

# Accordo sul trattamento dei dati

## Premesso che

- Tra TECH.TEAM di Stocco Thomas, con sede in Rovigo, Via L. Einaudi, 57/11 – 45100, P.I. IT01179920291 (di seguito la “TECH.TEAM”) e il Cliente è stato stipulato un contratto di servizio per l’utilizzo di uno o più software nella modalità software as a service e relativi termini di utilizzo (di seguito, **contratto SAAS**), di cui questo accordo ne è parte integrante. La violazione di questo accordo costituisce una violazione del **contratto SAAS** con le relative conseguenze per entrambi le parti.
- Il Cliente, ai sensi dell’art. 4 GDPR, assume la qualifica di Titolare (si seguito “Titolare”) dei dati personali mentre la Società quella di Responsabile (di seguito “Responsabile”) in qualità di fornitore del servizio.
- Il presente Accordo sul trattamento dei dati (“Accordo”) descrive le modalità con la Società, garantisce la conformità del trattamento dei dati personali effettuali per conto del Cliente “Titolare” alla normativa privacy (GDPR) ad oggi in vigore, nazionale e comunitaria;
- Nel caso di discordanza tra il presente Accordo e il “contratto SAAS” dovrà prevalere il presente accordo.

Con la stipula del presente accordo entrambe le Parti si impegnano al rispetto della normativa vigente, nazionale o sovra nazionale, in materia di protezione dei dati personali delle persone fisiche e in particolare il Responsabile compirà le attività di trattamento sui dati personali in modo lecito, trasparente e secondo correttezza nonché nel pieno rispetto di tutte le disposizioni normative in materia di trattamento dei dati personali, e in conformità a quanto stabilito dal presente accordo.

## 1. Oggetto

Il presente accordo ha lo scopo di definire le modalità e le condizioni legate al trattamento dati effettuato dal Responsabile per conto del Titolare in riferimento al “contratto SAAS”.

## 2. Durata

Il presente accordo sarà valido per l’intera durata del contratto SAAS; tuttavia i suoi effetti sui trattamenti perdureranno anche oltre come specificato al paragrafo 13 e nel caso sia richiesto da norme nazionali o Comunitarie.



### 3. Origine dei dati

Il Cliente si impegna ad utilizzare il Servizio esclusivamente per scopi leciti e ammessi dai Termini d'uso e dalle disposizioni di legge di volta in volta applicabili, dagli usi e consuetudini, dalle regole di diligenza ed in ogni caso, senza ledere qualsivoglia diritto di terzi, assumendosi ogni responsabilità in tal senso e manlevando e tenendo indenne la Società da qualsiasi richiesta eventualmente avanzata da terzi.

La Società si impegna a informare immediatamente il Cliente qualora, a suo parere, le istruzioni ricevute da questi e/o i trattamenti richiesti violino il codice Privacy o altre disposizioni nazionali o dell'Unione relative alla protezione dei dati.

Il Cliente dichiara di essere l'unico ed esclusivo amministratore del Servizio e come tale dichiara di essere l'unico responsabile della gestione di dati e/o informazioni e/o contenuti da egli trattati, della loro sicurezza e del loro salvataggio; del contenuto delle informazioni e dei dati accessibili o resi disponibili nel Servizio e comunque, a qualsiasi titolo, trasmessi dal Cliente; dei malfunzionamenti del Servizio per qualsiasi utilizzo non conforme ai Termini d'uso. Qualora il Cliente rendesse disponibile l'accesso ai suoi dipendenti, fornitori, clienti dichiara di averli debitamente informati.

### 4. Tipologie e natura dei dati personali

La Società tratterà due tipologie di dati:

- a) Dati personali raccolti al fine della stipula del contratto SAAS;
- b) Dati personali raccolti dal Titolare e gestiti per mezzo del software fornito dalla Società definito nel contratto SAAS

Le operazioni di trattamento su tali dati sono rispettivamente:

1. Gestione amministrativa del contratto e assistenza in fase di start up, per la cui informativa privacy rimandiamo al contratto SAAS;
2. La manutenzione, assistenza, aggiornamento del software e dell'infrastruttura di hosting nonché la messa in sicurezza dei dati in essa caricati dal Titolare, la cui conformità al GDPR è definita nel presente Accordo.

### 5. Personale Incaricato

Il personale che agisce sotto le dirette dipendenze del Responsabile viene incaricato per iscritto in modo da garantire che solo il personale autorizzato possa accedere ai dati necessari per svolgere la mansione assegnata. Il Responsabile garantisce la formazione del suo personale in materia di privacy e in particolare circa l'impatto sulla privacy dei processi di cui è incaricato e stipula con tutto il personale un accordo di riservatezza.

In relazione alle attività di cui al punto 2 il personale addetto verrà incaricato della funzione di Amministratore di Sistema previa verifica delle competenze documentate e/o comprovate avendo cura di registrare gli accessi al sistema. Il Cliente potrà richiedere al Responsabile l'elenco aggiornato degli Amministratori di Sistema.



## 6. Luogo del trattamento

I dati sono conservati e trattati all'interno dell'UE, nel caso in futuro fosse necessario eseguire il trattamento in tutto o in parte in paesi extra UE, il Responsabile ne darà comunicazione al Titolare per informarlo delle misure di sicurezza garantite e ottenere comunque l'autorizzazione salvo che lo richieda il diritto dell'Unione o nazione cui è soggetto il Responsabile. I dati personali vengono custoditi presso il datacenter

Trattamento	Datacenter
Punto 4.2	Datacenter ARUBA Spa Server sede TECH.TEAM

## 7. Misure di Sicurezza

Il Responsabile, come richiesto all'art.32 de GDPR si impegna a mettere in atto in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tra cui:

- la pseudonimizzazione e la cifratura dei dati personali, nel caso al termine del trattamento sia necessario conservare dati connessi a quelli personali ai fini statistici;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La società, al fine di adempiere a tali obblighi ha implementato le seguenti misure di sicurezza:

Livello	Descrizione	Nota
Applicazione	Cifratura automatica dei file caricati del portale	
Applicazione	Sistema di accesso con autenticazione a doppio fattore	attivabile dall'utente
Applicazione	Richiesta di password complesse	
Applicazione	Blocco account dopo 10 tentativi di accesso falliti	
Applicazione	Informazioni di data e ora dell'ultimo accesso	
Applicazione	Sistema di scadenza delle password	



Sistema Operativo	Firewall	
Sistema Operativo	Antivirus con scansione e aggiornamento automatico	
Procedura	Aggiornamento del sistema	Periodicità: min. aggiornamento manuale schedulato ogni 6 mesi
Procedura	Copie shadow dei file	Periodicità: 2 volte al giorno - Durata: media 30 giorni, (in funzione dello spazio su disco)
Procedura	Backup automatico DB	Periodicità: giornaliero – Durata: media 1 anno, (in funzione dello spazio su disco)
Infrastruttura	RAID disco fisico	
Infrastruttura	Hosting fisico in datacenter professionale, fornitore certificato ISO 27001	

## 8. Sub Responsabili

La Società si avvale di sub responsabili per l'hosting delle sue applicazioni come specificato al punto 6, oltre a quelli già indicati nel contratto SAAS alle attività contrattuali e precontrattuali. Il Responsabile provvederà a stipulare un apposito contratto che obblighi il sub responsabile al rispetto di quanto definito nel presente Accordo.

## 9. Data Breach

In conformità agli articoli 32-36 del GDPR, il Responsabile si impegna a collaborare con il Titolare del trattamento nell'adempimento degli obblighi di notifica al Garante e comunicazioni agli interessati circa violazioni di dati che costituiscano un rischio elevato per i diritti e le libertà delle persone fisiche. Si rende, inoltre disponibile, a collaborare con il Titolare in caso si rendesse necessaria una valutazione di impatto sulla protezione dei dati. Eventuali oneri emergenti per questa attività verranno preventivati e saranno interamente a carico del Cliente.

## 10. Verifiche e Ispezioni da parte del Titolare

Il Responsabile consentirà al Titolare le attività di revisione ed ispezione (previo congruo preavviso) al fine di verificare l'ottemperanza dell'operato suo, e degli eventuali sub responsabili, a quanto stabilito nel presente accordo.



Si farà, inoltre, parte attiva al fine di risolvere eventuali non conformità rilevate emergenti da tali verifiche.

Eventuali oneri emergenti per questa attività verranno preventivati e saranno interamente a carico del Cliente.

## 11. Comunicazione dei dati

Il Responsabile tratta i dati personali raccolti dal Titolare solo al fine dell'esecuzione del contratto SAAS riguardo esclusivamente i trattamenti di cui al paragrafo 4 punto 2. Per questi il Responsabile non deve trattare (se non indirettamente per effetto delle attività di gestione di cui al punto 4.2), modificare, aggiornare, correggere, trasferire i dati personali raccolti dal titolare e tanto meno comunicarli a terzi se non su richieste specifiche del Titolare. Viene fatta eccezione per trattamenti richiesti in ottemperanza a norme comunitario o nazionali, che dovranno comunque essere preventivamente comunicati al Titolare (salvo le stesse norme lo proibiscano), prima di ricominciare a trattare nuovamente i dati. E' in ogni caso esclusa la diffusione di tali dati.



## 12. Diritti degli interessati

Il Responsabile comunicherà tempestivamente e comunque senza indebito ritardo al Titolare, in caso di richieste pervenute da parte di un interessato del trattamento di dati personali inerente al proprio diritto di accesso, rettifica, limitazione del trattamento, cancellazione ("diritto all'oblio"), portabilità dei dati, diritto di opposizione al trattamento, o qualsiasi altra richiesta inerente i propri dati personali trattati da parte del Responsabile.

Il software permette al Titolare di accedere autonomamente ai dati, estrarli, cancellarli, in ottemperanza a quanto previsto dal GDPR in merito ai diritti dell'Interessato.

Il Responsabile, previa quantificazione economica, interamente a carico del Cliente, fornirà assistenza al Titolare nell'evadere tali richieste da parte dell'interessato.

## 13. Cancellazione o restituzione dei dati personali

Il Responsabile, nel caso di cessazione dell'erogazione dei servizi di cui al contratto SAAS o di recesso, procederà alla cancellazione degli stessi nel suo sistema informativo e in quello della piattaforma di hosting entro 30 giorni dal recesso. Il Responsabile, informa, che per motivi di sicurezza i dati verranno conservati nei backup per massimo 12 mesi dalla data del recesso e poi cancellati. I dati sono estraibili in formato Excel dal software stesso in modo autonomo da parte del titolare. In caso di contenziosi ancora aperti alla data del recesso o in ottemperanza a norme e regolamenti dell'Unione o degli Stati membri, i dati potranno essere conservati per un tempo maggiore, salvo il permanere delle garanzie di sicurezza e riservatezza definite in questo Accordo e limitatamente a tali finalità.

