AccordoDPACopernicoCRM

Il presente accordo per la protezione dei dati personali (ex art. 28 del Regolamento UE 2016/679) si applica al rapporto tra il Fornitore e l'Utente.

Per "**Fornitore**" si intendono, essendo esse parte del medesimo gruppo di imprese:

- la Società Copernico S.r.L., con sede in P.zza Tre Torri 2, 20145 Milano (Mi), P. Iva 10914540967, iscritta presso la Camera di Commercio di Milano al n. MI - 2566294 del Registro delle imprese e con Uffici operativi in Via Filzi 130/3 - Prato;
- la società Fam 3 S.r.L., con sede in Varese, via Cavour n. 39, cap. 21100, P. Iva 03210920124, indirizzo di posta certificata fam3@pecmail.area336.it., indicata nel Contratto e Concessionaria per la distribuzione di CopernicoCRM, unitamente a
- Very Fat People S.r.L. (o anche VFP), con sede in Varese, via Bernascone, P. Iva P.Iva 02953010127.

L'"**Utente**" è il soggetto che si è registrato e ha richiesto l'utilizzo del Servizio CopernicoCRM o ha scaricato la relativa applicazione dallo Store.

L'esecuzione delle prestazioni di cui al contratto comporta il trattamento di dati personali ai sensi delle normative attualmente in vigore (in particolare: Reg. Eu 679/2016 e D.Lgs. 196/2003 come mod. dal D.Lgs. 101/2018).

I servizi e le prestazioni di VFP e dei propri partner commerciali (Fam 3 S.r.L., Copernico S.r.L.), **sono messi a disposizione di Amministratori, Società, Studi professionali, Imprese, Tecnici specializzati**.

Resta inteso che **VFP, Copernico, Fam 3 e i propri partner trattano i dati e le informazioni** di cui sopra esclusivamente **nella qualità di Responsabili del trattamento** dei dati, ai sensi dell'art. 28 del Reg. Europeo n. 679/2016 (c.d. Gdpr), limitandosi a gestire e mettere a disposizione quanto Amministratori, Società, Studi, Condòmini, Imprese e Tecnici incaricati dagli Amministratori decidono di condividere.

Poiché è l'Amministratore, lo Studio o il Professionista (nella propria qualità di responsabile del trattamento per conto del Condominio ovvero nella propria qualità di Titolare del trattamento dei dati) che sceglie se e come rendere disponibili le informazioni, i soggetti interessati al trattamento dovranno rivolgersi all'Amministratore o Studio professionale per qualsiasi richiesta attinente il trattamento dei dati personali in relazione alle operazioni e verifiche di cui al presente accordo. L'Amministratore e/o lo Studio professionale si impegnano a fornire idonea informativa ai propri amministrati e rimangono i soggetti deputati ad assolvere alle eventuali richieste degli interessati in relazione ai relativi diritti (cfr. artt. 15 - 22 Gdpr).

Premesse

Con questo accordo ("DPA" o "Accordo") le Parti disciplinano le condizioni e le modalità del trattamento dei dati personali eseguito dal Fornitore nell'ambito del Contratto e della prestazione dei Servizi nonché le responsabilità connesse al trattamento, ivi incluso l'impegno assunto dal Fornitore quale Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento generale europeo sulla protezione dei dati n. 679 del 2016 (in seguito "GDPR").

Il complessivo trattamento e le specifiche caratteristiche dello stesso sono descritte nelle "Condizioni generali di contratto", disponibili sul sito www.copernicocrm.cloud o www.copernicocrm.it. Questo Accordo accede ed è riferito a tali Condizioni e ne costituisce allegato essenziale.

Art. 1. Ruolo delle Parti

Le Parti convengono che il Fornitore agisca quale Responsabile del trattamento in relazione ai dati personali che l'Utente tratta mediante il Servizio e che ciascun Utente agisca, nella generalità dei casi, quale Titolare del trattamento dei dati personali conferiti in CopernicoCRM.

Qualora l'Utente svolga operazioni di trattamento per conto di altro Titolare, l'Utente potrà agire come Responsabile del trattamento. In tal caso garantisce che le istruzioni impartite e le attività intraprese in relazione al trattamento dei dati personali, inclusa la nomina, da parte dell'Utente, del Fornitore Copernico S.r.L. quale ulteriore Responsabile del trattamento, è stata autorizzata dal relativo Titolare e si impegna ad esibire e fornire al Fornitore, a richiesta, la documentazione attestante tale qualità.

Copernico S.r.L. ha nominato un Responsabile della protezione dei dati (DPO), che può essere contattato al seguente indirizzo: dpo@copernicocrm.it.

Art. 2. Trattamento dei dati personali

L'Utente affida al Fornitore l'incarico di trattare i dati personali ai fini della prestazione dei Servizi specificati nelle Condizioni Generali di Contratto e di Servizio.

Il Fornitore si impegna ad osservare le Istruzioni dell'Utente e a trattare i dati personali in conformità alle stesse. Nel caso di richieste che, ad avviso del Fornitore, siano in violazione della normativa in materia di protezione dei dati personali, il Fornitore è autorizzato ad astenersi dall'eseguire tali Istruzioni. In tal caso informa senza ritardo l'Utente.

Il Fornitore tratta i dati personali con le modalità necessarie e soltanto nella misura in cui il trattamento sia necessario per erogare i Servizi o per adempiere agli obblighi previsti dal Contratto e da questo Accordo (o imposti dalla legge).

Il Personale del Fornitore che accede o tratta i dati personali è preposto al trattamento in forza di specifiche e idonee autorizzazioni e riceve periodica formazione. Il personale, composto da soggetti autorizzati o designati, è vincolato da precisi obblighi di riservatezza, anche ai fini di protezione dei dati personali.

Quanto sopra non pregiudica la possibilità per il Fornitore di utilizzare alcune informazioni, come ad esempio meta-dati o dati resi anonimi o aggregati, relativi ai documenti generati, caricati o trasmessi dall'Utente nel contesto della fruizione dei Servizi, per elaborare analisi statistiche o eseguire attività di test per migliorare la qualità e l'efficienza dei propri Servizi.

Art. 3. Subfornitori (Responsabili ulteriori)

L'Utente prende atto e acconsente espressamente che alcune operazioni di trattamento dal Fornitore ad altre società collegate a Copernico S.r.L. e/o a soggetti terzi con i quali il Fornitore abbia stipulato adeguati Contratti ai sensi dell'art. 28 del GDPR. Questa clausola vale come formale autorizzazione generale al Fornitore.

Allorché il Fornitore ricorra a ulteriori Responsabili del trattamento, si impegna ad avvalersi di Responsabili che garantiscano l'adozione di misure tecniche e organizzative adeguate e che trattino i dati esclusivamente nei limiti di quanto necessario per l'erogazione dei servizi subappaltati.

L'Utente può chiedere in ogni momento al Fornitore l'elenco dei sub responsabili.

Art. 4. Garanzie

Copernico S.r.L., Very Fast People S.r.L. e Fam 3 S.r.L. presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Reg. UE 679/2016 e garantisca la tutela dei diritti degli interessati. Si impegnano a effettuare i trattamenti in modo lecito, secondo correttezza e nel pieno rispetto di tutte le disposizioni emesse in materia di trattamento dei dati personali, nonché delle seguenti specifiche istruzioni.

Il Fornitore ed i propri partner facenti parte del gruppo imprenditoriale hanno un interesse legittimo a trasmettere dati personali all'interno del gruppo e ciò a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti (Cfr. Considerando 48 Gdpr).

Nell'eseguire il trattamento dei dati personali ai fini della prestazione dei Servizi il Fornitore si impegna a eseguire il trattamento:

- soltanto nella misura e con le modalità necessarie per erogare i Servizi o per adempiere opportunamente i propri obblighi previsti dal Contratto e dal presente Accordo ovvero imposti dalla legge o da un organo di vigilanza o controllo competente. In tale ultima circostanza il Fornitore ne informerà il Cliente (salvo il caso in cui ciò sia vietato dalla legge per ragioni di pubblico interesse);
- in conformità alle Istruzioni del Cliente.

Il Personale del Fornitore che accede, o comunque tratta i dati personali, è preposto al trattamento di tali dati sulla base di idonee autorizzazioni e ha ricevuto la necessaria formazione anche in merito al trattamento dei dati. Tale personale è altresì vincolato da obblighi di riservatezza e deve attenersi alle policy di protezione dei dati personali adottate dal Fornitore.

Art. 5. Misure di sicurezza

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile adotta idonee ed adeguate misure necessarie ai fini della sicurezza dei dati personali ai sensi dell'articolo 32 del GDPR, fra le quali, ad esempio e laddove possibile:

- la pseudonimizzazione e la cifratura dei dati personali;
- 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, comunicandolo al Titolare le soluzioni individuate ed adottate per rispettare tale obbligo.

Art. 6. Assistenza al Titolare

Il Responsabile assiste il Titolare ai fini del rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a sua disposizione.

Art. 7. Violazione di dati personali (data breach)

Il Responsabile implementa soluzioni atte a rilevare eventuali violazioni dei dati personali (ossia le violazioni di sicurezza che comportano 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) e, al verificarsi di tali violazioni, comunicarle tempestivamente al Titolare. Il Responsabile s'impegna, altresì, a collaborare attivamente con il Titolare ai fini delle conseguenti comunicazioni all'Autorità Garante per la protezione dei dati personali e, eventualmente, agli interessati ai sensi degli artt. 33 e 34 del GDPR.

Art. 8. Verifiche e controlli

Il Fornitore sottopone a periodici audit la sicurezza dei sistemi e degli ambienti ove avviene il trattamento dei dati personali per conto dei Clienti - Utenti.

Il Fornitore incarica professionisti indipendenti per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti sono riportati in specifici report. Tali report, che costituiscono informazioni confidenziali del Fornitore, potranno essere resi disponibili al Cliente per consentirgli di verificare la conformità del Fornitore agli obblighi di sicurezza di cui al presente Accordo.

Il Cliente concorda che il proprio diritto di verifica sarà esercitato attraverso la verifica dei Report messi a disposizione del Fornitore. Il Fornitore riconosce il diritto del Cliente, previo accordo, di effettuare audit indipendenti per verificare la conformità del Fornitore agli obblighi previsti nel presente Accordo e nei rispettivi DPA – Condizioni Speciali, e di quanto previsto dalla normativa. Il Cliente potrà avvalersi per tali attività di proprio personale specializzato o di revisori esterni, purché tali soggetti siano previamente vincolati da idonei impegni alla riservatezza. Il Fornitore potrà opporsi per iscritto alla nomina da parte del Cliente di eventuali revisori esterni che siano, ad insindacabile giudizio del Fornitore, non adeguatamente qualificati o indipendenti, siano concorrenti del Fornitore o che siano evidentemente inadeguati. In tali circostanze il Cliente sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.

Il Fornitore impronta i propri servizi ai principi di minimizzazione del trattamento (privacy by design & by default), fermo restando che è responsabilità esclusiva del Cliente assicurare che il trattamento sia condotto poi concretamente nel rispetto di detti principi e

verificare che le misure tecniche e organizzative di un Servizio soddisfino i requisiti di conformità, ivi inclusi i requisiti previsti dalla Legislazione in materia di protezione dei dati personali.

Il Cliente prende atto che, in caso di richieste di portabilità dei Dati Personali avanzate dai rispettivi Interessati, e solo in relazione ai Servizi che generano Dati Personali rilevanti a tal fine, il Fornitore presterà assistenza al Cliente mettendo a disposizione le informazioni necessarie per estrarre i dati richiesti in formato conforme a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali.

Art. 9. Restituzione o cancellazione dei dati

Alla cessazione del Servizio, per qualunque causa intervenuta, il Fornitore cesserà ogni trattamento dei Dati Personali e provvederà alla cancellazione dei Dati Personali (ivi incluse eventuali copie) dai sistemi o da quelli su cui lo stesso abbia controllo entro il termine previsto nel Contratto, tranne il caso in cui la conservazione dei dati da parte del Fornitore sia necessaria al fine di assolvere ad una disposizione di legge italiana o europea. Il Fornitore distruggerà eventuali Dati Personali conservati in formato cartaceo in suo possesso, tranne il caso in cui la conservazione dei dati da parte del Fornitore sia necessaria ai fini del rispetto di norme di legge italiane o europee e manterrà a disposizione del Cliente i Dati Personali per l'estrazione per 60 giorni successivi alla cessazione del Contratto. Il Cliente riconosce che è sua responsabilità provvedere all'estrazione totale o parziale dei soli Dati Personali che ritenga utile conservare e che tale estrazione dovrà essere effettuata prima del termine di cui sopra.

Art. 10. Descrizione dei trattamenti affidati al Fornitore

Materia	Decreto Ristori, Decreto Rilancio, superbonus 110%, bonus fiscali, agevolazioni, utilizzo diretto, sconto in fattura, cessione del credito.
Durata	Durata dello specifico incarico conferito, non oltre il termine previsto dalle agevolazioni, fermi restando altri obblighi discendenti dalla legge.
Natura e finalità del trattamento	Messa a disposizione della piattaforma - software as a service Copernico CRM e relative funzionalità, servizi, applicativi, api e integrazioni per l'esecuzione delle seguenti attività da parte del Cliente - Utente: • Predisposizione e redazione analisi, studi e valutazioni di fattibilità, • redazione, sottoscrizione, invio asseverazioni, congruità spese, richieste per detrazioni, • redazioni e asseverazioni rischio sismico, attestazioni congruità, • rilascio attestazioni prestazione energetica, dichiarazioni relative al miglioramento delle classi energetiche, • apposizione di visti di conformità, asseverazioni, • redazione studi e progetti, preventivi, capitolati, • redazione e predisposizione piani di lavoro, direzione tecnica, sicurezza e prevenzione sul lavoro, • stati di avanzamento lavori, fine lavori, collaudi e verifiche, • visti e attestazioni, • abbattimento barriere architettoniche, altre operazioni relative alla

	predisposizione di particolari conformità, • amministrazione e gestione contabile, contrattuale, fiscale e amministrativa dei rapporti connessi. • Integrazioni con banche dati, interrogazioni ed estrazioni di dati, correlazioni e, in generale • tutte le attività disponibili per il Cliente al fine della gestione degli incarichi ricevuti dai propri interlocutori.
Tipologia e categorie di dati personali	• Nome, cognome, ragione sociale, indirizzi di residenza, domicilio, titolo di studio, indirizzo email ordinario e/o certificato, nr. telefono, anche mobile, altri dati comunicati dal Cliente; • dati di pagamento, dati bancari, c.fiscale, p. iva., documenti di identità del Cliente. • Dati pertinenti e necessari rispetto allo svolgimento delle attività di gestione ed amministrazione dei bonus; • dati anagrafici, fiscali ed indirizzi dei partecipanti; • quote millesimali attribuite a ciascun condomino; • specifiche esigenze abitative derivanti anche da bisogni sanitari; • dati di posizioni contrattuali. • Verbali, documenti, file di immagine e scansioni di documenti e materiali elettronici conferiti dai condòmini. In alcuni casi, previo consenso, utenze telefoniche private e/o indirizzi e-mail. Il trattamento dei dati potrebbe riguardare dati personali anche rientranti in categorie particolari di cui all'art. 9 e 10 del Regolamento (laddove dati necessari all'abbattimento di barriere architettoniche).

Misure di sicurezza organizzative

Policy e Procedure

Il Fornitore ha adottato una specifica politica relativa al trattamento dei dati personali al fine di conformarsi alle norme rilevanti in materia; essa è parte integrante e operativa delle proprie attività. Essa è rivista e aggiornata periodicamente.

Ruoli e responsabilità

I ruoli e le responsabilità relativi al trattamento dei dati personali chiaramente definiti e assegnati in conformità con le politiche di sicurezza. In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, il Fornitore prevede una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione, con la conseguente riconsegna di materiali e mezzi del trattamento.

Il Fornitore applica specifiche procedure di sicurezza alle quali tutti i propri soggetti autorizzati o designati devono conformarsi; esse sono finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche.

Obblighi di confidenzialità imposti al personale

Il Fornitore impone a tutti i dipendenti, lavoratori e persone autorizzate al trattamento responsabilità e obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità sono chiaramente definiti, assegnati e comunicati durante il processo di pre-assunzione e/o di assunzione.

Formazione

Il Fornitore garantisce che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali sono adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.

Autorizzazioni e accessi

Il Fornitore definisce i profili di accesso nel rispetto del principio del c.d. “least privilege” in relazione alle necessità relative all’esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.

Assistenza

Gli interventi di assistenza sono regolamentati allo scopo di garantire l’esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo all'Utente o all’Utente Finale.

Valutazione d'impatto sulla protezione dei dati (DPIA)

In conformità agli artt. 35 e 36 del GDPR il Fornitore effettua, secondo una propria metodologia, l’analisi e la valutazione dei trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche allo scopo di mitigare i rischi derivanti agli interessati.

Gestione degli incidenti

Il Fornitore ha realizzato una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio.

Data Breach

Il Fornitore ha in essere un’apposita procedura finalizzata alla gestione degli eventi e degli incidenti di violazione dei dati personali che possano avere impatto sui dati personali. Essa definisce ruoli e responsabilità nel processo e assicura, in caso di incidente, le valutazioni previste dagli artt. 33 e 34 del GDPR.

Misure di sicurezza tecniche

Gestione risorse/asset

Il Fornitore dispone di un registro delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro include le seguenti informazioni necessarie (risorse IT, tipologia, posizione fisica o elettronica, ecc.). Sono imposti oneri e compiti di mantenimento e di aggiornamento di tale registro. Il censimento delle risorse e degli apparati IT è periodicamente rivisto e aggiornato.

Gestione delle modifiche apportate alle risorse, agli apparati ed ai sistemi IT

Il Fornitore si assicura che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da un soggetto specificamente designato e autorizzato. Il monitoraggio delle eventuali modifiche apportate al sistema IT avviene a cadenza regolare e periodica.

Gestione delle operazioni di sviluppo software e dei test di sviluppo

Lo sviluppo software viene eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Nel corso dei test sono utilizzati dati fittizi.

Responsabili del trattamento

Il Fornitore prevede e attua specifiche linee guida e procedure formali per il trattamento dei dati personali da parte dei responsabili del trattamento e dei sub responsabili prima dell'inizio delle attività di trattamento. Queste linee guida e procedure stabiliscono obbligatoriamente lo stesso livello di sicurezza dei dati personali richiesto nella politica di sicurezza dell'organizzazione del Fornitore.

I responsabili devono fornire prove sufficienti e documentate di conformità della rispettiva organizzazione e dei trattamenti svolti in relazione alle prescrizioni in materia di sicurezza.

Business continuity

Il Fornitore ha definito le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali.

Generazione di file di log e monitoraggio

Sono generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali; includono tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione). I file di log sono contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati.

Sicurezza di Server e Database

I server ove risiedono database e applicazioni sono configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente. I server ove risiedono database e applicazioni trattano solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).

Sicurezza delle Postazioni di lavoro

Gli utenti autorizzati del Fornitore non sono in grado di disattivare o bypassare le impostazioni di sicurezza. Le applicazioni anti-virus e le firme di rilevamento sono costantemente configurate con stretta periodicità.

Sicurezza della Rete e delle Infrastrutture di comunicazione Elettronica

Gli accessi al Servizio sono configurati tramite protocolli crittografici (TLS/SSL).

Backup

Le procedure di backup e ripristino dei dati sono essere definite, documentate e chiaramente collegate a ruoli e responsabilità. Ai backup sono assegnati livelli adeguati di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine. L'esecuzione dei backup è monitorata per garantirne la completezza.

Sicurezza fisica

Il perimetro fisico dell'infrastruttura del sistema IT non è accessibile da personale non autorizzato.

Sicurezza informatica

I dati personali sono protetti contro il rischio di intrusione con sistemi di Intrusion Detection & Prevention, aggiornati in relazione alle migliori tecnologie disponibili.

Ove gli accordi contrattuali lo prevedono è posto in uso un piano di continuità operativa integrato, ove necessario, con il piano di disaster recovery.

Amministratori di Sistema

Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.

Per il dettaglio di ulteriori misure di sicurezza adottate con riferimento ai servizi di data center erogati dai Responsabili Ulteriori del Trattamento è possibile richiedere ulteriori informazioni all'indirizzo info@copernicocrm.it.