INFOMINDS SPA

Sede legale ed amministrativa
BRESSANONE
Via Brennero, 72
I-39042 Bressanone (BZ)

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

CONTRATTO TRA TITOLARE E RESPONSABILE PER IL TRATTAMENTO DEI DATI

AI SENSI DELL'ART. 28 DEL REGOLAMENTO (UE) 2016/679

Tra

_____, con sede in _____, P.IVA _____, telefono _____, e-mail _____ e PEC: _____ quale Titolare del trattamento (di seguito anche "**Titolare**"),

e

INFOMINDS S.p.a., con sede legale in Via Brennero n. 72 – 39042 Bressanone (BZ), P.IVA 00899390215, telefono 0472057700, e-mail info@infominds.eu PEC info@pec.infominds.eu (di seguito anche "**Responsabile**").

Premesso che:

- tra il Titolare del trattamento e INFOMINDS S.P.A. è in essere uno o più rapporti contrattuali aventi ad oggetto uno o più servizi informatici erogati da INFOMINDS S.P.A. (di seguito anche "Contratto Principale");
- nell'esecuzione di tali servizi, INFOMINDS S.P.A. può effettuare trattamenti di dati personali per conto del Titolare del trattamento;
- in relazione alle attività affidate, il personale di INFOMINDS S.P.A. potrebbe svolgere funzioni riconducibili al ruolo di Amministratore di Sistema, ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modifiche e integrazioni, nella misura in cui intervenga su sistemi, banche dati, reti, credenziali o apparati con possibilità di accesso, anche accidentale, a dati personali;

Premesso altresì che:

- il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti della normativa pro tempore vigente e garantisca la tutela dei diritti degli interessati;
- il Responsabile deve procedere al trattamento dei dati personali esclusivamente secondo le istruzioni documentate impartite dal Titolare, con il presente Contratto e con eventuali istruzioni o accordi successivi;
- l'attribuzione delle funzioni di Amministratore di Sistema deve avvenire, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato;

Tutto ciò premesso, le parti, impegnandosi a rispettare la normativa applicabile in materia di protezione dei dati personali e, in particolare, il Regolamento (UE) 2016/679 ("GDPR") e il d.lgs. 196/2003, convengono e stipulano quanto segue:

1. Designazione del Responsabile del trattamento

Il Titolare del trattamento dei dati personali gestiti nell'esercizio della propria attività designa INFOMINDS S.P.A. quale Responsabile del trattamento ai sensi dell'art. 28 GDPR, autorizzandolo a effettuare tutti - ed esclusivamente - i trattamenti di dati necessari a eseguire i servizi di cui al "Contratto Principale".

Il Responsabile del trattamento conferma di possedere conoscenze specialistiche, affidabilità, risorse economiche, organizzative e gestionali, anche in termini di personale dedicato alle attività di trattamento, tali da consentire la messa in atto di misure tecniche e organizzative adeguate a tutela dei dati personali trattati per conto del Titolare.

2. Ambito di operatività quale Amministratore di Sistema

In relazione ai servizi oggetto del Contratto Principale, il personale di INFOMINDS S.P.A. potrebbe rivestire il ruolo di Amministratore di Sistema ("ADS").

INFOMINDS S.P.A. si impegna pertanto a ottemperare agli obblighi previsti dal Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modifiche e integrazioni e, in particolare, a:

- designare quali Amministratori di Sistema esclusivamente soggetti che, tenuto conto della loro esperienza professionale e delle capacità e affidabilità dimostrate nello svolgimento delle proprie mansioni, siano in possesso dei requisiti necessari per assolvere tale funzione nel rispetto della normativa applicabile;
- mantenere aggiornato l'elenco nominativo delle persone fisiche preposte a funzioni di Amministratore di Sistema, indicando almeno nome, cognome, ruolo/funzione, ambito di operatività, sistemi o servizi interessati e periodo di abilitazione, e metterlo a disposizione del Titolare su richiesta inviata con congruo preavviso, non inferiore a 15 (quindici) giorni lavorativi. L'elenco deve essere aggiornato tempestivamente in caso di nuove designazioni, cessazioni o modifiche degli ambiti di operatività;
- svolgere controlli periodici sull'operato degli Amministratori di Sistema designati e sugli accessi logici ai sistemi di elaborazione e agli archivi elettronici effettuati dagli stessi, in conformità alle previsioni del Provvedimento del Garante;
- assicurare il tracciamento degli accessi amministrativi ove tecnicamente applicabile e conservare i log secondo tempi e modalità coerenti con la normativa e con le istruzioni del Titolare. I log saranno protetti da alterazioni non autorizzate e conservati per un periodo non inferiore a sei mesi, salvo diverso termine indicato dal Titolare o previsto dalla normativa applicabile.

Con riferimento alla presente designazione, il Titolare individua i seguenti ambiti di operatività consentiti, nei limiti dei servizi effettivamente affidati:

Ambito operativo	**Funzioni**	**Dettaglio delle funzioni**	**Applicabilità SI/NO**
Gestione apparati e postazioni	Assistenza e manutenzione	Interventi su hardware, postazioni e periferiche affidate; eventuale sostituzione o ripristino apparati	

Gestione software gestionali	Installazione e aggiornamento	Manutenzione, aggiornamento, assistenza correttiva, adattativa ed evolutiva dei software	
Gestione software gestionali	Profili e credenziali	Supporto alla gestione di utenze, credenziali e profili autorizzativi, ove previsto dal servizio	
Database e archivi applicativi	Manutenzione	Interventi su basi dati, archivi applicativi, procedure di consultazione, salvataggio e ripristino	
Backup e recovery	Gestione e verifica	Esecuzione, verifica, ripristino e test di backup dei dati e dei sistemi affidati	
Conservazione sostitutiva/elettronica	Gestione documentale	Creazione, correzione, firma, invio in conservazione e gestione dei metadati dei documenti digitali, nei limiti del servizio	
Fatturazione elettronica	Gestione flussi	Supporto ai flussi di fatturazione elettronica attiva e passiva, ove attivati	
Accesso remoto e assistenza	Supporto tecnico	Collegamenti da remoto o interventi presso la sede del Titolare per assistenza, manutenzione e risoluzione anomalie	
Logging e monitoraggio	Controlli tecnici	Verifica dei log di sistema/applicazione e degli errori, ove previsto e tecnicamente applicabile	

Nello svolgere le suddette funzioni, INFOMINDS S.P.A. potrebbe avere accesso a dati personali del Titolare ed è autorizzata a trattarli esclusivamente nei limiti di quanto necessario a eseguire i compiti e le attività affidate. Non potranno essere effettuate ulteriori operazioni di trattamento al di fuori di quelle concordate con il presente Contratto o con ulteriori istruzioni formalizzate dal Titolare.

3. Durata del contratto

Il presente Contratto ha efficacia dal momento della sottoscrizione di entrambe le parti e avrà durata pari a quella del Contratto Principale. Qualora il Contratto Principale venisse meno o perdesse efficacia per qualsiasi motivo, ovvero il servizio oggetto del Contratto Principale non fosse più erogato, anche il presente Contratto cesserà automaticamente i propri effetti, salvi gli obblighi destinati per loro natura a permanere.

4. Obblighi generali del Responsabile del trattamento

Il Responsabile è tenuto, in forza di legge e del presente contratto, per sé e per le persone autorizzate al trattamento che collaborano con la sua organizzazione, a:

1. trattare i dati solo per le finalità sopra specificate e per l'esecuzione delle prestazioni contrattuali indicate o derivanti da ulteriori istruzioni scritte del Titolare, anche con riferimento all'eventuale trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale;
2. trattare i dati conformemente alle istruzioni documentate del Titolare; qualora ritenga che un'istruzione costituisca violazione del GDPR o di altre disposizioni applicabili in materia di protezione dei dati, informare immediatamente il Titolare;
3. informare il Titolare dell'eventuale obbligo di trasferire dati verso un paese terzo o un'organizzazione internazionale in virtù del diritto dell'Unione o dello Stato membro cui è soggetto, prima del trattamento, salvo che tale diritto vieti l'informazione per rilevanti motivi di interesse pubblico;
4. garantire la riservatezza dei dati personali trattati nell'ambito del presente Contratto;
5. individuare e designare, nell'ambito della propria struttura, le persone fisiche autorizzate al trattamento, fornendo loro adeguate istruzioni scritte circa le modalità del trattamento e vincolandole alla riservatezza anche per il periodo successivo alla cessazione del rapporto;
6. conservare direttamente e specificamente gli estremi identificativi delle persone fisiche eventualmente preposte quali amministratori di sistema e fornirli prontamente al Titolare su richiesta inviata con congruo preavviso, non inferiore a 15 (quindici) giorni lavorativi;
7. tenere conto, nell'utilizzo di materiali, prodotti, applicazioni o servizi, dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita;
8. non conservare su supporti propri dati personali del Titolare oltre quanto necessario per l'esecuzione del servizio o imposto da obblighi di legge, adottando comunque misure di sicurezza adeguate.

5. Ulteriori Responsabili del trattamento ("Sub-responsabili")

Il Titolare autorizza sin d'ora, in via generale e preventiva, il Responsabile a ricorrere a uno o più Sub-responsabili del trattamento per l'esecuzione delle attività oggetto del presente Contratto.

Il Responsabile garantisce che ciascun Sub-responsabile presenti garanzie sufficienti per l'adozione di misure tecniche e organizzative adeguate ai sensi della normativa applicabile in materia di protezione dei dati personali e si impegna a vincolarlo, mediante contratto o altro atto giuridico, al rispetto di obblighi in materia di protezione dei dati personali sostanzialmente equivalenti a quelli previsti dal presente Contratto.

Il Responsabile rimane responsabile nei confronti del Titolare per l'adempimento degli obblighi gravanti sui Sub-responsabili nei limiti previsti dalla normativa applicabile.

L'elenco aggiornato dei Sub-responsabili è reso disponibile dal Responsabile su richiesta del Titolare.

6. Misure di sicurezza

Il Responsabile è tenuto ad adottare le misure di sicurezza riportate all'Allegato 1 e, comunque, a predisporre e attuare ulteriori misure tecniche e organizzative adeguate al rischio, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Il Responsabile deve assicurare un livello di sicurezza adeguato al rischio, in particolare contro:

- la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso, in modo accidentale o illecito, a dati personali trasmessi, conservati o comunque trattati;
- il trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento.

Il Responsabile dichiara altresì di essere consapevole che, al fine di garantire l'adeguatezza delle misure di sicurezza rispetto ai rischi, a seguito di un riesame periodico, le misure di sicurezza di cui all'Allegato 1 richieste dal Titolare potrebbero cambiare nel tempo; di ciò il Responsabile sarà debitamente informato dal Titolare affinché possa valutare eventuali adeguamenti che si rendessero necessari.

Il Responsabile non potrà utilizzare i dati personali trattati per conto del Titolare per finalità di addestramento, sviluppo o miglioramento di sistemi di intelligenza artificiale, analytics, profilazione, benchmarking, arricchimento dati o finalità proprie, salvo preventiva autorizzazione scritta del Titolare e adeguata base giuridica.

7. Informazione agli interessati

Spetta al Titolare fornire agli interessati le informazioni previste dalla normativa applicabile in relazione ai trattamenti di dati personali effettuati.

8. Esercizio dei diritti degli interessati

Per quanto di sua competenza, il Responsabile deve assistere il Titolare nell'espletamento degli obblighi di riscontro alle richieste di esercizio dei diritti degli interessati, ivi inclusi diritto di accesso, rettifica, cancellazione, opposizione, limitazione del trattamento, portabilità dei dati e diritto di non essere sottoposti a decisioni automatizzate, ove applicabile.

Nel caso in cui il Responsabile riceva istanze dagli interessati, dovrà darne tempestiva comunicazione scritta al Titolare, preferibilmente a mezzo PEC, allegando copia della richiesta entro 5 giorni dalla ricezione, e dovrà assistere il Titolare con misure tecniche e organizzative adeguate al fine di consentire il riscontro.

9. Notifica della violazione dei dati personali (Data breach)

Venuto a conoscenza di una violazione di dati personali, il Responsabile si impegna a informare il Titolare e a fornire la più ampia collaborazione al Titolare e alle Autorità competenti, ove coinvolte, al fine di soddisfare gli obblighi previsti dalla normativa applicabile.

In particolare, il Responsabile notifica al Titolare, a mezzo PEC, ogni violazione o sospetta violazione di dati personali nel tempo massimo di 48 ore dall'avvenuta conoscenza, allegando ogni documentazione utile per permettere al Titolare di valutare e, se necessario, notificare la violazione all'Autorità di controllo e/o comunicarla agli interessati.

La notifica deve almeno:

- descrivere la natura della violazione dei dati personali, comprese, ove possibile, le categorie e il numero approssimativo di interessati coinvolti e di registrazioni interessate;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere informazioni;
- descrivere le probabili conseguenze della violazione;

- descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e attenuarne i possibili effetti negativi.

Qualora non sia possibile fornire le informazioni contestualmente, esse potranno essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

10. Assistenza nella valutazione d'impatto e nella consultazione preventiva

Il Responsabile, nella misura richiesta dall'art. 28 del GDPR e tenuto conto della natura del trattamento e delle informazioni a sua disposizione, presta ragionevole assistenza al Titolare ai fini dell'eventuale predisposizione della valutazione d'impatto sulla protezione dei dati (DPIA) e della consultazione preventiva dell'Autorità di controllo, ove necessarie.

Qualora le attività di assistenza richieste dal Titolare, ulteriori rispetto agli obblighi di assistenza previsti dalla normativa applicabile o dal presente Contratto, comportino un impiego di risorse del Responsabile eccedente una (1) giornata lavorativa, il Titolare riconoscerà al Responsabile il corrispettivo determinato sulla base dei listini di INFOMINDS S.P.A. vigenti. Il Responsabile fornirà preventiva evidenza dell'effort stimato e, a conclusione delle attività, idonea rendicontazione delle prestazioni svolte. Le attività saranno eseguite previa accettazione del relativo preventivo da parte del Titolare.

11. Responsabile della protezione dei dati

Il Responsabile ha provveduto a nominare un proprio Responsabile della protezione dei dati, il quale risulta contattabile al seguente indirizzo mail dpo@acsgroup.it.

12. Registro delle categorie di attività di trattamento

Il Responsabile dichiara di tenere per iscritto, ove previsto dalla normativa applicabile, un registro di tutte le categorie di attività di trattamento effettuate per conto del Titolare, contenente le informazioni richieste dall'art. 30, par. 2, GDPR.

13. Documentazione, audit e controlli

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal presente Contratto e dalla normativa applicabile, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, effettuate dal Titolare o da altro soggetto da questi incaricato.

Le attività di audit potranno essere svolte anche mediante richiesta documentale, questionari, certificazioni, report di audit indipendenti o verifiche da remoto. Eventuali ispezioni presso le sedi del Responsabile saranno effettuate con congruo preavviso, di almeno 15 giorni lavorativi, durante il normale orario lavorativo, nel rispetto delle misure di sicurezza e riservatezza del Responsabile. Qualora emergano non conformità rilevanti, il Responsabile dovrà predisporre e attuare un piano di remediation entro termini ragionevoli concordati con il Titolare.

Il Responsabile è inoltre tenuto a comunicare tempestivamente al Titolare istanze degli interessati, contestazioni, ispezioni o richieste dell'Autorità di controllo o dell'Autorità giudiziaria, nonché ogni altra notizia rilevante in relazione al trattamento dei dati personali.

In caso di attività di audit ovvero di verifica o revisione delegate a terzo soggetto, qualora venga rilevato tra quest'ultimo e il Responsabile del Trattamento un rapporto di concorrenza ovvero un conflitto di interessi, il Responsabile del Trattamento può rifiutare lo svolgimento delle predette operazioni da parte del soggetto incaricato.

14. Obblighi del Titolare del trattamento

Il Titolare:

- dichiara che i dati personali trasmessi al Responsabile sono stati raccolti e gestiti nel rispetto della normativa applicabile, rimanendo a carico del Titolare l'individuazione della base giuridica del trattamento;
- si impegna a comunicare ufficialmente al Responsabile qualsiasi variazione necessaria nelle operazioni di trattamento dei dati;
- si impegna a documentare per iscritto eventuali istruzioni aggiuntive riguardanti il trattamento dei dati da parte del Responsabile;
- vigilerà, per tutta la durata del trattamento, sul rispetto degli obblighi previsti dal GDPR da parte del Responsabile.

Il presente Contratto si applica esclusivamente ai trattamenti svolti dal Responsabile per conto del Titolare e sulla base delle istruzioni documentate di quest'ultimo. Qualora, nell'ambito del rapporto contrattuale, il Responsabile tratti dati personali per finalità proprie o in adempimento di obblighi normativi propri, tale trattamento dovrà essere qualificato separatamente e non sarà disciplinato dal presente Contratto, salvo diverso accordo scritto tra le parti.

15. Restituzione o cancellazione dei dati al termine delle prestazioni

Alla cessazione, per qualsiasi causa, dei servizi oggetto del presente Contratto, il Titolare avrà la facoltà di recuperare e migrare i propri dati personali per un periodo di quindici (15) giorni dalla data di cessazione del servizio.

Decorso tale termine, e salvo quanto diversamente previsto dalla normativa applicabile, il Responsabile potrà procedere alla cancellazione dei dati personali trattati per conto del Titolare senza necessità di ulteriori comunicazioni.

Resta inteso che il Titolare è responsabile dell'estrazione e della migrazione dei propri dati entro il suddetto termine. Su richiesta del Titolare, il Responsabile potrà fornire servizi di assistenza alla migrazione, soggetti a separata quotazione economica sulla base dei listini di INFOMINDS S.P.A. vigenti.

Il Responsabile potrà conservare i dati personali successivamente alla cessazione del servizio nella misura e per il tempo richiesti dalla normativa applicabile ovvero qualora ciò sia necessario per l'accertamento, l'esercizio o la difesa di un proprio diritto.

Su richiesta del Titolare, il Responsabile rilascerà una dichiarazione attestante l'avvenuta cancellazione dei dati personali, fatti salvi gli obblighi di conservazione previsti dalla legge.

16. Compensi, indennità o rimborsi

La designazione a Responsabile del trattamento non comporta di per sé compensi, indennità o rimborsi ulteriori rispetto a quelli previsti dal Contratto Principale.

Le parti concordano che eventuali attività richieste dal Titolare e non espressamente comprese nei servizi oggetto del Contratto Principale, incluse, a titolo esemplificativo e non esaustivo, attività di supporto in relazione all'esercizio dei diritti degli interessati, audit, verifiche, ispezioni, richieste delle autorità competenti, valutazioni d'impatto o altre attività che comportino un significativo impiego di risorse da parte del Responsabile, potranno essere remunerate

separatamente sulla base delle tariffe del Responsabile vigenti al momento della richiesta o secondo quanto diversamente concordato tra le Parti.

17. Revoca e sostituzione di precedenti accordi

Con il presente Contratto si intende espressamente revocare e sostituire ogni altro atto, nomina, contratto o accordo tra le parti inerente al trattamento dei dati personali, nella misura in cui riguardi i medesimi servizi oggetto del Contratto Principale.

Luogo e data: _____

_____ Titolare del trattamento _____	INFOMINDS S.P.A. Responsabile del trattamento _____

Allegato 1 - ELENCO MISURE DI SICUREZZA, TECNICO ED OPERATIVE

ELENCO MISURE DI SICUREZZA, TECNICO ED OPERATIVE	
Politica di alto livello che tratta la cybersecurity / sicurezza delle informazioni / sicurezza informatica.	Inclusiva di obiettivi e principi
	Approvata dall'alta direzione
	Resa disponibile a tutti i soggetti interni ed esterni rilevanti
	Aggiornata almeno annualmente
Politiche e procedure verticali collegate alla politica di alto livello.	Che normano la gestione degli incidenti
	Che normano il controllo degli accessi fisici
	Che normano il controllo degli accessi logici
	Che normano l'uso accettabile delle risorse IT
	Che normano la gestione degli aggiornamenti
	Che normano la gestione dei cambiamenti
	Che normano lo sviluppo sicuro del software
	Che normano la gestione del ciclo di vita dei sistemi
	Che normano la classificazione delle informazioni
	Che normano la gestione dei log
	Che normano il ciclo di vita dei dati
	Che normano la gestione dei fornitori
Piano per la gestione della continuità operativa.	Che viene testato con periodicità almeno annuale
	Che include la parte IT con una Business Impact Analysis ad esso relativa
	Che prevede un piano di disaster recovery per i servizi critici
	Che è mantenuto aggiornato almeno annualmente
Piano di continuità operativa dei sistemi ICT.	Con allocazione di risorse dimensionate in modo da garantire sempre la disponibilità
	Con ridondanza locale di tutti i sistemi critici adottando soluzioni ad alta affidabilità
	Con ridondanza geografica di tutti i sistemi critici in un sito remoto situato a più di 50 km dal sito primario

Formalizzazione delle responsabilità in merito alla cybersecurity / sicurezza delle informazioni / sicurezza informatica	Sono assegnate ad un Responsabile della Sicurezza delle Informazioni / Cybersecurity o CISO che riporta al responsabile IT o superiore
	Sono assegnate a chi gestisce dei sistemi informativi per garantirne la protezione
	Sono assegnate a tutto il personale affinché le informazioni e i sistemi informativi siano utilizzati correttamente
	Sono assegnate alle terze parti che hanno un ruolo nella protezione delle informazioni
	Sono assegnate a chi deve intraprendere azioni specifiche in caso di emergenza o incidente
	Sono documentate e mantenute aggiornate
Formalizzazione delle responsabilità in merito alla protezione dei dati personali	Nei confronti delle persone autorizzate al trattamento
	Nei confronti degli AdS (interni ed esterni)
	Nei confronti dei Responsabili del trattamento
	Nei confronti delle Società nel caso di attività di trattamento come Responsabile
	Sono documentate e mantenute aggiornate
	Sono supportate dalla presenza di un Data Protection Officer
Interventi formativi orientati ad aumentare la preparazione del personale sul tema della sicurezza delle informazioni e sulla tutela dei dati personali	Con cadenza almeno annuale
	A tutto il personale
	Al momento dell'assunzione e su esigenze specifiche
Elenco dei beni aziendali utilizzati per il trattamento delle informazioni	Sono inventariati i software e le componenti hardware utilizzate
	Sono inventariati i servizi fruiti e forniti
	Includono i dati trattati
	Includono i responsabili di tali beni
	Sono mantenuti aggiornati in modo costante o con periodicità fissa
Regolamentazione dei rapporti con parti terze attraverso clausole contrattuali	Clausole di sicurezza standard che vengono adattate a ogni contratto sviluppate tenendo in considerazione i requisiti dei propri Clienti
	Clausole che richiedono la propagazione dei vincoli di sicurezza lungo tutta la filiera di fornitura

	Clausole sulla non divulgazione delle informazioni
	Clausole sulle misure di sicurezza da osservare
	Clausole sulla gestione della continuità operativa
Valutazione del rischio relativo alla cybersecurity / sicurezza delle informazioni aziendali	Rivalutato almeno annualmente
	Utilizzando metodologie diffuse o di mercato
	Tramite un processo formale e documentato che prevede l'individuazione di un rischio accettabile
	Identificando e documentando minacce, vulnerabilità e impatti
Monitoraggio del livello di conformità della gestione della cybersecurity / sicurezza delle informazioni / sicurezza informatica	Sulla base di un programma formalizzato
	Da una funzione di audit interna o da un fornitore esterno indipendente
	Da personale con qualifiche professionali adeguate
	Con periodicità almeno annuale
Protocolli per lo sviluppo sicuro del software implementato da sviluppatori adeguatamente formati	Applicati con continuità durante tutta la catena di sviluppo e test
	Effettuati test di sicurezza formali prima dei principali passaggi in produzione
	Utilizzato di un ambiente separato da quello di produzione
Assegnazione di un budget per la cybersecurity / sicurezza delle informazioni / sicurezza informatica / per la sicurezza dei dati	Definito e allocato annualmente
Selezione attenta degli impatti dei servizi di Cloud Computing impiegati	Hanno tutti i dati all'interno della UE
	Sono tutti certificati secondo ISO/IEC 27001, 27017, 27018 o equivalenti
	Hanno tutti le responsabilità per la sicurezza formalmente suddivise con il loro fornitore
Valutazione del personale specialistico secondo criteri predefiniti	Richieste informazioni relative all'istruzione ricevuta
	Richieste informazioni relative agli impieghi precedenti
	Verificate, nel rispetto dei vincoli di legge, le informazioni richieste
	Si, e sono configurate delle DMZ che ospitano i sistemi accessibili dall'esterno

Presenza e configurazione di firewall verso internet, a protezione dei server aziendali e verso ogni collegamento a terze parti	Si, e creano delle VLAN con ACL configurate che segmentano la rete secondo le funzionalità necessarie
Utilizzo di reti wireless	Protette con meccanismi di crittografia WPA o superiore e le chiavi crittografiche sono sostituite periodicamente
Effettuazione dei backup delle informazioni aziendali	Secondo procedure definite
	Crittografati
	Sottoposti a test periodici di recovery (al più ogni due anni)
	Sottoposti a test di recovery in ambiente di produzione
	Con cadenza almeno settimanale
	Con possibilità di recupero dei dati fino (al più) alle precedenti 24h dalla compromissione del sistema.
Gestione regolamentata degli accessi logici dalla rete interna ai sistemi e alle principali applicazioni aziendali	Attraverso utenze personali e mai tramite utenze di gruppo o condivise
	Attraverso un'autenticazione a più fattori (password e token o biometrico)
	Per mezzo di password lunghe almeno 8 caratteri
	Per mezzo di password con una scadenza al più ogni 90 giorni
	Impiegando criteri di accesso più restrittivi di quelli applicati agli utenti
Gestione regolamentata degli accessi logici da remoto ai sistemi aziendali	Tramite una VPN o strumento equivalente che protegge la riservatezza del traffico di rete
	Utilizzando un'autenticazione che richiede più fattori di autenticazione (password e token o certificato o biometrico)
	Utilizzando un'autenticazione che richiede un'utenza individuale
	Solo se espressamente autorizzati e periodicamente confermati
Gestione regolamentata degli utenti a livello di sistema operativo e, ove applicabile, di software applicativi	A livello centrale
	Con privilegi corrispondenti con il minimo indispensabile per operare e gli amministratori sono limitati a un ristretto gruppo
	Tempestivo allineamento con le nuove assunzioni, con i cambi di ruolo e i licenziamenti

	Sottoposti a riesame sistematico dei privilegi con periodicità almeno semestrale
Controllo delle patch di sicurezza pubblicate dai vendor	Controllate costantemente e verifica dell'applicabilità
	Ove siano applicabili vengono testate in modo esaustivo su sistemi di test prima del rilascio
	Sono classificate in base alla loro criticità e rilasciate di conseguenza
Vulnerability assessment	Su tutti i sistemi informativi interni con una cadenza semestrale o superiore
	Classificando le vulnerabilità riscontrate in base alla loro criticità e risolvendole di conseguenza
	Utilizzando strumenti e personale qualificati
	A livello infrastrutturale
	A livello applicativo
Penetration test	Su tutti i sistemi informativi esposti con una cadenza annuale o superiore
	Classificando le vulnerabilità riscontrate in base alla loro criticità e risolvendole di conseguenza
	A livello infrastrutturale
	A livello applicativo
Registrazione dei log sui sistemi	Sì, e con controlli sulla loro integrità
	Con riesame periodico
	Con uno o più sistemi centralizzati
	Utilizzando un riferimento temporale allineato con una sorgente esterna affidabile
Misure di protezione dei dati memorizzati sui sistemi (data at rest)	Applicando soluzioni di cifratura forte del disco su tutti i sistemi
	Implementando firewall applicativi che filtrano le richieste ai database
	Implementando strategie di controllo degli accessi granulari
Misure di protezione dei dati scambiati con i sistemi attraverso Internet (data in transit) e per l'accesso amministrativo (ivi incluse credenziali, token di sessione ed eventuali altri elementi analoghi)	Applicando esclusivamente protocolli di comunicazione sicuri che implementano una cifratura forte del dato
	Adottando misure di autenticazione della sorgente o del destinatario

Protezione degli endpoint aziendali (portatili, smartphone, tablet)	Tramite password del BIOS o equivalente
	Tramite cifratura del disco o equivalente
	Tramite nome utente e password del sistema operativo
	Tramite criteri di sicurezza impostati con una piattaforma MDM (Mobile Device Management)
Configurazione e attivazione di sistemi base di protezione	Anti-malware con aggiornamento automatico o almeno giornaliero delle definizioni
	EDR (Endpoint Detection and Response)
	Antispam
	Proxy Firewall con funzionalità anti-malware
	IDS (Intrusion Detection System) o IPS (Intrusion Prevention System)
	DRM (Digital Rights Management)
	Anti-APT (Advanced Persistent Threat)
	SIEM (Security Incident and Event Management)
	File integrity monitoring
	Record DNS DMARC, DKIM ed SPF
Regolamentazione dell'uso di strumenti di elaborazione personale (inclusi tablet e smartphone)	Solo per navigare su Internet e attraverso reti guest separate
	Con l'obbligo di memorizzare e trasmettere i dati aziendali esclusivamente in forma crittografata
Regolamentazione della gestione degli incidenti relativi alla sicurezza delle informazioni / cybersecurity /dati personali	Registrazione, analisi, classificazione, azioni r e risoluzione
	Regolamentazione di un'eventuale condivisione con soggetti terzi secondo quanto previsto
	Supporto di personale specializzato disponibile 24/7 o di un SOC esterno
	Piano dettagliato di risposta agli incidenti che viene aggiornato periodicamente
	Analisi delle cause di ogni incidente usata anche per aggiornare il piano di risposta
	Test periodici per la risposta agli incidenti
	Attività di analisi forense in caso di necessità
Regolamentazione della notifica e della comunicazione degli incident e i dati breach	Coinvolgimento di varie funzioni nell'analisi
	Condivisione delle valutazioni

Cancellazione sicura dei dati	Attraverso sovrascrittura logica o distruzione fisica di tutti i supporti che lasciano l'azienda o vengono riassegnati in modo da rendere irrecuperabili i dati
	Richiedendo ai manutentori dei sistemi di assicurare la cancellazione sicura dei supporti da loro sostituiti o dismessi
Policy di data retention	Cancellazione anche automatica dopo i periodi di data retention previsti
	Verifiche periodiche sui tempi di data retention
Regolamentazione dei cambiamenti ai sistemi informativi e ai software	Registrati in modo da includere informazioni circa il richiedente, l'impatto previsto e la tipologia di cambiamento
	Approvati da un soggetto diverso dal richiedente prima della loro effettuazione
	Sottoposti a test prima del loro rilascio in produzione
Regolamentazione della configurazione dei sistemi operativi e dei principali software installati sui sistemi informativi	Effettuata modificando le configurazioni di default secondo procedure di hardening definite
	Basata su best practice di settore per l'hardening dei sistemi informativi
	Controllata centralmente attraverso sistemi o meccanismi di gestione delle configurazioni
	Aggiornata almeno annualmente
	Conforme al principio di minima funzionalità necessaria
	Verificata periodicamente per individuare modifiche non autorizzate
Adozione di sistemi di monitoraggio	Per individuare e registrare l'indisponibilità di un sistema
	Per verificare il traffico di rete
	Per verificare l'uso delle risorse
	Per verificare il funzionamento dei sistemi di sicurezza
	Per inviare allarmi in tempo reale in caso di anomalie o malfunzionamenti
Formalizzazione dell'architettura applicativa rilevante	Documento di descrizione complessiva dell'architettura dell'applicazione
	Documento di descrizione dei layer dell'applicazione (es.: database server, application server, web server, …)

	Documento che elenchi e descriva le interfacce di comunicazione dell'applicazione (protocolli, porte utilizzate, etc.)
Controlli relativi all'accesso al perimetro dell'organizzazione	Misure di videocontrollo
	Allarmi antintrusione al di fuori degli orari di ufficio
	E' mediato da una reception per ogni punto di accesso
Regolamentazione dell'accesso ai locali che ospitano i server	Il personale esterno accede solo se accompagnato
	E' effettuato tramite chiavi fisiche assegnate al personale interno
	E' registrato dettagliatamente e le informazioni raccolte sono mantenute almeno per 3 mesi
	Sistemi di antintrusione
Controllo della temperatura e dell'umidità nei locali che ospitano i server	La temperatura è controllata e sono configurati allarmi al superamento di soglie definite
	L'umidità è controllata e sono configurati allarmi al superamento di soglie definite
	Sono presenti apparati di condizionamento ridondati
Sistemi ridondanti di alimentazione elettrica nei locali che ospitano i server	Attraverso UPS
	Sì, con test periodici del funzionamento di UPS e/o gruppi elettrogeni
Sistemi di protezione da incendi dei locali che ospitano i server	Rilevatori antifumo collegati a un sistema di allarme
	Estintori manuali
Protezione degli archivi cartacei principali	Mantenuti chiusi a chiave al di fuori dell'orario lavorativo