INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | **F.** +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

DATA PROCESSING AGREEMENT
AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679 (GDPR)

Tra:

_____, con sede in _____ n. ___, cap _____ città _____, P.Iva _____, in persona del _____

("**Cliente**", "**Data Controller**" o "**Titolare del Trattamento**"),

e

Infominds S.p.a., con sede in Via Brennero 72, 39042 Bressanone (BZ), P.Iva 00899390215, in persona del legale rappresentante *pro tempore*
(**"Infominds", "Data Processor"** o **"Responsabile del Trattamento"**),

e di seguito anche denominati singolarmente come "Parte" e congiuntamente come "Parti".

Premesso che

1. Tra le Parti sono in essere uno o più contratti commerciali aventi ad oggetto uno o più servizi informatici erogati da Infominds al Cliente.
2. Nell'erogazione dei servizi di cui al punto precedente, Infominds effettua un trattamento di dati personali per conto del Cliente, rivestendo quest'ultimo il ruolo di titolare del trattamento.
3. Ai sensi della normativa vigente in materia di trattamento e protezione dei dati personali, ed in particolare del Regolamento UE 2016/679 del 27 aprile 2016 (di seguito anche "GDPR" o "Regolamento"), si rende necessario regolamentare il rapporto tra il Cliente, titolare del trattamento, ed Infominds, responsabile del trattamento, con riferimento al trattamento dati effettuato nell'erogazione dei servizi oggetto degli accordi commerciali in essere. A tal fine, il titolare del trattamento ritiene che il responsabile del trattamento possieda idonei requisiti di esperienza, professionalità, capacità, competenze tecniche ed affidabilità sufficienti per mettere in atto misure tecnico-organizzative con un livello di sicurezza adeguato al rischio.
4. Le Parti intendono disciplinare il rapporto in questione con il presente atto.

Tutto ciò premesso, si conviene e si stipula quanto segue

1. Le premesse costituiscono parte integrante e sostanziale del presente accordo.

2. Nomina a Responsabile del Trattamento

2.1. Ai sensi e per gli effetti dell'art. 28 del Regolamento, Il Titolare del Trattamento (di seguito "Data Controller"), in qualità di soggetto cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali, designa Infominds Spa quale Responsabile del Trattamento (di seguito "Data Processor").

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | F. +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

3. Durata del trattamento e luoghi del trattamento dei dati

3.1. La durata del trattamento ha la medesima durata dei servizi oggetto del contratto o dei contratti commerciali in essere tra le Parti. Alla cessazione di uno o più contratti commerciali, per una qualsiasi ragione, anche la presente nomina cesserà automaticamente con riferimento alle attività di sottese al contratto o i contratti cessati. Restano salvi specifici obblighi di legge che per loro natura sono destinati a permanere.

3.2. Il trattamento dei dati personali per conto del Data Controller avverrà da parte del Data Processor con modalità prevalentemente informatiche, e in ogni caso avverrà all'interno di uno Stato membro dell'Unione europea (UE) o di uno Stato membro dello Spazio Economico Europeo (SEE), ovvero in un paese extra UE o extra SEE il cui sistema privacy è stato soggetto ad una decisione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 45 del GDPR. In ogni altro caso, qualsiasi trasferimento di dati personali verso uno Stato che non è membro né dell'UE né dello SEE avverrà solo su istruzioni documentate del Cliente e nel rispetto delle condizioni specifiche di cui agli articoli 44 e ss. del GDPR.

4. Natura e Finalità del trattamento

4.1. Il trattamento affidato dal Data Controller al Data Processor è necessario per l'erogazione dei servizi e per lo svolgimento delle attività oggetto dei contratti commerciali in essere tra le Parti.

5. Categorie di dati personali trattati

5.1. Ai fini dell'erogazione dei servizi previsti dai contratti commerciali conclusi tra le Parti, il Data Processor tratterà dati personali forniti, archiviati, trasmessi o creati dal Data Controller e sotto l'esclusiva responsabilità di quest'ultimo. Il trattamento potrà riguardare diverse categorie di dati, come, a titolo esemplificativo, dati anagrafici ed identificativi (es. nome, cognome, codice fiscale, indirizzi IP, dati di geolocalizzazione etc.), dati di contatto, dati relativi a paghe e stipendi, presenze e assenze, contenuti multimediali (es. audio, foto, video, presentazioni aziendali, etc.), dati di log degli accessi nei sistemi e nelle applicazioni, e comunque ogni altro dato fornito dal Data Controller.

6. Categorie di interessati

6.1. I dati personali il cui trattamento è affidato dal Data Controller al Data Processor potranno appartenere a diverse categorie di interessati, quali, a titolo esemplificativo, dipendenti, collaboratori, Consiglio di Amministrazione e/o soggetti ad esso equiparati, clienti, fornitori, nonché qualsiasi altro soggetto diverso dalle predette categorie. A tal fine, il Data Controller dichiara di avere adempiuto a tutti gli oneri su di sé incombenti quale titolare del trattamento, ivi inclusi senza limitazione alcuna gli obblighi connessi alla fornitura dell'informativa e, ove richiesto, all'ottenimento da parte degli interessati di tutti i consensi e le autorizzazioni necessarie a consentire al Data Processor di effettuare le attività di cui al presente accordo.

7. Obblighi del Data Controller e Dichiarazioni

7.1. Il Data Controller determina in via esclusiva le finalità e le modalità del trattamento dei dati personali, e si impegna pertanto a comunicare al Data Processor, nelle forme e modalità stabilite dalla presente nomina, qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei suddetti dati. Resta inteso che in caso di modifica sostanziale delle operazioni di trattamento demandate, o qualora i trattamenti richiesti siano in contrasto con la normativa applicabile e/o con i provvedimenti delle autorità di controllo

competenti, ivi incluso l'EDPB, il Data Processor potrà recedere senza preavviso dal presente accordo mediante comunicazione scritta al Data Controller in tal senso.

7.2. Fermo restando gli obblighi in capo al Data Processor previsti nella presente nomina, il Data Controller mantiene la responsabilità generale per qualsiasi trattamento di dati personali che quest'ultimo abbia direttamente effettuato o che altri abbiano effettuato per suo conto, ed è pertanto tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il GDPR, compresa l'efficacia delle misure, le quali devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Il Data Controller, pertanto, è tenuto, a titolo meramente esemplificativo e non esaustivo, a predisporre ed adottare un sistema privacy conforme al GDPR ed alla normativa in materia, adottando, tra le altre, adeguate misure tecnico-organizzative ed effettuando la relativa valutazione di adeguatezza, ad acquisire legittimamente i dati personali e a fornire le informative ex artt. 13 e 14 agli interessati, ad effettuare la notifica al Garante nei casi previsti ex art. 33 previa relativa valutazione, a garantire la tutela dei diritti degli interessati e la conseguente gestione ed evasione delle richieste di questi ultimi, ad effettuare, ai sensi dell'art. 34 del GDPR e previa apposita valutazione, la comunicazione agli interessati nelle ipotesi di violazione dei dati personali (di seguito anche "Data Breach")

7.3. Il Data Controller dichiara che le attività di trattamento demandate al Data Processor sono conformi ai principi di liceità, correttezza, trasparenza, riduzione dei dati, accuratezza, limitazione, integrità dello spazio di archiviazione e riservatezza. Egli inoltre dichiara che i dati personali oggetto di operazioni trattamento in virtù dell'esecuzione del Contratto o dei Contratti di Servizi stipulati con il Data Processor sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati. Egli dichiara, infine, di aver correttamente individuato la base giuridica del trattamento dei dati personali degli interessati.

7.4. Il Data Controller dichiara che i dati personali e/o le eventuali categorie particolari di dati personali oggetto delle operazioni di trattamento affidate al Data Processor, sono stati raccolti e trasmessi rispettando ogni prescrizione della normativa applicabile, ivi inclusi gli obblighi gravanti sul titolare del trattamento in tema di informativa e, ove applicabili, di raccolta di valido consenso degli interessati.

7.5. Il Data Controller dichiara di rimanere l'unico responsabile delle modalità e dei mezzi di trasmissione dei dati personali qualora tali modalità si basino su procedure applicative sviluppate secondo sue regole e/o attraverso propri strumenti informatici o di telecomunicazioni. Nei casi, pertanto, di mancata trasmissione di tali dati per un qualsiasi motivo non imputabile al Data Processor, costui non potrà ritenersi responsabile del trattamento dei suddetti dati.

7.6. Ai sensi dell'art. 30 del GDPR, ove previsto, il Data Controller è obbligato alla tenuta ed aggiornamento del Registro dei Trattamenti.

7.7. Il Data Controller si attiene e si conforma alle prescrizioni stabilite nella presente nomina, in particolare per quanto riguarda l'eventuale attività di verifica e revisione nei confronti del Data Processor, nonché per quanto riguarda ogni eventuale richiesta di informazioni ed assistenza inoltrata al Data Processor, e sempre nei limiti degli obblighi stabiliti in capo a quest'ultimo.

7.8. Restano salvi gli ulteriori obblighi di legge previsti dalla normativa in materia.

8. Obblighi del Data Processor

8.1. Il Data Processor si obbliga a trattare i dati soltanto su istruzione documentata del Data Controller, anche in caso di trasferimento di dati personali verso un paese terzo o

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | F. +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Data Processor.

8.2. Il Data Processor garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

8.3. Ai sensi dell'art. 32 del GDPR, il Data Processor, nel trattare i dati personali oggetto della presente nomina, adotta le misure tecnico-organizzative di cui all'Allegato 2, che il Data Controller reputa e conferma espressamente essere del tutto adeguate, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, e del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

8.4. Tenendo conto della natura del trattamento, il Data Processor assiste il Data Controller con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Data Controller di dare seguito alle richieste per l'esercizio dei diritti degli interessati. Resta inteso che il Data Processor assisterà il Data Controller esclusivamente previe istruzioni documentate e che il punto di contatto con gli interessati resta il Data Controller.

8.5. Il Data Processor assiste il Data Controller nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni messe a disposizione del Data Processor. Resta inteso che l'assistenza è limitata, tra l'altro, al ruolo di Data Processor, alla durata, e all'ambito di operatività della presente nomina, con esclusione, a titolo esemplificativo, delle attività di consulenza legale ed informatica, e comunque di quelle attività tipiche fornite da figure professionali differenti quali, a titolo esemplificativo, il Consulente Privacy o il Responsabile della Protezione Dati (cd "DPO", ossia Data Protection Officer).

8.6. Il Data Processor, su scelta del Data Controller, cancella o restituisce tutti i dati personali dopo che è terminata la prestazione di servizi relativa al trattamento oggetto della presente nomina, e cancella le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati.

8.7. Il Data Processor mette a disposizione del Data Controller, su richiesta scritta e dettagliata, le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla presente nomina.

8.8. il Data Processor informa immediatamente il Data Controller qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati personali.

8.9. Ai sensi dell'art. 33 del GDPR, qualora si verificasse un Data Breach, il Data Processor informa il Data Controller senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

9. Obblighi specifici connessi alla funzione di Amministratore di Sistema

9.1. Ai sensi del Provvedimento del 27/11/2008 e successive modifiche, emanato dal Garante per la Protezione dei Dati Personali (di seguito "Provvedimento del Garante") e compatibile con il Regolamento, qualora, nell'erogazione dei servizi di cui al punto precedente, Infominds effettui un trattamento di dati personali per conto del Cliente con compiti ed attribuzioni tipiche dell'Amministratore di Sistema, il Data Processor ha l'onere di individuare all'interno della propria organizzazione le figure che, per competenze tecnico-professionali, esperienza ed affidabilità, possano svolgere le attività di Amministratore di Sistema ed essere soggette agli obblighi di legge e della presente nomina. Il Data Processor ha altresì l'onere di conservare ed aggiornare l'elenco degli Amministratori di Sistema.

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | F. +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

9.2. Su richiesta scritta del Data Controller, il Data Processor fornisce l'elenco degli Amministratori di Sistema con gli estremi identificativi e gli ambiti di operatività ad essi attribuiti.
9.3. L'Amministratore o gli Amministratori di Sistema adottano sistemi idonei alla registrazione degli accessi logici (cd "autenticazione informatica" o "access log") ai sistemi informatici. Tali registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono ricomprendere i riferimenti temporali e la descrizione sintetica dell'evento che le ha generate e devono essere conservate per un periodo di almeno 6 (sei) mesi. Ove l'Amministratore o gli Amministratori di Sistema sono chiamati ad operare direttamente sul sistema informatico del Data Controller, quest'ultimo dovrà adottare, ove non presente, un sistema idoneo alla registrazione degli accessi logici.
9.4. Su richiesta scritta del Data Controller, il Data Processor fornisce l'estratto delle registrazioni di cui al comma precedente relativo agli accessi dell'Amministratore o degli Amministratori di Sistema.
9.5. Al fine di soddisfare l'esigenza di verifica del Data Controller, previa richiesta scritta il Data Processor fornisce al Data Controller apposita relazione sull'attività svolta dagli Amministratori di Sistema. La richiesta dev'essere inviata con congruo preavviso, non inferiore a 15 (quindici) giorni lavorativi, e deve riguardare le attività svolte nell'arco del precedente anno solare. Può essere fornita una sola relazione per ciascun anno solare. Il Data Processor si riserva di richiedere un corrispettivo rapportato all'attività svolta, ai tempi ed alle risorse impiegate, e tenendo conto delle tariffe di legge o di mercato vigenti.

10. Sub Processor

10.1. Per l'esecuzione delle operazioni di trattamento oggetto della presente nomina, Il Data Controller autorizza sin d'ora il Data Processor a ricorrere ad ulteriori responsabili del trattamento (di seguito "Sub Processor"). Il Data Processor, nel servirsi di Sub-Processor, assicura che gli stessi si vincolino, con contratto od altro atto giuridico, ai medesimi obblighi e condizioni contenute nel presente atto di nomina, e che adottino garanzie sufficienti per mettere in atto misure tecnico-organizzative adeguate. Il data Controller può richiedere al Data Processor l'elenco aggiornato dei Sub-Processor incaricati.
10.2. In caso di aggiunta o sostituzione di Sub-Processor, il Data Processor comunicherà tempestivamente l'eventuale modifica al Data Controller, per consentire a quest'ultimo di opporsi a tali modifiche. Decorso il termine di 5 (cinque) giorni dal ricevimento della comunicazione senza che sia stata manifestata alcuna opposizione da parte del Data Controller, il Data Processor considererà accettate le modifiche apportate.

11. Ispezioni e controlli

11.1. Il Data Processor, nell'ambito dei trattamenti effettuati per conto del Data Controller, consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Data Controller o da altro soggetto da questi regolarmente incaricato.
11.2. In caso di attività di audit ovvero di verifica o revisione delegate a terzo soggetto, qualora venga rilevato tra quest'ultimo e il Data Processor un rapporto di concorrenza ovvero un conflitto di interessi, il Data Processor può rifiutare lo svolgimento delle predette operazioni da parte del soggetto incaricato.
11.3. Nelle ipotesi di audit ovvero di ogni altra operazione di verifica o ispezione, in special modo effettuate presso i locali del Data Processor, al fine di ridurre al minimo l'impatto sull'attività d'impresa di quest'ultimo nonché di consentire lo svolgimento delle suddette operazioni in maniera efficiente e proficua, il Data Controller si impegna ad inoltrare per

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | F. +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

iscritto l'istanza di audit ovvero verifica-revisione o ispezione con un preavviso di almeno 15 (quindici) giorni lavorativi, e a concordare, prima dell'avvio delle attività, i termini di tali verifiche (data di inizio e durata), le tipologie di controllo e l'oggetto delle verifiche, fermo restando che il Data Controller non potrà procedere a più di 1 (una) verifica all'anno, salvo il caso di Data Breach. Attesa la natura, le modalità e l'oggetto delle attività di cui al precedente capoverso, il Data Processor può subordinare l'esecuzione di tali attività alla sottoscrizione di un accordo di segretezza (cd "NDA") da parte del Data Controller.

11.4. Nelle ipotesi di ispezioni, revisioni e controlli, il Data Processor si riserva di richiedere al Data Controller congruo corrispettivo rapportato all'attività espletata, al numero di sessioni e risorse impiegate, tenendo conto delle tariffe orarie in vigore al momento del trattamento, ovvero di non evadere la richiesta laddove le attività di verifica esorbitano gli obblighi ed i limiti di cui alla presente nomina. E' sempre richiesto il corrispettivo per ogni attività di revisione, ispezione o controllo svoltasi presso i locali del Data Processor fuori l'ordinario orario di lavoro. In ogni caso tutte le spese per le attività di verifica e revisione restano a carico del Data Controller.

12. Responsabilità

12.1. Ai sensi dell'art. 82 del GDPR, il Data Controller risponde per il danno materiale o immateriale causato dal trattamento affidato al Data Processor qualora il danno derivi dalla violazione degli obblighi a lui imposti dalla normativa in materia di privacy e da quelli stabiliti nella presente nomina.

12.2. Ai sensi dell'art. 82 del GDPR, il Data Processor risponde per il danno materiale o immateriale causato dal trattamento affidatogli soltanto qualora non abbia adempiuto agli obblighi specificatamente diretti al data Processor e previsti dalla normativa in materia di privacy e da quelli stabiliti dalla presente nomina, ovvero abbia agito in modo difforme o contrario a legittime istruzioni impartite dal Data Controller.

12.3. Il Data Processor è in ogni caso esonerato da qualsiasi responsabilità per il trattamento affidatogli, qualora dimostri che l'evento dannoso non gli è in alcun modo imputabile, ovvero sia derivato da istruzioni illegittimamente impartite dal Data Controller nonostante l'informativa resa ai sensi dell'art. 8.8. Altresì il Data Controller è esonerato da ogni responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

13. Disposizioni finali

13.1. La presente nomina è soggetta esclusivamente al diritto della Repubblica italiana ed è altresì conforme alla normativa europea in materia di trattamento dati personali. La versione ufficiale della presente nomina è quella italiana, e pertanto, in caso di incongruenze e/o discrepanze tra la versione italiana e versioni redatte in altre lingue, prevale e fa fede la versione italiana.

13.2. Ove nella presente nomina sono utilizzati termini o definizioni a cui il Regolamento ed il Provvedimento del Garante attribuiscono un significato, a tali termini andrà dato tale specifico significato.

13.3. La presente nomina costituisce integrazione degli accordi contrattuali intercorsi tra le Parti. Essa sostituisce ogni eventuale precedente intesa, anche verbale, e costituisce pertanto l'unico accordo giuridicamente valido ed efficace in relazione alle materie da esso trattate. Le disposizioni della presente nomina si applicano altresì anche a tutti i futuri trattamenti di dati che il Data Processor potrà effettuare per conto del Data Controller, fatte salve eventuali integrazioni da effettuarsi in conformità dell'art. 13.6.

13.4. Con riferimento a richieste aventi ad oggetto attività e adempimenti che esorbitano quanto previsto dalla presente nomina, il Data Processor si riserva di chiedere al Data

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | **F.** +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

Controller un corrispettivo in base alle tariffe concordate negli accordi commerciali tra le Parti, o in alternativa in base alle tariffe di legge o di mercato vigenti, ovvero di non evadere la richiesta.

13.5. L'eventuale tolleranza di una Parte all'inadempimento dell'altra non potrà in alcun modo essere considerata come rinuncia ai diritti derivanti dal presente accordo.

13.6. Qualora una disposizione della presente nomina sia o diventi totalmente o parzialmente invalida o inapplicabile, ovvero in essa vi sia una lacuna, le restanti disposizioni resteranno comunque valide ed efficaci. Le Parti dovranno sostituire la disposizione non valida o non applicabile, ovvero colmare la lacuna, con una disposizione valida ed applicabile che si avvicini il più possibile alla natura ed allo scopo del presente accordo. Le modifiche o le integrazioni di cui al precedente capoverso dovranno avvenire tramite accordo scritto tra le Parti, ad integrazione della presente nomina.

13.7. Le Parti dichiarano di aver negoziato in modo specifico tutte le clausole della presente nomina. Qualora dovessero sorgere controversie concernenti la validità, l'interpretazione, l'esecuzione e la risoluzione del presente accordo ovvero di allegati o documenti ad esso collegati, le Parti si impegnano a cercare tra loro un equo e bonario componimento. In caso di mancato componimento bonario, la risoluzione della controversia è demandata in via esclusiva all'Autorità Giudiziaria di Bolzano.

13.8. Ai fini dell'esecuzione degli obblighi di cui alla presente nomina, le comunicazioni tra le Parti e le richieste dovranno avvenire esclusivamente agli indirizzi indicati nell'Allegato 1.

Luogo e data

_____, __/__/____

Per accettazione
Data Controller
Data Processor

_____

Infominds S.p.a.

_____

_____

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa

BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | **F.** +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

ALLEGATO 1: ISTRUZIONI SPECIFICHE DEL DATA CONTROLLER*

*Il presente allegato deve essere completato e sottoscritto dalle parti prima di qualsiasi trattamento di dato.

SOGGETTI	
Data Controller	
Nominativo del legale rappresentante (o di altra persona legittimata ad esprimere all'esterno la volontà del Data Controller)	_____
Data Processor	
Nominativo del legale rappresentante (o di altra persona legittimato ad esprimere all'esterno la volontà del Data Processor)	Luis Plunger, legale rappresentante
DPO e dati di contatto (eventuale)*	
Per il Data Controller	
nominativo	_____
email	_____
pec	_____
Posta ordinaria	_____
Per il Data Processor	
nominativo	N.A.
email	N.A.
pec	N.A.
Posta ordinaria	N.A.

*Quando stabilito dalla legge e qualora una o entrambe le parti abbiano nominato un *Data Protection Officer*, indicare i relativi dati di contatto. Ogni eventuale modifica dei dati deve essere tempestivamente fornita all'altra parte.

CATEGORIE DI DATI PERSONALI
Dati Comuni
☐ dati anagrafici (e.g. nome, cognome, Codice Fiscale, numero telefonico, email, etc.)
☐ dati di contatto (e.g. email, PEC, numero di telefono, indirizzi di residenza, etc.)
☐ account ad apparecchiature e servizi IT (e.g., credenziali d'accesso a postazioni di lavoro, posta elettronica, portali, etc.)
☐ identificativi informatici (e.g. indirizzi IP, access log, dati di geolocalizzazione, etc.)
☐ contenuti multimediali (e.g. audio, foto, video, etc.)
☐ informazioni lavorative e/o professionali (es. cv, buste paga, formazione, lettere di referenza, etc)
☐ Altro (specificare) _____

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa

BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | **F.** +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

CATEGORIE DI INTERESSATI
☐ Consiglio di Amministrazione e soggetti ad esso equiparati ☐ Dipendenti e collaboratori propri ☐ Dipendenti e collaboratori dei partner commerciali (e.g. dealer, fornitori, etc.) ☐ Clienti e potenziali clienti ☐ Altro (specificare) _____

CONTATTI*	
Per il Data Controller	
Persona di riferimento	_____
email	_____
pec	_____
Per il Data Processor	
Persona di riferimento	Dott. Manuel Mattia
email	privacy@infominds.eu
pec	info@pec.infominds.eu

***** Qualsiasi modifica relativa ai contatti deve essere tempestivamente comunicata all'altra parte.

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | F. +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

ALLEGATO 2: MISURE TECNICHE ED ORGANIZZATIVE CONFORMI ALLE DISPOSIZIONI PRIVACY, AI SENSI DELL'ART. 32 GDPR

Premessa

Il presente documento contiene le misure tecniche-organizzative per la sicurezza delle infrastrutture di Infominds in relazione all'articolo 32 del regolamento sulla protezione dei dati UE 2016/679, adottate da Infominds per proteggere i dati personali.

Le misure di sicurezza qui contenute si riferiscono sia alle sedi di Infominds, che alla sede del datacenter a Bolzano. Esse illustrano le misure di sicurezza adottate da Infominds in tutte le sedi dei datacenter e sono considerate lo standard per le sedi future.

Tutti i data center sono situati in Italia.

Il documento contiene le sezioni seguenti:

1. **Riservatezza (art. 32(1) (b) GDPR)**
    a. Protezione fisica
    b. Sicurezza di accesso
    c. Separazione dei dati dei clienti
    d. Crittografia
2. **Integrità (art. 32 (1)(b) GDPR)**
    a. Sicurezza dati in transito
    b. Sicurezza dell'elaborazione dati
    c. Sicurezza dei sistemi informatici
3. **Disponibilità e resilienza (art. 32(1)(b) GDPR)**
    a. Controllo della disponibilità
4. **Procedure periodiche di revisione, valutazione ed analisi (art. 32(1)(d) GDPR; Art. 25(1) GDPR)**
    a. Controllo ordini
    b. Sistemi organizzativi

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | F. +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

1. Riservatezza (Art. 32(1) (b) GDPR)

a. Protezione fisica

Misure di sicurezza fisica per la protezione contro l'accesso non autorizzato ai sistemi di elaborazione dati.

Misure di protezione dell'edificio (Datacenter):

a) Zona di sicurezza Datacenter – Bussola di sicurezza
b) Finestre bloccabili
c) Sistema d'allarme
d) Controlli da parte del servizio di vigilanza
e) Accesso solo per le persone autorizzate (con badge personale)
f) Videosorveglianza permanente delle aree d'ingresso
g) Uscite di emergenza protette d'allarme
h) Armadi rack bloccabili con chiave

Misure di protezione dell'edificio (Uffici Infominds)

a) Videosorveglianza delle aree di ingresso a Bolzano, Venezia
b) Sistema d'allarme in tutte le filiali
c) Regolamentazione per la sorveglianza e l'accompagnamento di persone esterne negli uffici

Misure di sicurezza organizzative

a) Controlli del servizio di vigilanza al di fuori dell'orario d'apertura
b) Regolamento di accesso alle sedi aziendali
c) Regole per l'uscita dei dipendenti dall'azienda

Norme di accesso fisico (Datacenter)

a) Regolamento per l'accesso dei singoli dipendenti al datacenter
b) Regolamento per l'accesso dei clienti/interessati e dei collaboratori al datacenter
c) Regolamento e controllo dei lavori necessari nel datacenter
d) La possibilità di concedere, modificare o bloccare accessi al datacenter

b. Sicurezza d'accesso

Misure per prevenire l'accesso non autorizzato a sistemi e applicazioni, nonché misure di protezione contro la lettura, la modifica e la cancellazione non autorizzata di dati personali.

Controllo dell'accesso

a) Regolamento per la gestione dei diritti degli utenti
b) Regolamento per la gestione di utenti e per la gestione dei sistemi
c) Controlli periodici dei diritti degli utenti
d) Le persone autorizzate s'identificano con un nome utente e una password individuale

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | F. +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

e) Gestione password degli account amministrativi (root, administrator)
f) Regole per la complessità della password: password complessa con 8 caratteri e almeno lettere maiuscole e minuscole, numeri e caratteri speciali.
g) Regolamento per l'assunzione/licenziamento di dipendenti
h) Blocco temporaneo degli account utente in caso di ripetuta immissione errata della password
i) Blocco dei computer in caso d'inattività per più di 10 minuti

Sicurezza di rete

a) Utilizzo di firewall e antivirus
b) Uso dei sistemi di rilevamento delle intrusioni (IDS)
c) Regolamento per la configurazione sicura di client e server
d) Regolamento per l'uso d'attrezzature nuove
e) Uso dei sistemi di controllo dell'accesso alla rete aziendale Infominds (802.1X)

Misure per la sicurezza degli accessi esterni

a) Regolamento per l'accesso esterno ai sistemi di elaborazione dati
b) Accesso esterno esclusivamente con autenticazione a due fattori alla rete aziendale Infominds
c) Regolamento per la gestione di sistemi da esterno
d) Regole per l'attribuzione dei diritti a persone esterne e partner commerciali
e) Blocco dell'accesso non autorizzato alla rete tramite Internet

Misure di sicurezza supplementari (Datacenter)

a) Utilizzo di macchine virtuali
b) Assegnazione di singoli account utente di amministrazione
c) Regolamento per l'assegnazione dei diritti amministrativi agli amministratori
d) Nomina individuale d'amministratori e amministratori di password
e) Registrazione protetta degli accessi attraverso account amministrativi
f) Controllo del trasporto e delle copie dei dati mediante supporti esterni
g) Regolamento per la distruzione dei dischi rigidi

Logging degli accessi

a) Registrazione protetta dell'accesso ai conti amministrativi
b) Registrazione degli accessi non autorizzati alla rete (firewall)

Ulteriori misure di protezione per documenti e dati su supporto cartaceo

a) Utilizzo di trituratori carta
b) Chiusura automatica delle porte degli uffici dell'amministrazione ed HR

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | F. +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

c. Separazione dei dati dei clienti

Separazione dei dati raccolti per diverse finalità di trattamento.

a) Sistemi server separati e archiviazione dei dati
b) Capacità multi-tenant del Software in uso
c) Distinzione tra sistemi per lo sviluppo, sistemi di test e sistemi produttivi
d) Regolamento della creazione di nuovi clienti e di nuovi utenti di clienti nell'ambiente Cloud.

d. Crittografia

Crittografia dei dati per impedire la lettura non autorizzata delle informazioni da parte di persone non autorizzate o di terzi.

a) Password crittografate
b) Crittografia del Backup-to-Disk
c) Crittografia dei file (individualmente da parte dell'incaricato)

2. Integrità (Art. 32 (1)(b) GDPR)

a. Sicurezza dati in transito

Protezione della connessione da lettura, modifica o cancellazione dei dati personali non autorizzata durante la connessione o il trasporto degli stessi.

a) l'uso di protocolli appropriati per l'accesso ai sistemi informatici (Citrix, RDP, VPN, SSH, SSL/TLS)
b) Utilizzo di PEC-Email
c) Determinazione delle persone autorizzate in base a un concetto d'autorizzazione

b. Sicurezza dell'elaborazione dati

Misure tecniche ed organizzative per determinare chi può inserire, modificare o cancellare dati nei sistemi d'elaborazione.

a) Definizione delle responsabilità per l'inserimento dei dati (e i loro sostituti)
b) Registrazione dell'inserimento, della modifica e della cancellazione di dati personali nel sistema ERP
c) Configurazione di diverse autorizzazioni utente (ad es. lettura, scrittura, modifica, cancellazione) nel sistema ERP

c. Sicurezza dei sistemi informatici

a) Whitelisting di applicazioni consentite (RaaS e EaaS)
b) Antivirus su tutti i sistemi (Server e Client)
c) Crittografia dei dischi rigidi dei notebook dei collaboratori Infominds

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | F. +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

3. Disponibilità e resilienza (Art. 32(1)(b) GDPR)

a. Controllo della disponibilità

Backup

a) Concetto di backup dei dati
b) Definizione delle linee guida in materia di conservazione dei dati
c) Salvaguardia dei dati su nastri custoditi in area protetta
d) Backup periodico di file, server virtuali e database
e) Definizione della denominazione dei nastri di backup
f) Dicitura dei nastri di backup
g) Inventario di tutti i backup e nastri di backup

Backup (Datacenter)

a) Concetto di backup dei dati per i servizi "Software gestionale as a Service"
b) Definizione delle linee guida in ambito della salvaguardia dei dati
c) Deposito dei nastri di backup in una cassaforte ignifuga
d) Archiviazione dei backup in due sedi diverse
e) Backup regolare di file, server virtuali e database
f) Definizione della denominazione dei nastri di backup
g) Dicitura die nastri di backup
h) Inventario di tutti i backup e nastri di backup

Misure per garantire la disponibilità dei sistemi

a) Gruppi di continuità (UPS)
b) Impianto di climatizzazione ridondato con funzionamento alternato
c) Monitoraggio della temperatura
d) Monitoraggio dei sistemi informatici con segnalazione automatica
e) Separazione dei singoli dipartimenti e del team informatico interno
f) Acquisto centralizzato di hardware e software
g) Linee guida per la documentazione dei processi
h) Formazione continua dei collaboratori

Misure per garantire la disponibilità dei sistemi (Datacenter)

a) Gruppi di continuità (UPS)
b) Gruppo elettrogeno
c) Sistema antincendio con segnalazione automatica
d) Impianto di climatizzazione ridondato
e) Monitoraggio della temperatura
f) Monitoraggio dei sistemi informatici con segnalazione automatica
g) Piani di emergenza (incluso responsabilità, regolamento di ripristino, Datacenter alternativi)

INFOMINDS AG | SPA

Rechts- u. Verwaltungssitz | Sede legale ed amministrativa
BRIXEN | BRESSANONE
Brennerstraße | Via Brennero, 72
I-39042 Brixen | Bressanone (BZ)

T. +39 0472 057 700 | F. +39 0472 057 701
info@infominds.eu | info@pec.infominds.eu
www.infominds.eu

h) Sistemi d'elaborazione critici ridondati (Firewall, Switch, Server)
i) Disaster Recovery Policy
j) Acquisto centralizzato di hardware e software
k) Linee guida per la documentazione dei processi
l) Linee guida per l'accesso al Datacenter ed il comportamento all'interno del Datacenter
m) Formazione continua dei collaboratori

Misure organizzative

a) Valutazione della sicurezza informatica a livello mensile (Penetration Test)
b) Regolamento della responsabilità per gli aggiornamenti dei sistemi informatici

4. Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

a. Controllo degli ordini

Senza previa autorizzazione da parte del titolare, ai sensi dell'art. 28 3 a) nessun dato personale verrà trattato da Infominds.

Accordi

a) Il titolare del trattamento comunica con un documento scritto o con un documento digitale con il responsabile del trattamento per fare un ordine.
b) Le istruzioni del titolare del trattamento sono fornite per iscritto. Istruzioni verbali verranno confermate per iscritto.

Subappaltatori

a) Le misure volte a garantire il rispetto delle leggi sulla privacy applicabili ad altri responsabili del trattamento possono essere riesaminate dal responsabile del trattamento.

b. Sistemi organizzativi

a) Persona di contatto dedicata per rispondere a domande sulla privacy
b) Audit annuale in merito alla privacy da parte di consulenti esterni
c) Nomina scritta dei dipendenti come personale autorizzato al trattamento dei dati personali
d) Linee guida per il personale autorizzato al trattamento a garantire la sicurezza dei dati personali
e) Procedura predefinita in merito alla gestione delle richieste sulla privacy