DOCUMENTAZIONE A SUPPORTO DEL TITOLARE

TRATTAMENTO DATI RELATIVI AL CRM MEDICO (OCUSUITE)

Documento aggiornato il 30 Settembre 2024

Supernova Data

Cell. +39 379 1888864
Tel. +39 06 86726510

Lungotevere dei Mellini, 45 – 00193 Roma, Italia

www.supernovadata.com
info@supernovadata.com

SOMMARIO

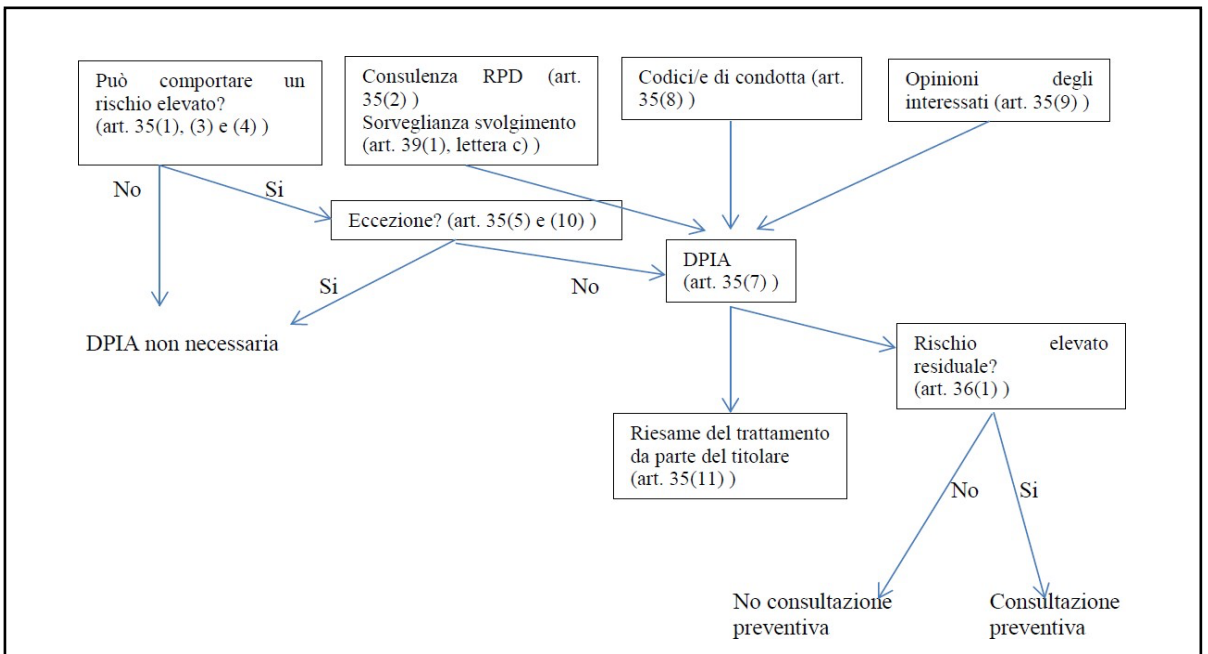
1. PREMESSA

La Valutazione d'Impatto sulla Protezione dei Dati (di seguito "DPIA) è un processo che il Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in particolare connesso all'impiego di nuove tecnologie, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone.

Il processo di DPIA è ritenuto uno degli aspetti di maggiore rilevanza nel nuovo quadro normativo definito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), in quanto esprime chiaramente la responsabilizzazione (c.d. accountability) del titolare nei confronti dei trattamenti dallo stesso effettuati.

Il Titolare del trattamento, infatti, è tenuto non solo a garantire l'osservanza delle disposizioni regolamentari, quanto anche a dimostrare adeguatamente in che modo egli garantisca tale osservanza.

Supernova Data S.r.l., nel suo ruolo di Responsabile del trattamento per la gestione del sistema di CRM MEDICO, con il presente documento intende fornire tutti gli elementi ai Titolari per svolgere la valutazione di impatto così come previsto dall'art. 35 del Regolamento.



Principi fondanti il processo di DPIA

2. DESCRIZIONE DELLA PIATTAFORMA CRM MEDICO

Supernova Data S.r.l., in qualità di responsabile del trattamento, si occupa della implementazione e manutenzione di un Software Gestionale per Studi Medici denominato "**OCUSITE**" per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.

ARCHITETTURA DI SISTEMA

Il sistema è composto da diverse componenti software, tra cui moduli e database. I database sono ridondanti e vengono salvati con copie di backup quotidiane, situate su istanze separate residenti sullo stesso server virtuale. Ogni componente software, sia i moduli che i database, risiede su server virtuali all'interno di infrastrutture cloud commerciali, nello specifico su Amazon Web Services (AWS).

SOFTWARE IMPIEGATO

Il **Software Gestionale per Studi Medici** "OCUSUITE" è un'applicazione cloud accessibile tramite qualsiasi browser web. Questo software è ospitato su server remoti e vi si accede tramite una connessione internet protetta dal protocollo HTTPS.

ARCHITETTURA DI RETE

Le macchine virtuali sono localizzate del data center afferente alla Region di Milano di AWS: i backup degli schemi dei database, come anche i file caricati dagli utenti del gestionale, sono effettuati quotidianamente con una retention di 15 giorni, su storage S3 (cifrati da AWS). Inoltre, viene effettuata, quotidianamente, una copia di backup, con retention 3 giorni, dell'intera macchina virtuale. (il disco della macchina virtuale non è cifrato al momento).

3. DESCRIZIONE E ANALISI DEL CONTESTO

Responsabilità connesse al trattamento	**Committente** > Titolare del trattamento **Utilizzatori** > Soggetto autorizzati dal Titolare del Trattamento **Supernova Data srl** > Responsabile del trattamento per la fornitura e la gestione del Software Gestionale per Studi Medici "**OCUSUITE**" **AWS** > Sub-Responsabile del trattamento, nominato da **Supernova Data S.r.l.,** per la gestione dell'infrastruttura (IaaS)
Standard applicabili	Il contesto normativo di riferimento richiede conformità a: ● Regolamento UE 2016/679 (GDPR) Il servizio erogato adotta misure progettate in aderenza allo standard internazionale sula sicurezza dele informazioni ISO/IEC 27001 su piattaforme AWS Il Responsabile adotta un modello di gestione dei propri processi di fornitura SaaS: ● ISO/IEC 27001 ● ISO 9001:2015 ● CSA STAR Level 1 ● ACN
Dati e operazioni di trattamento	Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità SaaS così come pattuito tra le parti. **Dati di registrazione:** Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio. **Categorie di dati personali:** Dati eventualmente contenuti nelle schede dei pazienti. **Categorie particolari di dati:** Dati eventualmente contenuti nelle schede dei pazienti. **Categorie di dati personali o particolari di soggetti terzi:** Dati di parenti eventualmente contenuti nelle schede dei pazienti.
Ciclo di vita del trattamento e dei dati	1) Attivazione della piattaforma 2) Configurazione della piattaforma 3) Fase d'uso della piattaforma con caricamento delle schede dai soggetti preposti 4) Gestione delle informazioni ai fini Medici e contabili dai soggetti preposti 5) Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore

4. VALUTAZIONI IN MERITO AI TRATTAMENTI

PRINCIPI FONDAMENTALI

Adeguatezza, pertinenza e limitazione a quanto è necessario in relazione alle finalità per le quali i dati sono trattati (minimizzazione)	Per la registrazione dell'operatore al servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Il Software Gestionale per Studi Medici predispone una scheda paziente con indicazioni relative ai dati personali per attività di contatto e contabile e particolari per fini medici. Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati sull'applicativo tracciano nei log di accesso, USER, indirizzo IP. Il Software Gestionale per Studi Medici è raggiungibile solo tramite connessione in Https con certificato registrato al fine di garantire la massima sicurezza nel Trattamento
Esattezza e aggiornamento dei dati	L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.
Periodo di conservazione dei dati	Policy di data retention è a carico del Titolare dei Dati. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio.
Definizione degli obblighi dei responsabili del trattamento e formalizzazione dei contratti	Gli accordi contrattuali sono definiti con le seguenti società: **Supernova Data S.r.l.** in qualità di Responsabile del trattamento • AWS in qualità di Sub-Responsabile del trattamento nominato da Supernova Data srl

5. MISURE DI SICUREZZA

CRITTOGRAFIA

L'applicativo SOFTWARE GESTIONALE STUDIO MEDICO implementa il protocollo crittografico HTTPS.

Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento

Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto.

CONTROLLO DEGLI ACCESSI LOGICI

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.

Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.

TRACCIABILITÀ

L'applicativo SOFTWARE GESTIONALE STUDIO MEDICO implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing.

Ogni log di audit viene mantenuto per un periodo massimo di 5 anni, fatto salvo il caso specifico dei log pertinenti le segnalazioni che vengono mantenuti per tutto il tempo di conservazione delle stesse.

I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent.

I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

ARCHIVIAZIONE

L'applicativo SOFTWARE GESTIONALE STUDIO MEDICO implementa un database SQLite integrato acceduto tramite ORM.

Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

GESTIONE DELLE VULNERABILITÀ TECNICHE

L'applicativo SOFTWARE GESTIONALE STUDIO MEDICO e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review.

A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente.

BACKUP

I sistemi sono soggetti a backup remoto con frequenza di 8 ore e policy di data retention di 7 giorni necessari per finalità di disaster recovery garantendo dunque una RPO di 8 ore.

SICUREZZA DEI CANALI INFORMATICI

Tutte le connessioni sono protette tramite protocollo TLS 1.2

Le connessioni amministrative privilegiate sono mediate tramite connessioni con protocollo SSH.

SICUREZZA DELL'HARDWARE

I datacenter del fornitore SaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7:24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7:24.

I datacenter del fornitore SaaS sono certificati ISO27001.

GESTIRE GLI INCIDENTI DI SICUREZZA E LE VIOLAZIONI DEI DATI PERSONALI

SUPERNOVA DATA SRL ha definito una procedura per la gestione delle violazioni dei dati personali.

6. INFORMAZIONI ADDIZIONALI

NOTE IMPORTANTI:

- I dati sono presenti solo su strutture locate su territorio Europeo

Riferimenti di contatto

- Ufficio Privacy: privacy@
- DPO: dpo@consulentegdpr.eu