

**Compliance Con Il GDPR Del Software Odoo**  
**Sviluppato/personalizzato Da Rapsodoo Italia**

|                                 |            |
|---------------------------------|------------|
| <b>Data</b>                     | 21/09/2020 |
| <b>Versione</b>                 | 3.0        |
| <b>Documenti di riferimento</b> |            |

## Sommario

|   |          |
|---|----------|
| <b>Introduzione.....</b>  | <b>3</b> |
| <b>Compliance GDPR Della Rapsodoo Italia S.r.l.....</b>   | <b>4</b> |
| <b>Come Responsabile Del Trattamento .....</b>  | <b>4</b> |
| Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (Art. 25) ..... | 4        |
| Sicurezza del trattamento (Art. 25 & 32) .....  | 4        |
| Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali (Art. 45 e 46)..... | 5        |
| <b>Come Titolare Del Trattamento .....</b>  | <b>5</b> |
| Diritto di accesso dell'interessato (Art. 15) e Diritto alla portabilità dei dati (Art. 20) .....     | 5        |
| Diritto alla cancellazione (Art. 17) .....  | 5        |
| Diritto di limitazione di trattamento (Art. 18) e Condizioni per il consenso (Art. 7) .....           | 5        |
| Diritto di rettifica (Art. 16) e Diritto all'accuratezza dei dati (Art. 5 (1) d) .....                | 6        |
| <b>Misure Di Sicurezza E Piano Di Mitigazione .....</b>   | <b>6</b> |
| <b>Riferimenti E Link Utili.....</b>  | <b>7</b> |

## Introduzione

In linea con l'Articolo 28 <sup>(1)</sup> del GDPR, la società Rapsodoo Italia S.r.l. (di seguito anche solo “Rapsodoo” o “Società”) ha verificato che il software di gestione aziendale Odoo, su cui si basano le personalizzazioni e gli sviluppi effettuati, e la piattaforma cloud di Amazon (Amazon Web Services o AWS), su cui vengono installati alcuni dei server (ambiente di collaudo e, su richiesta del cliente, ambiente di produzione), siano entrambi GDPR *compliant* come anche da loro dichiarato: [GDPR odoo](#), [GDPR AWS](#).

La *compliance* al GDPR di AWS, che per la tipologia di servizio offerto è solitamente il responsabile del trattamento, è garantita dalla sezione 83 dell'Accordo con il Cliente ([AWS Customer Agreement](#)) e dall'ulteriore Appendice al Trattamento dei Dati ([AWS GDPR Data Processing Addendum](#)). Per la *compliance* di Odoo, poiché le installazioni sono su *server* gestiti dalla Rapsodoo, la Società risulta sia controllore che responsabile del trattamento; in ogni caso, è stato verificato che il *software* Odoo abbia tutti gli strumenti per consentire un trattamento dei dati presenti nel software conforme agli standard GDPR [Art. 28 (3e)]<sup>(2)</sup> ([How does Odoo help you implement GDPR best practices](#)).

Rapsodoo, basandosi sul lavoro fatto sia da Odoo che da AWS e sfruttando gli strumenti messi a disposizione da loro, mantiene a sua volta la *compliance* GDPR implementando le “*best practices*” e gli standard GDPR.

---

1 Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2 (Il responsabile del trattamento) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

## Compliance GDPR Della Rapsodoo Italia S.r.l

### Come Responsabile Del Trattamento

Rapsodoo, in qualità di responsabile del trattamento, garantisce che le personalizzazioni del *software* gestionale Odoo e l'infrastruttura su cui è installato sono GDPR *compliant*, nello specifico adotta le “*best practices*” descritte in seguito nello sviluppo delle personalizzazioni e nelle installazioni dei server. A seconda della destinazione d'uso dei server (produzione, sviluppo o collaudo) non tutti i requisiti possono essere applicati. Questo è in linea con il GDPR, che richiede che la protezione dei dati sia proporzionale alla finalità ed al tipo di dato trattato.

### Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (Art. 25)

La sicurezza in Odoo è implementata fin dalla progettazione. Durante lo sviluppo, la Società usa le “migliori pratiche” per rendere il software sicuro, robusto e resiliente. Il controllo degli accessi viene implementato secondo il “*principle of least privilege*” (principio del privilegio minimo) e le *password* vengono salvate criptate con gli standard industriali di Odoo

- **Controllo Accessi** - Il meccanismo di base per controllare gli accessi consente di restringere l'accesso ai dati in funzione dei singoli ruoli e necessità. Si possono facilmente aggiungere o eliminare gruppi per adattarli alle esigenze aziendali.
- **Record Rules** - Come ulteriore controllo sugli accessi, Odoo implementa il meccanismo di *Record Rule* che consente di limitare l'accesso ai documenti, per esempio in lettura o in scrittura, in base a criteri specifici.
- **Passwords** - Odoo conserva le password criptate con standard industriali PBKDF2+SHA512; è anche possibile usare sistemi di autenticazione esterni quali OAuth 2.0 o LDAP. Le password degli ambienti di produzione e di collaudo vengono trasmessi su connessione sicura HTTPS.

### Sicurezza del trattamento (Art. 25 & 32)

La sicurezza dei dati inseriti in Odoo è a carico dell'utilizzatore finale (titolare del trattamento); Rapsodoo, in qualità di responsabile del trattamento, adotta le *best practices* consigliate da Odoo e da AWS per proteggere i dati delle installazioni. Per le installazioni di produzione vengono sempre applicate tutte le linee guida, mentre per le installazioni di collaudo o di sviluppo, che hanno dati fittizi o anonimizzati e/o non sono pubblicamente raggiungibili, alcune restrizioni vengono rilasciate.

Nello specifico, ogni volta che viene installato Odoo per conto di un cliente, la Società si assicura che siano adottate le seguenti misure di sicurezza:

- Creazione di login amministrativi separati con password forte (almeno 8 caratteri con maiuscole, minuscole, numeri e caratteri speciali); questi *account* vengono usati solo per gestire le installazioni e non per le attività giornaliere.
- Eliminazione di dati dimostrativi dal database che potrebbero consentire l'accesso al sistema.
- Accesso consentito al solo database di produzione di Odoo, La pagina di gestione dei database è protetta da una password forte come per i login amministrativi.
- Creazione di utenti del database PostgreSQL con i minori privilegi necessari per poter accedere; ogni utente può accedere solo ai propri database.
- Le installazioni sono tenute aggiornate con gli ultimi *bug-fix* e *security-fix* rilasciati.

- I server sono dimensionati in maniera adeguata con limiti appropriati di memoria e CPU in funzione delle necessità d'uso. Sui server sono installati i soli servizi necessari ad Odoo ed alla gestione del server stesso.
- Le installazioni di Odoo girano dietro un *webserver* che fornisce una terminazione HTTPS con certificato SSL. Il web *proxy* è configurato in maniera da limitare il numero e la grandezza delle richieste e con *timeout* opportuni e la modalità *proxy* di Odoo è attiva.
- L'accesso SSH al server è consentito solo tramite scambio di chiave pubblica. A seconda della destinazione d'uso, l'accesso SSH è anche limitato ad IP specifici.
- Il server è protetto sia da *firewall* che da *software* di protezione contro attacchi di forza bruta.
- Gli ambienti di produzione sono sempre tenuti separati da quelli di collaudo/sviluppo.
- Viene effettuato il backup giornaliero del database e dei dati del *filestore* di Odoo.
- I dati negli ambienti di collaudo e sviluppo vengono anonimizzati.

#### Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali (Art. 45 e 46)

I server AWS gestiti da Rapsodoo e su cui sono presenti le installazioni di Odoo risiedono tutti su territorio UE, solitamente nelle zone definite *eu-central-1* (basata intorno a Francoforte) o *eu-west-1* (basata in Irlanda); in alcuni casi, generalmente per lo storage a lungo termine su AWS S3, vengono utilizzate anche le *zone eu-west-3* (basata intorno a Parigi) ed *eu-west-2* (Londra). I server interni all'azienda, e i relativi dati, risiedono in Italia tranne per i *backup* su *cloud* AWS che risiedono nella UE nelle zone descritte precedentemente.

#### Come Titolare Del Trattamento

Odoo offre le seguenti caratteristiche per la gestione dei dati, in linea con la normativa GDPR, utilizzabili sia da Rapsodoo, nei casi in cui è parte responsabile del trattamento dei dati (titolare del trattamento) sia dagli utenti finali del software Odoo.

#### Diritto di accesso dell'interessato (Art. 15) e Diritto alla portabilità dei dati (Art. 20)

Odoo fornisce gli strumenti per consentire ai diretti interessati di accedere e di aggiornare le informazioni personali in maniera autonoma. Tutti i dati possono essere esportati direttamente o tramite funzioni di esportazione presenti nel menu azioni.

I formati elettronici sono conformi con il GDPR. Oltre ad esportare i dati in formato PDF, Odoo consente l'esportazione di qualsiasi insieme di dati in formato CSV o Excel.

#### Diritto alla cancellazione (Art. 17)

Il GDPR garantisce il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano in specifiche situazioni. Odoo consente di cancellare un contatto in maniera sicura e - se esistono documenti associati alla persona - l'operazione viene bloccata. In questo caso Odoo consente di anonimizzare il contatto rinominandolo ed eliminando i dati personali ad esso associati (email, indirizzi, etc) oppure assegnando il documento ad un generico utente anonimo.

#### Diritto di limitazione di trattamento (Art. 18) e Condizioni per il consenso (Art. 7)

Un compito ricorrente è gestire le richieste di cancellazione da mail commerciali. Se le mail sono inviate tramite Odoo gli utenti possono effettuare questa operazione in maniera autonoma tramite il *link* in calce alla mail. In alternativa esiste l'opzione "*opt-out*" che, se disabilitata, esclude automaticamente un contatto dall'elenco a cui vengono inviate le mail ma gli consente di poter ricevere email personali.

### Diritto di rettifica (Art. 16) e Diritto all'accuratezza dei dati (Art. 5 (1) d)

Indirizzi mail non validi o non più in uso sono una fonte comune di errore; utenti e clienti possono correggere/variare i propri dati personali (nome, email, indirizzo) in maniera autonoma attraverso il portale.

### Misure Di Sicurezza E Piano Di Mitigazione

Per i casi di violazione di dati personali <sup>(3)</sup> sono state predisposte misure di sicurezza e di mitigazione, in coerenza con i singoli SLA con i clienti.

Per i casi di *Data Loss* (la perdita o distruzione dei dati) e di *Data Breach* (violazione o modifica dei dati) dei server di produzione è possibile ripristinare ogni dato dai *backup* giornalieri. Questi *backup* vengono effettuati giornalmente durante la notte e solitamente vengono conservati per 14 giorni. Per quanto riguarda l'accesso ai dati, siano essi attuali o in *backup*, gli stessi sono salvati criptati; i dati in uso sono criptati nel database mentre i *backup* sono criptati nel *bucket* S3.

---

<sup>3</sup> violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati



## Riferimenti E Link Utili

- “GDPR.” Odoo S.A., [www.odoo.com/it\\_IT/gdpr](http://www.odoo.com/it_IT/gdpr).
- “Il GDPR in Italiano (2016/679/UE): Testo Integrale.” CyberLaws, 26 May 2018, [www.cyberlaws.it/2017/gdpr-privacy-italiano/](http://www.cyberlaws.it/2017/gdpr-privacy-italiano/).
- AWS GDPR DATA PROCESSING ADDENDUM. 2018, [https://d1.awsstatic.com/legal/aws-gdpr/AWS\\_GDPR\\_DPA.pdf](https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf)
- Woolf, Chad. “AWS GDPR Data Processing Addendum – Now Part of Service Terms | Amazon Web Services.” Amazon, Amazon, 22 May 2018, <https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/>