DPA – Data Processing Agreement

Nomina del partner a responsabile del trattamento dei dati personali

Definizioni

Nel presente documento denominato "Data Processing Agreement" (d'ora in avanti, "DPA"), i termini adottati hanno il medesimo significato indicato nel Regolamento (UE) 2016/679 (d'ora in avanti, "GDPR"), e nelle Condizioni di fornitura del Servizio (d'ora in avanti, "Contratto").

Art. 1 - Oggetto e scopo del documento

Art. 28 GDPR
Il presente DPA ha ad oggetto modalità e condizioni di trattamento di tutti i dati personali (di seguito, "Dati") trattati dal Partner nell'esecuzione delle attività di cui al Contratto, dati di cui è Titolare Aruba PEC S.p.a. (di seguito "Titolare" o "Aruba PEC"); in relazione a tali Dati, il Partner assumerà pertanto il ruolo di Responsabile del trattamento.
Ai fini del presente DPA, il Titolare e il Partner potranno essere riferiti collettivamente come "Parti".

Art. 2 - Modalità di trattamento dei dati personali

Art. 28 GDPR
Le Parti si danno reciprocamente atto che rispetto ai trattamenti di tutti i Dati di cui all'art. 1 è stata resa idonea informativa ed è stato raccolto il consenso, ove richiesto per legge. La durata del trattamento è strettamente connessa all'oggetto contrattuale; i Dati saranno trattati secondo le finalità proprie del contratto, funzionalmente allo svolgimento dell'oggetto contrattuale ed agli obblighi di legge.
Entrambe le Parti si impegnano a comunicare all'atto di sottoscrizione del presente contratto, gli estremi del Data Protection Officer o del Referente Privacy aziendale, se designati.
In relazione ai Dati, con particolare riguardo alle finalità e modalità del trattamento, il Partner si atterrà alle istruzioni ricevute dal Titolare.
In particolare, si offre qui di seguito un quadro schematico dei possibili trattamenti effettuati in relazione al Contratto, rispetto ai quali, come indicato all'art.1, il Partner assumerà il ruolo di Responsabile del Trattamento:

Esemplificazione delle categorie di dati personali trattati	**Esemplificazione della tipologia di dati personali trattati**	**Finalità del trattamento da parte del Partner**	**Categorie di interessati**
Dati anagrafici	nome, cognome, codice fiscale, luogo e data di nascita, indirizzo fisico e telematico, numero di telefono fisso e/o mobile e indirizzo e-mail aziendali e/o privati; numero della tessera sanitaria ed estremi della carta di identità, titolo di studio ed altri dati personali contenuti nei documenti contrattuali, copia carta di identità.	Adempimenti relativi alla gestione dei servizi di cui al Contratto	dipendenti, collaboratori, clienti partner
Dati particolari	dati relativi allo stato di salute	Adempimenti relativi alla gestione dei servizi di cui al Contratto	dipendenti, collaboratori, clienti partner

Art. 3 - Autorizzazione al trattamento dei dati personali in qualità di Responsabile o Sub Responsabile

Art. 28 GDPR

La presente autorizzazione al trattamento dei Dati da parte del Partner, che, per l'effetto, assume, a seconda dei casi descritti all'art. 1, la qualifica di Responsabile o Sub Responsabile del trattamento, decorre dalla data di sottoscrizione del Contratto, ha validità per tutta la durata del rapporto giuridico intercorrente tra le Parti e potrà essere revocata a discrezione del Titolare.
La perdita da parte del Partner dei requisiti di cui all'art. 28 e al considerando 81 del GDPR, come pure il suo inadempimento agli obblighi di cui al presente DPA e al Contratto, consentirà al Titolare di esercitare il diritto di revoca.
L'esercizio del diritto di revoca da parte del Titolare – senza obbligo di corresponsione di alcun risarcimento e/o indennità al Partner e fatto salvo quanto meglio specificato nel rapporto presupposto – avverrà mediante invio di una comunicazione contenente la manifestazione della volontà di revoca.

Art. 4 - Istruzioni generali per il trattamento di Dati

Art. 28 GDPR
Il Partner si impegna a:

1. collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;
2. individuare e autorizzare le persone al trattamento che operino sotto la propria direzione e/o autorità; dare loro le istruzioni idonee per il trattamento dei Dati ad essi affidati, nel rispetto e nell'osservanza dei limiti previsti dalla normativa applicabile, e procedere alla loro eventuale revoca; In particolare nello svolgimento dei servizi di cui al Contratto rispettare i principi di adeguatezza, pertinenza e non eccedenza;
3. vigilare affinché le persone autorizzate rispettino le istruzioni impartite e le misure tecniche e organizzative implementate;
4. richiamare le persone autorizzate al rispetto delle istruzioni impartite; nei casi più gravi, segnalando al Titolare il mancato rispetto di tali istruzioni;
5. osservare scrupolosamente tutte le misure di sicurezza, tecniche e organizzative, predisposte dal Titolare a protezione dei Dati;
6. ove concordato con separato accordo fra le Parti, conservare i Dati trattati in esecuzione del Contratto secondo le policy di data retention definite dal Titolare;
7. in caso di esercizio da parte dell'Interessato dei diritti di cui agli artt. da 15 a 22 GDPR, adoperarsi in buona fede in modo tale da consentire al Titolare o all'Interessato, a seconda dei casi, di riscontrare esaustivamente e tempestivamente le richieste e di compiere tutte le azioni che, in relazione ad esse, si rendano necessarie.
8. in caso di ricezione di richieste specifiche avanzate dall'Autorità Nazionale per la protezione dei dati personali o altre autorità, il Partner dovrà coadiuvare il Titolare per consentire a quest'ultima di rispondere alle suddette richieste, per quanto di sua competenza;
9. segnalare eventuali criticità al Titolare che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte della stessa, collaborare e a coadiuvare il Data Protection Officer Il Titolare (di seguito, DPO) nello svolgimento delle attività da questi effettuate;
10. coadiuvare il Titolare ed il DPO, segnalando per quanto di propria competenza rispetto all'incarico svolto, la necessità di valutare una analisi attraverso DPIA;
11. coadiuvare il Titolare ed il DPO nella redazione del Registro delle categorie dei trattamenti, segnalando anche, per quanto di propria competenza, eventuali modifiche da apportare al Registro, nel rispetto di quanto a riguardo previsto nel presente DPA;
12. verificare periodicamente o su indicazione del Titolare e/o del DPO che i trattamenti posti in essere rispettino le condizioni di liceità previste dall'art.6 GDPR;
13. individuare e nominare per iscritto i propri Amministratori di Sistema, sia interni che esterni, (di seguito, ADS) impartendo loro sempre per iscritto le idonee istruzioni, e procedere alla loro revoca in caso di perdita di tale qualifica, dandone eventuale conferma al Titolare ove richiesto;
14. vigilare sul rispetto delle istruzioni impartite agli ADS, sovrintendendo alle operazioni loro affidate nell'ambito di operatività consentito dal loro profilo di autorizzazione, ammonendoli, soprattutto, a mantenere l'assoluto riserbo sui Dati di cui vengono a conoscenza, anche incidentalmente o per caso fortuito, in ragione dell'esercizio delle funzioni assegnate;
15. aggiornare periodicamente il documento deputato a chiarire le competenze sui sistemi rispetto ai singoli ADS interni, ed altresì comunicare per iscritto ai medesimi l'avvenuta modifica di tale documento;
16. conservare una mappatura aggiornata degli ADS, predisponendo la documentazione necessaria per il rispetto della normativa, e creando profili di accesso conformi rispetto alla normativa di cui trattasi;

17. Con particolare riferimento con quanto specificato nel Contratto nel merito della soluzione proposta, garantire che la stessa risponda alle esigenze di loggatura degli ADS tenendo conto che le registrazioni oggetto di conservazione devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate, che la detta soluzione dovrà essere funzionale alle operazioni di loggatura degli accessi logici degli ADS e di verifica con cadenza almeno annuale, del loro profilo ai fini di accertare la rispondenza del loro operato alle misure organizzative, tecniche e di sicurezza predisposte per l'esercizio delle funzioni di ADS;
18. controllare periodicamente il corretto funzionamento del sistema di loggatura implementato, affinché questo garantisca la storicizzazione completa, inalterabile e incancellabile degli ADS, con possibilità delle verifiche della loro attività;
19. in caso di malfunzionamento del sistema di loggatura, attivarsi per risolvere le problematiche tecniche eventualmente riscontate;
20. predisporre e rendere funzionanti anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, le copie di sicurezza (operazioni di backup e recovery) dei Dati trattati e delle applicazioni utilizzate in esecuzione del Contratto, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei Dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, nel rispetto di quanto previsto in materia nel presente DPA;
21. accedere con le credenziali di Responsabile ADS e per le relative funzioni di assistenza e supervisione assegnate solo quando ciò si renda necessario ed esclusivamente per il perseguimento di tale incarico. Non sono pertanto ammesse attività ulteriori e diverse da quelle ora autorizzate con riferimento ai privilegi sussistenti;
22. entro il 15 dicembre di ogni anno, fornire al Titolare una relazione annuale relativa a quanto svolto in materia di ADS;
23. comunicare senza indebito ritardo e per iscritto al Titolare qualsiasi criticità supposta o verificata, che possa compromettere i propri sistemi e/o quelli di Il Titolare, ed attivarsi per apportare i correttivi necessari;
24. adottare e rispettare le misure di sicurezza indicate dal Titolare e altresì, individuare misure di sicurezza ulteriori a quelle già in uso, che dovesse ritenere necessarie per l'adeguato livello di protezione dei Dati;
25. vigilare affinché i dati personali degli interessati vengano comunicati solo a quei soggetti esterni (fornitori/consulenti) che presentino garanzie sufficienti nel rispetto di quanto previsto dal presente DPA in tema di subfornitura. Sono altresì consentite le comunicazioni richieste per legge nei confronti di soggetti pubblici;
26. affinché sia sempre sotto monitoraggio un livello di rischio accettabile, è compito del Partner esaminare periodicamente i livelli di rischio sui propri sistemi ed applicativi utilizzati per l'erogazione di tutto quanto forma oggetto del contratto secondo standard riconosciuti. In particolare, è compito del Partner identificare e definire i rischi nonché stimarne le criticità sulla base delle tipologie dei Dati trattati in esecuzione del Contratto il Titolare/Partner e delle peculiarità dei sistemi del Partner;
27. sviluppare strategie di contrasto e di mitigazione dei rischi, atte a ridurre, eliminare o accettare i rischi individuati. Tali strategie devono tener conto del contesto ove opera il Titolare, delle categorie di Dati e di interessati, nonché dei trattamenti effettuati nell'ambito dell'erogazione dei servizi oggetto del Contratto ed al progresso tecnologico raggiunto;
28. in attuazione delle strategie di cui sopra, il Partner deve pertanto definire un piano di sicurezza informatico pluriennale atto a presidiare i Dati trattati in esecuzione del Contratto Titolare/Partner ed i propri sistemi, che tenga conto di misure organizzative (procedurali e documentali) e tecniche (sia fisiche che logiche);
29. il piano di sicurezza informatica deve essere periodicamente riesaminato e perfezionato, ed in particolare in caso di incidenti di sicurezza, variazioni tecnologiche significative, modifiche all'architettura informatica utilizzata, aggiornamenti delle prescrizioni normative o best practices, risultanze di audit;
30. collaborare con altre funzioni aziendali in merito all'aggiornamento di ogni idoneo documento, anche di sintesi, capace di dare evidenza delle soluzioni tecniche ed organizzative, nonché delle politiche di sicurezza informatica adottate;
31. per misurare l'efficacia sul medio e lungo termine le contromisure implementate prevedere attività di monitoring a auditing con il precipuo fine di perfezionare o comunque migliorare tali contromisure;
32. tenersi sempre aggiornato sulle novità che ineriscono la sicurezza informatica, e ciò sia in via autonoma che ricorrendo a terzi qualificati;
33. promuovere iniziative volte a sensibilizzare il tema della sicurezza informatica all'interno della propria struttura;
34. gestire e aggiornare un inventario degli asset hardware e software utilizzati per l'esecuzione del Contratto Titolare/Partner;
35. tenuto conto dei Dati e dei trattamenti effettuati in esecuzione del Contratto Titolare/Partner, pianificare periodicamente vulnerability assessment e/o penetration test sui software e sui sistemi del Partner utilizzati per l'esecuzione del Contratto, ivi comprensivi dei successivi piani di remediation;

36. al fine di gestire adeguatamente eventi, problemi e incidenti, condurre regolarmente attività di monitoraggio sulla prestazione dei sistemi utilizzati per l'esecuzione del Contratto Titolare/Partner;
37. tenere un apposito registro dei data breach onde poter dimostrare al Titolare di essere in grado di rilevare e identificare attraverso i propri sistemi qualunque incidente di sicurezza.
38. Al Partner è richiesta, in ogni caso, una condotta propositiva in tema di data protection, esplicantesi in suggerimenti o/o proposte di modifica sulle misure adottate dal Titolare in adempimento al GDPR
39. Il Partner garantisce, nell'ambito dell'erogazione dei servizi di cui al Contratto e nell'utilizzo degli applicativi messi a disposizione dal Titolare, l'assoluto rispetto delle prescrizioni e dei divieti e delle relative le istruzioni impartiti dal Titolare, mediante specifici documenti riportanti le relative procedure di gestione e di accesso.

Art. 5 - Registro dei trattamenti

Art. 30 GDPR
Il Partner si impegna a coadiuvare il Titolare nella predisposizione degli elementi documentali necessari per i trattamenti di propria competenza, sì da consentire alla stessa la predisposizione e/o l'aggiornamento della documentazione richiesta dalla normativa vigente in materia di protezione del dato personale (quali, a titolo esemplificativo, il registro delle attività di trattamento). Il Partner, sarà tenuto a tenere nota del trattamento dei Dati personali di cui il Titolare è Titolare del trattamento all'interno di un apposito registro, che sarà tenuto in forma scritta, anche in formato elettronico. Tale registro dovrà contenere le seguenti informazioni:
Nome e dati di contatto del Responsabile del trattamento;
Categorie dei trattamenti effettuati per conto del Titolare;
Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e le altre informazioni relative ai trasferimenti di cui alla normativa in materia di protezione dei dati personali;
La descrizione generale delle misure di sicurezza tecniche ed organizzative approntate.

Art. 6 - Portabilità e migrazione

Artt. 20 e 28 GDPR
Il Partner assicura che i Dati trattati in esecuzione del Contratto ed alla soluzione proposta sono predisposti secondo formati e standard in grado di assicurare la leggibilità e la portabilità degli stessi.
Su richiesta del Titolare, il Partner provvederà senza indebito ritardo, tenuto conto anche degli obblighi assunti dal Partner ai sensi del presente DPA relativamente alla cancellazione dei Dati, a fornire i Dati trattati in esecuzione del Contratto in un formato strutturato, di uso comune e leggibile da dispositivo automatico, per consentire al Titolare il rispetto di quanto previsto dalla normativa con riferimento al diritto alla portabilità dei dati dell'interessato.

Art. 7 - Cancellazione dei dati

Art. 28 GDPR
Il Partner, ove previsto da diverso e specifico accordo fra le parti, conserva i Dati trattati in esecuzione del Contratto secondo le policy di data retention definite dal Titolare.
Alla scadenza del Contratto Titolare/Partner od alla data di cessazione dei suoi effetti a qualunque titolo intervenuta, nonché in ogni caso di richiesta del Titolare, il Partner si impegna, previo rilascio di apposita copia qualora detenga i Dati in via esclusiva, alla totale e definitiva cancellazione dalle proprie memorie magnetiche, dai propri sistemi informativi e/o da qualsiasi altro supporto fisico dei Dati trattati in esecuzione del Contratto, salvo quanto diversamente stabilito da obblighi di legge, dando avviso al Titolare ventiquattro ore prima e successiva comunicazione entro i cinque giorni dopo. Le operazioni di cancellazione avverranno in modo sicuro e nel rispetto della normativa di settore, senza arrecar danno agli interessati cui i Dati si riferiscono.

Art. 8 - Privacy by design

Art. 25 GDPR
Qualora il trattamento dei Dati da parte del Partner in esecuzione del Contratto avvenga per mezzo di proprio applicativi, il Partner dovrà garantire che le attività saranno adeguate alle norme vigenti, ivi compresi i provvedimenti dell'Autorità Garante per la

protezione dei dati personali e compiute in conformità ai principi della “privacy by design”, con particolare riferimento ai seguenti aspetti: 1) Approccio proattivo e non reattivo: prevenire e non correggere; valutazione del rischio dalla fase di progettazione precedente all’inizio del trattamento2) Privacy incorporata nella progettazione: principi di pertinenza e minimizzazione, configurazione della Fornitura in modo tale da ridurre al minimo il trattamento e l’acquisizione dei dati personali e identificativi; principio del need to know; principio del least privilege; 3) Piena protezione del ciclo vitale del sistema informatico; 4) Conciliazione tra massima funzionalità e rispetto dei diritti; 5) Visibilità e trasparenza; 6) Centralità dell’utente; 7) Privacy by default.
Il software e gli interventi manutentivi sullo stesso dovranno essere conformi ai suddetti principi di “privacy by design”, così come richiesto dalla normativa in materia di protezione del dato personale. In particolare, il software e gli interventi di manutenzione dello stesso dovranno prevedere: la configurazione di procedure di pseudonimizzazione dei dati personali, per tale intendendosi il trattamento dei dati personali in modo tale che detti dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; la configurazione di procedure di minimizzazione dei dati personali, per tale intendendosi il trattamento dei soli dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali gli stessi sono raccolti; la configurazione di procedure di conservazione del dato personale e conseguente cancellazione o anonimizzazione del medesimo allo spirare del termine indicato dal; l’adeguata possibilità di gestione ed implementazione della manifestazione dei consensi al trattamento dei dati personali da parte dell’interessato nei confronti del Titolare, ove necessario, ivi compresa la documentazione prescritta a tal riguardo dalla vigente normativa e la corretta e necessaria storicizzazione dei consensi stessi da parte del Titolare medesimo. Il Partner si impegna ad eseguire le attività oggetto del presente contratto con personale dotato dei requisiti tecnici e della capacità professionale adeguati alla complessità delle attività stesse, sì da assicurare la conoscibilità dei rischi in riferimento al trattamento dei dati personali.
Le parti concordano che le modalità di svolgimento del servizio indicate nel presente contratto sono considerate idonee al fine di prevenire commistioni tra distinti archivi gestiti dal responsabile del trattamento.

Art. 9 - Misure di sicurezza

Artt. 29 e 32 GDPR
Il Partner garantisce il rispetto delle misure di sicurezza indicate dalla normativa in materia di protezione dei dati personali nonché dai Provvedimenti delle Autorità competenti laddove applicabili con riguardo alle misure logiche, tecniche, fisiche ed organizzative che saranno poste in essere per proteggere i Dati da sottrazione o distruzione intenzionale o accidentale, perdita accidentale, alterazioni, uso non autorizzato, modifiche, divulgazione, diffusione, accessi non previsti e ogni altra forma di trattamento illecito.
In particolare, il Partner garantisce espressamente di aver messo in atto le misure di sicurezza tecniche ed organizzative indicate nel documento “Descrizione delle misure di sicurezza tecniche ed organizzative” allegato sub 1 al presente atto a formarne parte integrante e sostanziale, cui si fa espresso rinvio, garantendone il costante mantenimento per tutta la durata del contratto.
Il Partner garantisce che le misure di sicurezza predisposte sono idonee a garantire su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei dati oggetto di trattamento, nonché adeguate a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento dei Dati.
Il Partner si impegna altresì a mettere in atto le ulteriori misure di sicurezza che il Titolare, a proprio insindacabile giudizio, intendesse ritenere di adottare nel corso della durata del Contratto in essere tra le parti, anche in relazione al contesto normativo tempo per tempo vigente, per garantire un livello di sicurezza adeguato al rischio presentato.

Art. 10 - Audit

Art. 28, co. 3 lett. h GDPR
10.1 Il Partner rende disponibile al Titolare tutte le informazioni necessarie per dimostrare la propria ottemperanza agli obblighi imposti dalla normativa vigente in materia di trattamento di dati personali e dal presente DPA.
A tal fine, il Partner riconosce al Titolare il diritto di analizzare e/o verificare e/o valutare il rispetto da parte del Partner dei suddetti obblighi con particolare riferimento agli obblighi di sicurezza imposti a protezione dei Dati (“Audit”), ove ritenuto necessario e/o opportuno a insindacabile scelta del Titolare, senza corrispettivo ulteriore rispetto a quanto pattuito nel Contratto Titolare/Partner.
Le attività di Auditing potranno essere effettuate anche senza preavviso nella misura massima di quattro volte l’anno e, in aggiunta, tutte le volte che vi siano state violazioni e/o presunte violazioni dei Dati e/o problemi di sicurezza relativi al trattamento dei Dati.
Tali attività potranno essere effettuate dal Titolare ovvero da terzi appositamente incaricati dal Titolare.
Al fine di dare esecuzione a quanto sopra, il Partner si obbliga ad offrire la massima collaborazione in modo da permettere al Titolare, ovvero a terzi dalla stessa designati, di svolgere efficacemente la propria attività di Auditing.
Il Titolare ha diritto di effettuare Audit anche senza preavviso.

Nel corso delle attività di Auditing, il Titolare avrà diritto di accedere direttamente e/o tramite soggetti appositamente incaricati ai locali e/o ai sistemi del Partner, e/o avere copia di ogni dato, documento, informazione, elemento, contenuto di ogni genere e natura che possa risultare necessario, strumentale o comunque utile alla esecuzione dell'Audit medesimo.
Qualunque difetto di conformità dei sistemi del Partner che dovesse emergere nel corso delle attività di Audit rispetto agli obblighi previsti dalla normativa applicabile in materia di trattamento dei dati personali e dal presente DPA, dovrà essere risolta dal Partner a proprie spese e comunque in un lasso di tempo non superiore a due settimane di calendario salvo oggettive e comprovate ragioni che non permettano il rispetto di tale termine e/o salvo motivi di urgenza tali da raccomandare un adeguamento entro un termine più breve; è fatto, in ogni caso, salvo il diritto di il Titolare a pretendere il risarcimento del danno. Qualora, entro il termine sopra stabilito, il Partner non abbia posto rimedio alle eventuali difformità riscontrate, il Titolare avrà facoltà di risolvere il Contratto ai sensi e agli effetti dell'art. 1456 c.c. e di chiedere il risarcimento del danno in linea con le previsioni del Contratto.
10.2 Regolari Audit sulla conformità ai requisiti minimi di sicurezza di cui all'Allegato sub 1 devono effettuarsi almeno con cadenza biennale; i risultati devono essere elaborati sotto forma di una relazione di audit.
La relazione di Audit deve fornire un parere sulla rispondenza delle misure di sicurezza e dei controlli adottati con questi requisiti minimi di sicurezza, identificare eventuali carenze e (se presenti) proporre misure correttive o supplementari se necessario. Esso dovrebbe includere anche i dati, fatti e osservazioni su cui si basano i pareri raggiunti e le raccomandazioni proposte.
La relazione di Audit dovrà essere analizzata dal Responsabile della Sicurezza che dovrà riportare le conclusioni al Titolare del trattamento e restare a disposizione di quest'ultimo.

Art. 11 - Data breach

Artt. 28 e 33 GDPR
Qualora si verifichino eventi che comportino la violazione dei Dati o delle informazioni trattati dal Partner nell'esecuzione del Contratto Titolare/Partner ("data breach"), conosciuta o anche solo sospettata (di seguito, "evento"), il Partner avvertirà il Titolare immediatamente e comunque entro 12 ore dalla scoperta (se non contestuale al momento dell'evento) con comunicazione da inviarsi al seguente indirizzo: privacy@staff.aruba.it contenente tutte le informazioni necessarie a circoscrivere e definire l'evento medesimo. In particolare, la comunicazione contemplerà:
1. La data e l'ora dell'evento, nonché, se differente, il momento della sua scoperta;
2. L'indicazione del luogo in cui è avvenuto l'evento;
3. Una breve descrizione dell'evento;
4. Una sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei Dati e delle informazioni coinvolte nonché la loro natura, con indicazione della loro ubicazione.
Qualora già conosciute, nello stesso termine il Partner comunicherà altresì:
5. Le ragioni che non hanno consentito un'immediata rilevazione dell'evento laddove la scoperta non sia contestuale al verificarsi dell'evento;
6. Il numero approssimativo degli interessati coinvolti.
Laddove le informazioni sub 5. e 6. non siano inizialmente conosciute, il Partner si attiverà per fornire un riscontro ad Il Titolare entro 12 ore dalla prima comunicazione, precisandole una volta apprese.
In ogni caso il Partner assicura la massima collaborazione per approfondire tutti gli aspetti necessari ed utili per precisare l'evento. Una volta definite le ragioni dell'evento, il Partner di concerto con il Titolare e/o altro soggetto da quest'ultimo indicato, si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di un nuovo evento della stessa specie di quella verificatasi.

Art. 12 - Subfornitori

Art. 28 GDPR
Nell'esecuzione del Contratto, il Partner potrà avvalersi, previa autorizzazione scritta del Titolare a pena di nullità, di altri soggetti terzi, nel rispetto delle condizioni e delle prescrizioni ivi previste.
Il Partner dichiara che alla data di sottoscrizione del presente contratto e del Contratto Titolare/Partner i contratti stipulati dal medesimo per l'esecuzione delle attività ivi previste che determinino, o possano determinare, un accesso di terze parti ai segreti aziendali del Titolare e/o ai Dati sono:

Nominativo del Sub fornitore	**Attività svolta rispetto ai Servizi erogati**	**Dati o informazioni cui ha accesso e/o impatto sulle misure di sicurezza**	**Contratto**
			Oggetto: Data di sottoscrizione: Data di scadenza:
			Oggetto: Data di sottoscrizione: Data di scadenza:
			Oggetto: Data di sottoscrizione: Data di scadenza:
			Oggetto: Data di sottoscrizione: Data di scadenza:
			Oggetto: Data di sottoscrizione:

			Data di scadenza:
			Oggetto: Data di sottoscrizione: Data di scadenza:

Con riguardo a tale elenco, è fatto obbligo al Partner di conservare la copia dei contratti sottoscritti con tali terze parti, dai quali risulterà la loro nomina come Sub- responsabili del trattamento e nella quale saranno riportate almeno tutte le prescrizioni contenute nel presente DPA.
Il Partner si obbliga a sottoporre a preventiva autorizzazione del Titolare ogni variazione intervenuta riguardante l'aggiunta o la sostituzione di altri soggetti o delle attività da essi eseguite, dando facoltà al Titolare di opporsi a tali modifiche entro 7 giorni lavorativi a mezzo PEC, trascorsi i quali in mancanza di notifica esse si intendono approvate. In nessun caso, pertanto, il Partner è autorizzato a delegare o subappaltare l'erogazione integrale o parziale dei Servizi di cui al Contratto senza la preventiva autorizzazione scritta del Titolare.
Il Partner garantisce che ogni eventuale soggetto terzo ingaggiato rispetterà le obbligazioni previste dal presente DPA, e garantirà gli standard qualitativi e di sicurezza, anche in materia di protezione dei Dati, richiesti dal Titolare, secondo quanto previsto dal presente DPA.
Il Partner garantisce che i soggetti terzi autorizzati non ricorrano ad altri subfornitori, se non previa autorizzazione scritta da parte del Titolare.
L'avvalimento dei sopra indicati soggetti terzi non comporta alcuna modificazione agli obblighi e agli oneri del Partner che rimane unico e solo responsabile nei confronti del Titolare delle prestazioni da egli eventualmente affidate a terzi.
Il Partner che affidi la fornitura dei Servizi a terzi, pertanto, sarà in ogni caso ritenuto responsabile principale per l'adempimento delle proprie obbligazioni derivanti dal presente DPA e per gli atti, disservizi, ritardi, omissioni o negligenze dei subcontraenti, manlevando il Titolare da qualsiasi responsabilità a riguardo e da qualsiasi richiesta dovesse provenire da terzi in conseguenza dell'intervento dei predetti soggetti.
In caso di inadempimento da parte del Partner agli obblighi di cui ai precedenti commi, il Titolare avrà facoltà di risolvere il Contratto ai sensi e agli effetti dell'art. 1456 c.c e di chiedere il risarcimento del danno in linea con le previsioni del Contratto, ivi compreso l'ammontare delle eventuali sanzioni comminate da qualsiasi Ente e/o Autorità al Titolare derivanti in via diretta e/o indiretta dalle predette violazioni.

Art. 13 - Trasferimento di dati personali verso paesi terzi

Art. 44 GDPR
I Dati trattati dal Partner per l'erogazione dei Servizi oggetto del Contratto, di cui al presente DPA, sono ubicati nel territorio dell'Unione Europea, in ITALIA e in [indicare il numero delle location (uffici, o altro) in cui avverrà il trattamento] siti in cui, compatibilmente alla tipologia delle prestazioni erogate, vengono materialmente eseguite le procedure automatizzate per l'eventuale conservazione, duplicazione, backup e ripristino dei Dati qualora previste dall'accordo fra le Parti.

Art. 14 - Punto di contatto

I dati di contatto del Responsabile della sicurezza, comprensivi di e-mail e riferimento telefonico diretto, devono essere comunicati al Titolare del trattamento entro 30 (trenta) giorni dalla sottoscrizione del DPA. Eventuali modifiche di tali dati di contatto dovranno essere comunicate entro lo stesso termine decorrente dall'avvenuta variazione.
All'interno dei processi di Incident management e Data breach il punto di contatto incaricato dal Partner è il Responsabile della sicurezza.

Art. 15 - Rinvio

Per quanto non espressamente previsto e disciplinato nel presente DPA, le Parti rinviano al Contratto Il Titolare/Partner, alla normativa applicabile in materia di privacy, con specifico riferimento al GDPR, ed alla normativa di settore applicabile ai Servizi erogati con il Contratto.

Allegati:

Le parti dichiarano di ben conoscere tutti gli atti ed i documenti citati ed allegati alla presente scrittura, da ritenersi parte integrante ed essenziale della stessa, di seguito elencati:
Allegato 1: descrizione delle misure di sicurezza tecniche ed organizzative
Resta inteso che in caso di incompatibilità tra le disposizioni contenute nei documenti sopra indicati e quelle del presente accordo, prevarranno queste ultime.

Il Partner

ALLEGATO 1

Descrizione delle misure di sicurezza tecniche ed organizzative

Organizzativo	Alto livello	*Policy e Disciplinari*	Il Partner applica dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi, finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati personali nell'utilizzo delle risorse informatiche.
Organizzativo	Alto livello	*Autorizzazione accessi logici*	Il Partner definisce i profili di accesso nel rispetto dei *least privilege* necessari all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati personali necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.
Organizzativo	Alto livello	*Change Management*	Il Partner ha adottato una specifica procedura mediante la quale regolamenta il processo di Change Management in considerazione dell'introduzione di eventuali innovazioni tecnologiche o cambiamenti della propria impostazione e della propria struttura organizzativa.
Organizzativo	Alto livello	*Incident Management*	Il Partner ha posto in essere una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio.
Organizzativo	Alto livello	*Data Breach*	Il Partner ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare tempestivamente le comunicazioni delle violazioni di dati personali alla Società e all'Utente. Per quanto di pertinenza delll Partner tale procedura, mediante un apposito *incident report*, rileva: o la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali coinvolti; o le probabili conseguenze della violazione dei dati personali; o le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Organizzativo	Alto livello	*Formazione*	Il Partner eroga periodicamente ai propri dipendenti e/o collaboratori responsabili dello svolgimento delle varie attività oggetto del Contratto, con particolare riguardo all'assistenza tecnica, corsi di formazione riguardanti il trattamento dei dati personali ed è in grado di documentarne l'effettuazione.
Organizzativo	Alto livello	*Test delle procedure*	La procedura per la segnalazione, la gestione e la risposta agli incidenti dovrà essere testata almeno una volta all'anno. Tutti i risultati dei test effettati dal Partner per la segnalazione, gestione e la risposta agli incidenti deve essere fornita tempestivamente al titolare del trattamento per la relativa revisione.
Organizzativo	Alto livello	*Distribuzione dei supporti*	Eventuali supporti contenenti Dati Personali possono essere distribuiti solo se i dati sono stati crittografati per garantire che tali Dati Personali e altre informazioni non siano intelligibili o non possono essere manipolate in transito.
Organizzativo	Alto livello	*Reti di comunicazione*	I Dati Personali potranno essere eventualmente diffusi tramite reti di comunicazioni elettroniche solo se essi sono stati crittografati, cifrati o è utilizzato un altro meccanismo per garantire che le informazioni non sono intellegibili o non siano manipolate da terze parti
Tecnico	Alto livello	*Capacity planning*	Il Partner ha posto in essere un processo operativo per il riesame periodico delle prestazioni e delle capacita delle risorse IT organizzato con l'obiettivo di garantire performance idonee alle esigenze e alla continuità del servizio gestito. Il processo include la previsione delle esigenze future in base al carico di lavoro
Tecnico	Alto livello	*Hardening*	Sono previste e rese operative apposite attività di hardening finalizzate a prevenire il verificarsi di incidenti di sicurezza minimizzando le debolezze architetturali dei sistemi operativi, delle applicazioni e degli apparati di rete considerando - in particolare - la diminuzione dei rischi connessi alle vulnerabilità di sistema, la diminuzione dei rischi connessi al contesto applicativo presente sui sistemi e l'aumento dei livelli di protezione dei servizi erogati dai sistemi stessi
Tecnico	Alto livello	*Patch Management*	E' gestito un apposito processo di patch management finalizzato a garantire il costante aggiornamento dei sistemi al fine di prevenirne le vulnerabilità e a correggerne i difetti
Tecnico	Alto livello	*Firewall, IDPS*	I dati personali sono protetti contro il rischio d'intrusione, come previsto dalle vigenti e future normative in materia e mediante sistemi di Intrusion Detection & Prevention mantenuti aggiornati in relazione alle migliori tecnologie disponibili
Tecnico	Alto livello	*Protection from malware*	I sistemi sono protetti contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica (almeno ogni sei mesi). Sono in uso strumenti antivirus mantenuti costantemente aggiornati
Tecnico	Alto livello	*Sicurezza linee di comunicazione*	Per quanto di propria competenza, sono adottati dal Partner protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile, tali da garantire la sicurezza nella trasmissione dei dati e nel processo di autenticazione.
Organizzativo	Alto livello	*Accesso ai locali*	L'accesso fisico agli uffici dove si eroga il servizio è consentito esclusivamente al personale autorizzato secondo le modalità disciplinate in un'apposita procedura. Eventuali visitatori o soggetti esterni che dovessero avere necessita di accesso alle aree uffici, qualora autorizzati all'ingresso temporaneo, sono accompagnati durante l'intera visita da parte di personale dotato di autorizzazione permanente.

Tecnico	Alto livello	*Protezione fisica uffici*	La sicurezza perimetrale è garantita da sistemi di allarme configurati in relazione alle caratteristiche delle infrastrutture e da sistemi di videosorveglianza monitorati. I locali interni sono dotati di idonee misure di sicurezza ambientale (impianti antincendio, sistemi ups / gruppi elettrogeni per la continuità della fornitura di energia agli impianti, linee di comunicazione ridondate, etc.). Tutti gli impianti e i mezzi tecnici sono sottoposti a regolari e periodiche manutenzioni effettuate da ditte specializzate. I locali sono conformati al disposto del D.Lgs. 81/2008 *Testo Unico sulla salute e sicurezza sul lavoro* - e successive modifiche ed integrazioni.
Tecnico	Alto livello	*Credenziali di autenticazione*	I sistemi sono configurati con modalità idonee a consentire l'accesso unicamente a soggetti dotati di credenziali di autenticazione, che ne consentono la loro univoca identificazione, finalizzate al superamento di una procedura di autenticazione. Le stesse possono consistere in un codice associato a una parola chiave, riservata e conosciuta unicamente dal soggetto o in un dispositivo di autenticazione in possesso e uso esclusivo dello stesso, eventualmente associato a un codice identificativo o a una parola chiave.
Tecnico	Alto livello	*Sicurezza della password*	Relativamente alle caratteristiche di base ovvero, obbligo di modifica al primo accesso, lunghezza minima, assenza di elementi riconducibili agevolmente al soggetto, regole di complessità, scadenza, history, valutazione contestuale della robustezza, visualizzazione e archiviazione, la parola chiave è gestita conformemente alle best practice. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza.
Tecnico	Alto livello	*Strong Authentication*	Per quanto di competenza del Partner, ove sono trattati dati personali rilevanti in relazione ai rischi per i diritti e le libertà delle persone fisiche e/o ove le caratteristiche dei profili di autorizzazione sono di alto livello (a titolo puramente esemplificativo *full rights*) sono adottate tecniche di strong authentication idonee ad assicurare l'accesso esclusivamente al personale preposto all'esercizio di tali mansioni.
Tecnico	Alto livello	*Loggin*	I sistemi sono configurati con modalità che consentono il tracciamento degli accessi, e ove appropriato delle attività svolte, in capo alle diverse tipologie di utenze tecniche. Tali log saranno protetti da adeguate misure di sicurezza che ne garantiscono l'integrità.
Tecnico	Alto livello	*Continuità operativa*	Ove gli accordi contrattuali lo prevedono, sono adottate misure idonee per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi, compatibili con i diritti degli interessati. A garanzia del corretto funzionamento ed efficacia dei processi di backup in termini di integrità e disponibilità delle copie realizzate, vengono eseguiti appositi test di ripristino con frequenza stabilita in relazione alla rilevanza dei dati (generalmente trimestralmente).

Tecnico	Alto livello	*Vulnerabilty Assesment e Penetration Test*	Il Partner effettua periodicamente attività di analisi delle vulnerabilità finalizzate a rilevare lo stato di esposizione alle vulnerabilità note, sia in relazione agli ambiti infrastrutturali sia a quelli applicativi, considerando i sistemi in esercizio o in fase di sviluppo. Ove ritenuto appropriato in relazione ai potenziali rischi identificati, tali verifiche sono integrate periodicamente con apposite tecniche di Penetration Test, mediante simulazioni di intrusione che utilizzano diversi scenari di attacco, con l'obiettivo di verificare il livello di sicurezza di applicazioni / sistemi / reti attraverso attività che mirano a sfruttare le vulnerabilità rilevate per eludere i meccanismi di sicurezza fisica / logica ed avere accesso agli stessi. I risultati delle verifiche, resi disponibili previa richiesta alla Società, sono puntualmente e dettagliatamente esaminati per identificare e porre in essere le azioni di miglioramento necessarie a garantire l'elevato livello di sicurezza richiesto
Tecnico	Autorizzazione, identificazione, autenticazione	*Autorizzazione*	Sono autorizzati ad accedere ai Sistemi Informativi o ad effettuare un Trattamento dei Dati Personali esclusivamente i dipendenti che abbiano una legittima esigenza operativa ("Utenti Autorizzati"). Deve essere previsto un sistema che permetta di gestire le autorizzazioni tramite profili differienzati per scopo di trattamento
Tecnico	Autorizzazione, identificazione, autenticazione	*Identificazione*	Ogni Utente Autorizzato deve essere associato ad un codice di identificazione unico e personale ("User ID"). Tale codice non può essere assegnato ad un'altra persona, neanche in un momento successivo.
Tecnico	Autorizzazione, identificazione, autenticazione	*Elenco degli utenti autorizzati*	Deve tenersi un elenco aggiornato degli Utenti Autorizzati e del profilo di autorizzazione assegnato a ciascuno; le procedure di identificazione e di autenticazione devono essere previste per tutti gli accessi ai Sistemi Informativi o per il compimento di qualsiasi Trattamento dei Dati Personali
Tecnico	Autorizzazione, identificazione, autenticazione	*Autenticazione*	Gli Utenti Autorizzati sono ammessi al Trattamento di Dati Personali se sono dotati di credenziali di autenticazione che consentano di completare con successo una procedura di autenticazione relativa a una specifica operazione di Trattamento o a un insieme di operazioni di Trattamento.
Tecnico	Autorizzazione, identificazione, autenticazione	*Password e modalità di autenticazione alternative*	L'autenticazione deve essere basata su una password segreta connessa con ID Utente; la password deve essere nota solo all'Utente Autorizzato; in alternativa, l'autenticazione potrà avvenire con un dispositivo di autenticazione che è utilizzato e conservato esclusivamente dal soggetto a cui è affidato il Trattamento e può essere associato ad un codice ID o una password, o ancora l'autenticazione potrà avvenire in base ad una caratteristica biometrica che riguarda il soggetto incaricato del trattamento e può essere associata a un codice identificativo o una password.
Tecnico	Autorizzazione, identificazione, autenticazione	*Generazione e conservazione della password*	Ci deve essere una procedura che garantisce l'integrità e la riservatezza della password. Le password devono essere archiviate in un modo che le rende illeggibili, seppur siano valide. Ci deve essere una procedura per l'assegnazione, la distribuzione e la memorizzazione delle password
Tecnico	Autorizzazione, identificazione, autenticazione	*Formato della password*	La password deve contenere almeno otto caratteri, o, se questo non è tecnicamente consentito dai Sistemi informativi, una password è costituita dal massimo numero di caratteri consentiti. Le password non devono contenere alcun elemento che può essere facilmente correlato all'Utente Autorizzato incaricato del Trattamento e deve essere cambiata ad intervalli regolari, e tale intervalli devono essere indicati nel Documento di sicurezza.

Tecnico	Autorizzazione, identificazione, autenticazione	*Modifica della password*	Le password devono essere modificate dall'Utente Autorizzato con un valore segreto conosciuto solo dall'Utente Autorizzato al momento del suo primo accesso e, in seguito, almeno ogni sei mesi
Tecnico	Autorizzazione, identificazione, autenticazione	*Formazione sul corretto utilizzo della password*	Le istruzioni fornite agli Utenti Autorizzati devono prevedere l'obbligo, come condizione per l'accesso ai Sistemi Informativi, di prendere le precauzioni necessarie a garantire che la componente segreta delle credenziali di autentificazione sia mantenuta riservata e che i dispositivi utilizzati e tenuti esclusivamente da Utenti Autorizzati siano tenuti con la dovuta cura.
Tecnico	Autorizzazione, identificazione, autenticazione	*Disattivazione delle credenziali*	Le credenziali di autenticazione devono essere disattivate se non sono state utilizzate per almeno sei mesi, ad eccezione di quelle che sono state autorizzate esclusivamente per finalità di gestione e supporto tecnico. Le credenziali di autenticazione devono essere anche disattivate se l'Utente Autorizzato è de-qualificato o non più autorizzato all'accesso ai Sistemi Informativi o al Trattamento dei Dati Personali.
Tecnico	Autorizzazione, identificazione, autenticazione	*Blocco per abuso del sistema*	Devono essere previsti dei limiti per i tentativi di accesso non autorizzato al Sistema Informativo. Dopo, al massimo, 6 tentativi di autenticazione falliti, l'ID utente associato deve essere bloccato.
Tecnico	Autorizzazione, identificazione, autenticazione	*Credenziali per emergenze*	Laddove i dati e le apparecchiature elettroniche siano accessibili solo utilizzando le componenti riservate delle credenziali di autenticazione, sono fornite indicazioni appropriate, in anticipo e per iscritto, per specificare chiaramente le procedure con cui il Titolare del trattamento può garantire l'accesso ai dati o alle apparecchiature elettroniche nell'eventualità in cui l'incaricato del trattamento sia assente o non disponibile per un lungo tempo e l'accesso a tali apparecchiature e/o ai dati sia indispensabile per svolgere determinate attività, senza ritardo, esclusivamente per finalità connesse all'operatività del sistema e della sicurezza. In questo caso, copie delle credenziali devono essere tenute, in modo da garantire la loro riservatezza, specificando, per iscritto, i soggetti responsabili del mantenimento di tali credenziali. Tali soggetti dovranno informare, senza indugio, l'incaricato delle attività svolte.
Tecnico	Autorizzazione, identificazione, autenticazione	*Gestione delle credenziali di accesso ai sistemi Aruba*	A ciascun collaboratore autorizzato del Partner vengono date una o più credenziali di autenticazione in base al tipo di servizio interno abilitato. Il collaboratore dovrà custodire con la massima riservatezza tali credenziali, assicurandosi di non conservare né in formato digitale né cartaceo una copia scritta della password. Il collaboratore dovrà procedere con un regolare cambio password periodico (almeno ogni 90 giorni) durante l'intero periodo di collaborazione.
Tecnico	Autorizzazione, identificazione, autenticazione	*Disattivazione delle credenziali di accesso ai sistemi Aruba*	Il Partner dovrà comunicare senza alcun indugio ogni variazione all'elenco delle persone autorizzate in modo che Aruba possa procedere con la disattivazione immediata delle credenziali di accesso ai sistemi.
Tecnico	Autorizzazione, identificazione, autenticazione	*NDA*	La consegna delle credenziali di accesso ai sistemi di Aruba sarà completata solo dopo aver ricevuto un modulo NDA firmato dal singolo collaboratore per cui le credenziali sono generate.

Tecnico	Autorizzazione, identificazione, autenticazione	*VPN per accessi remoti*	Ai collaboratori che si collegano da remoto sarà fornito un account VPN nominale con scadenza. Per accedere alla VPN sarà richiesto l'inserimento di un codice OTP generato tramite applicazione Mobile. In caso di furto o smarrimento del telefono su cui è installata l'applicazione si richiede la notifica immediata al referente Aruba in modo che sia possibile disattivare la VPN e generare dei nuovi seed per l'OTP. Essendo la VPN nomianle se ne vieta la condivisione delle credenziali con soggetti terzi seppur autorizzati. Durante la sessione VPN il collaboratore non dovrà lasciare incostudito il proprio PC.
Tecnico	Gestione dei supporti fisici	*Ambiente sicuro*	I Sistemi informativi e i supporti fisici utilizzati per la memorizzazione o il trattamento di dati personali devono essere ospitati in un ambiente fisico sicuro. Devono essere adottate misure per impedire l'accesso fisico non autorizzato ai locali dei Sistemi Informativi.
Organizzativo	Gestione dei supporti fisici	*Istruzioni sul mantenimento e utilizzo di supporti removibili*	Devono essere previste ed impartite istruzioni organizzative e tecniche in relazione al mantenimento e all'utilizzo di supporti rimovibili su cui sono memorizzati i dati al fine di prevenire l'accesso e l'elaborazione non autorizzati. Tali misure saranno preventivamente discusse e concordate con Aruba.
Organizzativo	Gestione dei supporti fisici	*Etichettatura dei supporti*	i Supporti contenenti Dati Personali devono consentire di identificare e classificare il tipo di informazioni in essi contenuti (indicando la data di inserimento dei dati; l'utente autorizzato che ha inserito i dati e la persona da cui è stati ricevuti i dati; i dati personali immessi); detti Supporti devono essere archiviato in un luogo con accesso fisico limitato al personale autorizzato e indicato nel Documento di Sicurezza.
Tecnico	Gestione dei supporti fisici	*Smaltimento dei supporti*	Quando i Supporti o i sistemi informativi devono essere smaltiti o riutilizzati, prima di procedevi devono essere adottate le misure necessarie per impedire qualsiasi conseguente reperimento di Dati Personali e altre informazioni su questi memorizzate, che le informazioni siano comprensibili o ricostruite con qualsiasi mezzo tecnico. Tutti i Supporti riutilizzabili per l'archiviazione dei Dati Personali devono essere sovrascritti tre volte con dati randomizzati prima di essere smaltiti o riutilizzati. Particolare attenzione andrà dedicata alla gestione dei backup di tali supporti, al fine di assicurare la corretta cancellazione dei dati personali anche da questi ultimi.
Tecnico	Gestione dei supporti fisici	*Rimozione dei supporti*	La rimozione di Supporti contenenti Dati Personali dai locali designati deve essere specificamente autorizzata dal Titolare del trattamento
Tecnico	Gestione dei supporti fisici	*Cifratura dei dispositivi*	Tutti i sistemi su cui sono conservati anche solo temporaneamente dati personali dovranno essere cifrati. In base al tipo di sistema possono essere utilizzate diverse modalità di cifratura; per i laptop si richiede comunque la cifratura del disco rigido tramite BitLocker o sistemi simili. Per i dispositivi removibili, posto che siano stati precedentemente autorizzati, si richiede la cifratura del dispositivo.

Tecnico	Gestione dei supporti fisici	*Supporti cartacei*	I documenti cartacei sono una specifica categoria di supporto fisico in cui sono presenti i dati personali. Per questa particolare tipologia di supporto si richiede: o L'etichettatura di ciascun documento con il livello di riservatezza "Riservato" o La stampa in modalità protetta da password o simili accorgimenti per assicurarsi che solo l'autorizzato possa accedere al documento appena prodotto o la conservazione in luogo con accesso fisico limitato ai soli autorizzati al trattamento, ad esempio all'interno di cassetti chiusi a chiave o in appositi archivi sempre chiusi a chiave o la distruzione, ove necessario, tramite apposita macchina distruggi documenti prima dello smaltimento o la distribuzione di tutta la documentazione cartacea dovrà essere sempre fatta rispettando il livello di riservatezza associato al documento e sempre previa autorizzazione. I documenti cartacei contenenti Dati Personali devono essere trasferiti in un contenitore/busta sigillata che indica chiaramente che il documento deve essere consegnato a mano a un Utente Autorizzato. o Ove fosse necessario trasferire i documenti tramite terzi, ad esempio corrieri espressi o poste italiane, oltre che aver precedentemente ottenuto l'autorizzazione, sarà necessario imbustare la documentazione all'interno di un plico sigillato ed anonimo e procedere con il solo invio assicurato.
Tecnico	Gestione dei supporti fisici	*Disponibilità dei supporti*	I supporti contenenti Dati Personali o utilizzati per il trattamento di tali dati devono essere disponibili solo agli Utenti Autorizzati
Tecnico	Distribuzione dei supporti e trasmissione dei Dati Personali	*Crittografia*	La crittografia (128 bit o maggiore) o altra forma equivalente di protezione deve essere utilizzata per proteggere i Dati Personali che sono elettronicamente trasmessi su una rete pubblica o memorizzati su un dispositivo portatile, o laddove si debbano conservare o trattare Dati Personali in un ambiente fisicamente insicuro. In particolare, devono essere utilizzati sistemi di crittografia che non presentino vulnerabilità note e che utilizzino una chiave di lunghezza pari o superiore ai 128 bit, come avviene ad esempio per i sistemi AES-128 e AES-256
Tecnico	Distribuzione dei supporti e trasmissione dei Dati Personali	*Trasferimento dei supporti*	Quando i Supporti contenenti Dati Personali o utilizzati per il trattamento devono essere trasferiti in locali designati a seguito di operazioni di manutenzione, devono essere adottate le misure necessarie per evitare qualsiasi recupero non autorizzato dei Dati Personali e delle altre informazioni sugli stessi memorizzati
Tecnico	Distribuzione dei supporti e trasmissione dei Dati Personali	*Registro dei trasferimenti*	Deve essere istituito un sistema per la registrazione in entrata e in uscita dei Supporti che consenta l'identificazione diretta o indiretta del tipo di supporto, la data e ora, il mittente/destinatario, il numero di supporti, il tipo di informazioni contenute, come vengono inviati e la persona responsabile per la loro ricezione/ invio, che deve essere debitamente autorizzata
Tecnico	Distribuzione dei supporti e trasmissione dei Dati Personali	*Trasferimento elettronico*	Qualora i Dati Personali sono trasmessi o trasferiti su una rete di comunicazione elettronica, devono essere messe in atto misure per controllare il flusso di dati e registrare i tempi della trasmissione o del trasferimento, i Dati Personali trasmessi o ceduti, la destinazione degli eventuali Dati Personali comunicati o trasferiti e i dettagli dell'Utente Autorizzato che conduce la trasmissione o il trasferimento.

Tecnico	Antivirus e antintrusioni	*Sistemi di rilevamento*	Devono essere installati sui Sistemi Informativi software anti-virus e sistemi di rilevamento delle intrusioni per la protezione contro attacchi o altre attività non autorizzate sui Sistemi Informativi stesso. I software antivirus e i sistemi di rilevamento delle intrusioni devono essere aggiornati regolarmente secondo lo stato dell'arte e dell'industria esistenti per i Sistemi informativi interessati (e almeno ogni sei mesi)
Tecnico	Aggiornamenti software	*Vulnerabilty Assesment e Penetration Test*	Il software, il firmware e l'hardware utilizzato nei Sistemi Informativi sono riesaminati regolarmente al fine di rilevare le vulnerabilità e le falle nei Sistemi stessi e di risolvere tali vulnerabilità e i difetti. La verifica di vulnerabilità dei sistemi (Vulnerability Assessment) deve avvenire con cadenza trimestrale su tutti i sistemi, e devono esser previsti test di accesso non autorizzato (Penetration Test) per i sistemi esposti alla rete internet prima del rilascio di ogni modifica significativa e comunque con cadenza almeno annuale in caso di assenza di modifiche alle applicazioni. È richiesta la risoluzione entro 5 gg delle vulnerability "critical" ed entro 30gg delle vulnerability "high".
Tecnico	Aggiornamenti software	*Patching dei sistemi*	Deve essere previsto un processo di patching dei sistemi informativi volto a consentire l'implementazione in tempi rapidi delle patch di security e che preveda l'installazione sugli stessi sistemi del patch bundle più aggiornato con cadenza almeno annuale o trimestrale in base ai sistemi operativi in uso
Tecnico	Testing	*Test con dati reali*	In caso di implementazione o modifica del Sistema Informativo che Tratta Dati Personali, i test preliminari non dovranno utilizzare dati reali o 'live', a meno che tale utilizzo sia necessario e non ci sia nessuna alternativa ragionevole. Laddove vengano utilizzati dati reali o 'live', l'utilizzo sarà limitato nella misura necessaria ai fini della prova e dovrà essere garantito il livello di sicurezza corrispondente al tipo di dati personali trattati
Organizzativo	Gestione della sicurezza	*Responsabile della sicurezza*	È designato un Responsabile della Sicurezza, cui è affidata la verifica della compliance con i requisiti minimi di sicurezza di cui al presente documento. Detto soggetto deve essere adeguatamente formato, esperto nella gestione della protezione delle informazioni e dei dati personali e dotato di risorse adeguate per svolgere efficacemente le proprie mansioni.
Organizzativo	Gestione della sicurezza	*Piano della sicurezza*	Le misure adottate per conformarsi ai presenti requisiti minimi di sicurezza sono oggetto di un piano di sicurezza e precisati e riportati in un documento di sicurezza, che deve essere mantenuto fino ad una determinata data e revisionato ogni volta che vengono apportate modifiche rilevanti al Sistema informativo o alla sua organizzazione. Il documento di sicurezza deve registrare i cambiamenti significativi relativi alle misure di sicurezza o alle attività di Trattamento.
Organizzativo	Gestione della sicurezza	*Misure di sicurezza*	Il Piano di sicurezza dovrà indicare le Misure di sicurezza relative alla modifica e alla manutenzione del sistema utilizzato per Trattare i Dati Personali, compreso lo sviluppo e la manutenzione delle applicazioni
Organizzativo	Gestione della sicurezza	*Inventario hardware e software*	Il Piano di sicurezza dovrà indicare un inventario degli hardware e dei sistemi di sicurezza anche fisici, compresi i sistemi per la sicurezza degli edifici o dei locali dove si verifica il trattamento dei dati
Organizzativo	Gestione della sicurezza	*Sicurezza infrastrutturale*	Il Piano di sicurezza dovrà indicare la sicurezza delle infrastrutture di telecomunicazione e delle strumentazioni utilizzate, e le verifiche ambientali.

Organizzativo	Gestione della sicurezza	*Piano di emergenza*	Un Piano di emergenza che consenta di affrontare possibili pericoli per il sistema di seguito indicati e preveda criteri appropriati per determinare il momento in cui deve essere attivato detto Piano: le funzioni e i sistemi critici, la strategia per proteggere il sistema e le priorità nel caso in cui il Piano sia attivato; un elenco dei membri del personale interessato che può essere chiamato durante un'emergenza, come pure i numeri di telefono di altri soggetti interessati; delle procedure per il calcolo del danno subito; piani realistici di gestione del tempo necessario per consentire il recupero del sistema; assegnazione puntuale dei compiti al personale; possibile utilizzo di allarmi e dispositivi speciali (ad esempio, filtri aria, filtri di rumore); in caso di incendio, dovrebbero essere disponibili attrezzature speciali (ad es., estintore, pompe acqua, ecc.); dispositivi o metodi per la determinazione di temperatura, umidità e altri fattori ambientali (ad es., aria condizionata, termometri, ecc.); software di sicurezza speciale per rilevare violazioni della sicurezza; generatori speciali per trattare cali o interruzione di alimentazione elettrica; conservazione di copie del software o dei materiali in altri edifici protetti per evitare la perdita accidentale.
Organizzativo	Gestione della sicurezza	*Disaster Recovery*	Un piano di Disaster Recovery che precisi: le misure per ridurre al minimo le interruzioni del normale funzionamento del sistema; le misure per limitare la portata di eventuali danni e disastri; le misure per consentire una transizione graduale dei Dati Personali da un sistema ad un altro; se necessario, la previsione di mezzi alternativi per garantire i funzionamento di un sistema; le misure per educare, esercitare e far familiarizzare il personale con le procedure di emergenza; la previsione di indicazioni per il pronto e fluido ripristino di sistema così da ridurre al minimo gli effetti economici di qualsiasi evento di disastro
Organizzativo	Gestione della sicurezza	*Classificazione dei dati*	Il piano di sicurezza dovrà indicare i meccanismi di protezione dei dati per garantire l'integrità e la riservatezza dei dati; la classificazione dei dati stessi
Organizzativo	Gestione della sicurezza	*Sicurezza dei dispositivi*	Il piano di sicurezza dovrà indicare la sicurezza dei computer e dei sistemi di telecomunicazione, incluse le procedure per la gestione delle copie di back-up, le procedure di contrasto ai virus, le procedure per la gestione di segnali/codici, la sicurezza per implementazione del software, la sicurezza dei database, solo in caso di sviluppo software la sicurezza dei sistemi di collegamento a Internet, i controlli su eventuali tentativi di aggiramento di detti sistemi, i meccanismi per tenere conto dei tentativi di violazione della sicurezza del sistema o di ottenere un accesso non autorizzato
Organizzativo	Gestione della sicurezza	*Disponibilità del piano*	Il Documento di sicurezza dovrà essere disponibile al personale che ha accesso ai Dati Personali e, ove richiesto, al Titolare del trattamento ed ai Sistemi Informativi e deve riguardare, come minimo, i seguenti aspetti: Lo scopo del documento, con la specifica dettagliata delle risorse protette; Le misure, le procedure, i codici di condotta e le regole per garantire la sicurezza, include le misure e le regole per il controllo, l'ispezione e la vigilanza dei Sistemi Informativi; Le funzioni e gli obblighi del personale; La struttura dei file contenenti Dati Personali e una descrizione dei Sistemi di informativi su cui vengono Trattati; Le finalità per le quali i Sistemi informativi possono essere utilizzati; Le procedure di reporting, gestione e risposta agli incidenti; Le procedure per fare copie di back-up e ripristino dei dati, che prevedano la necessità di indicare la persona che ha intrapreso il processo, i dati ripristinati e, se del caso, quali dati dovevano essere inseriti manualmente nel processo di recupero.

Organizzativo	Gestione della sicurezza	*Auditing periodico*	Per tutti i fornitori che operano da remoto è previsto un ciclo periodico di verifiche sugli aspetti di sicurezza fisica dei locali in cui avviene il trattamento o la conservazione dei dati personali. Il Partner previo preavviso di 2 giorni dovrà mettere a disposizione del Titolare delle risorse per completare l'audit
Organizzativo	Gestione della sicurezza	*Conservazione della documentazione*	Il documento di sicurezza e qualsiasi altra documentazione devono essere conservati per un periodo minimo di 5 anni dalla fine del Trattamento.
Organizzativo	Gestione del personale	*Verifica dei dipendenti*	Solo i dipendenti che siano dotati di adeguata onestà, integrità e discrezione dovrebbero essere Utenti autorizzati o avere l'accesso ai locali dove si trovano i Sistemi Informativi o i Supporti contenenti Dati Personali. Il Personale dovrebbe essere vincolato da un obbligo di riservatezza nei confronti di qualsiasi accesso ai Dati Personali.
Organizzativo	Gestione del personale	*Formazione del personale*	Devono essere adottate le misure necessarie per formare il personale e renderlo competente a rispettare i presenti requisiti minimi di sicurezza, ogni pertinente disciplina o policy applicabile e/o rilevante per le attività loro affidate, gli obblighi in materia di trattamento dei Dati Personali e le conseguenze di qualsiasi violazione di questi obblighi
Organizzativo	Gestione del personale	*Documentazione funzioni e obblighi*	Le funzioni e gli obblighi del personale che ha accesso ai Dati Personali e ai Sistemi Informativi devono essere chiaramente definiti e documentati
Organizzativo	Gestione del personale	*Istruzioni sulla custodia*	Gli Utenti Autorizzati sono istruiti affinché le apparecchiature elettroniche non siano lasciate incustodite e rese accessibili durante le sessioni di Trattamento
Organizzativo	Gestione del personale	*Accessi fisici*	L'accesso fisico alle aree dove vengono conservati i Dati Personali deve essere limitato agli Utenti Autorizzati
Organizzativo	Gestione del personale	*Provvedimenti disciplinari*	I provvedimenti disciplinari per la violazione del Piano di sicurezza devono essere chiaramente definiti, documentati e comunicati al personale
Organizzativo	Registrazioni	*Registro degli accessi*	È tenuto un registro degli accessi degli Utenti Autorizzati o della divulgazione dei Dati Personali
Organizzativo	Registrazioni	*Registro degli accessi fisici*	Deve essere mantenuto un registro del personale che accede a tali locali, che indichi il nome, la data e l'ora di accesso
Organizzativo	Registrazioni	*Registro degli accessi ai sistemi informativi*	I dettagli minimi che devono essere registrati per ogni accesso ai Sistemi Informativi sono l'ID utente, la data e l'ora di accesso, il file o dati letti, il tipo di accesso e se questo è stato autorizzato o negato.
Organizzativo	Registrazioni	*Identificazione del documento interessato dall'accesso*	Se l'accesso è stato autorizzato, sarà necessario mantenere le informazioni che consentono di identificare il documento interessato dall'accesso.
Organizzativo	Registrazioni	*Responsabilità delle registrazioni*	I meccanismi che consentano di registrare i dati riportati in dettaglio nei paragrafi precedenti devono essere sotto il diretto controllo del Responsabile della sicurezza e in nessun caso deve essere permesso disattivarli
Organizzativo	Registrazioni	*Conservazione delle registrazioni*	Il periodo minimo per conservare i dati registrati è di due anni
Organizzativo	Registrazioni	*Auditing periodico*	Il Responsabile della Sicurezza esamina periodicamente le informazioni di controllo registrate e redige un rapporto sulle verifiche effettuate e i problemi rilevati almeno una volta al mese
Organizzativo	Gestione degli incidenti	*Procedura di segnalazione*	Deve esistere una procedura per la segnalazione, per la risposta e la gestione degli incidenti di sicurezza quali le violazioni della sicurezza dati o i tentativi di accesso non autorizzato

Organizzativo	Gestione degli incidenti	*Team per la gestione*	Definire una squadra chiaramente designata per gestire e coordinare la risposta a un incidente, guidata da un Responsabile della Sicurezza
Organizzativo	Gestione degli incidenti	*Documentazione del processo ed evidenze*	un processo documentato e testato per la gestione della risposta ad un incidente, incluso l'obbligo di tenere appropriati elementi e log delle azioni da cui risulto il momento in cui è avvenuto l'incidente, la persona che denuncia l'incidente o al quale l'incidente è stato riferito e gli effetti dello stesso
Organizzativo	Gestione degli incidenti	*Tempistiche di avviso*	La previsione che il Partner deve avvisare immediatamente il Titolare del trattamento se sembra che i Dati Personali siano stati coinvolti nell'incidente o nella violazione o potrebbero essere coinvolti o attaccati in qualche modo
Organizzativo	Gestione degli incidenti	*Collaborazione*	Il team di gestione degli incidenti e della sicurezza del Partner dovrà eventualmente lavorare insieme con i Responsabili della sicurezza del Titolare del trattamento, fin tanto che l'incidente o la violazione sono stati risolti in modo soddisfacente
Organizzativo	Punti di contatto	*Contatti*	I dati di contatto del Responsabile della sicurezza, comprensivi di e-mail e riferimento telefonico diretto, devono essere comunicati al Titolare del trattamento entro 30 (trenta) giorni dalla sottoscrizione del DPA. Eventuali modifiche di tali dati di contatto dovranno essere comunicate entro lo stesso termine decorrente dall'avvenuta variazione. All'interno dei processi di Incident management e Data breach il punto di contatto incaricato dal Partner è il Responsabile della sicurezza.