Proposta	n. PDET-2026-286 del 02/04/2026
Determinazione dirigenziale	n. DET-2026-258 del 09/04/2026
Oggetto	Servizio Sistemi Informativi e Innovazione Digitale. Affidamento del servizio triennale comprensivo di canone per noleggio di una istanza ATP Core “on Premise” con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato in esito a Trattativa diretta n. 6099360
Dirigente adottante	Servizio Sistemi Informativi E Innovazione Digitale - Cicognani Matteo
Dirigente proponente	Servizio Sistemi Informativi e Innovazione Digitale - Cicognani Matteo
Responsabile del procedimento	Cicognani Matteo

Questo giorno *09/04/2026* il Responsabile di Servizio Sistemi Informativi e Innovazione Digitale, Cicognani Matteo, ai sensi del Regolamento Arpae per l’adozione degli atti di gestione delle risorse dell’Agenzia, approvato con D.D.G. n. 19 del 26/02/2026 e dell’art. 4, comma 2 del D.Lgs. 30 marzo 2001, n. 165 determina quanto segue.

- la D.D.G. n. 159 del 30/12/2025: Direzione Amministrativa. Servizio Amministrazione, Bilancio e Controllo Economico. Approvazione del Bilancio pluriennale di previsione per il triennio 2026-2028, del Piano Investimenti 2026-2028, del Bilancio economico preventivo per l'esercizio 2026, del Budget generale e della Programmazione di Cassa per l'esercizio 2026;
- la D.D.G. n. 160 del 30/12/2025, avente ad oggetto: "Direzione Amministrativa. Servizio Amministrazione, Bilancio e Controllo Economico. Approvazione delle Linee Guida e assegnazione dei budget di esercizio e investimenti per l'anno 2026 ai centri di responsabilità dell'Agenzia per la Prevenzione, l'Ambiente e l'Energia dell'Emilia Romagna, così come modificata dalla D.D.G. n. 24 del 26/02/2026;
- il Decreto Legislativo del 31 marzo 2023 n. 36 "Codice dei contratti pubblici";
- il Regolamento per l'adozione degli atti di gestione dell'Agenzia approvato con D.D.G. n. 111 del 13/11/2019, revisionato con D.D.G. n 19 del 26/02/2026;
- il Regolamento per la disciplina dei contratti pubblici di servizi e forniture di Arpae;

PREMESSO:

- che Arpae è attualmente accreditata come CDRL (Centro di Registrazione Locale) nell'ambito del contratto stipulato con ARUBA PEC S.p.A. (DET-2023-261 del 29/03/2023), ossia come Registration Authority (RA) delegata dalla Certification Authority (CA) Aruba PEC all'identificazione certa e all'emissione dei certificati di Firma Digitale a pieno valore legale;
- che la condizione di CDRL con il fornitore uscente ARUBA PEC S.p.A. consente di continuare ad utilizzare fino a naturale scadenza, senza soluzione di continuità, tutti i kit di firma presenti in Arpae senza necessità di dover procedere con una riemissione massiva di nuovi certificati di firma, con ulteriore onere per l'ente sia in termini economici sia in termini di impiego di risorse interne e sia in termini di interruzione di operatività da parte dell'utenza deputata all'apposizione di firme elettroniche per i processi interni dell'Ente;
- che il contratto sopra richiamato che ha garantito l'emissione dei certificati di firma per i dipendenti Arpae è scaduto il 31/12/2025 e pertanto Arpae si è trovata nella necessità di dare continuità a tale attività;
- l'acquisizione dei kit del fornitore ARUBA PEC S.p.A. consente all'ente di non dover procedere alla modifica degli interfacciamenti applicativi tra i software in uso e i servizi di firma elettronica, evitando l'avvio di appositi progetti onerosi di modifica dei vari software

interessati dall'interfacciamento con necessità di coinvolgere i fornitori e gli sviluppatori delle ditte esterne, in quanto tutti gli applicativi in uso presso Arpae sono già interfacciati con i servizi di firma di Aruba;

- si rende necessaria l’introduzione di un servizio di verifica automatica delle firme elettroniche apposte sui documenti al fine di rendere più robusta l’architettura delle soluzioni di firma implementate nell’ambito di Google Workspace;
- si rende necessaria l’introduzione dell’opzione del “terzo interessato” sulla CDRL Arpae al fine di disporre, all’atto dell’emissione dei nuovi certificati di firma, della possibilità di annullare in maniera unilaterale da parte dell’Agenzia, la validità di un determinato certificato (a seguito di uscita del personale dall’organico dell’ente) e rendere più facile la gestione dei generatori di OTP installati sui dispositivi mobili;
- che in particolare il Servizio Sistemi Informativi e Innovazione Digitale ha svolto l’attività istruttoria volta ad identificare le caratteristiche tecniche necessarie per soddisfare le esigenze di Arpae;
- che per i motivi specifici sopra richiamati, la società ARUBA PEC S.p.A, avente sede legale in Via San Clemente 53 - 24036 Ponte San Pietro (BG), CF. e P. IVA n. 01879020517 è l’unica ditta in grado di garantire il servizio di cui trattasi, come da dichiarazione di affidamento diretto agli atti;

CONSIDERATO:

- che è stato stimato un costo complessivo del servizio triennale pari ad euro 42.922,00 (oltre a IVA al 22%), Oneri per la sicurezza euro 0,00;
- che, come da Richiesta di Acquisto del 03/03/2026, lo scrivente dott. Matteo Cicognani mantiene su di sé la funzione di RUP ai sensi dell’art. 15 del D, lgs. 36/2023;

DATO ATTO:

- che non sono attive convenzioni Consip di cui all'art. 26, comma 1, della legge n. 488/1999 né Intercent-ER di cui all'art. 21, della legge regionale n. 11/2004 aventi ad oggetto servizi analoghi a quelli relativi alla presente procedura di approvvigionamento;
- che sono stati condotti accertamenti volti ad appurare l’esistenza di rischi da interferenza nell’esecuzione dell’appalto in oggetto e che non sono stati riscontrati i suddetti rischi, pertanto non è stato necessario predisporre il DUVRI;
- che è stata verificata la possibilità di espletare tale procedura sul sistema del mercato elettronico messo a disposizione da Consip s.p.a., data l’attivazione del Bando “SERVIZI/Servizi ICT - Categoria: Firma elettronica qualificata - CPV: 79132100-9 Servizi di certificazione della firma elettronica” e che, in particolare, la ditta ARUBA PEC SPA è abilitata

al suddetto bando;

- che sono stati definiti gli atti della procedura, allegati al presente atto, e più precisamente:
  - Condizioni particolari (prot. n. 05.03.2026.41283.U);
  - Disciplinare tecnico
  - Capitolato speciale;
  - DGUE;
  - Dichiarazione d’offerta economica;
  - Atto di nomina del responsabile esterno per il trattamento dei dati personali;
- che, in data 05/03/2026, la suddetta società è stata invitata alla Trattativa diretta n. 6099360, espletata sul portale MEPA, corredata degli atti della procedura summenzionati;
- che, con lettera prot. 17.03.2026.49255.U il RUP, riscontrando la richiesta di chiarimenti pervenuta sul portale Mepa in data 13/03/2026, ha preso atto della circostanza per cui ARUBA PEC SPA, date le peculiarità del servizio richiesto, ai fini dell’esecuzione contrattuale, non riveste la qualità di Responsabile del trattamento ai sensi dell’art. 28 del Regolamento UE n. 2016/679 (GDPR), pertanto non è stata richiesta la sottoscrizione dell’atto di nomina del responsabile esterno per il trattamento dei dati personali in sede di presentazione di offerta;
- che, nella medesima nota prot. 49255/26 è stata espressa accettazione delle ulteriori condizioni contrattuali, laddove non in contrasto con la disciplina degli atti a corredo della Trattativa diretta n. 6099360, riportate nei seguenti documenti trasmessi da ARUBA PEC SPA a mezzo pec in data 13/03/2026 e acquisiti al ns. prot. 16.03.2026.47980.E e allegati alla presente determinazione quali parti integranti e sostanziali:
  - Condizioni generali di fornitura dei Servizi di certificazione Enterprise;
  - Service Level Agreement (SLA) e Penali;
  - Firma Remota;
  - Kit firma digitale

- che in data 13/03/2026, con comunicazione acquisita al ns prot. 16.03.2026.47985.E, la società ARUBA PEC SPA ha altresì anticipato ulteriore documentazione afferente il ruolo di CDRL ricoperto dall’Agenzia, allegata alla presente determinazione, da compilare e sottoscrivere per accettazione, la quale costituirà parte integrante del contratto;
- che, entro il termine di scadenza fissato alle ore 18:00 del 19/03/2026, è pervenuta regolarmente, sul portale Mepa, l’offerta della società invitata, agli atti dell’Amministrazione;
- che è stata ritenuta congrua l’offerta economica, formulata per un importo complessivo pari ad

Euro 42.922,00 (IVA esclusa) e così composta:

Voci	Descrizione della fornitura	Q.tà	Costo unitario IVA esclusa	Prezzo Totale triennio (Iva esclusa)
1	Canone annuale istanza ATP core “on Premise”	3	2.150,00 €	6.450,00 €
2	Canone annuale modulo di Firma Remota (manutenzione correttiva ed evolutiva limitatamente agli aspetti normativi)	3	1.600,00 €	4.800,00 €
3	Canone annuale modulo VOL (manutenzione correttiva ed evolutiva limitatamente agli aspetti normativi)	3	1.400,00 €	4.200,00 €
4	Kit firma remota con OTP Mobile (validità 3 anni)	800	34,00 €	27.200,00 €
5	Attivazione e configurazione profilo terzo interessato - gestione e manutenzione servizio	1	200,00 €	200,00 €
6	Certificato di Firma Automatica persona con poteri di rappresentanza	1	72,00 €	72,00 €
Corrispettivo complessivo del servizio offerto (IVA esclusa)				€ 42.922,00 €

- che la società ARUBA PEC SPA, in sede di dichiarazione di offerta economica, ha dichiarato di applicare al proprio personale il CCNL CED, Cod. H601;
- che la società suddetta è in possesso di comprovata esperienza pregressa nell’esecuzione delle prestazioni di cui all’oggetto, dati i precedenti affidamenti analoghi, nell’esecuzione dei quali il servizio prestato è stato accurato e puntuale e pertanto, ai sensi dell’art. 53 comma 4 del D. Lgs. 53/2023, non si è ritenuto necessario richiedere la garanzia definitiva per l’esecuzione del contratto;

DATO ATTO:

- che l'appalto non rientra nelle categorie merceologiche oggetto dei Criteri Ambientali Minimi di cui all’art. 57 del D.Lgs 36/2023;
- che il Codice Identificativo di Gara (CIG) verrà acquisito dal RUP sul Mepa, attraverso il sistema di interoperabilità con la Piattaforma Contratti Pubblici di ANAC;

RITENUTO per tutto quanto sopra esposto,

- di affidare, ai sensi dell'art. 50 comma 1 lett. b) del D.Lgs. n. 36/2023, il servizio triennale comprensivo di canone per noleggio di una istanza ATP Core "on Premise" con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato, alle condizioni di cui alla trattativa diretta n. 6099360 espletata sul Mepa, alla società ARUBA PEC S.p.A, avente sede legale in Via San Clemente 53 - 24036 Ponte San Pietro (BG), CF. e P. IVA n. 01879020517, come dettagliato negli atti del procedimento, allegati tutti al presente atto quali parti integranti e sostanziali ed alle condizioni di cui all'offerta presentata agli atti, e a quelle ulteriori acquisite al prot. 16.03.2026.47980.E, nei termini concordati con nota del RUP prot. 17.03.2026.49255.U, per l'importo complessivo di euro 42.922,00 (iva esclusa);
- di accettare le ulteriori condizioni contrattuali per lo svolgimento di attività inerenti il rilascio di servizi di certificazione digitale in qualità di CDRL (Centro Di Registrazione Locale) acquisite al prot. 16.03.2026.47985.E, allegate alla presente determinazione, le quali costituiranno parte integrante del contratto previa sottoscrizione;

DATO ATTO:

- che la stipula del contratto avverrà secondo le modalità previste dal mercato elettronico di Consip;

ATTESTATO:

- che è stato acquisito il DURC (on line) dell'impresa aggiudicataria, ed è risultato regolare;
- che è stato verificato il casellario ANAC;
- che attraverso il Fascicolo Virtuale dell'Operatore Economico (FVOE) reso disponibile dall'ANAC sono state effettuate, con esito positivo, le verifiche sul possesso dei requisiti di ordine generale in capo all'aggiudicatario di cui agli artt. 94 e 95 del D.Lgs. n. 36/2023, dichiarati, dalla società ARUBA PEC S.p.A nel DGUE, in sede di partecipazione;

ATTESTATO:

- la regolarità amministrativa del presente atto;

DATO ATTO:

- che non sussistono situazioni di conflitto di interesse, neppure potenziale, secondo quanto previsto dall'art. 16 del D.lgs. n. 36/2023;
- del parere di regolarità contabile espresso, ai sensi del regolamento sull'adozione degli atti di gestione delle risorse dell'agenzia approvato con D.D.G. n. 109 del 31/10/2019 e revisionato dalla D.D.G. n. 19 del 26/02/2026, dal Servizio Amministrazione Bilancio e Controllo Economico nella persona del dott. Giuseppe Bacchi Reggiani;

DETERMINA

1. di affidare, ai sensi dell'art. 50 comma 1 lett. b) del D.Lgs. n. 36/2023, il servizio triennale comprensivo di canone per noleggio di una istanza ATP Core "on Premise" con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato, alle condizioni di cui alla trattativa diretta n. 6099360 espletata sul Mepa, alla società ARUBA PEC S.p.A, avente sede legale in Via San Clemente 53 - 24036 Ponte San Pietro (BG), CF. e P. IVA n. 01879020517, come dettagliato negli atti del procedimento, allegati tutti al presente atto quali parti integranti e sostanziali ed alle condizioni di cui all'offerta presentata agli atti, e a quelle ulteriori acquisite al prot. 16.03.2026.47980.E, nei termini concordati con nota del RUP prot. 17.03.2026.49255.U per l'importo complessivo di euro 42.922,00 (iva esclusa);
2. di accettare le ulteriori condizioni contrattuali per lo svolgimento di attività inerenti il rilascio di servizi di certificazione digitale in qualità di CDRL (Centro Di Registrazione Locale) acquisite al prot. 16.03.2026.47985.E, allegate alla presente determinazione, le quali costituiranno parte integrante del contratto previa sottoscrizione;
3. di dare atto che al Responsabile Unico del Progetto sono assegnate le funzioni ed i compiti di cui all'art. 15 del D.Lgs. n. 36/2023 e ulteriormente specificati nell'allegato I.2 del Codice dei contratti, ed in particolare l'attestazione della regolare esecuzione della prestazione eseguita con riferimento alle prescrizioni contrattuali, anche ai fini del pagamento delle fatture
4. di dare atto che la spesa relativa al presente provvedimento, avente natura di "Servizi informatici" e stimata in euro 52.364,84 (IVA al 22% inclusa) è a carico pro-quota degli esercizi 2026-2027-2028 e trova copertura nel Budget 2026 e nel Bilancio economico preventivo pluriennale 2026-2028, con riferimento al centro di responsabilità "Servizio Sistemi Informativi e Innovazione digitale", e sarà compreso nel Budget e nei bilanci di

prossima approvazione;

5. di dare atto che agli obblighi di trasparenza si assolverà secondo le disposizioni di cui alla delibera ANAC n. 264 del 20/6/2023, come modificata dalla delibera n. 601 del 19/12/2023, in relazione alle procedure avviate dopo l'1/1/2024.

IL DIRIGENTE ADOTTANTE
Firmato digitalmente
Cicognani Matteo

Si dichiara che sono parte integrante del presente provvedimento gli allegati riportati a seguire [1], come file separati dal testo del provvedimento sopra riportato:

1 L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento

OGGETTO: Condizioni particolari per l'affidamento del servizio triennale comprensivo di canone per noleggio di una istanza ATP Core "on Premise" con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato.

Trattativa diretta n. 6099360

Con la presente si precisano le seguenti condizioni particolari di risposta alla trattativa diretta n. 6099360 predisposta da Arpae Emilia-Romagna.

1. OGGETTO E TEMPISTICA.

Oggetto dell'affidamento è il servizio triennale comprensivo di:

1. canone per il noleggio di una istanza ATP core "on Premise" che consente l'attivazione dei moduli aggiuntivi.
2. Canone per il noleggio del modulo di Firma Remota (manutenzione correttiva ed evolutiva limitatamente agli aspetti normativi).
3. Canone per il noleggio del modulo VOL (manutenzione correttiva ed evolutiva limitatamente agli aspetti normativi).
4. n. 800 Kit di Firma remota con OTP mobile e certificato di firma qualificata EIDAS con validità triennale.
5. Attivazione e configurazione profilo 3° interessato, gestione e manutenzione servizio
6. Fornitura di 1 Certificato di Firma Automatica usato da una persona con poteri di rappresentanza in un'organizzazione, che approverà l'emissione del certificato di Firma remota come 3° interessato.

Il servizio in oggetto deve essere garantito per un triennio sino al 31/12/2028, alle condizioni di cui al Disciplinare tecnico e al Capitolato speciale allegati alle presenti condizioni particolari.

Non sono ammesse offerte in aumento rispetto al valore indicato pari ad Euro 42.922,00 (IVA esclusa.) Oneri per la sicurezza euro 0,00.

I prezzi offerti sono fissi e invariabili e si intendono onnicomprensivi di ogni onere e spesa.

Agenzia regionale prevenzione, ambiente ed energia dell'Emilia-Romagna
via Po, 5 | 40139 Bologna | tel 051 6223811 - fax 051 6223897
P.IVA e C.F. 04290860370
e-mail: dirgen@cert.arpa.emr.it

Sono a carico del fornitore affidatario, senza alcuna possibilità di rivalsa nei riguardi di Arpae, tutte le spese di contratto, inclusa l'imposta di bollo pari a 40,00 euro sul documento di stipula generato dal Mercato elettronico, ai sensi dell' art. 18, comma 10 e l'Allegato I.4 al nuovo D.Lgs. n. 36/2023.

2. MODALITÀ DI RISPOSTA ALLA RICHIESTA DI OFFERTA

La documentazione da produrre in risposta alla richiesta di offerta consisterà in:

2.1 Documentazione amministrativa: questa comprenderà - a pena di esclusione:

a) Documento di gara unico europeo (DGUE);

b) Atto di nomina del Responsabile esterno per il trattamento dei dati personali.

In relazione alla predetta documentazione amministrativa, si precisa quanto segue:

a) Il DGUE, deve essere redatto secondo il modello allegato, firmato digitalmente dal legale rappresentante dell'impresa o da un suo procuratore, fornito di adeguati poteri di firma, attestante in particolare:
   1. la non sussistenza delle cause di esclusione di cui all'art. 94 e 95 del D. Lgs. 36/2023, 2.
   2. l'intenzione o meno di ricorrere al subappalto.

Le suddette dichiarazioni in ordine all'insussistenza delle cause automatiche di esclusione di cui all'articolo 94 commi 1 e 2 del Codice devono essere rese dall'operatore economico in relazione a tutti i soggetti indicati al comma 3.

Le dichiarazioni in ordine all'insussistenza delle cause non automatiche di esclusione di cui all'articolo 98, comma 4, lettere g) ed h) del Codice sono rese dall'operatore economico in relazione ai soggetti di cui al punto precedente.

Le dichiarazioni in ordine all'insussistenza delle altre cause di esclusione sono rese in relazione all'operatore economico.

Con riferimento alle cause di esclusione di cui all'articolo 95 del Codice, il concorrente dichiara:

- le gravi infrazioni di cui all'articolo 95, comma 1, lettera a) del Codice commesse nei tre anni antecedenti la data di pubblicazione del bando di gara;
- gli atti e i provvedimenti indicati all'articolo 98 comma 6 del codice emessi nei tre anni antecedenti la data di pubblicazione del bando di gara;
- tutti gli altri comportamenti di cui all'articolo 98 del Codice, commessi nei tre anni antecedenti la data di pubblicazione del bando di gara.

La dichiarazione di cui sopra deve essere resa anche nel caso di impugnazione in giudizio dei relativi provvedimenti.

L'operatore economico dichiara la sussistenza delle cause di esclusione che si sono verificate prima della presentazione dell'offerta e indica le misure di self-cleaning adottate, oppure dimostra l'impossibilità di adottare tali misure prima della presentazione dell'offerta.

L'operatore economico adotta le misure di self-cleaning che è stato impossibilitato ad adottare prima della presentazione dell'offerta e quelle relative a cause di esclusione che si sono verificate dopo tale momento.

b) Dovrà essere allegato l'atto di Nomina del responsabile esterno del trattamento dei dati personali, redatto secondo il modello Allegato, firmato digitalmente dal legale rappresentante dell'impresa o da un suo procuratore.

Si rammenta che, come disposto dal citato art. 96, comma 15 del D.lgs. 36/2023, in caso di presentazione di falsa dichiarazione o falsa documentazione, la stazione appaltante ne dà segnalazione all'ANAC che, se ritiene siano state rese con dolo o colpa grave in considerazione della rilevanza o della gravità dei fatti oggetto della falsa dichiarazione o della presentazione di falsa documentazione, dispone l'iscrizione nel casellario informatico ai fini dell'esclusione dalle procedure di gara e dagli affidamenti di subappalto ai sensi del comma 1 del medesimo articolo, fino a due anni, decorsi i quali l'iscrizione è cancellata e perde comunque efficacia.

2.2 Offerta economica

L'offerta economica dovrà consistere, a pena di esclusione, in:

a) un documento redatto secondo il modello allegato "Dichiarazione d'Offerta", reso disponibile dall'Amministrazione, riportante il dettaglio dei prezzi delle attività richieste nonché, ai sensi dell'art. 108 comma 9 del d.lgs. 36/2023,:

- gli oneri aziendali concernenti l'adempimento delle disposizioni in materia di salute e sicurezza sui luoghi di lavoro;
- la stima dei costi della manodopera
- il contratto nazionale collettivo (CCNL) applicato.

Tale dichiarazione contiene altresì il consenso al trattamento dei dati al fine della verifica del possesso dei requisiti tramite il Fascicolo Virtuale dell'Operatore Economico di ANAC (FVOE 2.0)

b) un'offerta economica riportante il prezzo complessivo della fornitura onnicomprensivo di tutte le

attività dettagliate nel disciplinare tecnico, secondo il modello generato dal sistema.

In caso di discrepanza tra il prezzo complessivo indicato nella dichiarazione di offerta e la somma dei prezzi unitari indicati nella medesima dichiarazione, prevarrà quest'ultima.
In caso di discrepanza tra il valore riportato nell'offerta economica generata dal sistema e la somma dei prezzi unitari riportati nella dichiarazione di offerta economica, prevarrà quest'ultima.
Tutti i documenti componenti l'offerta del Fornitore, devono essere sottoscritti, a pena di esclusione, con firma digitale dal legale rappresentante dell'impresa o da persona munita di idonea procura.

3. MODALITÀ DI AGGIUDICAZIONE

Saranno escluse le offerte nelle quali fossero sollevate eccezioni e/o riserve di qualsiasi natura alle condizioni di fornitura specificate ovvero che siano sottoposte a condizione, nonché offerte incomplete e/o parziali.
Qualora l'offerta presenti un prezzo manifestamente e anormalmente basso rispetto alla prestazione, Arpae si riserva di chiedere all'offerente le necessarie giustificazioni e, qualora queste non siano ritenute valide, ha facoltà di escluderla dalla procedura con provvedimento motivato.
Arpae si riserva la facoltà di non affidare la fornitura.
L'affidamento della fornitura sarà approvato con determinazione dirigenziale del Responsabile del Servizio Sistemi Informativi e Innovazione Digitale.
L'aggiudicazione è subordinata all'esito positivo dei controlli sulla sussistenza dei requisiti di ordine generale di cui agli artt. 94 e 95 del D.lgs. 36/2023, dichiarati dall'impresa con la sottoscrizione del DGUE in sede di partecipazione.
Le verifiche sui requisiti richiesti verranno effettuate tramite il sistema Fascicolo virtuale dell'operatore economico – FVOE 2.0, reso disponibile sul portale ANAC, al quale tutti i soggetti interessati a partecipare alla presente procedura devono registrarsi accedendo all'apposito link sul relativo portale (Servizio ad accesso riservato – FVOE 2.0) secondo le istruzioni ivi contenute.
L'Amministrazione, al fine di avviare le verifiche di rito, procederà con l'Accesso al Fascicolo virtuale dell'operatore economico – FVOE 2.0, reso disponibile sul portale ANAC, individuando nella dashboard il fascicolo relativo al CIG che identifica la procedura, previo consenso al trattamento dei dati rilasciato dall'operatore economico in sede di sottoscrizione dell'offerta.

Qualora, per motivi legati al funzionamento del sistema, non sia possibile procedere alla verifica dei requisiti mediante il sistema FVOE 2.0, l'Amministrazione si riserva di effettuare le verifiche fuori piattaforma.

Coerentemente con quanto disposto dall'art. 21 comma 2 del d.lgs. n. 82/2005 (Codice dell'amministrazione digitale), i documenti inseriti nel sistema FVOE dagli operatori economici, devono essere firmati digitalmente dal legale rappresentante della ditta o da un suo eventuale delegato. Pertanto tali soggetti devono dotarsi di un certificato di firma digitale, in corso di validità, rilasciato da un organismo incluso nell'elenco pubblico dei certificatori.

Il mancato riscontro circa la veridicità di quanto dichiarato in sede di presentazione di offerta comporterà la decadenza dall'aggiudicazione.

4. STIPULA

Con l'affidatario sarà stipulato un contratto secondo le modalità previste dal mercato elettronico di Consip. Il documento di stipula generato automaticamente sul sistema riporterà l'importo complessivo offerto.

La stipula della Trattativa diretta è subordinata altresì alla presentazione da parte del fornitore, entro il termine perentorio di 7 (sette) giorni dalla comunicazione di aggiudicazione, della documentazione di seguito indicata:

- dichiarazione di tracciabilità dei flussi finanziari, ai sensi della L. 136/2010;
- Attestazione dell'avvenuto pagamento all'erario delle spese di bollo di cui al paragrafo 1, mediante Modello F24 ELIDE

Qualora l'Aggiudicatario non produca la documentazione richiesta l'Agenzia procederà alla revoca dell'aggiudicazione della presente Trattativa diretta.

5. FORO COMPETENTE

Per tutte le questioni relative ai rapporti tra il Fornitore e Arpae sarà competente in via esclusiva il Foro di Bologna.

6 NORMA FINALE

Per quanto qui non indicato si rinvia alle condizioni del bando di abilitazione ME Fornitori di Consip "SERVIZI/Servizi ICT - Categoria: Firma elettronica qualificata - CPV: 79132100-9 Servizi di

certificazione della firma elettronica" del Mercato elettronico della Pubblica Amministrazione ed alla documentazione relativa (Condizioni generali di contratto, Capitolato d'oneri, Regole del Sistema di e-procurement, Capitolato tecnico")

7. RESPONSABILE UNICO DEL PROGETTO

Dott. Matteo Cicognani - Servizio Sistemi Informativi e Innovazione Digitale

8. COLLABORATORE AMMINISTRATIVO DI RIFERIMENTO

Dott.ssa Elisa Rodà del Servizio Acquisti e Patrimonio (tel. 331/7494607 – mail: eroda@arpae.it)

9. EVENTUALI CHIARIMENTI

Eventuali chiarimenti potranno essere richiesti entro il termine indicato nella Trattativa diretta esclusivamente all'indirizzo pec dirgen@cert.arpa.emr.it, in relazione alla specifica trattativa.

Documenti allegati:

- Disciplinare Tecnico
- Atto di nomina del Responsabile esterno per il trattamento dei dati personali.
- Modello DGUE
- Schema di dichiarazione di offerta economica

La Responsabile del Servizio Acquisti e Patrimonio
(Dott.ssa Elena Bortolotti)

Documento firmato digitalmente

Agenzia regionale prevenzione, ambiente ed energia dell'Emilia-Romagna
via Po, 5 | 40139 Bologna | tel 051 6223811 - fax 051 6223897
P.IVA e C.F. 04290860370
e-mail: dirgen@cert.arpa.emr.it

1. Oggetto e durata

Oggetto del presente Disciplinare tecnico è l‘affidamento del servizio triennale comprensivo del canone per il noleggio di una istanza ATP core ”on Premise” che consente l’attivazione dei moduli aggiuntivi, modulo di Firma Remota e modulo di verifica VOL in formato WebService. Kit di Firma remota con OTP mobile e certificato di firma qualificata EIDAS (Validità 3 anni). Certificato di Firma Automatica usato da una persona con poteri di rappresentanza in un’organizzazione, che approverà l’emissione del certificato di Firma come terzo interessato.

L'attivazione del servizio dovrà essere effettuato entro 30 giorni naturali e consecutivi dalla stipula del contratto sul portale MEPA ovvero dalla data di avvio dell’esecuzione in via d’urgenza e avrà una durata di 36 mesi.

2. Contesto

Arpae è attualmente accreditato come CDRL (Centro di Registrazione Locale) ossia come Registration Authority (RA) delegata dalla Certification Authority (CA) Aruba PEC all’identificazione certa e all'emissione dei certificati di Firma Digitale a pieno valore legale.

Attualmente, Arpae è in grado di garantire l’emissione dei certificati di firma per i propri dipendenti. I servizi dovranno essere garantiti per un triennio, sino al 31/12/2028.

Gli utenti Arpae utilizzano la firma remota qualificata ormai da anni e i sistemi informativi hanno implementato tale funzionalità nell’ambito di vari processi gestiti informaticamente negli applicativi tecnici e gestionali: gli utenti, infatti, non solo firmano e verificano file firmati sulle proprie postazioni di lavoro ma firmano direttamente nell’ambito degli applicativi LIMS, Sinadoc, Fatture ecc. i documenti all’interno di flussi di processo più ampi ed articolati.

Arpae ha pertanto l’esigenza di mantenere in esercizio tutti i servizi in essere erogati da Aruba, oltre la naturale scadenza dell’attuale contratto e di poter continuare ad emettere, in

autonomia, certificati di firma remota che garantiscano la propria operatività senza dover sostenere ulteriori oneri per l'adeguamento di tutti gli interfacciamenti in essere nell'ambito degli applicativi aziendali.

3. Elenco attività e prodotti da acquisire

Al fine di garantire la continuità operativa che consenta agli utenti Arpae di poter continuare a disporre degli strumenti e dei processi di firma inerenti a varie tematiche (tra cui la firma dei rapporti di prova prodotti dai laboratori analitici dell'ente, la firma delle fatture, la firma dei pareri e delle autorizzazioni ambientali) e migliorare il funzionamento dei medesimi è necessario che Arpae si doti degli strumenti elencati nel seguito:

- Mantenimento Fornitura di 800 Kit di firma remota con OTP mobile
- Fornitura di 1 Certificato di Firma Automatica usato da una persona con poteri di rappresentanza in un'organizzazione, che approverà l'emissione del certificato di Firma remota come 3° interessato.
- Attivazione e configurazione profilo 3° interessato, gestione e manutenzione servizio.
- Canone per il noleggio di una istanza ATP core "on Premise"
- Canone per il noleggio del modulo di Firma Remota (manutenzione correttiva ed evolutiva limitatamente agli aspetti normativi).
- Canone per il noleggio del modulo VOL (manutenzione correttiva ed evolutiva limitatamente agli aspetti normativi)

3.1 Mantenimento della CDRL e ODR

Attività propedeutica alla possibilità di emettere nuove firme remote è il mantenimento dell'attuale CDRL su delega di Aruba con eventuale rinnovo della sottoscrizione di un apposito accordo di delega e la definizione di un numero adeguato di operatori di registrazione (nel seguito denominati ODR), ossia gli operatori Arpae appositamente formati e certificati deputati alla gestione dell'intero ciclo di vita dei certificati di firma a partire dalla fase di riconoscimento de visu degli utenti a cui dovranno essere rilasciati i certificati.

Nell'ambito della CDRL dovranno essere disponibili gli strumenti e le procedure che consentono di svolgere telematicamente le operazioni di registrazione degli utenti, richiesta e ottenimento del certificato, attivazione del servizio di firma remota, nonché sospensione, riattivazione e revoca dei certificati. A tali strumenti e procedure potranno accedere solo gli operatori e gli applicativi integrati tramite web service espressamente autorizzati da Aruba.

3.2 Abilitazione dell'opzione del terzo interessato

L'attivazione di tale opzione avverrà contestualmente per tutti i certificati emissibili dalla CDRL di Arpae e sarà valida sui kit di firma oggetto del presente contratto

L'attivazione dell'opzione consentirà ad Arpae di revocare in autonomia i certificati di firma assegnati a dipendenti che non sono più titolari di un rapporto di lavoro di tipo subordinato con Arpae anche al fine di poter recuperare e riutilizzare le SIM Card dei dispositivi mobili a cui era stato associato il generatore di OTP del certificato di firma.

3.3 Fornitura di kit di firma remota qualificata EIDAS

La firma qualificata remota è una modalità evoluta di firma digitale che, garantendo lo stesso grado di sicurezza e gli stessi effetti di legge della tradizionale firma digitale basata su smart card o token USB, consente, rispetto a queste ultime modalità, di poter usufruire di numerosi vantaggi, quali:

- apporre firme digitali senza la necessità di ricorrere all'installazione di hardware o driver;
- sottoscrivere digitalmente documenti informatici via web in condizioni di massima sicurezza;
- disporre in ogni momento della propria firma digitale su diversi ambienti tecnologici installando il software Aruba Sign o l'apposita app Firma Digitale Aruba;
- eliminare le problematiche legate all'incompatibilità di particolari dispositivi (lettori, smart card e token USB) con determinate piattaforme hardware o software.

La firma remota è il risultato di una procedura informatica basata su un certificato qualificato e su un sistema di chiavi crittografiche correlate tra loro, una definita "pubblica" e l'altra "privata", che consente al titolare, tramite la chiave privata, di sottoscrivere digitalmente un documento e al destinatario, tramite la chiave pubblica, di verificare la provenienza e l'integrità dello stesso documento. La particolarità della firma qualificata remota sta nel fatto che la chiave privata assegnata al titolare del certificato da una Certification Authority, previa identificazione certa dell'identità e acquisizione del consenso del titolare, viene custodita direttamente dalla Certification Authority all'interno di appositi apparati certificati a tale scopo. Il titolare del certificato mantiene il controllo esclusivo del certificato (in particolare della chiave privata) mediante conoscenza delle credenziali di accesso al servizio di firma remota e possesso di un dispositivo (smartphone, telefono cellulare, token hardware, chiavetta USB "Yubico") con cui generare un OTP (One Time Password). I dati da firmare (o meglio la loro impronta, detta "hash") sono inviati dall'applicazione di firma ai sistemi remoti aruba attraverso la rete, e analogamente la risposta ritorna all'applicazione mediante la rete.

La firma remota qualificata si presenta come un servizio fruibile online: il certificato di firma

non è installato su un supporto fisico nelle disponibilità del firmatario ma risiede presso un "server sicuro" nei datacenter di Aruba. L'utilizzatore, per sottoscrivere digitalmente i propri documenti, richiama il proprio certificato inserendo username, password e un'ulteriore crenziale di autenticazione forte fornita da sistemi One-Time Password (OTP). Per quei contesti d'utilizzo enterprise nei quali si ha l'esigenza di abilitare flussi personalizzati e integrare le funzionalità della firma remota con i sistemi di gestione documentale interni all'organizzazione, è prevista la fornitura del componente server ATP (Aruba Trusted Platform) che rappresenta l'interfaccia applicativa che permette facilmente l'integrazione delle applicazioni e dei sistemi del cliente con il servizio di firma remota di Aruba.

Tutti i nuovi certificati emessi dall'Ente avranno la durata standard di 3 anni.

3.4 Aggiornamento e manutenzione del server ARSS

L'ARSS ATP è il componente software che permette una semplice integrazione delle applicazioni e dei sistemi con il Servizio di Firma Remota. Nel caso di applicazioni ospitate in infrastrutture IT differenti da quella dove risiede il Sistema di Firma Remota, ATP dialoga, su HTTPS con mutua autenticazione, con i Sistemi della CA, esponendo verso le applicazioni in questione tutte le funzionalità di firma digitale.

3.5 Attivazione del ATP modulo VOL

L'attivazione di tale modulo consentirà ad Arpae di integrare all'interno dei propri applicativi la possibilità di eseguire la verifica dell'integrità dei file firmati tramite API (application programming interface) fornendo accesso alle informazioni relative alla firma apposta (incluse le informazioni legate al certificato di firma come ad esempio le date di emissione di e di fine validità).

4. Piano delle attività

Arpae richiede l'esecuzione delle seguenti attività previste nel disciplinare tecnico:

1. Fornitura della licenza per consentire il mantenimento, senza soluzione di continuità, del server ATP
2. Attivazione dell'opzione del terzo interessato sui certificati di firma emessi da Arpae
3. Mantenimento attuale CDRL per emissione certificati di firma remota qualificata (durata 3 anni);

4. Aggiunta dei nuovi 800 kit di firma nell'attuale struttura CMS con possibilità di verificare il plafond relativo ai prodotti acquistati;
5. Attivazione del servizio ATP modulo VOL e rilascio contestuale della documentazione per il suo utilizzo

4.1 Tempistiche e decorrenze servizi

1. Le licenze per il mantenimento del servizio ATP in esercizio presso Arpae dovranno essere fornite entro 5 giorni solari consecutivi dalla stipula del contratto ovvero dall'avvio dell'esecuzione in via d'urgenza
2. L'opzione del terzo interessato sulla CDRL di Arpae dovrà essere attivata entro 15 giorni solari consecutivi dalla stipula del contratto ovvero dall'avvio dell'esecuzione in via d'urgenza, da cui andranno detratti eventuali tempi dovuti a disbrigo di attività amministrative da parte di Arpae.
3. L'aggiunta delle nuove licenze nell'attuale struttura CMS con contestuale possibilità di emettere nuovi certificati di firma dovrà essere resa disponibile entro 15 giorni solari consecutivi dalla stipula del contratto ovvero dall'avvio dell'esecuzione in via d'urgenza
4. L'attivazione del modulo ATP VOL dovrà essere effettuata entro 15 giorni solari consecutivi dalla stipula del contratto ovvero dall'avvio dell'esecuzione in via d'urgenza

5. Penali

Per quanto riguarda l'attivazione dei servizi oggetto del presente Disciplinare, per ogni giorno di ritardo rispetto al termine richiesto da Arpae nel paragrafo "**4.1 Tempistiche e decorrenze servizi"** il Fornitore sarà soggetto ad una penale dell'1 ‰ dell'ammontare netto del servizio.

Potranno essere applicate, altresì, penali pari all'1 ‰ dell'ammontare netto del servizio, per ogni giorno di mancato svolgimento, ritardo, o in caso di insoddisfacente esecuzione di una o più attività previste nel presente Disciplinare tecnico.

Arpae potrà applicare al Fornitore penali sino a concorrenza della misura massima pari al 10% (dieci per cento) del valore massimo contrattuale; oltre tale limite, Arpae ha la facoltà di dichiarare risolto di diritto il contratto.

Il Fornitore prende atto, in ogni caso, che l'applicazione delle penali previste dal presente articolo non preclude il diritto di Arpae a richiedere il risarcimento degli eventuali maggior danni.

La richiesta e/o il pagamento delle penali di cui al presente articolo non esonera in nessun caso il Fornitore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.

arpae 30 anni emilia-romagna	**Affidamento del servizio triennale comprensivo di canone per noleggio di una istanza ATP Core "on Premise" con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato.**	**All. B** **Trattativa diretta n. 6099360**

Art. 1 - Oggetto del servizio

Forma oggetto dell'appalto l'affidamento del servizio triennale comprensivo di canone per noleggio di una istanza ATP Core "on Premise" con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato, come descritto nell'allegato Disciplinare tecnico.

Con la presentazione dell'offerta il Fornitore si obbliga irrevocabilmente nei confronti di Arpae ad eseguire tutte le prestazioni oggetto del contratto secondo le modalità richieste.

Art. 2 - Fonti normative

L'esecuzione della fornitura e dei servizi oggetto del presente capitolato è regolato in via gradata:

a) dalle clausole del presente capitolato e dagli atti ivi richiamati, nonché dall'Offerta tecnica ed Economica dell'aggiudicatario, che costituiscono la manifestazione integrale di tutti gli accordi intervenuti con il Fornitore relativamente alle attività e prestazioni contrattuali;

b) dalle condizioni del bando di abilitazione del mercato elettronico di Consip "SERVIZI/Servizi ICT - Categoria: Firma elettronica qualificata - CPV: 79132100-9 Servizi di certificazione della firma elettronica" e dalla documentazione relativa (Capitolato speciale, Regole per l'utilizzo del mercato elettronico, patto di integrità);

c) dal D.Lgs. 31/03/2023, n. 36.

Per quanto non espressamente previsto nelle predette fonti, si rinvia formalmente al Codice civile ed alle norme comunitarie e nazionali vigenti in materia di contratti di diritto privato.

Art. 3 – Termini di esecuzione

Il fornitore si impegna ad eseguire le attività, secondo le modalità e le tempistiche definite nel Disciplinare tecnico.

Arpae verificherà la regolare esecuzione delle obbligazioni pattuite per ciascuna attività richiesta e descritta nell'allegato Disciplinare tecnico nel termine di 30 giorni dal completamento di ciascuna attività, da considerarsi quale "termine di accertamento della prestazione".
Arpae verificherà la regolare esecuzione di tutte le prestazioni del contratto, nel termine di 60 giorni dall'ultimazione di tutte le prestazioni pattuite, ai fini del pagamento dell'ultima fattura (termine di verifica della regolarità delle prestazioni).

Art. 4 - Condizioni generali di fornitura

Sono a carico del Fornitore, intendendosi remunerati con i corrispettivi contrattuali, tutti gli oneri e rischi relativi alla prestazione delle attività e dei servizi oggetto del contratto, nonché ogni attività che si rendesse necessaria per la prestazione degli stessi o, comunque, opportuna per un corretto e completo adempimento delle obbligazioni previste, ivi compresi quelli relativi ad eventuali spese di trasporto, di viaggio e di missione per il personale addetto all'esecuzione contrattuale.

Il Fornitore si obbliga ad eseguire tutte le prestazioni a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nel presente capitolato e nei suoi allegati.

In ogni caso, il Fornitore si obbliga ad osservare nell'esecuzione delle prestazioni contrattuali, tutte le norme e tutte le prescrizioni tecniche e di sicurezza in vigore nonché quelle che dovessero essere successivamente emanate.

Gli eventuali maggiori oneri derivanti dalla necessità di osservare le norme e le prescrizioni di cui sopra, anche se entrate in vigore successivamente alla data del contratto, resteranno ad esclusivo carico del Fornitore, intendendosi in ogni caso remunerati con il corrispettivo contrattuale ed il Fornitore non potrà, pertanto, avanzare pretesa di compensi, a tal titolo, nei confronti di Arpae, assumendosene ogni relativa alea.

Il Fornitore si impegna ad avvalersi di personale qualificato, in relazione alle diverse prestazioni contrattuali.

Arpae è esonerata da ogni responsabilità per danni, infortuni o altro che dovesse accadere al personale del Fornitore nell'esecuzione del contratto, convenendosi a tale riguardo che qualsiasi eventuale onere è già compensato e compreso nel corrispettivo del contratto.

Il Fornitore risponde pienamente per danni a persone e/o cose che potessero derivare dall'espletamento delle prestazioni contrattuali ed imputabili ad essa, o ai suoi dipendenti, o a suoi incaricati, tenendo al riguardo sollevata Arpae da ogni responsabilità ed onere.

Art. 5 - Obblighi derivanti dal rapporto di lavoro

Il Fornitore si obbliga ad ottemperare a tutti gli obblighi verso i propri dipendenti derivanti da disposizioni legislative e regolamentari vigenti in materia di lavoro, ivi compresi quelli in tema di igiene e sicurezza, nonché la disciplina previdenziale e infortunistica, assumendo a proprio carico tutti i relativi oneri.

Il Fornitore si obbliga ad applicare, nei confronti dei propri dipendenti occupati nelle attività contrattuali, il contratto collettivo nazionale e territoriale in vigore per il settore e per la zona

nella quale si eseguono le prestazioni di lavoro, stipulato dalle associazioni di datori e dei prestatori di lavoro comparativamente più rappresentative sul piano nazionale e quello il cui ambito di applicazione sia strettamente connesso con l’attività oggetto dell’appalto svolta dall'impresa anche in maniera prevalente.

Qualora l’amministrazione abbia eventualmente indicato nel bando o nell’invito il contratto collettivo applicabile al personale dipendente impiegato nell’appalto, il fornitore può indicare in offerta il differente contratto collettivo applicato, purché garantisca ai dipendenti le stesse tutele di quello indicato dalla stazione appaltante.

Prima di procedere all’affidamento o all’aggiudicazione l’amministrazione acquisisce la dichiarazione con la quale l’operatore economico si impegna ad applicare il CCNL e territoriale indicato nel bando o nell’invito nell’esecuzione delle prestazioni oggetto del contratto per tutta la sua durata, ovvero la dichiarazione di equivalenza delle tutele di cui al precedente paragrafo.

Il Fornitore si obbliga, altresì, a continuare ad applicare i suindicati Contratti Collettivi anche dopo la loro scadenza e fino alla loro sostituzione.

Gli obblighi relativi ai Contratti Collettivi Nazionali di Lavoro di cui ai commi precedenti vincolano il Fornitore anche nel caso in cui non aderisca alle associazioni stipulanti o receda da esse, per tutto il periodo di validità del presente Contratto.

Il Fornitore si impegna, anche ai sensi e per gli effetti dell’art. 1381 c.c., a far rispettare gli obblighi di cui ai precedenti commi del presente articolo anche agli eventuali esecutori di parti delle attività oggetto del Contratto.

Si applica per quanto riguarda la verifica della regolarità contributiva del Fornitore aggiudicatario quanto previsto dal Decreto Ministero del Lavoro e delle Politiche Sociali 30 gennaio 2015 “Semplificazione in materia di documento unico di regolarità contributiva (DURC)”.

Il Fornitore non avrà diritto ad alcun compenso o indennità oltre al corrispettivo maturato per le prestazioni effettivamente eseguite, calcolato sulla base dei prezzi unitari specificati nella dichiarazione d’offerta.

Art. 6 – Penali

In caso di mancato rispetto dei termini e delle condizioni contrattuali, Arpae applicherà al Fornitore le penali previste nel Disciplinare tecnico.

Deve considerarsi ritardo anche il caso in cui il Fornitore esegua le prestazioni contrattuali in modo anche solo parzialmente difforme da quanto stabilito nel presente Capitolato e nel Disciplinare tecnico. In tali casi saranno applicate le penali sino al momento in cui il contratto inizierà ad essere eseguito in maniera conforme alle disposizioni pattuite.

Gli eventuali inadempimenti contrattuali che danno luogo all'applicazione delle penali vengono contestati per iscritto al Fornitore da Arpae contraente; il Fornitore deve comunicare per iscritto in ogni caso le proprie deduzioni nel termine massimo di giorni 3 (tre) dal ricevimento della stessa contestazione. Qualora dette deduzioni non siano accoglibili, a insindacabile giudizio di Arpae, ovvero non vi sia stata risposta o la stessa non sia giunta nel termine indicato, sono applicate al Fornitore le penali come sopra indicate a decorrere dall'inizio dell'inadempimento.

Arpae potrà applicare al Fornitore penali sino a concorrenza della misura massima pari al 10% (dieci per cento) del valore massimo contrattuale; oltre tale limite, Arpae ha la facoltà di dichiarare risolto di diritto il contratto.

Il Fornitore prende atto, in ogni caso, che l'applicazione delle penali previste dal presente articolo non preclude il diritto di Arpae a richiedere il risarcimento degli eventuali maggiori danni.

La richiesta e/o il pagamento delle penali di cui al presente articolo non esonera in nessun caso il Fornitore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale.

Art. 7 – Corrispettivi

I prezzi di assegnazione si intendono fissi ed invariabili per l'intera durata del servizio.

I corrispettivi contrattuali dovuti al Fornitore sono determinati sulla base dell'Offerta economica del Fornitore.

Tutti i predetti corrispettivi si riferiscono ai servizi prestati a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali, e gli stessi sono dovuti unicamente al Fornitore e, pertanto, qualsiasi terzo, ivi compresi eventuali subfornitori o subappaltatori non possono vantare alcun diritto nei confronti di Arpae.

Tutti gli obblighi ed oneri derivanti al Fornitore dall'esecuzione della Fornitura e dall'osservanza di leggi e regolamenti, nonché dalle disposizioni emanate o che venissero emanate dalle competenti autorità, sono compresi nel corrispettivo contrattuale.

I corrispettivi contrattuali sono stati determinati a proprio rischio dal Fornitore in base ai propri calcoli, alle proprie indagini, alle proprie stime, e sono, pertanto, fissi ed invariabili indipendentemente da qualsiasi imprevisto o eventualità, facendosi carico il Fornitore di ogni relativo rischio e/o alea.

Il Fornitore non può vantare diritto ad altri compensi, ovvero ad adeguamenti, revisioni o aumenti dei corrispettivi come sopra indicati, fatto salvo quanto previsto nel paragrafo seguente.

Art. 8 Revisione prezzi

In conformità a quanto previsto dall'art. 60 e dall'Allegato II.2-bis del Codice, è ammessa la revisione dei prezzi contrattuali qualora, durante l'esecuzione dell'appalto, si verifichino particolari condizioni oggettive che determinino una variazione del costo del servizio, in aumento o in diminuzione, superiore al 5% dell'importo complessivo contrattuale.

La revisione si applica nella misura dell'80% della variazione eccedente la suddetta soglia e riguarda le prestazioni ancora da eseguire al momento dell'attivazione della clausola di revisione. Ai sensi dell'art. 60, comma 3, lett. b) e dell'art. 3 dell'Allegato II.2-bis del Codice, la determinazione della variazione avviene utilizzando l'indice PPS (Indice dei Prezzi alla Produzione dell'Industria) per codice economico (ATECO): [691] "Attività legali, contabilità, consulenza gestionale".

La variazione è calcolata come differenza fra il valore dell'indice al momento della rilevazione e il corrispondente valore del mese del provvedimento di aggiudicazione.

Il monitoraggio dell'indice avverrà con cadenza quadrimestrale a decorrere dalla data di stipula del contratto. In virtù del principio di buona fede contrattuale e leale collaborazione, il Fornitore è tenuto a segnalare tempestivamente all'Agenzia le variazioni dell'indice che comportino la necessità di revisione.

Qualora il Fornitore non proceda alla segnalazione, non potrà richiederne l'applicazione in maniera retroattiva.

Nel caso in cui, per effetto di quanto previsto dai capoversi precedenti, si proceda ad una revisione dei prezzi contrattuali, il nuovo riferimento per il calcolo della variazione dell'indice è il mese in cui si è proceduto alla revisione del prezzo; pertanto, l'ulteriore revisione del prezzo avverrà qualora il valore dell'indice vari, in aumento o in diminuzione, di più del 5% rispetto al valore dell'indice nel mese in cui è stata effettuata la prima revisione.

Nei contratti di subappalto o sub-contratti comunicati all'Agenzia, le clausole di revisione dei prezzi si applicano anche alle prestazioni subappaltate. Tali clausole, definite tra le parti, devono rispettare i limiti e i criteri previsti dal presente paragrafo. Il Fornitore è responsabile della corretta attuazione delle disposizioni sulla revisione dei prezzi nei confronti dei subappaltatori e dei subfornitori.

Oltre a quanto previsto sopra, decorso il primo anno dalla stipula del contratto, su richiesta del fornitore, verrà riconosciuto l'adeguamento dei prezzi in misura pari alla variazione dell'indice ISTAT dei prezzi al consumo per famiglie di operai e impiegati (nella versione che esclude il calcolo dei tabacchi). In particolare detto aggiornamento verrà calcolato sulla base della differenza percentuale rilevata tra il mese di inizio dell'esecuzione e il medesimo mese dell'anno successivo.

La revisione prezzi avviene secondo le modalità di cui all'allegato II.2 bis del Codice

Art. 9 Rinegoziazione

Se sopravvengono circostanze straordinarie e imprevedibili, estranee alla normale alea, all'ordinaria fluttuazione economica e al rischio di mercato e tali da alterare in maniera rilevante l'equilibrio originario del contratto, la parte svantaggiata, che non abbia volontariamente assunto il relativo rischio, ha diritto alla rinegoziazione secondo buona fede delle condizioni contrattuali.

Sulla parte svantaggiata grava l'onere di fornire gli elementi a comprova e, solo successivamente alla valutazione circa la sussistenza delle condizioni di cui al comma 1, viene riconosciuto il diritto alla rinegoziazione.

Se le circostanze sopravvenute di cui al comma 1 rendono la prestazione, in parte o temporaneamente, inutile o inutilizzabile per uno dei contraenti, questi ha diritto a una riduzione proporzionale del corrispettivo, secondo le regole dell'impossibilità parziale.

Il Fornitore è tenuto a comunicare senza ritardo all'Agenzia il verificarsi dell'evento che inibisce l'adempimento degli obblighi contrattuali. L'Agenzia valuta il sussistere delle condizioni di cui al comma 1 del presente articolo.

Il Fornitore che si trovi in tali condizioni è esonerato dall'obbligo di adempiere alle proprie obbligazioni contrattuali e da responsabilità per danni o inadempimento, a partire dal momento in cui comunica l'evento all'Agenzia.

Il Fornitore deve informare l'Agenzia non appena tali eventi cessino e lo stesso può riprendere l'adempimento delle proprie obbligazioni.

Qualora la durata dell'impedimento invocato sia, o diventi, insostenibile, sulla base delle esigenze dell'Agenzia, la stessa avrà il diritto di risolvere il Contratto.

Le parti convengono che, in assenza di diverso accordo, il Contratto potrà comunque essere risolto ove la durata dell'impedimento superi i 120 giorni.

Art. 10 - Obblighi dell'appaltatore relativi alla tracciabilità dei flussi finanziari

Ai sensi e per gli effetti dell'art. 3 e 8 della L. 136/2010 e s.m, il Fornitore si impegna a rispettare puntualmente quanto previsto dalla predetta disposizione in ordine agli obblighi di tracciabilità dei flussi finanziari.

Il Fornitore si obbliga a comunicare, entro sette giorni dalla data del contratto, gli estremi identificativi del conto corrente dedicato di cui all'art. 3 della L. 136/2010, nonché le generalità ed il codice fiscale delle persone delegate ad operare sul predetto conto corrente.

L'esecuzione delle transazioni, relative al presente contratto, eseguite senza avvalersi di bonifico bancario o postale ovvero con altri strumenti di pagamento o di incasso idonei a consentire la piena tracciabilità delle operazioni, costituisce causa di risoluzione del presente contratto, secondo quanto previsto dall'art. 3, comma 9 bis, della L. 136/2010 e s.m.

Il fornitore, si obbliga altresì ad inserire nei contratti sottoscritti con i subappaltatori o i subcontraenti, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla Legge 13 agosto 2010 n. 136. La mancata apposizione della clausola costituisce causa di risoluzione del contratto.

Per tutto quanto non espressamente previsto, restano ferme le disposizioni di cui all'art. 3 della L. 13/08/2010 n. 136 e s.m.

Art. 11 – Fatturazione e pagamenti

Le fatture saranno emesse conformemente alle modalità previste dalla normativa, anche secondaria. vigente in materia, nonché dal presente atto.

Le fatture dovranno essere emesse con le seguente modalità:

1. fornitura 800 kit firma remota con OTP mobile: all'attivazione
2. fornitura del Certificato di Firma Automatica usato da persona con poteri di rappresentanza: all'attivazione
3. abilitazione e configurazione profilo del terzo interessato gestione e manutenzione del servizio: all'attivazione
4. canone per noleggio istanza ATP core "on Premise": trimestrale posticipata
5. canone per noleggio modulo di Firma Remota comprensivo di manutenzione evolutiva e correttiva: trimestrale posticipata;
6. canone per noleggio modulo VOL comprensivo di manutenzione correttiva ed evolutiva: trimestrale posticipata;

Le fatture dovranno essere intestate ad Arpae Emilia-Romagna, Via Po, n. 5 - CAP 40139 - BOLOGNA C.F./P.I.: 04290860370 e riportare tutti i dati richiesti dall´art. 42 D.L. 66/2014 convertito in legge 23/6/2014, n. 89.

Le fatture dovranno:

• riportare numero e data fattura;

• ragione sociale e C.F./P.IVA del fornitore;

• oggetto della fornitura;

• importo totale con indicazione del regime IVA applicato e di eventuali altri oneri o spese;

• scadenza della fattura;

• CIG (che sarà comunicato successivamente)

• le coordinate bancarie e il n. di c/c bancario di appoggio dedicato alle commesse pubbliche, ai sensi dell'art. 3 legge 13 agosto 2010, n. 136.

Verranno accettate e potranno essere pagate solo fatture inviate in forma elettronica ai sensi del D.M. MEF n. 55 del 3 aprile 2013 e dell'art. 25 DL 66/2014 convertito nella L. n. 89 del 23 giugno 2014.

Le fatture dovranno riportare il Codice Univoco Ufficio di Arpae UFFRF4, reperibile anche al sito www.indicepa.gov.it.

Si applicano ad Arpae le norme relative al meccanismo della scissione dei pagamenti (split payment).

Il pagamento delle fatture relative a ciascuna attività sarà effettuato entro 30 giorni dal termine per l'accertamento della prestazione o –se successiva– entro 30 giorni dalla data di ricevimento delle fatture.

Il pagamento dell'ultima fattura sarà effettuato entro 30 giorni dal termine di verifica della regolarità di tutte le prestazioni del contratto, come previsto all'art 3 del presente Capitolato speciale o – se successiva – entro 30 giorni dalla data di ricevimento della fattura.

Sul totale di ogni fattura afferente i servizi di durata triennale e soggetti a fatturazione periodica, dovrà essere calcolata la ritenuta corrispondente allo 0,5%, come previsto dall'art. 11 comma 6, del D. Lgs. 36/2023 che verrà liquidata al termine del contratto, dopo approvazione del certificato di regolare esecuzione e previa acquisizione del Documento unico di regolarità contributiva (DURC).

In caso di ritardo, il saggio degli interessi decorrenti dalla data di scadenza del termine di pagamento come sopra individuato, sarà riconosciuto nella misura prevista dal D.Lgs. 231/2002, salvo diverso accordo con l'aggiudicatario.

Per i fini di cui all'art. 1194 C.C. le parti convengono che i pagamenti effettuati, ancorché in ritardo, siano da imputare prima alla quota capitale e solo successivamente agli interessi e alle spese eventualmente dovuti.

Per i pagamenti di importo superiore ad euro 5.000,00, Arpae procederà alle verifiche previste dal D.M. n.40/2008.

Gli interessi scaduti non producono interessi ai sensi dell'art. 1283 c.c..

Il Fornitore, sotto la propria esclusiva responsabilità, renderà tempestivamente noto ad Arpae le variazioni che si verificassero circa le modalità di accredito di cui sopra; in difetto di tale comunicazione, anche se le variazioni venissero pubblicate nei modi di legge, il Fornitore non potrà sollevare eccezioni in ordine ad eventuali ritardi dei pagamenti, né in ordine ai pagamenti già effettuati.

In caso di ottenimento da parte del Fornitore del DURC che segnali un'inadempienza contributiva relativa a uno o più soggetti impiegati nell'esecuzione del Contratto ovvero nel caso di ritardo nel pagamento delle retribuzioni dovute al personale dipendente dell'esecutore o del subappaltatore o dei soggetti titolari di subappalti trova applicazione quanto disposto dall'art. 11 comma 6 del d. lgs 36/2023.

Si applica per quanto riguarda la verifica della regolarità contributiva del Fornitore aggiudicatario quanto previsto dal Decreto Ministero del Lavoro e delle Politiche Sociali 30 gennaio 2015 "Semplificazione in materia di documento unico di regolarità contributiva (DURC)".

Art. 12 – Trasparenza

Il Fornitore espressamente ed irrevocabilmente:

a) dichiara che non vi è stata mediazione o altra opera di terzi per la conclusione della presente Fornitura;
b) dichiara di non aver corrisposto né promesso di corrispondere ad alcuno, direttamente o attraverso terzi, ivi comprese le imprese collegate o controllate, somme di denaro o altra utilità a titolo di intermediazione o simili, comunque volte a facilitare la conclusione della Fornitura stessa;
c) si obbliga a non versare ad alcuno, a nessun titolo, somme di danaro o altra utilità finalizzate a facilitare e/o a rendere meno onerosa l'esecuzione e/o la gestione della presente Fornitura rispetto agli obblighi con essa assunti, né a compiere azioni comunque volte agli stessi fini.

Qualora non risulti conforme al vero anche una sola delle dichiarazioni rese ai sensi del precedente comma, ovvero il Fornitore non rispetti gli impegni e gli obblighi ivi assunti per tutta la durata della presente Fornitura, la stessa si intende risolta di diritto ai sensi e per gli effetti dell'articolo 1456 c.c., per fatto e colpa del Fornitore, che è conseguentemente tenuto al risarcimento di tutti i danni derivanti dalla risoluzione.

Art. 13 – Risoluzione del contratto.

Oltre alle cause di risoluzione previste nel presente capitolato e nelle norme di legge, Arpae potrà risolvere l'accordo quadro ai sensi dell'art. 1456 c.c., previa dichiarazione da comunicarsi al Fornitore con posta elettronica certificata, nel caso di mancato adempimento delle prestazioni contrattuali a perfetta regola d'arte, nel rispetto delle norme vigenti e

secondo le condizioni, le modalità, i termini e le prescrizioni contenute nel Contratto e negli atti e documenti in esso richiamati.

In ogni caso Arpae potrà risolvere di diritto il contratto ai sensi dell'art. 1456 c.c., previa dichiarazione da comunicarsi al Fornitore con posta elettronica certificata, nei seguenti casi:

- accertamento della non veridicità del contenuto delle dichiarazioni presentate dal Fornitore nel corso della procedura di gara;
- violazione degli obblighi assunti con l'accettazione del Patto d'integrità allegato al Bando di abilitazione del Mercato elettronico di Consip di riferimento;
- in caso di applicazione di penali per un importo complessivo almeno pari alla misura del 10% (dieci per cento) del corrispettivo complessivo contrattuale;
- azioni giudiziarie per violazioni di diritti di brevetto, di autore ed in genere di privativa altrui, intentate contro Arpae;
- qualora disposizioni legislative, regolamentari ed autorizzative non ne consentano la prosecuzione in tutto o in parte;
- nei casi e modi previsti dall'art. 122 d.lgs. n. 36/2023.

In caso di grave inadempimento alle obbligazioni contrattuali assunte con la stipula del Contratto che si protragga oltre il termine, non inferiore comunque a 15 (quindici) giorni, che verrà assegnato a mezzo di posta elettronica certificata da Arpae, per porre fine all'inadempimento, la medesima Amministrazione ha la facoltà di considerare risolto di diritto il Contratto e/o di applicare una penale equivalente, nonché di procedere nei confronti del Fornitore per il risarcimento del danno.

La risoluzione del Contratto obbliga il Fornitore a porre in essere ogni attività necessaria per assicurare la continuità dei servizi residui.

Art. 14 – Recesso

Fermo quanto previsto dagli artt. 88, comma 4-ter e 92, comma 4 del D.lgs 159/2011 (codice delle leggi antimafia e misure di prevenzione), l'Agenzia ha diritto di recesso del contratto, ai sensi dell'art.123 del D.lgs 36/2023, in qualsiasi momento da comunicarsi al fornitore con posta elettronica certificata.

L'Agenzia ha altresì il diritto di recedere per sopravvenienza, durante l'esecuzione del contratto, di una convenzione stipulata da Consip spa e/o Intercent-ER a condizioni più vantaggiose rispetto a quelle del contratto stipulato ai sensi dell'art. 1 comma 13 del d.l. n. 95/2012.

Dalla data di efficacia del recesso, il Fornitore dovrà cessare tutte le prestazioni contrattuali, assicurando che tale cessazione non comporti danno alcuno ad Arpae.

In caso di recesso da parte di Arpae, il Fornitore ha diritto al pagamento delle prestazioni eseguite, purché correttamente ed a regola d'arte, secondo il corrispettivo e le condizioni contrattuali, rinunciando espressamente, ora per allora, a qualsiasi ulteriore eventuale pretesa, anche di natura risarcitoria, ed a ogni ulteriore compenso o indennizzo e/o rimborso delle spese, anche in deroga a quanto previsto dall'articolo 1671 c.c.

Art. 15 Brevetti industriali e diritti d'autore

Il Fornitore assume ogni responsabilità conseguente all'uso di dispositivi o all'adozione di soluzioni tecniche o di altra natura che violino diritti di brevetto, di autore ed in genere di privativa altrui.

Qualora venga promossa nei confronti di Arpae un'azione giudiziaria da parte di terzi per violazione di diritti di brevetto, di autore o di privativa industriale in relazione alle attività prestate in oggetto della presente Fornitura, il Fornitore si obbliga a manlevare e tenere indenne Arpae, assumendo a proprio carico tutti gli oneri conseguenti, inclusi i danni verso terzi, le spese giudiziali e legali a carico di Arpae medesima.

Arpae si impegna ad informare prontamente il Fornitore delle iniziative giudiziarie di cui al precedente comma; in caso di difesa congiunta, il Fornitore riconosce ad Arpae la facoltà di nominare un proprio legale di fiducia da affiancare al difensore scelto dal Fornitore.

Nell'ipotesi di azione giudiziaria per le violazioni di cui ai commi precedenti tentate nei confronti di Arpae, quest'ultima, fermo restando il diritto al risarcimento del danno nel caso in cui la pretesa azionata sia fondata, ha facoltà di dichiarare la risoluzione di diritto del contratto, per quanto di rispettiva ragione, recuperando e/o ripetendo il corrispettivo versato, detratto un equo compenso per i servizi erogati.

Art. 16 - Cessione di contratto e di credito

È fatto assoluto divieto al Fornitore di cedere, a qualsiasi titolo, il contratto, a pena di nullità delle cessioni stesse, salvo quanto previsto dall'art. 120 del D.Lgs. 36/2023.

È ammessa la cessione dei crediti maturati dal Fornitore nei confronti di Arpae a seguito della regolare e corretta esecuzione delle prestazioni oggetto del contratto, nel rispetto ed alle condizioni di cui all'art. 120 comma 12 del D.lgs 36/2023. In ogni caso è fatta salva ed impregiudicata la possibilità per Arpae di opporre al cessionario tutte le medesime eccezioni opponibili al Fornitore cedente, ivi inclusa, a titolo esemplificativo e non esaustivo, l'eventuale compensazione dei crediti derivanti dall'applicazione delle penali.

Art. 17 - Subappalto

Il subappalto, se previsto dal Fornitore in sede di offerta, è disciplinato all'art. 119 del D. Lgs. 36/2023 e s.m.i. e nel rispetto delle disposizioni di cui all'art. 3, comma 9, della Legge n. 136/2010.
Non può essere affidata in subappalto l'integrale esecuzione del contratto.

Il concorrente indica all'atto dell'offerta le parti del servizio/fornitura che intende subappaltare o concedere in cottimo.

In caso di mancata indicazione delle parti da subappaltare il subappalto è vietato.

L'aggiudicatario e il subappaltatore sono responsabili in solido nei confronti della stazione appaltante dell'esecuzione delle prestazioni oggetto del contratto di subappalto.

Art. 18 - Codice di comportamento

Gli obblighi di condotta previsti dal "Codice di comportamento aziendale di Arpae Emilia-Romagna", approvato con DDG n. 20 del 26/02/2026, ai sensi e per gli effetti del D.P.R. 16 aprile 2013 n. 62 "Codice di comportamento dei dipendenti pubblici" sono estesi, per quanto compatibili, ai collaboratori a qualsiasi titolo di imprese fornitrici di beni o servizi o che realizzino opere in favore dell'amministrazione.
Pertanto il fornitore è tenuto ad osservare, per quanto compatibili con la tipologia del contratto, le disposizioni contenute nel Codice di comportamento dei dipendenti pubblici di cui al D.P.R. n. 62/2013 modificato con DPR n. 81/2023 e pubblicato sul sito istituzionale di Arpae /sezione amministrazione trasparente/sottoscrizione disposizioni generali (www.Arpae.emr.it).
In caso di violazione dei suddetti obblighi, Arpae si riserva di risolvere anticipatamente il presente contratto nel rispetto dei principi di gradualità e proporzionalità.

Art. 19 - Informativa sul trattamento dei dati personali ai sensi del Regolamento (UE) 2016/679 (RGPD).
Arpae Emilia-Romagna, in qualità di titolare del trattamento dei dati personali (con sede in Via Po 5, 40139 Bologna, Centralino 051- 6223811), tratterà i dati personali conferiti con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 (RGPD), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri, ivi incluse le finalità di archiviazione, di ricerca storica e di analisi per scopi statistici.

I dati saranno trattati per tutto il tempo di durata del procedimento amministrativo di selezione del contraente e del contratto e successivamente saranno mantenuti in conformità alle norme sulla conservazione della documentazione amministrativa.
I dati saranno trattati esclusivamente dal personale e da collaboratori di Arpae Emilia-Romagna o dalle imprese espressamente nominate come responsabili esterni del trattamento. Al di fuori di queste ipotesi i dati non saranno comunicati a terzi né diffusi, se non nei casi specificamente consentiti dall'interessato o previsti dal diritto nazionale o dell'Unione Europea.
Gli interessati hanno il diritto di chiedere al titolare del trattamento l'accesso ai propri dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del RGPD). L'apposita istanza ad Arpae è presentata contattando il DPO (Responsabile della Protezione dei Dati) all'indirizzo presso Arpae.

Art. 20 – Foro competente.

Per tutte le questioni relative ai rapporti tra il Fornitore e Arpae sarà competente in via esclusiva il Foro di Bologna.

Art. 21 - Oneri fiscali e spese contrattuali

Il contratto relativo al presente servizio viene perfezionato mediante stipula sulla piattaforma del mercato elettronico di Consip.

Sono a carico del prestatore del servizio tutti gli oneri anche tributari relativi alla sottoscrizione del contratto, ad eccezione di quelli che fanno carico ad Arpae per legge.

In particolare il documento di accettazione dell'offerta da parte di Arpae equivale a scrittura privata, ai sensi dell' art. 18, comma 10 e l'Allegato I.4 al nuovo D.Lgs. n. 36/2023 e pertanto deve essere assoggettata ad imposta di bollo.

arpae 30 anni emilia-romagna	**Servizio triennale comprensivo di canone per noleggio di una istanza ATP Core "on Premise" con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato.**	**Trattativa diretta n. 6099360**

Spett.le
Agenzia regionale per la prevenzione, l'ambiente e l'energia dell'Emilia-Romagna
Via Po, 5
40139 Bologna

La _____ , con sede in _____ Via _____, tel. _____, capitale sociale Euro _____, iscritta al Registro delle Imprese di_____ codice fiscale _____, partita IVA n. _____, in persona del sig. _____ nella qualità di _____, della società medesima si impegna ad adempiere a tutte le obbligazioni previste nel Disciplinare tecnico per l'affidamento del servizio triennale comprensivo della piattaforma ATP Core on premise con attivazione dei moduli aggiuntivi, il modulo di Firma Remota e il modulo VOL con manutenzione normativa, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, attivazione del profilo per terzo interessato e certificato di Firma Automatica per soggetti con poteri di rappresentanza, comprensivo di ogni onere e spesa, comprese quelle di trasferta, al netto dell'IVA:

VOCI	**Descrizione della fornitura**	**Q.tà**	**Costo unitario IVA esclusa**	**Prezzo Totale triennio (Iva esclusa)** €
1	Canone annuale istanza ATP core "on Premise"	3		
2	Canone annuale modulo di Firma Remota (manutenzione correttiva ed evolutiva limitatamente agli aspetti normativi)	3		
3	Canone annuale modulo VOL (manutenzione correttiva ed evolutiva limitatamente agli	3		

arpae 30 anni emilia-romagna	**Servizio triennale comprensivo di canone per noleggio di una istanza ATP Core "on Premise" con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato.**	**Trattativa diretta n. 6099360**

	aspetti normativi)			
4	Kit firma remota con OTP Mobile (validità 3 anni)	800		
5	Attivazione e configurazione profilo terzo interessato - gestione e manutenzione servizio	1		
6	Certificato di Firma Automatica persona con poteri di rappresentanza	1		
	Corrispettivo complessivo del servizio offerto (IVA esclusa) (Voci da 1 a 6) *in cifre e in lettere*			€_____ euro_____

Sono compresi nel suddetto importo:

- i costi di manodopera, quantificati in euro _____;
- gli oneri aziendali concernenti l'adempimento delle disposizioni in tema di salute e sicurezza sui luoghi di lavoro, quantificati in euro:_____.

Si precisa che il contratto nazionale collettivo (CCNL) applicato è_____Cod._____

Il sottoscritto _____, in persona del _____ legale rappresentante _____, nell'accettare espressamente tutte le condizioni specificate dalla Stazione Appaltante, dichiara altresì:

a) che la presente offerta è irrevocabile ed impegnativa sino al 180° (centottantesimo) giorno successivo alla data di scadenza fissato per la presentazione dell'offerta;
b) nell'importo dei prezzi offerti è, altresì, compreso ogni onere, spesa e remunerazione per ogni adempimento contrattuale;
c) che nella formulazione della presente offerta ha tenuto conto di eventuali maggiorazioni per lievitazioni dei prezzi che dovessero intervenire durante l'esecuzione contrattuale, rinunciando sin da ora a qualsiasi azione ed eccezione in merito;

arpae 30 anni emilia-romagna	**Servizio triennale comprensivo di canone per noleggio di una istanza ATP Core "on Premise" con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato.**	**Trattativa diretta n. 6099360**

d) che la presente offerta non vincolerà in alcun modo Arpae;
e) di consentire il trattamento dei dati tramite il fascicolo virtuale di cui all'art. 24, nel rispetto di quanto previsto dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, ai fini della verifica del possesso dei requisiti di cui all'art. 99, nonché per le altre finalità del codice;
f) di aver preso visione ed incondizionata accettazione delle clausole e condizioni riportate nella Lettera di invito, nel Capitolato speciale e nel disciplinare tecnico e, comunque, di aver preso cognizione di tutte le circostanze generali e speciali che possono interessare l'esecuzione di tutte le prestazioni oggetto del contratto e che di tali circostanze ha tenuto conto nella determinazione dei prezzi richiesti e offerti, ritenuti remunerativi;
g) di non eccepire, durante l'esecuzione del Contratto, la mancata conoscenza di condizioni o la sopravvenienza di elementi non valutati o non considerati, salvo che tali elementi si configurino come cause di forza maggiore contemplate dal codice civile;
h) di rinunciare a chiedere la risoluzione del contratto per eccessiva onerosità sopravvenuta ai sensi dell'articolo 1467 cod. civ. ed alla revisione del corrispettivo;
i) di prendere atto che i termini stabiliti nel Capitolato Speciale sono da considerarsi a tutti gli effetti termini essenziali ai sensi e per gli effetti dell'articolo 1457 cod. civ.;
j) che il Capitolato speciale così come gli altri atti della Trattativa diretta, costituiranno parte integrante e sostanziale, anche se non materialmente allegati, del Contratto che verrà stipulato tra l'aggiudicatario ed Arpae sul mercato elettronico della pubblica amministrazione.

_____, lì _____

Firma

N.B. Il DGUE è utilizzato per tutte le procedure di affidamento di contratti di appalto di lavori, servizi e forniture nei settori ordinari e nei settori speciali nonché per le procedure di affidamento di contratti di concessione e di partenariato pubblico- privato disciplinate dal Codice.

Il DGUE, compilato dall'operatore economico con le informazioni richieste, accompagna l'offerta nelle procedure aperte e la richiesta di partecipazione nelle procedure ristrette, nelle procedure competitive con negoziazione, nei dialoghi competitivi o nei partenariati per l'innovazione.

Esso è utilizzato anche nei casi di procedura negoziata senza previa pubblicazione di un bando di gara di cui all'articolo 76, comma 2, lettera a) del Codice; negli altri casi previsti dal predetto articolo 76, comma 2, la valutazione circa l'opportunità del suo utilizzo è rimessa alla discrezionalità della stazione appaltante procedente.

Per le procedure di cui all'articolo 50, comma 1, lettere a) e b), di importo inferiore a 40.000 euro, l'articolo 52 del Codice prevede che gli operatori economici attestano il possesso dei requisiti con dichiarazione sostitutiva di atto di notorietà. Atteso che anche il DGUE consiste in una dichiarazione avente i requisiti di cui all'articolo 47 del d.P.R. 445/2000, in tali fattispecie, la stazione appaltante ha facoltà di scegliere se predisporre un modello semplificato di dichiarazione oppure se adottare il DGUE, privilegiando esigenze di standardizzazione e uniformità.

ALLEGATO C)

MODELLO DI FORMULARIO PER IL DOCUMENTO DI GARA UNICO EUROPEO (DGUE)

Parte I: Informazioni sulla procedura di appalto e sulla stazione appaltante o sull'ente concedente

Per le procedure di appalto per le quali è stato pubblicato un avviso di indizione di gara nella *Gazzetta ufficiale dell'Unione europea* le informazioni richieste dalla parte I saranno acquisite automaticamente, a condizione che per generare e compilare il DGUE sia utilizzato il servizio DGUE elettronico ([1]). Riferimento della pubblicazione del pertinente avviso o bando ([2]) nella *Gazzetta ufficiale dell'Unione europea*:

GU UE S numero [], data [], pag. [],

Numero dell'avviso nella GU S: [ ][ ][ ][ ]/S [ ][ ][ ]–[ ][ ][ ][ ][ ][ ][ ]

Se non è pubblicato un avviso di indizione di gara nella GU UE, la stazione appaltante o l'ente concedente deve compilare le informazioni in modo da permettere l'individuazione univoca della procedura di appalto:

Se non sussiste obbligo di pubblicazione di un avviso nella Gazzetta ufficiale dell'Unione europea, fornire altre informazioni in modo da permettere l'individuazione univoca della procedura di appalto (ad esempio il rimando ad una pubblicazione a livello nazionale): [....]

INFORMAZIONI SULLA PROCEDURA DI APPALTO

Le informazioni richieste dalla parte I saranno acquisite automaticamente a condizione che per generare e compilare il DGUE sia utilizzato il servizio DGUE in formato elettronico. In caso contrario tali informazioni devono essere inserite dall'operatore economico.

Identità del committente ([3])	**Risposta:**
Nome:	[Agenzia regionale per la Prevenzione,l'Ambiente e l'Energia de ll'Emilia-Romagna 04290860370
Codice fiscale	[

[redacted]

(1) I servizi della Commissione metteranno gratuitamente il servizio DGUE in formato elettronico a disposizione delle amministrazioni aggiudicatrici, degli enti aggiudicatori, degli operatori economici, dei fornitori di servizi elettronici e di altre parti interessate.

(2) Per le **amministrazioni aggiudicatrici:** un **avviso di preinformazione** utilizzato come mezzo per indire la gara oppure un **bando di gara**. Per gli **enti aggiudicatori**: un **avviso periodico indicativo** utilizzato come mezzo per indire la gara, un **bando di gara** o un **avviso sull'esistenza di un sistema di qualificazione.**

(3) Le informazioni devono essere copiate dalla sezione I, punto I.1 del pertinente avviso o bando. In caso di appalto congiunto indicare le generalità di tutti i committenti.

Di quale appalto si tratta?	**Risposta:**
Titolo o breve descrizione dell'appalto (4):	[servizio triennale comprensivo di canone per noleggio di una istanza ATP Core “on Premise” con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato.
Numero di riferimento attribuito al fascicolo dalla stazione appaltante o dall'ente concedente (ove esistente) (5):	[Trattativa diretta n. 6099360
CIG CUP: Codice progetto (ove l'appalto sia finanziato o cofinanziato con fondi europei)	[ ] [ ] [ ]

Tutte le altre informazioni in tutte le sezioni del DGUE devono essere inserite dall'operatore economico

[redacted]

(4) Cfr. punti II.1.1 e II.1.3. dell'avviso o bando pertinente.
(5) Cfr. punto II.1.1. dell'avviso o bando pertinente.

Parte II: Informazioni sull'operatore economico e sui soggetti di cui all'art. 94, comma 3, D. Lgs. n. 36/2023

A: INFORMAZIONI SULL'OPERATORE ECONOMICO

Dati identificativi	**Risposta:**
Nome:	[ ]
Partita IVA, se applicabile: Se non è applicabile un numero di partita IVA indicare un altro numero di identificazione nazionale, se richiesto e applicabile	[ ] [ ]
Indirizzo postale:	[……]
Persone di contatto (6): Telefono: PEC o e-mail: (indirizzo Internet o sito web) (*ove esistente*):	[……] [……] [……] [……]
Informazioni generali:	**Risposta:**
L'operatore economico è una microimpresa, oppure un'impresa piccola o media (7)?	[ ] Sì [ ] No

Solo se l'appalto è riservato ([8]): Si tratta di operatore economico, di cooperativa sociale o di un loro consorzio, il cui scopo principale è l'integrazione sociale e professionale delle persone con disabilità o svantaggiate, o l'esecuzione è stata riservata nel contesto di programmi di lavoro protetti quando almeno il 30 per cento dei lavoratori dei suddetti operatori economici è composto da lavoratori con disabilità o da lavoratori svantaggiati (art. 61 del Codice)? **In caso affermativo,** qual è la percentuale corrispondente di lavoratori con disabilità o svantaggiati? Se richiesto, specificare a quale o quali categorie di lavoratori con disabilità o svantaggiati appartengono i dipendenti interessati:	[ ] Sì [ ] No [……] [……...]
Se pertinente: l'operatore economico è iscritto in un elenco ufficiale di imprenditori, fornitori, o prestatori di servizi o possiede una certificazione o una attestazione rilasciata da organismi accreditati ? **In caso affermativo**: **Rispondere compilando le altre parti di questa sezione, la sezione B e, ove pertinente, la sezione C della presente parte, la parte III, la parte V se applicabile, e in ogni caso compilare e firmare la parte VI.** *a)* Indicare la denominazione dell'elenco o del certificato o dell'attestato e, se pertinente, il numero di iscrizione o della certificazione o dell'attestazione *b)* Se il certificato di iscrizione o la certificazione o l'attestazione è disponibile elettronicamente, indicare:	[ ] Sì [ ] No [ ] Non applicabile a) [ ] b) (indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……..…][……][……..…][……..…]

([6]) Ripetere le informazioni per ogni persona di contatto tante volte quanto necessario.

([7]) Cfr. raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36). Queste informazioni sono richieste unicamente a fini statistici.
Microimprese: imprese che **occupano meno di 10 persone** e realizzano un fatturato annuo oppure un totale di bilancio annuo **non superiori a 2 milioni di EUR. Piccole imprese:** imprese che **occupano meno di 50 persone** e realizzano un fatturato annuo o un totale di bilancio annuo **non superiori a 10 milioni di EUR. Medie imprese:** imprese che **non appartengono alla categoria delle microimprese né a quella delle piccole imprese**, *che* **occupano meno di 250 persone** e il cui **fatturato annuo non supera i 50 milioni di EUR e/o** il cui **totale di bilancio annuo non supera i 43 milioni di EUR**.

([8]) Cfr. il punto III.1.5 del bando di gara.

c) Indicare i riferimenti in base ai quali è stata ottenuta l'iscrizione o la certificazione o l'attestazione e, se pertinente, la classificazione ricevuta nell'elenco ufficiale ([9]):	c) [ ]
d) L'iscrizione o la certificazione o l'attestazione comprende tutti i criteri di selezione richiesti?	d) [ ] Sì [ ] No
In caso di risposta negativa alla lettera d): **le informazioni da fornire in ordine ai criteri di selezione non soddisfatti nella suddetta documentazione dovranno essere inserite nella Parte IV, Sezioni A, B o C**	
SOLO se richiesto dal pertinente avviso o bando o dai documenti di gara:	
e) L'operatore economico potrà fornire un **certificato** per quanto riguarda il pagamento dei contributi previdenziali e delle imposte, o fornire informazioni che permettano alla stazione appaltante o all'ente concedente di ottenere direttamente tale documento accedendo a una banca dati nazionale che sia disponibile gratuitamente in un qualunque Stato membro?	e) [ ] Sì [ ] No
Se la documentazione pertinente è disponibile elettronicamente, indicare:	(indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione) [……][……][……][……]
Se pertinente: l'operatore economico, in caso di contratti di lavori pubblici di importo superiore a 150.000 euro, è in possesso di attestazione rilasciata da Società Organismi di Attestazione (SOA), ai sensi dell'articolo 100 del Codice (settori ordinari)?	[ ] Sì [ ] No
ovvero	
è in possesso di attestazione rilasciata dai sistemi di qualificazione ai sensi dell'articolo 162 del Codice (settori speciali)?	[ ] Sì [ ] No
In caso affermativo:	
a) Fornire il nome dell'elenco o del certificato e il numero di registrazione o certificazione pertinente, se applicabile	a) (denominazione dell'Organismo di attestazione ovvero del Sistema di qualificazione, numero e data dell'attestazione) [……][……][……][ ]
b) Se il certificato di registrazione o certificazione è disponibile per via elettronica, si prega di indicare dove	b) (indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……][……][……][ ]
c) Indicare i riferimenti su cui si basa la registrazione o la certificazione e, se del caso, la classificazione ottenuta nell'elenco ufficiale	c) (categorie di qualificazione alla quale si riferisce l'attestazione) [……]
d) L'attestazione di qualificazione comprende tutti i criteri di selezione richiesti?	d) [ ] Sì [ ] No
Si evidenzia che gli operatori economici, iscritti in elenchi o in possesso di attestazione di qualificazione SOA (per lavori di importo superiore a 150.000 euro) di cui all'articolo 100 del Codice o in possesso di attestazione rilasciata da Sistemi di qualificazione di cui all'articolo 162 del Codice, non compilano le Sezioni A, B e C della Parte IV.	
Forma della partecipazione:	**Risposta:**
L'operatore economico partecipa alla procedura di appalto insieme ad altri ([10])?	[ ] Sì [ ] No
In caso affermativo, accertarsi che gli altri operatori interessati forniscano un DGUE distinto.	
In caso affermativo:	
a) Specificare il ruolo dell'operatore economico nel raggruppamento, ovvero consorzio, GEIE, rete di impresa di cui all' art. 65, comma 2, lett. e), f), g), h), ed all'art. 66, comma 1, lett. a), b), c), d), e), f), del Codice (capofila, responsabile di compiti specifici, ecc.)	a): [ ]
b) Indicare gli altri operatori economici che compartecipano alla procedura di appalto.	b): [ ]
c) Se pertinente, indicare il nome del raggruppamento partecipante	c): [ ]

[redacted]

(9) I riferimenti e l'eventuale classificazione sono indicati nella certificazione.

(10) Specificamente **nell'ambito di un raggruppamento, consorzio, joint-venture o altro**

d) Se pertinente, indicare la denominazione degli operatori economici facenti parte di un consorzio di cui all'art. 65, comma 2, lett. b), c), d), del Codice o di una Società di professionisti di cui all'art. 66, comma 1, lett. g), del Codice, che eseguono le prestazioni oggetto del contratto.	d): [ ]
Lotti	**Risposta:**
Se pertinente, indicare il lotto o i lotti per i quali l'operatore economico intende presentare un'offerta.	[ ]

B: INFORMAZIONI SUI RAPPRESENTANTI DELL'OPERATORE ECONOMICO

Se pertinente, indicare nome e indirizzo delle persone abilitate ad agire come rappresentanti, ivi compresi procuratori e institori, dell'operatore economico ai fini della procedura di appalto in oggetto; se intervengono più legali rappresentanti ripetere tante volte quanto necessario.

Si specifica che la dichiarazione da inserire in tale sezione deve riferirsi a tutti i soggetti elencati all'articolo 94, comma 3, del Codice e che, nel caso in cui il socio sia una persona giuridica, occorre indicare gli amministratori della stessa.

Eventuali rappresentanti:	**Risposta:**
Nome completo; se richiesto, indicare altresì data e luogo di nascita:	[.....]; [.....
Posizione/Titolo ad agire:	[.....]
Indirizzo postale:	[.....]
Telefono:	[.....]
E-mail:	[.....]
Se necessario, fornire precisazioni sulla rappresentanza (forma, portata, scopo, firma congiunta):	[.....]

C: INFORMAZIONI SULL'AFFIDAMENTO SULLE CAPACITÀ DI ALTRI SOGGETTI (Articolo 104 del Codice - Avvalimento)

Affidamento:	**Risposta:**
L'operatore economico fa affidamento sulle capacità di altri soggetti per soddisfare i criteri di selezione della parte IV e rispettare i criteri e le regole (eventuali) della parte V?	[ ]Sì [ ]No
L'operatore economico fa affidamento sulle capacità di altri soggetti per migliorare l'offerta?	[ ]Sì [ ]No
In caso affermativo: Indicare la denominazione degli operatori economici di cui si intende avvalersi	[.....]
Indicare i requisiti oggetto di avvalimento:	[.....]

In caso affermativo, indicare la denominazione degli operatori economici di cui si intende avvalersi, i requisiti oggetto di avvalimento e presentare per ciascuna impresa ausiliaria un DGUE distinto, debitamente compilato e firmato dai soggetti interessati, con le informazioni richieste dalle **sezioni A e B della presente parte, dalla parte III, dalla parte IV ove pertinente e dalla parte VI.**

Si noti che dovrebbero essere indicati anche i tecnici o gli organismi tecnici che non facciano parte integrante dell'operatore economico, in particolare quelli responsabili del controllo della qualità e, per gli appalti pubblici di lavori, quelli di cui l'operatore economico disporrà per l'esecuzione dell'opera.

Si specifica, inoltre, che l'avvalimento finalizzato a migliorare l'offerta va indicato con una formulazione generica in modo da non anticipare alcun elemento dell'offerta, a cui può essere collegato l'incremento premiale.

D: INFORMAZIONI CONCERNENTI I SUBAPPALTATORI SULLE CUI CAPACITÀ L'OPERATORE ECONOMICO NON FA AFFIDAMENTO (ARTICOLO 119 DEL CODICE - SUBAPPALTO)

(Tale sezione è da compilare solo se le informazioni sono esplicitamente richieste dalla stazione appaltante o dall'ente concedente)

Subappaltatore:	**Risposta:**

L'operatore economico intende subappaltare parte del contratto a terzi? **In caso affermativo:** Elencare i lavori o le parti di opere ovvero i servizi e le forniture o parti di servizi e forniture che si intende subappaltare sull'importo contrattuale	[ ]Sì [ ]No [……] [……]

Se l'operatore economico ha deciso di subappaltare una parte del contratto, ciascun subappaltatore, a seguito dell'autorizzazione al subappalto da parte della stazione appaltante o ente concedente, dovrà compilare il DGUE.

PARTE III: MOTIVI DI ESCLUSIONE (Articoli da 94 a 98 del Codice)

A: MOTIVI LEGATI A CONDANNE PENALI

L'articolo 57, paragrafo 1, della direttiva 2014/24/UE stabilisce i seguenti motivi di esclusione (Articolo 94, comma 1, del Codice):	
1.	Partecipazione a un'organizzazione criminale
2.	([11]) Corruzione ([12])
3.	Frode ([13]);
4.	Reati terroristici o reati connessi alle attività terroristiche ([14]);
5.	Riciclaggio di proventi di attività criminose o finanziamento al terrorismo ([15]); Lavoro minorile e altre forme di tratta di esseri umani ([16])
6.	CO
7.	DIC E Ogni altro delitto da cui derivi, quale pena accessoria, l'incapacità di contrattare con la pubblica amministrazione (lett. h, art. 94, comma 1, del Codice);

Motivi legati a condanne penali ai sensi delle disposizioni nazionali di attuazione dei motivi stabiliti dall'articolo 57, paragrafo 1, della direttiva (per l'elenco dei delitti si veda l'articolo 94, comma 1, del Codice):	**Risposta:**
I soggetti di cui all'art. 94, comma 3, del Codice sono stati **condannati con sentenza definitiva** o decreto penale di condanna divenuto irrevocabile per uno dei motivi indicati sopra con sentenza con effetto escludente ai sensi dei commi 8 e 9 dell'art. 96 del Codice o in seguito alla quale sia ancora applicabile un periodo di esclusione stabilito direttamente nella sentenza ai sensi dell'art. 96, comma 7, del Codice?	[ ] Sì [ ] No Se la documentazione pertinente è disponibile elettronicamente, indicare: (indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……..][……][……..……][…..……..…] ([17])
In caso affermativo, indicare ([18]): a) la data della condanna, del decreto penale di condanna, la relativa durata e il reato commesso tra quelli riportati all'articolo 94, comma 1, lettera da *a)* a *h)*, del Codice e i motivi di condanna b) dati identificativi delle persone condannate [ ]; c) se stabilita direttamente nella sentenza di condanna la durata della pena accessoria, indicare:	a) Data:[ ], durata: [ ], lettera comma 1, articolo 94 [ ], motivi: [ ], tipologia del reato commesso [ ], dati inerenti all'eventuale avvenuta comminazione della pena accessoria dell'incapacità di contrarre con la pubblica amministrazione e la relativa durata [ ] b) [……] c) durata del periodo d'esclusione [.….], lettera comma 1, articolo 94 [ ]
In caso di sentenze di condanna, l'operatore economico ha adottato misure sufficienti a dimostrare la sua affidabilità nonostante l'esistenza di un pertinente motivo di esclusione[19] **(autodisciplina o "Self-Cleaning", cfr. articolo 96, comma 6, del Codice)?**	[ ] Sì [ ] No
In caso affermativo, descrivere tali misure: L'operatore economico ha risarcito o si è impegnato a risarcire qualunque danno causato dal reato o dall'illecito	[…] Sì […] No

[redacted]

(11) Quale definita all'articolo 2 della decisione quadro 2008/841/GAI del Consiglio, del 24 ottobre 2008, relativa alla lotta contro la criminalità organizzata (GU L 300 dell'11.11.2008, pag. 42).

(12) Quale definita all'articolo 3 della convenzione relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee o degli Stati membri dell'Unione europea (GU C 195 del 25.6.1997, pag. 1) e all'articolo 2, paragrafo 1, della decisione quadro 2003/568/GAI del Consiglio, del 22 luglio 2003, relativa alla lotta contro la corruzione nel settore privato (GU L 192 del 31.7.2003, pag. 54). Questo motivo di esclusione comprende la corruzione così come definita nel diritto nazionale dell'amministrazione aggiudicatrice (o ente aggiudicatore) o dell'operatore economico.

(13) Ai sensi dell'articolo 1 della convenzione relativa alla tutela degli interessi finanziari delle Comunità europee (GU C 316 del 27.11.1995, pag. 48).

(14) Quali definiti agli articoli 1 e 3 della decisione quadro del Consiglio, del 13 giugno 2002, sulla lotta contro il terrorismo (GU L 164 del 22.6.2002, pag. 3). Questo motivo di esclusione comprende anche l'istigazione, il concorso, il tentativo di commettere uno di tali reati, come indicato all'articolo 4 di detta decisione quadro.

(15) Quali definiti all'articolo 1 della direttiva 2005/60/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo *(GU L 309 del 25.11.2005, pag. 15)*.

(16) Quali definiti all'articolo 2 della direttiva 2011/36/UE del Parlamento europeo e del Consiglio, del 5 aprile 2011, concernente la prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime, e che sostituisce la decisione quadro del Consiglio 2002/629/GAI (GU L 101 del 15.4.2011, pag. 1).

(17) Ripetere tante volte quanto necessario.

(18) Ripetere tante volte quanto necessario.

[19] In conformità alle disposizioni nazionali di attuazione dell'articolo 57, paragrafo 6, della direttiva 2014/24/UE.

L'operatore economico ha chiarito i fatti e le circostanze in modo globale collaborando attivamente con le autorità investigative	[…] Sì […] No
L'operatore economico ha adottato provvedimenti concreti di carattere tecnico, organizzativo e relativi al personale idonei a prevenire ulteriori reati o illeciti	[…] Sì […] No
Altro	[…….]
Le misure sono state adottate o devono essere ancora adottate?	[…….]
L'operatore economico ha descritto le misure in un documento separato, allegato al DGUE?	Sì […] No […]
Documentazione presente nel FVOE?	Sì […] No […]

B: MOTIVI LEGATI AL PAGAMENTO DI IMPOSTE O CONTRIBUTI PREVIDENZIALI

Pagamento di imposte, tasse o contributi previdenziali (art. 94, comma 6, e art. 95, comma 2, del Codice):	**Risposta:**	
L'operatore economico ha soddisfatto tutti **gli obblighi relativi al pagamento di imposte, tasse o contributi previdenziali,** sia nel paese dove è stabilito sia nello Stato membro della stazione appaltante o dell'ente concedente, se diverso dal paese di stabilimento?	[ ] Sì [ ] No	
In caso negativo, indicare:	**Imposte/tasse**	**Contributi previdenziali**
a) Paese o Stato membro interessato	a) [ ]	a) [ ]
b) Di quale importo si tratta	b) [ ]	b) [ ]
c) Come è stata stabilita tale inottemperanza:		
1) Mediante una **decisione** giudiziaria o amministrativa:	c1) [ ] Sì [ ] No	c1) [ ] Sì [ ] No
– Tale decisione è definitiva e vincolante?	- [ ] Sì [ ] No	- [ ] Sì [ ] No
– Indicare la data della sentenza di condanna o della decisione.	- […….]	- […….]
– Nel caso di una sentenza di condanna, **se stabilita direttamente nella sentenza di condanna**, la durata del periodo d'esclusione:	- […….]	- […….]
2) In **altro modo**? Specificare:	c2) [ ]	c2) [ ]
d) L'operatore economico ha ottemperato od ottempererà ai suoi obblighi, pagando o impegnandosi in modo vincolante a pagare le imposte, le tasse o i contributi previdenziali dovuti, compresi eventuali interessi o multe, avendo effettuato il pagamento o formalizzato l'impegno prima della scadenza del termine per la presentazione della domanda (articolo 94, comma 6, del Codice) oppure ha compensato il debito tributario con crediti certificati vantati nei confronti della pubblica amministrazione (art. 95, comma 2, ult. periodo, del Codice)?	d) [ ] Sì [ ] No **In caso affermativo**, fornire informazioni dettagliate: |……|	d) [ ] Sì [ ] No **In caso affermativo**, fornire informazioni dettagliate: |……|

Se la documentazione pertinente relativa al pagamento di imposte o contributi previdenziali è disponibile elettronicamente, indicare:	(indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione)([20]): [……][……][……..…]

C: MOTIVI LEGATI A INSOLVENZA, CONFLITTO DI INTERESSI O ILLECITI PROFESSIONALI ([21])

Si noti che ai fini del presente appalto alcuni dei motivi di esclusione elencati di seguito potrebbero essere stati oggetto di una definizione più precisa nel diritto nazionale, nell'avviso o bando pertinente o nei documenti di gara. Il diritto nazionale può ad esempio prevedere che nel concetto di "grave illecito professionale" rientrino forme diverse di condotta.

Informazioni su eventuali situazioni di insolvenza, conflitto di interessi o illeciti professionali	**Risposta:**
L'operatore economico ha violato, **per quanto di sua conoscenza**, **obblighi** applicabili in materia di salute e sicurezza sul lavoro, **di diritto ambientale, sociale e del lavoro,** ([22]) di cui all'articolo 95, comma 1, lett. a), del Codice?	[ ] Sì [ ] No
In caso affermativo, l'operatore economico ha adottato misure sufficienti a dimostrare la sua affidabilità nonostante l'esistenza di un pertinente motivo di esclusione (autodisciplina o "Self-Cleaning, cfr. articolo **96, comma 6, del Codice**)?	[ ] Sì [ ] No
In caso affermativo, descrivere tali misure:	
L'operatore economico ha risarcito o si è impegnato a risarcire qualunque danno causato dal reato o dall'illecito	[…] Sì […] No
L'operatore economico ha chiarito i fatti e le circostanze in modo globale collaborando attivamente con le autorità investigative	[…] Sì […] No
L'operatore economico ha adottato provvedimenti concreti di carattere tecnico, organizzativo e relativi al personale idonei a prevenire ulteriori reati o illeciti	[…] Sì […] No
Altro	[…….…]
Le misure sono state adottate o devono essere ancora adottate?	[…….…]
L'operatore economico ha descritto le misure in un documento separato, allegato al DGUE?	Sì […] No […]
Documentazione presente nel FVOE?	Sì […] No […]
L'operatore economico si trova in una delle seguenti situazioni oppure è sottoposto a un procedimento per l'accertamento di una delle seguenti situazioni di cui all'articolo 94, comma 5, lett. d), del Codice:	[ ] Sì [ ] No
a) liquidazione giudiziale	[ ] Sì [ ] No In caso affermativo indicare gli estremi dei provvedimenti […….…] […….…]
b) liquidazione coatta	[ ] Sì [ ] No In caso affermativo indicare gli estremi dei provvedimenti […….…] […….…]
c) concordato preventivo	[ ] Sì [ ] No In caso affermativo indicare gli estremi dei provvedimenti […….…] […….…]
d) nei cui confronti sia in corso un procedimento per l'accesso a una di tali procedure	[ ] Sì [ ] No In caso affermativo indicare gli estremi dei provvedimenti […….…] […….…]
In caso affermativo:	
L'operatore economico sarà comunque in grado di eseguire il contratto?	[ ] Sì [ ] No

[20] Ripetere tante volte quanto necessario.
[21] Cfr. articolo 57, paragrafo 4, della direttiva 2014/24/UE.

(22) Così come stabiliti ai fini del presente appalto dalla normativa nazionale, dall'avviso o bando pertinente o dai documenti di gara ovvero dall'articolo 18, paragrafo 2, della direttiva 2014/24/UE.

(**N.B. Il punto dev'essere compilato dal curatore autorizzato all'esercizio provvisorio che è stato autorizzato dal giudice delegato a partecipare a procedure di affidamento di contratti pubblici ai sensi dell'articolo 124, comma 4 del Codice, indicando gli estremi del provvedimento**).	In caso affermativo indicare gli estremi del provvedimento [ ]
L'operatore economico si è reso colpevole di **gravi illeciti professionali**([23]) di cui all'art. 98 del Codice? **In caso affermativo,** fornire informazioni dettagliate, specificando la tipologia di illecito tra le seguenti:	[ ] Sì [ ] No
● l'operatore economico ha subito l'irrogazione di una sanzione esecutiva dall'Autorità garante della concorrenza e del mercato o da altra autorità di settore, rilevante in relazione all'oggetto specifico dell'appalto (art. 98, comma 3, lett. a, del Codice)?	[ ] Sì [ ] No [……]
● l'operatore economico ha tentato di influenzare indebitamente il processo decisionale della stazione appaltante o di ottenere informazioni riservate a proprio vantaggio oppure ha fornito, anche per negligenza, informazioni false o fuorvianti suscettibili di influenzare le decisioni sull'esclusione, la selezione o l'aggiudicazione (art. 98, comma 3, lett. b, del Codice)?	[ ] Sì [ ] No [……]
● l'operatore economico ha dimostrato significative o persistenti carenze nell'esecuzione di un precedente contratto di appalto o di concessione che ne hanno causato la risoluzione per inadempimento oppure la condanna al risarcimento del danno o altre sanzioni comparabili, derivanti da inadempienze particolarmente gravi o la cui ripetizione sia indice di una persistente carenza professionale (art. 98, comma 3, lett. c, del Codice)?	[ ] Sì [ ] No [……]
● l'operatore economico ha commesso grave inadempimento nei confronti di uno o più subappaltatori (art. 98, comma 3, lett. d, del Codice)?	[ ] Sì [ ] No [……]
● l'operatore economico ha violato il divieto di intestazione fiduciaria di cui all'articolo 17 della legge 19 marzo 1990, n. 55, (art. 98, comma 3, lett. e, del Codice)? La violazione è stata rimossa?	[ ] Sì [ ] No [……] [ ] Sì [ ] No Se la documentazione pertinente è disponibile elettronicamente, indicare: indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……][……][……]
● omessa denuncia all'autorità giudiziaria da parte dell'operatore economico persona offesa dei reati previsti e puniti dagli articoli 317 e 629 del codice penale aggravati ai sensi dell'articolo 416-bis.1 del medesimo codice (art. 98, comma 3, lett. f, del Codice)? Ricorrono i casi previsti dall'articolo 4, primo comma, della legge 24 novembre 1981, n. 689?	[ ] Sì [ ] No [……] [ ] Sì [ ] No Se la documentazione pertinente è disponibile elettronicamente, indicare: indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……][……][……]
● contestata commissione da parte dell'operatore economico, ovvero dei soggetti di cui al comma 3 dell'articolo 94 di taluno dei reati consumati o tentati di cui al comma 1 del medesimo articolo 94 (art. 98, comma 3, lett. g, del Codice)?	[ ] Sì [ ] No [……]
● contestata o accertata commissione, da parte dell'operatore economico oppure dei soggetti di cui al comma 3 dell'articolo 94, di	[ ] Sì [ ] No [……]

([23]) Cfr., ove applicabile, il diritto nazionale, l'avviso o bando pertinente o i documenti di gara.

taluno dei seguenti reati consumati (art. 98, comma 3, lett. h, del Codice)?	
□ 1) abusivo esercizio di una professione, ai sensi dell'articolo 348 del codice penale;	[ ] Sì [ ] No [……]
□ 2) bancarotta semplice, bancarotta fraudolenta, omessa dichiarazione di beni da comprendere nell'inventario fallimentare o ricorso abusivo al credito, di cui agli articoli 216, 217, 218 e 220 del regio decreto 16 marzo 1942, n. 267;	[ ] Sì [ ] No [……]
□ 3) i reati tributari ai sensi del decreto legislativo 10 marzo 2000, n. 74, i delitti societari di cui agli articoli 2621 e seguenti del codice civile o i delitti contro l'industria e il commercio di cui agli articoli da 513 a 517 del codice penale;	[ ] Sì [ ] No [……]
□ 4) i reati urbanistici di cui all'articolo 44, comma 1, lettere b) e c), del testo unico delle disposizioni legislative e regolamentari in materia di edilizia, di cui al decreto del Presidente della Repubblica 6 giugno 2001, n. 380, con riferimento agli affidamenti aventi ad oggetto lavori o servizi di architettura e ingegneria;	[ ] Sì [ ] No [……]
□ 5) i reati previsti dal decreto legislativo 8 giugno 2001, n. 231.	[ ] Sì [ ] No [……]
In caso affermativo, l'operatore economico ha adottato misure di autodisciplina o "Self-Cleaning, (cfr. articolo **96, comma 6, del Codice)**?	[ ] Sì [ ] No
In caso affermativo, descrivere tali misure:	
L'operatore economico ha risarcito o si è impegnato a risarcire qualunque danno causato dal reato o dall'illecito	[…] Sì […] No
L'operatore economico ha chiarito i fatti e le circostanze in modo globale collaborando attivamente con le autorità investigative	[…] Sì […] No
L'operatore economico ha adottato provvedimenti concreti di carattere tecnico, organizzativo e relativi al personale idonei a prevenire ulteriori reati o illeciti	[…] Sì […] No
Altro	[…….]
Le misure sono state adottate o devono essere ancora adottate?	[…….]
L'operatore economico ha descritto le misure in un documento separato, allegato al DGUE?	Sì […] No […]
Documentazione presente nel FVOE?	Sì […] No […]
L'operatore economico è a conoscenza di qualsiasi conflitto di interessi([24]) legato alla sua partecipazione alla procedura di appalto (articolo 95, comma 1, lett. b, del Codice)?	[ ] Sì [ ] No
In caso affermativo, fornire informazioni dettagliate sulle modalità con cui è stato risolto il conflitto di interessi:	[…….]

([24]) **Come indicato nel diritto nazionale, nell'avviso o bando pertinente o nei documenti di gara.**

L'operatore economico o un'impresa a lui collegata **ha fornito consulenza** alla stazione appaltante o all'ente concedente o ha altrimenti **partecipato alla preparazione** della procedura d'aggiudicazione (articolo 95, comma 1, lett. c, del Codice)? **In caso affermativo**, fornire informazioni dettagliate sulle misure adottate per prevenire le possibili distorsioni della concorrenza:	[ ] Sì [ ] No [……]
L'operatore economico può confermare di: a) **non essersi reso** gravemente colpevole di **false dichiarazioni** nel fornire le informazioni richieste per verificare l'assenza di motivi di esclusione o il rispetto dei criteri di selezione? b) **non avere occultato** tali informazioni? c) **non essere iscritto** nel casellario informatico tenuto dall'ANAC per aver presentato false dichiarazioni o falsa documentazione nelle procedure di gara e negli affidamenti di subappalti? (art. 94, comma 5, lett. e, del Codice)? d) **non essere iscritto** nel casellario informatico tenuto dall'ANAC per aver presentato false dichiarazioni o falsa documentazione ai fini del rilascio dell'attestazione di qualificazione? (art. 94, comma 5, lett. f, del Codice)? e) non aver reso false comunicazioni sociali di cui agli articoli 2621 e 2622 del codice civile (art. 94, comma 1, lett. c, del Codice)?	[ ] Sì [ ] No [ ] Sì [ ] No [ ] Sì [ ] No [ ] Sì [ ] No Se la documentazione pertinente è disponibile elettronicamente, indicare: indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……..…][……..…][……..…] [ ] Sì [ ] No Se la documentazione pertinente è disponibile elettronicamente, indicare: indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione [……..…][……..…][……..…]

D: ALTRI MOTIVI DI ESCLUSIONE EVENTUALMENTE PREVISTI DALLA LEGISLAZIONE NAZIONALE DELLO STATO MEMBRO DELLA STAZIONE APPALTANTE O DELL'ENTE CONCEDENTE

MOTIVI DI ESCLUSIONE PREVISTI ESCLUSIVAMENTE DALLA LEGISLAZIONE NAZIONALE (art. 94, comma 1, lett. c) ed h), comma 2, comma 5, lett. a) e lett. b), e art. 53 comma 16-ter del D. Lgs. 165/2001)	**Risposta:**
Sussistono a carico dei soggetti indicati al comma 3 dell'art. 94 cause di decadenza, di sospensione o di divieto previste dall'articolo 67 del decreto legislativo 6 settembre 2011, n. 159 o di un tentativo di infiltrazione mafiosa di cui all'articolo 84, comma 4, del medesimo decreto, fermo restando quanto previsto dagli articoli 88, comma 4-bis, e 92, commi 2 e 3, del decreto legislativo 6 settembre 2011, n. 159, con riferimento rispettivamente alle comunicazioni antimafia e alle informazioni antimafia (Articolo 94, comma 2, del Codice)?	[ ] Sì [ ] No Se la documentazione pertinente è disponibile elettronicamente, indicare: (indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……..…][……..…][……..…][……..…] (25)
L'operatore economico si trova in una delle seguenti situazioni? 1. è stato soggetto alla sanzione interdittiva di cui all'articolo 9, comma 2, lettera c) del decreto legislativo 8 giugno 2001, n. 231 o ad altra sanzione che comporta il divieto di contrarre con la pubblica	[ ] Sì [ ] No

(25) Ripetere tante volte quanto necessario.

amministrazione, compresi i provvedimenti interdittivi di cui all'articolo 14 del decreto legislativo 9 aprile 2008, n. 81 (Articolo 94, comma 5, lettera a), del Codice);	Se la documentazione pertinente è disponibile elettronicamente, indicare: indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……..…][……..…][……..…]
2. è in regola con le norme che disciplinano il diritto al lavoro dei disabili di cui alla legge 12 marzo 1999, n. 68 (Articolo 94, comma 5, lett. b, del Codice);	[ ] Sì [ ] No [ ] Non è tenuto alla disciplina legge 68/1999 Se la documentazione pertinente è disponibile elettronicamente, indicare: indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……..…][……..…][……..…] Nel caso in cui l'operatore non è tenuto alla disciplina legge 68/1999 indicare le motivazioni: (numero dipendenti e/o altro) [……..…][……..…][ ]
3. si trova, rispetto ad un altro partecipante alla medesima procedura di affidamento, in una situazione tale da far ritenere che le offerte degli operatori economici siano imputabili ad un unico centro decisionale a cagione di accordi tra loro intercorsi (articolo 95, comma 1, lett. d, del Codice)?	[ ] Sì [ ] No Se la documentazione pertinente è disponibile elettronicamente, indicare: indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……..…][……..…][……..…]
4. L'operatore economico si trova nella condizione prevista dall'art. 53 comma 16-ter del D.Lgs. 165/2001 (pantouflage o revolving door) in quanto ha concluso contratti di lavoro subordinato o autonomo e, comunque, ha attribuito incarichi ad ex dipendenti della stazione appaltante o dell'ente concedente che hanno cessato il loro rapporto di lavoro da meno di tre anni e che negli ultimi tre anni di servizio hanno esercitato poteri autoritativi o negoziali per conto della stessa stazione appaltante o ente concedente nei confronti del medesimo operatore economico?	[ ] Sì [ ] No

Parte IV: Criteri di selezione

(artt. 100 e 103 del Codice)

In merito ai criteri di selezione (sezione α o sezioni da A a D della presente parte) l'operatore economico dichiara che:

L'operatore economico deve compilare questo campo solo se la stazione appaltante o l'ente concedente ha indicato nell'avviso o bando pertinente o nei documenti di gara ivi citati che l'operatore economico può limitarsi a compilare la sezione della parte IV senza compilare nessun'altra sezione della parte IV:

α: INDICAZIONE GLOBALE PER TUTTI I CRITERI DI SELEZIONE

Rispetto di tutti i criteri di selezione richiesti	**Risposta**
Soddisfa i criteri di selezione richiesti:	[ ] Sì [ ] No

A: IDONEITÀ (Articolo 100, comma 1, lettera *a)*, del Codice)

Tale Sezione è da compilare solo se le informazioni sono state richieste espressamente dalla stazione appaltante o dall'ente concedente nell'avviso o bando pertinente o nei documenti di gara

Idoneità	Risposta

1) Iscrizione in un registro professionale o commerciale tenuto nello Stato membro di stabilimento ([26]) per un'attività pertinente anche se non coincidente con l'oggetto dell'appalto Se la documentazione pertinente è disponibile elettronicamente, indicare:	[……..…] (indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……][……..…][……]
2) Per gli appalti di servizi, forniture e lavori: È richiesta una particolare **autorizzazione o appartenenza** a una particolare organizzazione (elenchi, albi, ecc.) per poter prestare il servizio di cui trattasi nel paese di stabilimento dell'operatore economico? Se la documentazione pertinente è disponibile elettronicamente, indicare:	[ ] Sì [ ] No In caso affermativo, specificare quale documentazione e se l'operatore economico ne dispone: […] [ ] Sì [ ] No (indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……][……..…][……]

[redacted]

(26) Conformemente all'elenco dell'allegato XI della direttiva 2014/24/UE; **gli operatori economici di taluni Stati membri potrebbero dover soddisfare altri requisiti previsti nello stesso allegato.**

Tale Sezione è da compilare solo se le informazioni sono state richieste espressamente dalla stazione appaltante o dall'ente concedente nell'avviso o bando pertinente o nei documenti di gara.

B: CAPACITÀ ECONOMICA E FINANZIARIA (Articolo 100, comma 1, lettera *b)*, del Codice)

Capacità economica e finanziaria	**Risposta*:***
1a) Il **fatturato globale** maturato nel triennio precedente a quello di indizione della procedura è il seguente (art. 100, comma 11, del Codice): **e** **(per gli appalti di lavori di importo pari o superiore ai 20 milioni di Euro):**	Fatturato globale [……] […] valuta
1) l'operatore economico fornisce i parametri economico-finanziari significativi richiesti, certificati da società di revisione ovvero da altri soggetti preposti che si affianchino alle valutazioni tecniche proprie dell'organismo di certificazione, da cui emerga in modo inequivoco l'esposizione finanziaria dell'operatore economico al momento in cui partecipa a una gara di appalto (art. 103, comma 1, lett. a, del Codice) **in alternativa**	[ ] Sì [ ] No Indicare i parametri • […….…] • […….…]
2) l'operatore economico possiede un volume d'affari in lavori pari a due volte l'importo a base di gara, che l'operatore economico deve aver realizzato nei migliori cinque dei dieci anni antecedenti alla data di pubblicazione del bando (art. 103, comma 1, lett. a, del Codice)	[ ] Sì [ ] No Indicare il volume di affari [ ] valuta
Se le informazioni relative al fatturato globale non sono disponibili per tutto il periodo richiesto, indicare la data di costituzione o di avvio delle attività dell'operatore economico:	[…….]
1b) Per quanto riguarda gli **eventuali altri requisiti economici o finanziari** specificati nell'avviso o bando pertinente o nei documenti di gara, l'operatore economico dichiara che:	[…….]
Se la documentazione pertinente **eventualmente** specificata nell'avviso o bando pertinente o nei documenti di gara è disponibile elettronicamente, indicare:	(indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……..][……..][……..…]

C: CAPACITÀ TECNICHE E PROFESSIONALI (Articolo 100, comma 1, lettera *c)*, del Codice)

Tale Sezione è da compilare solo se le informazioni sono state richieste espressamente dalla stazione appaltante o dall'ente concedente nell'avviso o bando pertinente o nei documenti di gara.

Capacità tecniche e professionali	**Risposta*:***
1a) Unicamente per gli **appalti pubblici di lavori,** durante il periodo di riferimento([27]) l'operatore economico **ha eseguito i seguenti lavori del tipo specificato**:	Numero di anni (periodo specificato nell'avviso o bando pertinente o nei documenti di gara): […] Lavori: […….]

[redacted]

(27) Le amministrazioni aggiudicatrici possono **richiedere** fino a cinque anni e **ammettere** un'esperienza che risale a **più** di cinque anni prima.

Se la documentazione pertinente sull'esecuzione e sul risultato soddisfacenti dei lavori più importanti è disponibile per via elettronica, indicare: **e** **(per gli appalti di lavori di importo pari o superiore a 100 milioni di euro):** l'operatore economico fornisce prova di aver eseguito lavori per entità e tipologia compresi nella categoria individuata come prevalente a quelli posti in appalto opportunamente certificati dalle rispettive stazioni appaltanti, tramite presentazione del certificato di esecuzione lavori (art. 103, comma 1, lett. b, del Codice)	(indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……][……..…][……..…] [ ] Sì [ ] No Indicare i lavori [ ]
1b) Unicamente per gli ***appalti pubblici di forniture e di servizi***: di aver eseguito nel precedente triennio dalla data di indizione della procedura di gara contratti analoghi a quello in affidamento anche a favore di soggetti privati (art. 100, comma 11, del Codice):	Numero di anni (periodo specificato nell'avviso o bando pertinente o nei documenti di gara): [……..] Descrizione | importi | date | destinatari
2) Per quanto riguarda gli **eventuali altri requisiti tecnici e professionali** specificati nell'avviso o bando pertinente o nei documenti di gara, l'operatore economico dichiara che: Se la documentazione pertinente **eventualmente** specificata nell'avviso o bando pertinente o nei documenti di gara è disponibile elettronicamente, indicare:	[……] (indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……..][……..…][……..…]

L'operatore economico deve fornire informazioni solo se i programmi di garanzia della qualità e/o le norme di gestione ambientale sono stati richiesti dalla stazione appaltante o dall'ente concedente nell'avviso o bando pertinente o nei documenti di gara ivi citati.

D: SISTEMI DI GARANZIA DELLA QUALITÀ E NORME DI GESTIONE AMBIENTALE

Sistemi di garanzia della qualità e norme di gestione ambientale	**Risposta:**
L'operatore economico potrà presentare **certificati** rilasciati da organismi indipendenti per attestare che egli soddisfa determinate **norme di garanzia della qualità**, compresa l'accessibilità per le persone con disabilità? **In caso negativo**, spiegare perché e precisare di quali altri mezzi di prova relativi al programma di garanzia della qualità si dispone: Se la documentazione pertinente è disponibile elettronicamente, indicare:	[ ] Sì [ ] No [……..…] [……..…] (indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……..…][……..…][……..…]
L'operatore economico potrà presentare **certificati** rilasciati da organismi indipendenti per attestare che egli rispetta determinati **sistemi o norme di gestione ambientale**? **In caso negativo**, spiegare perché e precisare di quali altri mezzi di prova relativi ai **sistemi o norme di gestione ambientale** si dispone: Se la documentazione pertinente è disponibile elettronicamente, indicare:	[ ] Sì [ ] No [……..…] [……..…]

	(indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……][……..][……..]

Parte V: Riduzione del numero di candidati qualificati (ARTICOLO 70, COMMA 6, DEL CODICE)

L'operatore economico deve fornire informazioni solo se la stazione appaltante o l'ente concedente ha specificato i criteri e le regole obiettivi e non discriminatori da applicare per limitare il numero di candidati che saranno invitati a presentare un'offerta o a partecipare al dialogo. Tali informazioni, che possono essere accompagnate da condizioni relative ai (tipi di) certificati o alle forme di prove documentali da produrre eventualmente, sono riportate nell'avviso o bando pertinente o nei documenti di gara ivi citati.

Solo per le procedure ristrette, le procedure competitive con negoziazione, le procedure di dialogo competitivo e i partenariati per l'innovazione:

L'operatore economico dichiara:

Riduzione del numero	**Risposta:**
Di **soddisfare** i criteri e le regole obiettivi e non discriminatori da applicare per limitare il numero di candidati, come di seguito indicato :	[……]
Se sono richiesti determinati certificati o altre forme di prove documentali, indicare per **ciascun documento** se l'operatore economico dispone dei documenti richiesti:	[ ] Sì [ ] No ([29])
Se alcuni di tali certificati o altre forme di prove documentali sono disponibili elettronicamente ([28]), indicare per **ciascun documento**:	(indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione): [……..…][……][……]([30])

Parte VI: Dichiarazioni finali

Il sottoscritto/I sottoscritti dichiara/dichiarano formalmente che le informazioni riportate nelle precedenti parti da II a V sono veritiere e corrette e che il sottoscritto/i sottoscritti è/sono consapevole/consapevoli delle conseguenze di una grave falsa dichiarazione, ai sensi dell'articolo 76 del DPR 445/2000.

Ferme restando le disposizioni degli articoli 40, 43 e 46 del DPR 445/2000, il sottoscritto/I sottoscritti dichiara/dichiarano formalmente di essere in grado di produrre, su richiesta e senza indugio, i certificati e le altre forme di prove documentali del caso, con le seguenti eccezioni:

a) se la stazione appaltante o l'ente concedente hanno la possibilità di acquisire direttamente la documentazione complementare accedendo a una banca dati nazionale che sia disponibile gratuitamente in un qualunque Stato membro ([31]), oppure

b) a decorrere al più tardi dal 18 aprile 2018 ([32]), la stazione appaltante o l'ente concedente sono già in possesso della documentazione in questione.

Il sottoscritto/I sottoscritti autorizza/autorizzano formalmente [nome della stazione appaltante o dell'ente concedente di cui alla parte I, sezione A] ad accedere ai documenti complementari alle informazioni, di cui [alla parte/alla sezione/al punto o ai punti] del presente documento di gara unico europeo, ai fini della procedura relativa all'affidamento in oggetto.

Data, luogo e, se richiesto o necessario, firma/firme: [ ]

[28] Indicare chiaramente la voce cui si riferisce la risposta.
[29] Ripetere tante volte quanto necessario.
[30] Ripetere tante volte quanto necessario.
[31] A condizione che l'operatore economico abbia fornito le informazioni necessarie (*indirizzo web, autorità o organismo di emanazione, riferimento preciso della documentazione) in modo da consentire all'amministrazione aggiudicatrice o all'ente aggiudicatore di acquisire la documentazione. Se necessario, accludere il pertinente assenso.*
[32] In funzione dell'attuazione nazionale dell'articolo 59, paragrafo 5, secondo comma, della direttiva 2014/24/UE.

Oggetto: Servizio triennale comprensivo di canone per noleggio di una istanza ATP Core "on Premise" con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato.

NOMINA RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

1. Con la sottoscrizione della presente da parte di **Arpae Emilia-Romagna con sede in Via Po 5, 40139 Bologna, dirgen@cert.arpa.emr.it - Centralino 051- 6223811**, il Fornitore
Aruba PEC S.p.A. - Via San Clemente, 53 - 24036 Ponte San Pietro (BG) P.IVA 01879020517
PEC UFFICIOGARE@ARUBA.PEC.IT è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), per tutta la durata del contratto relativo all'affidamento della:

Sevizio piattaforma ATP Core on premise con attivazione dei moduli aggiuntivi **triennio 2026-27-28.**

A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto di Arpae Emilia-Romagna (Titolare del Trattamento), le sole operazioni di trattamento necessarie per fornire il servizio oggetto del contratto, nei limiti delle finalità ivi specificate, nel rispetto del Regolamento UE 2016/679, del D.Lgs. 196/2003 e s.m.i e del D. Lgs. n. 101/2018 (nel seguito anche "Normativa in tema di trattamento dei dati personali"), e delle istruzioni nel seguito fornite.

2. Il Fornitore/Responsabile si impegna a presentare su richiesta dell'Amministrazione garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile iniziale.

3. Le finalità del trattamento riguardano le attività erogate per servizio affidamento del servizio triennale per la di fornitura di Kit di Firma remota qualificata eIDAS, inclusa l'abilitazione dell'opzione del terzo interessato, Canoni ATP/VOL, Servizi CDRL e Manutenzione ARSS per Arpae.

In particolare tutti i dati personali raccolti (nome e cognome, numero di cellulare, indirizzo mail, comune di residenza e indirizzo, codice fiscale, password, chiave privata/pubblica ecc) per il rilascio della firma digitale remota.

4. Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: i) dati comuni (es. dati anagrafici e di contatto ecc.);

5. Le categorie di interessati sono: **utenti/dipendenti di Arpae e tutti i dati che interagiscono nei sistemi oggetto della fornitura.**

6. Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:

a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;

b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni

contrattuali;

c) trattare i dati personali conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente il Titolare del trattamento;

d) garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:

- si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
- ricevano la formazione necessaria in materia di protezione dei dati personali;
- trattino i dati personali osservando le istruzioni impartite dal Titolare al Responsabile;

e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);

f) adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

g) su eventuale richiesta dell'Amministrazione, assistere quest'ultima nello svolgimento della valutazione d'impatto sulla protezione dei dati personali, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;

h) ai sensi dell'art. 30 del Regolamento UE e nei limiti di quanto esso prescrive, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con l'Amministrazione e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta.

7. Ai sensi dell'articolo 32 del RGPD, adottare e mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche cui i dati personali oggetto di trattamento si riferiscono.

8. Il Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di cinque giorni lavorativi; nel caso in cui all'esito di tali verifiche periodiche le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, o risulti che il Fornitore agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima diffiderà il Fornitore ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzione entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi

dell'art. 1454 cc, l'Amministrazione, in ragione della gravità dell'inadempimento, potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

9. Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento (di seguito, "sub-Responsabile del trattamento") per gestire attività di trattamento dei dati per conto del Titolare. il Responsabile del trattamento deve informare tempestivamente il Titolare della nomina dei sub responsabili e loro variazione.

10. Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; l'Amministrazione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite verifiche anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inidonee l'Amministrazione potrà chiedere la presentazione di garanzie sufficienti entro un termine congruo ed in caso di mancato riscontro risolvere il contratto con il Responsabile iniziale.

Nel caso in cui all'esito delle verifiche le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento o risulti che il sub responsabile agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima diffiderà lo stesso a far adottare al sub-Responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzione entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione potrà, in ragione della gravità dell'inadempimento, risolvere il contratto attuativo con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

11. Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati. Qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ad informare tempestivamente il Titolare del trattamento, fornendo adeguato riscontro agli interessati, in nome e per conto del Titolare del trattamento, nei termini previsti dalla Regolamento UE.

12. Il Responsabile del trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del trattamento si impegna a supportare il Titolare nell'ambito di tale attività.

13. Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto.

14. Il Responsabile del trattamento deve comunicare al Titolare del trattamento il nome ed i dati del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati del Titolare.

15. Al termine della prestazione dei servizi oggetto del contratto, il Responsabile, su richiesta del Titolare, si impegna a: i) restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati; ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.

16. Il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali, trattati in esecuzione del contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Responsabile, o da un sub-Responsabile.

17. Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.

18. Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento.

19. Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

20. Il Responsabile del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Protezione dei Dati Personali e/o della disciplina sulla protezione dei dati personali contenuto nel Contratto comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o subappaltatori e/o sub-contraenti e/o subfornitori.

Con la sottoscrizione del presente atto, il Responsabile accetta la nomina e, in ottemperanza di quanto disposto dal Regolamento UE n.679/2016 , dal d.lgs 193/2003 e s.m.i. si impegna ad attenersi alle istruzioni impartite dal Titolare.

Luogo, Bologna

Il Titolare
ARPAE EMILIA ROMAGNA
(firma apposta in forma digitale secondo le norme vigenti)

Il Responsabile del trattamento
Aruba PEC S.p.A
(firma apposta in forma digitale secondo le norme vigenti)

Service Level Agreement (SLA) e Penali

È definita *Service Level Agreement* ("SLA") la metrica di Servizio che Aruba Pec si impegna a rispettare nei confronti del Cliente.

Obiettivo dello SLA è misurare il livello di qualità del Servizio erogato. Tale obiettivo viene perseguito attraverso la definizione del livello qualitativo standard garantito per l'erogazione del Servizio a cui vengono associati parametri oggettivi atti a monitorarne il rispetto, quali *Key Performance Indicators* ("KPI") e algoritmi di calcolo per la misurazione degli stessi.

Gli SLA possono essere distinti in 4 categorie principali:

- SLA di disponibilità del Servizio;
- SLA di reattività ad un *input*;
- SLA di rispetto dei tempi di reportistica;
- SLA di performance.

Le disposizioni contenute nel presente Allegato si applicano esclusivamente ai livelli del Servizio espressamente identificati come SLA nell'Allegato Tecnico o nell'apposita sezione della relativa Scheda Prodotto.

I KPI associati ai SLA sono continuamente monitorati da parte di Aruba Pec, attraverso strumenti e software dedicati. In nessun caso saranno prese in considerazione misurazioni dei KPI operate attraverso strumenti diversi dai sistemi predisposti da Aruba Pec.

In caso di mancato raggiungimento di uno o più SLA, in accordo a quanto previsto nelle Condizioni Generali di Contratto ed entro i limiti ivi previsti, Aruba Pec si impegna a riconoscere al Cliente un indennizzo a titolo di penale, fatto salvo il caso in cui il mancato raggiungimento dello SLA dipenda da:

- cause di forza maggiore;
- fatto del Cliente o di terza parte allo stesso riconducibile, indipendentemente dal fatto che lo stesso costituisca inadempimento
  o violazione contrattuale (in via meramente esemplificativa e non esaustiva: errato utilizzo del Servizio, errata configurazione o esecuzione, anche involontaria, di comandi atti a cagionare l'irraggiungibilità, l'interruzione o il malfunzionamento del Servizio, inadempimento o violazione del Contratto, etc.);
- volumi di Servizio che eccedano i limiti previsti;
- difetto di uno o più componenti software (ad es. bug) installati e/o comunque nella sfera di responsabilità del Cliente o di terza parte allo stesso riconducibile;
- mancata esecuzione di un intervento di manutenzione ordinaria o straordinaria, in tutti i casi in cui l'esecuzione dello stesso sia già stata proposta da Aruba Pec ma differita su richiesta del Cliente, ed il mancato raggiungimento del SLA sia dovuto ad un evento occorso nel periodo di differimento che l'intervento di manutenzione avrebbe evitato;
- circostanze al di là del ragionevole controllo di Aruba Pec (in via meramente esemplificativa e non esaustiva: guasti nella rete internet esterna al perimetro di Aruba);
- attacchi di hacker o Denial of Service volti a danneggiare il Servizio o altri servizi erogati da Aruba Pec e oggetto di denuncia all'autorità competente;
- guasti non dimostrabili, comunicati dal cliente ma non riscontrati da Aruba Pec.

Si sottolinea che, ai fini della misurazione dei KPI per la verifica del raggiungimento dello SLA, non saranno conteggiati i tempi relativi agli interventi di manutenzione programmata, così come definiti nelle Condizioni Generali del Contratto.

Al fine di verificare il rispetto degli SLA da parte di Aruba Pec, il Cliente può richiedere, con periodicità pari al periodo di riferimento previsto per la quantificazione delle penali, un report riepilogativo dei dati relativi al monitoraggio dei KPI di proprio interesse relativi allo SLA del servizio. La richiesta deve pervenire ad Aruba Pec, attraverso il sistema di trouble ticketing, entro e non oltre il giorno 15 del mese successivo al termine del periodo di riferimento per la quantificazione delle penali. Aruba Pec consegnerà il report al cliente entro 10 giorni lavorativi.

Entro 10 giorni lavorativi dal ricevimento del report, il Cliente deve notificare eventuali presunti casi di superamento dello SLA ad Aruba Pec tramite il sistema di trouble ticketing. Trascorso il suddetto termine il Cliente non avrà più diritto a richiedere il pagamento delle penali eventualmente dovute.

A seguito della notifica, Aruba Pec provvederà ad analizzare i dati in proprio possesso per valutare la fondatezza di quanto oggetto di contestazione, l'effettivo mancato raggiungimento di uno o più SLA e l'eventuale presenza di una delle condizioni di non applicazione delle penali ad esso associate. All'esito delle proprie valutazioni, Aruba Pec comunicherà al Cliente la propria intenzione di accogliere o rigettare la contestazione.

Aruba Pec dovrà accogliere la richiesta del Cliente in ogni caso in cui non sia in grado di fornire prova del rispetto dello SLA oggetto di contestazione o della sussistenza di una delle condizioni di non applicazione delle penali.

L'importo dell'indennizzo riconosciuto a titolo di penale sarà calcolato sulla base delle regole esposte nelle tabelle che seguono.

Modelli di calcolo delle penali relative agli SLA

Penali relative allo SLA di disponibilità del servizio

Classe di appartenenza SLA	Penale	Importo massimo di indennizzo
Uptime > 99,8%	2% del canone del periodo di riferimento relativo allo specifico servizio impattato per ogni ora (o parte di essi) di eccedenza (eccedenza = indisponibilità complessiva del servizio nel periodo di riferimento dopo il superamento dello SLA).	50% del canone del periodo di riferimento relativo allo specifico servizio impattato.
Uptime ≤ 99,8%	0,5% del canone del periodo di riferimento relativo allo specifico servizio impattato per ogni ora (o parte di essi) di eccedenza (eccedenza = indisponibilità complessiva del servizio nel periodo di riferimento dopo il superamento dello SLA)	30% del canone del periodo di riferimento relativo allo specifico servizio impattato

Il periodo di riferimento per la quantificazione delle penali si intende mensile, ove non diversamente specificato nell'Allegato Tecnico, se presente, o nella Scheda Prodotto.

Resta inteso che nel caso in cui i corrispettivi del Servizio siano definiti su base annuale, la penale sarà quantificata sul valore del canone annuale ripartito uniformemente su 12 mensilità.

La "classe di appartenenza SLA" corrisponde allo SLA del servizio come riportato nell'Allegato Tecnico, se presente, o nella Scheda Prodotto e si intende calcolato su base annuale, salvo che sia diversamente indicato nel medesimo Allegato Tecnico, se presente, o nella Scheda Prodotto.

Lo SLA di servizio annuale viene conteggiato a partire dalla data del collaudo o del rilascio in produzione del servizio. Nel caso di contratti di durata inferiore a 12 mesi con tacito rinnovo, viene preso come data d'inizio il giorno della prima attivazione. Il conteggio del tempo di indisponibilità si azzera dopo 12 mesi.

Penali relative allo SLA di reattività ad un *input*

Classe di appartenenza SLA	Penale	Importo massimo di indennizzo
Assistenza Small Enterprise / Enterprise	50€ per ogni ticket aggiuntivo in violazione dello SLA rispetto alla soglia di tolleranza pari al 10% dei ticket gestiti nel periodo di riferimento	1.000€ nel periodo di riferimento. L'importo si intende cumulativo per tutte le penali applicate a seguito di violazioni riscontrate a qualsivoglia SLA previsto per la classe di appartenenza.
Assistenza Enterprise Plus / Premium	1% del canone del periodo di riferimento relativo allo specifico servizio di Assistenza Premium o Enterprise Plus, se esplicitamente quotato, oppure 100€ per ogni ticket aggiuntivo in violazione dello SLA rispetto alla soglia di tolleranza pari al 10% dei ticket gestiti nel periodo di riferimento	50% del canone del periodo di riferimento relativo allo specifico servizio di Assistenza Premium o Enterprise Plus, se esplicitamente quotato, oppure di 2.000€ nel periodo di riferimento. L'importo si intende cumulativo per tutte le penali applicate a seguito di violazioni riscontrate a qualsivoglia SLA previsto per la classe di appartenenza.

Il periodo di riferimento, ove non diversamente specificato, si intende trimestrale.

Si sottolinea che, ai fini della misurazione dei KPI per la verifica del raggiungimento del SLA, non saranno conteggiati i tempi di attesa relativi ad attività in carico al Cliente.

Si specifica che l'indennizzo a titolo di penale sarà dovuto esclusivamente nel caso in cui il servizio sia attivato per un periodo non inferiore ad un trimestre e siano gestiti un numero di almeno 10 ticket nel periodo di riferimento.

Penali relative allo SLA di rispetto dei tempi di reportistica

Classe di appartenenza SLA	Penale	Importo massimo di indennizzo
Report Assistenza Small/Enterprise	100€ di ritardo per ogni intervallo completo di 10 giorni lavorativi eccedenti la data prevista	500€ nel periodo di riferimento
Report Assistenza Enterprise Plus/Premium	50€ di ritardo per ogni giorno lavorativo eccedente la data prevista	500€ nel periodo di riferimento

Il periodo di riferimento, ove non diversamente specificato, si intende trimestrale.

Si sottolinea che, ai fini della misurazione dei KPI per la verifica del raggiungimento del SLA, non saranno conteggiati i tempi di attesa relativi ad attività in carico al Cliente o a terze parti responsabili di fornire le informazioni necessarie.

Penali relative allo SLA di performance

Classe di appartenenza SLA	Penale	Importo massimo di indennizzo
Performance	100€ per ogni ora completa in cui lo standard di performance non è stato rispettato	10% del canone del periodo di riferimento relativo al servizio interessato dal mancato rispetto delle performance contrattualizzate

Il periodo di riferimento, ove non diversamente specificato, si intende trimestrale.

FIRMA REMOTA

La **Firma Remota** è una modalità di firma digitale che, garantendo lo stesso grado di sicurezza e gli stessi effetti di legge della tradizionale firma digitale basata su smart card o token USB, consente di poter usufruire di numerosi vantaggi, tra i quali ad esempio:

- apporre firme digitali senza la necessità di ricorrere all'installazione di hardware o driver;
- sottoscrivere digitalmente documenti informatici via web in condizioni di massima sicurezza;
- disporre in ogni momento della propria firma digitale su diversi ambienti (Windows, Linux, Mac, tablet, smartphone) semplicemente installando il software Aruba Sign o l'apposita app Firma Digitale Aruba;
- eliminazione delle problematiche legate all'incompatibilità di particolari dispositivi (lettori, smart card e token USB) con determinate piattaforme hardware o software.

La Firma Remota è il risultato di una procedura informatica basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. La particolarità della Firma Remota sta nel fatto che la chiave privata assegnata al titolare del certificato viene custodita direttamente dalla Certification Authority all'interno di appositi apparati certificati a tale scopo (normalmente un HSM – Hardware Security Module) - i dati da firmare (o meglio la loro impronta) sono inviati allo HSM attraverso la rete, e la risposta ritorna all'utente sempre attraverso la rete.

Possono dotarsi di Firma Remota tutte le persone fisiche – cittadini, amministratori e dipendenti di società e pubbliche amministrazioni – che hanno l'esigenza di verificare e sottoscrivere a validità legale tutti quei documenti elettronici (contratti, documenti, moduli) che richiedono l'apposizione di una firma. Professionisti, aziende, Pubblica Amministrazione e privati possono intraprendere lo scambio di documentazioni in formato elettronico, con una notevole velocizzazione dei tempi e un maggiore livello di sicurezza rispetto alle metodiche tradizionali.

I documenti firmati tramite soluzione di Firma Remota conservano le caratteristiche di:

- **Autenticità** | La Firma Remota garantisce l'identità del sottoscrittore (verificata da un Operatore di Riconoscimento della Certification Authority che rilascia il certificato).
- **Integrità** | La Firma Remota è legata al documento elettronico sul quale è apposta e assicura che il documento non sia stato modificato dopo la sottoscrizione.
- **Non ripudio** | Il documento assume piena validità legale e pertanto non può essere ripudiato dal sottoscrittore, in piena conformità alla normativa nazionale (DPCM 22 febbraio 2013) e alla normativa europea (Regolamento UE n. 910/2014 del 23 luglio 2013 – EIDAS).

COME FUNZIONA

Per riuscire ad offrire le garanzie sopra descritte (in particolar modo la non ripudiabilità) è necessario che l'utente venga identificato con certezza dall'Autorità di Certificazione che rilascia il certificato. Questo consente di assicurare la corrispondenza tra la Firma Digitale e il titolare; il grado di affidabilità di questa associazione è legato a diversi fattori, quali, ad esempio, la modalità con cui il certificatore ha emesso il certificato, le misure di sicurezza adottate e le garanzie offerte dallo stesso, gli obblighi assunti dal titolare per la protezione della propria chiave privata.

Al fine di permettere la definizione di processi di rilascio di certificati digitali che meglio possano adattarsi alle esigenze di business del cliente, Actalis e Aruba PEC, in qualità di Trust Service Provider Qualificati eIDAS, mettono a disposizione differenti procedimenti di riconoscimento, che spaziano dalle modalitá a distanza (es. con SPID o CIE) a quelle con il supporto di un operatore (DVO). Sono disponibili anche metodi di riconoscimento in presenza con processi dematerializzati.

L'utente, una volta che è stato riconosciuto, viene dotato del Kit di Firma Digitale Remota composto dai tre elementi descritti di seguito nel dettaglio:

- **Certificato qualificato** | Custodito e mantenuto dalla Certification Authority sui propri HSM (Hardware Security Model, cioè apparati sicuri, a prova di manomissione anche fisica, che garantiscono l'impossibilità di estrazione della chiave privata del certificato di firma e di conseguenza il suo utilizzo senza l'approvazione del titolare).
- **Dispositivo OTP** | Utilizzato per generare il secondo fattore di autenticazione, tramite le tipologie di dispositivi di seguito descritte:
  - **Token OTP hardware-display** | Un piccolo apparecchio dotato di display LCD e pulsante per la generazione dei codici temporanei.
  - **Token OTP hardware-USB** | Una chiavetta USB dotata di un pulsante a sfioramento che genera il codice temporaneo e lo scrive automaticamente nel relativo campo del software di firma, precedentemente selezionato con il mouse.
  - **App Aruba OTP** | Un'applicazione da installare su una vasta gamma di dispositivi mobile.
  - **Aruba SMS** | Soluzione che prevede l'invio del codice OTP tramite SMS sul numero di cellulare.
- **Software di firma e verifica** | Il software di firma e verifica è fornito in versione sia desktop che mobile e viene utilizzato dall'utente per generare e verificare firme digitali (oltre ad altre funzionalità operative).

Per quei contesti d'utilizzo *Enterprise* nei quali si ha l'esigenza di integrare le funzionalità della Firma Remota con i sistemi di gestione documentale interni all'organizzazione è inoltre prevista la possibilità di fornitura del componente ATP (Aruba Trusted Platform).

ATP è il componente software che permette una semplice integrazione delle applicazioni e dei sistemi con il Servizio di Firma Remota. Nel caso di applicazioni ospitate in infrastrutture IT differenti da quella dove risiede il Sistema di Firma Remota, ATP dialoga, su HTTPS con mutua autenticazione, con i Sistemi della CA, esponendo verso le applicazioni in questione tutte le funzionalità di firma digitale.
La soluzione di Firma Remota – ATP è estremamente flessibile e consente due diverse modalità di erogazione Enterprise:

- **On-premise** | viene fornita completa dei componenti software necessari per l'erogazione di tutte le funzionalità del sistema. Nella modalità On-premise può essere configurata la ridondanza affiancando più "sistemi" identici, per realizzare soluzioni in High Availability (HA) o predisporre siti di Disaster Recovery (DR).
- **Cloud** | viene erogata dai Data Center Aruba attraverso:
  - una piattaforma condivisa, configurata in modalità HA nativa e con DR geografico;
  - una soluzione dedicata al cliente, con possibilità di attivazione di HA e/o DR.

CARATTERISTICHE TECNICO – FUNZIONALI

COMPLIANCE

Normativa di riferimento	**D.P.C.M. 22 febbraio 2013** | Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali **C.A.D. 7 marzo 2005** | Codice dell'Amministrazione Digitale **Regolamento UE n. 910/2014 del 23 luglio 2014** | Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno
Autorità di Certificazione	**Actalis S.p.A**. e **Aruba PEC S.p.A**. sono i certificatori qualificati per la fornitura di servizi fiduciari qualificati iscritti all'elenco dei prestatori di servizi fiduciari stabiliti in Italia, tenuto presso l'AgID (Agenzia per l'Italia Digitale) e reso pubblico dalla Commissione europea attraverso un proprio elenco
Garanzia	I documenti così sottoscritti assumono piena efficacia probatoria

CARATTERISTICHE DEL SERVIZIO

Scalabilità	Orizzontale con bilanciamento e *fault tolerance* - L'architettura del sistema consente una scalabilità orizzontale, permettendo di aggiungere, in modo trasparente, ulteriori linee di erogazione sia nella componente di *front end* ATP che in quelle di *back end*: è quindi sempre possibile garantire adeguate performance all'aumentare dei volumi
Disponibilità del servizio	*High Availability & Disaster Recovery* - Il sistema garantisce requisiti continuità operativa e bilanciamento di carico poiché ogni componente (sia fisico che applicativa) dell'architettura può essere ridondato al fine di escludere singoli punti di *failure*. Nelle soluzioni dedicate, on premise o in cloud, dipende dalla configurazione acquistata
Certificati	Qualificati in standard X.509 conformi al Regolamento UE n. 910/2014 del 23 luglio 2013 – EIDAS – e alle Linee guida AgID (Determinazione 147 del 4 giugno 2109)
Tipologia di firma	CAdES PAdES (visibile e invisibile) XadES JAdES ASiC-S e ASiC-E
Marca Temporale	Attached, Detached
Verifica documenti firmati	Integrazione applicativa tramite il modulo aggiuntivo di validazione on line

SERVICE LEVEL AGREEMENT (SLA)

SLA di disponibilità del servizio di Firma Digitale Remota e del servizio di emissione certificati (CMS)	• Uptime garantito del 99,95%
SLA di disponibilità del servizio di verifica validità della firma (CRL, OCSP)	• Uptime garantito del 99,95%
SLA di disponibilità del servizio di sospensione e revoca	• Uptime garantito del 99,95%
Incident Management e Service Request	• Vale quanto previsto ed indicato nella scheda relativa al servizio di Assistenza Enterprise

I servizi effettivamente offerti sono esclusivamente quelli espressamente indicati nell'Offerta Economica.

KIT DI FIRMA DIGITALE

Il **Kit di Firma Digitale** è l'insieme di dispositivi necessari per sottoscrivere documenti digitalmente, tramite certificati di firma digitale. La firma digitale costituisce la più forte istanza di sottoscrizione informatica perché può essere utilizzata in ogni contesto con lo stesso valore giuridico della firma autografa (DPCM 22 febbraio 2013, Deliberazione CNIPA n. 45/2009 e s.m.i.). Con il Regolamento eIDAS (Regolamento UE n. 910/2014 del 23 luglio 2013) è, inoltre, di valore europeo e interoperabile all'interno del mercato interno, poiché le regole tecniche sono comuni a tutti gli Stati membri.
La firma digitale ha le seguenti caratteristiche:

- **autenticità**: la firma digitale garantisce l'identità del sottoscrittore (verificata da un Operatore di Riconoscimento della Certification Authority che rilascia il certificato);
- **integrità**: la firma digitale è legata al documento elettronico sul quale è apposta e assicura che il documento non sia stato modificato dopo la sottoscrizione;
- **non ripudio**: la firma digitale attribuisce piena validità legale al documento, pertanto il documento non può essere ripudiato dal sottoscrittore.

La firma digitale è il risultato di una procedura informatica basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Possono dotarsi di firma digitale tutte le persone fisiche – cittadini, amministratori e dipendenti di società e pubbliche amministrazioni – che hanno l'esigenza di verificare e sottoscrivere a validità legale tutti quei documenti elettronici (contratti, documenti, moduli) che richiedono l'apposizione di una firma. Professionisti, aziende, Pubblica Amministrazione e privati possono intraprendere lo scambio di documentazioni in formato elettronico, con una notevole velocizzazione dei tempi e un maggiore livello di sicurezza rispetto alle metodiche tradizionali.
Aruba Enterprise ha deciso di fondere le funzionalità di firma digitale a quelle CNS (Carta Nazionale dei Servizi) perché oggi la CNS è sempre più richiesta sia dai cittadini che dalle aziende e per alcune categorie professionali è diventata uno strumento necessario per autenticarsi ai propri punti di accesso telematici, come per gli avvocati è lo strumento necessario per il processo civile telematico, per gli architetti lo è per lo scambio di pratiche con le PA o per altre categorie come geometri, ingegneri e commercialisti ecc.

COME FUNZIONA

Per riuscire ad offrire le garanzie sopra descritte (in particolar modo la non ripudiabilità) è fondamentale che l'utente che richiede un Kit di Firma Digitale venga identificato con certezza dall'Autorità di Certificazione che rilascia i Certificati.
Il processo di riconoscimento può essere eseguito con strumenti informatici o tramite procedura DeVisu di persona o da remoto con webcam o smartphone tramite gli Operatori di Registrazione (OdR), personale specializzato che viene delegato dalle Autorità di Certificazione che rilasciano i Certificati (Aruba PEC e Actalis) all'identificazione dei Titolari e, eventualmente, all'emissione diretta e in loco di certificati a pieno valore legale.
In caso si desideri ottenere la Delega di OdR, ed essere autonomi nelle operazioni di riconoscimento ed emissione, è necessario un processo di formazione online al termine del quale l'operatore viene dotato di un accesso al sistema di Certificate Management System (CMS) per il riconoscimento ed emissione dei certificati qualificati di firma qualificata e CNS.

L'utente, una volta che è stato riconosciuto, viene dotato del **Kit di Firma Digitale** composto da:

- **Smart/SIM Card** contente due certificati:
  - il certificato di Firma Qualificata che identifica il titolare e grazie al quale è possibile firmare documenti a valore legale;
  - il certificato di autenticazione CNS (Carta Nazionale dei Servizi) che permette al titolare di accedere ai servizi online offerti dalla Pubblica Amministrazione.
- **Lettore di Smart Card** (opzionale) permette l'interazione del PC con la Smart/SIM Card;

- **Software di Firma e Verifica** utilizzato dall'utente per generare e verificare Firme Digitali (oltre ad altre funzionalità operative) e, previa attivazione di un account, apporre un riferimento temporale certo (Marcatura Temporale).

Per generare una firma digitale su un documento informatico, è necessario che l'utente inserisca il PIN del proprio Kit di firma digitale all'interno del software di Firma; l'operazione genererà un nuovo documento informatico arricchito dei metadati che permetteranno al destinatario del documento la verifica di autenticità, integrità e non ripudio.

In caso di necessità il titolare può richiedere la sospensione e revoca immediata del certificato secondo quanto riportato nel manuale operativo reperibile online sul sito della CA di riferimento (www.pec.it per Aruba PEC e www.actalis.it per Actalis).

CARATTERISTICHE TECNICO – FUNZIONALI

COMPLIANCE

Normativa di riferimento	**D.P.C.M. 22 febbraio 2013** | Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali **C.A.D. 7 marzo 2005** | Codice dell'Amministrazione Digitale **Regolamento UE n. 910/2014 del 23 luglio 2014** | Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno
Autorità di Certificazione	**Actalis S.p.A**. e **Aruba PEC S.p.A**. sono le Autorità di Certificazione iscritte all'Elenco Pubblico dei Certificatori accreditati, tenuto presso l'AgID (Agenzia per l'Italia Digitale)
Garanzia	I documenti così sottoscritti assumono piena efficacia probatoria

CARATTERISTICHE DEL SERVIZIO

Tipologie di firma	• CadES • PadES (visibile e invisibile) • XAdES • ASiC-S e ASiC-E
Tipologie di Kit	• ArubaKey: SIM Card + pendrive USB con 2 GB di memoria + software portable preinstallato • Token: SIM Card + pendrive USB • SIM Card / Smart Card + lettore USB
Software di firma e verifica	• ArubaKey preinstallato nel Kit ArubaKey • ArubaSign o File Protector installabile nei computer dell'utente
Marca temporale	• Attached (TSD) • Detached (TSR)

SERVICE LEVEL AGREEMENT (SLA)

SLA di disponibilità del servizio di verifica validità della firma (CRL, OCSP)	Uptime garantito del 99,95%
SLA di disponibilità del servizio di emissione certificati (CMS)	Uptime garantito del 99,95%
SLA di disponibilità del servizio di sospensione e revoca	Uptime garantito del 99,95%

I Servizi effettivamente offerti, comprese le loro caratteristiche tecnico funzionali, sono esclusivamente quelli espressamente indicati nell'Offerta Economica.

Condizioni Generali di fornitura dei Servizi di Certificazione Enterprise

Disposizioni di carattere generale

Le presenti Condizioni generali disciplinano il rapporto contrattuale per la fornitura dei Servizi di Certificazione che si perfeziona tra Aruba PEC S.p.A., con sede in Ponte San Pietro, Via San Clemente n. 53, P.I. e C.F. 01879020517 (di seguito anche "Aruba PEC") ed il Cliente, così come indicato nel Modulo d'ordine; quando indicati congiuntamente Aruba PEC ed il Cliente saranno denominati "Parti".

INDICE DEGLI ARTICOLI ..... ERRORE. IL SEGNALIBRO NON È DEFINITO.

1. Definizioni

I termini sotto riportati hanno il seguente significato, siano essi indicati al singolare o al plurale:

24/7/365: acronimo utilizzato nel Contratto per indicare la continuità del Servizio 24 ore su 24, 7 giorni alla settimana, 365 giorni all'anno.

Allegato Tecnico: se presente, il documento, alternativo alla Scheda prodotto, redatto e trasmesso da Aruba PEC al Cliente, nel quale sono descritte le specifiche tecniche del Servizio.

Aruba PEC: Aruba PEC S.p.A. società del Gruppo Aruba, iscritta negli elenchi pubblici dei Gestori di Posta Elettronica Certificata, dei Certificatori, dei Prestatori di Servizi Fiduciari e dei Conservatori accreditati predisposti, tenuti ed aggiornati dall'Agenzia per l'Italia Digitale, che gestisce ed eroga il Servizio di Posta Elettronica Certificata, emette Certificati di Firma Digitale e Marche Temporali aventi valore legale a norma del combinato disposto del D.lgs. n. 82/2005 e del D.P.C.M. 22 febbraio 2013 e successive modifiche ed integrazioni, certificati elettronici qualificati, sigilli elettronici qualificati e servizi di Validazione temporale elettronica qualificata a norma del Regolamento (UE) n. 910/2014 nonché svolge attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82 (di seguito anche "Certificatore").

Cliente: la persona giuridica, o altro tipo di società o ente, indicata nel Modulo d'ordine, che nell'ambito della propria attività imprenditoriale, commerciale, artigianale o professionale conclude con Aruba PEC il Contratto per la fornitura dei Servizi.

Centro di Registrazione Locale - CDRL: il soggetto che, in forza di autonomo contratto stipulato con Aruba Pec mediante la sottoscrizione dell'apposito Modulo di Adesione, è autorizzato da Aruba Pec stessa allo svolgimento delle attività finalizzate all'emissione di servizi di certificazione digitale.

Certificato di autenticazione: Il Certificato consistente nell'attestato elettronico che assicura l'autenticità delle informazioni necessarie per l'identificazione in rete del titolare della CNS rilasciato da Aruba Pec su delega dell'Ente Emettitore come previsto nel D.P.R. 2 marzo 2004, n. 117, e nel Manuale Operativo CNS e che permette l'accesso ai sistemi informatici detenuti dalle Pubbliche Amministrazioni;

Certificato di firma: Il Certificato che collega i dati utilizzati per verificare la Firma digitale al titolare e confermare la sua identità, emesso dal Certificatore ARUBA PEC S.p.A. come previsto nell'art. 3, 1° comma, n. 15 del Regolamento, nel CAD, nelle regole tecniche da esso richiamate e nel Manuale Operativo.

Certificato: la definizione utilizzata nel Contratto per indicare indifferentemente il Certificato di firma e/o il Certificato di autenticazione e quando non è necessario specificare di quale certificato si tratti;

CMS (Content Management System): Pannello messo a disposizione del Cliente al fine di agevolare la creazione e la gestione della documentazione per erogare il Servizio oltre che per eseguire le attività di identificazione ed emissione dei certificati.

Condizioni generali: il presente documento.

Contratto: il complesso dei documenti indicati all'art. 2.1.

Data Processing Agreement - DPA: se previsto, l'accordo, redatto da Aruba PEC in osservanza della disciplina prevista dal Regolamento UE 2016/679 e dalla normativa di settore vigente, avente ad oggetto le modalità e le condizioni di trattamento dei dati personali.

Firma automatica: particolare procedura informatica di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo;

Firma digitale "one shot": particolare tipo di Firma digitale remota basata su un certificato di sottoscrizione utilizzabile esclusivamente per la sottoscrizione di documenti provenienti da specifiche procedure informatiche c.d. "one shot" previste sul sito www.pec.it e secondo le modalità e con le limitazioni previste nel Manuale e nel Contratto.

Firma digitale CNS: tipologia di Firma digitale contenente anche il Certificato di autenticazione;

Firma digitale remota: particolare tipo di firma digitale, generata su HSM sotto il pieno controllo di Aruba Pec, che garantisce al Cliente un controllo esclusivo sulle chiavi private; su richiesta del Cliente tale firma può essere fornita anche con l'opzione "Moda lità verificata" giusto quanto previsto dall'art. 19 DPCM 22 febbraio 2013;

Firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Cliente tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici**;**

Incaricato al Riconoscimento – I.R.: il soggetto incaricato da Aruba Pec o dal C.D.R.L. nel rispetto delle istruzioni impartite dal Certificatore, che è preposto allo svolgimento delle attività propedeutiche al rilascio di servizi di certificazione digitale;

Informativa Privacy Aruba PEC: il documento pubblicato alla pagina https://www.pec.it/documents/tc-files/it/93_informativaprivacyarubapec.pdf che descrive le modalità di trattamento dei dati personali dei Clienti Aruba PEC;

Intervento di emergenza: intervento volto a risolvere una situazione critica o potenzialmente critica per il funzionamento del Servizio.

Manuale Operativo (Manuale Operativo "Servizi di certificazione"): ove applicabile, il documento pubblicato o pubblico a norma di

legge, predisposto da Aruba PEC e verificato dall'Agenzia per l'Italia Digitale, contenente l'indicazione delle procedure di rilascio, delle modalità operative e le istruzioni per l'uso del Servizio, disponibile al link http://www.pec.it/Documentazione.aspx .

Manuale Operativo "Carta Nazionale dei Servizi – CNS": il manuale pubblicato e pubblico a norma di legge contenente l'indicazione delle procedure di rilascio del Certificato di autenticazione (quando insieme al Manuale Operativo "Servizi di Certificazione", Manuale o anche "Manuali") disponibile per il download al link http://www.pec.it/DocumentazioneFirmaDigitale.aspx , che il Cliente, con la sottoscrizione del Modulo d'ordine, dichiara di aver visionato, di conoscere, di accettare e di fare proprio in ogni sua parte.

Manuale CPS (Certificate Policy Standard): il manuale pubblicato e pubblico a norma di legge contenente l'indicazione delle procedure di rilascio del Certificato eIDAS e del Sigillo eIDAS (quando insieme al Manuale Operativo "Carta Nazionale dei Servizi – CNS" Manuale o anche "Manuali") disponibile per il download al link http://www.pec.it/DocumentazioneFirmaDigitale.aspx , che il Cliente con la sottoscrizione del Modulo d'ordine, dichiara di aver visionato, di conoscere, di accettare e di fare proprio in ogni sua parte;

Manuale Validazione Temporale: il Manuale Operativo del Servizio, presente al link https://www.pec.it/DocumentazioneMarcheTemporali.aspx, il quale riporta la politica e la descrizione del Servizio di Validazione Temporale Elettronica Qualificata, le sue caratteristiche, i livelli di servizio, le eventuali limitazioni d'uso del medesimo e le prescrizioni per coloro che accedano alla verifica delle validazioni temporali elettroniche.

Manutenzione Programmata: intervento di manutenzione programmata effettuato al fine di garantire nel tempo le normali condizioni di funzionamento del Servizio e di prevenire e/o eliminare eventuali guasti o anomalie.

Manutenzione Straordinaria: intervento di manutenzione programmata eseguito al verificarsi di situazioni non prevedibili che richiedono una pronta soluzione.

Modulo d'ordine: modulo predisposto da Aruba PEC che, sottoscritto dal Cliente mediante un proprio rappresentante legale o un procuratore o un delegato o un diverso soggetto dotato dei necessari poteri di firma e dal medesimo trasmesso alla stessa Aruba PEC, costituisce accettazione del Contratto.

Modulistica per il Titolare del Servizio: modulo predisposto da Aruba PEC, reperibile sul Pannello di Gestione, se presente, o altrimenti trasmessa al Cliente da Aruba Pec, che, compilato e sottoscritto dal Cliente o dal Titolare (se diverso dal Cliente) e da quest'ultimo consegnato al Cliente medesimo, formalizza la richiesta di attivazione del Servizio ed indica le informazioni necessarie alla identificazione del Cliente o del Titolare;

Offerta Economica: il documento redatto e trasmesso da Aruba PEC al Cliente nel quale sono descritte le condizioni economiche del Servizio.

Operatore di Registrazione – O.D.R.: il soggetto incaricato dal C.D.R.L. che, nel rispetto delle istruzioni impartite dal Certificatore, è preposto allo svolgimento delle attività inerenti il rilascio di servizi di certificazione digitale oggetto del contratto;

PKI Disclosure Statement PDS: il documento che, unitamente al Manuale/CPS, al presente Contratto ed alla normativa applicabile disciplina il servizio di rilascio di certificati eIDAS e sigilli eIDAS.

Policy di sicurezza per Soluzioni di firma in-house: il documento, applicabile se previsto nell'Allegato Tecnico o nella Scheda Prodotto, che definisce i requisiti tecnici e organizzativi che il Cliente deve soddisfare per poter adottare soluzioni di firma in-house nonché le responsabilità del Cliente stesso nei confronti della Certification Autority, comprensivo della Dichiarazione di sussistenza dei requisiti.

Requisiti per riconoscimento con modalità 6 del MO: il documento redatto da Aruba PEC, ed applicabile al Cliente eventualmente nominato C.D.R.L., che definisce i requisiti organizzativi e di sicurezza che il Cliente, in qualità di datore di lavoro, deve soddisfare per poter procedere all'identificazione del Richiedente ai sensi della modalità 6 del Manuale Operativo.

Regolamento: il Regolamento UE n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014, in materia di "identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno", la normativa tecnica in esso richiamata, gli atti esecutivi dello stesso della Commissione Europea ed eventuali successive modifiche ed integrazioni.

Request for Change (o RFC): è il meccanismo, così come previsto anche dallo standard ITIL, per richiedere un cambiamento al Servizio. La RFC deve contenere tutte le informazioni necessarie affinché un cambiamento possa essere valutato, approvato e implementato.

Pannello di Gestione: l'area e/o le aree per la gestione e/o il monitoraggio di ciascun Servizio alla quale il Cliente accede con le apposite Credenziali di accesso, attraverso una applicazione sicura raggiungibile via web.

Scheda prodotto: se presente, il documento, alternativo all'Allegato Tecnico, redatto e trasmesso da Aruba PEC al Cliente nel quale sono descritte le specifiche tecniche del Servizio.

Service Level Agreement - SLA: il complesso di informazioni contenute nelle presenti Condizioni generali e nelle Specifiche Tecniche di ciascun Servizio che definiscono i livelli di servizio e le penali a carico di Aruba PEC in caso di mancato raggiungimento dei livelli di servizio stabiliti.

Aruba PEC S.p.A.
VIA SAN CLEMENTE 53
24036 PONTE SAN PIETRO (BG)
Tel. +39 0575.0500 – FAX +39 0575.862020
enterprise.aruba.it

Capitale Sociale € 6.500.000,00 i.v.
REA: 445886
Codice Fiscale 01879020517
Partita IVA 01879020517

Servizio/i: ciascuno dei Servizi di certificazione forniti da Aruba PEC su richiesta del Cliente, il tutto come meglio descritto nell'Allegato Tecnico o nella Scheda Prodotto e nel Manuale operativo.

Specifiche tecniche: complesso di informazioni contenute nel Manuale Operativo e/o nella Scheda Prodotto o nell'Allegato Tecnico che definiscono le caratteristiche tecniche, funzionali, qualitative e logistiche del Servizio.

Titolare/i: il soggetto individuato nella Modulistica per il Titolare del Servizio, intestatario di un servizio di certificazione.

Restano ferme le altre definizioni riportate nel Manuale Operativo.

2. Struttura del Contratto e ordine di prevalenza

2.1 Costituiscono parte integrante del Contratto i documenti sotto indicati da interpretarsi ed applicarsi con l'ordine di prevalenza che segue:

1) Condizioni generali;
2) Offerta Economica;
3) Modulo d'ordine;
4) Allegato Tecnico o Scheda Prodotto;
5) Modulo di Adesione al contratto per lo svolgimento di attività inerenti il rilascio di servizi di certificazione digitale – C.D.R.L., se previsto;
6) Modulistica per il Titolare del Servizio;
7) Manuale Operativo, se applicabile, per lo specifico servizio;
8) Policy di Sicurezza per Soluzioni di firma in house, applicabile se previsto dall'Allegato Tecnico o dalla Scheda Prodotto e relativa Dichiarazione di sussistenza dei requisiti;
9) Requisiti per riconoscimento con modalità 6 del MO, se applicabile;
10) Data Processing Agreement, se previsto;
11) SLA e Penali.

Resta inteso che per i documenti sottoscritti in data successiva al perfezionamento del Contratto gli stessi formeranno parte integrante del medesimo a far data e per effetto di tale sottoscrizione.

2.2 Il Cliente dichiara e riconosce che il Manuale Operativo è di esclusiva proprietà di Aruba PEC, la quale come tale è l'unica ed esclusiva titolare di ogni relativo diritto intellettuale. Il Cliente dichiara di aver preso visione, di conoscere, di accettare e di fare proprio in ogni sua parte, il contenuto del Manuale.

3. Oggetto del Contratto, perfezionamento

3.1 Oggetto del Contratto è la fornitura al Cliente del Servizio alle condizioni indicate nel Contratto e conformemente alle previsioni della normativa applicabile.

3.2 Qualsiasi prestazione ulteriore rispetto a quelle oggetto del Contratto potrà essere fornita, previo esame di fattibilità, su richiesta specifica del Cliente a condizioni, termini e corrispettivi da concordare.

3.3 Il Contratto si perfeziona quando Aruba PEC riceve il Modulo d'Ordine sottoscritto dal Cliente. Il Contratto è concluso in lingua italiana, eventuali altre versioni in lingua straniera sono messe a disposizione del Cliente esclusivamente a titolo di cortesia.

4 Durata e rinnovo del Contratto

4.1 La durata del Contratto è quella indicata nell'Offerta Economica.

4.2 Qualora sia indicata nell'Offerta Economica la modalità di rinnovo tacito, il Contratto si rinnova automaticamente alla scadenza per il periodo indicato nell'Offerta Economica e così di seguito alle scadenze successive, salvo disdetta comunicata dal Cliente ad Aruba PEC entro 60 (sessanta) giorni prima della scadenza mediante lettera raccomandata A/R ad Aruba PEC S.p.a. - Ponte San Pietro, 24036 (BG), Via San Clemente n. 53, o posta elettronica certificata (PEC) all'indirizzo recessi@aruba.pec.it.

4.3 Salvo quanto previsto al precedente articolo 4.2 e dal successivo art. 5.3, per proseguire con l'erogazione del Servizio sarà necessaria la stipula di un nuovo contratto. Resta fermo che, al fine di garantire la continuità dell'erogazione del Servizio da parte di Aruba PEC, il Cliente, entro un ragionevole termine antecedente la data di scadenza del Contratto, dovrà manifestare la propria volontà di stipulare un nuovo contratto per la fornitura del Servizio.

4bis. Durata e rinnovo dei Certificati

4bis.1. Il Certificato ha validità fino alla data di sua scadenza. All'approssimarsi della predetta data, Aruba PEC a mero titolo di cortesia e quindi senza con ciò assumere alcuna obbligazione nei confronti del Cliente o del Titolare, si riserva di inviare avvisi di prossima scadenza del Certificato. In caso si intenda continuare ad usufruire del Certificato, il Cliente o il Titolare potranno richiederne l'emissione

di uno nuovo sulla base delle condizioni contrattuali vigenti al momento della richiesta. Il Cliente o il Titolare sollevano ora per allora Aruba PEC da ogni e qualsiasi responsabilità derivante da ordini, transazioni o pagamenti effettuati trascorso il termine di scadenza del Certificato ovvero in tempi tali da pregiudicare la continuità del Servizio fornito al Cliente e/o al Titolare e si impegna a manlevarla e tenerla indenne da ogni conseguente richiesta o pretesa di risarcimento per danni diretti o indiretti, avanzata dal Titolare, dal Cliente e/o da chiunque in genere.

4bis.2 Fermo quanto sopra, in fase di richiesta o rinnovo del Certificato di firma e di accettazione delle presenti Condizioni generali al Cliente è riconosciuta la facoltà di attivare la modalità di rinnovo tacito del Certificato di firma digitale remota. Nei casi di esercizio di tale facoltà da parte del Cliente, alla data di scadenza del Certificato di firma digitale remota lo stesso sarà rinnovato in automatico secondo la procedura descritta all'interno del Manuale Operativo. E' fatta sempre salva la possibilità per il Cliente in qualunque momento di disattivare la modalità di rinnovo tacito del Certificato di firma digitale remota nel rispetto dei termini e con le modalità stabiliti dalla Certification Authority.

4bis.3 Il Cliente prende atto ed accetta che, nel caso in cui il supporto hardware (Dispositivo di firma digitale) su cui il Certificato è contenuto sia oggetto di perdita o scadenza della certificazione di sicurezza prevista dalla normativa di riferimento, non potrà essere più utilizzabile e sarà revocato da Aruba PEC secondo le modalità previste dal Manuale Operativo.

5. Corrispettivi, modalità e termini di pagamento

5.1 Salvo diverso accordo scritto tra le Parti, i termini di fatturazione decorrono dalla data di attivazione del Servizio; le modalità e i termini di pagamento sono indicati in Offerta Economica. In caso il Cliente attivi più Servizi nell'ambito del Contratto, i termini di fatturazione per ciascuno di detti Servizi decorreranno a far data dall'attivazione di ciascuno di essi secondo quanto specificato nell'Offerta Economica ai sensi del successivo art. 6.

5.2 Fatta salva l'applicazione del successivo art. 12, in caso di mancato o parziale pagamento dei corrispettivi dovuti entro la data di scadenza pattuita, Aruba PEC invierà una comunicazione scritta al Cliente concedendo al medesimo un termine di 15 (quindici) giorni per provvedere al pagamento, durante il quale Aruba PEC garantirà la continuità di erogazione del Servizio. Trascorso tale termine senza che il Cliente abbia provveduto al pagamento di quanto dovuto, Aruba PEC si riserva la facoltà di sospendere, per quanto tecnicamente possibile, i Servizi interessati. In caso di mancato, parziale o ritardato pagamento dei corrispettivi pattuiti si applicano gli interessi di cui al D. Lgs. 231/2002.

5.3 A fronte di una espressa richiesta del Cliente, Aruba PEC potrà continuare ad erogare il Servizio/i, anche in assenza di un formale rinnovo del contratto per un periodo definito e condiviso per iscritto dalle parti. In tal caso il Cliente sarà tenuto al pagamento dei corrispettivi per tutto il periodo di effettiva erogazione del/i Servizio/i, intendendosi questo prorogato per il periodo di effettiva erogazione del/i Servizio/i, alle medesime condizioni previste nell'Offerta Economica, per il periodo concordato, fermo quanto previsto dal successivo art. 16. In caso di mancato, parziale o ritardato pagamento dei corrispettivi pattuiti si applicano gli interessi di cui al D. Lgs. 231/2002. Tale proroga può essere attivata per un massimo di due volte.

5.4 Ogni eventuale ritardo di Aruba PEC nell'emissione della fattura non può essere interpretato dal Cliente come acquiescenza o modifica alle pattuizioni disciplinate nel presente articolo.

6. Attivazione ed accettazione del Servizio

6.1 A seguito del perfezionamento del Contratto, se previsto per il Servizio, Aruba PEC consegna al Cliente le Credenziali di accesso al Pannello di gestione, mediante il quale il medesimo potrà chiedere il rilascio di Certificati ad Aruba PEC. Il Cliente prende atto ed accetta che il rilascio del Certificato è subordinato alla corretta compilazione, sottoscrizione e trasmissione della Modulistica per il Titolare e al compimento da parte del Cliente delle eventuali attività propedeutiche al rilascio del Certificato previste nel Manuale Operativo nonché al rispetto delle seguenti tempistiche:

- entro 90 giorni solari dalla ricezione del link per effettuare il riconoscimento, il Cliente dovrà completare correttamente la procedura di riconoscimento;
- effettuato positivamente il riconoscimento, entro i successivi 90 giorni solari il Cliente dovrà procedere all'attivazione del Certificato. L'attivazione costituisce conferma della correttezza dei dati contenuti nel certificato o nel sigillo ed accettazione dei medesimi.

Resta inteso che, qualora non venga rispettato anche solo uno dei due termini sopraindicati, il Certificato non sarà più utilizzabile. In tale ipotesi il Cliente, se del caso, dovrà acquistare un nuovo Dispositivo di Firma digitale senza poter avanzare alcuna pretesa nei confronti di Aruba Pec, anche a titolo di rimborso, per il Certificato divenuto non più utilizzabile.
Qualora il Cliente acquisti il certificato per terzi soggetti dal medesimo autorizzati, Titolari del Certificato, questi dovrà informare i medesimi delle condizioni ed obblighi applicati al Servizio, ivi inclusi quelli indicati sul Manuale applicabile.

6.2 Salvo quanto previsto dal successivo art. 6.3, la data di attivazione del Servizio corrisponde alla data di emissione del Certificato richiesto dal Cliente. Resta inteso che eventuali ritardi nell'attivazione del Servizio dovuti all'inerzia del Cliente e/o comunque alla mancata esecuzione di attività poste a suo carico (a titolo esemplificativo e non esaustivo, corretta compilazione, sottoscrizione e trasmissione della Modulistica per il Titolare del Servizio) non saranno imputabili ad Aruba PEC.

6.2.1 In parziale deroga a quanto previsto al comma che precede, il Cliente prende atto ed accetta che nel caso in cui sia applicabile il documento Policy di sicurezza per Soluzioni di firma in-house, come previsto nell'Allegato tecnico o nella Scheda Prodotto, l'attivazione del Servizio resta espressamene subordinata alla corretta compilazione della Dichiarazione di sussistenza dei requisiti da parte del Cliente nonché al positivo esito di tutte le verifiche condotte dalla Certification Authority, descritte nella Policy.

6.3 Il Cliente, entro 5 (cinque) giorni lavorativi dalla data di attivazione del Servizio, dovrà comunicare per iscritto ad Aruba PEC eventuali vizi e/o difformità relative al Servizio stesso; decorso il predetto termine senza che Aruba PEC abbia ricevuto tale comunicazione, il Servizio sarà considerato accettato.

6.4 All'approssimarsi della data di scadenza di ciascun Servizio, Aruba PEC a mero titolo di cortesia e quindi senza con ciò assumere alcuna obbligazione nei confronti del Cliente, si riserva di inviare avvisi di prossima scadenza dei Servizi.

6.5 Il Cliente, attraverso il Pannello di Gestione e così come meglio descritto nell'Allegato Tecnico o nella Scheda Prodotto, avrà accesso alla documentazione ed agli strumenti per consentire l'emissione di singole Firme Digitali a propri dipendenti o collaboratori. Nel caso in cui il Cliente svolga attività di C.D.R.L., e sottoscriva il relativo modulo ex art. 2.1 lett. 5), gli verrà attivato, unitamente al Pannello di Gestione, anche il CMS. Gli obblighi e le responsabilità legate al corretto utilizzo di tale pannello sono individuati nel Modulo di Adesione al contratto per lo svolgimento di attività inerenti il rilascio di servizi di certificazione digitale – C.D.R.L.

6.6 In parziale deroga a quanto previsto al precedente art. 6.2, il Cliente prende atto ed accetta che potrà procedere al riconoscimento dei Richiedenti, in qualità di datore di lavoro, ai sensi della modalità 6 del Manuale Operativo, solo dopo (i) essere stato nominato C.D.R.L. mediante la relativa modulistica (ii) aver accettato e debitamente sottoscritto il documento "Requisiti per riconoscimento con modalità 6 del MO".

6.7 Tutte le richieste del Cliente, ulteriori rispetto a quanto già attivato ed accettato, secondo le modalità descritte ai commi precedenti, saranno interpretate da Aruba PEC come RFC e quindi sottoposte ad una nuova e specifica Offerta.

6.8 Qualora, ai fini dell'attivazione del Servizio, siano necessarie attività in capo al Cliente, quali, a titolo esemplificativo e non esaustivo, l'invio di documentazione, l'esecuzione di specifiche configurazioni tecniche, la messa a disposizione di ambienti operativi, oppure qualsiasi altra attività propedeutica alla delivery del Servizio, il Cliente si impegna a completare tali attività entro un congruo termine indicato da Aruba PEC.

6.9 In caso di mancato adempimento da parte del Cliente entro il suddetto termine, Aruba PEC invierà un formale sollecito a mezzo PEC o in alternativa, a mezzo email, concedendo al Cliente un termine per adempiere non inferiore a 15 (quindici) giorni.
Decorso inutilmente anche tale termine, salvo in ogni caso il diritto di Aruba PEC di risolvere il Contratto ai sensi e per gli effetti dell'art. 1456 c.c., Aruba PEC sarà autorizzata ad addebitare al Cliente:
- i costi di attivazione sostenuti sino a quel momento;
- una penale pari all'1% (uno percento) del valore annuale del Contratto per ogni giorno di ritardo nell'adempimento da parte del Cliente.

7. Diritti e obblighi delle Parti e limitazioni di responsabilità di Aruba PEC

7.1 Il Cliente ha il diritto di utilizzare il Servizio conformemente a quanto previsto nel Contratto. Nel caso in cui il Cliente si avvalga di propri collaboratori e/o dipendenti e/o soggetti terzi nell'utilizzo del Servizio, Egli si assume di fronte ad Aruba PEC la piena responsabilità del loro operato come se detto operato fosse stato eseguito da esso medesimo.

7.1.1 Qualora il Cliente sia nominato CDRL di Aruba Pec ed assuma l'incarico di svolgere in nome e per conto di quest'ultima le attività finalizzate all'emissione di Certificati è tenuto al rispetto degli obblighi indicati nel Modulo di Adesione al contratto per lo svolgimento di attività inerenti il rilascio di servizi di certificazione digitale, nonché, in caso di riconoscimento eseguito ai sensi della modalità 6 del Manuale Operativo, del rispetto degli obblighi previsti dal documento "Requisiti per riconoscimento con modalità 6 del MO".

7.1.2 Qualora l'Allegato Tecnico o la Scheda Prodotto preveda l'applicazione del documento Policy di sicurezza per Soluzioni di firma in-house, il Cliente prende atto ed accetta di essere tenuto al rispetto di tutti gli obblighi indicati nel medesimo documento ed al mantenimento degli standard tecnici e organizzativi ivi descritti, come verificati dalla Certification Authority. Il mancato rispetto dell'Allegato Policy di sicurezza per Soluzioni di firma in-house costituisce grave inadempimento al presente contratto, ad ogni effetto.

7.2 Il Cliente è tenuto a: (i) provvedere al pagamento del corrispettivo con le modalità ed i termini indicati al precedente art. 5; (ii) utilizzare il Servizio nel rispetto del Contratto e della normativa di legge tempo per tempo vigente.

7.3 Salvo quanto previsto ai precedenti art. 6.4 e 7.1, il Cliente garantisce di essere l'unico ed esclusivo amministratore del Pannello di Gestione e/o del Pannello CSM e del Servizio e come tale di essere l'unico soggetto in possesso delle relative credenziali di accesso nonché unico responsabile: (i) a proprio rischio, della gestione di dati e/o informazioni e/o contenuti trattati ai fini del Contratto, della loro sicurezza e del loro salvataggio e del compimento di ogni altra attività ritenuta utile o necessaria a garantirne l'integrità, impegnandosi, per l'effetto, a fare applicazione, a sua cura e spese, di misure di sicurezza idonee ed adeguate; (ii) dei malfunzionamenti di ciascun Servizio per qualsiasi utilizzo non conforme al Contratto; (iii) dello smarrimento o della divulgazione delle credenziali di accesso o degli ulteriori codici ricevuti da Aruba PEC.

7.4 Il Cliente non potrà acquistare il Servizio per rivenderlo in favore di terzi estranei alla propria organizzazione. Il Servizio non è

liberamente rivendibile, nel caso in cui il Cliente voglia commercializzare il Servizio a terzi, diversi da propri dipendenti o collaboratori, dovrà sottoscrivere con Aruba PEC un separato contratto.

7.5 Aruba PEC garantisce al Cliente la fornitura del Servizio in conformità a quanto previsto dal Contratto, ed in particolare ai livelli di servizio previsti dalle presenti Condizioni generali e/o dalle Specifiche Tecniche e/o dall'Allegato SLA e Penali.

7.6 Gli obblighi e le responsabilità di Aruba PEC verso il Cliente sono quelli definiti dal Contratto, pertanto, in qualsiasi caso di violazione o inadempimento imputabile ad Aruba PEC, la stessa risponderà nei limiti previsti dal successivo art. 9 restando espressamente escluso, ora per allora, qualsiasi altro indennizzo o risarcimento al Cliente per danni diretti o indiretti di qualsiasi natura e specie.

7.7 Salvo diverso e specifico accordo scritto tra le Parti, resta esclusa qualsiasi responsabilità di Aruba PEC per l'uso fatto dal Cliente del Servizio in relazione a situazioni critiche che comportino, a titolo esemplificativo, rischi specifici per l'incolumità delle persone, danni ambientali, rischi specifici in relazione a servizi di trasporto di massa, alla gestione di impianti nucleari e chimici e di dispositivi medici.

7.8 Aruba PEC non assume alcuna responsabilità circa il contenuto dei dati e/o delle informazioni a qualsiasi titolo immessi e/o trattati e/o trasmessi tramite il Servizio.

7.9 Resta fermo che Aruba PEC non è responsabile per le attività svolte e/o per i servizi erogati da Soggetti Terzi incaricati direttamente dal Cliente, in riferimento alle prestazioni dei quali Aruba PEC rimane estranea.

8. Assistenza, rilevamento guasti e/o anomalie

8.1 L'assistenza tecnica è resa nei tempi e secondo le modalità indicate nell'Allegato Tecnico o nella Scheda Prodotto. Il Cliente è tenuto in ogni caso a comunicare tempestivamente ad Aruba PEC eventuali irregolarità o disfunzioni dal medesimo rilevate nei Servizi.
8.2 Guasti e/o anomalie del Servizio possono essere segnalati dal Cliente ad Aruba PEC secondo le modalità indicate nell'Allegato SLA e Penali entro 48 ore dal verificarsi del guasto a pena di decadenza del riconoscimento dei crediti descritti all'art. 9.
8.3 I detti crediti saranno presi in considerazione soltanto se confermati dalla struttura di monitoraggio di Aruba PEC. Tuttavia il Cliente, se dispone di un proprio servizio di monitoraggio, potrà misurare autonomamente gli eventuali disservizi. Nel caso in cui gli esiti dei rispettivi monitoraggi fossero discordanti, le Parti si impegnano a valutare congiuntamente le misurazioni.

8.4 Aruba PEC, in caso di Incident ed a fronte di una specifica richiesta del Cliente in tal senso, può mettere a disposizione Incident report redatto e gestito secondo gli standard e le policy delineate da ITIL.

9. Livelli di Servizio

9.1 I livelli di servizio garantiti per ciascun Servizio sono indicati nelle Specifiche Tecniche del relativo Servizio e nell'Allegato SLA e Penali. Aruba PEC farà ogni ragionevole sforzo per garantire la massima disponibilità dell'Infrastruttura e dei Servizi oggetto del Contratto.

9.2 Il mancato rispetto dei livelli di servizio di cui al comma precedente deve essere accertato in conformità a quanto previsto dall'Allegato SLA e Penali e costituisce disservizio per il quale, in base alla sua durata, è dovuto al Cliente, a titolo di indennizzo, qualora applicabile, il credito determinato secondo le modalità ed i criteri descritti all'interno del medesimo Allegato.

9.3 Gli indennizzi riconosciuti da Aruba PEC saranno gestiti sotto forma di rimborso o riduzione del dovuto sulla mensilità successiva qualora rimanente così come descritto nell'Allegato SLA e Penali.

10. Manutenzione

10.1 Sono possibili interventi di:
- manutenzione ordinaria, che Aruba PEC comunica al Cliente con un preavviso di 7 (sette) giorni;
- manutenzione straordinaria, che Aruba PEC comunica al Cliente con un preavviso di 48 (quarantotto) ore;
- emergenza, che Aruba PEC effettua tempestivamente e ne dà comunicazione al Cliente nel più breve tempo possibile.

10.2 In caso di interventi di manutenzione ordinaria e straordinaria – e, ove possibile, negli interventi di emergenza – la comunicazione al Cliente contiene gli eventuali periodi di interruzione del Servizio, i tempi di ripristino stimati e i possibili impatti.

10.3 Il Cliente è consapevole che durante gli interventi di manutenzione e di emergenza, i Servizi potrebbero subire una riduzione in termini di prestazioni, ridondanza o stabilità. Aruba PEC può suggerire al Cliente eventuali misure di mitigazione.

11. Sospensione dei Servizi

11.1 Fatta salva l'applicazione degli artt. 5, 10 e 12, Aruba PEC, senza che l'esercizio di tale facoltà possa essergli contestata come inadempimento o violazione del Contratto, si riserva la facoltà di sospendere i Servizi, anche senza alcun preavviso, nel caso in cui:

a) si verifichino casi di forza maggiore;
b) sia necessario procedere ad Interventi di Emergenza o relativi alla risoluzione di problemi di sicurezza, pericolo per l'intera rete e/o per persone o cose e salvo che tali interventi siano necessari a causa di inadempimenti di Aruba PEC;

Aruba PEC S.p.A.
VIA SAN CLEMENTE 53
24036 PONTE SAN PIETRO (BG)
Tel. +39 0575.0500 – FAX +39 0575.862020
enterprise.aruba.it

Capitale Sociale € 6.500.000,00 i.v.
REA: 445886
Codice Fiscale 01879020517
Partita IVA 01879020517

in tali casi, il Servizio sarà ripristinato quando Aruba PEC, a sua discrezione, abbia valutato che siano state effettivamente rimosse o eliminate le cause che avevano determinato la sua sospensione/interruzione;

11.2 Aruba PEC potrà sospendere il Servizio anche in caso di violazione da parte del Cliente degli obblighi posti a suo carico in base a quanto previsto dal Manuale Operativo e dalle presenti Condizioni generali, ivi compresi la Policy di sicurezza per Soluzioni di firma in-house, la Dichiarazione di sussistenza dei requisiti ed il documento "Requisiti per riconoscimento con modalità 6 del MO", se applicabili, dandone comunicazione al Cliente e fatta salva ogni eventuale azione di rivalsa nei riguardi del Cliente anche tramite la successiva risoluzione del Contratto.

11.3 In tutti i casi in cui si verifichi una sospensione del Servizio o una sua disattivazione prima della data di naturale scadenza, è obbligo del Cliente darne specifica e preventiva comunicazione ai Titolari, in caso essi siano soggetti diversi dal Cliente medesimo.

12. Risoluzione del Contratto

12.1 Senza pregiudizio per quanto previsto in altre clausole del Contratto, nel caso di violazione da parte del Cliente degli obblighi previsti agli Artt. 5, 7, 15 e 22 delle presenti Condizioni generali, nonché dai documenti dai medesimi richiamati, ivi compresi la Policy di sicurezza per Soluzioni di firma in-house, la Dichiarazione di sussistenza dei requisiti ed il documento "Requisiti per riconoscimento con modalità 6 del MO", Aruba PEC comunicherà al Cliente l'inadempimento diffidando il medesimo ad adempiere agli obblighi assunti entro un termine di 60 giorni dalla ricezione della stessa comunicazione. In caso di mancato adempimento da parte del Cliente entro i termini sopra indicati Aruba PEC potrà procedere alla risoluzione del rapporto contrattuale ai sensi dell'art. 1456 c.c. .

12.2 In relazione ai Servizi per i quali è indispensabile la nomina di Aruba PEC quale Responsabile del trattamento dei dati ai fini della corretta erogazione del Servizio, il contratto sarà da intendersi risolto di diritto nel caso di revoca da parte del Cliente di questa nomina. In tal caso il Cliente sarà comunque tenuto a pagare i corrispettivi previsti fino alla scadenza del Contratto a titolo di penale.

12.3 A far data dalla risoluzione del Contratto verificatasi nei casi previsti dal presente articolo, il Pannello di Gestione e/o il Pannello CMS viene disattivato. Aruba PEC avrà la facoltà di addebitare al Cliente ogni eventuale ulteriore onere che la stessa abbia dovuto sopportare, restando in ogni caso salvo il suo diritto al risarcimento degli eventuali danni subiti.

13. Cessazione del contratto

13.1 In tutte le ipotesi di cessazione del Contratto il/i Servizio/i sarà/anno disattivati e l'accesso al Pannello di Gestione e/o al Pannello CMS sarà/anno inibito/i senza ulteriore preavviso, eccezione fatta per i Certificati attivati in data antecedente a detta cessazione, i quali saranno erogati fino alla loro naturale data di scadenza. Le operazioni di cancellazione dei dati trattati da Aruba PEC in qualità di titolare del trattamento avverranno nel rispetto del Regolamento UE 2016/679, del Codice Privacy italiano (D. Lgs. 196/03) oltre che della normativa di settore vigente. Con specifico riferimento alle utenze di Firma Digitale, trascorso inutilmente il termine di 90 (novanta) giorni decorrenti dalla data di loro scadenza da considerarsi quale improrogabile ed essenziale, realizzandosi la condizione risolut iva apposta dette utenze saranno disattivate rendendo non più possibile da parte del Titolare la sottoscrizione di nuovi documenti con il Servizio restando esplicitamente esclusa, ora per allora, ogni e qualsiasi responsabilità da parte di Aruba PEC.

14. Aggiornamenti e variazioni

14.1 Il Cliente prende atto ed accetta che i Servizi oggetto del Contratto sono caratterizzati da tecnologia in continua evoluzione, per questi motivi Aruba PEC si riserva il diritto di modificare in meglio le specifiche tecnologiche degli stessi e degli strumenti ad essi correlati

14.4 In considerazione delle previsioni di cui al presente articolo il Cliente accetta espressamente che le pubblicazioni effettuate sul Pannello di gestione e/o sul Pannello CMS a cui egli ha accesso siano pienamente valide e rilevanti a tutti gli effetti di legge ai fini della conoscenza da parte sua di quanto ivi pubblicato.

15. Licenze e copyright

15.1 I software di Aruba PEC come qualsiasi altro diritto di autore o altro diritto di proprietà intellettuale sono di proprietà esclusiva di Aruba PEC e/o dei suoi danti causa, pertanto il Cliente non acquista nessun diritto o titolo al riguardo ed è autorizzato all'utilizzo degli stessi soltanto nel periodo di vigenza contrattuale.

15.2 Il Cliente dichiara di essere in regola con le eventuali licenze dei software necessarie per l'utilizzo del Servizio e di rispettare i relativiaccordi di licenza. Nel caso di software forniti da terze parti per il tramite di Aruba PEC, l'utilizzo degli stessi sarà regolato dai rispettivi accordi di licenza che il Cliente, ora per allora, dichiara di aver visionato ed accettato. Il Cliente si impegna altresì ad utilizzare detti software secondo le modalità indicate dai rispettivi licenziatari ed esclusivamente per uso proprio, con esclusione di qualsiasi responsabilità di Aruba PEC.

16. Revisione dei prezzi

16.1 Per la fornitura del Servizio Aruba PEC può acquistare da terze parti beni e servizi, quali a titolo esemplificativo e non esaustivo,

licenze software, i cui prezzi non sono controllati da Aruba PEC. Il Cliente accetta che i corrispettivi previsti dal presente Contratto potranno essere variati unilateralmente da Aruba PEC, in caso di aumenti dei costi applicati da terze parti che forniscono beni e/o servizi necessari per l'esecuzione del presente Contratto. La variazione sarà comunicata per iscritto al Cliente con un preavviso non inferiore a 30 giorni, tramite comunicazione a mezzo PEC/email o pubblicazione sul Pannello di Gestione, ove presente, specificando la motivazione dell'aumento.

16.2 Aruba PEC si riserva altresì il diritto di aggiornare i corrispettivi di cui al presente Contratto a propria discrezione previa comunicazione scritta al Cliente tramite PEC/email o pubblicazione sul Pannello di Gestione, ove presente, con un preavviso non inferiore a 30 giorni rispetto alla data di applicazione della variazione. Il Cliente che non intende accettare la variazione avrà la facoltà di recedere dal Contratto senza alcun onere o penalità entro il suddetto termine, mediante comunicazione scritta da inviare ad Aruba PEC all'indirizzo PEC recessi@aruba.pec.it. Il credito residuo presente eventualmente sul Pannello di Gestione verrà restituito da Aruba PEC al netto dei corrispettivi per i Servizi già erogati o in corso di erogazione alla data del recesso del Cliente. In caso di mancato recesso entro il suddetto termine, la modifica si intenderà accettata dal Cliente e diventerà efficace alla data indicata nella comunicazione di Aruba PEC.

17. Comunicazioni tra le Parti

17.1 Salvo sia diversamente previsto nelle presenti Condizioni generali, le comunicazioni di Aruba PEC al Cliente saranno inviate all'indirizzo dal medesimo riportato sul Modulo d'ordine ovvero, qualora indicati ai referenti dallo stesso riportati nel Modulo d'ordine secondo le competenze di seguito indicate:

- Referente amministrativo: l'interlocutore indicato dal Cliente per le comunicazioni/richieste amministrative e deputato a ricevere le fatture elettroniche;
- Referente tecnico: l'interlocutore indicato dal Cliente per le comunicazioni/richieste tecniche relative al Servizio;
- Responsabile del Contratto: interlocutore indicato dal Cliente per le richieste inerenti al Contratto diverse da quelle di competenza del referente tecnico e del referente amministrativo;
- Referente Privacy: interlocutore indicato dal Cliente per le comunicazioni/richieste inerenti al trattamento dei dati personali.

Salvo sia diversamente indicato nelle presenti Condizioni generali, le comunicazioni di Aruba PEC al Cliente saranno effettuate indistintamente a mano, tramite posta elettronica, certificata e non, a mezzo di lettera raccomandata A/R, oppure posta ordinaria. Eventuali variazioni degli indirizzi e dei recapiti del Cliente compreso l'indirizzo e-mail indicato nel Modulo d'ordine non comunicate ad Aruba PEC non saranno ad essa opponibili.

17.2 Salvo sia diversamente indicato nelle presenti condizioni, le comunicazioni del Cliente ad Aruba dovranno essere trasmesse al seguente indirizzo di posta elettronica certificata: arubapec@aruba.pec.it.

18. Sicurezza delle Informazioni e confidenzialità

18.1 Le Parti dovranno mantenere la più completa riservatezza, confidenzialità e segretezza su qualsiasi notizia, informazione, da to o documento di cui lo stesso verrà in possesso o di cui venga a conoscenza, o comunque abbia raccolto o trattato, nel corso dell'esecuzione del Contratto che, per normativa, natura o altra circostanza, sia da reputare coperto da riservatezza. Ai fini del Contratto sono "Informazioni Riservate" tutte le informazioni, in qualunque forma (cartacea, elettronica o verbale) che siano:

- Relative ad attività passate, presenti o future riguardanti l'impresa, la ricerca, lo sviluppo, le attività commerciali, le attività anche non a fine di lucro, i prodotti, i servizi, le conoscenze tecniche ed informatiche, i know-how e i segreti industriali, qualunque forma essi assumano, nonché le informazioni su clienti, i progetti e i piani di organizzazione degli stessi, i progetti commerciali, ivi incluse le informazioni rivelate o sviluppate per finalità di cui al Contratto;
- Identificate per iscritto come "riservate" ovvero che si possano ragionevolmente identificare o considerare come "riservate".

Non sono considerate riservate, indipendentemente dalla loro classificazione, le informazioni che siano o siano diventate in corso d'opera di dominio pubblico ed in nessun caso, potranno venire considerate riservate:

a) le informazioni che al momento della comunicazione siano di dominio pubblico o lo diventino successivamente, senza che la Parte che le ha ricevute abbia violato il presente Contratto;
b) le informazioni che al momento della comunicazione siano già conosciute legittimamente dalla Parte che le riceve, sempre che tale conoscenza non sia stata fraudolentemente ottenuta e la Parte possa darne prova;
c) le informazioni che al momento della comunicazione siano già conosciute dalla Parte che le riceve, essendole state precedentemente trasmesse da un terzo legittimato a farlo e non vincolato a un obbligo di riservatezza relativo all'utilizzazione o comunicazione di tali informazioni;
d) le informazioni elaborate da ciascuna delle Parti in modo del tutto indipendente;
e) le informazioni che la Parte sia obbligata a comunicare o divulgare in ottemperanza a un ordine legittimo di qualsiasi Autorità, 9 sempre che in tal caso la Parte che ha ricevuto l'ordine ne dia immediata notizia scritta alla Parte proprietaria delle Informazioni Riservate, affinché quest'ultima possa richiedere i più adeguati provvedimenti giudiziali a tutela dei propri interessi o altro idoneo rimedio, oppure svincolare l'altra Parte dall'obbligo di riservatezza;
f) le informazioni la cui divulgazione sia stata preventivamente autorizzata per iscritto dalla Parte che le ha trasmesse.

Ciascuna Parte si impegna a non utilizzare per scopi diversi da quelli individuati nel Contratto le informazioni coperte da riservatezza fornite dall'altra nello svolgimento delle attività oggetto del medesimo e di non divulgarle ai propri dipendenti e/o collaboratori se non per

adempiere esclusivamente alle finalità legate all'esecuzione del Contratto.

18.2 La Parte divulgante in ogni momento potrà richiedere alla Parte Ricevente la distruzione o la restituzione di qualsiasi documento, cartaceo o elettronico, contenente informazioni riservate e/o confidenziali in possesso della Parte Ricevente, ovvero di propri eventuali dipendenti, ausiliari e collaboratori, nonché dei propri eventuali subappaltatori o subcontraenti in genere e dei dipendenti, ausiliari e collaboratori di questi ultimi. La Parte Ricevente si impegna a provvedere alla cancellazione entro 5 (cinque) giorni dalla richiesta medesima.

18.3 Le Parti rispondono, con diretta assunzione di responsabilità, dei comportamenti in violazione di quanto previsto dal presente articolo assunti dai propri dipendenti e/o collaboratori e/o da eventuali terzi incaricati.

18.4 Ciascuna Parte prende atto che i suddetti obblighi di riservatezza saranno validi e vincolanti per tutta la durata del Contratto e per un periodo 2 (due) anni dalla data di cessazione, per qualsivoglia motivo, dello stesso.

18.5 In caso di violazione degli obblighi di cui al presente articolo, per ciascuna violazione la parte inadempiente sarà tenuta al versamento in favore dell'altra parte, di una penale pari al 2 % del corrispettivo su base mensile previsto nell'Offerta Economica.

19. Coperture assicurative

19.1 Aruba PEC ha stipulato e si impegna a mantenere attive durante la vigenza contrattuale le assicurazioni obbligatorie per legg e, nonché quelle RC/T e RC Professionale.

20. Legge applicabile e foro competente

20.1 Il Contratto è regolato esclusivamente dalla legge italiana restando esclusa qualsiasi applicazione della convenzione delle Nazioni Unite sulla vendita internazionale delle merci.

20.2 L'Autorità Giudiziaria italiana sarà giurisdizionalmente competente, in via esclusiva, a risolvere e decidere ogni e qualsiasi controversia relativa all'interpretazione e/o esecuzione e/o applicazione del Contratto.

20.3 Per ogni e qualsiasi controversia relativa all'interpretazione, esecuzione e risoluzione del presente Contratto sarà esclusivamente competente il Foro di Arezzo.

21. Trattamento dei dati personali

21.1 Il trattamento dei dati personali del Cliente e dallo stesso comunicati ad Aruba PEC ai fini della stipula del Contratto e della successiva erogazione del Servizio, avverrà in conformità al D.lgs. 196/2003, al Regolamento UE 2016/679 e all'informativa privacy disponibile al link https://www.pec.it/documents/tc-files/it/93_informativaprivacyarubapec.pdf.

21.2 Aruba PEC nelle fasi di raccolta, trattamento e gestione dei dati, necessarie ai fini dell'erogazione dei Servizi, si pone quali Titolare autonomi del trattamento in conformità alle definizioni dei ruoli descritte nel Regolamento UE 2016/679. Il Cliente garantisce, in riferimento ai dati di terzi da egli stesso trattati in fase di ordine e/o di utilizzo dei Servizi, di aver preventivamente fornito loro le informazioni di cui all'art. 13 Regolamento UE 2016/679 e di aver idonea base giuridica al trattamento.

21.3 Nel caso in cui il Cliente acquisti uno dei seguenti Servizi:

FIRMA REMOTA:
- ARSS Cloud as a service
- Dedicato in cloud

FIRMA AUTOMATICA ASB - R:

- as a service;
- installata ne cloud gestito dal Fornitore da Aruba

Aruba PEC, per esigenze correlate alla corretta esecuzione di tale Servizio, dovrà trattare dati personali di titolarità del Cliente, pertanto la stessa verrà nominata Responsabile del trattamento secondo le modalità definite nel Data Processing Agreement allegato.

22. Modello di Organizzazione, Gestione e Controllo

22.1 Il Cliente è a conoscenza che il Gruppo Aruba ha adottato un Modello di Organizzazione, Gestione e Controllo ex D.lgs. 231/01, con il relativo Codice Etico pubblicati alla seguente pagina web https://www.aruba.it/documents/tc-files/it/27_modello_231_aruba_spa.aspx
Il Cliente si impegna a rispettare i principi del Modello di organizzazione, gestione e controllo e a tutti i documenti dal medesimo richiamati e, in generale, ad astenersi da qualsivoglia comportamento atto a configurare le ipotesi di reato indicate nel D.lgs 231/01 e sue successive modifiche ed integrazioni.

Aruba PEC S.p.A.
VIA SAN CLEMENTE 53
24036 PONTE SAN PIETRO (BG)
Tel. +39 0575.0500 – FAX +39 0575.862020
enterprise.aruba.it

Capitale Sociale € 6.500.000,00 i.v.
REA: 445886
Codice Fiscale 01879020517
Partita IVA 01879020517

Il Cliente si impegna altresì a rispettare e a far rispettare ad eventuali suoi collaboratori, tutti gli obblighi e i principi contenuti nella suddetta documentazione. La violazione delle regole previste rappresenta grave inadempimento contrattuale, sulla base del quale Aruba PEC potrà risolvere il contratto ai sensi dell'art. 12 delle Condizioni generali.
Il Cliente si impegna a tenere indenne Aruba PEC da eventuali sanzioni o danni che dovessero derivare a quest'ultima quale conseguenza della violazione degli obblighi e dei principi derivanti dal presente articolo, previsti a carico del il Cliente o di suoi eventuali collaboratori.

23 Disposizioni finali

23.1 Il Contratto annulla e sostituisce ogni altro precedente accordo o intesa eventualmente intervenuta tra Aruba PEC e il Client e in ordine allo stesso oggetto. Nessuna modifica, postilla o clausola comunque aggiunta al Contratto sarà valida ed efficace tra le Parti, se non specificatamente ed espressamente approvata per iscritto da entrambe. In caso di accordi particolari con il Cliente questi dovranno essere formulati per iscritto e costituiranno addendum al Contratto. Resta fermo che Aruba PEC ed il Cliente sono soggetti autonomi e indipendenti e che il presente Contratto non stabilisce alcun rapporto di collaborazione o di agenzia tra Aruba PEC e il Cliente. Né Aruba PEC né il Cliente avranno il potere di impegnare l'altro o di assumere obblighi per conto dell'altro, senza il consenso scritto dell'altro.

23.2 In nessun caso eventuali inadempimenti e/o comportamenti del Cliente difformi rispetto al Contratto, potranno essere considerati quali deroghe al medesimo o tacita accettazione degli stessi, anche se non contestati da Aruba PEC. L'eventuale inerzia di Aruba PEC nell'esercitare o far valere un qualsiasi diritto o clausola del Contratto, non costituisce rinuncia a tali diritti o clausole.

23.3 L'eventuale inefficacia e/o invalidità, totale o parziale, di una o più clausole del Contratto non comporterà l'invalidità delle altre, le quali dovranno ritenersi pienamente valide ed efficaci.

23.4 È fatto divieto al Cliente di cedere il Contratto a terzi senza la previa autorizzazione scritta di Aruba PEC.

23.5 Aruba PEC avrà la facoltà di utilizzare il nome ed il marchio del Cliente sui propri siti web o in presentazioni pubbliche o riservate al solo scopo di referenza sul Servizio oggetto del Contratto, senza rivelarne ulteriori informazioni. Parimenti, sarà facoltà del Cliente dichiarare l'utilizzazione dell'Infrastruttura di Aruba PEC per il Servizio ai terzi.

23.6 Per quanto non espressamente previsto e disciplinato nel presente Contratto, le Parti rinviano alle norme del Codice civile e dell'ordinamento giuridico vigente in quanto applicabili.

Aruba PEC S.p.A.
VIA SAN CLEMENTE 53
24036 PONTE SAN PIETRO (BG)
Tel. +39 0575.0500 – FAX +39 0575.862020
enterprise.aruba.it

Capitale Sociale € 6.500.000,00 i.v.
REA: 445886
Codice Fiscale 01879020517
Partita IVA 01879020517

DPA – Data Processing Agreement

Nomina del Cliente 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 contrattuali stipulate tra Aruba PEC S.p.a. e il Cliente (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 Personali") trattati dal Cliente 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 Cliente assumerà pertanto il ruolo di Responsabile del trattamento.
Ai fini del presente DPA, il Titolare e il Cliente potranno essere riferiti collettivamente come "Parti".

Art. 2 - Modalità di trattamento dei dati personali

Art. 28 GDPR

Il Cliente tratterà i Dati Personali esclusivamente per dare esecuzione al Contratto, nei limiti e secondo le modalità di quanto disposto dallo stesso, dal presente DPA, dalla normativa in materia di protezione dei dati personali e nel rispetto degli obblighi di legge.
In relazione ai Dati, con particolare riguardo alle finalità e modalità del trattamento, il Cliente:

1. si atterrà alle istruzioni ricevute dal Titolare;
2. si impegna a collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;
3. si impegna a 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 del GDPR.

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 Cliente 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 Cliente	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, copia carta di identità.	Adempimenti relativi alla gestione dei servizi di cui al Contratto	dipendenti, collaboratori, clienti
Immagini/audio	Riprese audio/video delle registrazioni mediante il "Servizio Identificazione a Vista da Remoto (DVO)", qualora rientrante nell'ambito delle attività contrattuali	Adempimenti relativi alla gestione dei servizi di cui al Contratto	dipendenti, collaboratori, clienti

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

Art. 28 GDPR
La presente autorizzazione al trattamento dei Dati da parte del Cliente, che, per l'effetto, assume, la qualifica di 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 Cliente 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.

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** pec.it

L'esercizio del diritto di revoca da parte del Titolare – senza obbligo di corresponsione di alcun risarcimento e/o indennità al Cliente e fatto salvo quanto meglio specificato nel rapporto presupposto – avverrà mediante invio di una comunicazione contenente la manifestazione della volontà di revoca.

Art. 4 - Gestione degli Autorizzati

Il Cliente, anche in ottemperanza a quanto prescritto dall'art. 32 co. 4 del Regolamento, si impegna a:

a) consentire il trattamento dei Dati Personali unicamente agli Autorizzati che:
   i) per esperienza, capacità e formazione, risultano idonei ad assicurare il rispetto della normativa in materia di protezione dei dati personali;
   ii) siano stati nominati Autorizzati mediante nomina formale e per iscritto alle operazioni di trattamento dei Dati Personali e ai quali siano state impartite per iscritto dettagliate istruzioni operative circa gli obblighi a cui sono tenuti nel trattamento dei Dati Personali e, in particolare, circa le precauzioni da adottarsi per:
      1) garantire il trattamento dei Dati Personali in conformità col presente DPA e con la normativa in materia di protezione dei dati personali;
      2) evitare violazioni dei Dati Personali e mettere in atto le opportune attività da compiere in caso di violazione di dati personali;
      3) dare seguito alle eventuali richieste di esercizio dei diritti da parte degli Interessati;
   iii) siano stati vincolati per iscritto al dovere di riservatezza nel trattamento dei Dati Personali, qualora non siano già legalmente vincolati a tale dovere, e
   iv) siano assoggettati alla vigilanza sull'esatto adempimento delle istruzioni ricevute e degli obblighi cui sono sottoposti;
b) fare in modo che gli Autorizzati abbiano accesso esclusivamente ai Dati Personali che sono strettamente necessari per dare corretta esecuzione al Contratto o per adempiere ad obblighi di legge, in conformità col presente DPA e con la normativa in materia di protezione dei dati personali;
c) approntare misure di sicurezza adeguate, atte a far sì che:
   i) ciascun Autorizzato possa avere accesso esclusivamente ai Dati Personali che possono essere trattati in base al proprio profilo di autorizzazione, tenendo conto delle attività che devono compiere nell'esecuzione del Contratto;
   ii) eventuali trattamenti dei Dati Personali in violazione del Contratto e/o della normativa in materia di protezione dei dati personali siano prontamente identificate e notificate al Titolare, nel rispetto della tempistica di cui all'articolo 11;
   iii) al venir meno del Contratto o dell'incarico attribuito, ivi compresi i casi di cessazione del rapporto lavorativo o di collaborazione, l'Autorizzato cessi immediatamente i trattamenti dei Dati Personali e non conservi nella propria disponibilità nessuna copia dei Dati Personali in formato elettronico o cartaceo.

Art. 5 - Registro delle attività relative al trattamento

Art. 30 GDPR

Il Cliente si impegna a tenere un registro separato e aggiornato delle attività di trattamento dei Dati Personali svolte per conto del Titolare, così come disciplinato ai sensi dell'art. 30 co. 2 e 3 del GDPR, salvo che la tenuta del registro non risulti necessaria, come previsto ai sensi dell'art. 30 co. 5.

Il Cliente, su richiesta del Titolare, si impegna a fornire prontamente allo stesso copia del registro di cui sub 5.1.

Il Cliente si impegna altresì 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 dei dati personali (quali, a titolo esemplificativo e non esaustivo, il Registro delle attività di trattamento).

Art. 6 - Valutazione d'impatto

Art. 35 GDPR

Il Cliente si impegna ad assistere il Titolare nelle attività relative alle analisi del rischio dei trattamenti svolti per conto del Titolare e all'eventuale valutazione d'impatto di cui all'art. 35 del GDPR che dovesse rendersi necessaria in caso di trattamenti giudicati a rischio elevato per i diritti e le libertà degli interessati, segnalandone anche la necessità, per quanto di propria competenza, rispetto all'incarico svolto.

Art. 7 - Gestione degli Amministratori di sistema

Il Cliente si impegna, ove applicabile, al rispetto del Provvedimento emesso dal Garante per la protezione dei dati personali in data 27/11/2008 recante "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" e ad eventuali successivi aggiornamenti normativi.

Nei casi di cui il trattamento da parte del Cliente, derivante dal Contratto, implichi l'utilizzo di Amministratori di Sistema, il Cliente si impegna:

1. a 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;

2. a 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;
3. ad 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;
4. a 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;
5. con particolare riferimento con quanto specificato nel Contratto nel merito della soluzione proposta, a 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;
6. a 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;
7. in caso di malfunzionamento del sistema di loggatura, attivarsi per risolvere le problematiche tecniche eventualmente riscontate;
8. ad 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;
9. entro il 15 dicembre di ogni anno, a fornire al Titolare una relazione annuale relativa a quanto svolto in materia di ADS.

Art. 8 - Gestione dei Sub Responsabili

Art. 28 GDPR
Nell'esecuzione del Contratto, il Cliente 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 Cliente dichiara che alla data di sottoscrizione del presente DPA e del Contratto 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 responsabile	**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:

Con riguardo a tale elenco, è fatto obbligo al Cliente 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 Cliente 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 Cliente 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 Cliente 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 Cliente 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 Cliente che rimane unico e solo responsabile nei confronti del Titolare delle prestazioni da egli eventualmente affidate a terzi.
Il Cliente che affidi la fornitura dei Servizi a terzi, pertanto, sarà in ogni caso ritenuto responsabile 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 Cliente 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. 9 - Privacy by design

Art. 25 GDPR
Qualora il trattamento dei Dati da parte del Cliente avvenga per mezzo di proprio applicativi, il Cliente 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", in particolare, il software e gli interventi di manutenzione dello stesso dovranno prevedere:

a) ove necessaria, 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;
b) 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;
c) la configurazione di procedure di conservazione del dato personale e conseguente cancellazione o anonimizzazione del medesimo allo spirare del termine indicato dal Titolare;
d) ove necessaria, l'adeguata possibilità di gestione ed implementazione della manifestazione dei consensi al trattamento dei dati personali da parte dell'interessato nei confronti del Titolare, 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.

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. 10 - Misure di sicurezza tecniche e organizzative

Artt. 29 e 32 GDPR
Il Cliente garantisce il rispetto delle misure di sicurezza indicate dalla normativa in materia di protezione dei dati personali, dal presente DPA, 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 Cliente 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 Cliente 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 Cliente 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.
Il Cliente si impegna altresì:

1. a 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;

2. a 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;
3. ad adottare e rispettare le misure di sicurezza indicate dal Titolare nel presente DPA e altresì, individuare misure di sicurezza ulteriori a quelle già in uso, che dovesse ritenere necessarie per l'adeguato livello di protezione dei Dati;
4. a 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;
5. affinché sia sempre sotto monitoraggio un livello di rischio accettabile, ad 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 Cliente identificare e definire i rischi nonché stimarne le criticità sulla base delle tipologie dei Dati trattati in esecuzione del Contratto e delle peculiarità dei sistemi del Cliente;
6. a 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;
7. in attuazione delle strategie di cui sopra, a definire un piano di sicurezza informatico pluriennale atto a presidiare i Dati trattati in esecuzione del Contratto ed i propri sistemi, che tenga conto di misure organizzative (procedurali e documentali) e tecniche (sia fisiche che logiche);
8. a riesaminare e perfezionare periodicamente il piano di sicurezza informatica, 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;
9. a 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;
10. per misurare l'efficacia sul medio e lungo termine delle contromisure implementate a prevedere attività di monitoring a auditing con il precipuo fine di perfezionare o comunque migliorare tali contromisure;
11. a tenersi sempre aggiornato sulle novità che ineriscono la sicurezza informatica, e ciò sia in via autonoma che ricorrendo a terzi qualificati;
12. a promuovere iniziative volte a sensibilizzare il tema della sicurezza informatica all'interno della propria struttura;
13. a gestire e aggiornare un inventario degli asset hardware e software utilizzati per l'esecuzione del Contratto;
14. tenuto conto dei Dati e dei trattamenti effettuati in esecuzione del Contratto, a pianificare periodicamente vulnerability assessment e/o penetration test sui software e sui sistemi del Cliente utilizzati per l'esecuzione del Contratto, ivi comprensivi dei successivi piani di remediation;
15. al fine di gestire adeguatamente eventi, problemi e incidenti, a condurre regolarmente attività di monitoraggio sulla prestazione dei sistemi utilizzati per l'esecuzione del Contratto;
16. a 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;
17. a 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;
18. a garantire, 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 di cui al presente DPA, mediante specifici documenti riportanti le relative procedure di gestione e di accesso;
19. ad osservare scrupolosamente tutte le misure di sicurezza, tecniche e organizzative, predisposte dal Titolare a protezione dei Dati di cui al presente DPA.

Al Clienteè richiesta, in ogni caso, una condotta propositiva in tema di data protection, esplicantesi suggerimenti e /o proposte di modifica sulle misure adottate dal Titolare in adempimento al GDPR.

Art. 11 - Violazione dei Dati Personali

Artt. 28 e 33 GDPR

In caso di violazione dei Dati Personali (es. perdita, danneggiamento o distruzione dei Dati Personali in formato sia cartaceo che elettronico, accesso non autorizzato da parte di terze parti ai Dati Personali o qualsivoglia diversa violazione degli stessi) o delle informazioni trattate, conosciuta o anche solo sospettata (di seguito "Evento"), ivi comprese le violazioni occorse quale conseguenza della condotta di eventuali Sub Responsabili del Cliente e/o dei suoi Autorizzati, il Cliente dovrà:

a) informare il Titolare immediatamente, e comunque entro e non oltre 4 (quattro) ore dal momento in cui ne è venuto a conoscenza, inviando una comunicazione via e-mail all'indirizzo: dpo@staff.aruba.it. 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 Personali e delle informazioni coinvolte nonché la loro natura, con indicazione della loro ubicazione. Qualora già conosciute, nello stesso termine il Cliente 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 Cliente si attiverà per fornire un riscontro al Titolare entro 8 (otto) ore dalla prima comunicazione, precisandole una volta apprese.
In ogni caso, il Cliente assicura la massima collaborazione per approfondire tutti gli aspetti necessari ed utili per precisare l'Evento. Una volta definite le ragioni dell'Evento il Cliente, 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 atte ad arginare il verificarsi di un nuovo evento della stessa specie di quella verificatasi.

b) con il placet del Titolare riguardo alle modalità, adottare immediatamente, e comunque senza ingiustificato ritardo, ogni necessaria misura atta a minimizzare i rischi di qualsivoglia natura per gli Interessati derivanti dalla violazione dei Dati Personali, al fine di porvi rimedio e/o attenuarne i possibili effetti negativi;
c) collaborare con il Titolare al fine di identificare e implementare le misure tecniche e organizzative adeguate a prevenire violazioni simili in futuro.

Ai fini del presente DPA, il Cliente dichiara e garantisce che la propria struttura e i propri eventuali Sub Responsabili hanno adottato misure tecniche e organizzative:

a) in grado di identificare prontamente eventuali violazioni dei Dati Personali, di fornire le informazioni e di compiere ogni attività utile e necessaria a minimizzare l'accadimento e/o gli effetti di qualsivoglia violazione dei Dati Personali;
b) tali da rendere improbabile che un'eventuale violazione dei Dati Personali presenti un rischio per i diritti e le libertà dei relativi interessati, anche tramite l'utilizzo di tecnologie, quali la cifratura, che rendano incomprensibili i Dati Personali a chiunque non sia autorizzato ad accedervi.

Ai fini del presente DPA, il Cliente si impegna a redigere e mantenere aggiornato un Registro delle violazioni dei dati personali e fornire una copia dello stesso su richiesta da parte del Titolare, al fine di poter dimostrare al Titolare di essere in grado di rilevare e identificare attraverso i propri sistemi qualunque evento.

Art. 12 - Diritti degli Interessati e richieste da parte delle Autorità

Il Cliente si impegna:

a) in caso di esercizio da parte dell'Interessato dei diritti di cui agli artt. da 15 a 22 GDPR, ad 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.
b) in caso di ricezione di richieste specifiche avanzate dall'Autorità Nazionale per la protezione dei dati personali o altre autorità, a coadiuvare il Titolare per consentire a quest'ultimo di rispondere alle suddette richieste, per quanto di sua competenza.

Art. 13 - Cancellazione dei dati

Art. 28 GDPR
Il Cliente, 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.
In ogni caso, alla scadenza del Contratto od alla data di cessazione dei suoi effetti a qualunque titolo intervenuta, nonché in ogni caso di richiesta del Titolare, il Cliente 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. 14 - Trasferimento di dati personali verso paesi terzi

Art. 44 GDPR
I Dati trattati dal Cliente per l'erogazione dei Servizi oggetto del Contratto, di cui al presente DPA, sono ubicati nel territorio dell'Unione Europea, in ITALIA.
Il Cliente non potrà trasferire i Dati Personali al di fuori del territorio dell'Unione Europea, senza il previo consenso scritto del Titolare, fermo restando che – anche qualora detto consenso fosse prestato – Il Cliente dovrà attenersi strettamente alle indicazioni impartite dal Titolare per effettuare il trasferimento.

Art. 15 - 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 Cliente è il Responsabile della sicurezza.

Art. 16 - Audit

Art. 28, co. 3 lett. h GDPR
Il Cliente 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 Cliente riconosce al Titolare il diritto di verificare il rispetto da parte del Cliente dei propri obblighi di sicurezza imposti a protezione dei Dati Personali attraverso l'effettuazione di audit ("Audit"), ove ritenuto necessario e/o opportuno a insindacabile scelta del Titolare, senza corrispettivo ulteriore rispetto a quanto pattuito nel Contratto.
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 dalla stessa incaricati.
Il Cliente si rende disponibile sin da ora ad offrire la massima collaborazione in modo da permettere al Titolare di svolgere efficacemente gli Audit.
Nel corso degli Audit, il Titolare avrà diritto di accedere direttamente, e/o tramite soggetti appositamente incaricati, ai locali e/o ai sistemi del Cliente e 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 Cliente che dovesse emergere nel corso delle attività di Audit rispetto agli obblighi previsti dalla normativa in materia di protezione dei dati personali e dal presente DPA, dovrà essere risolta dal Cliente, a proprie spese, e comunque in un lasso di tempo non superiore a una settimana 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 del Titolare a pretendere il risarcimento dei danni eventualmente subiti in conseguenza dei suddetti difetti di conformità. Qualora, entro il termine sopra stabilito, il Cliente 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.
Il Cliente si impegna a riportare le clausole del presente articolo nei contratti stipulati con i propri fornitori che rivestiranno la qualifica di Sub Responsabili del Titolare.
Con riferimento al punto precedente il Titolare potrà richiedere al Cliente di effettuare, a proprie spese, audit verso i propri fornitori (Sub Responsabili del Cliente) con la stessa frequenza e con le stesse modalità riportate nel presente articolo.

Art. 17 - Durata

La presente nomina Responsabile del trattamento del Cliente e le clausole del presente DPA hanno durata pari a quella del Contratto intercorso tra il Cliente e il Titolare.
La nomina ed il presente atto cesseranno automaticamente di avere efficacia in ipotesi di risoluzione, recesso o perdita di efficacia del Contratto, salvo il tempo eventualmente necessario a consentire al Titolare di recuperare i Dati, come contrattualmente convenuto tra le Parti nel presente DPA.
Parimenti, in caso di tacito rinnovo del Contratto la nomina a Responsabile del trattamento del Cliente ed il presente DPA si considererà automaticamente rinnovato per durata pari a quella contrattuale.

Art. 18 - Rinvio

Per quanto non espressamente previsto e disciplinato nel presente DPA, le Parti rinviano al Contratto, 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.

Allegato 1

DESCRIZIONE DELLE MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Organizzativo	Alto livello	Policy e Disciplinari	Il Cliente 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 Cliente 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 Cliente 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 Cliente 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 Cliente 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 del Cliente 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 Cliente 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 Cliente 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 Cliente 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 Cliente 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 necessità 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.

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** pec.it

Tecnico	Alto livello	Strong Authentication	Per quanto di competenza del Cliente, 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 Cliente 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 differenziati 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.

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** pec.it

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 alfanumerici (dodici in caso di amministratore di sistema), almeno una lettera maiuscola, almeno una lettera minuscole e almeno un carattere speciale. 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 tali intervalli devono essere indicati nel Documento di sicurezza. Le password degli amministratori di sistema devono contenere almeno dodici Documento di sicurezza.
Tecnico	Autorizzazione, identificazione, autenticazione	Gestione dell'identità e degli accessi	Ove applicabile, per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte). L'autenticazione a due fattori (autenticazione forte) deve preferibilmente essere implementata per accedere ai sistemi che elaborano i dati. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.
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.

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** pec.it

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 del Titolare	A ciascun collaboratore autorizzato del Cliente 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 del Titolare	Il Cliente dovrà comunicare senza alcun indugio ogni variazione all'elenco delle persone autorizzate in modo che il Titolare 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 del Titolare 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 del Titolare in modo che sia possibile disattivare la VPN e generare dei nuovi seed per l'OTP. Essendo la VPN nominale se ne vieta la condivisione delle credenziali con soggetti terzi seppur autorizzati. Durante la sessione VPN il collaboratore non dovrà lasciare incustodito 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 il Titolare.
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.

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** pec.it

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: • L'etichettatura di ciascun documento con il livello di riservatezza "Riservato" • La stampa in modalità protetta da password o simili accorgimenti per assicurarsi che solo l'autorizzato possa accedere al documento appena prodotto • 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 • la distruzione, ove necessario, tramite apposita macchina distruggi documenti prima dello smaltimento • 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. • 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 (256 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 256 bit, come avviene ad esempio per i sistemi AES-256

Tecnico	Trasmissione di Dati	Protocolli sicuri e crittografia in transito	I protocolli su cui viaggeranno i Dati dovranno essere sicuri (HTTPS) e i Dati in transito dovranno essere crittografati secondo I migliori standard di settore (non inferiore a TLS 1.2).
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 Cliente 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 Cliente 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 Cliente 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 email 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 Cliente è il Responsabile della sicurezza.

Scheda INCARICATI AL RICONOSCIMENTO - I.R.

N. 1	N. 7
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale
Rapporto con il C.D.R.L.	Rapporto con il C.D.R.L.
N. 2	**N. 8**
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale
Rapporto con il C.D.R.L.	Rapporto con il C.D.R.L.
N. 3	**N.9**
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale
Rapporto con il C.D.R.L.	Rapporto con il C.D.R.L.
N. 4	**N. 10**
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale
Rapporto con il C.D.R.L.	Rapporto con il C.D.R.L.
N. 5	**N. 11**
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale
Rapporto con il C.D.R.L.	Rapporto con il C.D.R.L.

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

N. 6	N. 12
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale
Rapporto con il C.D.R.L.	Rapporto con il C.D.R.L.

Documentazione da utilizzare per la nomina di Incaricati al Riconoscimento - IR:

- lettera di nomina ad Incaricato al Riconoscimento - Persona Fisica;

Il C.D.R.L., come identificato nel "Modulo di Adesione al contratto per lo svolgimento di attività inerenti il rilascio di servizi di certificazione digitale C.D.R.L. – Enterprise v 1.0"

Luogo _____ **Data** _____ **Firma e timbro** _____

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

Dichiarazione di accettazione delle clausole vessatorie

Il sottoscritto, come identificato nel "Modulo di Adesione al contratto per lo svolgimento di attività inerenti il rilascio di servizi di certificazione digitale C.D.R.L. – Enterprise" e munito, come da visura camerale aggiornata allegata**,** dei necessari poteri per impegnare il CDRL ivi menzionato nei termini di cui al presente documento

DICHIARA

di aver preso chiara ed esatta visione e di approvare espressamente ed in modo specifico, ai sensi e per gli effetti degli art. 1341 e 1342 c.c., le seguenti clausole delle "**Condizioni Generali di contratto per lo svolgimento di attività inerenti il rilascio di servizi di certificazione digitale**" allegate al predetto Modulo di Adesione: 3) Conclusione del Contratto 4) Obblighi e responsabilità del Cliente; 6) Clausola risolutiva espressa; 7) Cessazione del Contratto e revoca dei certificati; 8) Risarcimento danni.

Luogo _____ **Data** _____ **Firma e timbro** _____

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

Scheda OPERATORI DELLA REGISTRAZIONE - O.D.R.

N. 1	N. 7
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale
N. 2	**N. 8**
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale
Rapporto con il C.D.R.L.	Rapporto con il C.D.R.L.
N. 3	**N.9**
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale
Rapporto con il C.D.R.L.	Rapporto con il C.D.R.L.
N. 4	**N. 10**
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale
Rapporto con il C.D.R.L.	Rapporto con il C.D.R.L.
N. 5	**N. 11**
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

Rapporto con il C.D.R.L.	Rapporto con il C.D.R.L.
N. 6	**N. 12**
Nome	Nome
Cognome	Cognome
Data di Nascita	Data di Nascita
Luogo di Nascita	Luogo di Nascita
Codice Fiscale	Codice Fiscale
Rapporto con il C.D.R.L.	Rapporto con il C.D.R.L.

Documentazione da utilizzare per la nomina di Operatore di Registrazione - ODR:

- lettera di nomina ad Operatore di Registrazione (documento 1).

Il C.D.R.L., come identificato nel "Modulo di Adesione al contratto per lo svolgimento di attività inerenti il rilascio di servizi di certificazione digitale C.D.R.L. – Enterprise v. 1.0"

Luogo _____ **Data** _____ **Firma e timbro** _____

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

Modulo di Adesione al contratto per lo svolgimento di attività inerenti il rilascio di servizi di certificazione digitale C.D.R.L. – Enterprise

Il/La Sottoscritto/a _____

Codice fiscale _____

Documento identità (**da allegare**): ☐ Carta d'Identità ☐ Patente di Guida ☐ Passaporto Numero

nella Sua qualità di Legale Rappresentante/Dirigente Responsabile, della Società/Ente (di seguito C.D.R.L. o CDRL)

_____ P. Iva. _____,

Con Sede Legale in _____ Pr. (_____) Cap._____,

in Via/Piazza _____ N. _____ come sopra identificato ed individuato, nella consapevolezza che chiunque rilascia dichiarazioni mendaci è punito ai sensi del codice penale e delle leggi speciali in materia, ai sensi e per gli effetti di cui all'art. 46 D.P.R. n. 445/2000, dichiara di essere munito dei poteri necessari al compimento del presente atto, con il presente modulo di adesione compilato in ogni sua parte,

DICHIARA

di voler eseguire, per conto di Aruba PEC (in qualità di Certification Authority), le attività di identificazione e di registrazione dei Richiedenti di certificati qualificati commercializzati dal Partner di Aruba Pec, secondo le modalità specificate nelle Condizioni allegate al presente Modulo di Adesione, nel Manuale Operativo (pubblicato alla pagina web http://www.pec.it/DocumentazioneFirmaDigitale.aspx) che con la sottoscrizione del presente modulo, dichiara di conoscere ed accettare integralmente nel loro contenuto, e di essere nominata, per effetto di ciò, Centro di Registrazione Locale di Aruba Pec S.p.A.
In considerazione di quanto sopra dichiarato ed accettato,

INDICA

Nella Scheda, allegata al presente Modulo, i dati di coloro che sono nominati quali *(barrare solo la voce che interessa)*:

☐ **Operatore di Registrazione – O.D.R.** ☐ **Incaricato al Riconoscimento - I.R.**

COMUNICA

di seguito i dati del/i Responsabile/i della gestione dei rapporti:

Nome:	Cognome:
Telefono e fax:	Indirizzo E-Mail:

DICHIARA

a) di impegnarsi ad osservare quanto stabilito Condizioni Generali allegate al presente Modulo;
b) che i dati forniti ai fini della conclusione ed esecuzione del presente Contratto, sono esatti e veritieri;
c) di accettare la nomina a **Responsabile del Trattamento dei Dati Personali**, nei termini indicati nelle Condizioni Generali e, a tal fine, di essere in possesso dei requisiti di esperienza, capacità ed affidabilità, previsti dalla legge, tali da fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza.

Luogo _____ **Data** _____ **Firma e timbro** _____

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

Condizioni generali di contratto per lo svolgimento di attività inerenti il rilascio di servizi di certificazione digitale

Indice degli articoli

1. Definizioni

Ai fini del presente accordo si intende per:

Addetti: i soggetti, persone fisiche, titolari di un rapporto contrattuale definito con il CDRL o altra società ad esso collegata, che a vario titolo sono coinvolti nella esecuzione delle attività poste dal presente Contratto a carico del CDRL (in via meramente esemplificativa ODR, IR, dipendenti, collaboratori o consulenti del CDRL).

Agenzia per l'Italia Digitale: ente pubblico non economico, con competenza nel settore delle tecnologie dell'informazione e della comunicazione nell'ambito della pubblica amministrazione;

Carta Nazionale dei Servizi: strumento principale per l'accesso ai dati detenuti dalle Pubbliche Amministrazioni e quindi non solo ai dati di dominio pubblico ma anche a tutto ciò che riguarda le informazioni personali del cittadino, quali a titolo esemplificativo dati fiscali, previdenziali, sanitari (di seguito C.N.S.);

Centro Di Registrazione Locale: il soggetto pubblico o privato che, mediante la conclusione del presente contratto con Aruba Pec, è nominato da questa quale Centro di Registrazione Locale per lo svolgimento delle attività inerenti il rilascio di servizi di certificazione digitale (di seguito, C.D.R.L.);

Certification Authority: Aruba Pec quale soggetto che esegue la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati;

Certificato: una rappresentazione digitale di dati informatici che deve contenere i dati identificativi del Certificatore e del richiedente/sottoscrittore del certificato, la Chiave pubblica del sottoscrittore, un numero seriale identificativo, la firma digitale del Certificatore e deve identificare il periodo di validità del certificato;

Chiave Privata: componente della coppia di chiavi asimmetriche, destinato ad essere noto esclusivamente al soggetto che ne è titolare (Utente), mediante il quale quest'ultimo appone la Firma digitale su un documento informatico oppure decifra un documento informatico in precedenza cifrato mediante la corrispondente Chiave Pubblica;

Chiave pubblica: componente della coppia di chiavi asimmetriche destinato ad essere reso pubblico, mediante il quale si verifica la Firma digitale apposta sul documento informatico del titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi;

Condizioni: le Condizioni generali di contratto Enterprise Aruba Pec;

Contratto: l'accordo, comprensivo di tutti i documenti che ne fanno parte ai sensi dell'art. 2 delle Condizioni di Fornitura del Servizio di Firma Digitale Enterprise;

Modulistica Titolare – Servizio di Certificazione: le Condizioni di Erogazione Servizi di Certificazione complete dei relativi allegati come ivi menzionati.

Documentazione Titolare: è la documentazione che disciplina le modalità di richiesta e di utilizzo del Kit di firma digitale da parte del Richiedente/Titolare e che deve essere compilata, sottoscritta ed accettata da quest'ultimo. Tale documentazione è costituita dal Modulo di Richiesta Firma Digitale, di seguito "Modulo"(ossia il modulo utilizzato dal Richiedente il certificato e nel quale Egli deve indicare i dati diretti e necessari a consentire la sua identificazione e ad individuare il Certificato di suo interesse) e dalle Condizioni Generali di Contratto - Firma Digitale (ossia le condizioni che disciplinano l'emissione della Firma Digitale ed il suo utilizzo da parte del Titolare), allegate alle presenti Condizioni Generali di Contratto;

Data Processing Agreement (DPA): l'accordo, redatto da Aruba PEC in osservanza della disciplina prevista dal Regolamento UE 2016/679 e dalla normativa di settore vigente, avente ad oggetto le modalità e le condizioni di trattamento dei dati personali.

Firma automatica: particolare procedura informatica di firma elettronica qualificata eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo;

Firma digitale remota: particolare tipo di firma digitale, generata su HSM sotto il pieno controllo di Aruba Pec, che garantisce al C.D.R.L. un controllo esclusivo sulle chiavi private;

Firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al C.D.R.L. tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

HSM: insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche;

Incaricato al Riconoscimento: se presente in ragione della modalità di riconoscimento adottata, il soggetto pubblico o privato che, mediante la conclusione del presente contratto con Aruba Pec, o mediante nomina diretta da parte del C.D.R.L., è nominato quale Incaricato al Riconoscimento per lo svolgimento delle attività inerenti il rilascio di servizi si certificazione digitale (di seguito, I.R.);

Informativa privacy: il documento pubblicato alla pagina https://www.pec.it/documents/tc-files/it/93_informativaprivacyarubapec.pdf che descrive le modalità di trattamento dei dati personali dei Clienti Aruba PEC.

Kit di firma digitale: il kit distribuito da Aruba Pec descritto in dettaglio nel Manuale Operativo ed avente ad oggetto l'emissione in favore del Richiedente di uno o più Certificati di Firma Digitale, in base alla tipologia di kit dal medesimo scelta tra quelle messe a sua disposizione, conforme a quanto previsto nel D.P.R. 445/2000, nel D.P.C.M. 13 gennaio 2004 e successive modifiche ed integrazioni;

Lettera di nomina: la lettera mediante la quale il C.D.R.L. nomina i soggetti (O.D.R. e I.R., ove previsto) a cui saranno assegnate le attività oggetto di Contratto;

Modulo di Adesione: il modulo generato da Aruba Pec che deve essere debitamente compilato e sottoscritto dal C.D.R.L. e restituito ad Aruba Pec, tramite fax o servizio postale, quale documento finalizzato alla conclusione del presente Contratto;

Operatore di Registrazione: se presente in ragione della modalità di riconoscimento adottata, il soggetto incaricato dal C.D.R.L. che, nel rispetto delle istruzioni impartite dal Certificatore, è preposto allo svolgimento delle attività inerenti il rilascio di servizi di certificazione digitale oggetto del contratto (di seguito, O.D.R.);

Partner: la persona, fisica o giuridica, che offre il Servizio al Titolare in forza di autonomo e specifico contratto concluso con Aruba Pec.

Richiedente/Titolare: il soggetto che, in qualità di Titolare, richiede la fornitura del kit di Firma Digitale al Partner;

Requisiti per riconoscimento con modalità 6 del MO: il documento redatto da Aruba PEC, ed applicabile al C.D.R.L. che definisce i requisiti organizzativi e di sicurezza che il C.D.R.L., in qualità di datore di lavoro, deve soddisfare per poter procedere all'identificazione del Richiedente ai sensi della modalità 6 del Manuale Operativo.

Responsabile di Processo: se presente, in relazione alla modalità di riconoscimento ai sensi della normativa Antiriciclaggio, il soggetto indicato dal C.D.R.L. che attesta la corretta trasmissione al Certificatore dei dati del Richiedente, come identificato ai sensi della vigente normativa Antiriciclaggio.

T.U.: Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa approvato con il D.P.R. 28 dicembre 2000 n. 445.

Terzo Interessato: soggetto che, in caso di rilascio di Certificati per firmare in funzione di un ruolo o di cariche rivestite per conto di organizzazioni terze che prevedono il conferimento di poteri, da parte di terzi, a colui che richiede il Certificato, unitamente al Titolare, avendo un interesse diretto nella gestione del Certificato, è legittimato alla revoca e/o sospensione del Certificato.

2. Oggetto del Contratto

2.1 Oggetto del Contratto è il conferimento, a titolo non esclusivo, mediante la nomina quale C.D.R.L., da parte di Aruba Pec dell'incarico di svolgere in nome e per conto di quest'ultima le attività finalizzate all'emissione di Certificati Digitali, commercializzati dal Partner. A tal fine, il Partner fornirà la documentazione da far firmare ai Richiedenti ed Aruba Pec emetterà il certificato nonché i beni e i materiali da consegnare a questi ultimi, previo pagamento del relativo prezzo indicato nell'Offerta.

3. Conclusione del Contratto

3.1 Il Contratto si considera concluso, efficace e vincolante tra le Parti dalla data del ricevimento da parte di Aruba Pec del Modulo di Adesione, correttamente compilato e debitamente sottoscritto.

3.2. Il C.D.R.L. prende atto ed accetta che potrà procedere al riconoscimento dei Richiedenti, in qualità di datore di lavoro, ai sensi della modalità 6 del Manuale Operativo, solo dopo (i) essere stato nominato C.D.R.L. mediante la relativa modulistica (ii) aver accettato e debitamente sottoscritto il documento "Requisiti per riconoscimento con modalità 6 del MO". Il C.D.R.L. prende atto che tale modalità di riconoscimento non comporta l'attivazione del CMS né la nomina di IR o ODR.

4. Obblighi e responsabilità

4.1 Il C.D.R.L. dichiara di essere a conoscenza dell'importanza che la funzione di identificazione ed autenticazione assume nell'ambito del Servizio di Certificazione di Aruba Pec, ed in genere, ai fini della normativa sulla Firma Digitale che consente di sottoscrivere elettronicamente atti e documenti rilevanti agli effetti di legge e di ricondurli univocamente alla persona che li ha sottoscritti. Il C.D.R.L., con la sottoscrizione, del presente Contratto, assume l'obbligo di svolgere, in nome e per conto del Certificatore ed ai fini dell'emissione di Certificati Digitali e delle C.N.S., le attività indicate nelle presenti Condizioni Generali di Contratto e, altresì, si obbliga nei confronti del Certificatore a:

a) adempiere agli obblighi derivanti dal presente Contratto nel rispetto della normativa vigente, e con la massima diligenza professionale ed impegno, con particolare riferimento all'identificazione certa di coloro che richiedono l'emissione di Certificati e delle C.N.S.;
b) nominare ed indicare per iscritto contestualmente alla conclusione del Contratto, uno o più soggetti (di seguito, addetti) che si occuperanno dello svolgimento delle attività indicate in Contratto, relativamente ai prodotti ed ai servizi commercializzati dal Partner, i quali assumeranno la qualifica e le relative competenze indicate nel prosieguo. I nominativi degli addetti di cui sopra e tutti i dati necessari ai fini della loro identificazione (data di nascita, residenza, codice fiscale, eventuali recapiti telefonici, indirizzo e-mail, tipo di rapporto intercorrente con essi) dovranno essere comunicati per iscritto ad Aruba Pec, contestualmente alla conclusione del Contratto, mediante l'apposita scheda allegata al Modulo di Adesione, che ne costituisce parte integrante ed essenziale;
c) svolgere in nome e per conto del Certificatore, mediante gli addetti come sopra nominati, l'attività di raccolta delle richieste per l'emissione di Certificati per Firma Digitale, di registrazione, identificazione ed autenticazione dell'identità del richiedente, di trasmissione della richiesta al Certificatore e di consegna al Richiedente del dispositivo di firma (Smart-Card) sul quale dovrà essere generata la chiave privata del Certificato. Nel caso in cui il C.D.R.L. svolga operazioni di rilascio di certificati o della C.N.S., gli addetti nominati provvedono alle operazioni di comunicazione verso il Certificatore, al fine di consentire l'emissione del Certificato idoneo, in conformità a quanto previsto per legge;
d) informare compiutamente e per iscritto i propri addetti dei compiti loro assegnati e delle responsabilità assunte dai medesimi nello svolgimento delle loro attività e far sottoscrivere loro l'apposito documento di accettazione della nomina, predisposto da Aruba Pec (Lettera di Nomina);
e) vigilare e, quindi, garantire il corretto operato dei propri addetti, affinché le attività oggetto del presente Contratto, siano da essi svolte personalmente, con la massima cura e diligenza e nel pieno rispetto di quanto in esso stabilito, ed a porre in essere senza indugio ogni rimedio che si renda opportuno e/o necessario in caso di non corretto adempimento dei propri obblighi da parte degli addetti;
f) impedire ai propri addetti la prosecuzione delle attività che sono state loro assegnate qualora, per qualsiasi causa, si sia interrotto il rapporto in essere con il C.D.R.L.. In tali casi, quest'ultimo dovrà prontamente informare Aruba Pec per iscritto, mediante raccomandata a.r. o posta elettronica certificata all'indirizzo direzione.ca@arubapec.it dell'accaduto e dei provvedimenti adottati indicando, altresì, i nominativi degli addetti nei cui confronti essi sono stati presi;
g) comunicare per iscritto al Certificatore ogni eventuale modifica delle informazioni o dei dati forniti a norma del presente Contratto, tempestivamente e comunque non oltre 7 (sette) giorni dalla data in cui tali modifiche sono divenute note al C.D.R.L.;
h) informare il Richiedente sulle modalità di utilizzo della firma digitale, della CNS, con particolare riferimento alle modalità di revoca, sospensione e rinnovo dei certificati digitali, nonché sugli aspetti normativi e sulle conseguenze giuridiche derivanti dall'utilizzo di detti strumenti;

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

i) conservare e custodire le buste sigillate contenenti i codici segreti di emergenza e i dispositivi di firma in modo da evitare che possa esserne violata l'integrità, rispondendo direttamente della loro sottrazione, perdita o deterioramento a qualsiasi causa dovuti;
j) non utilizzare e non trattare, in violazione delle prescrizioni contenute nel D.lgs. 196/2003 e nel Regolamento UE 2016/679, i dati personali acquisiti in forza dell'esecuzione del presente Contratto.

4.1.1 Gli obblighi di cui alle lettere b), c), d) e) f) del precedente articolo 4.1 non trovano applicazione nelle ipotesi in cui l'attività di identificazione sia eseguita da un Intermediario finanziario o altro Soggetto Esercente Attività Finanziaria che operi il corretto riconoscimento della propria C.D.R.L.la secondo le previsioni della vigente normativa in materia di Antiriciclaggio (Direttiva 2005/60/CE e con specifico riferimento al contesto italiano, D.Lgs. 231/07 e s.m.i.) e del Manuale Operativo.
Nell'ipotesi in cui l'attività di identificazione sia eseguita da un Intermediario finanziario o altro Soggetto Esercente Attività Finanziaria, il C.D.R.L.:

a. dichiara, sotto la propria esclusiva responsabilità, di svolgere l'attività di Intermediario finanziario o altro Soggetto Esercente Attività Finanziaria in conformità alla vigente normativa e di rispettare la vigente normativa in materia di Antiriciclaggio (Direttiva 2005/60/CE e con specifico riferimento al contesto italiano, D.Lgs. 231/07 e s.m.i.) con specifico riguardo all'identificazione della C.D.R.L.la, manlevando espressamente Aruba PEC da qualsiasi conseguenza pregiudizievole, richiesta di risarcimento e/o pretesa anche di terzi in relazione allo svolgimento di tale attività;
b. si impegna ad acquisire e verificare, sotto la propria responsabilità, i canali di contatto personali dei Richiedenti (ovvero indirizzo di posta elettronica del Richiedente e numero di telefono cellulare sul quale il Richiedente intende ricevere SMS), che saranno utilizzati per le procedure sicure di rilascio del certificato digitale e/o degli eventuali strumenti e informazioni per il suo utilizzo, predisposte dal Certificatore. In Particolare il C.D.R.L. si obbliga a (i) acquisire i canali di contatto del Richiedente e (ii) verificare che tali canali di contatto siano effettivamente riconducibili, in modo univoco, al Richiedente medesimo;
c. prende atto ed accetta che, al fine di attivare la modalità di riconoscimento ai sensi della normativa Antiriciclaggio, il Certificatore deve acquisire i dati del Richiedente, come identificato dal C.D.R.L. ai sensi della normativa Antiriciclaggio. A tal fine resta inteso che: (i) il C.D.R.L. dovrà essere abilitato dal Certificatore al riconoscimento ai sensi della normativa Antiriciclaggio, secondo le procedure predisposte dal Certificatore; (ii) il C.D.R.L. è tenuto ad indicare un proprio Responsabile di Processo; (iii) il Responsabile di Processo, come sopra identificato, richieda l'emissione di una firma automatica e/o di un sigillo qualificato tramite il modulo di richiesta predisposto dal Certificatore, al fine di attestare la correttezza dei dati del Richiedente e l'avvenuto riconoscimento del medesimo ai sensi della vigente normativa Antiriciclaggio nelle comunicazioni con il Certificatore;
d. dichiara di aver compiutamente informato il Responsabile di Processo dei propri obblighi relativamente alla corretta trasmissione al Certificatore dei dati del Richiedente, come identificato ai sensi della vigente normativa Antiriciclaggio;
e. il C.D.R.L. rimane Responsabile, nei confronti del Certificatore e del Richiedente, di tutte le operazioni compiute dal Responsabile di Processo.

4.1.2 Gli obblighi di cui alle lettere b), c), d) e) f) del precedente articolo 4.1 non trovano applicazione nelle ipotesi in cui l'attività di identificazione sia eseguita tramite la modalità di riconoscimento n. 6 del Manuale Operativo. Fermo quanto previsto dal precedente articolo 3.2, resta espressamente inteso che l'esecuzione dell'attività di riconoscimento eseguita dal C.D.R.L. e datore di lavoro, è subordinata al rispetto degli obblighi e degli impegni previsti dal documento "Requisiti per riconoscimento con modalità 6 del MO".

4.2 Fermo restando tutti i casi di responsabilità che possono essere imputati al C.D.R.L. per l'esecuzione di quanto previsto nel presente Contratto, quest'ultimo è responsabile nei confronti del Certificatore per l'esatta osservanza, anche da parte di coloro di cui dovesse avvalersi per l'esecuzione del Contratto, degli obblighi contenuti nel presente Contratto. Il C.D.R.L. è, altresì, direttamente e solidalmente responsabile nei confronti di Aruba Pec per tutti i danni da questa subiti e/o subendi e per quelli eventualmente subiti e/o subendi dal Richiedente e/o da terzi, che siano riconducibili a propri comportamenti (attivi e/o omissioni) nonché a quelli dei propri addetti nell'esercizio delle attività oggetto del presente Contratto, e si impegna ora per allora a manlevare e tenere indenne Aruba Pec da ogni e qualsiasi responsabilità e/o richiesta risarcimento che dovesse essere avanzata nei suoi confronti per i motivi sopra indicati.

4.3 Nell'ipotesi in cui il C.D.R.L. o i propri addetti violino le procedure disposte dal Certificatore ed indicate nel Manuale Operativo, specie in riferimento alle attività di identificazione dell'Utente, Il C.D.R.L. si impegna a manlevarla e/o tenere indenne Aruba Pec da qualsiasi richiesta danni e/o sanzione da chiunque avanzata al riguardo.

4.4 Il C.D.R.L. solleva ora per allora Aruba Pec da ogni e qualsiasi responsabilità conseguente alla mancata e/o ritardata e/o incompleta consegna dei documenti richiesti da Aruba Pec e comunque si impegna a manlevarla e/o tenerla indenne da qualsiasi richiesta danni e/o sanzione da chiunque avanzata al riguardo.

4.5 Il C.D.R.L. prende atto ed accetta che Aruba Pec non effettua nessun backup specifico dei dati e/o informazioni e/o contenuti trattati mediante i Servizi. Il C.D.R.L. è pertanto tenuto ad informare il Richiedente affinché effettui, a propria cura e spese, il backup completo dei dati e/o informazioni e/o contenuti da egli stesso immessi e/o trattati mediante il Servizio ed a prendere tutte le necessarie misure di sicurezza per la salvaguardia dei medesimi. Aruba Pec in ogni caso non offre alcuna garanzia relativamente all'utilizzo del Servizio per quanto riguarda la tutela e la conservazione dei suddetti dati e/o informazioni e/o contenuti.

4.6 In caso di Firma Automatica, il servizio consente di utilizzare, attraverso apposite interfacce applicative, l'infrastruttura di Firma automatica con certificati qualificati rilasciati dal Certificatore. Il C.D.R.L. consapevole che l'utilizzo di una Firma automatica per cui sia

stato emesso il relativo Certificato comporta la possibilità di sottoscrivere atti e documenti rilevanti a tutti gli effetti della legge italiana e riconducibili unicamente in capo al soggetto a nome del quale risulta essere stata emessa, informerà il Titolare:

a) che Egli stesso è l'unico responsabile dell'utilizzo della chiave privata, del dispositivo di firma e del codice di attivazione ad esso associato (PIN);
b) dell'obbligo previsto a suo carico di adottare tutte le misure idonee ad evitare che, dall'utilizzo del sistema di chiavi asimmetriche o della Firma automatica, derivi danno ad altri.

5. Caratteristiche dell'attività

5.1 Il C.D.R.L. nominato da Aruba CDRL si avvarrà di propri addetti (dipendenti, collaboratori, etc.), nominativamente individuati e comunicati ad Aruba Pec per l'esecuzione delle attività ad esso delegate.

5.2.1 Gli addetti incaricati dal CDRL rivestiranno il ruolo di ODR o IR a seconda dei casi.

5.2.1.1 La nomina di un ODR è subordinata alle seguenti condizioni tutte:

a) insussistenza di carichi pendenti o condanne penali;
b) frequenza di un corso formativo avente ad oggetto le specifiche nozioni di natura tecnica, giuridica ed amministrativa necessarie allo svolgimento delle attività che gli saranno assegnate da svolgersi con le modalità previste e comunicate da Aruba Pec S.p.a. e contenente le prescrizioni da rispettare rigorosamente nello svolgimento delle attività stesse. Resta inteso, e di ciò il CDRL prende atto ed accetta, che le spese di soggiorno relative alla frequentazione da parte di ciascun ODR del predetto corso formativo saranno a totale carico del CDRL medesimo.

5.2.1.2 La nomina di un IR è subordinata alle seguenti condizioni tutte:

a) insussistenza di carichi pendenti o condanne penali
b) frequenza di un corso formativo avente ad oggetto le nozioni relative alle attività di identificazione e contenente le prescrizioni da rispettare rigorosamente nello svolgimento delle attività stesse. Nel caso in cui l'attività di formazione sia svolta dal Certificatore quest'ultimo comunicherà, all'occorrenza, le modalità e le tempistiche di svolgimento del predetto corso. Resta inteso, e di ciò il CDRL prende atto ed accetta, che le spese di soggiorno relative alla frequentazione da parte di ciascun IR del predetto corso formativo saranno a totale carico del CDRL medesimo. Nel caso in cui il CDRL abbia manifestato la propria volontà di provvedere direttamente all'attività di formazione di coloro che saranno nominati IR, dovrà sostenere tutte le spese correlate alla predetta attività ed attenersi alle prescrizioni ed alle direttive che il Certificatore, all'occorrenza, gli indicherà per l'organizzazione del corso e l'individuazione delle tematiche da trattare.

5.2.1.3 Aruba Pec, all'esito positivo della procedura di nomina e di verifica sopra descritta, rilascerà all'addetto nominato ODR e, solo se previsto in offerta, all'IR, un Certificato Digitale mediante il quale egli dovrà firmare digitalmente le richieste di Certificato a lui presentate dai Clienti, verificare ed autenticare l'identità dei medesimi, ed effettuare in genere tutte le comunicazioni informatiche con Aruba Pec.
Il Certificato Digitale rilasciato all'ODR o IR, al pari di ogni altro Certificato, è strettamente personale e, pertanto, deve ritenersi sottoposto ai limiti e gli obblighi ad esso connessi a norma delle Condizioni di Erogazione Servizi di Certificazione, che l'ODR o l'IR sono tenuti a sottoscrivere, anche in modalità telematica, se abilitata, al momento del ricevimento del proprio Certificato Digitale. Resta inteso che il predetto Certificato Digitale è rilasciato all'ODR o all'IR in funzione delle attività che quest'ultimo deve svolgere per il CDRL; egli, pertanto, non può delegare nessun altro soggetto per l'adempimento delle proprie competenze che, per loro natura, sono rigorosamente personali.
In considerazione di quanto sopra e considerata la sua qualità di Terzo Interessato, il C.D.R.L. ha l'obbligo di:

- revocare il predetto Certificato Digitale in caso di cessazione del rapporto di lavoro/collaborazione con l'ODR o l'IR;
- revocare e/o sospendere il predetto Certificato Digitale in caso di inadempimento da parte dell'ODR o dell'IR alle procedure assegnate da Aruba Pec;
- revocare e/o sospendere il predetto Certificato Digitale in ogni caso di inadempimento o perdita di fiducia nei confronti del medesimo.

Il CDRL dovrà prontamente informare Aruba Pec per iscritto, di tali fatti, con le modalità e nei termini previsti nel Contratto. Resta inteso che il CDRL non potrà rilasciare alcun Certificato o considerare identificato un C.D.R.L. avvalendosi di un ODR o IR il cui Certificato Digitale sia revocato o scaduto. In aggiunta agli obblighi indicati al successivo comma 5.2.1.4 gli ODR dovranno altresì eseguire, personalmente e con la massima cura e diligenza, le attività di:

a) ingresso, con autenticazione forte mediante l'apposito certificato digitale e con le Credenziali Pannello fornitegli dal C.D.R.L., nel Pannello ODR per eseguire la compilazione del Modulo di Registrazione informatico di richiesta di Certificato;
b) invio ad Aruba Pec delle informazioni necessarie alla generazione dei certificati di firma qualificata, in base al tracciato record concordato e firmato digitalmente dall'ODR;

Aruba PEC S.p.A.
Via San Clemente 53, Ponte San Pietro 24036 (BG)
Partita I.V.A. 01879020517 | **Codice Fiscale** 01879020517
REA 445886 | **C.S.** € 6.500.000,00 i.v. | **PEC** arubapec@aruba.pec.it | **Sito** enterprise.aruba.it

c) ricezione del file degli esiti di produzione relativi alle richieste precedentemente inviate al Certificatore. Sarà inoltre dovere dell'ODR eseguire l'attività di:
d) enrollment del certificato su dispositivo di firma sicuro (smart card).

5.2.1.4 Gli addetti nominati ODR o IR, con la sottoscrizione dell'apposita Lettera di Nomina, assumono l'obbligo di svolgere personalmente, in nome e per conto del CDRL e, quindi, di Aruba Pec, le attività di identificazione, autenticazione, registrazione del Richiedente, nonché di consegna del Dispositivo di Firma al medesimo, in rigorosa conformità alle previsioni contenute nel Manuale applicabile, al Contratto ed alle istruzioni impartite dal Certificatore ed alla normativa vigente.
Nello specifico, l'ODR o l'IR dovranno eseguire, personalmente e con la massima cura e diligenza, le attività di seguito indicate:

a) identificazione certa del Richiedente, mediante la consegna e l'esibizione da parte del medesimo (che dovrà necessariamente essere presente e non potrà essere sostituito da alcuno), di uno dei documenti di riconoscimento indicati nel Manuale applicabile e nel Modulo, in corso di validità, unitamente al codice fiscale e ad ogni altro documento che si riveli essere a tal fine necessario. Nel caso in cui sia richiesto il Certificato in funzione di un ruolo o di cariche, rivestite dal Richiedente in nome e per conto di organizzazioni terze ovvero che prevedono il conferimento di poteri al Richiedente da parte di terzi, l'ODR o l'IR dovranno verificare, altresì, la documentazione attestante il possesso del relativo ruolo e/o dei poteri da parte di colui che richiede il Certificato per conto del terzo, seguendo le istruzioni ed i protocolli che saranno di volta in volta forniti dal Certificatore. In caso di richiesta di Sigillo eIDAS l'ODR o l'IR dovranno verificare, altresì, la documentazione attestante il possesso da parte del richiedente dei poteri di rappresentanza della Persona Giuridica da parte dello stesso nonché quelli relativi alla esistenza e validità della persona giuridica medesima, come indicati nel Manuale CPS.
b) ricevimento del Modulo compilato e sottoscritto dal Richiedente, verifica della sua corretta compilazione e sottoscrizione (le firme del Richiedente devono essere apposte, alla presenza dell'ODR o dell'IR, in calce al Modulo) e, ove richiesto, della documentazione necessaria per il rilascio di un Certificato in funzione di un ruolo, come sopra indicata, acquisizione della fotocopia del documento di riconoscimento fornito dal Richiedente, ai sensi di quanto previsto alla precedente lett. a), rilascio della relativa ricevuta, sottoscritta dal Richiedente e dall'ODR o IR;
c) consegna al Richiedente di copia del Modulo di Richiesta, delle Condizioni Generali di Contratto, della documentazione relativa ai Certificati digitali ed alla CNS predisposta da Aruba Pec;
d) consegna del Dispositivo di Firma, con i certificati generati e delle buste contenenti i codici PIN/PUK;
e) invio ad Aruba Pec di tutta la documentazione, in originale, consegnata dal Richiedente, nei termini e nei modi dalla medesima indicati, e necessaria ai fini dell'erogazione del Servizio.

5.2.1.5 L'ODR e l'IR rimangono responsabili nei confronti di Aruba Pec, del Partner, del CDRL, del Richiedente e dei Soggetti Terzi per le procedure e per le attività dai medesimi svolte in nome e per conto di Aruba Pec in rigorosa conformità alle istruzioni impartite da quest'ultimo, con le sole limitazioni indicate nel Manuale applicabile.

5.2.1.6 L'ODR e l'IR, in fase di rinnovo prima della scadenza del certificato per il C.D.R.L., operano secondo le modalità indicate nei Manuali nonché in quelle pubblicato sul sito ww.pec.it e, qualora mantengano lo stesso supporto hardware (dispositivo di firma digitale) su cui detto certificato è contenuto si premurano di verificare che il supporto rispetti i requisiti minimi di sicurezza imposti, tempo per tempo, dalla normativa applicabile in materia e dai Manuali.

5.3 Resta inteso che gli obblighi di cui al presente art. 5 non trovano applicazione nelle ipotesi in cui l'attività di identificazione sia eseguita da un Intermediario finanziario o altro Soggetto Esercente Attività Finanziaria che operi il corretto riconoscimento della propria C.D.R.L.la secondo le previsioni della vigente normativa in materia di Antiriciclaggio (Direttiva 2005/60/CE e con specifico riferimento al contesto italiano, D.Lgs. 231/07 e s.m.i.) e del Manuale Operativo.

5.4 Resta altresì inteso che gli obblighi di cui al presente art. 5 non trovano applicazione nelle ipotesi in cui l'attività di identificazione sia eseguita dal C.D.R.L., in qualità di datore di lavoro, tramite la modalità di riconoscimento n.6 del Manuale Operativo. Fermo quanto previsto dal precedente articolo 3.2, resta espressamente inteso che l'esecuzione dell'attività di riconoscimento eseguita dal C.D.R.L., in qualità di C.D.R.L. e datore di lavoro, è subordinata al rispetto degli obblighi e degli impegni previsti dal documento "Requisiti per riconoscimento con modalità 6 del MO".

6. Clausola risolutiva espressa

6.1. Fatta salva ogni diversa previsione contrattuale e ferme restando le ulteriori ipotesi di cessazione del rapporto contrattuale di cui alle presenti Condizioni Generali di Contratto, il mancato rispetto da parte del C.D.R.L. anche di uno solo degli obblighi previsti agli Artt. 5 e 6 delle presenti Condizioni Generali di Contratto ovvero degli obblighi previsti dal documento "Requisiti per riconoscimento con modalità 6 del MO" se applicabile, costituisce grave inadempimento e legittima Aruba Pec alla risoluzione immediata del rapporto contrattuale ai sensi dell'Art. 1456 c.c.
Il Contratto si intenderà risolto di diritto ai sensi dell'Art. 1456 Cod. Civ., anche nell'ipotesi in cui:

a) il C.D.R.L. o la sua organizzazione subisca delle modifiche tali da porre in discussione la regolare esecuzione degli obblighi contrattuali;

b) il C.D.R.L. sia stato dichiarato insolvente, sia stato ammesso o sottoposto ad una qualsiasi procedura concorsuale, sia stato sottoposto a procedimento penale oppure quando nei suoi confronti risultino essere state promosse procedure esecutive;
c) le dichiarazioni rilasciate dal C.D.R.L. nel Modulo di Adesione risultino essere non veritiere ad insindacabile giudizio di Aruba Pec.

6.2 Nelle ipotesi indicate nel presente articolo, la risoluzione si verifica di diritto mediante dichiarazione unilaterale di Aruba Pec, da eseguirsi con lettera raccomandata a.r. o tramite posta elettronica certificata da inviare al C.D.R.L., senza bisogno di alcun preavviso o messa in mora. Resta salvo, in ogni caso, il diritto di Aruba Pec di ottenere il risarcimento di qualsiasi danno, subito e/o subendo, possa ad essa derivare da detto inadempimento, come previsto al successivo Art. 8.

6.3 In ogni caso il C.D.R.L. resta l'unico responsabile nei confronti dei propri addetti, del Richiedente, dei Terzi e di Aruba Pec per tutti i danni diretti o indiretti da questi patiti a causa della risoluzione o della sospensione che sia imputabile a violazione da parte del C.D.R.L. o dei suoi addetti degli obblighi sopra indicati.

7. Cessazione del Contratto e revoca dei certificati

7.1 In caso di cessazione del presente Contratto a qualsiasi causa dovuta, il C.D.R.L. ed i suoi addetti sono obbligati a cessare immediatamente qualsiasi attività posta in essere in base al presente Contratto ed a restituire al Partner i materiali ricevuti ai fini dell'espletamento dell'incarico. In tali casi, né il C.D.R.L. né i suoi addetti potranno vantare nei confronti di Aruba Pec alcuna richiesta o pretesa, di alcun genere e titolo, neanche per eventuali danni dai medesimi subiti e/o subendi in conseguenza della cessazione del Contratto. Resta inteso che i Certificati attivati in data anteriore alla cessazione del presente Contratto rimarranno validi fino alla loro data di scadenza, raggiunta la quale saranno disattivati.

7.2 Fatta salva ogni diversa previsione contrattuale e gli altri casi di revoca dei Certificati previsti dalla legge, il mancato rispetto da parte del C.D.R.L. e/o degli addetti dal medesimo nominati, anche di uno solo degli obblighi previsti all'Art. 5 delle presenti Condizioni Generali di Contratto ovvero degli obblighi previsti dal documento "Requisiti per riconoscimento con modalità 6 del MO" se applicabile, legittimerà Aruba Pec a disporre la revoca immediata e senza preavviso dei certificati emessi nei confronti degli addetti, coinvolti nella violazione degli articoli sopra indicati, e di quelli emessi da questi ultimi nei confronti dei Richiedenti. Resta inteso che i Certificati da questi ultimi rilasciati ai Richiedenti, nella piena osservanza di quanto disposto dal presente Accordo, rimarranno validi e non saranno revocati.

8. Risarcimento dei danni

8.1 Aruba Pec ha facoltà di agire per ottenere il risarcimento di tutti i danni subiti e subendi in conseguenza di qualsiasi inadempimento del C.D.R.L. o dei suoi addetti agli obblighi del Contratto, e ciò indipendentemente dal fatto che al predetto inadempimento abbia fatto seguito la risoluzione del Contratto o il recesso di Aruba Pec. Resta inteso che il diritto al risarcimento del danno potrà essere esercitato da Aruba Pec sia a titolo esclusivo che congiuntamente ad altro rimedio. Sulla somma richiesta a titolo di risarcimento del danno si applicheranno gli interessi di legge decorrenti dalla data in cui l'inadempimento si è verificato.

9. Trattamento dei dati personali

9.1 Il trattamento dei dati personali del C.D.R.L. e dallo stesso comunicati ad Aruba PEC ai fini della stipula del presente Modulo e della successiva erogazione del Servizio, avverrà in conformità al D.lgs. 196/2003, al Regolamento UE 2016/679 e all'informativa privacy disponibile al link https://www.pec.it/documents/tc-files/it/93_informativaprivacyarubapec.pdf.

10. Nomina a Responsabile del Trattamento dei dati

Per effetto della stipula del presente Contratto, ed in caso di delega delle attività di C.D.R.L., lo stesso viene nominato da Aruba Pec quale Responsabile del Trattamento dei dati personali comunicati dal C.D.R.L., ai fini della fornitura del Servizio, conformemente a quanto previsto nel Contratto, nei termini ed alle condizioni indicate nel DPA allegato al presente contratto.

PROPOSTA N. PDET 286 del 02/04/2026

Centro di Responsabilità:

OGGETTO: Servizio Sistemi Informativi e Innovazione Digitale. Affidamento del servizio triennale comprensivo di canone per noleggio di una istanza ATP Core “on Premise” con attivazione dei moduli aggiuntivi, modulo di Firma Remota, modulo di verifica VOL in formato WebService, kit di Firma Remota con OTP mobile e certificato eIDAS valido 3 anni, certificato di Firma Automatica per soggetti con poteri di rappresentanza, certificato di firma del terzo interessato in esito a Trattativa diretta n. 6099360

PARERE CONTABILE

Il sottoscritto Bacchi Reggiani Giuseppe - Servizio Amministrazione Bilancio e Controllo economico esprime parere di regolarità contabile ai sensi del Regolamento Arpae per l’adozione degli atti di gestione delle risorse dell’Agenzia.

Data 02/04/2026

Bacchi Reggiani Giuseppe