DPA – Data Processing Agreement

Ai sensi dell'art. 9 della Legge sulla Protezione dei Dati (LPD) e dell'art. 28 del Regolamento (UE) 2016/679 (GDPR), il Responsabile del trattamento dichiara di essere stato informato dell'obbligo di fornire adeguate garanzie contrattuali in materia di sicurezza, riservatezza e trasferimento dei dati personali. Il Responsabile riconosce che l'obiettivo del presente DPA è garantire l'adempimento degli obblighi previsti dalla LPD, dal GDPR e da qualsiasi altra normativa nazionale o internazionale applicabile in materia di protezione dei dati. Inoltre, il DPA e i suoi allegati costituiscono le Istruzioni fornite dal Titolare del trattamento al Responsabile per l'esecuzione del servizio, in conformità alle disposizioni di legge e alle linee guida delle autorità di protezione dei dati competenti.

Indice

1. DEFINIZIONI

Ai sensi dell'art. 5 della LPD e dell'art. 4 del GDPR s'intende:

"Dati personali" tutte le informazioni concernenti una persona fisica identificata o identificabile.

Si riferisce a qualsiasi informazione relativa a un **Utente** identificato o identificabile, direttamente o indirettamente, in particolare con riferimento a un identificativo come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più fattori specifici della loro identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale.

"Trattamento" qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la registrazione, la conservazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione, la cancellazione o la distruzione di dati.

"Titolare del trattamento" il soggetto, privato o pubblico, che determina, singolarmente o congiuntamente con altri, le finalità e i mezzi del trattamento dei dati personali. Il Titolare del trattamento è il soggetto che, sotto la propria responsabilità, stabilisce le finalità e le modalità del trattamento, ed è responsabile per l'osservanza della normativa in materia di protezione dei dati.

Si riferisce al **Cliente** ovvero il soggetto giuridico che conclude il Contratto mediante la sottoscrizione del Modulo d'Ordine per conto della quale i Dati personali vengono elaborati dal Responsabile del trattamento.

"Responsabile del trattamento" il soggetto, privato o pubblico, che tratta i dati personali per conto del Titolare del trattamento. Il Responsabile del trattamento è il soggetto che tratta i dati personali sotto l'autorità del Titolare rispettando le istruzioni impartite dallo stesso. In entrambi i casi, il Responsabile è tenuto a garantire la protezione dei dati e a seguire le disposizioni legali in materia di sicurezza.

Si riferisce a **TeamFence** che elabora i dati su istruzione del Titolare del trattamento.

"Sub-Responsabile" il soggetto a cui il Responsabile del trattamento affida, in tutto o in parte, l'esecuzione di attività relative al trattamento dei dati personali, restando comunque responsabile (nei confronti del Titolare del trattamento) della conformità alle normative applicabili sulla base delle istruzioni ricevute. Il Responsabile del trattamento mantiene la piena responsabilità per la protezione dei dati e per l'osservanza delle istruzioni impartite nei confronti del Titolare del trattamento.

Si riferisce principalmente a eventuali terze parti a cui **TeamFence** subappalta parti del sevizio erogato.

"Comunicazione" Si intende la trasmissione di dati personali o il fatto di renderli accessibili.

"Violazione della sicurezza dei dati (Data Breach)" Si intende una violazione della sicurezza in seguito alla quale, in modo accidentale o illecito, dati personali vengono persi, cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate.

"Autorità competente" ai sensi della LPD e del GDPR, si intende l'ente o l'organo designato dalle rispettive normative per vigilare sul rispetto delle disposizioni relative alla protezione dei dati personali. In Svizzera, l'autorità competente per l'applicazione della LPD è l'Incaricato Federale per la protezione dei dati e la trasparenza (IFPDT), mentre a livello europeo, ai sensi del GDPR, l'autorità competente è l'autorità di protezione dei dati stabilita in ogni Stato membro dell'Unione Europea. Queste autorità sono responsabili della supervisione, dell'adozione di provvedimenti in caso di violazioni e dell'assistenza a individui e organizzazioni in materia di protezione dei dati.

2. PARTI COINVOLTE

La Società

TeamFence SA, con sede legale in Via Cantonale 19 6900 Lugano, Svizzera c/o Cortesi & Associati SA, CHE 197.469.909 (Svizzera), di seguito denominata "TeamFence" o "Responsabile del trattamento" ai sensi dell'art. 5 lett. k) della LPD e degli artt. 4(8) e 28 del GDPR.

E:

Il Cliente il soggetto giuridico o persona fisica che conclude il Contratto e utilizza direttamente i Servizi nel seguito anche "Titolare del trattamento" ai sensi dell'art. 5 lett. j) della LPD e dell'art. 4(7) e 24 del GDPR.

3. AMBITO DI APPLICAZIONE SCOPO DEL DPA

I trattamenti di Dati Personali sono esternalizzati al Responsabile del trattamento dal Titolare del trattamento, in conformità con le condizioni stabilite nel presente DPA. L'obiettivo del DPA è garantire la protezione dei Dati personali affidati o messi a disposizione del Responsabile del trattamento nell'ambito delle sue operazioni. Esso definisce i diritti e gli obblighi sia del Titolare che del Responsabile del trattamento.
I dettagli relativi all'ambito di applicazione, alla durata del trattamento, alla natura e agli scopi del trattamento, nonché alla tipologia di dati personali e alle categorie di soggetti interessati per ciascun tipo di trattamento, sono specificati nell'***Appendice 1*** del presente DPA.

4. OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

Gli obblighi del Responsabile del trattamento, come definiti nel presente DPA, si intendono regolati in conformità alle disposizioni della LPD e del GDPR. Ogni riferimento a tali normative deve essere inteso come un riferimento agli obblighi previsti dalle normative vigenti in materia di protezione dei dati personali. Con l'adozione del presente DPA, il Responsabile del trattamento si impegna nei confronti del Titolare del trattamento, assumendo una serie di obblighi specifici. Il Responsabile del trattamento dichiara di essere pienamente informato dell'obbligo di fornire garanzie contrattuali adeguate in materia di sicurezza, riservatezza e trasferimento dei Dati personali. Il Responsabile riconosce che l'obiettivo del presente DPA è garantire l'adempimento degli obblighi previsti dalle normative applicabili e conferma che il presente accordo è strettamente connesso e inscindibile dal servizio a lui affidato dal Titolare del trattamento.

Obblighi del Responsabile del trattamento:

I. Istruzioni fornite dal Titolare del trattamento:
Ai sensi dell'art. 9 della LPD e dell'art. 28, par. 3 del GDPR, il Responsabile del trattamento deve assistere e supportare il Titolare nella corretta gestione delle operazioni di trattamento, che devono essere effettuate nel rispetto della LPD e del GDPR. A tal proposito, il Responsabile del trattamento deve trattare i dati personali solo sulla base di istruzioni documentate del Titolare, anche in caso di comunicazione dei dati personali a un Paese situato al di fuori Svizzera, UE e SEE, a meno che non sia richiesto dalla Legge. In tal caso, il Responsabile del trattamento deve informare il Titolare di tale obbligo di legge prima del trattamento. Le istruzioni al Responsabile del trattamento sono esclusivamente quelle riportate nel presente documento, e le Parti concordano che nessun altro aspetto o incarico è contemplato al di fuori di quanto espressamente indicato, se non previo accordo specifico tra le Parti.

II. Riservatezza:
Il Responsabile del trattamento deve garantire, per sé e per le persone autorizzate da lui stesso o dal Titolare del trattamento a trattare i dati personali, la piena riservatezza rispetto ai trattamenti effettuati. Sarà cura del Responsabile del trattamento, qualora lo ritenga opportuno, vincolare le persone autorizzate al trattamento dei dati alla segretezza mediante un adeguato obbligo legale di riservatezza, anche per il periodo successivo alla cessazione del rapporto di lavoro con il Responsabile del trattamento, in relazione ai trattamenti da esse effettuati (art. 8 LPD e art. 32 del GDPR).
III. Misure di sicurezza:
Ai sensi dell'art. 8 della LPD e dell'art. 32 del GDPR, il Responsabile del trattamento è tenuto a mettere in atto misure tecniche e organizzative adeguate, per garantire un livello di sicurezza adeguato al rischio in relazione al trattamento dei dati effettuato. Si veda l'***Appendice 2***.
IV. Richieste di informazioni: Il Responsabile del trattamento riferirà al Titolare del trattamento, nel caso in cui dovesse ricevere richieste di informazioni relative al trattamento di dati personali effettuato per conto del Titolare del trattamento. L'obbligo di reporting da parte del Responsabile del trattamento si intende limitato a quanto previsto dal presente DPA (es. richieste pervenute dagli interessati al trattamento, da Autorità competenti in materia di protezione dei dati).
V. Audit:
Il Responsabile del trattamento, previa adeguata informazione e accordo tra le Parti, contribuirà alle attività di audit (nel limite di 1 audit per anno solare).
VI. Persone autorizzate al trattamento dei dati:
Il Responsabile del trattamento si avvale di persone autorizzate al trattamento dei dati che operano sotto la sua responsabilità, in quanto incaricate del trattamento, e alle quali fornisce specifiche istruzioni scritte (artt. 6 e 8 LPD, art. 1 OPDa e relativo rapporto esplicativo, art. 29 del GDPR), è compito del Responsabile designato vigilare sulla corretta esecuzione delle istruzioni impartite, garantendo che il trattamento dei dati sia conforme alle normative applicabili sulla protezione dei dati personali. In particolare, il Responsabile deve assicurarsi che tutte le persone autorizzate al trattamento agiscano esclusivamente sotto la sua direzione e seguano le istruzioni stabilite dal Titolare del trattamento.
VII. Sub responsabile:
Ai sensi dell'art. 9 della LPD e dell'art. 28, par. 2 del GDPR, il Titolare autorizza il Responsabile del trattamento, qui designato, a nominare un altro Responsabile (di seguito "Sub responsabile") per l'esecuzione di specifiche attività di trattamento. Il Responsabile del trattamento trasmetterà al Titolare del trattamento la nomina del "Sub responsabile" e informerà il Titolare del trattamento di eventuali modifiche relative all'aggiunta o alla sostituzione di altri Responsabili del trattamento, alle quali il Titolare del trattamento conserva il diritto di opporsi. Gli stessi obblighi di protezione dei dati contenuti nel contratto tra il Titolare e il Responsabile del trattamento sono imposti al "Sub responsabile" mediante un accordo specifico. Il "Sub responsabile" è tenuto a: osservare, valutare e organizzare il trattamento dei dati personali e la loro protezione (mettendo in atto tutte le misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio derivante dal trattamento dei dati effettuato) in modo che siano trattati in modo lecito e pertinente e nel rispetto della normativa vigente. Qualora il "Sub responsabile" del trattamento non adempia ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare del trattamento la piena responsabilità per l'adempimento degli obblighi del "Sub responsabile" anche per il risarcimento di eventuali danni causati dal trattamento, a meno che non dimostri che l'evento dannoso non gli è in alcun modo imputabile. Il Responsabile del trattamento dovrà fornire al Titolare del trattamento l'elenco dei "Sub responsabili" autorizzati e del luogo di trattamento, utilizzando l'***Appendice 3***.
VIII. Registro dei trattamenti:
Ai sensi dell'art. 12 della LPD e dell'art. 30 del GDPR, il Responsabile del trattamento è tenuto a mantenere un registro delle attività di trattamento svolte sotto la sua responsabilità. Il Registro, che può essere anche in formato elettronico, deve contenere una serie di informazioni dettagliate che il Responsabile raccoglie interagendo con i reparti o gli uffici della società che trattano i dati personali per conto del Titolare. In particolare, il Registro deve includere:

- l'identità del Responsabile del trattamento;
- l'identità del Titolare del trattamento;
- i trattamenti effettuati per conto di ciascun Titolare;
- una descrizione generale delle misure adottate per garantire la sicurezza dei dati personali, se possibile;
- se i dati sono comunicati all'estero, l'indicazione dello Stato destinatario e delle garanzie adottate per la comunicazione all'estero.

Il Responsabile del trattamento deve mettere il Registro a disposizione delle Autorità Competenti, se richiesto, affinché possa essere utilizzato come strumento di controllo dei trattamenti effettuati.
IX. Diritti dell'interessato:
Ai sensi del GDPR e della LPD, il Responsabile del trattamento deve informare tempestivamente il Titolare del trattamento, per iscritto, del ricevimento di eventuali richieste da parte degli interessati riguardanti, tra l'altro, le finalità e le modalità del trattamento, l'origine dei dati, l'aggiornamento, la rettifica, la cancellazione, la portabilità, la limitazione del trattamento o l'opposizione al trattamento (compresa la profilazione) o la revoca del consenso prestato. In particolare, il Responsabile del trattamento è tenuto a:

- coordinarsi con le funzioni interne incaricate dal Titolare del trattamento di relazionarsi con i soggetti interessati;
- informare tempestivamente per iscritto il Titolare del trattamento, allegando copia della richiesta;
- accertare l'identità del richiedente per verificare la legittimità della richiesta;
- attivare le procedure necessarie per dare seguito alle richieste di esercizio dei diritti degli interessati, senza ingiustificato ritardo.

X. Data Breach (Violazione dei dati):
Ai sensi dell'art. 24 della LPD e degli articoli 33 e 34 del GDPR, il Responsabile del trattamento deve informare tempestivamente il Titolare del trattamento, senza ingiustificato ritardo, nel caso venga a conoscenza di una violazione dei dati personali (Data Breach). Il Titolare del trattamento, in seguito alla notifica, potrà procedere, se necessario, a notificare la violazione all'autorità di protezione dei dati e, se la violazione presenta un rischio elevato per i diritti e le libertà delle persone fisiche, a notificare la violazione all'interessato.
Il Responsabile del trattamento supporta il Titolare nella gestione delle violazioni dei dati, fornendo tutti gli elementi necessari per gestire la violazione e documentando per iscritto ogni incidente subito, le circostanze che l'hanno causato, le conseguenze e le misure correttive adottate.
Le Parti concordano che il Responsabile deve notificare la violazione dei dati al Titolare del trattamento entro 24 ore dal momento in cui ne è venuto a conoscenza.
XI. Trasferimenti di Dati Personali:
In ottemperanza a quanto previsto dalla LPD e dal GDPR, i trasferimenti di dati personali verso Paesi al di fuori della Svizzera, dell'Unione Europea e dello Spazio Economico Europeo, possono avvenire solo se soddisfano entrambe le seguenti condizioni:
a) Indicazione del luogo del trattamento: Il Responsabile del trattamento si impegna a indicare con precisione il Paese o la località dove avviene il trattamento dei dati personali, riportando l'ubicazione dei trasferimenti nell'***Appendice 3***.
b) Quadro giuridico adeguato: Il trasferimento di dati personali deve avvenire in un contesto che rispetti le condizioni di adeguatezza e conformità stabilite dalla LPD e dal GDPR. In tal caso, il Responsabile del trattamento dovrà garantire che il trasferimento sia coperto da uno dei seguenti strumenti giuridici:
- Documenti che dimostrino che il Responsabile del trattamento nonché i Sub-Responsabili rispettano le condizioni imposte dalla LPD e dal GDPR, quali ad esempio la Certificazione nel Data Privacy Framework (UE/Swiss – US DPF), le Clausole Contrattuali Standard (SCC) approvate dalla Commissione Europea e adottate dall'Incaricato Federale per la protezione dei dati.
- L'assoggettamento alle Norme Vincolanti d'Impresa (Binding Corporate Rules - BCR), applicabili esclusivamente ai trasferimenti di dati all'interno del Gruppo del Responsabile del trattamento.
Nel caso in cui le condizioni legali per il trasferimento dei dati vengano meno, le Parti convengono di incontrarsi tempestivamente per riesaminare e determinare un quadro giuridico alternativo per il trasferimento dei dati personali in conformità con le leggi applicabili.

5. RESPONSABILITÀ DEL RESPONSABILE DEL TRATTAMENTO

Le responsabilità del Responsabile del trattamento in relazione al trattamento dei dati personali sono definite e disciplinate dal Contratto in essere tra le Parti, che costituisce il quadro giuridico completo e include il presente DPA come parte integrante. Il Responsabile del trattamento si impegna a rispettare gli obblighi previsti dalla LPD, dal GDPR e da altre normative applicabili, come stabilito nel Contratto e nel DPA.

6. INIZIO - DURATA - CESSAZIONE DEL TRATTAMENTO

Il ruolo e le responsabilità assegnati al Responsabile del trattamento con il presente atto hanno la stessa durata ed efficacia del Contratto tra le Parti e sono pertanto tacitamente rinnovati ogni anno fino alla cessazione dell'Contratto o fino alla revoca da parte del Titolare del trattamento. Si rimanda, tutto quanto non preciso, alle disposizioni di dettaglio di cui al Contratto.

Il presente accordo riguarda esclusivamente gli aspetti relativi alla protezione dei dati personali. Esso annulla e sostituisce qualsiasi disposizione contrattuale e/o discussione precedente alla sua entrata in vigore in merito a questo punto. Il presente accordo avrà effetto retroattivo a partire dalla data in cui il **Cliente** ha consentito al responsabile del trattamento di accedere ai dati in qualsiasi modo OPPURE dalla data in cui lo scopo di trattamento è stato affidato al responsabile, se precedente.

Al termine del trattamento per conto del Titolare del trattamento, il Responsabile del trattamento deve cancellare i dati personali e le copie esistenti, secondo le procedure automatizzate previste dal software.
Allo stesso modo il Cliente dovrà distruggere o restituire al Fornitore (a scelta di quest'ultimo) tutte le copie del Software e della documentazione in suo possesso, custodia o controllo e, in caso di distruzione, certificare per iscritto al Fornitore di avervi provveduto.
Ricordiamo inoltre l'importanza degli obblighi di legge in materia di trattamento dei dati personali, nonché il fatto che la violazione di tali norme può comportare sanzioni amministrative e penali sia per il Titolare sia per il Responsabile del trattamento.

Il Responsabile del trattamento riconosce che per l'assunzione del Ruolo di Responsabile del trattamento non gli sarà dovuto alcun compenso o rimborso, come previsto dalla Legge. Qualora il Titolare del trattamento richieda attività accessorie che

comportano costi aggiuntivi (es. coinvolgimento in audit di durata estesa o altre attività non previste nel Contratto), tali costi saranno a carico del Titolare, previa discussione e accordo tra le Parti.

7. **CONTATTI DEL RESPONSABILE DEL TRATTAMENTO**

Il responsabile del trattamento è contattabile all'indirizzo e-mail: privacy@teamfence.io

APPENDICE 1 – DESCRIZIONE DEL TRATTAMENTO

1 – Finalità del trattamento	
(Esempi di finalità: gestione delle assunzioni, gestione dei clienti, indagine di soddisfazione, monitoraggio dei locali, ecc.) Specificare l'asset / DB / Sistema	I dati saranno raccolti e trattati dal responsabile al fine dell'erogazione dei seguenti servizi (previsti dal Contratto tra le Parti): Fornitura dei Servizi come definiti nei Termini e Condizioni. Erogazione dei servizi di Browser Detection and Response, E-Learning e gestione Campagne Phishing, secondo le configurazioni impostate dal Cliente tramite l'Utente Master.
2- Tipologia di dato (personale / sensibile / giudiziario)	
☒ dati identificativi (nome, cognome) ☒ Dati di contatto (indirizzi e-mail aziendale) ☐ Dati di fatturazione ☐ Dati di previdenziali e assicurativi ☐ Dati contabili ☐ Dati retributivi ☐ Stato civile ☐ Immagini ☐ Vita personale (stile di vita, comportamento d'acquisto, tracciamento degli ordini, situazione familiare, ecc.) ☐ Spese sostenute ☐ Formazione, specializzazione ☐ Informazioni economiche e finanziarie (monitoraggio dei pagamenti, reddito, posizione finanziaria, posizione fiscale, ecc.) ☒ Dati di connessione (autenticazione e log di accesso, URL visitati, applicazioni SaaS utilizzate, estensioni installate) ☒ Metadati di sicurezza (eventi di rilevamento minacce, findings, alert, azioni di remediation) ☒ Dati derivanti dalle campagne phishing simulate: tassi di click, segnalazioni, comportamenti ☒ Dati formativi (progress, completamento moduli, risultati test) ☐ Dati di localizzazione (spostamenti, dati GPS e GSM, ecc.) ☐ AVS ☐ Dati che rivelano l'origine razziale o etnica ☐ Dati idonei a rivelare le opinioni politiche ☐ Dati idonei a rivelare le convinzioni religiose o filosofiche ☐ Dati che rivelano l'appartenenza a un sindacato ☐ Dati genetici ☐ Dati biometrici per identificare una persona fisica in modo univoco	//

☐ Dati relativi alla salute ☐ Dati relativi alla vita sessuale o alle preferenze sessuali ☐ Dati relativi a condanne o reati penali	
3 - Categorie di interessati	
☒ clienti ☒ clienti dell'MSP ☒ dipendenti ☒ collaboratori ☒ consulenti e agenti del Cliente ☒ utenti autorizzati ad accedere ai sistemi IT aziendali ☐ fornitori	
4 – Durata del trattamento	
Si vedano le condizioni di cui al punto 4. *Durata del trattamento* e di cui al Contratto.	
5 – Conservazione dei dati	
<u>In caso di conclusione del contratto</u> Il responsabile deve: ☒ distruggere I dati che tratta in qualità di Responsabile del trattamento Entro: si vedano le condizioni di cui al punto 4. *Durata del trattamento* e di cui al Contratto.	//

APPENDICE 2 – MISURE DI SICUREZZA

Ai sensi dell'art. 8 della LPD e dell'art. 32 del GDPR, il Responsabile del trattamento deve adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato ai rischi, tra cui:

1. Pseudonimizzazione e cifratura dei dati personali;
2. Garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi di trattamento;
3. Capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente;
4. Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure di sicurezza.

Il Responsabile deve tenere in considerazione i rischi come la distruzione accidentale o illecita, la perdita, l'alterazione o la divulgazione non autorizzata dei dati. Tutti i trattamenti devono essere conformi sia al GDPR che alla LPD, per garantire la protezione dei dati personali. A tale scopo, il Responsabile fornisce l'elenco delle misure di sicurezza.

AREE DI SICUREZZA	PUNTO	MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI
1. NETWORK E SISTEMI DI SICUREZZA	1.1	Utilizzo di firewall e router configurati specificamente per limitare il traffico dati, sia in entrata che in uscita. Questo controllo impedisce l'accesso da parte di reti e sistemi non attendibili
	1.2	Utilizzo di configurazioni di rete che consentono l'offuscamento degli indirizzi IP dei server di origine (Origin Shielding) e l'instradamento del traffico attraverso una rete Anycast globale, che mitiga nativamente attacchi di tipo DDoS ai livelli 3, 4 e 7 dello stack OSI. Il sistema applica automaticamente un set di regole di sicurezza predefinite per l'identificazione di minacce note e bot malevoli, garantendo al

AREE DI SICUREZZA	PUNTO	MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI
		contempo l'estinzione del traffico non crittografato mediante l'obbligo di protocolli TLS/SSL per ogni transazione di dati.
	1.3	Applicazione del principio del Least Privilege a tutta l'infrastruttura. Ogni componente dell'applicativo è eseguito con privilegi minimi, operando con utenti non-root e restrizioni di accesso alle risorse di sistema e di rete strettamente limitate alle proprie funzioni.
	1.4	Esecuzione di aggiornamenti sistematici dei sistemi operativi (client e server) e degli applicativi di base con cadenza periodica, garantendo la risoluzione delle vulnerabilità note. Le patch critiche di sicurezza vengono installate tempestivamente non appena rilasciate dai fornitori, riducendo al minimo la finestra di esposizione a potenziali minacce e garantendo che il software sia sempre allineato agli standard di protezione più recenti.
	1.5	Panificazione ed esecuzione di attività di Vulnerability Assessment (VA) e Penetration Test (PT) con cadenza almeno annuale sui sistemi critici utilizzati per l'erogazione dei servizi, coinvolgendo ove necessario i nostri sub-responsabili. Analizziamo sistematicamente ogni vulnerabilità o finding emerso, attivando tempestivamente le procedure di rimedio e mitigazione del rischio per garantire la massima protezione dei dati.
2. SICUREZZA DEI DATI	2.1	Il periodo di conservazione dei dati personali deve essere limitato nella misura necessaria richiesta da ogni singolo servizio erogato, nel rispetto degli obblighi legali e/o regolamentari vigenti.
	2.2	Adottiamo protocolli per la cancellazione sicura e irreversibile dei Dati Personali non più necessari alle finalità del trattamento o in fase di dismissione degli asset ICT. Prima dello smaltimento o del riutilizzo di qualsiasi supporto di memoria, garantendo l'impossibilità di recupero delle informazioni. Qualora la cancellazione logica non sia tecnicamente realizzabile, procediamo alla distruzione fisica dei supporti o alla loro totale inattivazione, impedendo definitivamente l'accesso a qualsiasi dato residuo.
	2.3	Garantiamo la massima riservatezza anche per le informazioni analogiche attraverso lo smaltimento sicuro di ogni supporto fisico.
	2.4	I dati di produzione (dati reali) devono essere consentiti e limitati solo agli ambienti di produzione. In casi eccezionali e con le approvazioni necessarie, gli ambienti QA possono elaborare Dati Personali (reali) solo se sono protetti come gli ambienti di produzione. Gli altri ambienti di pre-produzione (es. sviluppo, *test*, UAT,…) devono utilizzare dati resi anonimi o di sintesi.
	2.5	I Dati Personali vengono resi illeggibili (ad esempio sfruttando la crittografia) se archiviati su supporti digitali portatili, di *backup, log files*.
	2.6	Il numero degli archivi di Dati Personali (*database,* file, copie, archivi) è ridotto al minimo, evitando inutili duplicazioni.
	2.7	La trasmissione di Dati Personali su reti aperte, pubbliche o non attendibili, deve essere protetta mediante *strong cryptography* e l'utilizzo di protocolli sicuri. Nel caso in cui la crittografia del canale non sia possibile, i file e gli allegati contenenti Dati Personali devono essere protetti mediante crittografia ogni volta che vengono trasmessi su reti aperte, pubbliche o non attendibili.
	2.8	Utilizzo di strumenti di sicurezza per monitorare e controllare il flusso di Dati Personali attraverso gli *endpoint* e verso le reti esterne.
	2.9	La crittografia dei *database*/archivi di dati deve essere basata su una classificazione appropriata degli *asset* in ambito, in base al livello di criticità. Il

AREE DI SICUREZZA	PUNTO	MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI
		Responsabile (e/o i Sub-Responsabili), in mancanza di una specifica richiesta del Titolare, decide se implementare o meno la crittografia e con quale granularità applicarla (ad esempio a livello di *database/files* o di tabella) e la applica ogni volta che il Titolare ne faccia richiesta.
	2.10	I Dati Personali non devono essere copiati su supporti rimovibili, ad eccezione dei supporti espressamente autorizzati dal Responsabile per attività specifiche.
	2.11	I Dati Personali presenti nello *storage* devono essere protetti mediante crittografia quando vengono memorizzati dai fornitori di servizi *cloud* e/o da altri Sub-Responsabili.
	2.12	I supporti (rimovibili e non rimovibili) contenenti Dati Personali devono essere protetti contro l'accesso non autorizzato attraverso adeguate misure di sicurezza fisica e logica.
	2.13	I dipendenti devono essere adeguatamente istruiti e formati sulle corrette regole di condotta da adottare per la protezione dei Dati Personali contenuti nei documenti cartacei (es. in caso di allontanamento dalla postazione di lavoro assicurarsi che nessuno possa accedere alle informazioni riservate, proteggere i documenti originali e le fotocopie da furto o uso non autorizzato, conservare la documentazione in cassetti e armadi chiusi alla fine della sessione di lavoro).
3. DISPONIBILITA' DEI DATI	3.1	Devono essere messe in atto procedure adeguate a garantire la disponibilità dei Dati Personali (come diritto dell'interessato) in modo tempestivo. Le procedure di *backup* devono garantire copie dei Dati Personali almeno settimanalmente.
4. IDENTITY AND ACCESS MANAGEMENT	4.1	L'autorizzazione ad accedere agli ambienti di produzione contenenti Dati Personali deve essere fornita secondo i principi del "*need to know*" e del "*least privilege*".
	4.2	Le *policy* e le procedure devono essere implementate per garantire la corretta identificazione degli utenti e degli amministratori che accedono alle componenti di sistema che gestiscono i Dati Personali. A ogni utente deve essere assegnato un nome utente prima di consentire l'accesso ai sistemi di autenticazione e ai Dati Personali. Ogni nome utente deve identificare solo una persona.
	4.3	Gli accessi amministrativi remoti individuali ai sistemi che gestiscono i Dati Personali devono essere protetti mediante un meccanismo di autenticazione. Inoltre, si consiglia di dotarsi di strumenti per la gestione delle password (*tool ad hoc*) per garantire la sicurezza delle credenziali.
	4.4	Le *password* per i sistemi e i dispositivi che gestiscono Dati Personali devono essere complesse (almeno otto caratteri e ad esempio una combinazione di lettere maiuscole o minuscole, numeri e caratteri speciali) non facilmente attribuibili all'utente.
	4.5	Le risorse di sistema e il diritto di accesso devono essere assegnati in modo univoco ad ogni *user account*.
	4.6	L'accesso da remoto (da reti esterne) all'ambiente che tratta Dati Personali deve essere protetto mediante autenticazione a più fattori.
	4.7	Tutti gli accessi ai *database* contenenti Dati Personali devono essere protetti / controllati al fine di garantire i principi di "*need to know*", "*least privilege*" e la tracciabilità.
	4.8	I diritti di accesso ai Dati Personali degli utenti devono essere rivisti / ricertificati a intervalli regolari e, in ogni caso, almeno una volta all'anno, secondo il corretto processo di *Identity and Access Management*.

AREE DI SICUREZZA	PUNTO	MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI
5. LOGGING E MONITORAGGIO	5.1	Ove applicabile in relazione alla tipologia di servizio, ogni accesso ai Dati Personali (consultazione, modifica, cancellazione, inserimento) da parte degli utenti qualificati come amministratori di sistema deve essere tracciato registrando le informazioni minime richieste per ricostruire le modalità di accesso effettuato e permettere il monitoraggio sul sistema, registrando almeno: - Identificazione dell'utente - Tipo di evento - Data e ora - Indicazione di successo o fallimento - Fonte dell'evento - Identità dei dati interessati (identificativo del soggetto interessato), dei componenti di sistema o risorse.
	5.2	Il Responsabile (e/o i Sub-Responsabili), a seguito di richiesta del Titolare, ha il dovere di fornire i *log* degli accessi per il trattamento dei Dati Personali.
6. ORGANIZZAZIONE E SICUREZZA DELLE PERSONE	6.1	Devono essere messe in atto procedure adeguate a garantire la disponibilità continua di Dati Personali; il personale di *back up* deve essere identificato per garantire la continuità del servizio all'interessato che desidera accedere ai propri Dati Personali.
	6.2	È necessario attuare un programma formale di sensibilizzazione sulla sicurezza per rendere consapevole tutto il personale delle politiche e procedure relative alla sicurezza dei Dati Personali. Ad esempio, possono essere eseguiti *test* periodici o simulazioni per valutare se i dipendenti fanno clic su un collegamento contenuto in *e-mail* sospette o forniscono informazioni personali / sensibili senza seguire procedure di sicurezza appropriate per verificare l'affidabilità della fonte. Di conseguenza, deve essere fornita una formazione mirata a quei dipendenti che sono vittima del *test.*
	6.3	Devono essere stipulati chiari accordi contrattuali con eventuali sub-fornitori dei servizi, al fine di pattuire la loro responsabilità in merito alla sicurezza dei Dati Personali che elaborano / memorizzano / trasmettono per conto del Titolare. Tali accordi devono riflettere almeno le istruzioni e misure indicate in questo documento.
	6.4	Le responsabilità e i doveri dei dipendenti relative alla riservatezza dei Dati Personali devono essere chiaramente esplicitate come valevoli anche dopo la cessazione o il cambio di impiego.
7. DATA PROTECTION BY DESIGN	7.1	I processi e gli strumenti per il *Secure Software Development Lifecycle* (SDLC) devono essere integrati con controlli e requisiti di sicurezza appropriati, al fine di garantire che i nuovi *software*/applicazioni ICT siano progettati e sviluppati tenendo in considerazione i requisiti della sicurezza integrata.
	7.2	I processi di gestione delle modifiche ICT devono essere integrati con controlli e requisiti di sicurezza appropriati, al fine di garantire la protezione continua del *software* / applicazioni ICT in vigore subito dopo modifiche rilevanti.
8. VIOLAZIONE DEI DATI PERSONALI	8.1	I processi e gli strumenti per la gestione degli incidenti devono essere correttamente implementati e/o migliorati al fine di consentire il rilevamento e la classificazione delle violazioni dei Dati Personali in modo che siano correttamente

AREE DI SICUREZZA	PUNTO	MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI PERSONALI
		comunicati al Titolare affinché possano provvedere entro i termini stabiliti nell'art. 4 lett g).
	8.2	Deve essere creato e mantenuto aggiornato uno specifico registro delle violazioni dei Dati Personali.