NOEVA — Datasheet di Sicurezza Cloud

Riferimento: ISO/IEC 27017:2015 — Controlli di sicurezza per i servizi cloud

Campo	Valore
Documento	Cloud Security Datasheet — ISO/IEC 27017
Fornitore del servizio	4D S.R.L.
Prodotto	NOEVA — Piattaforma AI SaaS
Versione documento	1.0
Data emissione	2025
Classificazione	Riservato — Uso certificazione
Destinatario	Ente certificatore / Auditor ISO 27001+27017

> *Il presente documento descrive le misure di sicurezza implementate da **4D S.R.L.** nell'erogazione del servizio cloud NOEVA, in conformità ai controlli specifici per i servizi cloud definiti dalla norma **ISO/IEC 27017:2015** ("Code of practice for information security controls based on ISO/IEC 27002 for cloud services").*
>
> *Il documento è redatto a supporto dell'estensione della certificazione ISO/IEC 27001 del cliente con il dominio cloud (ISO 27017) e fornisce evidenza dei controlli implementati lato **Cloud Service Provider (CSP)**.*

1. Identità del Fornitore e Descrizione del Servizio

1.1 Fornitore

Campo	Dettaglio
Ragione sociale	4D S.R.L.
Prodotto	NOEVA
Tipologia servizio	Software as a Service (SaaS)
Modello di deployment	Cloud pubblico (AWS) con VPC privata dedicata — vedi §1.3 per varianti
Contatto sicurezza	support@noeva.ai

1.2 Descrizione del Servizio

NOEVA è una piattaforma di intelligenza artificiale aziendale erogata in modalità **SaaS multi-tenant**, che fornisce:

- **Gestione documentale e Knowledge Base** — indicizzazione semantica, RAG (Retrieval Augmented Generation), ricerca AI
- **Workflow Automation e Agent AI** — agenti specializzati, automazione processi, esecuzione task complessi
- **Moduli verticali** — HR (timbratura, onboarding), Produzione (reparti zero carta), Finance (analisi bilanci), CRM
- **Dashboard e Analytics** — monitoraggio consumi, metriche operative
- **Integrazioni** — API aperte verso sistemi terzi

1.3 Modello di Responsabilità Condivisa (Shared Responsibility)

In conformità al controllo **CLD.6.3.1** della ISO/IEC 27017, le responsabilità di sicurezza variano in base al **modello di deployment** adottato. NOEVA supporta tre modelli:

Modelli di Deployment Supportati

Modello	Descrizione
SaaS Cloud (standard)	Tutta la piattaforma su infrastruttura AWS gestita da 4D S.R.L. (eu-west-1)
Hybrid — AWS Anywhere	Worker e processi specifici del Cliente istanziati su server fisici connessi tramite **AWS Anywhere** all'infrastruttura, mantenendo l'orchestrazione centrale su AWS cloud
On-Premise	Deploy completo della piattaforma NOEVA sull'infrastruttura fisica del Cliente (opzione enterprise su contratto dedicato)

Tabella Responsabilità per Modello di Deployment

Area	SaaS Cloud (CSP)	SaaS Cloud (Cliente)	Hybrid (CSP)	Hybrid (Cliente)	On-Prem (CSP)	On-Prem (Cliente)
Infrastruttura fisica	Sì — AWS (delegato)	No	Sì — Cloud centrale	Sì — Server fisici locali	No	Sì
Sicurezza rete e VPC	Sì	No	Sì — Cloud centrale	Sì — Rete locale	Condivisa — Linee guida	Sì
Hardening OS e container	Sì	No	Sì — Cloud centrale	Sì — Nodi locali	Condivisa — Linee guida	Sì
Sicurezza applicativa	Sì	No	Sì	No	Sì	No
Gestione identità piattaforma	Sì (framework)	Sì (utenti propri)	Sì (framework)	Sì (utenti propri)	Sì (framework)	Sì (utenti propri)
Contenuti caricati	No	Sì	No	Sì	No	Sì
Credenziali di accesso	No	Sì	No	Sì	No	Sì
Conformità uso dati (finalità)	No	Sì	No	Sì	No	Sì
Conformità uso dati (infrastruttura)	Sì	No	Sì — Cloud centrale	Sì — Nodi locali	Condivisa — Supporto	Sì
Configurazione workspace	Sì (strumenti)	Sì (configurazione)	Sì (strumenti)	Sì (configurazione)	Sì (strumenti)	Sì (configurazione)

> ***Legenda***: *Sì = responsabilità primaria | No = non applicabile | Condivisa = responsabilità condivisa con linee guida fornite da 4D S.R.L.*
>
> ***Nota sulla conformità uso dati***: *la responsabilità è **distinta per livello**. 4D S.R.L. (CSP) è responsabile della conformità del trattamento infrastrutturale (sicurezza, residenza, misure tecniche ex Art. 32 GDPR). Il Cliente (Titolare) è responsabile della conformità delle finalità del trattamento (base giuridica, consensi, categorie di dati trattati). Questa distinzione riflette il modello Titolare/Responsabile del GDPR Art. 28.*
>
> ***Riferimento normativo***: *ISO/IEC 27017:2015 — CLD.6.3.1 "Shared roles and responsibilities within a cloud computing environment"*

2. Architettura Tecnica dell'Infrastruttura Cloud

2.1 Cloud Provider e Localizzazione

Parametro	Valore
Cloud Provider primario	Amazon Web Services (AWS)
Regione primaria	eu-west-1 (Irlanda)
Residenza dei dati	100% Europa — nessun dato trasferito fuori UE
Modello di rete	VPC privata dedicata (Virtual Private Cloud)
Compute	Amazon EC2 (istanze in VPC privata)
Inferenza AI	Amazon Bedrock (eu-west-1)
CDN	Cloudflare (edge globale, uptime garantito 99,99%)

2.2 Architettura a Microservizi

La piattaforma NOEVA è costruita su un'architettura a **16 microservizi** indipendenti, ciascuno con responsabilità ben definita e isolamento a livello di rete:

Microservizio	Funzione
server-api	Gestione complessiva delle API, orchestrazione richieste client
agents	Server di gestione agenti AI, workflow AI, collegamento all'inferenza
inference-manager	Gestione e controllo del layer di inferenza AI (routing, throttling, fallback)
agents-ui	Interfaccia chat AI per gli utenti finali
client-noeva	Interfaccia principale della piattaforma NOEVA
vertical-interfaces	Interfacce verticali di prodotto
worker-api	Gestione delle code di processi asincroni
worker-heavy	Esecuzione di processi computazionalmente intensivi (elaborazioni batch, AI pesante)
langfuse	Log applicativi centralizzati (self-hosted), osservabilità AI
task-services	Microservizi dedicati all'esecuzione di task specifici di dominio

> ***Nota**: tutti i microservizi operano all'interno della VPC privata AWS eu-west-1. La comunicazione inter-servizio avviene su rete interna privata, non esposta a Internet.*

2.3 Stack Dati e Storage

Componente	Fornitore	Ruolo	Localizzazione
Database relazionale	Supabase (PostgreSQL)	Dati applicativi, utenti, metadati, embedding vettoriali	AWS eu-west-1 (Irlanda)

Componente	Fornitore	Ruolo	Localizzazione
Autenticazione	Supabase Auth	Gestione identità, sessioni, JWT	AWS eu-west-1 (Irlanda)
Object Storage	Supabase Storage	File e documenti caricati dai clienti	AWS eu-west-1 (Irlanda)
Cache / Sessioni	Redis Cloud	Caching temporaneo, gestione sessioni, ottimizzazione performance	AWS eu-west-1 (Irlanda)
Analytics / Log	ClickHouse	Analisi dati, logging tecnico, metriche	AWS eu-west-1 (Irlanda)
Log AI	Langfuse (self-hosted)	Osservabilità modelli AI, trace, metriche inferenza	AWS eu-west-1 (Irlanda)

> ***Nota**: tutti i componenti dello stack dati risiedono nella medesima regione AWS eu-west-1 (Irlanda), garantendo residenza dei dati 100% europea e latenza minima inter-componente.*
>
> ***Riferimento normativo**: ISO/IEC 27017:2015 — CLD.9.5.1 "Segregation in virtual computing environments", CLD.9.5.2 "Hardening of virtual computing environment"*

3. Sicurezza di Rete e Isolamento dell'Infrastruttura

3.1 Architettura di Rete

Tutta l'infrastruttura NOEVA è ospitata all'interno di una **VPC (Virtual Private Cloud) privata** su AWS eu-west-1. Le istanze EC2 che eseguono i microservizi non sono direttamente esposte a Internet.

Misure implementate:

- **VPC privata dedicata**: isolamento completo a livello di rete da altri tenant AWS
- **Security Groups**: regole di firewall a livello di istanza, con principio del minimo privilegio (least privilege) — ogni microservizio espone solo le porte strettamente necessarie
- **Subnet private**: i servizi interni (database, cache, worker) operano su subnet non raggiungibili da Internet
- **NAT Gateway**: il traffico in uscita dai servizi interni è mediato da NAT, senza IP pubblici esposti
- **CDN Cloudflare**: protezione DDoS, WAF (Web Application Firewall), terminazione TLS a livello edge prima di raggiungere l'infrastruttura AWS
- **Firewall e IDS**: sistemi di rilevamento intrusioni attivi sull'infrastruttura

3.2 Protezione del Traffico

Livello	Misura	Standard
Traffico client → CDN	TLS 1.2+ obbligatorio	HTTPS enforced
CDN → AWS	Connessione cifrata dedicata	TLS 1.2+
Inter-microservizi (VPC)	Comunicazione su rete privata interna	VPC internal routing
Applicazione → Database	Connessione cifrata	TLS (Supabase)
Applicazione → Redis	Connessione cifrata	TLS in transito
Applicazione → Bedrock	AWS SDK con autenticazione IAM	AWS SigV4

3.3 Protezione DDoS

- **Cloudflare** fornisce protezione DDoS fino a 1 Tbps (edge network globale, >200 PoP)
- In caso di attacchi oltre la capacità CDN, 4D S.R.L. non è responsabile per il downtime risultante (forza maggiore)
- Rate limiting applicativo: 60 richieste AI/minuto per utente

> ***Riferimento normativo**: ISO/IEC 27017:2015 — CLD.13.1.4 "Alignment of security management for virtual and physical networks"; ISO/IEC 27002 — 13.1 Network security management*

4. Controllo degli Accessi e Gestione delle Identità

4.1 Autenticazione

Meccanismo	Dettaglio
Autenticazione utenti	Username + password (hash sicuro) tramite Supabase Auth
Complessità password	Policy di password complesse enforced a livello applicativo
2FA	Autenticazione a due fattori disponibile
Sessioni	Token JWT con scadenza, gestiti tramite Supabase Auth + Redis
Revoca accessi	Revoca immediata sessioni attive in caso di compromissione

4.2 Autorizzazione e Controllo Accessi Applicativo

NOEVA implementa un modello di autorizzazione **multi-livello e capillare**, che copre ogni risorsa della piattaforma:

Livello 1 — Separazione per Organization

Ogni cliente opera all'interno di una **Organization** isolata. Non è possibile accedere a dati di Organization diverse.

Livello 2 — Separazione per Workspace

All'interno di una Organization, i dati sono ulteriormente segmentati per **Workspace**. Gli utenti hanno accesso solo ai Workspace per cui sono stati esplicitamente autorizzati.

Livello 3 — Row Level Security (RLS) sul Database

Il database PostgreSQL (Supabase) implementa **Row Level Security (RLS)** a livello di database engine. Ogni query è automaticamente filtrata in base all'identità dell'utente autenticato: è impossibile, anche in caso di bug applicativo, che un utente acceda a righe di dati di un altro tenant.

Livello 4 — Bucket Storage con Regole di Visibilità

I file e documenti caricati sono archiviati in **bucket separati per Organization/Workspace**, con regole di visibilità che impediscono l'accesso cross-tenant a livello di storage object.

Livello 5 — Autorizzazioni Funzionali per Utente

Le autorizzazioni applicative sono gestite a livello di **singolo utente nominativo**, con controllo granulare su:

- Funzionalità accessibili (moduli, azioni)
- Accesso alle informazioni (documenti, knowledge base)
- Interrogazioni AI (il contesto AI rispetta i permessi dell'utente richiedente)
- Accesso fino al **singolo file** all'interno di un workspace

4.3 Principio del Minimo Privilegio

- Ogni microservizio dispone solo delle credenziali e dei permessi strettamente necessari alla propria funzione

- Le credenziali di accesso ai servizi interni (DB, Redis, Bedrock) sono gestite tramite variabili d'ambiente cifrate e IAM roles AWS
- Nessun microservizio ha accesso diretto a dati di altri tenant

4.4 Accesso Amministrativo

- L'accesso amministrativo all'infrastruttura è limitato al personale autorizzato di 4D S.R.L.
- Tutto il personale con accesso ai sistemi è vincolato da accordi di riservatezza (NDA) e ha ricevuto formazione GDPR
- 4D S.R.L. **non accede ai contenuti del Cliente** salvo: supporto tecnico su richiesta esplicita, indagini su violazioni di sicurezza, obblighi di legge

> ***Riferimento normativo**: ISO/IEC 27017:2015 — CLD.9.5.1 "Segregation in virtual computing environments"; ISO/IEC 27002 — 9.1 Business requirements of access control, 9.4 System and application access control*

5. Crittografia e Protezione dei Dati

5.1 Crittografia in Transito

Tutti i dati in transito tra client e piattaforma, e tra i componenti interni, sono protetti da crittografia:

Flusso	Protocollo	Note
Client → Cloudflare CDN	TLS 1.2 / TLS 1.3	HTTPS enforced, HSTS
Cloudflare → AWS	TLS 1.2+	Connessione cifrata end-to-end
Microservizi → Supabase DB	TLS	Connessione cifrata PostgreSQL
Microservizi → Redis	TLS	Crittografia in transito
Microservizi → AWS Bedrock	HTTPS + AWS SigV4	Autenticazione IAM + cifratura
Microservizi → ClickHouse	TLS	Connessione cifrata

5.2 Crittografia a Riposo

Componente	Crittografia	Standard
Database PostgreSQL (Supabase)	Cifratura a riposo	AES-256 (AWS EBS encryption)
Object Storage (Supabase Storage)	Cifratura a riposo	AES-256 (AWS S3 SSE)
Backup	Backup cifrati	AES-256
Redis	Dati volatili (non persistenti primari)	Cifratura in transito
EC2 EBS Volumes	Cifratura disco	AES-256 (AWS KMS)

5.3 Gestione delle Chiavi

- Le chiavi di cifratura sono gestite tramite **AWS Key Management Service (KMS)**
- Rotazione delle chiavi gestita secondo le policy AWS KMS
- Nessuna chiave di cifratura è esposta nei log o nelle variabili d'ambiente in chiaro

5.4 Zero Data Training

I dati dei clienti **non vengono mai utilizzati per addestrare modelli AI pubblici o di terze parti**. L'elaborazione tramite Amazon Bedrock avviene in modalità inference-only, senza persistenza dei dati di input/output sui sistemi dei provider AI.

> ***Riferimento normativo**: ISO/IEC 27017:2015 — CLD.10.1.1 "Policy on the use of cryptographic controls for cloud services"; ISO/IEC 27002 — 10.1 Cryptographic controls*

6. Segregazione e Isolamento dei Dati (Multi-Tenancy)

6.1 Modello Multi-Tenant

NOEVA è una piattaforma **multi-tenant** che garantisce l'isolamento completo dei dati tra clienti diversi attraverso un modello a tre livelli:

```
Organization (Tenant)
  |-- Workspace (Sotto-tenant)
        |-- Utenti nominativi (con permessi granulari)
              |-- File / Documenti (con visibilità per-file)
```

6.2 Meccanismi di Isolamento

Meccanismo	Livello	Descrizione
Separazione logica per Organization	Applicativo	Ogni Organization è un namespace isolato
Separazione per Workspace	Applicativo	Workspace indipendenti all'interno di una Organization
Row Level Security (RLS)	Database	PostgreSQL RLS: ogni query restituisce solo dati del tenant autenticato
Bucket separati	Storage	File archiviati in bucket distinti con policy di accesso per Organization/Workspace
Regole di visibilità file	Applicativo	Controllo accesso fino al singolo file all'interno di un workspace
Contesto AI isolato	AI Layer	Le interrogazioni AI rispettano i permessi dell'utente: nessun dato cross-tenant nelle risposte

6.3 Garanzie di Non-Interferenza

- Un utente autenticato in una Organization **non può** accedere, visualizzare o interrogare dati di un'altra Organization, nemmeno tramite API dirette
- Il layer RLS è implementato a livello di **database engine** (non solo applicativo), garantendo isolamento anche in caso di vulnerabilità applicative
- I bucket di storage hanno policy IAM che impediscono l'accesso cross-tenant a livello di AWS

> ***Riferimento normativo**: ISO/IEC 27017:2015 — CLD.9.5.1 "Segregation in virtual computing environments"; CLD.8.1.3 "Protection and separation of the cloud service customer's virtual environment"*

7. Monitoraggio, Logging e Gestione degli Incidenti

7.1 Logging Centralizzato

NOEVA implementa un sistema di logging centralizzato e multi-livello:

Sistema	Tipologia Log	Retention
Langfuse (self-hosted)	Log applicativi AI, trace agenti, metriche inferenza	Configurabile
ClickHouse	Log tecnici, analytics, metriche di sistema	Configurabile
Supabase	Log accessi database, query audit	Configurabile
AWS CloudWatch	Log infrastruttura EC2, VPC flow logs	90 giorni (default AWS)
Cloudflare	Log accessi CDN, richieste HTTP, eventi WAF	Configurabile

> *__Nota__: Langfuse è deployato in modalità __self-hosted__ all'interno della VPC NOEVA, garantendo che i log AI non escano dall'infrastruttura controllata da 4D S.R.L.*

7.2 Monitoraggio Disponibilità

- **Availability monitoring automatizzato**: uptime misurato in tempo reale
- **Status page**: comunicazione proattiva agli utenti in caso di incidenti
- **Alert automatici**: notifiche al team operativo per anomalie di sistema
- **Dashboard consumi**: i clienti hanno visibilità in tempo reale sui propri consumi (storage, token AI) con alert automatici all'80% della soglia

7.3 Gestione degli Incidenti di Sicurezza

Fase	Azione	Tempistica
Rilevamento	Monitoraggio automatizzato + alert	Continuo
Classificazione	P1 (critica) → P4 (bassa)	Immediato
Prima risposta P1	Presa in carico	Entro 4 ore lavorative
Risoluzione P1	Target risoluzione	Entro 16 ore lavorative
Notifica Data Breach	Comunicazione al Titolare	Senza ingiustificato ritardo (≤72h per GDPR)
Post-mortem	Analisi causa radice e azioni correttive	Entro 5 giorni lavorativi

7.4 Notifica Data Breach

In caso di violazione dei dati personali (Data Breach), 4D S.R.L. si impegna a:

1. Notificare il Cliente (Titolare del trattamento) **senza ingiustificato ritardo**

2. Fornire tutte le informazioni necessarie per la notifica all'Autorità di controllo (Garante Privacy) entro **72 ore** dall'accertamento
3. Documentare l'incidente nel Registro dei Trattamenti
4. Implementare misure correttive per prevenire il ripetersi dell'evento

> ***Riferimento normativo**: ISO/IEC 27017:2015 — CLD.12.1.5 "Monitoring of cloud services"; CLD.12.4.5 "Monitoring of cloud service administrator activities"; ISO/IEC 27002 — 16.1 Management of information security incidents*

8. Continuità Operativa e Service Level Agreement

8.1 SLA Garantiti

Metrica	Target	Misurazione
Uptime mensile	≥ 99,0%	Availability monitoring automatizzato
Uptime annuale	≥ 98,8%	Media ponderata 12 mesi
Downtime massimo mensile	≤ 7h 18min	Calcolato su mese calendario
Disponibilità endpoint AI	≥ 98,0% mensile	Monitoring dedicato
Fallback AI automatico	Entro 60 secondi	Switch provider alternativo

8.2 Latenze API Garantite

Operazione	P50	P95	P99
Autenticazione	< 100ms	< 200ms	< 500ms
Lettura dati	< 150ms	< 300ms	< 800ms
Scrittura dati	< 200ms	< 400ms	< 1.000ms
Ricerca RAG	< 500ms	< 1.500ms	< 3.000ms
AI Chat (risposta breve ~200 token)	—	—	< 5s (P90)
AI Chat (risposta lunga ~1000 token)	—	—	< 15s (P90)

8.3 Resilienza e Disaster Recovery

Componente	Misura	Dettaglio
Architettura compute	Multi-AZ	Ridondanza geografica dentro regione eu-west-1
Database	Backup automatici cifrati	Supabase backup con replica
Disaster Recovery	Backup datacenter secondario	Regione EU diversa dalla primaria
AI Inference	Fallback automatico	Switch su provider alternativo entro 60s, retry logic fino a 3 tentativi
CDN	Cloudflare edge	>200 PoP globali, uptime 99,99%

8.4 Manutenzioni Programmate

- **Frequenza massima**: 4 manutenzioni/mese
- **Durata massima**: 4 ore per manutenzione
- **Finestra preferenziale**: Sabato 22:00 – Domenica 06:00 CET
- **Preavviso**: minimo 7 giorni via email

- **Manutenzioni d'emergenza** (patch sicurezza critiche): preavviso ridotto 24h

> ***Riferimento normativo**: ISO/IEC 27017:2015 — CLD.17.2.2 "Availability of the cloud service"; ISO/IEC 27002 — 17.1 Information security continuity*

9. Gestione dei Sub-Responsabili (Sub-Processors)

In conformità all'Art. 28(2) GDPR e al controllo **CLD.6.3.1** ISO 27017, 4D S.R.L. si avvale dei seguenti sub-responsabili autorizzati per l'erogazione del servizio NOEVA. Per ciascuno sono indicate le garanzie di sicurezza e conformità.

9.1 Elenco Sub-Responsabili Autorizzati

Amazon Web Services (AWS)

Campo	Dettaglio
Fornitore	Amazon Web Services EMEA SARL
Ruolo	Cloud Infrastructure Provider
Servizi utilizzati	EC2 (compute), VPC (rete), Bedrock (inferenza AI), KMS (chiavi), CloudWatch (log)
Localizzazione dati	eu-west-1 (Irlanda)
Certificazioni	ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3, CSA STAR
Conformità GDPR	Data Processing Addendum AWS, Standard Contractual Clauses

Supabase

Campo	Dettaglio
Fornitore	Supabase Inc.
Infrastruttura sottostante	Amazon Web Services (eu-west-1)
Ruolo	Database, Autenticazione, Object Storage
Servizi utilizzati	PostgreSQL con RLS, Supabase Auth, Supabase Storage
Localizzazione dati	AWS eu-west-1 (Irlanda)
Garanzie	Data Processing Agreement Supabase, crittografia a riposo e in transito, hosting su AWS EU

Redis Cloud

Campo	Dettaglio
Fornitore	Redis Ltd.
Ruolo	Caching temporaneo, gestione sessioni, ottimizzazione performance
Natura dei dati	Dati volatili e temporanei (non archiviazione persistente primaria)
Localizzazione dati	AWS eu-west-1 (Irlanda)
Garanzie	Crittografia in transito, hosting su AWS eu-west-1

ClickHouse

Campo	Dettaglio
Fornitore	ClickHouse Inc.
Infrastruttura sottostante	Amazon Web Services (eu-west-1)
Ruolo	Analisi dati, logging tecnico, metriche di sistema
Natura dei dati	Dati di monitoraggio e analisi tecnica (non dati business primari)
Localizzazione dati	AWS eu-west-1 (Irlanda)

9.2 Obblighi Contrattuali verso i Sub-Responsabili

4D S.R.L. impone contrattualmente a ciascun sub-responsabile:

- Obblighi di protezione dei dati equivalenti a quelli del DPA con il Cliente
- Divieto di sub-affidamento ulteriore senza autorizzazione
- Obbligo di notifica in caso di data breach
- Diritto di audit da parte di 4D S.R.L.

4D S.R.L. **resta pienamente responsabile** verso il Cliente per l'adempimento degli obblighi di ciascun sub-responsabile.

> ***Riferimento normativo**: ISO/IEC 27017:2015 — CLD.6.3.1; GDPR Art. 28(2); ISO/IEC 27002 — 15.1 Information security in supplier relationships*

11. Riepilogo Controlli ISO/IEC 27017:2015

La tabella seguente riepiloga la copertura dei controlli specifici cloud della ISO/IEC 27017:2015 da parte di NOEVA:

Controllo	Titolo	Stato	Sez. rif.
CLD.6.3.1	Ruoli e responsabilità condivise nell'ambiente cloud	Implementato	§1.3
CLD.8.1.3	Protezione e separazione dell'ambiente virtuale del cliente	Implementato	§6
CLD.8.1.5	Restituzione e rimozione degli asset del cliente	Implementato	§10.1
CLD.9.5.1	Segregazione negli ambienti di computing virtuale	Implementato	§6.2
CLD.9.5.2	Hardening dell'ambiente di computing virtuale	Implementato	§2, §3
CLD.10.1.1	Policy sull'uso dei controlli crittografici per i servizi cloud	Implementato	§5
CLD.12.1.5	Monitoraggio dei servizi cloud	Implementato	§7.1, §7.2
CLD.12.4.5	Monitoraggio delle attività dell'amministratore del servizio cloud	Implementato	§7.1
CLD.13.1.4	Allineamento della gestione della sicurezza per reti virtuali e fisiche	Implementato	§3
CLD.16.1.3	Notifica delle violazioni dei dati	Implementato	§7.4
CLD.17.2.2	Disponibilità dell'infrastruttura di elaborazione delle informazioni	Implementato	§8
CLD.18.1	Conformità ai requisiti legali e contrattuali	Implementato	§10

12. Gestione della Restituzione e Cancellazione dei Dati

In conformità al controllo **CLD.8.1.5** della ISO/IEC 27017 e all'Art. 28 GDPR:

12.1 Restituzione dei Dati

Su richiesta del Cliente, 4D S.R.L. fornisce:

- Export dei dati in formato standard (CSV, JSON, PDF secondo il tipo di dato)
- Accesso ai documenti caricati tramite funzionalità di download della piattaforma
- Supporto tecnico per l'estrazione massiva dei dati in caso di migrazione

12.2 Cancellazione dei Dati

Al termine del contratto o su richiesta esplicita del Cliente:

5. **Cancellazione logica immediata**: i dati non sono più accessibili dalla piattaforma
6. **Cancellazione fisica**: i dati vengono rimossi dai sistemi di storage entro i termini contrattuali

7. **Backup**: i backup cifrati vengono eliminati secondo il ciclo di retention configurato
8. **Attestazione**: 4D S.R.L. fornisce attestazione scritta dell'avvenuta cancellazione su richiesta

12.3 Portabilità dei Dati

Il Cliente mantiene la piena proprietà dei propri Contenuti (documenti, dati, configurazioni) per tutta la durata del contratto e ha diritto alla portabilità in qualsiasi momento.

13. Dichiarazione del Fornitore

Il presente documento è emesso da **4D S.R.L.**, fornitore del servizio cloud NOEVA, a supporto del processo di certificazione ISO/IEC 27017 del Cliente.

Le informazioni contenute nel presente datasheet riflettono le misure di sicurezza implementate e mantenute da 4D S.R.L. nell'erogazione del servizio NOEVA alla data di emissione del documento.

4D S.R.L. si impegna a:

- Mantenere e migliorare continuamente le misure di sicurezza descritte
- Notificare il Cliente in caso di modifiche sostanziali all'architettura di sicurezza
- Fornire documentazione aggiuntiva su richiesta dell'auditor
- Supportare il processo di audit del Cliente con evidenze tecniche

Campo	Valore
Fornitore	4D S.R.L.
Servizio	NOEVA — Piattaforma AI SaaS
Contatto	support@noeva.ai
Versione documento	1.0
Data	2025
Classificazione	Riservato — Uso certificazione

Documento generato per supporto alla certificazione ISO/IEC 27001 + ISO/IEC 27017. Tutti i riferimenti normativi sono alla versione vigente delle norme citate.