturali o aggiornamenti software impattanti che invece possano impattare sulla produzione per un tempo non definito (es. funzionalità dell'infrastruttura IT costituente l'ambiente Cloud, o della rete) vengono anch'essi comunicati al Referente Tecnico del Cliente, ma con almeno 3 giorni lavorativi di anticipo rispetto alla data di pianificazione, e fatti seguire da ulteriori comunicazioni all'avvio e alla conclusione dell'attività.

Solo eccezionalmente interventi urgenti inerenti la sicurezza possono essere effettuati senza preavviso se ritenuti particolarmente critici, ma con notifica a posteriori.

Schematizzando, si applicano i seguenti criteri:

- Patch di sicurezza: applicazione entro 7 giorni
- Change (es. Release funzionali): quando necessario; change log comunicato al cliente mezzo mail con preavviso di minimo 3 giorni.
- Finestra di manutenzione: lunedì mattina; durata tipica 30 min; attività impattanti comunicate con 3 giorni di anticipo.

2.10. Evoluzione del servizio

Al fine di garantire che l'ambiente cloud computing utilizzato per l'erogazione del servizio Cloud SaaS sia mantenuto sempre allineato allo stato dell'arte della tecnologia, e quindi l'evoluzione degli ambienti software in linea con i requisiti di sicurezza delle informazioni, IL Dato si impegna a predisporre adeguate e periodiche roadmap evolutive, di tipo infrastrutturale ed applicativo, in modo da permettere gli aggiornamenti dell'infrastruttura e del software con una continua valutazione e gestione del rischio.

Una roadmap applicativa continua può avvenire anche su richiesta dei clienti e/o su necessità adeguamento a livello normativo/legislative, che in ogni caso viene sempre condiviso con i Clienti.

2.11. Gestione malfunzionamenti, incidenti di sicurezza e data breach

Il Dato in qualità di Provider di servizi Cloud, assicura la gestione H24x365 dei malfunzionamenti e degli incidenti aventi impatto sulla disponibilità del servizio di Cloud SaaS o sull'integrità o riservatezza dei dati trattati da essi.

I malfunzionamenti/incidenti di competenza del Cloud service provider sono quelli relativi ai sistemi costituenti gli ambienti di cloud computing, le interfacce web di gestione, le reti di connettività interne e verso internet, ai log, agli attacchi informatici provenienti dall'esterno da parte di malintenzionati, fino ai furti di credenziali rispetto alle quali sia richiesta una azione rapida del provider (blocco, reset, etc.).

I malfunzionamenti/incidenti (inclusi quelli di sicurezza) possono essere rilevati sia attraverso un monitoraggio proattivo da parte de Il Dato sia tramite la ricezione di segnalazioni fatte pervenire dai Clienti attraverso i canali messi a disposizione da Il Dato per il supporto tecnico (vedi § 6 per dettagli).

Il Dato si impegna ad assicurare i livelli di servizio relativi alla risoluzione del malfunzionamento /incidente o più in generale al supporto tecnico, in base a quanto riportato al § 5, dipendenti dalla gravità ad esso assegnata (vedi anche § 6).

Il Dato per gli incidenti di sicurezza si è dotata di una specifica procedura scritta per la gestione degli incidenti di sicurezza delle informazioni e cyber, che viene condivisa con il cliente negli aspetti più essenziali. Il Cliente è così in grado di verificare se l'assegnazione delle responsabilità per la gestione degli incidenti di sicurezza delle informazioni e la relativa classificazione in base all'impatto sul servizio Cloud SaaS e sui dati in esso trattati (in termini di disponibilità, integrità e riservatezza), è adeguata e soddisfi i propri requisiti.

Il Cliente viene mantenuto aggiornato in relazione alla gestione del malfunzionamento/incidente di sicurezza fino alla sua risoluzione nelle seguenti modalità:

- In caso di segnalazione proveniente dal Cliente: attraverso i canali messi a disposizione (mail di supporto o help desk telefonico) o attraverso il sistema di ticketing a cui il Cliente può accedere autonomamente (vedi dettagli nel § 6);
- in caso di rilevazione da parte de Il Dato: tramite mail o telefonicamente al referente indicato successiva alla rilevazione del malfunzionamento/incidente di sicurezza e ulteriore mail successiva alla sua risoluzione (in caso di incidente grave, entro 24h da quando è stato rilevato o ne abbia avuto notizia).

In caso di eventi catastrofici, Il Dato ha previsto l'attivazione di una unità di crisi, che assume la responsabilità di dichiarare lo stato di "emergenza" e coordinare la gestione della stessa, comprese le comunicazioni verso l'esterno ovvero ai clienti, così come previsto nella procedura stessa di gestione degli incidenti. La gestione dell'emergenza può richiedere anche l'attivazione del Disaster Recovery, se ritenuto necessario.

Quando l'incidente si configura come violazione di dati personali (Data Breach), Il Dato procede in ottemperanza agli Art. 33 e 34 del Regolamento UE 2016/679 (GDPR) e in particolare attiva la propria procedura interna ricompresa all'interno della procedura di gestione incidenti di sicurezza, con le relative comunicazioni verso gli interessati e i Clienti, non oltre le 24h.

A seguito della risoluzione del malfunzionamento/incidente di sicurezza, Il Dato ne richiede una verifica da parte del Cliente prima della chiusura del caso (o ticket eventualmente aperto).

Altri aspetti presidiati e gestiti all'interno della già menzionata procedura sono in sintesi:

- Classificazione gravità: varia in base a impatto su disponibilità, integrità, riservatezza delle informazioni e dei servizi.
- Privacy: ruoli [Titolare/Responsabile], DPA/ATTO DI NOMINA disponibile; DPIA a cura del Titolare con supporto documentale del Fornitore.
- Data breach: gestione in conformità agli artt. 33–34 GDPR; notifica al Titolare entro 24 ore dal riscontro; notifica verso il Garante della Privacy entro le 72h; supporto alla valutazione del rischio e alle comunicazioni eventualmente dovute.

2.12. Altre misure di sicurezza delle informazioni e compliance

Al fine di garantire la conformità sia alle norme ISO/IEC 27001 e alle linee guida ISO/IEC 27017/27018, sia ai requisiti cogenti applicabili (in particolare GDPR, Misure Minime di Sicurezza ICT per le PA emanate da AgID, requisiti di qualificazione Agid per i CSP della PA), Il Dato si è

dotata di adeguate misure tecniche e organizzative, che provvede ad attuare, monitorare, correggere e migliorare in modo continuativo. Di seguito vengono sinteticamente riportate le principali misure adottate oltre a quelle già elencate nei punti precedenti:

- sicurezza fisica dei Data Center utilizzati (Aruba): videosorveglianza, impianto antintrusione, controllo accessi, servizio di vigilanza, etc..;
- sicurezza ambientale e delle infrastrutture di supporto dei data center utilizzati: impianto antincendio, sensori antiallagamento, impianto di condizionamento idronico ridondato, unità di condizionamento in row all'interno delle cage, impianto elettrico ridondato, sistemi di continuità elettrica e gruppo elettrogeno, esecuzione di manutenzioni preventive e test periodici;
- progettazione e implementazione delle infrastrutture IT costituenti gli ambienti di cloud computing e delle piattaforme software utilizzate per l'erogazione dei servizi di Cloud SaaS, e delle relative evoluzioni, al fine di garantire la continuità operativa tramite l'uso di ridondanze e meccanismi di alta affidabilità in tutti i componenti (es. facility, rete, server, storage, piattaforma di virtualizzazione, etc.);
- attività di sviluppo software in ambienti di test e produzione sicuri (adozione di framework noti e conosciuti) e separati, con utilizzo di dati di prova non reali (ambiente di test) (le operazioni di sviluppo sono governate da specifiche procedure interne che tengono conto di principi come la Security by design e dei migliori standard di riferimento per lo sviluppo sicuro, es. top 10 OWASP); su esplicita richiesta del cliente può essere condivisa la politica di sviluppo sicuro adottata da Il Dato;
- segregazione tra le risorse di amministrazione dell'infrastruttura di cloud computing e degli ambienti dei Tenant e dei dati in essi contenuti, anche a livello di logging e interfacce di gestione, attraverso l'uso di applicazioni multitenant per la gestione delle funzionalità, mantenendo un isolamento logico ad ogni livello;
- esecuzione di analisi e valutazioni dei rischi per la sicurezza delle informazioni con periodicità annuale o in caso di cambiamenti significativi (è presente una procedura di cancellazione management);
- utilizzo di un sistema di gestione degli asset e delle configurazioni centralizzato per tutte le componenti fisiche, virtuali, risorse logiche, software, etc. (l'inventario adottato da Il Dato tiene conto in particolare delle informazioni e delle risorse associate e archiviate nell'ambiente di cloud computing);
- identificazione ed etichettatura di ogni informazione dislocata nell'ambiente di cloud computing (un apposita procedura ne garantisce l'applicazione);

- politiche e procedure scritte per lo smaltimento sicuro o il riutilizzo degli asset e altre risorse IT (hardware, networking, etc.);
- procedure di cancellazione sicura dei dati dei clienti in caso di cessazione del servizio;
- gestione degli accessi ai sistemi e alle applicazioni da parte dei clienti e del provider: procedure per la registrazione/deregistrazione degli utenti e per l'assegnazione/revoca dei diritti di accesso, account individuali, adeguate password policy, protocolli di logon sicuri, registrazione e conservazione dei log degli accessi;
- utilizzo di procedure di autenticazione sicure basate su più fattori di autenticazione (client to webapp SaaS in particolare);
- cifratura dei dati in transito tramite l'adozione di protocolli che la implementano (es. TLS v.1.2+, SSH (con algoritmi AES – es. VPN o tecniche per la negoziazione chiavi RSA più recenti), RDP, etc..) o a riposo nei file system o e negli storage utilizzati nell'infrastruttura di Cloud Computing per l'erogazione del servizio Cloud SaaS (Bitlocker, AES 256) – vedi tabella 1 più sotto per dettagli;
- procedure per il controllo e la manutenzione dell'efficacia delle chiavi crittografiche e certificati per ciascuna fase del ciclo di vita (ossia generazione, modifica o aggiornamento, memorizzazione, ritiro, recupero, mantenimento e distruzione);
- presenza di sistemi e dispositivi di protezione a livello perimetrale (next generation firewall e IDS/IPS) in grado di controllare e filtrare il traffico di rete interessato;
- presenza di sistemi e dispositivi di protezione a livello di Host ed endpoint (EDR, XDR, etc.);
- presenza di sistemi e dispositivi di rilevamento e analisi dei log ed eventi di sicurezza più in generale, nonché di protezione interna (IDS, XDR, etc.), monitorato proattivamente 24x7h da un sistema di monitoraggio interno, in grado di notificare al CSP in modo opportuno, e in base alla severità, un eventuale evento di sicurezza dovesse manifestarsi;
- sincronizzazione del clock dell'infrastruttura cloud con una fonte di riferimento affidabile (Il Dato adotta una policy di sincronizzazione di tutti gli orologi aziendali, e ne verifica periodicamente l'applicazione, in modo da garantire che tutti i sistemi dell'ambiente di cloud computing sia sincronizzato);
- esecuzione periodica (almeno annualmente) di verifiche di sicurezza (es. vulnerability assessment (VA, WAS), penetration test (PT/WAPT) sull'ambiente di cloud computing (e relativi sistemi) e sui servizi applicativi erogati in modalità cloud esposti;

- rilevazione e gestione (remediation) delle vulnerabilità tecniche rilevate, che possono influenzare l'erogazione dei servizi cloud SaaS forniti (Il Dato adotta una specifica Policy di Vulnerability Assessment and remediation);
- attività di hardening dell'infrastruttura costituente l'ambiente di cloud computing e relativi sistemi (Il Dato a tal proposito adotta un proprio standard definito in template base, che prevede tecniche di hardening predefinite- ad esempio solo porte e protocolli dei servizi strettamente necessari, etc.);
- servizio di supporto tecnico ai clienti H9x5 gg (lavorativi) e sistema di trouble ticketing accessibile dai clienti per segnalazioni di malfunzionamenti e incidenti e per richieste di modifica di configurazioni di competenza del cloud service provider (trattato in dettaglio nel § 5);
- utilizzo di personale tecnico professionale e altamente qualificato, di cui viene assicurata la formazione continua e la consapevolezza in tema di continuità e disponibilità del servizio SaaS e della sicurezza delle informazioni;
- utilizzo di fornitori adeguatamente selezionati e qualificati, e le cui attività sono strettamente monitorate e tenute sotto controllo da personale qualificato.

Tabella 1 – protocolli crittografici adottati ai vari livelli da IL Dato

SERVIZIO	METODO CRITTOGRAFICO
Endpoint con sistema operativo Windows (desktop, laptop, etc..)	BitLocker (Advanced Encryption Standard, AES 256)
Protezione dati in transito e a riposo	Cifratura dati in transito: TLS per proteggere i flussi di dati da e verso i server, con autenticazione del server tramite chiave RSA a 2048 bit e cifratura della sessione con AES 256 Cifratura dati a riposo nei sistemi di storage: AES 256
VPN gestita da Firewall (Vpn concentrator e client)	Barracuda con supporto per AES 256 e TLS 1.2+
Comunicazione client cliente – applicativo SaaS	HTTPS (TLS 1.2+)

3. Attivazione del servizio

3.1. Prerequisiti

Per l'attivazione del servizio, il Cliente deve disporre di:

- Connettività Internet stabile con banda minima consigliata di **30 Mbps**
- Browser supportati: Chrome nelle ultime 2 versioni.

- Eventuali certificati digitali come meccanismo di autenticazione.
- Un referente tecnico-amministrativo designato, responsabile dei rapporti con Il Dato.

3.2. Richiesta di attivazione

La richiesta di attivazione di uno o più servizi (pacchetti) Cloud de Il Dato deve essere formalizzata tramite sottoscrizione di un contratto indicando:

- Quali componenti applicativi sono richiesti (compresi i dettagli sulle relative integrazioni);
- Denominazione e dati anagrafici del Cliente;
- Dati del referente tecnico sia amministrativo che business (nome, cognome, email, telefono);
- Dati del destinatario delle comunicazioni del cliente (o per conto di esso);
- Numero e tipologia di utenti iniziali da abilitare (il Tenant viene attivato di default);
- Eventuali configurazioni iniziali richieste (es. loghi, domini email, etc.);
- Nome del referente tecnico che sarà l'unica persona abilitato ad aprire ticket con il supporto e a segnalare eventuali richieste di integrazione o sviluppo
- Qualora siano necessarie delle stampe personalizzate, i template dei documenti comprensivi degli elementi grafici necessari

Le condizioni economiche del servizio vengono definite sulla base di risorse massime allocate per l'ambiente cloud del Cliente, e vengono definite al momento della stipula del contratto e successivamente modificabili su richiesta del Cliente stesso.

Il Cliente ha la possibilità di mantenere visibilità sulle risorse acquistate inoltrando una richiesta ai servizi di assistenza e supporto messi a disposizione da IL Dato.

3.3. Tempistiche di attivazione

Il Dato si impegna ad attivare il servizio entro 5 giorni lavorativi dalla sottoscrizione del contratto.

L'attivazione si considera conclusa con la consegna al Cliente delle credenziali amministrative e del completamento delle configurazioni operative iniziali sull'ambiente di produzione.

Qualora fossero necessarie configurazioni o richieste aggiuntive, i tempi saranno concordati tra le parti.

3.4. Onboarding e configurazioni iniziali

All'attivazione vengono fornite al Cliente:

- Credenziali di accesso per l'Amministratore di Organizzazione.

- Le credenziali sono consegnate via email con obbligo di cambio automatico al primo accesso.
- Viene impostato sull'utente dell'Amministratore di Organizzazione l'uso dell'MFA per l'autenticazione
- Manuale utente e guida rapida per la configurazione iniziale, eventualmente con sessioni formative dedicate.
- Assistenza dedicata per le fasi di avvio (inclusa nel contratto).
- Possibilità di richiesta assistenza tramite contatto di supporto (via mail o ticket su sistema dedicato al servizio)

3.5. Decorrenza contrattuale

La data di consegna delle credenziali amministrative costituisce data di inizio erogazione del servizio.

Da tale data decorrono fatturazione, SLA e obblighi contrattuali.

4. Esercizio del servizio

4.1. Ambito di responsabilità della Società

La Società IL Dato S.r.l. si impegna a garantire la gestione completa del servizio SaaS, comprendente:

- Disponibilità e funzionamento dei servizi cloud SaaS acquisiti.
- Gestione dell'infrastruttura sottostante (server, rete, storage, database).
- Monitoraggio proattivo del servizio a livello infrastrutture per rilevare anomalie e incidenti;
- Esecuzione e verifica dei backup secondo la policy definita al § 2.11.
- Supporto tecnico secondo i livelli di servizio descritti al § 5.
- Gestione degli incidenti di sicurezza e dei data breach in conformità al GDPR, con relative comunicazioni (vedi § 2.11);
- Applicazione delle patch e aggiornamenti di sicurezza: attuati in best effort prima possibile da Il Dato (vedi § 2.12);
- Le nuove versioni della piattaforma vengono rilasciate secondo la roadmap descritta al § 2.10.
- Il supporto e cooperazione verso il cliente per consentire l'esercizio dei diritti dell'interessato, in materia di trattamento, accesso, modifica e cancellazione di dati personali (PII).

4.2. Ambito di responsabilità del Cliente

Il Cliente è responsabile di:

- Configurazione e utilizzo delle funzionalità applicative messe a disposizione.
- Gestione delle proprie utenze (creazione, sospensione, cancellazione).
- Corretto uso del servizio in conformità alle normative vigenti (GDPR, copyright, ecc.).
- Qualità e legittimità dei dati caricati sulla piattaforma.
- Definizione e applicazione delle proprie policy interne di sicurezza e privacy.
- Collaborazione nella risoluzione degli incidenti segnalando tempestivamente malfunzionamenti o anomalie.

4.3. Continuità operativa

La Società garantisce l'erogazione continuativa del servizio con disponibilità minima del 99,5% su base mensile.

In caso di disservizi critici, verranno applicate le procedure di continuità e disaster recovery definite al § 2.11.

Eventuali eventi di forza maggiore (es. calamità naturali, blackout estesi, interruzioni di rete a livello nazionale) sono esclusi dagli SLA.

4.4. Aggiornamenti e nuove versioni

Gli aggiornamenti di sicurezza vengono applicati automaticamente dalla Società.

Le nuove versioni della piattaforma vengono rilasciate secondo la roadmap descritta al § 2.12.

Il Cliente riceverà comunicazione preventiva in caso di cambiamenti rilevanti o interruzioni programmate con almeno 3 giorni lavorativi di preavviso.

Alla comunicazione verrà data informazione anche della categoria di modifiche (infrastrutturali, funzionali, ecc.) e la descrizione tecnica delle modifiche.

4.5. Audit e verifiche

Il Cliente può richiedere verifiche/audit sul servizio previa comunicazione formale con almeno 30 giorni di preavviso.

L'attività sarà svolta nel rispetto delle misure di sicurezza e potrà avere durata massima di n. 4 ore.

Il Dato fornirà la documentazione necessaria a comprovare la conformità agli standard (es. certificazioni ISO, report di audit esterni).

5. Gestione e Monitoraggio

5.1. Livelli di servizio (SLA)

La Società garantisce i seguenti livelli di servizio per ciascuno prodotto cloud:

- Disponibilità/Uptime:
 - Obiettivo: 99,5% su base annua.
 - Finestra di erogazione: H24x365.
 - Esclusioni: manutenzioni programmate, eventi di forza maggiore, errori imputabili al Cliente.
- Tempo di presa in carico ticket di funzionamento dell'infrastruttura:
 - Gravità urgente (bloccante): risposta entro 30 minuti lavorativi.
 - Gravità alta (non bloccante): risposta entro 2 ore lavorative.
 - Gravità media: risposta entro 1 giorno lavorativo.
 - Gravità bassa: risposta entro 2 giorni lavorativi.
- Tempo massimo di risoluzione anomalie:
 - Gravità alta: entro 8 ore lavorative nel 95% dei casi.
 - Gravità media: entro 36 ore lavorative nel 95% dei casi.
 - Gravità bassa: entro 7 giorni lavorativi nel 95% dei casi.
- Supporto tecnico:
 - Disponibile tramite ticket 24x7 con visibilità sullo stato delle richieste.
 - Orari del supporto telefonico: lun-ven 8:00–17:30.

5.2. Monitoraggio del servizio

- La Società effettua monitoraggio proattivo delle componenti applicative e infrastrutturali, H24x365.
- Sono controllati indicatori quali: disponibilità del portale, tempi di risposta, errori applicativi, integrità dei dati.
- Il Cliente riceve su richiesta report periodici con i principali indicatori di performance.

- In caso di superamento delle soglie critiche, la Società apre automaticamente un ticket di incidente.

5.3. Reportistica periodica

- Con cadenza trimestrale, la Società fornisce report contenenti:
 - Statistiche di disponibilità del servizio.
 - Incidenti rilevati e tempi di risoluzione
 - Aggiornamenti software e manutenzioni effettuate.
 - Eventuali piani di miglioramento.

5.4. Cessazione del servizio

- Il Cliente può richiedere la cessazione del servizio 2 mesi prima della scadenza del contratto con comunicazione formale (es. via PEC o raccomandata).
- Entro 60 giorni dalla data di cessazione, la Società garantisce al Cliente la possibilità di esportare i dati nei formati standard CSV, PDF.
- Decorso tale termine, i dati saranno cancellati in modo sicuro e irreversibile secondo le policy di data sanitization adottate dalla Società.
- Al termine della cessazione, tutte le credenziali del Cliente saranno disattivate.

6. Servizio di Assistenza

6.1. Canali di supporto

La Società mette a disposizione del Cliente un servizio di helpdesk, accessibile tramite:

- Portale web <https://appsupport.ildato.it>
- Email: supporto@ildato.it .
- Telefono: 035 0432869

Tutti i canali di supporto sono collegati al sistema di **ticketing** centralizzato, che permette al Cliente di seguire lo stato della propria richiesta in tempo reale.

Questi riferimenti possono essere utilizzati anche per richieste documentali non direttamente riferite a disservizi o anomalie.

Per quanto riguarda segnalazioni inerenti la privacy, il contatto email è privacy@ildato.it

6.2. Orari di disponibilità

- Supporto telefonico standard: dal lunedì al venerdì, ore 8:30 – 17:30.
- Supporto tramite portale di gestione dei ticket e via email 24x7, con risposte automatizzate per le principali tipologie di disservizio.

6.3. Classificazione delle richieste

Le richieste vengono classificate secondo tre livelli di gravità:

- Gravità alta (bloccante):
 - indisponibilità completa del servizio o grave perdita di funzionalità;
 - tempi di presa in carico: entro 2 ore lavorative;
 - tempi di risoluzione: entro 8 ore lavorative.
- Gravità media (parzialmente bloccante):
 - malfunzionamenti che riducono le funzionalità principali, ma con workaround temporanei;
 - tempi di presa in carico: entro 1 giorno;
 - tempi di risoluzione: entro 36 ore .
- Gravità bassa (non bloccante):
 - problemi minori o richieste di chiarimento/documentazione;
 - tempi di presa in carico: entro 2 giorni lavorativi;
 - tempi di risoluzione: entro 7 giorni lavorativi

6.4. Flusso di gestione ticket

2. Apertura ticket da parte del Cliente tramite mail.
3. Classificazione della gravità da parte della Società.
4. Presa in carico da parte di un operatore di supporto.
5. Comunicazioni periodiche di aggiornamento fino alla risoluzione.
6. Richiesta di conferma al Cliente prima della chiusura del ticket.
7. Archiviazione e reportistica dell'incidente.