Provincia di Padova
AREA SEGRETERIA GENERALE
SERVIZIO SISTEMI INFORMATIVI

DETERMINAZIONE DIRIGENZIALE

Proposta n. 2122 del **2025**

Determina n. 816 del 18/07/2025

Oggetto: APPROVAZIONE SCHEMI CONTRATTUALI PER LO SVOLGIMENTO DI ATTIVITÀ DI UFFICIO DI REGISTRAZIONE E RILASCIO DI SERVIZI DI CERTIFICAZIONE DIGITALE E DELLA CARTA NAZIONALE DEI SERVIZI TRA LA PROVINCIA DI PADOVA (ENTE EMETTITORE) E INFOCERT SPA (CERTIFICATION AUTHORITY)

IL DIRIGENTE

Visti:
- Il D. Lgs 165/2001 (TUPI) e ss.mm.ii;
- il D. Lgs n. 267/2000 (TUEL) e ss.mm.ii ed in particolare l'art. 107;
- il vigente Statuto con riferimento alle funzioni dei dirigenti;
- il Regolamento Provinciale n. 33, disciplinante il “Sistema di Direzione” (approvato con D.G.P. in data 22.12.1998 n. 467) ed in particolare l’art. 7 sulle competenze dirigenziali;
- la L. n. 56/2014 all’art. 1, commi 54, 55 e 56;
- la L. n. 241/1990 e ss.mm.ii;
- il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR per brevità).

Vista la Delibera del Consiglio Provinciale n. 21 del 30/9/2024 di approvazione del “Documento Unico di Programmazione (DUP) 2025-2027” e quella n. 30 del 19.12.2024 di approvazione del “Bilancio di Previsione 2025-2027”.

Visto l'Atto del Presidente n. 165 del 19/12/2024, relativo all'approvazione del Piano esecutivo di gestione e del Piano dettagliato degli obiettivi 2025-2027, che prevedono, fra gli obiettivi del Servizio Sistemi Informativi e per quanto di pertinenza, quello di favorire "*la convergenza digitale degli Enti del territorio provinciale per semplificare l'accesso ai servizi e alle informazioni da parte degli utenti/cittadini*", includendo nell'azione 4 la "*Gestione dell'ufficio RAO per l'emissione delle CNS (Carta Nazionale dei Servizi). Gestione convenzione trilaterale Provincia InfoCert e partner sul territorio per il rilascio CNS con la possibilità di creare economie di gestione*".

Visto e richiamato il decreto presidenziale n. 103 del 02.09.2024 avente ad oggetto "*Conferimento incarichi dirigenziali*" con il quale si attribuisce espressamente allo scrivente la funzione di Dirigente dell'Area Segreteria Generale, alla quale il Servizio Sistemi Informativi afferisce;

Visto il provvedimento n. 288 del 07.08.2008 della Giunta provinciale avente ad oggetto l'"*Approvazione convenzione con InfoCert Spa per autorizzazione all'attività di RAO - ufficio di registrazione dispositivi firma digitale*" grazie al quale, sin dal 2008, l'Ente Emettitore, Provincia di Padova – anche in qualità di Ufficio di Registrazione – svolge per conto di InfoCert Spa (di seguito "Infocert") le operazioni preliminari di raccolta dei dati relativi ai richiedenti i Certificati, la loro identificazione nonché il successivo eventuale rilascio di CNS e firma digitale.

Ricordato che:

- ai sensi del d.p.r. 2 marzo 2004, n. 117, la Provincia ricopre la funzione di Ente Emettitore della Carta Nazionale dei Servizi (CNS) e che, in tale ambito, InfoCert provvede al rilascio e alla gestione dei certificati da inserire nelle CNS, agli utenti che ne facciano richiesta;
- InfoCert è C.A. ("*Certification Authority*") ossia una società iscritta nell'elenco pubblico dei certificatori, giusta delibera del 19.07.2007, emanata dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (ora "Agenzia per l'Italia Digitale" o "**AgID**") e presta il Servizio di Certificazione ai sensi del Regolamento (UE) N. 910/2014 del 23.07.2014 sulla base di una valutazione di conformità rilasciata dalle competenti Autorità ai sensi delle vigenti normative di settore in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno;
- ai sensi dell'art. 4.1 del Decreto Interministeriale del 9 dicembre 2004 e ss.mm.ii., recante "*Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati*

per la produzione della Carta Nazionale dei Servizi", la Provincia di Padova ha valutato l'opportunità di utilizzare i servizi di InfoCert per le attività previste dal modello del circuito di emissione della CNS, non possedendo le risorse *hardware* e *software* necessarie per la produzione delle CNS;

Considerato che, giusta Decreto del Presidente della Provincia di Padova, n. 41 del 25.05.2020 e ss.mm.ii. (da ultimo il d.p.p. n. 156 del 16.12.2024), è in scadenza un accordo tra la C.A., InfoCert Spa e l'Ente Emettitore, Provincia di Padova, disciplinante, fra le parti, i seguenti rapporti principali:

a mandato a InfoCert ("Mandato CNS") in virtù del quale quest'ultima è autorizzata dall'Ente Emettitore ad avvalersi – per lo svolgimento di attività di Ufficio di registrazione per il rilascio della Carta Nazionale dei Servizi – di propri dipendenti e collaboratori a vario titolo ("RAO" di InfoCert), anche terzi rispetto alla propria organizzazione (Partner/Rivenditori di InfoCert, in qualità di "*Ufficio di Registrazione*"), appositamente incaricati e nominativamente individuati per l'esercizio delle attività di identificazione e registrazione ad essi demandate (e correlati schemi di atti di conferimento d'incarico);

b convenzione bilaterale ("Convenzione RAO") per lo svolgimento di attività di Ufficio di registrazione e rilascio di servizi di certificazione digitale e della CNS e per lo svolgimento di attività di incaricato per il rilascio di servizi di certificazione digitale (e correlati schemi di atti di conferimento d'incarico);

c redazione della manualistica operativa concernente le procedure di rilascio dei servizi digitali oggetto delle attività regolamentate fra le parti.

Visti gli accordi sopra citati, che stabiliscono in cinque anni (dalla firma del maggio 2020 al 31.12.2025) la durata della stessa.

Dato atto che, affinché la Provincia possa, dal 1 gennaio 2026, continuare, senza soluzione di continuità, ad offrire alla propria utenza, nell'ambito del territorio provinciale, i servizi derivanti dal suo ruolo di Ente Emettitore nel rilascio delle C.N.S. e di tutti gli altri supporti digitali per il tramite di una *Certification Authority,* è necessario rinnovare gli stessi, in via di scadenza.

Considerato che i servizi che l'Ente è in grado di offrire con il rilascio delle CNS e dei *digital trust* sono elemento indispensabile per proseguire ed accrescere il percorso di innovazione digitale e di accompagnamento dei Comuni del territorio, garantendo loro il giusto ed efficiente supporto tecnico, coerentemente con le indicazioni della normativa europea, nazionale e regionale.

Dato atto che, a seguito dell'istruttoria effettuata dagli uffici del Servizio Sistemi Informativi è emerso quanto segue:

- la Provincia di Padova ha valutato positivamente l'esperienza svolta nel corso degli ultimi 17 anni in qualità di Ufficio di Registrazione e rilascio di servizi di certificazione digitale, per le proprie esigenze e per le necessità manifestate dai Comuni del proprio territorio, per cui si ritiene opportuno rinnovare il servizio con le medesime modalità;
- a seguito di confronto con InfoCert, si è accertata la comune volontà di proseguire nei rapporti, apportando agli schemi contrattuali delle modifiche derivanti dagli aggiornamenti tecnologici, relativi alla manualistica di riferimento e alle nuove direttive AgID, volte a formalizzare una catena di controllo più breve nel processo di riconoscimento ed emissione dei prodotti digitali;
- l'offerta collaborativa proposta da InfoCert risulta vantaggiosa in quanto risponde a criteri di efficienza ed economicità, grazie a una gestione unica centralizzata e standard di qualità certificati e collaudati nel corso dell'esperienza pluriennale con la Provincia di Padova.

Considerato che il rapporto regolato dai contratti in parola comporta un vantaggio per la Provincia, poiché è prevista un'entrata a beneficio dell'Ente stesso per il riconoscimento da parte di InfoCert di un contributo a titolo di indennità – il cui importo è stato aumentato rispetto a quello attualmente percepito – per lo svolgimento delle attività in oggetto e per ogni carta emessa da un RAO esterno all'Ente Emettitore.

Ritenuto opportuno, per tutto quanto finora esposto, rinnovare, in vista della scadenza del prossimo 31 dicembre 2025 i rapporti con InfoCert SpA, per la durata di anni 6 (sei) a decorrere dal 1° gennaio 2026 e quindi sino al 31.12.2031.

Ritenuta la propria competenza.

Dato atto del parere contabile favorevole del Dirigente Area Gestione delle Risorse - Servizio Programmazione Finanziaria e Bilancio, espresso in ordine alla presente proposta ai sensi dell'art. 49 del Testo Unico delle leggi sull'ordinamento degli Enti Locali, approvato con D. Lgs. 18.8.2000 n. 267

DETERMINA

1 di **approvare**, per quanto sin qui esposto, gli schemi di atti di cui trattasi e i relativi allegati come di seguito elencato:

a Accordo tra InfoCert SpA, quale C.A. ("*Certification Authority*") e Provincia di Padova, quale Ente Emettitore, per lo svolgimento di attività di Certification Authority e Ufficio di Registrazione per il rilascio della carta nazionale dei servizi

("**Accordo**") e, nell'ambito della medesima, i seguenti allegati di riferimento:

- **All. a)1** Accordo fra le parti per la nomina della Provincia di Padova a R.A. ("*Registration Authority*") e per lo svolgimento da parte di quest'ultima delle attività di Ufficio di Registrazione ("**Accordo R.A. Provincia di Padova**") e, nell'ambito del medesimo, il seguente:
- **All. a)2** Mandato trilaterale per lo svolgimento di attività da parte dell'Operatore dell'Ufficio di Registrazione incaricato ("*R.A.O. – Registration Authority Officer*") per il rilascio di servizi trust di InfoCert SpA. ("**Mandato Rao**").

b Manuale contenente le regole e le procedure operative che governano l'emissione della Carta Nazionale dei Servizi (CNS) e dei relativi certificati emessi dal Certificatore InfoCert SpA, Trust Service Provider, su affidamento dell'Ente Emettitore, Provincia di Padova ("**Manuale Operativo Ente Emettitore – CNS**").

2 di **prendere atto**, per quanto specificamente meglio indicato in Accordo sub a) all'art. 1.4 e per la durata di anni 6 (sei) con decorrenza dal 1° gennaio 2026 sino al 31 dicembre 2031, degli schemi sotto elencati:

c Accordo Quadro fra InfoCert e i suoi Clienti ("**Accordo Quadro InfoCert SpA – Clienti**") per la fornitura dei servizi InfoCert sottoposti a regolamentazione normativa specifica per i servizi "*digital trust*" e tutti gli allegati richiamati dal medesimo e necessari per lo svolgimento delle attività commerciali e statutarie di InfoCert SpA:

- **All. c)1** Offerta Commerciale;
- **All. c)2** Data Processing Agreement (DPA);
- **All. c)3** Certificati qualificati e di autenticazione;
- **All. c)4** Misure di Sicurezza;
- **All. c)5** Certificati Remoti e Dispositivo (CNS) - Mandato Master RAO - Mandato RAO Supplier - Mandato RAO - Requisiti Compliance Registration Authority;

3 di dare atto che l'Accordo **sub a)** decorrerà dal 1° gennaio 2026 e avrà la durata di anni 6 (sei) e comunque non oltre il 31 dicembre 2031;

4 di dare atto che tutti i precedenti accordi fra InfoCert e la Provincia di Padova cesseranno di avere efficacia al 31 dicembre 2025 in quanto sostituiti dall'Accordo **sub a),** una volta sottoscritto fra le parti, con decorrenza dal 1° gennaio 2026, fatto salvo quanto puntualmente disciplinato fra le parti nell'Accordo stesso (sub a) per quanto attiene la validità temporale delle certificazioni e dei supporti digitali emessi in costanza della precedente convenzione;

5 di riservare allo scrivente dirigente la successiva sottoscrizione con InfoCert SpA

dell'"**Accordo**" sub a) e dell'"**Accordo R.A. Provincia di Padova**" sub a)1, delegando al responsabile del Settore Sistemi Informativi *pro tempore* la firma di **Mandati Rao** secondo il modello sub All. a)2;

6 di dichiarare il presente provvedimento immediatamente eseguibile stante la necessità di sottoscrivere a stretto giro il nuovo "**Accordo**" **sub a)** e così permettere ad InfoCert di allestire in tempo, per la decorrenza del 1° gennaio 2026, la sovrastruttura hardware e software necessaria per lo svolgimento delle attività convenzionate e a beneficio della Provincia di Padova quale Ente Emettitore e Registration Authority e Ufficio di Registrazione.

Sottoscritto dal Dirigente
(NICASTRO FRANCO)
con firma digitale

ACCORDO PER

LO SVOLGIMENTO DI ATTIVITA' DI CERITIFICATION AUTHORITY E

UFFICIO DI REGISTRAZIONE PER IL RILASCIO

DELLA CARTA NAZIONALE DEI SERVIZI

("Accordo")

TRA

Provincia di Padova, con sede legale in Padova, Piazza Antenore, 3, C.F./P.IVA 80006510285/00700440282, rappresentata dal Dirigente *pro tempore* ("**Ente Emettitore**");

E

InfoCert S.p.A., società soggetta alla direzione ed al coordinamento di Tinexta S.p.A., con sede legale in Roma, Piazzale Flaminio 1/B, e sede operativa in Padova, P.zza Luigi da Porto 3, P.IVA 07945211006 in persona dell'Amministratore Delegato dott. Danilo Cattaneo ("**InfoCert**" o "**Certification Authority**" o "**CA**");

congiuntamente anche le Parti ("**Parti**");

PREMESSO CHE:

a) InfoCert, società iscritta nell'elenco pubblico dei certificatori, con delibera del 19.07.2007, emanata dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (ora "Agenzia per l'Italia Digitale" o "**AgID**"), presta il Servizio di Certificazione (il/i "**Servizio/i**") anche quale prestatore di servizi fiduciari qualificati, ai sensi del Regolamento (UE) N. 910/2014 del 23.07.2014 (il "**Regolamento**"), sulla base di una valutazione di conformità rilasciata dal Conformity Assessment Body CSQA Certificazioni S.r.l., come da Regolamento, norme ETSI EN 319 401, ETSI EN 319 411-1; ETSI EN 319 411-2 e schema di valutazione eIDAS definito da ACCREDIA, ai sensi delle norme ETSI EN 319 403 e UNI CEI ISO/IEC 17065:2012; nonché ai sensi del regolamento eIDAS 2 - 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 e che abroga la direttiva 1999/93/CE, modificato da Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024;

b) L'Ente Emettitore, ai sensi del D.P.R. 117/2004 e ss.mm.ii., ricopre la funzione di Ente Emettitore della Carta Nazionale dei Servizi ("**CNS**") e, in tale ambito, InfoCert provvede al rilascio e alla gestione dei certificati da inserire nelle CNS, agli utenti che ne facciano richiesta (i "**Titolari**" o "**Richiedenti**");

c) ai sensi del Mandato CNS, InfoCert è autorizzata dall'Ente Emettitore ad avvalersi di propri dipendenti e collaboratori a vario titolo ("**RAO**" di InfoCert), anche terzi rispetto alla propria organizzazione (Partner/Rivenditori di InfoCert, in qualità di "**Ufficio di Registrazione**"), appositamente incaricati e nominativamente individuati per l'esercizio delle attività di identificazione e registrazione ad essi demandate;

d) le procedure di rilascio della Carta Nazionale Servizi ("**CNS**") sono esposte (i) nel Manuale Operativo pubblicato dall'Ente Emettitore ("**Manuale Operativo Ente Emettitore**"), (ii) nella Certificate Policy dei Certificati di Autenticazione per la CNS "ICERT-INDI-CPCA-CNS" emessa da InfoCert disponibili sul sito www.infocert.it, nonché (iii) nei provvedimenti legislativi e amministrativi richiamati nei suddetti documenti, che InfoCert e/o l'Ufficio di Registrazione dichiara di conoscere accettando gli obblighi conseguenti a suo carico;

e) con la Determina n._____, l'Ente Emettitore approva espressamente il contenuto del presente atto, che sostituisce integralmente il testo approvato da precedente Decreto del Presidente della Provincia di Padova n. 41 del 25.5.2020.

tutto ciò premesso, le Parti convengono e stipulano quanto segue:

Art. 1 - Valore delle premesse e allegati

1.1. Le premesse, gli Allegati e i Manuali Operativi di InfoCert e dell'Ente Emettitore che disciplinano i servizi di certificazione previsti nel presente accordo (in seguito "**Accordo**") formano parte integrante del presente accordo.

1.2. Sono allegati al presente atto e formano parte integrante dell'Accordo i seguenti documenti:
A. Accordo Quadro di fornitura dei servizi InfoCert ("**Accordo Quadro**").

1.3. Le Parti precisano che, oltre al presente Accordo, i loro rapporti, con riferimento al solo svolgimento da parte della Provincia di Padova / Ente Emettitore delle attività di RA (Registration Authority) e di RAO da parte dei dipendenti e/o collaboratori interni di quest'ultima, saranno disciplinati anche da un separato "Accordo per lo svolgimento delle attività di Ufficio di Registrazione" che sarà allegato alla presente unitamente alla documentazione sub 1.2.

1.4. La Provincia di Padova dichiara e InfoCert acconsente, riconosce e nulla oppone, che l'"Accordo Quadro" predetto sub 1.2, unitamente alla documentazione ad esso allegata – e che InfoCert sottopone ai suoi Clienti per la regolamentazione dell'esercizio delle attività di fornitura di servizi Digital Trust in particolare di rilascio delle CNS e delle Firme Digitali – sono documenti facenti parte del presente Accordo a titolo conoscitivo/informativo e la Provincia ne prende mero atto, rimanendo ogni effetto e/o conseguenza derivante dall'esecuzione dei medesimi, che non sia qui o altrove altrimenti disciplinata fra le Parti, di esclusiva pertinenza contrattuale della stessa InfoCert e della sua clientela senza alcun pregiudizio per la Provincia di Padova.

Art. 2 - Oggetto

2.1. L'Ente Emettitore conferisce ad InfoCert mandato non esclusivo a espletare la funzione di Certification Authority e a svolgere funzione di rilascio di CNS, in qualità di Ufficio di Registrazione.

2.2. L'Ente Emettitore autorizza InfoCert, in qualità di CA, a delegare l'attività di richiesta e rilascio di CNS a soggetti terzi delegati da InfoCert in qualità di Ufficio di Registrazione.

2.3 Il rapporto tra InfoCert (in qualità di CA) e il terzo Ufficio di Registrazione sarà regolato da apposito Accordo Quadro e dai relativi allegati, di cui sarà data notizia di volta in volta all'Ente Emettitore per opportuna condivisione.

2.4 In particolare, InfoCert, in qualità di Ufficio di Registrazione, nel rilascio della Carta Nazionale dei Servizi ("**CNS**") con Certificato digitale di sottoscrizione[1] e di autenticazione CNS, si impegna ad osservare i seguenti obblighi:

a. A far sottoscrivere il mandato ai RAO nonché a rispettare e far rispettare ai propri incaricati (di seguito definiti quale "**Master RAO/RAO**") le procedure di registrazione di cui ai paragrafi 3 e 4 del Manuale Operativo ICERT-INDI-MO (per il rilascio dei certificati di sottoscrizione);
b. far rispettare ai propri RAO le previsioni e gli obblighi dei mandati a loro conferiti e le previsioni procedurali di cui agli allegati tecnici acclusi all'Accordo Quadro;
c. conservare le richieste di rilascio, revoca, sospensione, ripristino di validità e rinnovo della CNS e del certificato digitale di sottoscrizione ricevute dai richiedenti, correttamente compilate in ogni loro parte;
d. conservare gli originali delle richieste debitamente compilate di cui al punto precedente, nel rispetto dei Manuali Operativi.

2.5. Ai fini del rilascio della CNS, l'Ente Emettitore conferisce mandato ad InfoCert per esercitare le funzioni gestorie del certificato indicate nella Certificate Policy dei Certificati di Autenticazione per la CNS (ICERT-INDI-CPCA-CNS) di InfoCert e nel Manuale Operativo Ente Emettitore. InfoCert, in qualità di Ufficio di Registrazione assume, pertanto, tutti gli obblighi previsti dal Manuale Operativo Carta Nazionale dei Servizi presente sul sito internet dell'Ente Emettitore, obbligandosi ad osservare strettamente le procedure di identificazione e registrazione iniziale dei Richiedenti richiamate dal medesimo Manuale Operativo, garantendo di aver già l'organizzazione di personale e di beni adeguata all'esercizio della suddetta attività.

2.6. InfoCert, anche in qualità di Ufficio di Registrazione, si obbliga altresì al rispetto delle procedure di gestione della CNS di cui al Decreto 9.12.2004 recante "Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei servizi"[2] e, in particolare ai paragrafi 4 e 5 delle stesse.

Art. 3 - Obblighi di InfoCert

3.1. InfoCert, in qualità di Ufficio di Registrazione nonché di Certification Authority, si impegna a:

a) svolgere le attività previste nel presente Accordo con la diligenza del mandatario di cui all'art.1710, c.c., assumendosi anche la responsabilità delle attività eseguite, per suo conto, dagli Uffici di Registrazione e dai RAO di cui InfoCert si avvale per l'erogazione delle CNS e dei certificati, anche in deroga al disposto dell'art. 1717 co. 2 c.c.;

b) svolgere l'attività di registrazione nel rispetto della normativa vigente e delle procedure di cui ai Manuali Operativi, con particolare riferimento all'identificazione personale certa dei Richiedenti nel rispetto di quanto indicato di seguito alla lett. c). In tal senso, InfoCert si impegna ad assumere ogni responsabilità in punto di verifica dell'identità del richiedente la CNS anche per conto dell'Ente Emettitore e, parimenti, si

[1] Il certificato di sottoscrizione è il certificato di firma remota digitale qualificato ai sensi del regolamento eIDAS, rilasciato dalla CA e inserito su dispositivo fisico CNS.

[2] https://www.agid.gov.it/sites/default/files/repository_files/documentazione_trasparenza/decreto_9_dicembre_2004.pdf

impegna a gestire tutto il ciclo di vita della CNS e del certificato anche per conto dell'Ente Emettitore medesimo;

c) svolgere a mezzo dei propri RAO le seguenti attività (i)ove applicabile, procede alla identificazione certa dei Richiedenti mediante esibizione di un documento di riconoscimento da parte di questi ultimi, dovendosi sin d'ora precisare che l'attività di identificazione dei Richiedenti dovrà obbligatoriamente avvenire attraverso l'esibizione della CIE originale (non essendo ammissibile la sola copia del documento) integra ed in corso di validità e/o di documento di identità originale e Tessera Sanitaria in corso di validità; (ii) raccolta della Richiesta di attivazione dei Richiedenti, compilata e sottoscritta in ogni sua parte; (iii) verifica della integrale compilazione della Richiesta di attivazione, con particolare riferimento all'inserimento da parte del Richiedente dei dati personali obbligatori, fra cui l'indirizzo mail e il numero di telefono cellulare che dovranno essere direttamente riconducibili a quest'ultimo; (iv) verifica attraverso i sistemi della CA che i dati obbligatori rilasciati (indirizzo email e numero di cellulare indicato nella Richiesta di attivazione) non siano abbinati ad un codice fiscale già appartenente ad un diverso Titolare; (v) consegna al Richiedente della documentazione informativa precisando a quest'ultimo che la ricezione dei codici di attivazione (e revoca) avverranno mediante l'invio direttamente dalla CA di una busta virtuale all'indirizzo email indicato in sede di Richiesta di attivazione;

d) informare i Richiedenti su come utilizzare il dispositivo per firmare e/o autenticarsi ai siti WEB, con particolare riferimento alle modalità di revoca, sospensione e rinnovo dei certificati digitali nonché sugli aspetti normativi e sulle conseguenze giuridiche derivanti dall'utilizzo degli stessi;

e) informare i Richiedenti la CNS dell'esistenza di un call center e dei relativi recapiti, a cui gli stessi possono rivolgersi per assistenza, revoca e sospensione della CNS;

f) utilizzare e trattare i dati personali acquisiti conformemente a quanto previsto dal D.L.vo 196/2003 e ss.mm.ii, nonché del Regolamento generale sulla protezione dei dati n. 679/2016/UE;

g) individuare nominativamente i propri RAO/RAO Supplier/Master RAO facendo sottoscrivere loro apposito mandato in cui vengano elencati i dati degli stessi e comunicarne le generalità all'Ente Emettitore, anche attraverso condivisione mediante opportune piattaforme in uso della CA per lo scopo;

h) regolamentare le modalità di rilascio delle CNS per il tramite degli Uffici di Registrazione, nonché le attività riguardanti la formazione, le responsabilità e gli obblighi derivanti dall'espletamento della funzione di Ufficio di Registrazione, in apposito Accordo Quadro sottoscritto tra InfoCert e i suoi clienti/partner;

i) svolgere le funzioni di approvvigionamento, produzione e numerazione dei dispositivi smart card per conto dell'Ente Emettitore;

j) garantire all'Ente Emettitore un accesso riservato, operativo già a far data dal primo giorno di efficacia del presente Accordo (1.1.2026), alle piattaforme gestionali di InfoCert, attraverso cui avere un aggiornamento in tempo reale degli Uffici di Registrazione e dei RAO e Master RAO operanti per suo conto.

Art. 4 - Corrispettivi e fornitura

4.1. L'Ufficio di Registrazione per lo svolgimento dell'attività prevista nel presente Accordo corrisponde all'Ente Emettitore a titolo di indennità 2,50 euro per ogni carta emessa da un RAO esterno all'Ente Emettitore.

4.2. Con cadenza trimestrale InfoCert comunicherà all'Ente Emettitore il numero di certificati emessi per ciascun Uffici di Registrazione, RAO e Master RAO attivi, indicando la denominazione completa dell'ufficio; la partita IVA o CF e il codice identificativo univoco dell'ufficio per i sistemi di Infocert. Tale elenco sarà fornito alla Provincia in formato tabellare digitale (csv o xlsx) entro il mese successivo al trimestre di riferimento dei dati.

4.3 Come da richiesta dell'Ente Emettitore (o dal cliente/partner di InfoCert), i dispositivi saranno personalizzati con applicazione del ~~solo~~ logo dell'Ente Emettitore e di InfoCert e recheranno impressa chiara dicitura con specifica dei recapiti per l'assistenza di competenza di InfoCert e/o dei rispettivi Uffici di registrazione

Art. 5 – Durata, decorrenza e recesso

5.1. Il presente Accordo avrà efficacia a far data dal 01.01.2026 fino al 31.12.2031.

5.2. Durante tutto il periodo di vigenza del presente Accordo l'Ente Emettitore e/o InfoCert avranno diritto, senza pagamento di alcun corrispettivo e salvo quanto previsto al successivo art. 9.3, di recedere da essa, con un preavviso di 60 giorni, con comunicazione della volontà di esercitare tale diritto a mezzo PEC; spetta, inoltre, all'Ente Emettitore il diritto di recesso di cui all'art. 11 comma 4, L. n. 241/1990, con esclusione di qualsiasi indennizzo a favore delle controparti.

5.3. In caso di recesso e/o revoca, l'Ufficio di Registrazione non potrà vantare alcuna richiesta nei confronti dell'Ente Emettitore e/o di InfoCert, neanche per eventuali danni subiti in conseguenza dello stesso.

5.4. Il recesso di una delle Parti comporterà il venir meno dell'efficacia del presente Accordo nei confronti di tutte le altre.

5.5. Resta inteso che il supporto e l'assistenza di Infocert sui certificati regolarmente emessi dovrà essere garantita in qualunque caso sino alla scadenza naturale dei certificati stessi.

Art. 6 - Esclusiva e responsabilità

6.1. InfoCert, in qualità di Ufficio di Registrazione e l'Ente Emettitore prendono atto che non possono vantare alcuna esclusiva per l'esercizio delle suddette attività; queste sono pertanto libere di stipulare intese di contenuto analogo alla presente anche con altri soggetti.

6.2. InfoCert, in qualità di Ufficio di Registrazione, è direttamente e solidalmente responsabile nei confronti dell'Ente Emettitore oltre che dei danni da questi subiti, anche per eventuali danni patiti dai Richiedenti e/o da terzi, direttamente conseguenti a propri comportamenti e/o omissioni colpevoli, nonché per i comportamenti e/o le omissioni colpevoli dei propri RAO nell'esercizio dell'attività di identificazione e registrazione e nell'espletamento degli obblighi nascenti dalla normativa vigente e dal presente Accordo e relativi allegati, senza possibilità di esonero neanche parziale e anche in deroga all'art. 1717, c. 2, c.c.

6.3. InfoCert, in qualità di Ufficio di Registrazione, prende atto e accetta che la violazione degli obblighi di corretta e certa identificazione di cui al precedente art. 3.1. comporta responsabilità civili nei confronti dell'Ente Emettitore.

6.4. Nel caso in cui un richiedente o un qualunque terzo avanzasse pretese economiche nei confronti dell'Ente Emettitore, per fatti direttamente o indirettamente ricollegabili ad inadempimenti e/o negligenze di InfoCert, in qualità di Ufficio di Registrazione, quest'ultima si obbliga a tenere indenne e/o manlevare l'Ente Emettitore da qualsiasi conseguenza pregiudizievole, anche in termini di spese legali.

Art. 7 - Normativa antimafia e codice etico

7.1. Le Parti prendono atto che la validità del presente Accordo è subordinata all'integrale rispetto della vigente normativa antimafia nonché della normativa in materia di responsabilità delle persone giuridiche di cui al D.L.vo 231/2001 e ss. mm. ii., da parte dei propri amministratori, dipendenti, collaboratori o fornitori e che il mancato rispetto della richiamata normativa comporterà la risoluzione di diritto del presente Accordo, *ex* art. 1456, c.c., con conseguente diritto di InfoCert al risarcimento dei danni subiti. Le Parti, inoltre, nell'esecuzione delle attività derivanti dal presente Accordo, si impegneranno ad osservare il Codice Etico adottato da InfoCert e disponibile sul sito istituzionale *www.infocert.it*, come di volta in volta integrato e modificato e dichiarano altresì di conformarsi alle previsioni del Modello di Organizzazione Gestione e Controllo ai sensi del d.lgs. 8 giugno 2001, n. 231, alla Politica per la Prevenzione della Corruzione adottati da InfoCert e disponibili parimenti sul sito istituzionale di quest'ultima, nonché al Protocollo di legalità ai fini della prevenzione dei tentativi di infiltrazione della criminalità organizzata, sottoscritto da Prefetture del Veneto, Regione Veneto, UPI e ANCI in data 17/09/2019 e successive modifiche e/o integrazioni.

Art. 8 - Privacy

8.1. Le Parti si impegnano alla piena osservanza, per quanto di rispettiva competenza, del dettato del D.L.vo 196/2003 e ss.mm.ii, nonché del Regolamento generale sulla protezione dei dati n. 679/2016/UE (il "**Regolamento Privacy**"). InfoCert e l'Ente Emettitore danno atto del fatto che:

a) l'Ente Emettitore agisce in qualità di titolare autonomo del trattamento rispetto al rilascio della CNS, ai sensi dell'art. 24 del GDPR;

b) InfoCert, ai sensi dell'art. 24 del GDPR, agisce quale titolare autonomo del trattamento rispetto all'emissione e gestione dei certificati contenuti nella CNS.

8.2. Nello svolgimento delle operazioni di trattamento dei dati personali degli interessati/Richiedenti, l'Ente Emettitore nomina InfoCert, in qualità di Ufficio di Registrazione, quale responsabile del trattamento dei dati ai sensi degli artt. 28 e ss. del GDPR. Fatti salvi gli altri obblighi previsti dalle disposizioni di legge e regolamentari applicabili, ivi inclusi i provvedimenti delle Autorità di controllo in materia di dati personali, il Responsabile è obbligato a rispettare quanto segue e pertanto dichiara di:

a) trattare i dati personali nel pieno rispetto del Regolamento e della normativa privacy tempo per tempo vigente, sulla base del presente Accordo di ogni altra istruzione impartita dal Titolare ai sensi dell'Accordo e dei relativi allegati e adottare idonei sistemi informatici per il trattamento dei dati personali;

b) garantire, per conto delle persone autorizzate al trattamento dei dati personali (RAO), l'obbligo di riservatezza in merito a tutte le informazioni e i dati acquisiti in esecuzione dell'Accordo;

c) designare le persone autorizzate al trattamento (ossia i propri dipendenti, come pattuito nell'Accordo ovvero i RAO), formare adeguatamente le stesse mediante appositi eventi formativi in materia di trattamenti dei dati personali e conferire loro, in forma scritta, l'incarico di compiere le operazioni di trattamento nonché

le medesime istruzioni impartite dal Titolare al Responsabile sulla base del presente Accordo, istruirle sulle modalità di elaborazione dei dati ai quali hanno accesso e vigilare sulle stesse, nonché comunicare al Titolare, su richiesta di quest'ultimo, i nominativi delle persone autorizzate;

d) adottare tutte le misure di sicurezza richieste ai sensi dell'art. 32 del Regolamento Privacy (anche attraverso la valutazione dei trattamenti e la valutazione strutturata dei rischi) tra le quali anche le misure di attuazione dei principi di privacy by design e privacy by default;

e) con riferimento al paragrafo 6.3.1 della norma ISO/IEC 29134, essere in possesso di una policy che definisca le regole per la valutazione del rischio ed i criteri di accettazione;

f) essere in possesso di una procedura di gestione accessi logici basata sul principio della minimizzazione dei permessi e del *need to know;*

g) assistere il Titolare con misure tecniche e organizzative adeguate, per l'adempimento degli obblighi connessi all'esercizio dei diritti degli Interessati, previsti dagli artt. 15 – 22 del Regolamento;

h) assistere il Titolare nell'adempimento degli obblighi in materia di misure di sicurezza tecniche ed organizzative di cui all'art. 32 del Regolamento così come individuate di volta in volta dal medesimo Titolare, ivi incluse le seguenti: (i) pseudonimizzazione e/o cifratura dei dati personali; (ii) resilienza dei sistemi e dei servizi di trattamento; (iii) capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; (iv) procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

i) adottare e aggiornare un registro delle violazioni dei dati personali, stabilire le procedure interne che disciplinano il processo di gestione del *"data breach"*, assistere il Titolare nell'adempimento degli obblighi in materia di notificazione dei dati personali di cui agli artt. 33 e 34 del Regolamento e, in particolare, informare il Titolare della eventuale violazione di dati personali, entro e non oltre 24 (ventiquattro) ore decorrenti dal momento della violazione stessa;

j) assistere il Titolare nelle attività connesse alla valutazione d'impatto sulla protezione dei dati personali di cui all'art. 35 del Regolamento e, se richiesto, cooperare con il Titolare nell'ambito delle consultazioni preventive di cui all'art. 36 del Regolamento;

k) cancellare o restituire - a scelta del Titolare - tutti i dati personali oggetto di trattamento in caso di cessazione dell'efficacia del presente Accordo salvi gli obblighi di conservazione dei dati personali eventualmente derivanti dal diritto dell'Unione o degli Stati membri;

l) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente art. 9. A tale riguardo, il Responsabile si impegna a tenere aggiornato il registro dei trattamenti dei dati personali effettuati ai sensi del presente Accordo, mettendolo a disposizione del Titolare in caso di sua richiesta, all'ordinata e diligente tenuta della documentazione inerente le attività di trattamento e la prestazione dei servizi di cui all'Accordo, rendendola accessibile al Titolare o ai soggetti da questi designati per eventuali ispezioni. Con un preavviso minimo di 24 (ventiquattro) ore - non dovuto in caso di violazioni di dati personali -, il Titolare potrà disporre un accesso presso la sede del Responsabile o altro luogo nella disponibilità giuridica del Responsabile in cui sia conservata la documentazione relativa alle attività di trattamento, sostenendone i relativi costi e dando preventiva comunicazione al Responsabile delle generalità

dei soggetti incaricati delle verifiche. I costi delle verifiche di cui al presente articolo saranno addebitati al Responsabile qualora, all'esito delle stesse, risulti un grave inadempimento agli obblighi di cui al presente Accordo;

m) informare il Titolare qualora, ad avviso del Responsabile, un'istruzione impartita dal Titolare sia in violazione del Regolamento o di altre disposizioni di legge applicabili in materia di protezione dei dati personali;

n) tenere aggiornato il registro dei trattamenti dei dati personali effettuati ai sensi del presente Accordo, mettendolo a disposizione del Titolare in caso di sua richiesta nonché delle Autorità di controllo;

o) laddove applicabile, adempiere alle prescrizioni impartite dal Garante per la protezione dei dati personali relativamente alle attribuzioni di amministratore di sistema, con il Prov. del 27.11.2008. Il Responsabile si impegna, in particolare, a nominare gli amministratori di sistema e verificare le attività svolte dagli stessi, in modo da assicurarne la conformità con gli obblighi di cui alla nomina prevista dal presente articolo 9;

p) ove applicabile, fornire agli Interessati l'informativa predisposta dal Titolare;

q) non comunicare a terzi, salvo quanto previsto dall'art. 3 ovvero in caso di consenso espresso in forma scritta del Titolare, i dati personali oggetto di trattamento;

r) se richiesto, curare, di concerto con il Titolare, i rapporti con le Autorità di controllo in materia di protezione dei dati personali, anche nell'ambito di procedimenti amministrativi e giurisdizionali inerenti l Titolare;

s) rispettare quanto prescritto dal Regolamento sulla raccolta del consenso informato degli Interessati, al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale nonché solo ed esclusivamente per le finalità e secondo le modalità operative indicate dal Titolare fornite dagli Interessati, per conto del Titolare, idonea informativa nel rispetto delle istruzioni ricevute, prima che il trattamento abbia inizio.

8.3. Il Responsabile può ricorrere a uno o più sub-responsabili (di seguito, "**Sub-Responsabile**") per l'esecuzione del presente Accordo in virtù di un contratto che disciplini i rapporti tra Responsabile e Sub-Responsabile. Resta ferma la piena e integrale responsabilità del Responsabile nei confronti del Titolare, in caso di inadempimento del Sub-Responsabile agli obblighi previsti nel presente Accordo.

8.4. Il Responsabile si obbliga a manlevare e a tenere indenne il Titolare da qualsiasi danno, pregiudizio, costo, spesa (incluse le spese legali), sanzione o qualsivoglia altro onere derivante da pretese o azioni giudiziarie, arbitrali o amministrative da parte di qualsiasi terzo, per effetto di violazioni del presente articolo 8.

8.5. Le Parti si impegnano a modificare, negoziando in buona fede, l'assetto privacy descritto nel precedente comma 8.1. e 8.2 qualora il loro rapporto, sotto il profilo del trattamento dei dati, dovesse andare incontro a modifiche successive alla sottoscrizione del presente Accordo.

Art. 9 - Ispezioni e verifiche

9.1 L'Ente Emettitore ha la facoltà di effettuare, anche attraverso soggetti da essa incaricati, verifiche presso InfoCert, in modalità self-assessment e/o audit on-site, allo scopo di accertare il rispetto delle misure

di sicurezza e di trattamento dei dati personali, nonché verificare il puntuale rispetto delle previsioni della presente Convezione e dei relativi Allegati ("**Audit**").

9.2 In caso di Audit, InfoCert si impegna sin da ora a collaborare con l'Ente Emettitore e con i soggetti da questa incaricati, fornendo senza ritardo tutte le informazioni richieste e illustrando i processi della propria organizzazione. L'Ente Emettitore, a fronte di criticità emerse in fase di Audit, si riserva di esercitare, a propria discrezione, il diritto di richiedere ulteriori approfondimenti, eseguiti anche eventualmente da parte di società terze specializzate, per le finalità del presente Accordo.

9.3 Nel caso in cui l'Ente Emettitore rilevi, all'esito degli accertamenti a proprio insindacabile giudizio, che InfoCert non si sia attenuto a quanto stabilito nel presente Accordo, InfoCert si impegna ad uniformarsi alle indicazioni ed alle istruzioni comunicate dall'Ente Emettitore con diffida ad adempiere ex art. 1454 c.c., entro i tempi indicati dalla stessa. Decorso inutilmente il congruo termine imposto dall'Ente Emettitore, quest'ultimo potrà recedere dal presente Accordo, ai sensi dell'art. 5, con un preavviso di 60 giorni.

9.4 InfoCert si impegna, a favore dell'Ente Emettitore nonché dell'Autorità di vigilanza, a garantire l'accesso alla propria sede legale e alle sedi operative, oltre ai propri server, database ecc., utilizzati per l'erogazione del Servizio/Software, per verifiche ispettive in relazione al presente Accordo.

9.5 InfoCert garantisce analogo accesso da parte dell'Ente Emettitore anche per i propri eventuali subappaltatori, subfornitori, fornitori e consulenti esterni al fine di assicurarne la conformità alla normativa applicabile ed alle condizioni contrattuali.

9.6 Ogni Audit sarà effettuato con un ragionevole preavviso scritto, in ogni caso non inferiore a 10 (dieci) giorni lavorativi, salvo che vi siano ragioni di emergenza o di effettività dell'ispezione che non consentano di rispettare tale termine.

9.7 Ciascun Audit avrà una durata massima di 3 (tre) giorni lavorativi. In particolare, InfoCert accetta che il suddetto diritto di Audit possa essere esercitato a titolo gratuito, durante un anno solare, limitatamente alle prime 3 (tre) giornate in cui le verifiche saranno messe in atto. In caso di durata maggiore, ancorché dietro richiesta dell'Autorità di Vigilanza, le Parti concorderanno in buona fede un corrispettivo per InfoCert, proporzionato all'impiego di tempo e risorse.

9.8 Le attività di Audit possono essere utilizzate avvalendosi di:

a. verifiche congiunte di Audit organizzate unitamente ad altri clienti di InfoCert ed eseguite anche da un soggetto terzo nominato dai clienti stessi, al fine di utilizzare in modo più efficiente le risorse di Audit e ridurre gli oneri organizzativi sia per i clienti sia per InfoCert;

b. certificazioni di soggetti terzi e relazioni di soggetti terzi o dell'Audit interno messe a disposizione da InfoCert.

9.9 L'Ente Emettitore a seguito di accessi e/o ispezioni e/o audit presso InfoCert può ottenere copia della documentazione pertinente coperta da riservatezza e con il divieto di condivisione della stessa verso terze parti che non siano state autorizzate per iscritto da InfoCert.

Art. 10 - Disposizioni finali

10.1 Il presente Accordo è soggetta a registrazione solo in caso d'uso, ai sensi dell'art. 5 del D.P.R. 131/1986, in quanto le prestazioni ivi previste, ove determinative di corrispettivo, sono soggette ad I.V.A.

10.2. Le informazioni concernenti la registrazione sono conservate da InfoCert per conto dell'Ente Emettitore nel proprio sistema di conservazione, in modo conforme al Codice dell'Amministrazione Digitale (CAD)[3].

10.3. Nel caso di cessazione dell'attività di certificazione, InfoCert comunicherà questa intenzione all'AgID, con un anticipo di almeno 3 (tre) mesi, indicando, eventualmente, il certificatore sostitutivo, il depositario del registro dei certificati e della relativa documentazione. Con pari anticipo, InfoCert informa della cessazione delle attività tutti i possessori di certificati da esso emessi. Nella comunicazione, nel caso in cui non sia indicato un certificatore sostitutivo, sarà chiaramente specificato che tutti i certificati non ancora scaduti al momento della cessazione delle attività della CA saranno revocati.

10.4. Salvo che, per determinate ipotesi, sia diversamente previsto, le comunicazioni formali concernenti il presente Accordo possono avvenire solo a mezzo PEC, ai seguenti indirizzi:

a) per InfoCert - PEC: infocert@legalmail.it; Indirizzo: InfoCert S.p.A. - Piazzale Flaminio 1/B - 00196 – Roma;

b) Per l'Ente Emettitore – PEC: protocollo@pec.provincia.padova.it; indirizzo: Provincia di Padova -piazza Bardella 2 CAP 35131 Padova

10.5. La modifica dei suddetti recapiti deve avvenire, a pena di nullità, esclusivamente per iscritto e con le medesime modalità di cui all'art. 10.4.

Art. 11 - Legge applicabile e foro competente

11.1. Il presente Accordo è soggetto alla legge italiana.

11.2. Le Parti si impegnano a risolvere, in via amichevole e bonaria, qualsiasi controversia dovesse insorgere in ordine alla medesima, comprese quelle relative alla validità, interpretazione, esecuzione e risoluzione della stessa Qualora ciò non sia possibile o il tentativo non sia andato a buon fine, la controversia sarà devoluta in via esclusiva al Tribunale di Padova.

11.3. È escluso il ricorso all'arbitrato.

Luogo e data

Ente Emettitore **InfoCert S.p.A.**

[3] Decreto legislativo 7 marzo 2005, n. 82; successivamente modificato e integrato con il decreto legislativo 22 agosto 2016 n. 179; successivamente modificato e integrato con il decreto legislativo 13 dicembre 2017 n. 217.

ACCORDO PER NOMINA DELLA PROVINCIA DI PADOVA A R.A. ("REGISTRATION AUTHORITY") E PER LO SVOLGIMENTO DELLE ATTIVITÀ DI UFFICIO DI REGISTRAZIONE

Premesse

- Tra la Provincia di Padova, in qualità di Ente Emettitore (di seguito anche solo "Provincia") e InfoCert S.p.a. (di seguito anche solo "InfoCert"), in qualità di CA (Certification Authority) è stipulato un Accordo – avente durata di anni 6 con decorrenza dal 1.1.2026 e scadenza al 31.12.2031 – per lo svolgimento di Attività di Ufficio di Registrazione e rilascio dei servizi di certificazione digitale, in particolare CNS (Carta Nazionale dei Servizi) e firma digitale, come da determina dirigenziale n._____ del_____ (prot.n. _____del_____), alla quale le parti si richiamano integralmente per ogni aspetto non specificamente disciplinato dal presente accordo.
- In particolare, con la predetta Intesa, la Provincia, quale Ente Emettitore, conferisce ad InfoCert mandato non esclusivo a espletare la funzione di Certification Authority e a svolgere funzione di rilascio di CNS, in qualità di Ufficio di Registrazione anche mediante certificato di sottoscrizione svolto da remoto.
- La Provincia già svolge, sulla base di un precedente accordo, per conto di InfoCert le operazioni di raccolta dei dati relativi ai richiedenti i Certificati, la loro identificazione, nonché il successivo eventuale rilascio del Certificato emesso da InfoCert, in qualità di Ufficio di Registrazione.
- La Provincia e InfoCert stipulano il presente accordo al fine di disciplinare le Attività necessarie all'attivazione del servizio di certificazione predetto agli utenti che ne facciano richiesta (gli "Utenti" o "Richiedenti") e riconoscono nell'Ufficio di Registrazione il soggetto che esegue le operazioni di autenticazione, identificazione, raccolta e conservazione dei dati relativi ai Richiedenti i certificati di sottoscrizione e di autenticazione.
- Come meglio dettagliato nel prosieguo, la Provincia di Padova, per svolgere la propria Attività di Registration Authority, si avvale, quale RAO (Operatori della Registrazione), unicamente di personale qualificato interno, cui si impegna a far sottoscrivere idoneo mandato.

Ciò premesso, le parti convengono quanto segue:

* * *

1.1 Oggetto

1.1.1 Ad integrazione del citato Accordo, InfoCert, nel suo ruolo di Autorità di Certificazione ("**CA**") e di gestore dell'identità digitale ("**IdP**") ai sensi del D.P.C.M. 24.10.2014 nonché di prestatore di servizi fiduciari accreditato presso l'Agenzia per l'Italia Digitale ("**AgID**"), ai fini dell'emissione dei propri Servizi è tenuta ad effettuare l'Attività di identificazione degli Utenti, ferma restando la facoltà di delegare tali Attività anche a soggetti terzi, ai sensi dell'art. 24 del Regolamento (UE) n. 910/2014 come modificato dal Regolamento (UE) n. 1183/2024 ("**Regolamento eIDAS**").

1.1.2 A tal fine, InfoCert – effettuate le necessarie verifiche e constatatane la competenza e l'adeguata struttura organizzativa oltre che la citata pregressa positiva esperienza collaborativa nello svolgimento delle medesime Attività – nomina la Provincia di Padova quale Ufficio di Registrazione (anche "**Registration Authority**" o, per brevità, "**RA**"), per l'esecuzione delle Attività di seguito identificate nel rispetto degli obblighi specifici del presente accordo correlati al ruolo di RA e dei Manuali Operativi in vigore, nonché dei provvedimenti legislativi e amministrativi ivi richiamati.

1.1.3 InfoCert metterà a disposizione della Provincia di Padova quale RA – Ufficio di Registrazione –l'accesso ad una piattaforma dedicata ("**Piattaforma**"), propedeutica al caricamento e alla gestione di tutta la documentazione afferente al rapporto in essere con la RA medesima, quale, a titolo meramente esemplificativo e non esaustivo, i mandati necessari per lo svolgimento dell'Attività da parte dei propri dipendenti e/o collaboratori;

1.1.4 InfoCert, inoltre, metterà a disposizione della Provincia di Padova tutta la tecnologia e la sovrastruttura informatica necessaria per consentire all'Ente, di svolgere al meglio l'Attività di Ufficio di Registrazione, così come meglio specificato al successivo punto 1.4.

1.1.5 Con la sottoscrizione del presente Accordo la Provincia di Padova viene nominata quale RA di InfoCert, per l'erogazione della CNS e del servizio di Firma Digitale ovvero di SPID e/o ogni altro servizio Digital Trust che le parti riterranno opportuno nell'ambito dell'Accordo in essere e del ruolo svolto dalla Provincia di Padova come Ente Emettitore.

1.2 Servizi oggetto delle Attività

1.2.1 Le Attività svolte dalla RA sono propedeutiche all'identificazione certa degli Utenti, anche qualora ne facciano richiesta per il tramite di altri soggetti ("**Richiedenti**"), che hanno interesse ad usufruire dei servizi InfoCert come meglio infra descritti.

1.2.2 I servizi per la cui emissione ("**Servizi Trust**") è necessario l'espletamento delle Attività di RA, durante le quali vengono acquisiti i dati forniti dall'Utente, sono i seguenti:

a) Rilascio CNS (Carta Nazionale dei Servizi);
b) Certificato qualificato, la cui emissione è propedeutica al rilascio di una firma elettronica qualificata, ("**Certificato/i**"), intendendosi per tale "*l'insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la chiave pubblica del soggetto certificato*";
c) Credenziali SPID, ossia le credenziali necessarie per il rilascio dell'identità digitale ("**Identità Digitale**" o "**SPID**"), per l'accesso ai servizi in rete erogati dai fornitori che aderiscono al sistema SPID.

1.2.3 Le procedure di identificazione e registrazione sono esposte, rispetto al Certificato, nel Manuale Operativo ICERT-INDI-MO e ss.mm.ii. ("**Manuale Operativo Certificati**") e, rispetto al rilascio di Credenziali SPID, nel Manuale ICERT-MO-SPID e ss.mm.ii. ("**Manuale Operativo SPID**"), entrambi depositati presso l'AgID, e disponibili sul sito internet di InfoCert nell'ultima versione aggiornata, nonché sono esposte nei provvedimenti legislativi e amministrativi richiamati nei Manuali stessi (congiuntamente, "**Manuali**" o "**Manuali Operativi**").

1.2.4 La RA svolgerà le Attività secondo una o più modalità di identificazione tra quelle previste all'interno dei Manuali e/o secondo le procedure di volta in volta definite con InfoCert.

1.3 Responsabilità e Obblighi dell'Ufficio di Registrazione

1.3.1 Per l'esercizio delle Attività ad esso demandate, l'Ufficio di Registrazione si avvarrà esclusivamente di propri dipendenti e collaboratori a vario titolo appositamente incaricati quali Operatori di Registrazione ("**Registration Authority Officer**", per brevità "**R.A.O.**"), per i quali l'Ufficio di Registrazione si impegna a far sottoscrivere idoneo mandato.

1.3.2 Il rapporto tra InfoCert e l'Ufficio di Registrazione sarà disciplinato esclusivamente dal presente accordo.

1.3.3 Ferma la responsabilità di InfoCert per quanto concerne l'erogazione dei Servizi, l'Ufficio di Registrazione si impegna a:

a) rispettare le procedure operative (anche di rinnovo, revoca o sospensione dei Servizi Trust) definite con InfoCert;
b) esercitare le Attività nell'interesse di InfoCert con la diligenza del mandatario, ex art. 1710, c.c.;
c) far sottoscrivere ai propri R.A.O. idoneo mandato, secondo il modello allegato al presente accordo sub a);
d) informare tempestivamente InfoCert di eventuali vizi, difetti, interruzioni o malfunzionamenti del sistema;
e) se necessario, in conseguenza delle problematiche riscontrate sub c), consentire agli incaricati di InfoCert di accedere nei propri locali per prestare idonea assistenza;
f) fornire evidenza, nelle tempistiche assegnate, della documentazione relativa alle Attività di RA, qualora la richiesta derivi da un'Autorità di vigilanza, dalla Polizia Giudiziaria e/o da altra Autorità preposta ovvero da InfoCert stessa ai fini delle Attività di verifica e controllo obbligatorie poste in essere da quest'ultima nell'ambito della propria operatività;
g) sottoporre ai Richiedenti, siano esse persone fisiche o giuridiche che richiedono l'emissione dei Servizi Trust per conto dell'Utente, la documentazione contrattuale messa a disposizione da InfoCert, nonché concordare preventivamente con quest'ultima qualsiasi documento da rilasciare al Richiedente e/o Utente, relativamente alle Attività di registrazione e/o di rilascio dei Servizi Trust;
h) mantenere strettamente riservate le credenziali ricevute da InfoCert per l'accesso alla Piattaforma e fornirle esclusivamente ai propri dipendenti/collaboratori interni, nonché ad utilizzare correttamente la Piattaforma, nelle modalità concordate con InfoCert, anche per l'eventuale caricamento/aggiornamento di documentazione;

1.3.4 L'Ufficio di Registrazione prende atto e accetta che non potrà vantare alcuna esclusiva per l'esercizio delle suddette Attività per conto di InfoCert; quest'ultima sarà pertanto libera di delegare tali Attività anche ad altri soggetti.

1.4 Obblighi di InfoCert

1.4.1 InfoCert si impegna nei confronti dell'Ufficio di Registrazione a:

a) fornire le eventuali apparecchiature hardware e software necessarie per l'espletamento delle Attività, oltre che le indicazioni sul loro corretto utilizzo;
b) impartire la formazione necessaria a svolgere le Attività, tramite corsi e documentazione *ad hoc*;
c) aggiornare periodicamente, con una cadenza concordata e/o comunque qualora fossero modificati i disciplinari operativi delle Attività di RA e RAO, mediante opportuni corsi di formazione specifica;
d) dare consulenza e assistenza sulle problematiche connesse all'espletamento delle Attività;
e) svolgere con periodicità annuale le verifiche di sicurezza e di qualità dei Servizi Trust offerti;
f) conservare le informazioni concernenti l'identificazione, la registrazione ed emissione dei Certificati, sul proprio sistema di conservazione, ai sensi delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti*", emanate da AgID con determinazione n. 407 del 2020 e ss.mm.ii., per 20 (venti) anni dalla scadenza di ogni Certificato;
g) conservare le informazioni concernenti la fase di identificazione e la documentazione contrattuale sottoscritta dagli Utenti, nel proprio sistema di conservazione, conformemente al DPCM 23.10.2014 e ss. mm. ii., per 20 (venti) anni decorrenti dalla scadenza o dalla revoca dell'Identità Digitale. L'Ufficio di Registrazione può accedervi, formulando specifica richiesta scritta.

1.5 Limitazioni e responsabilità

1.5.1 L'Ufficio di Registrazione nell'espletamento delle Attività osserverà le indicazioni fornite da InfoCert per l'utilizzo delle risorse strumentali messe a disposizione dalla stessa. Nel caso in cui InfoCert rilevi eventuali anomalie o irregolarità nello svolgimento delle Attività da parte della RA verranno avviate Attività di audit e/o confronto con l'Ufficio di Registrazione per avere gli opportuni chiarimenti.

1.6 Corrispettivi

1.6.1 Per lo svolgimento delle Attività, l'Ufficio di Registrazione non potrà vantare il pagamento di somme, corrispettivi, provvigioni o quant'altro da parte di InfoCert, salvo quanto già previsto nel citato Accordo o in altro accordo separato stipulato fra le parti.

1.7 Privacy

1.7.1 Per le finalità del presente incarico, InfoCert, in qualità di Titolare autonomo del trattamento ai sensi dell'art. 8.1.b) dell'Accordo per lo svolgimento di attività di Certification Authority e Ufficio di Registrazione per il rilascio della Cart Nazionale dei Servizi, nomina la Provincia di Padova Responsabile esterno ex art 28 GDPR, come dettagliato di seguito.

1.7.2 Fatti salvi gli obblighi previsti dalle disposizioni di legge e regolamentari applicabili, il Responsabile si obbliga a:

a) trattare i dati personali soltanto sulla base del presente Accordo e di ogni altra istruzione impartita dal Titolare ai sensi dello stesso;
b) garantire, per conto delle persone autorizzate al trattamento dei dati personali, l'obbligo di riservatezza in merito a tutte le informazioni e i dati acquisiti in esecuzione del presente Accordo;
c) designare le persone fisiche autorizzate al trattamento (ossia i propri dipendenti) e conferire loro, in forma scritta, l'incarico di compiere le operazioni di trattamento nonché le medesime istruzioni impartite dal Titolare al Responsabile sulla base del presente contratto, istruirle sulle modalità di elaborazione dei dati ai quali hanno accesso e vigilare sul loro operato; comunicare al Titolare, su richiesta di quest'ultimo, i nominativi delle persone autorizzate;
d) adottare tutte le misure di sicurezza richieste ai sensi dell'art. 32 GDPR;
e) assistere il Titolare con misure tecniche e organizzative adeguate, per l'adempimento degli obblighi connessi all'esercizio dei diritti degli Interessati, ivi inclusi i diritti alla limitazione del trattamento e alla portabilità dei dati;
f) assistere il Titolare nell'adempimento degli obblighi in materia di misure di sicurezza tecniche ed organizzative di cui all'art. 32 GDPR così come individuate di volta in volta dal medesimo Titolare, ivi incluse, a titolo meramente esemplificativo, le seguenti: pseudo-anonimizzazione e/o cifratura dei dati personali; resilienza dei sistemi e dei servizi di trattamento; capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente

fisico o tecnico; procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

g) assistere il Titolare nell'adempimento degli obblighi in materia di notificazione dei dati personali di cui agli artt. 33 e 34 GDPR e, in particolare, informare il Titolare della eventuale violazione di dati personali entro e non oltre 24 (ventiquattro) ore decorrenti dal momento della scoperta della violazione stessa;
h) assistere il Titolare nelle attività connesse alla valutazione d'impatto sulla protezione dei dati personali di cui all'art. 35 GDPR e, se richiesto, cooperare con il Titolare nell'ambito delle consultazioni preventive di cui all'art. 36 GDPR
i) cancellare o restituire - a scelta del Titolare - tutti i dati personali oggetto di trattamento in caso di cessazione dell'efficacia del presente Contratto, salvi gli obblighi di conservazione dei dati eventualmente derivanti dal diritto dell'Unione o degli Stati membri;
j) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo. Con un preavviso minimo di 24 (ventiquattro) ore - non dovuto in caso di violazioni di dati personali -, il Titolare potrà disporre un accesso presso la sede del Responsabile o altro luogo nella disponibilità giuridica del Responsabile in cui sia conservata la documentazione relativa alle attività di trattamento, sostenendone i relativi costi e dando preventiva comunicazione al Responsabile delle generalità dei soggetti incaricati delle verifiche;
k) informare il Titolare qualora, ad avviso del Responsabile, un'istruzione impartita dal Titolare sia in violazione del Regolamento o di altre disposizioni di legge applicabili in materia di protezione dei dati personali;
l) tenere aggiornato il registro dei trattamenti dei dati personali effettuati ai sensi del presente Contratto e dell'Accordo, mettendolo a disposizione del Titolare in caso di sua richiesta;
m) laddove applicabile, adempiere alle prescrizioni impartite dal Garante per la protezione dei dati personali relativamente alle attribuzioni di amministratore di sistema, impegnandosi, in particolare, a nominare gli amministratori di sistema, vigilando sulla correttezza del relativo operato.

1.7.3 Il Responsabile non può ricorrere a Sub-Responsabili per l'esecuzione del presente contratto, senza preventiva autorizzazione da parte del Titolare;

1.7.4 La presente nomina è efficace dal momento della sottoscrizione dell'Accordo e cessa allo scadere dello stesso, fatti salvi eventuali obblighi di legge o regolamentari

1.8 Durata e decorrenza. Risoluzione e recesso.

1.8.1 Il presente Accordo di nomina avrà durata pari a quella dell'Intesa fra le medesime parti citata in premesse a cui afferisce e di cui costituisce parte integrante e ha pertanto validità per il periodo 1 gennaio 2026-31 dicembre 2031, anche per quanto concerne i casi sospensione, recesso e/o revoca.

1.9 Legge applicabile e Foro competente

1.9.1 Il presente Accordo è soggetto alla legge italiana. Le Parti si impegnano a risolvere, in via amichevole e bonaria, qualsiasi controversia dovesse insorgere in ordine al medesimo. Qualora ciò non sia possibile o il tentativo non sia andato a buon fine, la controversia sarà devoluta in via esclusiva al Tribunale di Padova.

Allegati:

1) Mandato R.A.O.

Luogo _____, data _____

Per la PROVINCIA di PADOVA

Per INFOCERT SPA

MANDATO TRILATERALE PER LO SVOLGIMENTO DI ATTIVITA' DA PARTE DEL R.A.O. PER IL RILASCIO DI SERVIZI TRUST DI INFOCERT

Tra

InfoCert S.p.A., con sede legale in Roma, Piazzale Flaminio 1/B, CF e P. IVA 07945211006, in persona dell'Amministratore Delegato e legale rapp.te *pro-tempore* dott. Danilo Cattaneo, società soggetta a direzione e coordinamento di Tinexta S.p.A. (di seguito "**InfoCert**")

e

XXXX, con sede in _____ n. _____, CF e P. IVA _____, in persona del legale rappresentante *pro tempore* _____ munito dei necessari poteri, come dichiara e garantisce (di seguito, anche "**Ufficio di Registrazione**" o "**R.A.**")

e

XXXX, residente in _____ n. _____, CF _____, (di seguito, "**Operatore dell'Ufficio di Registrazione"** o "**R.A.O.**")

PREMESSO CHE:

a) L'Ufficio di Registrazione ed InfoCert, in data _____ hanno stipulato apposita intesa (di seguito "**Accordo"**), con la quale è stato conferito mandato alla prima di svolgere le funzioni di Ufficio di Registrazione, per il rilascio dei Certificati di firma, secondo quanto previsto dal Manuale Operativo ICERT-INDI-MO (di seguito il "**Manuale Operativo Certificati**") e/o per il rilascio dello SPID secondo quanto previsto dal Manuale Operativo ICERT-MO-SPID **("Manuale Operativo SPID")**;
b) ai sensi dell'Accordo, la R.A. ha facoltà di operare anche attraverso propri Operatori dell'Ufficio di Registrazione, che si impegneranno ad osservare gli obblighi meglio dettagliati nel prosieguo;
c) con il presente atto, si desidera conferire all'Operatore dell'Ufficio di Registrazione apposito mandato per l'esecuzione delle attività di sua competenza, concernenti le fasi identificazione, autenticazione, registrazione e revoca degli utenti (gli "**Utenti**"), nonché quelle di emissione, revoca e sospensione dei certificati e consegna del dispositivo ("**Servizi Trust**"), ai sensi del Manuale Operativo;
d) l'Operatore dell'Ufficio di Registrazione si è reso disponibile a svolgere le attività elencate al punto precedente e meglio dettagliate nel presente atto (il "**Mandato**");
e) le procedure di registrazione sono analiticamente esposte nel Manuale Operativo di InfoCert sopra citato, pubblicato sul sito Internet "*www.infocert.it"*, e nei provvedimenti legislativi e amministrativi eventualmente ivi richiamati.

TUTTO CIO' PREMESSO, e Parti convengono quanto segue:

1. PREMESSE

1.1. Le premesse, nonché il PDS e il Manuale Operativo Certificati e Manuale Operativo SPID disponibili sul sito InfoCert (https://www.firma.infocert.it/documentazione/) formano parte integrante del presente Mandato che sarà espletato secondo le specifiche condizioni ivi previste.

2. OGGETTO

2.1. InfoCert e la R.A. conferiscono mandato non esclusivo all'Operatore dell'Ufficio di Registrazione a svolgere parte dell'attività di cui alla lett. c) delle premesse e, in particolare, a identificare gli Utenti con certezza, esclusivamente attraverso sistemi autorizzati da InfoCert e secondo le modalità concordate da InfoCert e dalla R.A.

3. OBBLIGHI DELLE PARTI

3.1. La R.A., ferme rimanendo le obbligazioni di cui all'Accordo, provvederà a:

a) supervisionare, per conto di InfoCert, l'attività di formazione e/o aggiornamento dei R.A.O.;
b) verificare che gli Operatori dell'Ufficio di Registrazione eseguano con la dovuta diligenza le attività a loro assegnate;
c) monitorare costantemente che gli Operatori dell'Ufficio di Registrazione mantengano i requisiti di competenza, affidabilità, onorabilità ed esperienza ai sensi dell'art. 24 par. 2 lett. b) del Regolamento eIDAS;
d) assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniqualvolta venga revocato il Mandato da InfoCert o dalla R.A., qualora cessi il rapporto di dipendenza/collaborazione tra l'Ufficio di Registrazione e il R.A.O., ovvero si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del R.A.O.), dandone tempestiva comunicazione per iscritto ad InfoCert entro 24 (ventiquattro) ore lavorative;
e) fornire i beni ed i materiali ai R.A.O. da consegnare agli Utenti.

3.2 L'Operatore dell'Ufficio di Registrazione, con la diligenza del mandatario *ex* art. 1710, c.c., dovrà:

a) conseguire la formazione necessaria per le finalità del presente mandato, partecipando ai corsi di formazione come predisposti dal R.A. ai sensi dell'art. 3.1 lett. a);
b) prendere visione delle istruzioni contenute nei Manuali Operativi, nell'ultima versione tempo per tempo disponibile online sul sito di InfoCert, e garantire di possedere e mantenere in essere requisiti di onorabilità e professionalità necessari all'esercizio delle Attività;
c) rispettare le procedure operative di rinnovo, revoca o sospensione dei Servizi Trust definite da InfoCert;
d) esercitare le Attività nell'interesse di InfoCert e con la diligenza del mandatario, ex art. 1710, c.c.;
e) svolgere le Attività nel rispetto della normativa vigente, dei Manuali Operativi e delle istruzioni ricevute da InfoCert, con particolare riferimento all'identificazione personale certa degli Utenti che richiedono l'emissione dei Servizi Trust;
f) informare entro 12 (dodici) ore InfoCert di eventuali vizi, difetti, interruzioni o malfunzionamenti del sistema e/o di errori nello svolgimento delle attività di identificazione e registrazione;
g) consentire alle Autorità di vigilanza, nonché alle R.A. di InfoCert, di accedere nei propri locali per verificare il corretto espletamento delle Attività ed il rispetto delle procedure per lo svolgimento delle stesse;
h) fornire evidenza, entro e non oltre 3 (tre) giorni dalla richiesta da parte di InfoCert, di tutta la documentazione relativa alle Attività, qualora la richiesta derivi dall'Autorità di vigilanza;
i) sottoporre agli Utenti, siano esse persone fisiche o giuridiche che richiedono l'emissione dei Servizi Trust per conto dell'Utente, la documentazione contrattuale messa a disposizione da InfoCert, nonché concordare

preventivamente con quest'ultima qualsiasi documento da rilasciare al Richiedente e/o Utente, relativamente all'attività di registrazione del Certificato e/o di rilascio dei Servizi Trust;

j) mantenere strettamente riservate le credenziali ricevute da InfoCert per l'accesso alla piattaforma dedicata, propedeutica al caricamento e alla gestione di tutta la documentazione afferente al ciclo-vita della R.A. ("**Piattaforma**");
k) obbligarsi ad un corretto utilizzo della Piattaforma, nelle modalità indicate da InfoCert;
l) provvedere ad un regolare caricamento/aggiornamento sulla Piattaforma di tutta la documentazione richiesta da InfoCert (a titolo meramente esemplificativo e non esaustivo: mandati, modulistica dei Servizi Trust), che dovrà essere fornita a quest'ultima entro i termini con essa convenuti, e in ogni caso qualora InfoCert ne faccia espressa richiesta.

3.3. L'Operatore dell'Ufficio di Registrazione e la R.A. saranno solidalmente responsabili nei confronti di InfoCert per le attività previste nel presente Mandato.

3.4. La violazione di uno qualsiasi degli obblighi di cui al comma 3.2. e 3.3 del presente articolo costituirà giusta causa di revoca del presente Mandato da parte di InfoCert o della R.A., che sarà esercitata a mezzo di apposita comunicazione, fatto salvo il diritto al risarcimento dei danni eventualmente subiti e *subendi*. In caso di revoca, l'Operatore dell'Ufficio di Registrazione è obbligato a cessare qualsiasi attività posta in essere in base al presente atto ed a restituire i materiali ricevuti al fine dell'espletamento dell'incarico.

4. CORRISPETTIVI E FORNITURA

4.1. L' Operatore dell'Ufficio di Registrazione e la R.A. per lo svolgimento dell'attività prevista nel Mandato non potranno pretendere il pagamento di alcun corrispettivo da parte di InfoCert né vantare alcuna esclusiva nei suoi confronti.

4.2. L'esclusione di cui al precedente comma è altresì valida con riferimento ai mezzi necessari per l'esecuzione del Mandato e alle anticipazioni e spese sostenute dal mandatario.

5. DURATA E DECORRENZA

5.1. Il Mandato avrà efficacia per il periodo di un anno dalla data della sua sottoscrizione e si rinnoverà tacitamente per periodi annuali, salvo disdetta di una delle Parti, da comunicarsi per iscritto almeno 3 (tre) mesi prima della scadenza del periodo annuale, a mezzo Posta Elettronica Certificata o lettera raccomandata A/R. Il Mandato perderà automaticamente efficacia, in ogni caso di cessazione dell'Accordo in essere tra InfoCert e la R.A..

5.2. Durante il periodo di vigenza del Mandato, InfoCert avrà diritto, senza pagamento di alcun corrispettivo, di recedere da esso in qualsiasi momento, con comunicazione della volontà di esercitare tale diritto a mezzo Posta Elettronica Certificata o raccomandata A/R.

5.3. In caso di recesso e/o revoca, l'Operatore dell'Ufficio di Registrazione non potrà vantare alcuna richiesta nei confronti della R.A. e/o di InfoCert, neanche per eventuali danni subiti in conseguenza dello stesso.

5.4. Resta salvo tra le Parti che in caso di risoluzione del presente Mandato, l'Accordo rimane valido ed efficace tra InfoCert e la R.A. fino a naturale vigenza della stessa.

6. PRIVACY

6.1. La R.A. e l'Operatore dell'Ufficio di Registrazione si impegnano alla piena osservanza, per quanto di rispettiva competenza, del dettato del Regolamento (UE) 679/2016 e della normativa italiana compatibile con lo stesso.

6.2. Nell'espletamento del mandato, l'Operatore dell'Ufficio di Registrazione sarà autorizzato al trattamento dei dati per lo svolgimento delle sole attività oggetto del presente Mandato, sotto la diretta autorità della R.A. e InfoCert attenendosi alle istruzioni impartite da quest'ultima.

6.3. In particolare, l'Operatore dell'Ufficio di Registrazione metterà in atto le seguenti operazioni di trattamento:

a) verifica del documento di identità del richiedente, della relativa validità e della corrispondenza al soggetto richiedente;
b) trascrizione o verifica (in base alle indicazioni fornite in sede di formazione) delle informazioni inerenti alla persona fisica del richiedente;
c) produzione della documentazione che attesta l'avvenuto riconoscimento dell'Utente;
d) raccolta dei documenti firmati, se applicabile sulla base della procedura di identificazione messa in atto.

7. LEGGE APPLICABILE E FORO COMPETENTE

7.1. Il presente Mandato è soggetto alla legge italiana.

7.2. Le Parti si impegnano a risolvere, in via amichevole e bonaria, qualsiasi controversia dovesse insorgere in ordine alla medesima, comprese quelle relative alla validità, interpretazione, esecuzione e risoluzione della stessa. Qualora ciò non sia possibile o il tentativo non sia andato a buon fine, la controversia sarà devoluta in via esclusiva al Tribunale di Padova.

Luogo _____, data _____

InfoCert S.p.A.	Ufficio di Registrazione	Operatore dell'Ufficio di Registrazione
_____	_____	_____

Si intendono espressamente approvati ai sensi e per gli effetti degli artt. 1341 e 1342, c.c., i seguenti articoli: 3 (Obblighi delle Parti); 4 (Corrispettivi e fornitura); 5 (Durata e decorrenza).

_____

(Ufficio di Registrazione)

_____

(Operatore dell'Ufficio di Registrazione)

Provincia di Padova

MANUALE OPERATIVO

Emissione Carta Nazionale dei Servizi

CODICE DOCUMENTO	01/2025
VERSIONE	4.0
DATA	30/06/2025

tinexta infocert

Sommario

Questa pagina è lasciata intenzionalmente bianca.

1 NOVITÀ INTRODOTTE RISPETTO ALLA PRIMA EMISSIONE

***Versione**:*	*1.0*	***Data Versione/Release**:*	*15/04/2013*
Descrizione modifiche:	*Nessuna*		
Motivazioni:	*Prima emissione*		

***Versione**:*	*2.0*	***Data Versione/Release**:*	*15/05/2018*
Descrizione modifiche:	*riferimenti normativi, dati dei responsabili, operatività (identificazione)*		
Motivazioni:			

***Versione**:*	*3.0*	***Data Versione/Release**:*	*15/05/2025*
Descrizione modifiche:	*riferimenti normativi, responsabilità, dati dei responsabili, loghi*		
Motivazioni:			

***Versione**:*	*4.0*	***Data Versione/Release**:*	***30/06/2025***
Descrizione modifiche:	*modifiche ad adeguamento del nuovo testo di Accordo*		
Motivazioni:			

2 SCOPO E CONTENUTO DEL DOCUMENTO

Il presente documento contiene le regole e le procedure operative che governano l'emissione della Carta Nazionale dei Servizi (CNS) e dei relativi certificati emessi dal Certificatore InfoCert, Trust Service Provider, su affidamento dell'Ente Emettitore, Provincia di Padova.

Questo manuale indica, inoltre, le procedure da seguire in caso di smarrimento, furto o sospetta compromissione della carta.

Le indicazioni di questo documento hanno validità per le attività relative all'Ente Emettitore, per InfoCert nel ruolo di Certificatore, per gli Uffici di registrazione (RA), per i soggetti incaricati ad effettuare l'identificazione/registrazione dei Titolari e/o a consegnare i dispositivi CNS ai medesimi, per gli stessi Titolari e per gli Utenti.

Per la compilazione di questo documento si è fatto riferimento alla seguente documentazione InfoCert, reperibile sul sito www.infocert.it/documentazione:

- Manuale Operativo Certificate Policy - Certificate Practice Statement (ICERT-INDI-MO);
- Manuale Operativo per il rilascio del certificato digitale di autenticazione (ICERT-INDI-MOCA);
- InfoCert Ente Certificatore - Certificati di Autenticazione per la Carta Nazionale dei Servizi - Certificate Policy (ICERT-INDI-CPCA-CNS).

3 RIFERIMENTI NORMATIVI

- D.P.R. n. 445/2000 Testo Unico del Documento Amministrativo e successive modifiche e integrazioni;
- Decreto Legislativo 7 marzo 2005, n. 82 (G.U. n.112 del 16 maggio 2005) – Codice dell'Amministrazione Digitale (nel seguito referenziato come CAD) e successive modifiche e integrazioni, comprese le sue Regole Tecniche e Linee Guida;
- Decreto del Presidente della Repubblica 2 marzo 2004, n. 117, Regolamento concernente la diffusione della carta nazionale dei servizi;
- Regolamento UE eIDAS (electronic IDentification Authentication and Signature) - n° 910/2014, come modificato dal Regolamento n. 1183/2024;
- Regolamento UE GDPR (General Data Protection Regulation) - n° 679/2016;
- **https://www.agid.gov.it/it/piattaforme/carta-nazionale-servizi.**

3.1 Definizioni e acronimi

Campo	*Descrizione*
AgID	Agenzia per l'Italia Digitale.
CNS	Carta Nazionale dei Servizi.
CRL	Certificate Revocation List - Lista dei certificati revocati o sospesi.
DN	Distinguished Name - Identificativo del Titolare di un certificato di chiave pubblica. Tale codice è unico nell'ambito degli utenti del Certificatore.
Ente Emettitore	Ente responsabile della formazione e del rilascio della CNS. È la Pubblica Amministrazione che rilascia la CNS ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della CNS.
ERC	Emergency Request Code. Acronimo assegnato al codice di emergenza.
HTTPS	HyperText Transfer Protocol Secure
ISO	International Organization for Standardization.
IUT	Identificativo Univoco del Titolare, è un codice associato al Titolare che lo identifica univocamente presso il Certificatore. Il Titolare ha codici diversi per ogni ruolo per il quale può firmare.
LDAP	Lightweight Directory Access Protocol, protocollo utilizzato per accedere al registro dei certificati.
Lista dei Certificati Revocati o Sospesi (Certificate Revocation List – CRL)	Lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza. L'operazione è chiamata revoca se definitiva, sospensione se temporanea. Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla lista CRL.
OCSP	Online Certificate Status Protocol.
OID	Object Identifier, è costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
PIN	Personal Identification Number, codice associato alla CNS, utilizzato dall'utente per accedervi alle funzioni. Altre funzioni installate sulla CNS richiedono PIN specifici della funzione.
PUK	Codice personalizzato per ciascuna CNS, utilizzato dal Titolare per riattivare il proprio dispositivo di firma in seguito al blocco dello stesso per errata digitazione del PIN. Altre funzioni installate sulla CNS richiedono PUK specifici della funzione.
RAO	Registration Authority Officer, soggetto incaricato a verificare l'identità e, se

Campo	Descrizione
	applicabile, ogni specifico attributo di un Titolare, nonché ad attivare la procedura di certificazione per conto del Certificatore.
Revoca o sospensione di un Certificato	Operazione con cui il Certificatore annulla la validità del certificato prima della naturale scadenza. Vedi Lista dei Certificati Revocati o Sospesi - CRL.
Richiedente - Subscriber	Soggetto fisico che richiede all'Ente Emettitore il rilascio della CNS.
Titolare - Subject	Soggetto in favore del quale è rilasciata la CNS ed è identificato nel certificato digitale come il legittimo possessore della chiave privata, corrispondente alla chiave pubblica contenuta nel certificato stesso. Al Titolare stesso è attribuita la firma elettronica avanzata generata con la chiave privata della coppia.
Uffici di Registrazione (Registration Authority – RA)	Soggetto delegato che svolge le attività necessarie al rilascio dei certificati digitali e alla consegna della CNS.
Utente - Relying Party	Soggetto che riceve un certificato digitale e che fa affidamento sul certificato medesimo o sulla firma elettronica avanzata basata su quel certificato.

4 PARTECIPANTI E RESPONSABILITÀ

Un certificato digitale è l'associazione tra una chiave pubblica di crittografia ed un insieme di informazioni che identificano il soggetto che possiede la corrispondente chiave privata, chiamato anche Titolare della coppia di chiavi asimmetriche (pubblica e privata). Il certificato è utilizzato da altri soggetti (gli Utenti) per ricavare la chiave pubblica, contenuta e distribuita con il certificato, e verificare, tramite questa, il possesso della corrispondente chiave privata, identificando in tal modo il Titolare della stessa.

Il certificato garantisce la corrispondenza tra la chiave pubblica ed 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.

A tale proposito i certificati di Autenticazione CNS emessi dall'Ente Certificatore InfoCert sono emessi su richiesta diretta del Titolare, successivamente all'identificazione fisica dello stesso da parte dell'Ente Emettitore o di altro soggetto da questi delegato, e rilasciati su dispositivo sicuro di firma (Smart card o Token USB).

Il presente documento contiene le procedure operative che si attuano per l'emissione delle CNS e dei relativi Certificati di Autenticazione (in seguito anche chiamati più brevemente Certificati) sottoscritti dal Certificatore, le procedure da seguire in caso di smarrimento, furto o sospetta compromissione della CNS, ed è liberamente disponibile sul sito dell'Ente Emettitore.

4.1 Ente Emettitore

L'Ente Emettitore è, in generale, la Pubblica Amministrazione che rilascia la CNS ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della CNS. Si precisa che tali attività sono delegate dall'Ente Emettitore a soggetti terzi come l'Autorità di Certificazione e le Registration Authorities da quest'ultima incaricate. I dati completi dell'organizzazione, che svolge la funzione di Ente Emettitore, sono i seguenti:

Campo	Descrizione
Denominazione Sociale	Provincia di Padova
Sede legale	Piazza Antenore 3, 35121 Padova
Rappresentante legale	Presidente in carica “pro tempore”
Numero verde	800185017
PEC	protocollo@pec.provincia.padova.it
N° Codice Fiscale	80006510285
N° partita IVA	00700440282
Sito web	https://www.provincia.padova.it
Sito web per i servizi di certificazione digitale	https://cst.provincia.padova.it/
Supporto e assistenza	Servizio di supporto per gli utenti dei servizi C.S.T. - Centro Servizi Territoriali - Servizi Informativi (dal lunedì al venerdì delle giornate lavorative) 800.18.50.17 support@provincia.padova.it

4.2 Certification Authority – Autorità di Certificazione

La Certification Authority (CA) è il soggetto terzo e fidato che emette, pubblica nel registro e revoca i certificati ed a cui è stata delegata dall’Ente Emettitore la responsabilità della sicurezza del circuito di emissione e del rilascio della carta a soggetti terzi.

I dati completi dell’organizzazione che svolge la funzione di CA sono i seguenti:

Campo	Descrizione
Denominazione Sociale	InfoCert S.p.A. Società Soggetta alla Direzione ed al coordinamento di Tinexta S.p.A.
Sede legale	Piazzale Flaminio 1/B, 00196 – Roma (RM)
Sedi operative	Via Giandomenico Romagnosi 4, 00196 – Roma (RM) Via Fernanda Wittgens 2, 20123, Milano (MI) Piazza Luigi da Porto 3, 35131, Padova (PD)
Call center	Consultare il link https://help.infocert.it/contatti/ per maggiori dettagli
Rappresentante legale	Danilo Cattaneo in qualità di Amministratore Delegato
Numero di telefono	+39 06 836691
N° Codice Fiscale	07945211006
N° partita IVA	07945211006
Sito web	https://www.firma.infocert.it - https://www.infocert.it

4.3 Ufficio di Registrazione - RA

L’Ente Emettitore si può avvalere di un’altra organizzazione per le attività necessarie al rilascio dei certificati digitali, nonché alla consegna della CNS.

L’Ente Emettitore ha delegato InfoCert che, a sua volta, si può avvalere di altri soggetti che operano sotto la sua supervisione.

Questi soggetti delegati vengono denominati “Registration Authority” (RA).

I rapporti tra InfoCert, Ente Emettitore e RA sono definiti da appositi accordi di servizio.

4.4 Richiedente – Subscriber

È il soggetto fisico che richiede all'Ente Emettitore il rilascio della CNS e può coincidere con il Titolare.

4.5 Titolare – Subject

Il titolare è il soggetto in favore del quale è rilasciata la CNS ed è identificato nel certificato digitale come il legittimo possessore della chiave privata, corrispondente alla chiave pubblica, contenuta nel certificato stesso.

Il titolare è tenuto a:

- garantire la correttezza, la completezza e l'attualità delle informazioni fornite all'Ente Emettitore o ai suoi delegati per la richiesta della CNS;
- proteggere e conservare le proprie chiavi private con la massima accuratezza al fine di garantirne l'integrità e la riservatezza;
- proteggere e conservare il codice di attivazione (PIN) utilizzato per l'abilitazione delle funzionalità della CNS, in un luogo sicuro e diverso da quello in cui è custodito il dispositivo stesso;
- adottare ogni altra misura atta ad impedire la perdita, la compromissione o l'utilizzo improprio della chiave privata e della CNS;
- utilizzare le chiavi e il certificato per le sole modalità previste nel presente Manuale Operativo;
- inoltrare all'Ente Emettitore o al Certificatore, senza ritardo, la richiesta di revoca o sospensione dei certificati al verificarsi di quanto previsto nel presente Manuale Operativo;
- adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

L'Ente Emittente ed il Certificatore in nessun caso risponderanno di eventi ad essi non imputabili ed in particolare di danni subiti dal Titolare o da qualsiasi terzo, causati direttamente o indirettamente dal mancato rispetto da parte degli stessi delle regole indicate nel presente Manuale Operativo, ovvero dalla mancata assunzione da parte di detti soggetti delle misure di speciale diligenza idonee ad evitare la causazione di danni a terzi che si richiedono al fruitore di servizi di certificazione, ovvero dallo svolgimento di attività illecite.

L'Ente Emettitore ed il Certificatore non saranno altresì responsabili di qualsiasi inadempimento o comunque di qualsiasi evento dannoso determinato da caso fortuito o da cause di forza maggiore.

5 OPERATIVITÀ

5.1 Identificazione

L'Ente Emettitore, direttamente o tramite un soggetto delegato, verifica con certezza l'identità del Richiedente prima di procedere al rilascio della CNS e del relativo certificato di Autenticazione CNS richiesto.

La modalità di identificazione LiveID o *de visu* prevede un incontro di persona tra il Richiedente e uno dei soggetti abilitati a eseguire il riconoscimento, che provvede ad accertare la sua identità mediante l'esibizione in originale di uno o più documenti in corso di validità.

Il Richiedente deve essere in possesso anche del Codice Fiscale, la cui esibizione può essere richiesta dal soggetto abilitato ad eseguire il riconoscimento.

La procedura di identificazione comporta che il Richiedente sia riconosciuto personalmente, attraverso il controllo di uno dei seguenti documenti:

- Carta d'identità;
- Passaporto;
- Patente di guida.

Ove possibile potranno essere utilizzati, in conformità con quanto previsto nei Manuali Operativi di InfoCert, ulteriori strumenti di riconoscimento che non prevedano la presenza fisica del Titolare presso gli uffici di registrazione. L'Ente Emettitore ritiene idonee tutte le modalità di identificazione che sono ammissibili nell'ambito del rilascio di una Firma Elettronica Qualificata.

L'identità del Richiedente può essere accertata da uno dei soggetti di seguito indicati:

1. L'Ente Emettitore, anche tramite suoi Incaricati o Delegati;
2. il Certificatore, anche attraverso i propri Uffici di registrazione (RA).

I passi principali a cui il Richiedente deve attenersi per ottenere una CNS ed un certificato di autenticazione CNS sono:

- prendere visione della documentazione di cui alla sezione 2 del presente documento;
- fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
- sottoscrivere la richiesta di registrazione, con firma autografa o digitale, e prendere visione, accettandole, delle modalità di utilizzo della CNS.

Dopo il rilascio del Certificato viene inviata al Richiedente una busta virtuale cifrata contenente un codice segreto di emergenza (ERC), che consente la revoca o la sospensione del Certificato stesso.

Nella richiesta di registrazione sono contenute le informazioni che devono comparire nel certificato e quelle che consentono di gestire in maniera efficace il rapporto tra l'Ente Emettitore ed il Richiedente/Titolare.

Il modulo di richiesta deve essere sottoscritto dal Richiedente/Titolare.

Sono considerate obbligatorie le seguenti informazioni:

- Cognome e Nome;
- Data e luogo di nascita;
- Codice Fiscale;
- Indirizzo di residenza;
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso;
- Indirizzo e-mail;
- Numero di telefono.

5.2 Registrazione dei dati del Titolare della CNS

Per procedere all'emissione del certificato per la CNS è necessario eseguire una procedura di registrazione, successiva all'identificazione, durante la quale i dati del Titolare vengono memorizzati negli archivi del Certificatore.

La registrazione iniziale è effettuata presso l'Ente Emettitore o una RA.

Durante questo passaggio iniziale i dati del Titolare vengono inseriti nel sistema in uso al Certificatore.

Conclusasi la fase di registrazione iniziale, per il rilascio dei certificati digitali e la consegna della CNS verrà generata la coppia di chiavi sul dispositivo CNS e, dopo le opportune verifiche, verrà emesso il Certificato. Successivamente, il dispositivo verrà consegnato al Titolare. La CNS viene personalizzata, a cura del Certificatore, con il PIN consegnato al Richiedente attraverso la busta virtuale cifrata inviata all'indirizzo e-mail indicato al momento della registrazione.

La segretezza del PIN personale durante le fasi di personalizzazione della CNS è garantita da adeguati sistemi di cifratura. Tale codice PIN, generato in modo casuale, è conservato in modo protetto all'interno dei sistemi del Certificatore, e viene comunicato al solo Titolare. La CNS così personalizzata con la coppia di chiavi generate è protetta da tale PIN personale.

5.3 Generazione delle chiavi e protezione delle chiavi private

La coppia di chiavi per l'autenticazione è generata utilizzando le funzionalità offerte dalla CNS.

Le chiavi sono generate all'interno del microprocessore e veicolate dalla smart card o dal token USB.

Le chiavi del soggetto possono essere:

- chiavi asimmetriche RSA con lunghezza non inferiore a 2048 bits;
- chiavi asimmetriche EC su una delle curve ellittiche previste dal documento ETSI TS 119 312 - Cryptographic Suites di lunghezza non inferiore a 256 bit.

La chiave privata del Titolare è generata e memorizzata in un'area protetta del dispositivo di firma che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione rende illeggibile la carta, a protezione dei dati in essa contenuti.

Per utilizzare la chiave privata a bordo della CNS, il possessore deve autenticarsi correttamente fornendo il proprio PIN segreto.

5.4 Emissione del certificato

L'emissione del certificato di autenticazione CNS viene effettuata in modo automatico dalle procedure del Certificatore, secondo i seguenti passi:

1) viene verificata la correttezza della richiesta del certificato, controllando che:

   - il Richiedente/Titolare sia stato correttamente registrato e siano state fornite tutte le informazioni necessarie al rilascio del certificato;
   - la chiave pubblica che si intende certificare sia una chiave valida e della lunghezza prevista;
   - la richiesta sia autentica e il Titolare possieda la corrispondente chiave privata;

2) viene controllata la validità della firma dell'incaricato che ha convalidato la richiesta;

3) si procede alla generazione del certificato e alla sua pubblicazione nel registro dei certificati;

4) il certificato viene memorizzato all'interno della CNS come dispositivo sicuro di firma del Titolare.

Il certificato ha validità di tre anni a partire dalla data di emissione ovvero fino alla data di pubblicazione della sua revoca o sospensione, se effettuate precedentemente a tale data.

5.5 Interdizione di una CNS

L'interdizione della CNS si attua tramite la revoca (interdizione definitiva) o la sospensione (interdizione temporanea) del relativo certificato, che ne tolgono la validità e rendono non validi gli utilizzi della corrispondente chiave privata effettuati successivamente al momento di revoca o sospensione. I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dal Certificatore e pubblicata ogni 24 ore nel registro pubblico dei certificati. Quest'ultimo è accessibile, con protocollo "LDAP" o "HTTPS", all'indirizzo indicato all'interno del certificato stesso. Oltre alla pubblicazione della CRL nei registri pubblici, il Certificatore mette a disposizione un servizio "OCSP" per la verifica online dello stato del certificato. L'URL del servizio è indicato nel certificato. Il servizio è disponibile 24 ore al giorno, 7 giorni alla settimana.

La revoca e la sospensione di un certificato hanno efficacia dal momento di pubblicazione della lista e comportano l'invalidità dello stesso e degli utilizzi della corrispondente chiave privata, effettuati successivamente a tale momento.

La revoca o sospensione del certificato può avvenire:

- su richiesta del Titolare;
- su iniziativa dell'Ente Emettitore;
- su iniziativa del Certificatore.

Il Certificatore verifica la provenienza della richiesta di revoca o di sospensione.

L'Ente Emettitore, direttamente o tramite il Certificatore, verifica l'identità del Titolare richiedente la revoca o sospensione e si accerta delle motivazioni della stessa.

La richiesta viene effettuata sul sito www.infocert.it, in un'apposita sezione. Il Titolare (per la sola sospensione) si autentica fornendo il codice di emergenza segreto (ERC), consegnato assieme al certificato che si intende sospendere.

Se la richiesta viene fatta presso l'Ufficio di registrazione (RA), l'autenticazione del Titolare avviene con le modalità previste per l'identificazione.

È fatto obbligo di richiedere la revoca nel caso in cui si verifichino le seguenti condizioni:

- la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
- sia stata smarrita o rubata la CNS;
- sia venuta meno la segretezza della chiave privata o del codice di attivazione per accedervi;
- si sia verificato un qualunque evento che abbia compromesso il livello di affidabilità della chiave privata;
- il Titolare non riesce più ad utilizzare la CNS in suo possesso (es: guasto del dispositivo sicuro);
- si verifica un cambiamento dei dati del Titolare presenti nel certificato;
- viene verificata una sostanziale condizione di non conformità del presente Manuale Operativo.

5.6 Procedura per la richiesta di revoca

La richiesta di revoca viene effettuata con modalità diverse, a seconda del Richiedente. Sono previsti i seguenti casi:

- **Revoca su iniziativa del Titolare**

L'utente Titolare richiede la revoca tramite l'Ufficio presso cui è stato registrato, il quale, ottenuti i dati necessari (la motivazione della revoca e il codice di emergenza del certificato) ed effettuate tutte le verifiche del caso, procede ad inoltrare la revoca al Certificatore.

Nell'impossibilità di identificare con certezza il Titolare si potrà procedere con una sospensione del Certificato, in attesa della corretta identificazione del Richiedente attraverso un form presente sul sito del Certificatore nella pagina relativa all'assistenza.

- **Revoca su iniziativa del Certificatore**

Il Certificatore esegue la sospensione del certificato su propria iniziativa o su richiesta del Titolare.

Il Certificatore attiva una richiesta di revoca con la seguente modalità:

il Certificatore comunica al Titolare anticipatamente, salvo casi di motivata urgenza, l'intenzione di revocare il certificato, fornendo il motivo della revoca e la data di decorrenza. La procedura di revoca del certificato viene poi completata con l'inserimento nella lista dei certificati revocati o sospesi (CRL).

- **Revoca su iniziativa dell'Ente Emettitore**

L'Ente Emettitore attiva una richiesta di revoca con la seguente modalità:

comunica al Titolare anticipatamente, salvo casi di motivata urgenza, l'intenzione di revocare il certificato, fornendo il motivo della revoca e la data di decorrenza. La procedura di revoca del certificato viene poi completata con l'inserimento nella lista dei certificati revocati o sospesi (CRL).

5.7 Procedura per la richiesta di sospensione

La sospensione deve essere effettuata nel caso si verifichino le seguenti condizioni:

- viene effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
- il Titolare o il Certificatore acquisiscono elementi di dubbio sulla validità del certificato;
- è necessaria un'interruzione della validità del certificato.

Il Titolare richiede la sospensione tramite l'Ufficio presso cui è stato registrato, il quale, ottenuti i dati necessari (la motivazione della sospensione e il codice di emergenza del certificato) ed effettuate tutte le verifiche del caso, procede ad inoltrare la richiesta di sospensione al Certificatore.

Alla scadenza dei periodi indicati, se non viene riattivato, il certificato passa in stato "revocato".

5.8 Rinnovo del certificato

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "validity period" (periodo di validità) con gli attributi "not after" (non dopo il) e "not before" (non prima del).

Al di fuori di questo intervallo di date il certificato è da considerarsi non valido.

Il certificato ha validità di tre anni dalla data di emissione.

La procedura di rinnovo richiede la generazione di una nuova coppia di chiavi: la richiesta di un nuovo certificato deve essere avviata prima della scadenza dello stesso.

La nuova coppia di chiavi è generata all'interno della CNS, l'emissione e la pubblicazione del certificato seguono il procedimento descritto in caso di nuova richiesta.

Le modalità operative per effettuare la procedura di rinnovo del certificato sono indicate dal

Certificatore nel proprio sito.

Il Certificato e il dispositivo possono essere rinnovati una sola volta. Dopo il primo rinnovo, si dovrà procedere ad una nuova emissione del Certificato e del dispositivo.

5.9 Conservazione della contrattualistica

La documentazione tecnica e contrattuale a supporto del riconoscimento e del rilascio della CNS è conservata dal Certificatore in modalità analogica e/o digitale per ventitrè anni dalla data di emissione, secondo quanto previsto dal Codice dell'Amministrazione Digitale.

In qualsiasi momento l'Ente Emettitore può richiederne copia facendone domanda al Certificatore.

ACCORDO QUADRO DI FORNITURA DEI SERVIZI INFOCERT
("Accordo")

InfoCert S.p.A., società soggetta a direzione e coordinamento di Tinexta S.p.A., con sede legale in Roma, Piazzale Flaminio, 1/B, 00196 C.F. e P.IVA 07945211006, PEC *infocert@legalmail.it*, in persona dell'Amministratore Delegato e legale rappresentante *pro-tempore* Dott. Danilo Cattaneo, domiciliato per la carica presso la sede della stessa società (di seguito per brevità denominata "**InfoCert**")

e

[…] con sede legale in via **[…]**, **[…]**, C.F. e P. IVA **[…]**, PEC **[…]**, in persona dell'**[…]** legale rappresentante *pro-tempore* munito dei necessari poteri come dichiara e garantisce, domiciliato per la carica presso la sede della stessa società (di seguito, per brevità denominata il "**Cliente**")

(di seguito congiuntamente "**Parti**" e singolarmente "**Parte**")

***

1. OGGETTO

1.1 Con il presente Accordo, InfoCert concede al Cliente:

a) la fornitura di servizi sottoposti a regolamentazione normativa specifica per i servizi *Trust* (di seguito i "**Servizi**"), osservando le modalità previste per ciascuno di essi, nel rispetto della disciplina afferente ai dati personali disciplinata nell'**Allegato B - DPA** e nell'**Allegato C – Allegato Tecnico** e nel **Manuale Operativo** che il Cliente ha letto e compreso e i cui riferimenti sono inseriti all'interno di ciascun **Allegato C**, ove è applicabile. I Servizi, ove possibile, potranno essere impiegati anche da parte di soggetti terzi utilizzatori (di seguito "**Utente(i)**"), il cui numero è indicato nella relativa **Offerta Commerciale – Allegato A**, e l'Utente potrà accedervi unicamente tramite accesso remoto dai propri terminali; e/o

b) se previsto, la licenza d'uso ("**Licenza**") di una piattaforma ("**Software**") come meglio definita anch'essa nell'**Allegato A** – **Offerta Commerciale** e nell'**Allegato C** - **Allegato Tecnico**.

1.2 InfoCert si impegna, ove previsto, a fornire al Cliente il supporto tecnico secondo i livelli di servizio specificati nell'**Allegato C** - **Allegato Tecnico**; e, sempre ove previsti, eventuali servizi di formazione, di consulenza e assistenza disciplinati nell'**Allegato A – Offerta Commerciale**.

1.3 In caso di contrasto tra le previsioni contenute nei suddetti Allegati e quelle dell'Accordo, queste ultime prevarranno.

2. OBBLIGHI E GARANZIE DEL CLIENTE

2.1 Il Cliente, si impegna a:

a) utilizzare i Servizi e/o il Software nel rispetto delle leggi, dei regolamenti vigenti e per le finalità d'uso ai sensi del presente Accordo;

b) non depositare, inviare, pubblicare, trasmettere e/o condividere applicazioni o documenti informatici che: (i) siano in contrasto o violino diritti di proprietà intellettuale, segreti commerciali, marchi, brevetti o altri diritti di proprietà di terzi; (ii) veicolino contenuti diffamatori, calunniosi o minacciosi; (iii) contengano materiale pornografico, osceno o comunque contrario alla pubblica morale; (iv) contengano virus, *worm*, *trojan* o altre caratteristiche di contaminazione o distruttive; (v) danneggino, violino o tentino di violare il segreto della corrispondenza e il diritto alla riservatezza; (vi) siano in contrasto alle disposizioni normative e/o regolamentari applicabili; (vii) possano causare malfunzionamenti o danni ai sistemi di InfoCert;

c) non trasferire, cedere, copiare, modificare, decompilare, disassemblare, distribuire anche *online*, concedere in uso a terzi (ad eccezione degli Utenti), rivendere, noleggiare e/o riallocare il Servizio e/o il Software;
d) non porre in essere alcun comportamento che possa costituire violazione dei diritti di proprietà intellettuale sulla Licenza e/o sui Servizi oggetto del presente Accordo;
e) rendere edotto l'Utente delle previsioni del presente Accordo e, in particolare, degli obblighi ed oneri specificamente richiesti ai fini dell'utilizzo dei Servizi e/o del Software. Il Cliente, anche per conto dell'Utente, si impegna a fornire tutte le informazioni necessarie all'attivazione dei Servizi e/o Software e a dotarsi di tutti i requisiti necessari per l'accesso agli stessi come meglio specificati nei relativi Allegati;
f) assumere, anche per conto degli Utenti, ogni responsabilità sull'utilizzo dei Servizi e/o del Software sulle azioni e sulle attività poste in essere dagli stessi;
g) attenersi ai principi di buona fede e correttezza nell'uso e nella fruizione del Software e/o dei Servizi;
h) a fornire in modo chiaro tutte le informazioni e i dati utili o necessari a consentire la corretta esecuzione del contratto

2.2 Il Cliente si impegna per tutta la durata dell'Accordo a garantire che eventuali servizi di informatica, prestati in suo favore da terze parti, non interferiscano con la corretta erogazione dei Servizi e/o del Software e non ostacolino o rendano l'esecuzione più onerosa per InfoCert, rispetto a quanto previsto nel presente Accordo. Nel caso in cui rilevi problemi nella fruizione del Software e/o dei Servizi, il Cliente si impegna a dare tempestiva comunicazione scritta a InfoCert, ai sensi dell'art. 22.1, e comunque entro 5 giorni lavorativi, identificando in dettaglio le disfunzioni riscontrate, così da consentire ad InfoCert l'adozione di tutte le misure eventualmente necessarie.

2.3 Qualora, nella fornitura di Licenza, sia previsto lo sviluppo del *front-end* da parte del Cliente, quest'ultimo si impegna a rispettare tutte le misure, garanzie e specifiche, come definite nell'Allegato Tecnico *sub* C.

2.4 Il Cliente si impegna a rispettare e/o implementare le misure di sicurezza come previste negli Allegati *sub* B e D.

2.5 Il Cliente si impegna a verificare, prima dell'acquisto del Servizio e/o della Licenza (e così del Software) che, rispetto a quelli richiesti per l'utilizzo e per le finalità degli stessi, i propri sistemi *hardware* e software siano idonei ed aggiornati all'ultima versione disponibile e/o, comunque, compatibile con quella eventualmente indicata da InfoCert. Il Cliente, pertanto, provvederà personalmente a configurare correttamente il proprio *hardware* e software e a installare il Software idoneo propedeutico all'utilizzo del Servizio. Il Cliente usufruirà dei Servizi e/o del Software tramite il collegamento internet di cui si dovrà dotare autonomamente per il tramite di un operatore di telecomunicazioni, rispondente ai requisiti indicati nell'Allegato *sub* C e nel Manuale Operativo.

2.6 Il Cliente prende atto ed accetta integralmente il contenuto di cui all'**Allegato D** rubricato **"Misure di Sicurezza"** che le misure di sicurezza, tecniche e organizzative implementate da InfoCert che saranno poste in essere per permettere, a titolo esemplificativo ma non esaustivo, l'esecuzione di pratiche di sicurezza nel cloud, la continuità di servizio, le procedure di *disaster recovery* e la gestione degli *incident*.

3. OBBLIGHI E GARANZIE DI INFOCERT

3.1 InfoCert dichiara e garantisce:
(a) di rispettare le misure di sicurezza indicate dalla normativa in materia di protezione dei dati personali nonché dai provvedimenti delle autorità competenti laddove applicabili;
(b) con riguardo alla tutela dei dati, di proteggere gli stessi in caso di 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;

(c) di utilizzare i sistemi di accesso dotati di funzionalità di *data security* atti a monitorare e controllare il flusso di dati personali attraverso gli *endpoint* (a titolo esemplificativo, analisi e correlazione *real-time* dei *log* mediante servizio SOC/SIEM ai fini dell'identificazione di eventi anomali) o verso le reti esterne (a titolo esemplificativo, limitazione dell'accesso di rete ai soli servizi web funzionali alla richiesta dei certificati);

3.2 InfoCert non fornisce alcuna garanzia espressa o implicita relativamente ai Servizi e/o Software forniti per: assenza di vizi; originalità o idoneità del Software e/o dei Servizi per un uso specifico o per il raggiungimento di un particolare scopo.

3.3 È escluso ogni obbligo di vigilanza e/o sorveglianza, da parte di InfoCert, sui contenuti dei documenti formati, trasmessi o conservati nell'ambito dell'esecuzione del presente Accordo, essendo tali attività svolte sotto l'esclusivo controllo, e quindi di esclusiva responsabilità, del Cliente.

3.4 Fatto salvo quanto previsto dal precedente paragrafo, InfoCert potrà modificare, a costi e spese del Cliente stesso – come concordati tra le Parti - e su richiesta scritta di quest'ultimo, le modalità di erogazione del Software e/o Servizi che si dovessero rendere necessarie a causa di:

(a) informazioni errate fornite dal Cliente;

(b) informazioni derivanti da errori di programmazione o di elaborazione di dati imputabili al Cliente.

3.5 Ferma rimanendo la facoltà di sub-esternalizzare in tutto o in parte l'esecuzione dei Servizi, avvalendosi di terze parti, ferma restando la responsabilità di InfoCert per le condotte del subappaltatore, o del subfornitore, InfoCert si obbliga:

- a controllare che i Servizi sub-affidati al terzo siano eseguiti nel rispetto degli obblighi assunti con il Contratto nei confronti del Cliente;
- ad informare il Cliente di qualsiasi circostanza sopravvenuta o modifica nel rapporto col subappaltatore/subfornitore che potrebbe incidere negativamente sulla corretta esecuzione dei Servizi;
- a far sì che il Cliente e l'Autorità di vigilanza possano esercitare, presso e nei confronti del subappaltatore, i medesimi diritti di audit esercitabili verso InfoCert.

3.6 Ai sensi del Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale ("**Regolamento DORA**"), InfoCert provvederà: (i) a dare tempestiva comunicazione al Cliente in caso di grave incidente e comunque entro 24 ore ; (ii) all'adeguamento di carattere tecnico e normativo dei Servizi e/o del Software, dandone tempestiva – e comunque entro 5 giorni lavorativi comunicazione tramite posta elettronica certificata al Cliente i quali si impegnano ad adeguare le caratteristiche dei propri sistemi e la propria strumentazione alle modifiche indicate, entro il termine assegnato da InfoCert; (iii) alla manutenzione correttiva ed all'aggiornamento dei Servizi e/o del Software per esigenze di rettifica degli eventuali errori presenti sul Software e/o sui Servizi. L'aggiornamento consiste nell'attività necessaria a adeguare i Servizi e/o il Software ad eventuali evoluzioni normative. In caso di particolari mutamenti della normativa od obsolescenza della tecnologia utilizzata che rendano eccessivamente onerosa l'attività di aggiornamento (i.e., modifiche del Software superiori al 25%), InfoCert si riserva la facoltà di non adeguare i Servizi e/o il Software provvedendo al rilascio di nuovi applicativi Software, secondo le condizioni tecniche ed economiche che saranno previamente comunicate al Cliente.

InfoCert si obbliga a prestare assistenza al Cliente a un costo stabilito separatamente, in caso di incidente connesso alle Tecnologie dell'Informazione e della Comunicazione ("**TIC**") – come meglio specificato nel successivo comma- relativo al servizio fornito.

3.7 Qualora si verifichi un significativo incidente TIC, che eserciti un impatto sugli interessi finanziari del Cliente, InfoCert, senza indebito ritardo e comunque entro il termine di 24 ore da quando ne sia venuta a conoscenza, informa il Cliente e il CSIRT tramite una pre-notifica indicando se l'incidente possa essere il risultato di atti illegittimi o malevoli, ed entro 72 ore da quando ne sia venuta a conoscenza, trasmette una notifica

dell'incidente al Cliente e al CSIRT aggiornando quanto precedentemente comunicato ed indicando gravità, impatto e, ove possibile, gli indicatori di compromissione. InfoCert si impegna altresì, in caso di minaccia informatica significativa, se del caso, a informare il Cliente, qualora questo sia potenzialmente interessato da tale minaccia, informandolo in merito alle opportune misure di protezione che lo stesso può considerare di adottare.

3.8 InfoCert si obbliga a collaborare senza riserve con le Autorità competenti e con le Autorità di risoluzione del Cliente, comprese le persone da queste nominate.

3.9 Il presente comma regola i termini e le condizioni relativi all'utilizzo dei servizi TIC (Tecnologie dell'Informazione e della Comunicazione) da parte di InfoCert, conformemente all'art. 30 del Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio (DORA).

Gli accordi contrattuali, tra il Cliente e InfoCert, di servizi TIC includono i seguenti elementi:

a) Livelli di servizio

Qualora i servizi TIC siano a supporto di funzioni essenziali o importanti, InfoCert fornisce una descrizione di tali livelli di servizio, ivi compresi i relativi aggiornamenti e revisioni, indicando obiettivi quantitativi e qualitativi, in termini di prestazioni, tali da consentire un monitoraggio efficace da parte del Cliente e l'applicazione, senza indebito ritardo, di opportune azioni correttive qualora i livelli di servizio concordati non siano rispettati.

b) Partecipazione a programmi di sensibilizzazione e formazione

InfoCert partecipa, su indicazione del Cliente e conformemente all'articolo 13, paragrafo 6, del Regolamento DORA, ai programmi di sensibilizzazione sulla sicurezza delle TIC e alle attività di formazione sulla resilienza operativa digitale del Cliente.

3.10 Qualora il Cliente determini, e di questo ne dia comunicazione scritta ad InfoCert, che i servizi TIC siano a supporto di proprie funzioni essenziali o importanti, InfoCert dichiara di garantire obblighi di segnalazione verso il Cliente, e relativi termini di preavviso, tra cui la notifica di eventuali sviluppi che potrebbero esercitare un impatto significativo sulla propria capacità di prestare tali servizi a supporto in maniera efficace, in linea con i livelli di servizio concordati;

InfoCert dichiara inoltre di attuare e testare i piani operativi d'emergenza e predisporre misure, strumenti e politiche per la sicurezza, tali da offrire un adeguato livello di sicurezza.

3.11 InfoCert si impegna a partecipare e cooperare pienamente ai test di penetrazione guidati dalla minaccia (TLPT), come definiti dal Regolamento DORA, i quali verranno di norma effettuati in modalità congiunta tra più clienti, qualora abbiano ad oggetto servizi simili al Servizio fornito nell'ambito dell'Accordo, e che saranno condotti da uno di tali clienti o soggetti da questi nominati ("**Test congiunto/i**"). Resta espressamente inteso che, laddove non venga o non possa essere effettuato il Test Congiunto, InfoCert si impegna a partecipare e cooperare pienamente ai TLPT condotti dal Cliente.

InfoCert provvederà ad invitare al Test Congiunto tutti i clienti/entità finanziarie che abbiano aderito a tale servizio; in seguito, recepiti i requisiti di partecipazione da parte dei clienti/entità finanziarie, InfoCert effettuerà una valutazione dei costi relativi al Test Congiunto e invierà ai clienti/entità finanziarie coinvolti la proposta tecnico-economica di partecipazione al Test Congiunto.

Sulla base dell'accettazione della proposta tecnico-economica da parte di almeno 5 (cinque) dei clienti/entità finanziarie invitati, InfoCert darà avvio alla cooperazione al Test Congiunto, inviando ai partecipanti una conferma di esecuzione del Test Congiunto ed incaricando a tal fine un soggetto esterno, con il preventivo consenso del Cliente, che sarà responsabile dell'esecuzione del suddetto test.

4. QUALITÀ DEI SERVIZI

4.1 Fermo quanto previsto ai precedenti articoli, i Servizi verranno da InfoCert realizzati secondo modalità, caratteristiche e contenuti indicati nel relativo Allegato Tecnico. InfoCert risponderà, nei confronti del Cliente, solo ed esclusivamente di quei difetti di conformità e/o completezza del Servizio rispetto a tali modalità, caratteristiche e contenuti, che rendano il Servizio inidoneo all'uso cui è destinato (c.d. difetti sostanziali).

4.2 L'eventuale presenza, nel Servizio reso, di difetti sostanziali dovrà essere dal Cliente denunciata, a pena di decadenza, entro 8 (otto) giorni dalla scoperta e, in ogni caso, entro e non oltre 90 (novanta) giorni dall'evasione del Servizio contestato. Una volta ricevuta la denuncia di cui al precedente punto, InfoCert procederà, ove necessario, all'immediato integrale rifacimento del Servizio contestato. Il relativo costo sarà addebitato al Cliente, qualora venisse dimostrato che il Servizio originariamente reso non presentava difetti sostanziali; diversamente resterà a carico di InfoCert.

4.3 Relativamente ai Servizi per i quali è previsto un corrispettivo unitario, qualora, per causa imputabile ad InfoCert, il singolo Servizio reso dovesse presentare difetti sostanziali, la stessa InfoCert corrisponderà al Cliente, a titolo di penale, un importo pari al doppio del corrispettivo dal Cliente stesso dovuto per il Servizio risultato inficiato da difetti sostanziali. In ogni caso, nessuna penale e nessun risarcimento saranno dovuti se, nel corso del mese, risulterà evaso senza difetti sostanziali almeno il 95% (novantacinque per cento) dei Servizi a corrispettivo unitario resi al Cliente in quello stesso mese.

4.4 Relativamente ai Servizi per i quali è previsto un corrispettivo a canone forfettario, qualora in un determinato mese dovessero essere messi a disposizione del Cliente Servizi che − per causa imputabile a InfoCert a titolo di dolo o colpa grave − presentassero difetti sostanziali in percentuale superiore al 5% rispetto al complesso dei Servizi messi a disposizione del Cliente stesso nel mese, InfoCert corrisponderà a quest'ultimo, a titolo di penale, un importo pari al 6% del canone mensile contrattualmente previsto per il Servizio risultato inficiato da difetti sostanziali.

4.5 In ogni caso, per ogni anno di vigenza del rapporto contrattuale, non potranno esser corrisposte da InfoCert penali per un importo che superi l'ammontare dei corrispettivi annui dovuti dal Cliente a InfoCert per la fornitura dei Servizi.

4.6 InfoCert dichiara – ed il Cliente ne prende atto – che attualmente la stessa ha in essere e che manterrà in essere anche in futuro una polizza assicurativa a copertura dei rischi derivanti dalla violazione delle previsioni di cui al presente articolo.

5. SUPPORTO E ASSISTENZA

5.1 Per qualsiasi informazione relativa a modalità, caratteristiche e contenuti dei Servizi fruiti in forza del presente Accordo, il Cliente potrà mettersi in contatto con la funzione Customer Care, operativa dalle ore 9:00 alle ore 18.00 dal lunedì al venerdì, tramite apposita piattaforma di ticketing, attraverso cui aprire le segnalazioni. Per segnalazioni di anomalie bloccanti il cliente potrà avvalersi del presidio di Continuità Operativa (disponibile 24hx7gg) con le modalità indicate nell'apposito allegato.

6. ADEMPIMENTI IN MATERIA DI SICUREZZA E SALUTE SUL LAVORO

6.1 Con esclusivo riferimento alla richiesta di fornitura di Servizi da parte del Cliente, InfoCert si impegna a rispettare ed a far rispettare, dalle persone delle quali si avvale per l'esecuzione delle proprie attività, tutte le norme di legge per la prevenzione degli infortuni e sull'igiene sul lavoro.
A tal fine, ai sensi dell'art. 26, c. 1 lett. b), D.Lgs. 81/2008, ove applicabile, il Cliente invierà ad InfoCert ogni informazione relativa ai rischi specifici esistenti nei luoghi in cui InfoCert opererà nonché alle misure di prevenzione e di emergenza adottate in relazione alla propria attività e a tali luoghi, sia nel caso in cui i

dipendenti di InfoCert prestino la propria attività lavorativa presso i locali del Cliente sia che prestino tale attività altrove.

6.2 InfoCert si impegna a corrispondere ai propri lavoratori i trattamenti retributivi, contributivi, assicurativi e fiscali dovuti. InfoCert, su richiesta scritta del Cliente, inoltrerà a quest'ultimo copia del Documento Unico di Regolarità Contributiva (DURC) in corso di validità. I costi relativi alla sicurezza sono specificatamente indicati negli Ordini.

6.3 Con esclusivo riferimento alla fornitura di Servizi, ai sensi e per gli effetti di cui all'art. 26, comma 3, del D.Lgs. 81/2008 e successive modifiche e integrazioni, qualora le Parti, all'esito della valutazione dei rischi di eventuali interferenze, non escludano la sussistenza di rischi da interferenza, in particolare in relazione con le attività dei lavoratori del Cliente, quest'ultimo predisporrà un Documento Unico di Valutazione dei Rischi di eventuali Interferenze (DUVRI), recante descrizione delle misure adottate per eliminare possibili interferenze, che verrà allegato all'Accordo e che costituirà parte integrante e sostanziale di quest'ultimo.

7. PROPRIETA' INTELLETTUALE

7.1 Tutti i diritti di utilizzazione e di sfruttamento, anche economico, del Servizio e/o della Licenza in essi presenti, sono riservati a InfoCert. Al Cliente e/o all'Utente è concesso l'uso dei Servizi e/o della Licenza nei limiti e alle condizioni stabilite nel presente Accordo.

7.2 Tutti i dati, documenti e/o materiali forniti da InfoCert relativi ai Servizi, nonché il Software acquisito in Licenza d'uso da InfoCert ("**Diritti IP**"), rimarranno di esclusiva proprietà di InfoCert.

7.3 I Diritti IP relativi al Software ed ai Servizi e qualsivoglia ulteriore modifica, incremento, revisione o cambi effettuati da InfoCert rimarranno di proprietà di InfoCert.

7.4 Se applicabile, la Licenza è personale, non esclusiva, non trasferibile a terzi ad alcun titolo e limitata nel tempo fino alla data di scadenza e/o cessazione del presente Accordo.

7.5 Ciascuna Parte si impegna a non rendere dichiarazioni o tenere comportamenti che possano ledere in qualsiasi modo l'immagine e/o il nome dell'altra o che possano comunque arrecare pregiudizio commerciale all'altra.

7.6 Resta inteso che il marchio, il dominio e tutti i segni distintivi del Cliente, come pure tutti i diritti di utilizzazione e di sfruttamento dell'immagine, del nome e dell'identità economica della stessa sono liberamente impiegabili da parte di InfoCert (a titolo esemplificativo e non esaustivo sul sito istituzionale, sui social media e per presentazioni della forza vendita). Viceversa, il marchio, il dominio e tutti i segni distintivi di InfoCert, come pure tutti i diritti di utilizzazione e di sfruttamento dell'immagine, del nome e dell'identità economica della stessa, non potranno essere liberamente utilizzati dal Cliente per qualsiasi finalità, salvo previa autorizzazione scritta di InfoCert.

8. LIMITAZIONI E RESPONSABILITA'

8.1 InfoCert s'impegna a fornire i Servizi e/o la Licenza (e così il Software) richiesti dal Cliente, in osservanza di quanto stabilito dal presente Accordo, dai relativi Allegati e dalla rispettiva normativa di settore tempo per tempo applicabile, non assumendo alcuna responsabilità al di fuori di quanto in essi espressamente stabilito.

8.2 Salvi i casi di dolo o colpa grave, InfoCert non sarà in alcun caso responsabile di qualsiasi danno, diretto e/o indiretto, derivante in via anche alternativa: i) per danni costituiti da lucro cessante, perdita di opportunità commerciali o di risparmi, perdita di dati, perdita di interesse, danni all'immagine o perdita di reputazione commerciale, né per multe, ammende, soprattasse o altre sanzioni, derivanti, direttamente o indirettamente, da atti od omissioni di InfoCert ai sensi del presente Accordo; ii) dall'uso non conforme dei Servizi e/o del Software a quanto previsto dal presente Accordo, ed eventuali successive modifiche; iii) per manomissioni

o interventi sui Servizi e/o sul Software effettuati dal Cliente e/o dall'Utente stesso e/o da parte di terzi non autorizzati da InfoCert, anche qualora non cagionino espressamente un danno alle Parti o a terzi; iv) da un improprio utilizzo delle credenziali e/o dei Servizi e/o della Licenza e/o del Software da parte del Cliente e/o dell'Utente; v) dalla mancata fruizione del Servizio e/o Software dovuta a malfunzionamenti o blocchi della rete internet o a fronte di ritardi o interruzioni o per errori e/o malfunzionamenti rientranti nell'ambito dei parametri di indisponibilità indicati nell'Allegato Tecnico.

8.3 InfoCert, in ipotesi di dolo o colpa grave del Cliente e/o dell'Utente, si riserva, oltre al diritto al risarcimento del danno e/o al recupero dei crediti spettanti, la facoltà di trattenere il Corrispettivo a compensazione parziale o totale degli eventuali danni, pregiudizi o spese sostenute per l'erogazione o gestione della singola fattispecie.

8.4 Fermo quanto previsto e/o pattuito in altre clausole dell'Accordo, resta inteso che, in ogni caso, qualora InfoCert risultasse responsabile per eventuali danni, sarà tenuta a corrispondere al Cliente, a titolo di risarcimento del danno da questo subito, un importo non superiore al 10% del Corrispettivo complessivo del valore annuo dell'Accordo ("**Indennizzo Massimo**"). L'Indennizzo Massimo sarà riconosciuto solo previo accertamento degli eventuali inadempimenti verificatisi nel relativo anno solare di vigenza dell'Accordo e comprenderà tutti i danni derivanti da violazione di legge o di contratto e qualsiasi penale, restituzione di prezzo e costo che InfoCert sia tenuta a corrispondere al Cliente.

8.5 Nessuna azione potrà essere iniziata dal Cliente, a pena di decadenza, decorsi 9 (nove) mesi dalla data in cui l'Accordo si è risolto o è cessato.

8.6 Nel caso in cui il Cliente (e/o l'Utente) compia atti che costituiscano violazione di diritti di proprietà intellettuale di un terzo, il Cliente, anche per conto dell'Utente, manleverà e/o terrà indenne InfoCert da qualsiasi danno o spesa, compresi onorari e spese legali, che quest'ultima sopporti, in conseguenza delle rivendicazioni del terzo.

8.7 Il Cliente si obbliga, anche per conto dell'Utente, a garantire e tenere indenne InfoCert da qualsiasi perdita, danno, spesa, costo o altro onere che questa possa sopportare in conseguenza di azioni e/o pretese avanzate da terzi in relazione all'esecuzione del presente Accordo, per fatti imputabili al Cliente medesimo e/o all'Utente.

9. AUDIT

9.1 InfoCert ha la facoltà di effettuare, anche attraverso soggetti da essa incaricati, verifiche presso il Cliente, in modalità *self-assessment* e/o audit *on-site*, allo scopo di accertare il rispetto delle misure di sicurezza e di trattamento dei dati personali, nonché verificare il puntuale rispetto delle previsioni del presente Accordo e dei relativi Allegati ("**Audit**").

9.2 In caso di Audit, il Cliente si impegna sin da ora a collaborare con InfoCert e con i soggetti da questa incaricati, fornendo senza ritardo tutte le informazioni richieste e illustrando i processi della propria organizzazione. InfoCert, a fronte di criticità emerse in fase di Audit, si riserva di esercitare, a propria discrezione, il diritto di richiedere ulteriori approfondimenti, eseguiti anche eventualmente da parte di società terze specializzate, per le finalità del presente Accordo.

9.3 Nel caso in cui InfoCert rilevi, all'esito degli accertamenti a proprio insindacabile giudizio, che il Cliente non si sia attenuto a quanto stabilito nel presente Accordo, il Cliente si impegna ad uniformarsi alle indicazioni ed alle istruzioni comunicate da InfoCert con diffida ad adempiere ex art. 1454 c.c., entro i tempi indicati dalla stessa. Decorso inutilmente il congruo termine imposto da InfoCert, il presente Accordo si intenderà senz'altro risolto, ai sensi del successivo art. 14.

9.4 InfoCert si impegna, a favore del Cliente nonché dell'Autorità di vigilanza, a garantire l'accesso alla propria sede legale e alle sedi operative, oltre ai propri server, database ecc., utilizzati per l'erogazione del Servizio/Software, per verifiche ispettive in relazione al presente Accordo.

9.5 InfoCert garantisce analogo accesso da parte del Cliente anche per i propri eventuali subappaltatori, subfornitori, fornitori e consulenti esterni al fine di assicurarne la conformità alla normativa applicabile ed alle condizioni contrattuali.

9.6 Ogni Audit sarà effettuato con un ragionevole preavviso scritto, in ogni caso non inferiore a 10 (dieci) giorni lavorativi, salvo che vi siano ragioni di emergenza o di effettività dell'ispezione che non consentano di rispettare tale termine.

9.7 Ciascun Audit avrà una durata massima di 3 (tre) giorni lavorativi. In particolare, InfoCert accetta che il suddetto diritto di Audit possa essere esercitato a titolo gratuito, durante un anno solare, limitatamente alle prime 3 (tre) giornate in cui le verifiche saranno messe in atto. In caso di durata maggiore, ancorché dietro richiesta dell'Autorità di Vigilanza, le Parti concorderanno in buona fede un corrispettivo per InfoCert, proporzionato all'impiego di tempo e risorse.

9.8 Le attività di Audit possono essere utilizzate avvalendosi di:

a. verifiche congiunte di Audit organizzate unitamente ad altri clienti di InfoCert ed eseguite anche da un soggetto terzo nominato dai clienti stessi, al fine di utilizzare in modo più efficiente le risorse di Audit e ridurre gli oneri organizzativi sia per i clienti sia per InfoCert;
b. certificazioni di soggetti terzi e relazioni di soggetti terzi o dell'Audit interno messe a disposizione da InfoCert.

9.9 Il Cliente ha diritto ad eseguire accessi, ispezioni, audit presso Infocert e di ottenere copia della documentazione pertinente coperta da riservatezza e con il divieto di condivisione della stessa verso terze parti che non siano state autorizzate per iscritto da InfoCert.

9.10 In tema di accessi relativi all'ambito d'applicazione del Regolamento Dora, al fine di verificare le prestazioni dei Servizi oggetto dell'Accordo, il Cliente ha il diritto di effettuare controlli tramite attività di audit (modalità di verifica in presenza e con raccolta delle evidenze in diretta) e/o attività di assessment (modalità di monitoraggio attraverso la somministrazione di questionari e/o call da remoto e raccolta di evidenze in modalità differita).

9.11 Le attività sopra descritte potranno essere svolte non più di una volta all'anno, salvo circostanze eccezionali di crisi o di emergenza che giustifichino audit aggiuntivi. Le attività di audit potranno avere luogo per una durata che potrà variare da 1 (una) giornata lavorativa fino ad un massimo di 2 (due) giornate lavorative su base annua; diversamente, al protrarsi di tali attività, InfoCert avrà diritto a vedersi riconosciuto un corrispettivo in buona fede, commisurato al tempo e alle risorse impiegate per lo svolgimento delle attività di audit.

9.12 InfoCert, a fronte di esplicita richiesta scritta da parte del Cliente, si impegna a collaborare con la stessa nell'esecuzione di assessment volti a certificare la presenza di adeguati presidi in ambito sicurezza informatica, continuità operativa e data protection. Nell'ambito degli assessment InfoCert si impegna a condividere puntuali evidenze richieste dal Cliente. L'impegno richiesto dalle suddette attività sarà calcolato in ore impiegate e si intende sostitutivo dei 2 giorni di audit descritti sopra; al protrarsi di tali attività, InfoCert avrà diritto a vedersi riconosciuto un corrispettivo in buona fede, commisurato al tempo e alle risorse impiegate per lo svolgimento delle attività di assessment.

9.13 L'attività di assessment potrà essere sostituita o integrata con certificazioni, attestazioni e reportistica generale per agevolare le esigenze di verifica da parte del Cliente.

9.14 Per la corretta pianificazione delle attività di audit, il Cliente dovrà dare ad InfoCert un preavviso di almeno 15 giorni lavorativi prima della data effettiva dell'audit, a meno che non sia impossibile a causa di una situazione di emergenza o di crisi, e gli fornirà le seguenti informazioni:

- l'elenco dei siti da visitare;
- lo scopo e la portata dell'audit;
- l'identità della persona o delle persone che condurranno l'audit.

10. DURATA

10.1 Il presente Accordo avrà la durata di _____ mesi ("**Durata**") a decorrere dalla data di sottoscrizione.

10.2 Alla scadenza, il presente Accordo si rinnova in automatico per periodi di 1 (un) anno ciascuno, salvo che una delle Parti dia disdetta, con comunicazione da inviarsi entro e non oltre 90 (novanta) giorni prima della scadenza dell'Accordo.

11. CORRISPETTIVI

11.1 Il Cliente si impegna a pagare i corrispettivi a InfoCert secondo quanto previsto nell'Offerta ("**Corrispettivo/i**").

11.2 I Corrispettivi saranno dovuti dal Cliente entro 60 (sessanta) giorni dalla data di invio della fattura da parte di InfoCert. Resta inteso tra le Parti che, in caso di mancato pagamento entro tale termine, saranno dovuti gli interessi di cui al D.lgs. 231/2002, in via automatica e senza necessità di previa costituzione in mora del Cliente.

11.3 In caso di mancato pagamento dei Corrispettivi, InfoCert si riserva il diritto di risolvere il presente Accordo ai sensi del successivo art. 14, nonché il diritto di sospendere l'erogazione del Servizio e/o il relativo accesso al medesimo e/o l'utilizzo del Software fino al pagamento dei Corrispettivi dovuti.

11.4 Le Parti convengono che i Corrispettivi sono soggetti a variazione annuale in funzione dell'indice ISTAT dei prezzi al consumo per le famiglie di operai ed impiegati applicata a decorrere dal 31 gennaio di ogni anno successivo a quello di rilevazione.

12. PRIVACY

12.1 Con la sottoscrizione del presente Accordo le Parti si impegnano, informandosi reciprocamente, a far sì che tutti i dati personali forniti direttamente dalle Parti o dei quali le stesse vengano in possesso durante la vigenza del presente Accordo e comunque connessi con l'Accordo stesso, relativi al proprio personale o ai propri collaboratori o a terzi, saranno oggetto di trattamento, automatizzato e non, esclusivamente per le finalità gestionali e amministrative inerenti l'adempimento degli obblighi contrattuali e legislativi. A tal fine, InfoCert, in qualità di titolare del trattamento dei dati forniti dal Cliente, informa lo stesso che, i relativi dati personali saranno trattati, per le finalità e nelle modalità illustrate nell'informativa presente sul sito www.infocert.it, di cui il Cliente dichiara di aver preso visione.

12.1.1 Il conferimento dei dati, come previsto al paragrafo precedente, è necessario per l'assolvimento delle predette finalità e in difetto non sarà possibile realizzarle in tutto o in parte. I dati saranno utilizzati dalle Parti solo con modalità e procedure necessarie al perseguimento delle finalità indicate. Le Parti dichiarano e si danno reciprocamente atto che, in relazione al trattamento dei dati personali di cui al presente articolo, gli interessati potranno esercitare i diritti di cui agli articoli 15-22 del Regolamento (UE) 2016/679.

12.1.2 Per le finalità del presente Accordo e sulla base delle modalità di erogazione/utilizzo del Servizio e/o del Software, le Parti sottoscriveranno un separato accordo sul trattamento dei dati ai sensi dell'**Allegato B – DPA.**

12.2 Presso il data center, sono messi a disposizione appositi macchinari *hardware* per la gestione dei dati dei Clienti, necessari all'erogazione/utilizzo dei Servizi e/o Software.

12.2.1 Il data center è organizzato e amministrato nel rispetto delle norme legislative applicabili sulle misure di sicurezza, e fornito di appositi sistemi di protezione logica e fisica, al fine di impedire accessi non autorizzati. Le regole di sicurezza sono autonomamente stabilite e implementate da InfoCert; in particolare, le stesse potranno essere modificate, per essere rese conformi ad eventuali mutamenti della disciplina di cui al Regolamento UE 679/2016, ed alle successive disposizioni legislative e regolamentari in materia di sicurezza dei dati personali.

12.2.2 Il Cliente riconosce e accetta che InfoCert si avvale di terze parti, debitamente nominate come responsabili del trattamento dei dati personali, tra cui la fornitura di servizi di *storage* dei dati in *cloud*, su *server* situati all'interno dell'Unione Europea e operanti nel pieno rispetto della normativa in materia di trattamento dei dati personali. Per maggiori informazioni è disponibile il seguente indirizzo di posta elettronica: richieste.privacy@legalmail.it.

13. RISERVATEZZA

13.1 Ai fini del presente Accordo, con "**Informazioni Confidenziali**" si intende qualsiasi informazione riguardante, ma non limitata a contenuti base, contenuti, marchio, programmi informatici, codici, algoritmi, nomi e capacità di lavoratori dipendenti ed autonomi, *know-how*, formule, procedimenti, idee, invenzioni (brevettabili o meno), schemi ed altri piani tecnici, commerciali, finanziari e di sviluppo, previsioni, strategie, prezzi, profitti, utili, margini, elenco o dettagli di clienti, sia individualmente, sia collettivamente, ed altre informazioni non pubbliche. Ciascuna delle Parti si impegna a mantenere riservate le Informazioni Confidenziali relative all'altra Parte, nella stessa misura in cui protegge le proprie Informazioni Confidenziali e di utilizzare tali Informazioni Confidenziali soltanto nella misura strettamente necessaria per l'adempimento delle obbligazioni derivanti dal presente Accordo.

13.2 Tali restrizioni sulla comunicazione e sull'utilizzo delle informazioni resteranno in vigore per 5 (cinque) anni successivi alla risoluzione o cessazione dell'Accordo.

13.3 Resta salva la possibilità di una Parte di comunicare a terzi tali informazioni, a seguito di ordine del Giudice o della Pubblica Autorità e previa comunicazione, ove possibile, all'altra Parte.

13.4 InfoCert si riserva il diritto, in caso di diffusione non autorizzata delle Informazioni Riservate, di tutelare i propri diritti in ogni più opportuna sede.

14. SOSPENSIONE – RISOLUZIONE - RECESSO

14.1 InfoCert ha il diritto di sospendere e/o cessare l'erogazione del Software e/o del Servizio e/o bloccare l'accesso del Cliente e/o dell'Utente allo stesso, quando:

(a) abbia fondato motivo di ritenere che si sia verificato, anche per ragioni non imputabili al Cliente stesso, un evento che possa mettere a rischio la sicurezza delle informazioni e dei dati contenuti nel Software e/o Servizi. La sospensione può durare, senza che il Cliente possa avanzare alcuna pretesa al riguardo, finché InfoCert non riterrà fondatamente superato il rischio di cui sopra;

(b) in caso di utilizzo improprio del Software e/o dei Servizi ovvero di impedire l'accesso ai documenti e/o ai dati ivi contenuti da parte del Cliente e/o dell'Utente, dando, se del caso, idonea comunicazione dell'illecito alle autorità competenti;

(c) venga a conoscenza della violazione di uno o più divieti di cui al presente Accordo o come previsti sul Manuale Operativo di riferimento o venga avanzata espressa richiesta in tal senso da un organo giurisdizionale o amministrativo competente in materia in base alle norme vigenti;

(d) vengano superati i limiti di utilizzo indicati nel presente Accordo o qualora si verifichino situazioni che possano compromettere la sicurezza del Servizio e/o del Software.

14.2 Nelle ipotesi di cui sopra, InfoCert, salvo cause di Forza Maggiore e/o per ordine di un'autorità pubblica, provvederà a comunicare al Cliente a mezzo e-mail e/o PEC - all'indirizzo indicato ai sensi dell'art. 22.1 - le motivazioni dell'adozione dei provvedimenti ivi stabiliti e avrà facoltà di risolvere il presente Accordo, senza alcun preavviso e senza per questo essere tenuta ad alcun risarcimento, e fatta salva ogni altra azione di rivalsa nei confronti del responsabile delle violazioni.

14.3 Salvo quanto specificato nei paragrafi successivi, qualora il Cliente si rendesse inadempiente ad un obbligo previsto nell'Accordo e non ponesse rimedio a tale inadempimento entro 30 (trenta) giorni dal ricevimento di una diffida ad adempiere *ex* art. 1454, c.c., inviata da InfoCert e contenente la descrizione dell'inadempimento e l'invito ad eseguire correttamente la prestazione entro il suddetto termine, il presente Accordo si intenderà risolto di diritto.

14.4 Sarà facoltà di InfoCert risolvere di diritto il presente Accordo *ex* art. 1456 c.c. mediante comunicazione scritta al Cliente, qualora quest'ultimo violi i seguenti articoli: art.1 (Oggetto); art.2 (Obblighi e garanzie del Cliente); art.7 (Proprietà Intellettuale); art.12 (Privacy); art.13 (Riservatezza); art.18 (Normativa antimafia e anticorruzione); art. 19 (D.Lgs. 231/2001 e Codice Etico).

14.5 Ciascuna Parte potrà recedere con effetto immediato, nel caso in cui l'altra Parte (i) sia dichiarata fallita o sottoposta a procedure concorsuali, o presenti essa stessa istanza per il proprio fallimento o per l'ammissione a procedure concorsuali (ii) abbia deliberato lo scioglimento e/o la messa in liquidazione.

14.6 Per salvaguardare la continuità dei Servizi oggetto dell'Accordo anche successivamente alla cessazione dello stesso, ove richiesto per iscritto dal Cliente, InfoCert si impegna a prestare i Servizi anche successivamente alla cessazione dell'efficacia dell'Accordo, per qualsiasi ragione intervenuta, per un periodo adeguato a garantire il completamento della transizione ad altro fornitore, periodo che in ogni caso non potrà superare i 6 (sei) mesi dalla data di cessazione di efficacia dell'Accordo.

14.7 Per la durata di tale proroga, InfoCert avrà diritto, per la prosecuzione dell'erogazione dei Servizi, ai medesimi corrispettivi già previsti nelle condizioni economiche concordate.

14.8 A fronte di apposito ulteriore corrispettivo da concordarsi in buona fede tra le Parti, InfoCert si impegna a fornire al Cliente la necessaria assistenza, anche quanto al trattamento dei dati, al fine di consentire l'eventuale affidamento ad altro e diverso fornitore dei medesimi servizi.

14.9 Le Parti, a decorrere da 6 (sei) mesi prima della scadenza dell'Accordo, avvieranno, su richiesta scritta del Cliente, le trattative volte alla predisposizione di un piano per il trasferimento dei Servizi e dei dati ad un terzo fornitore.

14.10 Ove raggiunto l'accordo, il piano prevederà:

- la definizione delle responsabilità di ciascuna delle Parti in relazione al trasferimento;
- la descrizione delle attività che ognuna delle Parti dovrà svolgere in relazione al trasferimento stesso;
- il calendario di esecuzione delle attività a carico di ciascuna delle Parti;
- il corrispettivo (anche eventualmente unitario, in termini di uomini/giorno) in favore di InfoCert per le attività di trasferimento.

14.11 Nel caso in cui non sia raggiunto un accordo sul piano di trasferimento, InfoCert sarà tenuta, alla scadenza del Contratto, esclusivamente a restituire al Cliente i dati oggetto del Servizio, in un formato standard comunemente utilizzato per quella tipologia di dati.

14.12 E' facoltà del Cliente, qualora intenda risolvere il presente Accordo di procedere nel rispetto delle casistiche previste dalla legge. Resta intesto che InfoCert garantisce, in sede di cessazione del contratto, un periodo di transizione obbligatorio: i) durante il quale InfoCert continuerà a prestare i suoi servizi TIC

o a esercitare le sue funzioni allo scopo di ridurre il rischio di perturbazioni presso il Cliente; ii) che permetta al Cliente di migrare verso un altro fornitore terzo di servizi TIC oppure di adottare soluzioni interne coerenti con la complessità del servizio prestato.

15. MODIFICHE CONTRATTUALI

15.1 Ogni modifica sarà valida ed efficace solo se concordata per iscritto tra le Parti. Ogni variazione dovrà essere comunicata da InfoCert per iscritto e acquisterà efficacia a partire dal trentesimo giorno successivo alla data di ricezione della comunicazione da parte del Cliente, salvo quest'ultimo decida di non voler accettare tale variazione e, pertanto, intenda recedere, dandone comunicazione ad InfoCert medesima.

16.OBBLIGHI POST CONTRATTUALI

16.1 Ove applicabile, in caso di cessazione del presente Accordo, le Parti si impegnano, previo accordo scritto circa le modalità e le condizioni economiche, a collaborare in buona fede al fine di assicurare il passaggio ordinato al Cliente, o ad altro fornitore da questi designato, dei dati e dei documenti oggetto del presente Accordo e/o di quanto necessario a garantire la continuità del Servizio al nuovo fornitore.

16.2 In caso di mancato accordo di cui sopra, InfoCert depositerà tali dati e documenti nell'area riservata del Cliente per un periodo di 60 (sessanta) giorni successivi alla cessazione del presente Accordo, affinché il Cliente stesso possa scaricarli nel formato definito da InfoCert.

16.3 In nessun caso, InfoCert sarà tenuta, senza la previsione di apposito corrispettivo, a trasferire i dati al Cliente o a terzi, in un formato diverso da quello definito da InfoCert, o ad interfacciarsi con i sistemi informatici di terzi soggetti indicati dal Cliente.

17.FORO COMPETENTE

17.1 Il presente Accordo è regolato dalla legge italiana.

17.2 In caso di controversia derivante o inerente al presente Accordo, la sua interpretazione, efficacia, esecuzione o risoluzione le Parti avranno la facoltà di raggiungere tra di loro una eventuale soluzione bonaria, entro 30 (trenta) giorni dal sorgere della controversia.

17.3 Rimasto infruttuoso il tentativo di conciliazione di cui al precedente 17.2, ciascuna Parte avrà il diritto di agire a propria tutela. In tal caso le Parti, di comune accordo, riconoscono e stabiliscono che per qualsiasi controversia dovesse insorgere in ordine al presente Accordo e/o relativi contratti/ordini attuativi, comprese quelle relative alla sua validità, interpretazione, esecuzione e risoluzione, sarà competente in via esclusiva il Foro di Roma.

18.NORMATIVA ANTIMAFIA E ANTICORRUZIONE

18.1 Nell'esecuzione del presente Accordo, il Cliente si obbliga a rispettare per sé e per i propri incaricati e/o dipendenti e/o collaboratori la normativa Antimafia e Anticorruzione, secondo quanto disposto rispettivamente dal D. Lgs. n. 159/2011 e dalla Legge n. 190/2012, e successive modificazioni e integrazioni ("**Normativa Antimafia e Anticorruzione**").

18.2 Il Cliente dichiara inoltre che nei propri confronti o dei propri incaricati e/o dipendenti e/o collaboratori non sussistono le cause di divieto, di sospensione o di decadenza previste dall'articolo 67 del D. Lgs. n. 159/2011.

19.D. LGS. 231/2001 E CODICE ETICO

19.1 Nell'esecuzione del presente Accordo, il Cliente si obbliga a rispettare per sé e per i propri incaricati e/o dipendenti e/o collaboratori, in maniera integrale e rigorosa, il D. Lgs. 231/2001 e ss.mm.ii., nonché il "Modello 231" e il Codice Etico adottati da InfoCert, presenti sul sito internet istituzionale, da considerarsi parte integrante e sostanziale del presente Accordo.

19.2 Resta espressamente inteso che, in caso di inadempimento del Cliente ad una qualsiasi delle obbligazioni di cui al presente articolo, InfoCert avrà facoltà di risolvere l'Accordo *ex* art. 1456, c.c., mediante semplice comunicazione scritta.

20. CESSIONE

20.1 Il presente Accordo non potrà essere ceduto dal Cliente, se non previo consenso scritto di InfoCert.
Resta salvo tra le Parti, che le società controllate come definite ai sensi dell'art.2359 c.c. del Cliente e/o società di cui il Cliente sia una controllata possono accedere al presente Accordo previa autorizzazione scritta da parte di InfoCert.

21. CAMBIO DI CONTROLLO

21.1 Nel caso in cui il Cliente sia soggetto al cambio di controllo, il Cliente si obbliga ad informare preventivamente InfoCert, la quale può riservarsi di recedere da tale Accordo a seguito della comunicazione.

22. VARIE

22.1 Le Parti comunicheranno mediante gli indirizzi che seguono:

- Se dirette a InfoCert: InfoCert S.p.A., Piazzale Flaminio 1/B, 00196 Roma; PEC: infocert@legalmail.it
- Se dirette al Cliente: agli indirizzi indicati nell'intestazione dell'Accordo.

Qualora una delle Parti cambiasse il suo indirizzo, questa darà comunicazione scritta all'altra Parte del nuovo indirizzo e della data dalla quale diventerà effettivo. In mancanza, qualsiasi comunicazione inviata ai precedenti recapiti si considererà consegnata, anche in caso di tentativo di recapito andato a vuoto.

22.2 Ciascuna Parte sarà sollevata da responsabilità ed esentata dall'obbligo di fornire la prestazione per tutto il tempo e fino a quando la stessa sia nell'impossibilità di adempiere, in tutto o in parte, per l'insorgenza di una causa di Forza Maggiore (a titolo meramente esemplificativo, guerra, moti popolari, scioperi o provvedimenti di autorità giudiziarie, disservizi dei gestori della rete elettrica, azioni di terzi o altre cause al di fuori del ragionevole controllo della/e Parte/i che impediscono in tutto o in parte l'esecuzione). In tali ipotesi, la mancata erogazione dei Servizi e/o del Software non costituirà inadempimento o motivo di sospensione dei pagamenti o di risoluzione del presente Accordo. La Parte che abbia avuto notizia di un evento causato da Forza Maggiore, ne darà immediata comunicazione scritta all'altra Parte e le Parti si incontreranno immediatamente, al fine di concordare gli eventuali rimedi preordinati al tempestivo ripristino della normale funzionalità dei Servizi e/o adempimento delle prestazioni previste dal presente Accordo, a seconda del caso.
In ogni caso, qualora un evento causato da Forza Maggiore impedisca la regolare esecuzione del presente Accordo per un periodo superiore a 60 (sessanta) giorni, ciascuna delle Parti avrà la facoltà di recedere dal presente Accordo dandone comunicazione all'altra Parte ai sensi dell'art. 22.1. e senza che nulla sia dovuto a quest'ultima a titolo di risarcimento o mancato guadagno, salvo il diritto di InfoCert al Corrispettivo per le attività già svolte e per quelle ulteriormente necessarie.

22.3 Qualora una clausola del presente Accordo fosse dichiarata nulla, entrambe le Parti saranno sollevate da tutti gli obblighi derivanti da detta clausola, senza che tale nullità affligga le altre clausole dell'Accordo. Per

quanto possibile, le clausole dichiarate nulle saranno automaticamente sostituite con nuove clausole di contenuto equivalente che perseguano le medesime finalità delle clausole dichiarate nulle.

22.4 Le Parti si danno reciprocamente atto che il presente Contratto ha formato oggetto di trattativa tra le Parti stesse, in ogni sua previsione, e che pertanto non trovano applicazione gli artt. 1341 e 1342, c.c., per i quali è prevista l'approvazione specifica.

23. NOMINA PER LO SVOLGIMENTO DELLE ATTIVITÀ DI UFFICIO DI REGISTRAZIONE ("Convenzione")

23.1 Oggetto

23.1.1 Ad integrazione dell'Accordo, InfoCert, nel suo ruolo di Autorità di Certificazione ("**CA**") e di gestore dell'identità digitale ("**IdP**") ai sensi del D.P.C.M. 24.10.2014 nonché di prestatore di servizi fiduciari accreditato presso l'Agenzia per l'Italia Digitale ("**AgID**"), ai fini dell'emissione dei propri Servizi è tenuta ad effettuare l'attività di identificazione degli Utenti, ferma restando la facoltà di delegare tali attività anche a soggetti terzi, ai sensi dell'art. 24 del Regolamento (UE) n. 910/2014 come modificato dal Regolamento (UE) n. 1183/2024 ("**Regolamento eIDAS**"). A tal fine, InfoCert può nominare il Cliente quale Ufficio di Registrazione (anche "**Registration Authority**" o, per brevità, "**RA**"), che ne faccia richiesta e che sia in possesso dei requisiti di legge, per lo svolgimento di specifiche attività qui di seguito identificate e lo stesso dovrà impegnarsi al rispetto degli obblighi specifici contenuti nell'Accordo e nei Manuali Operativi di riferimento del singolo Servizio nonché dei provvedimenti legislativi e amministrativi ivi richiamati.

23.1.2 La RA ha dichiarato di essere una persona giuridica dotata di una struttura organizzativa stabile, tale da garantire il corretto adempimento degli obblighi previsti nella presente Convenzione, nonché di essersi dotata dei requisiti minimi di sicurezza e di aver conseguito idonea certificazione ISO 27001 o di possedere requisiti equivalenti a tale certificazione, meglio esplicitati nell'Allegato E;

23.1.3 InfoCert metterà a disposizione dell'Ufficio di Registrazione un accesso ad una piattaforma dedicata ("**Piattaforma**"), propedeutica al caricamento e alla gestione di tutta la documentazione afferente al rapporto in essere con la RA medesima, quale, a titolo meramente esemplificativo e non esaustivo, i mandati necessari per lo svolgimento dell'attività da parte dei propri dipendenti e/o collaboratori;

23.1.4 Le attività di identificazione degli Utenti, richiesta di registrazione, emissione, revoca e sospensione dei certificati e consegna del dispositivo previste nei Manuali Operativi ("**Attività**") possono essere delegate dalla RA a singole persone fisiche, nelle modalità e nei termini meglio disciplinati nella presente Convenzione.

23.1.5 Con la sottoscrizione della presente Convenzione, il Cliente viene nominato quale RA di InfoCert, per l'erogazione del servizio di Firma Digitale, e/o di Carta Nazionale dei Servizi, e/o Certificati di Autenticazione e/o di SPID, a seconda di quanto specificato nell'allegato di Processo *sub* Allegato E, nonché di quanto previsto nell'Allegato A.

23.2 Servizi oggetto delle Attività

23.2.1 Le Attività svolte dalla RA sono propedeutiche all'identificazione certa degli Utenti, anche qualora ne facciano richiesta per il tramite di altri soggetti ("**Richiedenti**"), che hanno interesse ad usufruire dei servizi InfoCert come meglio infra descritti.

23.2.2 I servizi per la cui emissione ("**Servizi Trust**") è necessario l'espletamento delle Attività, durante la quale vengono acquisiti i dati forniti dall'Utente, sono i seguenti:

a) Certificato qualificato, la cui emissione è propedeutica al rilascio di una firma elettronica qualificata ("**Certificato/i**"), intendendosi per tale "*l'insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la chiave pubblica del soggetto certificato*";

b) Carta Nazionale dei Servizi ("**CNS**"), ossia il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni. In tale documento è contenuto un certificato digitale, ovvero l'associazione tra una chiave pubblica di crittografia ed un insieme di informazioni che identificano il soggetto che possiede la corrispondente chiave privata;

c) Certificato di Autenticazione, rilasciati e gestiti dal certificatore InfoCert, devono essere utilizzati nell'ambito dei protocolli S/MIME e SSL, con strumenti quali i Web browser e i prodotti di posta elettronica per verificare firme elettroniche avanzate create tramite dispositivo sicuro;

d) Credenziali SPID, ossia le credenziali necessarie per il rilascio dell'identità digitale ("**Identità Digitale**" o "**SPID**"), per l'accesso ai servizi in rete erogati dai fornitori che aderiscono al sistema SPID.

23.2.3 Le procedure di identificazione e registrazione sono esposte, rispetto al Certificato, nel Manuale Operativo ICERT-INDI-MO e ss.mm.ii. ("**Manuale Operativo Certificati**"), per CNS nel Manuale Operativo ICERT-INDI-CPCA-CNS e ss.ii. ("**Manuale Operativo CNS**"), per i Certificati di Autenticazione nel Manuale Operativo ICERT-INDI-MOCA e ss.ii. ("**Manuale Operativo Autenticazione**") e, rispetto al rilascio di Credenziali SPID, nel Manuale ICERT-MO-SPID e ss.mm.ii. ("**Manuale Operativo SPID**"), tutti depositati presso l'AgID, e disponibili sul sito internet di InfoCert nell'ultima versione aggiornata, nonché sono esposte nei provvedimenti legislativi e amministrativi richiamati nei Manuali stessi (congiuntamente, "**Manuali**" o "**Manuali Operativi**").

23.2.4 La RA svolgerà le Attività secondo una o più modalità di identificazione tra quelle previste all'interno dei Manuali, secondo le procedure di volta in volta definite con InfoCert e meglio descritte all'interno dell'allegato di processo sub Allegato E alla presente Convenzione.

23.3 Responsabilità e Obblighi dell'Ufficio di Registrazione

23.3.1 Per l'esercizio delle Attività ad esso demandate, l'Ufficio di Registrazione avrà facoltà di avvalersi di propri dipendenti e collaboratori a vario titolo, anche terzi rispetto alla propria organizzazione, appositamente incaricati e nominativamente individuati anche da InfoCert come Operatori di Registrazione ("**Registration Authority Officer**", per brevità "**R.A.O.**").

23.3.2 Ogni Ufficio di Registrazione dovrà altresì nominare, tra i propri R.A.O., un minimo di due soggetti che avranno compiti di gestione operativa e organizzativa delle attività tipiche della Piattaforma e che, pertanto, agiranno in nome e per conto della RA stessa ("**Master R.A.O.**"). Le attività demandate ai Master RAO e gli obblighi a loro carico saranno identificati nell'apposito mandato trilaterale sottoscritto tra questi, la RA e InfoCert ("**Mandato Master R.A.O.**").

23.3.3 Il rapporto tra InfoCert, l'Ufficio di Registrazione e i R.A.O. sarà disciplinato, anche sotto il profilo del trattamento dei dati personali, esclusivamente da un contratto di mandato che, a seconda dei casi, potrà essere trilaterale ("**Mandato R.A.O.**") o, qualora il R.A.O. lavori alle dipendenze di o in collaborazione con una persona giuridica diversa dalla RA, quadrilaterale ("**Mandato R.A.O. Supplier**", congiuntamente con il Mandato Master R.A.O., i "**Mandati**", i cui modelli si allegano sub E) alla presente Convenzione).

23.3.4 InfoCert conserva per sé e conferisce alle RA e ai propri Master R.A.O. la facoltà di revocare i suddetti Mandati in qualunque momento e a loro insindacabile giudizio, senza che il soggetto destinatario di tale provvedimento possa opporsi o avanzare pretese - anche economiche - al riguardo.

23.3.5 Ferma la responsabilità di InfoCert per quanto concerne l'erogazione dei Servizi, l 'Ufficio di Registrazione si impegna ad osservare i seguenti obblighi:

a) assumere, come di fatto assume con la sottoscrizione della Convenzione, gli obblighi descritti nei Manuali Operativi, nell'ultima versione tempo per tempo disponibile online sul sito di InfoCert, e garantire - come difatti garantisce con la sottoscrizione della Convenzione - di possedere e mantenere già un'organizzazione di personale e di beni adeguata all'esercizio delle Attività;
b) rispettare le procedure operative di rinnovo, revoca o sospensione dei Servizi Trust definite da InfoCert;
c) impedire l'accesso ai sistemi di InfoCert a Master R.A.O. e R.A.O. e assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniqualvolta venga revocato il rispettivo relativo Mandato da InfoCert, qualora cessi il rapporto di dipendenza/collaborazione tra l'Ufficio di Registrazione e il R.A.O. e/o Master R.A.O., ovvero si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del R.A.O.), dandone comunicazione per iscritto ad InfoCert entro 24 (ventiquattro) ore lavorative;
d) esercitare le Attività nell'interesse di InfoCert e con la diligenza del mandatario, ex art. 1710, c.c.;
e) svolgere le Attività nel rispetto della normativa vigente, dei Manuali Operativi e delle istruzioni ricevute da InfoCert, con particolare riferimento all'identificazione personale certa degli Utenti che richiedono l'emissione dei Servizi Trust;
f) verificare che ciascun Master R.A.O. e R.A.O., individuato per l'espletamento delle Attività, soddisfi i requisiti di competenza, affidabilità, onorabilità ed esperienza ai sensi dell'art. 24, par. 2, lett. b) del Regolamento eIDAS;
g) vigilare su Master R.A.O. e R.A.O., nel rispetto della normativa vigente, dei Manuali Operativi e delle istruzioni ricevute da InfoCert;
h) supervisionare, per conto di InfoCert, l'attività di formazione e/o aggiornamento dei R.A.O. e Master R.A.O.;
i) informare entro 8 (otto) ore InfoCert di eventuali vizi, difetti, interruzioni o malfunzionamenti del sistema e/o di errori nello svolgimento delle attività di identificazione e registrazione da parte dei R.A.O. e dei Master R.A.O.;
j) consentire alle Autorità di vigilanza, nonché agli incaricati di InfoCert, di accedere nei propri locali per verificare il corretto espletamento delle Attività ed il rispetto delle procedure per lo svolgimento delle stesse;
k) fornire evidenza, entro e non oltre 3 (tre) giorni dalla richiesta da parte di InfoCert, di tutta la documentazione relativa alle Attività, qualora la richiesta derivi da un'Autorità di vigilanza, dalla Polizia Giudiziaria e/o da altra Autorità ovvero da InfoCert stessa ai fini delle attività di verifica e dei controlli qualità che la stessa pone in essere nell'ambito della propria operatività;
l) sottoporre ai Richiedenti, siano esse persone fisiche o giuridiche che richiedono l'emissione dei Servizi Trust per conto dell'Utente, la documentazione contrattuale messa a disposizione da InfoCert, nonché concordare preventivamente con quest'ultima qualsiasi documento da rilasciare al Richiedente e/o Utente, relativamente alle attività di registrazione e/o di rilascio dei Servizi Trust;
m) mantenere strettamente riservate le credenziali ricevute da InfoCert per l'accesso alla Piattaforma e fornirle esclusivamente ai propri Master R.A.O. debitamente nominati, che ne avranno altresì l'obbligo di custodia (con contestuale espresso divieto di cessione anche temporanea a terzi in genere e ad altri operatori/collaboratori della RA), per un utilizzo finalizzato all'esclusivo espletamento delle attività precipue e nel rispetto delle obbligazioni assunte nel Mandato Master R.A.O.;

n) solidalmente con i Master R.A.O., obbligarsi ad un corretto utilizzo della Piattaforma, nelle modalità indicate da InfoCert;
o) provvedere ad un regolare caricamento/aggiornamento sulla Piattaforma di tutta la documentazione richiesta da InfoCert (a titolo meramente esemplificativo e non esaustivo: Mandati, modulistica di attivazione dei Servizi Trust), che dovrà essere fornita a quest'ultima entro i termini con essa convenuti, e in ogni caso qualora InfoCert ne faccia espressa richiesta.

23.3.6 L'Ufficio di Registrazione prende atto e accetta che non potrà vantare alcuna esclusiva per l'esercizio delle suddette Attività per conto di InfoCert; quest'ultima sarà pertanto libera di delegare tali Attività anche ad altri soggetti.

23.4 Obblighi di InfoCert

23.4.1 InfoCert si impegna nei confronti dell'Ufficio di Registrazione a:

a) fornire indicazioni sulle apparecchiature hardware e software necessarie per l'espletamento delle Attività;
b) impartire la formazione necessaria a svolgere le Attività, tramite corsi e documentazione *ad hoc*, utilizzabile dalla RA stessa anche per assolvere essa stessa gli obblighi formativi nei confronti dei R.A.O.;
c) impartire adeguata formazione ai Master R.A.O.;
d) aggiornare periodicamente, con una cadenza almeno di 12 mesi, adeguatamente il personale dell'Ufficio di Registrazione, ivi compresi Master R.A.O. e R.A.O., mediante opportuni corsi di formazione specifica;
e) dare consulenza e assistenza sulle problematiche connesse all'espletamento delle Attività;
f) svolgere con periodicità annuale le verifiche di sicurezza e di qualità dei Servizi Trust offerti;
g) conservare le informazioni concernenti l'identificazione, la registrazione ed emissione dei Certificati, sul proprio sistema di conservazione, ai sensi delle "*Linee Guida sulla formazione, gestione e conservazione dei documenti*", emanate da AgID con determinazione n. 407 del 2020 e ss.mm.ii., per 20 (venti) anni dalla scadenza di ogni Certificato;
h) conservare le informazioni concernenti la fase di identificazione e la documentazione contrattuale sottoscritta dagli Utenti, nel proprio sistema di conservazione, conformemente al DPCM 23.10.2014 e ss. mm. ii., per 20 (venti) anni decorrenti dalla scadenza o dalla revoca dell'Identità Digitale. L'Ufficio di Registrazione può accedervi, formulando specifica richiesta scritta e versando i corrispettivi all'uopo indicati.

23.5 Limitazioni e responsabilità

23.5.1 Fatte salve le disposizioni dei Manuali Operativi, l'Ufficio di Registrazione sarà responsabile, anche solidalmente con i propri R.A.O. e Master R.A.O., e sarà tenuta a manlevare InfoCert per ogni:

(i) danno diretto e indiretto, perdita, spesa legale e/o costo subito e/o sostenuto da InfoCert e/o dai titolari dei Certificati e/o da terzi, quale conseguenza diretta nell'esercizio delle attività delegate ivi previste, con espressa esclusione di ogni danno, diretto o indiretto, cagionato per caso fortuito o forza maggiore;
(ii) sanzione amministrativa e/o pecuniaria comminata ad InfoCert per violazioni riconducibili alle condotte dell'Ufficio di Registrazione e/o dei propri R.A.O. e Master R.A.O..

23.5.2 Nel caso in cui InfoCert rilevi eventuali anomalie o irregolarità nello svolgimento delle Attività, da parte di RA, Master R.A.O. o R.A.O., potrà valutare l'adozione di azioni specifiche, anche mediante eventuali escalation e/o azioni puntuali e/o attività di audit nei confronti dell'Ufficio di Registrazione.

23.6 Corrispettivi

23.6.1 Per lo svolgimento delle Attività, l'Ufficio di Registrazione non potrà vantare il pagamento di somme, corrispettivi, provvigioni o quant'altro da parte di InfoCert.

23.6.2 La fatturazione all'Ufficio di Registrazione dei Servizi – anche Trust – resi da InfoCert e dell'eventuale materiale da questa fornito per l'espletamento delle Attività, verrà effettuata in base all'Offerta allegata sub A) appositamente formulata dalla stessa InfoCert e/o in base al listino tariffario, e sue eventuali modifiche, vigente durante il periodo di validità dell'Accordo.

23.7 Privacy

23.7.1 Per le finalità della presente Convenzione, le Parti definiranno i rispettivi ruoli all'interno del separato accordo sul trattamento dei dati ai sensi dell'Allegato B – DPA all'Accordo.

23.8 Sospensione. Risoluzione. Recesso. Clausola risolutiva espressa.

23.8.1 Facendo salvo quanto previsto ai sensi dell'art. 14 dell'Accordo, sarà facoltà di InfoCert risolvere di diritto la presente Convenzione, ex art. 1456 c.c., qualora l'Ufficio di Registrazione violi le disposizioni dell'art. 23.3.5 e in particolare non adempia all'obbligo di cui alla lett. c) d'impedire l'accesso ai sistemi di InfoCert a Master R.A.O. e R.A.O. nonché l'obbligo di assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività qualora InfoCert disponga la revoca di uno o più Mandati.

23.8.2 In caso di cessazione da parte di InfoCert dell'erogazione dei Servizi, l'Ufficio di Registrazione verrà debitamente informato tramite una comunicazione di Posta Elettronica Certificata almeno con un anticipo di 3 (tre) mesi sulla data di efficacia della cessazione.

23.8.3 Qualora InfoCert ravvisi nell'ambito dell'operato della RA dei comportamenti dolosi o riconducibili a colpa grave e/o che comunque siano lesivi degli interessi di InfoCert in quanto afferenti alla sfera di comportamenti censurabili (in questi casi, anche quindi per colpa lieve), a titolo esemplificativo, da un punto di vista antifrode, InfoCert si ritiene libera di risolvere l'Accordo ai sensi dell'art. 1456 c.c.

23.8.4 Nei casi previsti agli articoli 23.8.1., 23.8.2. e 23.8.3, l'Ufficio di Registrazione non potrà vantare alcuna richiesta nei confronti di InfoCert, neanche per eventuali danni subiti in conseguenza di tali eventi, né altresì in caso di recesso e/o di revoca della presente Convenzione proveniente da InfoCert.

Lista Allegati:

Allegato A – Offerta Commerciale
Allegato B – DPA
Allegato C – Allegato Tecnico
Allegato D – Misure di Sicurezza
Allegato E – Documentazione per l'Ufficio di Registrazione (Modello di Mandato R.A.O.; Mandato R.A.O. Supplier e Mandato Master R.A.O.; Allegato di processo)

_____ (InfoCert S.p.A.)

_____ (Il Cliente)

tinexta infocert

NOME CLIENTE

Offerta commerciale

Trasmissione a mezzo e-mail all'indirizzo xxxxxxxxxxx

Luogo e data

Spettabile Cliente,

con la presente siamo lieti di proporVi la nostra migliore Offerta economica per la fornitura dei seguenti Servizi:

Servizio	Prezzo (IVA esclusa)	Descrizione	Fascia

Qui di seguito, altresì, sono esposte le **Modalità di Fatturazione** applicabili:

Servizio	Modalità di Fatturazione	Percentuale

Per maggiori dettagli relativi alla descrizione dei Servizi, si rinvia al relativo Allegato Tecnico ed al Manuale operativo (laddove presente).

La presente Offerta, che ci auguriamo possa incontrare le Vostre esigenze, ha validità di due mesi dalla data della stessa.

Vi precisiamo che l'erogazione della fornitura dei Servizi menzionati nella presente Offerta, che Vi preghiamo di restituirci sottoscritta per accettazione, verrà regolata dall'apposito Contratto di Fornitura dei Servizi InfoCert ("**Accordo**") in essere tra le Parti, sottoscritto in data xxxxxxxxxxxxxx.

Per qualsiasi necessità in merito alla presente potete contattare XXXXXXXXXXXXXXX.

In attesa di un Vostro gradito riscontro, cogliamo l'occasione per porgere i nostri migliori saluti.

Lista Allegati:
Allegato C – Allegato Tecnico

InfoCert S.p.A.
xxxxxxx

_____
Firma del Cliente per accettazione

ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI

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

TRA

[-], con sede legale in [-], C.F. e P.IVA [-], in persona del proprio legale rappresentante *pro tempore* xxxxxxx(“**Cliente**”)

E

InfoCert S.p.A., società soggetta alla direzione ed al coordinamento di Tinexta S.p.A., con sede legale in Piazzale Flaminio 1/B, 00196 - Roma (Italia), C.F. e P.IVA 07945211006, in persona di Danilo Cattaneo (“**InfoCert**”)

(InfoCert e il Cliente, ciascuna singolarmente, anche "**Parte**" e, congiuntamente, "**Parti**").

Premesso che

A. InfoCert ed il Cliente stanno formalizzando un Accordo di fornitura dei servizi (di seguito l’“**Accordo**”) – di cui questo accordo costituisce un allegato – avente ad oggetto la fornitura al Cliente di servizi sottoposti alla regolamentazione normativa specifica dei servizi Trust (di seguito i “**Servizi**”), ed una licenza d’uso (“**Licenza**”) di una piattaforma (“**Software**”), come meglio definita negli allegati all’ Accordo;

B. il Cliente, prima di affidare ad InfoCert lo svolgimento dei Servizi, ha valutato che InfoCert ha posto in essere misure tecniche e organizzative adeguate, affinché il trattamento soddisfi i requisiti del Regolamento (UE) 2016/679 ("**Regolamento**" o “**GDPR**”), del D.lgs. 196/2003 e ss.mm.ii. (“**Codice Privacy**”) e, in genere, della normativa *data protection* applicabile, ivi inclusi i provvedimenti e le linee guida emesse dalle Autorità di controllo competenti e dal Comitato Europeo per la Protezione dei Dati (“**EDPB**”), e ad assicurare la tutela dei dati personali trattati e dei diritti delle persone fisiche a cui questi si riferiscono (“**Interessati**”), tenuto conto della natura dei dati personali trattati, delle finalità per cui tali dati sono trattati e del contesto dell’organizzazione;

C. con il presente accordo ("**Contratto**"), il Cliente intende nominare InfoCert quale proprio responsabile del trattamento dei dati personali ai sensi dell’articolo 28 del GDPR e fornirle le istruzioni funzionali a disciplinare le attività di trattamento dei dati personali di cui il Cliente è titolare affidate alla stessa InfoCert. In questo senso, InfoCert dichiara e garantisce di aver posto in essere misure tecniche e organizzative adeguate al soddisfacimento dei requisiti del Regolamento e del Codice Privacy e, in genere, della normativa *data protection* applicabile e ad assicurare la tutela degli Interessati, tenuto conto della natura dei dati personali trattati, delle finalità per cui tali dati sono trattati e del contesto dell’organizzazione;

D. parimenti, potrebbe verificarsi che il Cliente effettui, per conto di InfoCert, attività di trattamento di dati personali di cui InfoCert è titolare ai sensi del Regolamento e, in tal senso, il Cliente viene, pertanto nominato responsabile. A tal fine dichiara e garantisce di aver posto in essere misure tecniche e organizzative adeguate al soddisfacimento dei requisiti del Regolamento, del Codice Privacy e, in genere,

della normativa *data protection* applicabile, ivi inclusi i provvedimenti e le linee guida emesse dalle Autorità di controllo competenti e dall'EDPB e ad assicurare la tutela dei dati personali trattati e degli Interessati, tenuto conto della natura dei dati personali trattati, delle finalità per cui tali dati sono trattati e del contesto dell'organizzazione;

E. la definizione dei ruoli sopra descritti varia a seconda del servizio scelto ed è rinvenibile nella tabella riportata sub-allegato I;

F. con il presente Contratto si intende pertanto perfezionare la nomina a responsabile del trattamento dei dati personali, ai sensi dell'articolo 28, GDPR, e fornire le istruzioni necessarie per svolgere le operazioni di trattamento dei dati personali.

Tutto ciò premesso, le Parti convengono e stipulano quanto segue.

1. Premesse e allegati

1.1. Le premesse e gli allegati costituiscono parte integrante e sostanziale del Accordo.

2. Interpretazione

2.1. Quando il Contratto utilizza termini definiti nel GDPR, tali termini hanno il medesimo significato di cui al Regolamento.

2.2. Le clausole di cui al Contratto vanno lette alla luce delle disposizioni del GDPR, del Codice Privacy e, in genere, della normativa data protection applicabile.

2.3. Le clausole di cui al Contratto non devono essere interpretare in un senso che non sia conforme ai diritti e agli obblighi previsti nel Regolamento, nel Codice Privacy, e, in genere, nella normativa data protection applicabile, e/o che pregiudichi i diritti e le libertà fondamentali degli Interessati.

3. Gerarchia

3.1. In caso di contraddizione tra le clausole del Contratto e le disposizioni di accordi correlati, vigenti tra le Parti alla data dell'Accordo, o conclusi successivamente, le clausole del Contratto avranno prevalenza.

4. Descrizione del trattamento

4.1. I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati dal Responsabile per conto del Titolare, sono specificati nell'allegato I.

5. Obblighi delle Parti

5.1. Fermo restando quanto sancito dalle disposizioni di legge e regolamentari applicabili, il Titolare è obbligato a:

5.1.1. determinare la tipologia di dati personali che il Responsabile può trattare nell'ambito del rapporto stabilito tra le Parti e fornire chiare e precise istruzioni per iscritto al Responsabile in merito al trattamento configurato;

5.1.2. garantire che agli Interessati siano state fornite sufficienti informazioni, in conformità con le disposizioni applicabili in materia di protezione dei dati personali, in merito al trattamento dei loro dati personali;

5.1.3. garantire che sussiste una base legale per il trattamento dei dati personali degli Interessati, inclusi i necessari consensi qualora siano richiesti dalle norme applicabili in materia di protezione dei dati personali;

5.1.4. garantire che il trattamento che il Responsabile è tenuto ad effettuare per conto del Titolare, ai sensi del presente Accordo, avvenga nel rispetto di tutti i doveri e gli obblighi che gravano sul Titolare ai sensi delle disposizioni applicabili in materia di protezione dei dati personali.

5.2. Fatti salvi gli altri obblighi previsti dalle disposizioni di legge e regolamentari applicabili, il Responsabile si impegna a:

5.2.1. trattare i dati personali soltanto sulla base del presente Contratto dei relativi allegati e su istruzione documentata impartita dal Titolare, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile. In tal caso, il Responsabile informa il Titolare circa tale obbligo giuridico prima di effettuare l'ulteriore trattamento, a meno che il diritto applicabile lo vieti per rilevanti motivi di interesse pubblico. Il Titolare può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate;

5.2.2. informare immediatamente il Titolare qualora, ad avviso del Responsabile, un'istruzione impartita dal Titolare sia in violazione del Regolamento o di altre disposizioni di legge applicabili in materia di protezione dei dati personali. In tal caso, il Titolare si impegna a modificare le istruzioni oggetto della segnalazione, fermo restando che, in nessun caso, il Responsabile potrà ritenersi imputabile di eventuali violazioni della normativa applicabile derivanti dalla istruzione contestata;

5.2.3. trattare i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato I, salvo ulteriori istruzioni del Titolare;

5.2.4. trattare i dati personali soltanto per la durata specificata nell'allegato I;

5.2.5. mettere in atto le misure di sicurezza tecniche e organizzative specificate nell'allegato II. Nel valutare l'adeguato livello di sicurezza, le Parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione per il Responsabile, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli Interessati e di eventuali violazioni dei dati personali;

5.2.6. concedere l'accesso ai dati personali oggetto di trattamento ai membri del suo personale o a suoi collaboratori soltanto nella misura strettamente necessaria per l'attuazione e la gestione del Accordo e/o dei Servizi. Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali si sono impegnate alla riservatezza o hanno un adeguato obbligo legale di riservatezza;

5.2.7. applicare limitazioni specifiche e/o garanzie supplementari qualora il trattamento riguardi dati personali che rivelino dati biometrici intesi a identificare in modo univoco una persona fisica, ("**Dati particolari**");

5.2.8. adottare misure che gli consentano di dimostrare il rispetto del Contratto;

5.2.9. rispondere prontamente e adeguatamente alle richieste di informazioni del Titolare relative al trattamento dei dati e mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto da parte del Responsabile degli obblighi di cui al Contratto e di quelli che derivano direttamente dal Regolamento e/o dalla normativa data protection applicabile, purché ciò non pregiudichi la riservatezza di altri clienti del Responsabile o obblighi normativi di riservatezza a cui lo stesso è tenuto. Su richiesta del Titolare, il Responsabile consente e contribuisce alle attività di revisione delle attività di trattamento di cui al Contratto, a intervalli ragionevoli o se vi sono evidenze o indizi di inosservanza. Il Titolare può scegliere di condurre l'attività di revisione autonomamente o incaricare un consulente indipendente. Il Responsabile, inoltre, riconosce ed accetta che tale attività, se del caso, potrebbe essere condotta anche direttamente dal titolare del trattamento o da consulenti dallo stesso incaricati. A tale riguardo, il Responsabile si impegna all'ordinata e diligente tenuta della documentazione inerente alle attività di trattamento e alla prestazione dei Servizi di cui al Contratto, rendendola accessibile al Titolare o ai soggetti da questi designati per eventuali ispezioni. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del Responsabile. In tal caso, con un preavviso minimo di 24 (ventiquattro) ore, il Titolare del trattamento - potrà disporre un accesso presso la sede del Responsabile o altro luogo nella disponibilità giuridica del Responsabile in cui sia conservata la documentazione relativa alle attività di trattamento - sostenendone i relativi costi e dando preventiva comunicazione al Responsabile delle generalità dei soggetti incaricati delle verifiche. I costi delle verifiche di cui al presente paragrafo saranno addebitati al Responsabile qualora, all'esito delle stesse, risulti un inadempimento anche di solo uno degli obblighi di cui al presente Contratto o al Accordo ovvero violazioni del Regolamento e/o della normativa data protection applicabile. Su richiesta, le Parti mettono a disposizione della o delle Autorità di controllo competenti le informazioni di cui al presente paragrafo, compresi i risultati di eventuali attività di revisione;

5.2.10. notificare al Titolare del trattamento eventuali richieste provenienti dagli Interessati, non rispondere egli stesso alle richieste, a meno che sia stato autorizzato in tal senso dal Titolare, e assistere il Titolare nell'adempimento degli obblighi di rispondere alle richieste degli Interessati per l'esercizio dei loro diritti;

5.2.11. tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del Responsabile e ferma restando la esclusiva responsabilità del Titolare nello svolgimento di tali attività, assistere il Titolare nelle eventuali attività connesse alla valutazione d'impatto sulla

protezione dei dati personali di cui all'art. 35 del Regolamento e, se richiesto, cooperare con il Titolare nell'ambito delle consultazioni preventive di cui all'art. 36 del Regolamento;

5.2.12. assistere il Titolare nell'obbligo di garantire che i dati personali siano esatti e aggiornati;

5.2.13. assistere il Titolare nell'adempimento degli obblighi in materia di misure di sicurezza tecniche ed organizzative di cui all'art. 32 del Regolamento, nella misura prevista ai sensi dell'allegato II;

5.2.14. tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile, assistere il Titolare nell'adempimento degli obblighi in materia di notificazione dei dati personali che incombono su quest'ultimo ai sensi degli artt. 33 e 34 del Regolamento. Nello specifico:

a. in caso di violazione riguardante i dati trattati dal Titolare, il Responsabile assiste il Titolare, per quanto di propria competenza in ragione dei rapporti contrattuali in essere tra le Parti: (i) nel notificare, ove opportuno/necessari ai sensi del GDPR, la violazione dei dati personali alla o alle Autorità di controllo competenti; (ii) nell'ottenere le informazioni che, in conformità dell'articolo 33, paragrafo 3, del Regolamento, devono essere indicate nella notifica del Titolare; (iii) nell'adempiere, in conformità dell'articolo 35 del Regolamento, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali agli Interessati, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

b. In caso di violazione dei dati personali trattati dal Responsabile, quest'ultimo ne dà notifica al Titolare senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica del Responsabile al Titolare contiene almeno: (x) una descrizione della natura della violazione; (y) i recapiti di un punto di contatto del Responsabile presso il quale possono essere ottenute maggiori informazioni; (z) indicazioni in merito a probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione o per attenuarne i possibili effetti negativi. Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale del Responsabile al Titolare contiene le informazioni disponibili in quel momento; le altre informazioni sono fornite successivamente, non appena disponibili.

5.2.15. cancellare o restituire - a scelta del Titolare - tutti i dati personali oggetto di trattamento in caso di cessazione dell'efficacia del presente Contratto, salvi gli obblighi di conservazione dei dati personali eventualmente derivanti dal diritto dell'Unione o degli Stati membri;

5.2.16. non comunicare a terzi, salvo quanto previsto dall'articolo 6 ovvero in caso di consenso espresso in forma scritta del Titolare, i dati personali oggetto di trattamento;

6. Designazione di sub-responsabili

6.1. Laddove InfoCert operi in qualità di Responsabile, ha l'autorizzazione generale del Titolare per ricorrere a sub-responsabili del trattamento ("***Sub*-responsabili**") sulla base di un elenco sempre disponibile per

il Titolare a richiesta dello stesso all'indirizzo mail richieste.privacy@legalmail.it. Il Responsabile fornisce al Titolare le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

6.2. Laddove il Cliente assuma la veste di Responsabile, non può affidare a un *sub*-responsabile del trattamento ("***Sub*-responsabile**") i trattamenti da effettuare per conto del Titolare senza la preventiva autorizzazione specifica e scritta del Titolare, ma deve presentare la richiesta di autorizzazione specifica almeno 30 giorni prima di ricorrere al *Sub*-responsabile del caso, unitamente alle informazioni necessarie per consentire al Titolare di decidere in merito alla concessione o meno dell'autorizzazione.

6.3. Qualora il Responsabile ricorra a un *Sub*-responsabile per l'esecuzione di specifiche attività di trattamento, l'accordo che disciplina i rapporti tra Responsabile e *Sub*-responsabile dovrà prevedere l'imposizione, nei confronti del *Sub*-responsabile, di obblighi nella sostanza equivalenti a quelli gravanti sul Responsabile ai sensi del presente Accordo.

6.4. Il Responsabile si assicura che il *Sub*-responsabile rispetti gli obblighi a cui il Responsabile è soggetto a norma dell'Accordo e del Regolamento.

6.5. Il Responsabile rimane responsabile nei confronti del Titolare dell'adempimento degli obblighi del *Sub*-responsabile del trattamento derivanti dall'accordo che questi ha stipulato con il Responsabile, notificando al Titolare eventuali gravi inadempimenti, da parte del *Sub*-responsabile, degli obblighi contrattuali ove questi possano comportare una violazione del Regolamento.

7. Trasferimenti internazionali

7.1. Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del Responsabile è effettuato nel rispetto del capo V del Regolamento.

7.2. Il Titolare conviene che, qualora il Responsabile ricorra a un *Sub*-responsabile conformemente al precedente articolo 6 per l'esecuzione di specifiche attività di trattamento per conto del Titolare e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del Regolamento, il Responsabile e il *Sub*-responsabile possono garantire il rispetto del capo V del Regolamento utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del Regolamento, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

8. Durata ed effetti dell'Accordo

8.1. Il presente Contratto è efficace dal momento della sottoscrizione. Esso cesserà di avere efficacia in caso di cessazione, a qualsiasi causa dovuta, dell'efficacia dell'Accordo.

9. Inosservanza dell'Accordo, recesso e risoluzione

9.1. Qualora il Responsabile violi gli obblighi che gli incombono a norma del Contratto, il Titolare può dare istruzione al Responsabile di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti l'Accordo. Il Responsabile informa prontamente il Titolare qualora, per qualunque motivo, non sia in grado di rispettare il Contratto.

9.2. Il Titolare ha diritto di risolvere il Contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

9.2.1. il trattamento dei dati personali da parte del Responsabile sia stato sospeso dal Titolare in conformità al precedente paragrafo 9.1 e il rispetto delle clausole del Contratto non sia ripristinato entro un termine ragionevole in ogni caso entro un mese dalla sospensione;

9.2.2. il Responsabile violi in modo sostanziale o persistente le clausole del Contratto o gli obblighi che gli incombono a norma del Regolamento e/o della normativa data protection applicabile;

9.2.3. il Responsabile non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle Autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità al Contratto o al Regolamento e/o della normativa data protection applicabile.

9.3. Il Responsabile ha il diritto di risolvere il Contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il Titolare che le sue istruzioni violano i requisiti giuridici applicabili, il Titolare del trattamento insista sul rispetto delle istruzioni.

10. Disposizioni finali

10.1. Il corrispettivo del Responsabile per l'esecuzione del presente Contratto si intende ricompreso nel corrispettivo concordato dalle Parti per l'esecuzione dell'Accordo.

10.2. L'invalidità, inefficacia o inapplicabilità di talune disposizioni del presente Contratto non inficia la validità, efficacia o applicabilità delle altre disposizioni del presente Contratto. Le Parti si impegnano a sostituire una disposizione invalida, inefficace o altrimenti inapplicabile con una disposizione valida ed efficace che si avvicini all'intento originario dal punto di vista economico. Lo stesso vale per le disposizioni mancanti.

10.3. Il presente Contratto è regolato dalla legge italiana, con esclusione delle norme di diritto internazionale privato.

10.4. Ogni controversia relativa alla validità, efficacia e interpretazione del presente Contratto è devoluta alla competenza esclusiva del Foro di Roma.

10.5. Le modifiche e le integrazioni al Contratto devono essere approvate in forma scritta dalle Parti. Lo scambio di *email* non integra il requisito della forma scritta. Gli accordi orali sono inefficaci. Per tutto quanto non espressamente in questa sede previsto, il presente Contratto è disciplinato dalle disposizioni di legge applicabili.

10.6. Il mancato esercizio ad opera di una delle Parti di un qualsiasi diritto o facoltà garantiti dalla legge o dal presente Contratto non costituirà rinuncia a tali diritti e facoltà.

10.7. Le Parti danno atto che il presente Contratto è stato oggetto di trattativa individuale e che, pertanto, gli articoli 1341 e 1342, c.c., non trovano applicazione.

[LUOGO E DATA]

InfoCert S.p.A. [-]

_____ _____

tinexta infocert

ALLEGATO I

SERVIZIO	TITOLARE	RESPONSABILE
FIRMA DIGITALE (QUALIFICATA)	InfoCert	Cliente RA
FIRMA ELETTRONICA AVANZATA (ITALIA)	Cliente	InfoCert
FIRMA ELETTRONICA AVANZATA (INTERNAZIONALE)	InfoCert	Cliente RA
FIRMA SEMPLICE	Cliente	InfoCert
FIRMA ONE SHOT	InfoCert	Cliente RA
SIGNATURE API	Cliente	InfoCert
SIGNATURE API (HASH)	Cliente	InfoCert
MARCA TEMPORALE	Cliente	InfoCert
SERVIZIO DI CONVALIDA DI FIRME E SIGILLI QSVS	Cliente	InfoCert
DEVICE ID	InfoCert	Cliente RA
TOP	Cliente	InfoCert
TOP ID PROTECT	Cliente	InfoCert
LEGALDOC	Cliente	InfoCert
SAFE LTA	Cliente	InfoCert
SECURE DRIVE	Cliente	InfoCert
GOSIGN	Cliente	InfoCert
LEGAL MAIL	InfoCert/ Cliente	
LEGAL INVOICE HUB	InfoCert/ Cliente	
LEGAL INVOICE PRO	InfoCert/ Cliente	
LEGAL INVOICE START-GO	InfoCert/ Cliente	
GONOTICE	Cliente	InfoCert
SPID (IDENTITY PROVIDER)	InfoCert	Cliente RA
EIDGATEWAY	Cliente	InfoCert
IPP	InfoCert	Cliente
NCAR	InfoCert	Cliente
PROXYSIGN	Cliente	InfoCert
AUTOGESTIONE	InfoCert	Cliente
TRUSTY	Cliente	InfoCert
SERVIZIO DI TROUBLE TICKETING (FRUITO DIRETTAMENTE DALL'UTENTE DEL SERVIZIO)	InfoCert	
SERVIZIO DI TROUBLE TICKETING (FRUITO DALL'UTENTE DEL SERVIZIO PER IL TRAMITE DEL CLIENTE)	Cliente	InfoCert
LEGALCARE	CLIENTE	INFOCERT

DESCRIZIONE DEL TRATTAMENTO EFFETTUATO DA INFOCERT IN QUALITÀ DI RESPONSABILE

A. Categorie di interessati i cui dati personali sono trattati

Utenti finali dei Servizi

B. Categorie di dati personali trattati

In generale:

- nominativo, indirizzo, codice fiscale o altri elementi di identificazione personale, ivi inclusi i dati contenuti all'interno del documento d'identità e dei chip presenti sui documenti di riconoscimento;
- Dati di contatto (e-mail, pec, recapito telefonico, indirizzo di residenza/domicilio);
- Dati finanziari (IBAN, account paypal, numero carta di credito);
- Log applicativi e log di accesso ai Servizi;
- Credenziali (user ID e Password);

In particolare, a seconda della tipologia di servizio acquistato, potranno essere trattati in aggiunta a quelli sopra menzionati, i seguenti dati:

- dati relativi allo svolgimento delle attività economiche dell'interessato (tra cui P.IVA) ed ogni altra informazione contenuta all'interno delle fatture;
- tutti i dati potenzialmente contenuti all'interno dei documenti inviati in conservazione nonché i metadati di conservazione a norma;
- dati biometrici;
- immagini selfie e video
- tutti i dati contenuti all'interno dei file caricati nelle piattaforme messe a disposizione dal Responsabile.

C. Dati particolari trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.

A seconda della tipologia di Servizio acquistata potrebbero essere trattati dati biometrici

D. Natura del trattamento

Raccolta, Registrazione, Organizzazione, Strutturazione, Conservazione, Adattamento o modifica, Estrazione, Consultazione, Uso, Comunicazione mediante trasmissione, Raffronto, Interconnessione, Limitazione, Cancellazione, Distruzione.

E. Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

In generale, la finalità consiste nel trattamento dei dati strettamente necessari all'erogazione dei Servizi ed il relativo supporto tecnico.

F. Durata del trattamento

SERVIZIO	DURATA DEL TRATTAMENTO
FIRMA ELETTRONICA AVANZATA (ITALIA)	durata del contratto
FIRMA SEMPLICE	durata del contratto
SIGNATURE API	durata del contratto
SIGNATURE API (HASH)	durata del contratto
MARCA TEMPORALE	durata del contratto
SERVIZIO DI CONVALIDA DI FIRME E SIGILLI QSVS	durata del contratto
TOP	90 giorni
TOP ID PROTECT	durata del contratto
LEGALDOC	durata del contratto
SAFE LTA	durata del contratto
SECURE DRIVE	durata del contratto
GOSIGN	60 GIORNI
LEGAL INVOICE HUB	durata del contratto
LEGAL INVOICE PRO	durata del contratto
LEGAL INVOICE START-GO	durata del contratto
GONOTICE	durata del contratto
E ARCHIVING	durata del contratto
EIDGATEWAY	durata del contratto
TRUSTY	durata del contratto
LEGALCARE	durata del contratto
SERVIZIO DI TROUBLE TICKETING (FRUITO DALL'UTENTE DEL SERVIZIO PER IL TRAMITE DEL CLIENTE)	3 anni dalla chiusura del ticket

DESCRIZIONE DEL TRATTAMENTO EFFETTUATO DAL CLIENTE IN QUALITÀ DI RESPONSABILE

A. Categorie di interessati i cui dati personali sono trattati
Utenti finali

B. Categorie di dati personali trattati

Dati anagrafici
Documenti di identità
Dati di contatto
Eventuali dati relativi al servizio oggetto dell'Accordo

C. Dati particolari trattati (se del caso) e limitazioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, ad esempio una rigorosa limitazione delle finalità, limitazioni all'accesso (tra cui accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, limitazioni ai trasferimenti successivi o misure di sicurezza supplementari.

N.A.

D. Natura del trattamento

Raccolta, consultazione, uso, cancellazione (su richiesta dell'interessato)

E. Finalità per le quali i dati personali sono trattati per conto del titolare del trattamento

In generale, la finalità consiste nel trattamento dei dati strettamente necessari all'erogazione dei Servizi

F. Durata del trattamento

SERVIZIO	RETENTION PERIOD
FIRMA DIGITALE QUALIFICATA	Durata del contratto
FIRMA ELETTRONICA AVANZATA (INTERNAZIONALE)	Durata del contratto
FIRMA ONE SHOT	Durata del contratto
DEVICE ID	Durata del contratto
NCAR	Durata del contratto
AUTOGESTIONE	Durata del contratto
SPID (IDENTITY PROVIDER)	Durata del contratto
IPP	Durata del contratto

ALLEGATO II

MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

A. Misure di sicurezza tecniche e organizzative richieste al e messe in atto dal Responsabile per garantire un adeguato livello di sicurezza e per essere in grado di fornire assistenza al Titolare.

Ai fini della descrizione completa delle misure tecniche ed organizzative per la sicurezza dei dati possono essere forniti i seguenti documenti di dettaglio:

1. Framework Nazionale Cyber Security: misure di sicurezza adottate con relative evidenze, relativamente ai controlli applicabili al servizio in oggetto.

B. Misure specificamente previste per la condivisione dei dati personali con eventuali Sub-responsabili, e misure tecniche e organizzative che l'eventuale Sub-responsabile deve prendere per essere in grado di fornire assistenza al Titolare.

Il Responsabile del Trattamento si impegna a trasferire sul Sub-responsabile le misure indicate alla lettera A) del presente allegato ed a dare ulteriori istruzioni al Sub-responsabile sulla base della tipologia di trattamento effettuata.

ALLEGATO TECNICO

Certificati qualificati e di autenticazione e servizi di firma qualificata.

Sommario

***

1. RIFERIMENTI ESTERNI

Documentazione	Link di dettaglio
CP e CPS (Manuale Operativo) per emissione certificati qualificati	https://pki.infocert.it/pdf/ICERT_INDI_MO.pdf
CP e CPS (Manuale operativo) per emissione certificati di Autenticazione	https://pki.infocert.it/pdf/ICERT_INDI_MOCA.pdf
per certificati di autenticazione CNS	Ente Certificatore InfoCert Certificati di Autenticazione per la Carta Nazionale dei Servizi Certificate Policy
PDS (PKI Disclosure Statement) per i certificati qualificati	https://pki.infocert.it/pdf/ICERT_INDI_PDS.pdf
Link di supporto (FAQ, Video, Guide)	https://help.infocert.it/cerca? = searchText Firma%20Digitale&idProdotto=33

2. DESCRIZIONE DEL SERVIZIO - INTRODUZIONE

InfoCert opera in qualità di prestatore di servizi fiduciari qualificati (d'ora in avanti, "**QTSP**" *Qualified Trust Service Provider*) per il servizio di emissione di Certificati Qualificati su dispositivo fisico o remoto, nel rispetto del proprio Manuale Operativo (d'ora in avanti anche "**CPS**" *Certificate Practice Statement)* e del proprio *PKI Disclosure Statement* (d'ora in avanti, "**PDS**").

Per tale servizio InfoCert ha ottenuto una valutazione di conformità effettuata dal *Conformity Assesment Body* CSQA Certificazioni S.r.l., ai sensi del Regolamento (UE) n. 910/2014 così come modificato dal Reg. (UE) 2024/1183 of the European Parliament and of the Council of April 2024.(d'ora in avanti, "**Regolamento eIDAS**") e delle norme ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, secondo lo schema di valutazione eIDAS definito da ACCREDIA a fronte delle norme ETSI EN 319 403

e UNI CEIISO/IEC 17065:2012, nonché dal D.P.C.M. 22.02.2013, e dal Decreto Legislativo 7 marzo 2005, n. 82 (CAD) e successive modifiche (collettivamente, d'ora in avanti, la "**Normativa Applicabile**").
Per tale servizio InfoCert ha ottenuto accreditamento presso AgID ed è presente, come previsto dal regolamento eIDAS nella *Trusted Service List* Europea (https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls).
La firma elettronica qualificata o digitale o di sottoscrizione (d'ora in avanti, "**FD**" o "**Servizio FD**") consente di firmare i documenti direttamente da PC o smartphone mantenendo lo stesso valore legale della tradizionale firma autografa.
È il risultato di una trasformazione crittografica dei dati che garantisce l'autenticazione dell'origine, l'integrità e il non ripudio degli stessi da parte firmatario. Le chiavi crittografiche utilizzate per questa operazione sono conservate su un dispositivo fisico o remoto. Le chiavi sono associate ad un soggetto attraverso un Certificato digitale (d'ora in avanti, "**Certificato**"), che contiene i suoi dati identificativi.
Le chiavi di crittografia sono generate, conservate e utilizzate attraverso un dispositivo *sicuro Qualified Signature Creation Device* (d'ora in avanti anche "**QSCD**"), che può essere un dispositivo fisico consegnato al Soggetto oppure un dispositivo situato in un'area del data center ad alta sicurezza o HSTZ (*High Security Trusted Zone*).
Il tipo di Certificato è contraddistinto da un numero chiamato O.I.D. (*Object Identifier*), ossia un codice che identifica il Certificatore (InfoCert), l'uso del Certificato e la "*policy e procedure"* a cui esso è conforme. La definizione e descrizione completa degli O.I.D. si trova nel CPS.
I Certificati dettagliati nel presente allegato tecnico sono di due tipologie:
a) Certificati qualificati di sottoscrizione su dispositivo fisico o remoto;
b) Certificati di Autenticazione: fungono da strumento digitale per l'autenticazione del Titolare per l'accesso ai servizi online dedicati.

2.1 Definizione Delle Parti

Soggetto/Titolare: Il Soggetto, definito anche **Titolare**, si riferisce alla persona fisica titolare del Certificato Qualificato. Tale Soggetto è l'utilizzatore dei servizi offerti e ha i suoi dati identificativi fondamentali inseriti nel Certificato.

Richiedente: Il Richiedente è la persona fisica o giuridica che richiede il rilascio di Certificati digitali al QTSP per un Soggetto. **Il Richiedente può coincidere con il Soggetto/Titolare**, quando una persona fisica richiede un Certificato per sé stessa. In altre situazioni, il Richiedente può essere un ente o un'organizzazione, che agisce per conto di persone fisiche collegate da rapporti commerciali o nel quadro di una struttura organizzativa.

Ente Emettitore: Ente responsabile del rilascio di un dispositivo fisico (SmartCard o Token) opportunamente predisposto per ospitare un certificato di autenticazione CNS (Carta Nazionale Dei Servizi) come descritto nel paragrafo 3.2.1.3 del presente documento. È la Pubblica Amministrazione che emette la CNS ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della stessa.

Terzo interessato: persona fisica o giuridica interessata e/o responsabile dell'informazione inclusa nel Certificato relativa al Ruolo e/o all'Organizzazione.

3. SPECIFICHE TECNICO-NORMATIVE

3.1.1 Rilascio e Utilizzo del Servizio FD

Il Servizio FD è erogato da InfoCert in favore del Soggetto, in forza del presente Allegato Tecnico e delle Condizioni Generali di Contratto (d'ora in avanti, "**CGC**") stipulate con lo stesso.
Il Richiedente deve richiedere al QTSP la registrazione e l'emissione del Certificato seguendo le modalità stabilite nel Manuale Operativo pertinente, utilizzando l'apposita Richiesta di Attivazione fornita da InfoCert (d'ora in avanti "**Richiesta di Attivazione**").
Il rilascio del Certificato da parte di InfoCert in favore del Soggetto è subordinato all'esito positivo della preventiva e necessaria procedura di identificazione di quest'ultimo, come rappresentato nel par. 3.2.3 del CPS (*Certification Practice Statement*) e nel par. 3.1.3 del presente documento.
Pertanto, in caso di esito negativo dell'identificazione, il Certificato non sarà rilasciato dal QTSP; mentre in caso di esito positivo dell'identificazione, il Certificato verrà rilasciato al Soggetto ai sensi del CPS.
Il Certificato rilasciato può essere utilizzato per firmare documenti utilizzando strumenti messi a disposizione dal QTSP o dal Richiedente non Titolare, per sbloccare le chiavi di firma, e dopo aver svolto un processo di autenticazione tramite strumenti dedicati, il QTSP conserverà le informazioni relative alla reale identità della persona per almeno venti (20) anni dalla scadenza del Certificato stesso, fino a un massimo di 23 (ventitre) anni dalla data di emissione.
Nel caso in cui il QTSP termini la propria attività, provvederà al trasferimento di tali informazioni a terze parti, alle medesime condizioni ivi esposte, così come indicato nel Manuale Operativo pertinente.

3.1.2 Certificato Digitale

Un Certificato digitale è un documento elettronico, firmato da InfoCert, che certifica l'associazione tra il Soggetto e la sua coppia di chiavi crittografiche (pubblica e privata), utilizzate per la firma digitale o per l'autenticazione. Le chiavi vengono generate e gestite in un dispositivo crittografico sicuro sotto il controllo di InfoCert o del Soggetto stesso.
Il QTSP garantisce la corretta associazione delle chiavi con il Soggetto, emettendo il Certificato conformemente alla normativa applicabile e al Manuale Operativo pertinente.
I Certificati possono contenere delle limitazioni d'uso così come previste nel Manuale Operativo pertinente.

3.1.3 Processo di verifica di identità

Prima di procedere con il riconoscimento, il Titolare deve assicurarsi di essere in possesso dei documenti di identità in formato originale e di un codice fiscale.
Questi devono essere in originale, in buono stato e in corso di validità.
Sono accettabili esclusivamente i documenti elencati nel documento "CPS Addendum – Documenti di identità accettabili" presente sul sito InfoCert al seguente link: CPS_doc_identita.pdf.
Le modalità di identificazione di seguito elencate sono descritte nel dettaglio nel paragrafo 3.2.3 del CPS.

Modalità di identificazione	Richiedenti che acquistano il servizio per se stessi	Richiedenti che acquistano per conto di altri Soggetti

1. LiveID	☒	☒
2. AMLID	☐	☒
3. SignID	☒	☒
4. AutID	☒	☒
5. VideoID	☒	☒
6. eDocID	☐	☒

3.1.4 Rinnovo del Certificato

Il Soggetto può rinnovare il Certificato, prima della sua scadenza, utilizzando gli strumenti messi a disposizione da InfoCert. La richiesta di rinnovo viene sottoscritta con la chiave privata, corrispondente alla chiave pubblica contenuta nel Certificato da rinnovare. L'esito del rinnovo è di fatto l'emissione di un nuovo Certificato.
Il rinnovo non è possibile se gli attributi indicati nel Certificato non sono più validi. Dopo la revoca o la scadenza del Certificato non è possibile eseguire il rinnovo del Certificato, diventando quindi necessaria una nuova identificazione.
In merito alla disposizione di cui al punto 7.2 delle CGC, nel caso in cui il Titolare dia la disdetta anticipata rispetto al rinnovo automatico annuale delle suddette Condizioni, la possibilità di utilizzare il Certificato verrà bloccata, e su richiesta del Titolare, lo stesso verrà revocato.

3.1.5 Sospensione o Revoca del Certificato

La revoca o sospensione del Certificato può avvenire su richiesta autenticata del Soggetto o del Richiedente non Titolare (Terzo Interessato nel caso in cui quest'ultimo abbia espresso il suo consenso per l'inserimento del Ruolo e/o il campo Organizzazione) ovvero su iniziativa del QTSP. Gli ulteriori dettagli in materia sono regolati nel Manuale Operativo pertinente.

3.2 SERVIZI

3.2.1 Certificati su Dispositivo

I dispositivi in possesso del Titolare, che contengono le chiavi crittografiche del Certificato, possono contenere, oltre ai Certificati di firma qualificata, anche "Certificati di autenticazione" o "Certificati di autenticazione – CNS".
I Certificati sono identificati dai seguenti Object Identifiers (OID), ossia un codice che identifica il QTSP, l'uso del Certificato e la policy a cui esso è conforme:

Servizio	OID
Firma su Dispositivo	1.3.76.36.1.1.1 e 1.3.76.36.1.1.61
Autenticazione	1.3.76.36.1.1.3
Autenticazione CNS	1.3.76.36.1.1.4

I dispositivi configurabili, tutti dotati di un chip crittografico al loro interno, sono i seguenti:

- Il token USB o wireless (di seguito anche "*business key*") è un dispositivo utilizzabile su qualsiasi PC dotato di porta USB o connessione wireless.

Per utilizzare la business key è sufficiente collegarla alla porta USB o alla connessione wireless del computer, installare i driver e il software forniti (se necessario) e avviare il software di firma per selezionare i documenti da firmare o accedere ai servizi digitali online inserendo il PIN associato al dispositivo.

- La *smart card* è una tessera elettronica che richiede un lettore di smart card dedicato per poter essere utilizzata. Per utilizzare la smart card, è necessario collegare il lettore di smart card al computer tramite cavo USB, inserire la carta nel lettore, verificare il riconoscimento tramite i driver specifici e utilizzare un software compatibile per apporre firme digitali o accedere ai servizi online tramite autenticazione.

Questi dispositivi possono essere utilizzati per firmare digitalmente con il Certificato di firma qualificata o per autenticarsi a determinati servizi online tramite il Certificato di autenticazione o autenticazione CNS.
Qualora venga trovata una falla di sicurezza che ne pregiudica un conforme utilizzo, il dispositivo potrebbe diventare non più utilizzabile e dovrà essere sostituito quanto prima per non invalidare le firme emesse.

3.2.1.1 Certificato di Firma Qualificata su dispositivo
Questi Certificati, vengono rilasciati su dispositivi fisici sicuri quali smart card, o business key. Il Titolare è tenuto a custodire con cura il dispositivo di firma e le relative credenziali d'accesso, adottando misure organizzative e tecniche adeguate a prevenire danni a terzi e garantire l'uso esclusivamente personale e sicuro del dispositivo e delle credenziali.
Il Certificato di Firma Qualificata ha validità di tre anni a partire dalla data di emissione, ovvero fino alla data di pubblicazione della sua revoca o sospensione, se effettuate precedentemente a tale data.

3.2.1.2 Certificato di Autenticazione su dispositivo
Il Certificato di Autenticazione rilasciato da InfoCert funge da strumento digitale per l'autenticazione del Titolare. Questo Certificato è essenziale per garantire l'integrità e l'autenticità delle comunicazioni digitali del Titolare, associando inequivocabilmente la sua identità alla chiave pubblica registrata. È utilizzabile per una varietà di servizi digitali che richiedono sicurezza elevata, come firme elettroniche, transazioni crittografate e autenticazione sicura nei sistemi informatici. Il processo di emissione, gestione e uso del Certificato è strettamente regolato dal Manuale Operativo ICERT-INDI-MOCA.
Il Certificato di Autenticazione ha validità di tre anni a partire dalla data di emissione, ovvero fino alla data di pubblicazione della sua revoca o sospensione, se effettuate precedentemente a tale data.

3.2.1.3 Certificato di Autenticazione CNS - Carta Nazionale dei Servizi
Il Certificato di Autenticazione CNS è rilasciato da un "Ente Emettitore", e funge da strumento digitale per l'autenticazione del Titolare per l'accesso ai servizi online dedicati. L'Ente Emettitore conferisce ad InfoCert mandato non esclusivo a espletare la funzione di Certification Authority (CA) per il rilascio di CNS. L'Ente Emettitore autorizza InfoCert, in qualità di CA, a delegare l'attività di richiesta e rilascio di CNS a soggetti terzi delegati da InfoCert in qualità di Ufficio di Registrazione.
Questo certificato è essenziale per garantire l'integrità e l'autenticità delle comunicazioni digitali del Titolare, associando inequivocabilmente la sua identità alla chiave pubblica registrata. Il processo di emissione, gestione e uso del Certificato è regolato dalla policy InfoCert ICERT-INDI-CPCA-CNS

reperibile sul sito del Certificatore e dal manuale operativo dell'Ente Emettitore reperibile sul sito di quest'ultimo.
Le procedure operative adottate dall'Ente Emettitore e dal Certificatore stesso per l'erogazione dei servizi di certificazione digitale sono riportate nel Manuale Operativo CNS redatto e reso disponibile dall'Ente Emettitore stesso.
Il Certificato di Autenticazione CNS ha validità di tre anni a partire dalla data di emissione, ovvero fino alla data di pubblicazione della sua revoca o sospensione, se effettuate precedentemente a tale data.
Il Certificato e il dispositivo possono essere rinnovati una sola volta. Dopo il primo rinnovo, si dovrà procedere ad una nuova emissione del Certificato e del dispositivo.

3.2.2 Certificati qualificati per Firma Remota

I Certificati di firma remota di cui ai paragrafi successivi sono identificati dai seguenti Object Identifiers (OID):

Servizio	OID
Emissione di certificati qualificati per Firma Remota	1.3.76.36.1.1.22 e 1.3.76.36.1.1.63
Emissione certificato qualificato per firma remota utilizzabile esclusivamente nel/i dominio/i definiti dal Richiedente	1.3.76.36.1.1.35 e 1.3.76.36.1.1.65
Emissione certificato qualificato per firma remota automatica	1.3.76.36.1.1.2 e 1.3.76.36.1.1.62
Emissione certificato qualificato per firma remota - Firma remota One Shot (OS)	1.3.76.36.1.1.34 e 1.3.76.36.1.1.64

3.2.2.1 Firma Remota

In caso di richiesta di un Certificato di sottoscrizione per procedura remota, il Servizio ha ad oggetto la generazione di una coppia di chiavi crittografiche e l'emissione di un Certificato Qualificato di firma elettronica remota con durata triennale. La firma remota consente al Titolare di apporre firme digitali senza la necessità di utilizzare dispositivi fisici personali, come token USB o smart card.
I Certificati di sottoscrizione per procedure di firma remota rilasciati da InfoCert sono utilizzati mediante apposite procedure informatiche che si collegano in maniera sicura al servizio di Firma Remota erogato da InfoCert. Tale servizio garantisce il rispetto del Regolamento e di quanto previsto al dall'art. 35 del CAD, Codice dell'Amministrazione Digitale, tramite l'utilizzo di un dispositivo crittografico sicuro (**QSCD**).
Il Servizio prevede che al Titolare sia messa a disposizione, una procedura informatica, implementata sui sistemi di InfoCert o del Richiedente non Titolare, quando presente, mediante la quale il medesimo Titolare può gestire il proprio Certificato di sottoscrizione.
I Certificati di Firma Remota possono essere rilasciati nel dominio messo a disposizione dal Richiedente non Titolare. Qualora il Richiedente chieda il rilascio, per i Titolari, di certificati il cui utilizzo è limitato esclusivamente al dominio informatico per il quale è stato emesso, tale certificato sarà utilizzabile esclusivamente nel/i dominio/i definiti dal Richiedente stesso e nei rapporti tra Titolare e Richiedente.
Le chiavi crittografiche necessarie per la firma sono custodite in un QSCD, gestito da InfoCert. Il Titolare mantiene il controllo esclusivo sull'apposizione della firma mediante un processo di autenticazione di "livello elevato", che prevede l'utilizzo combinato di PIN e OTP. Ogni sessione di firma richiede una

nuova autenticazione per garantire la sicurezza del processo, e le operazioni possono essere eseguite sia su desktop che su smartphone.
La firma remota può essere utilizzata tramite applicativi di firma messi a disposizione da InfoCert oppure può essere integrata via API dall'applicazione messa a disposizione dal Richiedente non Titolare.
La firma remota prevede la configurazione di un user e una password ed è attivabile o direttamente dal processo TOP (*Trust Onboarding Platform*) o dal portale di InfoCert MySign secondo le istruzioni inviate per mail, a cui il Titolare può accedere tramite le suddette credenziali e gestire il certificato in termini di modalità di ottenimento codici OTP, oppure dalle modalità previste dall'applicazione del Richiedente.

3.2.2.2 Firma remota automatica
La Firma automatica è un tipo di firma remota che rispetta l'adempimento dei requisiti previsti dell'art. 35, comma 3 del Codice, il Titolare deve utilizzare una coppia di chiavi destinata a tale scopo, diversa da tutte le altre in suo possesso.
Il Servizio, in aggiunta a quanto previsto dal paragrafo 3.2.1 del presente Allegato Tecnico, consente la generazione automatica delle firme su documenti inviati attraverso procedure informatiche automatizzate. In tal caso non è necessario per il Titolare confermare la volontà di firmare perché è a conoscenza dei documenti che vengono generati dalla procedura informatica di cui sopra.
La gestione del servizio di firma automatica comprende l'autenticazione del Titolare mediante strumenti specifici e la gestione remota del Certificato digitale. Il processo prevede pertanto il rilascio di un Certificato di firma automatica contenente il seguente limite d'uso: "*Il presente certificato è valido solo per firme apposte con procedura automatica*".
La firma automatica dei documenti viene effettuata dal sistema solo dopo che il Titolare ha attivato il Certificato, senza ulteriori interventi umani a meno che il Titolare stesso non richieda una sospensione temporanea del Certificato o dell'utilizzo dello stesso nella procedura automatica. L'accesso iniziale al sistema avviene tramite PIN e OTP, che sono richiesti soltanto alla prima sessione, dopodiché i documenti vengono firmati automaticamente al momento del caricamento, nel rispetto delle autorizzazioni concesse. La firma automatica di cui al presente paragrafo si avvale di un Certificato specifico, destinato unicamente a questa tipologia di utilizzo. Il Titolare è tenuto ad utilizzare Certificati diversi in procedure automatiche diverse, in modo da minimizzare i rischi di sicurezza legati ad un utilizzo improprio.
A ciascun Certificato digitale per procedura di firma automatica può essere associata una sola procedura informatica di trasmissione dei documenti.

3.2.2.3 Firma Remota One Shot
La firma digitale One Shot (d'ora in avanti, "**OS**" o "**Servizio OS**") è una firma remota le cui chiavi, una volta generate, sono disponibili solo ed esclusivamente per la transazione di firma per la quale sono state generate. Immediatamente dopo il loro utilizzo la chiave privata viene distrutta.
I certificati afferenti a questa firma hanno una validità ridotta al tempo necessario per eseguire le firme. In questa categoria sono compresi anche certificati denominati "short-term" per i quali il periodo di validità è inferiore al tempo massimo per evadere una richiesta di revoca come specificato nel Manuale di riferimento.
Il Servizio OS consente al Titolare, previo riconoscimento della sua identità e di una conferma attraverso codice OTP, di autenticarsi e di utilizzare la Firma Remota collegata al Certificato. L'emissione del Certificato da parte di InfoCert in favore del Titolare è subordinata all'esito positivo della necessaria

procedura di identificazione e riconoscimento di quest'ultimo, nelle modalità rappresentate nel paragrafo 3.1.3. del presente Allegato Tecnico.
In deroga a quanto stabilito all'articolo 10.4 delle CGC, poiché il Servizio OS, per sua natura, richiede l'esecuzione immediata, il Titolare accetta espressamente la perdita del diritto di recesso ai sensi dell'art. 59, lett. a), del Codice del Consumo.
Qualora il Certificato abbia la durata di 60 minuti, e in deroga a quanto previsto dal paragrafo 3.1.5 del presente documento, essendo la durata del certificato minore o uguale del tempo minimo (60 minuti) previsto per rendere pubblica l'informazione sulla subentrata invalidità dello stesso, per tali Certificati non è prevista la possibilità di revoca e sospensione.
Qualora il Certificato abbia la durata di 30/45/60 giorni, il contratto relativo al Servizio FD è sospensivamente condizionato al buon esito dell'identificazione che deve avvenire entro e non oltre i 30/45/60 giorni.

3.3 Obblighi e Responsabilità

3.3.1. Obblighi e Responsabilità di Soggetto e Richiedente non Titolare

Gli obblighi e le responsabilità del Soggetto e, quando applicabile, del Richiedente non Titolare sono determinati dalla normativa applicabile, dal presente Allegato Tecnico, dal Manuale Operativo pertinente e dalle CGC nella versione in vigore alla data della Richiesta di Attivazione. Se, al momento dell'identificazione, il Soggetto cela la sua reale identità o il Richiedente non Titolare o il Titolare stesso agiscono in modo da compromettere l'identificazione e le relative risultanze indicate nel Certificato, saranno considerati responsabili per tutti i danni derivanti al QTSP e/o a terzi dall'inesattezza delle informazioni contenute nel Certificato. Il Richiedente e/o Soggetto sono tenuti a garantire e manlevare il QTSP da eventuali richieste di risarcimento danni.
Sono anche responsabili per i danni derivanti al QTSP e/o a terzi in caso di ritardo nell'attivazione delle procedure di revoca o sospensione del Certificato, come previsto dal Manuale Operativo pertinente. Devono assicurarsi di rispettare i requisiti hardware e software necessari per il corretto utilizzo dei Certificati.
Il Soggetto e il Richiedente non Titolare sono gli unici responsabili dei documenti che attraverso le applicazioni InfoCert o del Richiedente stesso saranno trasmesse ai fini della firma, assumendo, pertanto, ogni e più ampia responsabilità in merito al funzionamento della stessa procedura informatica e al contenuto, validità e titolarità di detti documenti, sollevando il Certificatore da ogni e qualsiasi responsabilità in merito.

3.3.2. Obblighi Specifici del Soggetto

Gli strumenti di autenticazione (a titolo esemplificativo, il PIN, l'OTP o lo strumento che lo genera) per la procedura di attivazione del Certificato sono strettamente personali. Pertanto, il Titolare è tenuto a proteggere la segretezza di detti strumenti, omettendo di comunicarli o divulgarli a terzi, anche solo in parte, conservandoli in un luogo sicuro.
Il Soggetto, consapevole che l'utilizzo di un Certificato di firma comporta la possibilità di sottoscrivere atti e documenti rilevanti a tutti gli effetti della legge italiana e riconducibili unicamente alla sua persona, è obbligato ad osservare la massima diligenza nell'indicazione, utilizzo, conservazione e protezione degli strumenti di autenticazione messi a disposizione dal QTSP o dal Richiedente non Titolare.
Deve esercitare la massima diligenza nell'uso del Certificato di firma, verificando il contenuto dei documenti da firmare e assicurandosi che riflettano la sua volontà.
È inoltre tenuto a non utilizzare il Certificato dopo la sua scadenza, revoca o sospensione.

È responsabile per la veridicità dei dati comunicati durante l'identificazione e nella Richiesta di Attivazione.

3.3.3 Obblighi del Richiedente non Titolare

Il Richiedente non Titolare è responsabile della richiesta del Certificato al Certificatore ed è responsabile della sua gestione, conformemente al PDS e al Manuale Operativo. Deve adottare misure adeguate a prevenire danni derivanti dall'uso del sistema di chiavi asimmetriche o del Certificato. Se gestisce il processo di autenticazione, deve garantire una autenticazione con un livello elevato di sicurezza come previsto da Regolamento di Esecuzione (UE) 2015/1502 e secondo le modalità concordate con InfoCert. È inoltre tenuto a ricordare che l'uso del Certificato, dopo la sua scadenza, revoca o sospensione, determina l'apposizione di una firma non valida e, pertanto, è obbligato a manlevare InfoCert da qualsivoglia responsabilità per uso improprio del Certificato medesimo.

3.3.4 Obblighi del QTSP

Gli obblighi del QTSP sono esclusivamente quelli indicati dalla normativa applicabile, dal presente Allegato Tecnico, dei Manuali Operativi e dall'Accordo.
In particolare, il QTSP si obbliga a conservare in un apposito archivio digitale non modificabile per almeno venti (20) anni dalla scadenza del certificato, fino a un massimo di 23 (ventitré) anni dalla data di emissione, tutti i certificati emessi, i *log* di attivazione degli stessi e le evidenze di riconoscimento, nelle modalità previste dal Manuale Operativo.
In particolare, il QTSP non presta alcuna garanzia relativamente a:

- il corretto funzionamento e la sicurezza dei macchinari *hardware* e dei *software* utilizzati dal Titolare;
- usi diversi della chiave privata, del dispositivo sicuro di firma e/o di autenticazione e del Certificato rispetto a quelli previsti dalle norme italiane vigenti e dal Manuale Operativo pertinente;
- il regolare e continuativo funzionamento di linee elettriche e telefoniche nazionali e/o internazionali;
- la validità e rilevanza, anche probatoria, – della firma nei confronti di soggetti e per atti e documenti sottoposti a legislazioni differenti da quella italiana;
- la segretezza di qualsiasi messaggio, atto o documento firmato (quindi, eventuali violazioni di quest'ultima sono, di norma, rilevabili dal Titolare o dal destinatario attraverso l'apposita procedura di verifica).

Il QTSP garantisce unicamente il funzionamento del Prodotto, secondo i livelli di servizio indicati al Titolare nel Manuale Operativo pertinente.

3.3.5 Ruolo e Organizzazione

Conformemente al Manuale Operativo e alle normative vigenti delineate nell'articolo 28, comma 3, del Codice dell'Amministrazione Digitale (CAD) e nella determinazione dell'Agenzia per l'Italia Digitale (AgID) n. 121/2019 e successivi emendamenti, il Richiedente non Titolare o il Titolare stesso possono richiedere l'inserimento nel Certificato di specifiche informazioni relative al Ruolo del Titolare. Queste informazioni possono includere:

- titoli e/o abilitazioni professionali;
- poteri di rappresentanza di persone fisiche o di enti di diritto privato o pubblico;
- appartenenza a tali enti;

- esercizio di funzioni pubbliche.

Questo inserimento deve avvenire secondo le modalità delineate nel Manuale Operativo di riferimento. Per richiedere l'inserimento del Ruolo, è necessario il consenso del **Terzo Interessato**, che può coincidere con il Richiedente, e che può altresì richiedere la revoca o la sospensione del Certificato in qualunque momento. Se il Richiedente non Titolare vuole che il Certificato rifletta l'appartenenza del Soggetto stesso alla propria organizzazione, è responsabilità del Richiedente non Titolare, in qualità di Terzo Interessato, comunicare ad InfoCert eventuali cambiamenti relativi alla appartenenza del soggetto all'organizzazione.
Le richieste di certificati che indicano l'appartenenza all'organizzazione, sono accettate solo se provenienti da entità con una forma giuridica definita e verificabile presso il Registro delle Imprese. La ragione sociale, la denominazione e il codice identificativo dell'Organizzazione saranno inclusi nel Certificato solo se l'organizzazione ha espressamente autorizzato il rilascio del Certificato, anche senza una specifica indicazione di Ruolo, come da Manuale Operativo.

4. SLA

4.1 SLA di servizio

In termini di erogazione, i valori di disponibilità mensile del servizio sono rappresentati dettagliatamente nel Manuale Operativo pertinente.

tinexta infocert

ALLEGATO D – MISURE DI SICUREZZA

Scopo del presente Allegato è illustrare l'elenco della documentazione afferente alle Misure Tecniche e Organizzative adottate da InfoCert.

InfoCert ha predisposto un set documentale di alto livello che potrà essere consultato dal Cliente che ne faccia espressamente richiesta.

Di seguito è riportato l'elenco della documentazione di cui sopra e la relativa descrizione:

DOCUMENTO	DESCRIZIONE
Report SOC2 Type II InfoCert	Il documento fornisce al cliente una risposta standardizzata e certificata dei punti normalmente esaminati nelle attività di Customer Risk Management.
Report SOC2 Type II AWS	Il report documenta in che modo vengono conseguiti i controlli e gli obiettivi chiave di conformità, consentendo di raccogliere informazioni sui controlli previsti per supportare operatività e compliance, relativi a sicurezza, disponibilità e riservatezza, nell'ambito dei sistemi di AWS.
Report Framework Nazionale Cyber Security	Il documento consente di fornire un report, strutturato e completo di evidenze, sull'insieme di controlli di sicurezza implementati da InfoCert
Security Practices in the AWS Cloud EX EN	Il documento descrive le valutazioni e le azioni intraprese da InfoCert per garantire la sicurezza dei dati dei propri clienti all'interno del cloud AWS.
DD 4D.05 n.01 Business Continuity Plan EX (o EX EN)	Il documento definisce la strategia di continuità operativa di InfoCert, includendo la metodologia di Business Impact Analysis adottata per l'analisi del rischio e per la definizione delle soglie di allarme.
DD 4D.05 n.02 Disaster Recovery Plan EX (o EX EN)	Il documento descrive la procedura di attivazione del piano di risposta allo scenario di indisponibilità dei sistemi informativi (logici e/o fisici), sia in caso di simulazione del disastro che nel caso di disastro dichiarato.
IS 4D.07 n.02 Incident Response Plan EX	Il Piano di Risposta agli Incidenti (Incident Response Plan - IRP) stabilisce le fasi e le attività di gestione degli incidenti di sicurezza significativi per garantire che l'organizzazione possa affrontarli tempestivamente e scongiurare il rischio di compromissione di informazioni sensibili, di identificazione personale non autorizzata, o più in generale di subire un grave impatto sulla sua capacità di produzione/erogazione dei servizi. Specifica i metodi organizzativi per la preparazione, il rilevamento, l'analisi, l'eradicazione e il contenimento di un incidente di sicurezza significativo.

Resta espressamente inteso che la documentazione, condivisa da InfoCert con la controparte, dovrà essere da quest'ultima consultata e custodita diligentemente e secondo principio di buona fede e nel rispetto della riservatezza dei contenuti ivi indicati. Tale documentazione, inoltre, non potrà in nessun caso essere condivisa con l'esterno o comunque verso soggetti terzi senza la previa scritta autorizzazione da parte di InfoCert e, altresì, verrà condivisa internamente alla compagine societaria della controparte solamente con quei soggetti che devono averne conoscenza per specifiche esigenze di esecuzione del contratto cui il presente documento costituisce allegato.

InfoCert SpA
Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00

tinexta infocert

ALLEGATO DI PROCESSO CERTIFICATI QUALIFICATI E DI AUTENTICAZIONE
PROCESSO DI SOTTOSCRIZIONE E MODALITÀ DI RICONOSCIMENTO

Parte 1

1) Il processo di identificazione e di rilascio di un Certificato di firma può essere attivato dalla RA (Registration Authority) tramite la Piattaforma fornita da InfoCert, in forza dell'Accordo sottoscritto, con la necessaria presenza di un ente emettitore (in seguito "Ente Emettitore") per il rilascio del dispositivo fisico CNS.

Nell'ambito del processo di seguito descritto, si distinguono i seguenti soggetti:

- InfoCert:
  - eroga i Servizi servendosi del riconoscimento posto in essere dalla RA;
  - gestisce il *front end* standard della Piattaforma di erogazione dei Servizi, salvo personalizzazioni che verranno eseguite dalla RA a propria cura e spese, nel rispetto di quanto eventualmente pattuito;
  - fornisce al Titolare gli strumenti standard di autenticazione alla procedura di rilascio dei Certificati, salvo personalizzazioni che verranno eseguite dalla RA a propria cura e spese, nel rispetto di quanto eventualmente pattuito.
- La RA:
  - identifica l'Utente sotto la propria responsabilità;
  - invia a InfoCert l'asserzione d'identità o il verbale di riconoscimento che attesta l'avvenuta identificazione del Titolare;
  - gestisce l'eventuale personalizzazione del *front end* della Piattaforma di erogazione dei Servizi, sulla base delle linee guida fornite da InfoCert;
  - fornisce il dispositivo fisico al Titolare, anche per conto di InfoCert o, nei casi di emissione della Carta Nazionale dei Servizi (CNS), dell'Ente Emettitore, se appositamente delegato

Il processo per il rilascio dei certificati, di cui agli articoli 2A e 2B, varia sulla base della tipologia di Piattaforma fornita da InfoCert.
Qualora la RA fruisca della Piattaforma IPP, si prega di far riferimento anche al processo descritto al seguente link: Infocert Partner Platform

2A) CERTIFICATI REMOTI

Il processo di identificazione delegato alla RA tramite idonea documentazione contrattuale è finalizzato al rilascio di una delle seguenti tipologie di certificato qualificato definite all'art. 3.2 dell'allegato tecnico:

- ***Certificato di Firma Remota***
- ***Certificato Long Term***
- ***Certificato OneShot***
- ***Certificato OneShot di durata***.

In ogni caso, detto processo standard prevede i seguenti step:

1. l'Utente Finale entra in contatto con la RA per richiedere un servizio e fornisce alla RA i propri dati personali.

2. La RA identifica l'Utente sotto la propria responsabilità, in conformità all'Accordo e nel rispetto della normativa vigente, secondo una delle modalità descritte nel paragrafo 3.2.3. del Manuale Operativo ICERT-INDI-MO.
3. La RA invia a InfoCert l'asserzione di identità o il verbale di riconoscimento che attesta l'avvenuta corretta identificazione dell'utente e in base alla quale InfoCert emette il Certificato di firma. L'asserzione di identità o il verbale sono firmati digitalmente attraverso un certificato di firma qualificata con procedura automatica da parte di un soggetto delegato dalla RA. Può accadere che il Certificato venga rilasciato anteriormente al ricevimento delle evidenze della avvenuta identificazione: in tale ipotesi, la validità del Certificato è sospensivamente condizionata al positivo esito del riconoscimento.
4. Qualora venga richiesto un Certificato di Firma Remota, il Titolare deve creare il proprio Profilo Utente inserendo il nome utente e la password necessari per utilizzare il certificato su altre piattaforme.
5. Il Titolare visualizza la documentazione contrattuale di InfoCert relativa al Servizio scelto, accessibile mediante link dalla Piattaforma (il tutto visualizzabile sul sito istituzionale di InfoCert) e, al fine dell'emissione, procede con l'accettazione della stessa.
6. Il Titolare visualizza la documentazione che la RA reputa necessario far firmare con il Servizio InfoCert, accettandone la sottoscrizione.
7. Il Titolare si autentica alla procedura tramite OTP (One Time Password - per i certificati di Firma Remota e *Long Term* viene richiesta la creazione e/o inserimento di un PIN) e procede a sottoscrivere la documentazione.
8. La RA (o InfoCert se espressamente concordato) mette a disposizione del Titolare i contratti firmati (sia quelli di InfoCert, sia quelli eventuali della RA).

2B) CERTIFICATI SU DISPOSITIVO

Il processo di identificazione delegato alla RA tramite idonea documentazione contrattuale è finalizzato al rilascio di un certificato di sottoscrizione e/o un certificato di autenticazione tramite uno dei seguenti dispositivi:

- ***Token USB***
- ***Token Wireless***
- ***Smart Card***

All'interno dei tali Dispositivi, possono essere inseriti uno o più dei seguenti Certificati, definiti all'art. 3.2 dell'allegato tecnico:

- **Certificato di Firma elettronica Qualificata**
- **Certificato di autenticazione**
- **Certificato di autenticazione-CNS**

In ogni caso, il processo standard prevede i seguenti step:

1. Il Titolare entra in contatto con la RA per richiedere un Certificato di sottoscrizione e/o autenticazione su dispositivo e fornisce alla RA i propri dati personali.

2. Il Titolare visualizza la documentazione contrattuale di InfoCert relativa al Servizio scelto (Richiesta di Attivazione, Condizioni Generali di Contratto, Privacy Policy e Allegato/i Tecnico/i), accessibile mediante link dalla Piattaforma di riconoscimento e sul sito istituzionale di InfoCert.
3. La RA identifica il Titolare sotto la propria responsabilità, in conformità all'Accordo e nel rispetto della normativa vigente, secondo una delle modalità descritte nel paragrafo 3.2.3. del Manuale Operativo ICERT-INDI-MO. Infatti, a seconda del tipo di Servizio erogato, l'identità del Titolare deve essere accertata dalla RA prima dell'emissione del Certificato o entro 30 giorni dal momento dell'emissione dello stesso.
4. La RA invia a InfoCert l'asserzione di identità o il verbale di riconoscimento firmati digitalmente, che attesta l'avvenuta corretta identificazione dell'utente e in base alla quale InfoCert emette il Certificato di sottoscrizione e/o di autenticazione.
5. Il Titolare sottoscrive la Richiesta di attivazione di un Certificato di sottoscrizione e/o autenticazione su dispositivo, contenente i dati raccolti e validati.
6. Il Titolare riceve una e-mail all'indirizzo indicato durante il processo all'interno della quale sarà allegata una busta accessibile tramite una *passphrase* o, qualora quest'ultima non sia stata scelta, tramite il Codice fiscale del Titolare.
7. Aperta la busta, il Titolare è dettagliatamente accompagnato al processo di attivazione dei propri certificati. Verrà generata la coppia di chiavi e, dopo le opportune verifiche della RA, verrà emesso il Certificato richiesto all'interno del Dispositivo vergine.
8. Qualora venga richiesta l'emissione di una CNS, per il tramite di un Ente Emettitore, il numero di serie del dispositivo fisico che supporta i Certificati identifica l'Ente Emettitore e deve essere verificato dalla RA.
9. Sulla Carta deve essere presente la scritta "Carta Nazionale dei Servizi" ed il nome dell'Ente Emettitore che l'ha emessa.
10. Conclusasi la fase di registrazione ed emissione del Certificato di sottoscrizione e/o autenticazione il Titolare riceve il dispositivo di firma e/o autenticazione nelle modalità concordate o presso l'Ente Emettitore.

3) DURATA

In deroga a quanto disposto dall'Accordo, qualora la RA si dovesse avvalere di un dispositivo fisico emesso dalla Provincia di Padova questo potrà avvenire per tutta la durata della convenzione sottoscritta tra InfoCert e la Provincia medesima, ossia il 31 dicembre 2031, anche se la durata dell'Accordo concluso fosse comunque successiva.

Parte 2

(A) Modalità di identificazione:

A.1 L'identità dell'Utente deve essere accertata dalla RA, secondo le modalità di cui all'art. 3.2.3 del CPS, prima dell'emissione del Certificato di cui al punto 2A e 2B o entro 30 giorni dal momento dell'emissione dello stesso. In tal senso, l'attestazione di avvenuta identificazione deve giungere ai sistemi di InfoCert antecedentemente alla richiesta di certificazione o entro e non oltre il periodo di 30 giorni successivi all'emissione del certificato. In quest'ultimo caso, InfoCert invia alla RA e al Titolare la documentazione sottoscritta solo una volta ricevuta l'attestazione di avvenuto riconoscimento.

(B) Strumenti di autenticazione alla procedura di firma remota:

B.1 La chiave privata del Titolare, contenuta negli HSM (Hardware Security Module) di InfoCert, può essere utilizzata unicamente dal Titolare stesso tramite i seguenti strumenti di autenticazione:

- Autenticazione Interna:
  - Per certificati di Firma Remota e *Long Term*: tramite il codice PIN scelto in autonomia al momento della richiesta del Certificato e una *One Time Password* ("OTP") generata e resa disponibile da InfoCert al numero di telefonia mobile associato al Titolare.
  - Per certificati *One Shot*: tramite una *One Time Password* ("OTP") generata e resa disponibile da InfoCert al numero di telefonia mobile associato al Titolare.
- Autenticazione Esterna: tramite il codice PIN fornito dalla RA o scelto dal Titolare al momento della richiesta del Certificato e una *One Time Password* ("OTP") generata e resa disponibile al Titolare dalla RA stessa.

(C) Customizzazione del Front End: sviluppo e mantenimento

C.1 Qualora il *Front End* attraverso il quale il Titolare verrà guidato nelle fasi di richiesta, registrazione, emissione ed eventuale utilizzo del Certificato, venga customizzato dalla RA, secondo modalità preventivamente condivise con InfoCert, debbono esser osservate le seguenti prescrizioni:

a) il *Front End* deve assicurare che i dati raccolti sugli applicativi della RA non subiscano alcuna variazione e che siano quindi trasmessi a InfoCert in maniera integrale per i servizi di registrazione e di emissione del Certificato;
b) il *Front End* sviluppato dalla RA deve esser sottoposto a un *test* di collaudo da parte di InfoCert, a spese della RA, prima dell'avvio in produzione per assicurare che tutti gli elementi indispensabili siano stati implementati, che siano funzionanti e che l'ordine delle chiamate applicative sia stato rispettato. Il collaudo avviene in contraddittorio tra le Parti;
c) in caso di mancato superamento del *test*, si distinguono due ipotesi. Se esso dipende da errori tecnici o malfunzionamenti dell'applicazione sviluppata dalla RA, l'efficacia degli accordi nell'ambito dei quali è stato eseguito il *test* prosegue regolarmente, salva l'impossibilità di processare richieste di rilascio di Certificati; sarà dunque onere e interesse della RA porre rimedio a sue spese al malfunzionamento del *Front End*. Se, invece, il mancato superamento dipende invece dalla *non compliance* del *Front End* rispetto alla normativa regolamentare e/o tecnica concernente il rilascio dei Certificati, InfoCert ha il diritto di sospendere l'esecuzione dei Servizi a suo carico e l'erogazione dei certificati finché la RA non rende il *Front End* conforme a detta normativa; per il resto, l'efficacia degli accordi tra le parti nell'ambito del quale è stato eseguito il *test* prosegue regolarmente;
d) nell'ipotesi soprastante, l'accertamento della soluzione del problema (tecnico o di *compliance*) deve essere effettuato mediante un nuovo *test* di collaudo;
e) la RA si impegna a non modificare in alcun modo il *Front End* implementato dopo il positivo *test* di collaudo, se non previa comunicazione ad InfoCert. In tali ipotesi, la RA, con un preavviso di almeno 60 giorni, deve dare evidenza, in apposito documento tecnico, delle modifiche che si richiedono. Allorché InfoCert nulla eccepisca nei successivi 60 giorni, la RA potrà procedere con le modifiche dichiarate. In ogni caso, qualsivoglia variazione al *Front End* dovrà essere valutata da InfoCert con un nuovo *test* di collaudo, sempre in contraddittorio, trovando applicazione quanto espresso ai punti precedenti.

MANDATO MASTER R.A.O.

tra

InfoCert S.p.A., con sede legale in Roma, Piazzale Flaminio 1/B, CF e P. IVA 07945211006, in persona dell'Amministratore Delegato e legale rapp.te *pro-tempore* dott. Danilo Cattaneo, società soggetta a direzione e coordinamento di Tinexta S.p.A. (di seguito "**InfoCert**")

e

XXXX, con sede in _____ n. _____, CF e P. IVA _____, in persona del legale rappresentante *pro tempore* _____ munito dei necessari poteri, come dichiara e garantisce (di seguito, anche "**Ufficio di Registrazione**" o "**R.A.**")

e

XXXX, residente in _____ n. _____, CF _____, (di seguito, "**Master R.A.O.**")

PREMESSO CHE:

a) L'Ufficio di Registrazione ed InfoCert, in data _____ hanno stipulato apposita convenzione (di seguito "**Convenzione"**), con la quale è stato conferito mandato alla prima di svolgere le funzioni di Ufficio di Registrazione, per il rilascio dei Certificati di firma, secondo quanto previsto dal Manuale Operativo ICERT-INDI-MO (di seguito il "**Manuale Operativo Certificati**") e/o per il rilascio dello SPID secondo quanto previsto dal Manuale Operativo ICERT-MO-SPID **("Manuale Operativo SPID")**;
b) ai sensi della Convenzione, la R.A. ha facoltà di operare anche attraverso propri Master R.A.O., che si impegneranno ad osservare gli obblighi meglio dettagliati nel prosieguo;
c) con il presente atto, si desidera conferire al Master R.A.O. apposito mandato per l'esecuzione delle attività di sua competenza ai sensi della Convenzione, concernenti le fasi identificazione, autenticazione , revoca e registrazione degli utenti (gli "**Utenti**"), nonché quelle di rilascio ed erogazione dei servizi InfoCert ("**Servizi Trust**"), ai sensi del Manuale Operativo in aggiunta alla gestione operativa e organizzativa delle attività tipiche della piattaforma dedicata, propedeutica al caricamento e alla gestione di tutta la documentazione afferente al ciclo-vita della R.A. ("**Piattaforma**") e che, pertanto, agirà in nome e per conto della RA stessa;
d) Il Master R.A.O. si è reso disponibile a svolgere le attività elencate al punto precedente e meglio dettagliate nel presente atto (il "**Mandato**");
e) le procedure di registrazione sono analiticamente esposte nel Manuale Operativo di InfoCert sopra citato, pubblicato sul sito Internet "*www.infocert.it"*, e nei provvedimenti legislativi e amministrativi eventualmente ivi richiamati.

TUTTO CIO' PREMESSO, le Parti convengono quanto segue:

1. PREMESSE

1.1. Le premesse, nonché il PDS e il Manuale Operativo Certificati e Manuale Operativo SPID disponibili sul sito InfoCert (https://www.firma.infocert.it/documentazione/) formano parte integrante del presente Mandato che sarà espletato secondo le specifiche condizioni ivi previste.

2. OGGETTO

2.1. InfoCert e la RA conferiscono mandato non esclusivo al Master R.A.O. a svolgere parte dell'attività di cui alla lett. c) delle premesse e, in particolare, a identificare gli Utenti con certezza, esclusivamente attraverso sistemi autorizzati da InfoCert) e secondo le modalità concordate da InfoCert e dalla R.A.

3. OBBLIGHI DELLE PARTI

3.1 La R.A., ferme rimanendo le obbligazioni di cui alla Convenzione, provvederà a:

a) supervisionare, per conto di InfoCert, l'attività di formazione e/o aggiornamento del Master R.A.O.;
b) verificare che il Master R.A.O. esegua con la dovuta diligenza le attività a lui assegnate;
c) monitorare costantemente che il Master R.A.O. mantenga i requisiti di onorabilità, competenza, affidabilità ed esperienza ai sensi dell'art. 24 par. 2 lett b) del Regolamento eIDAS;
d) assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniqualvolta venga revocato il Mandato da InfoCert, qualora cessi il rapporto di dipendenza/collaborazione tra l'Ufficio di Registrazione e il Master R.A.O., ovvero si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del Master R.A.O.), dandone tempestiva comunicazione per iscritto ad InfoCert entro 24 (ventiquattro) ore lavorative.

3.2 Il Master R.A.O. con la diligenza del mandatario ex art. 1710, c.c., dovrà:

a) conseguire la formazione necessaria per le finalità del presente mandato, partecipando ai corsi di formazione come predisposti dalla R.A. e/o da InfoCert ai sensi dell'art. 3.1 lett. a);
b) assumere gli obblighi descritti nei Manuali Operativi, nell'ultima versione tempo per tempo disponibile online sul sito di InfoCert, e garantire di possedere e mantenere già un'organizzazione di personale e di beni adeguata all'esercizio delle Attività;
c) conservare debitamente le credenziali della Piattaforma, attraverso cui coordinerà le attività per conto della R.A.;
d) rispettare le procedure operative di rinnovo, revoca o sospensione dei Servizi Trust definite da InfoCert;
e) assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniqualvolta venga revocato il Mandato da InfoCert o dalla R.A., qualora cessi il rapporto di dipendenza/collaborazione tra l'Ufficio di Registrazione e il R.A.O., ovvero si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del R.A.O.), dandone tempestiva notizia per iscritto ad InfoCert;
f) esercitare le Attività nell'interesse di InfoCert e con la diligenza del mandatario, ex art. 1710, c.c.;
g) svolgere le Attività nel rispetto della normativa vigente, dei Manuali Operativi e delle istruzioni ricevute da InfoCert, con particolare riferimento all'identificazione personale certa degli Utenti che richiedono l'emissione dei Servizi;
h) informare entro 8 (otto) ore InfoCert di eventuali vizi, difetti, interruzioni o malfunzionamenti del sistema e/o di errori nello svolgimento delle attività di identificazione e registrazione da parte dei R.A.O.;
i) consentire alle Autorità di vigilanza, nonché agli incaricati di InfoCert, di accedere nei propri locali per verificare il corretto espletamento delle Attività ed il rispetto delle procedure per lo svolgimento delle stesse;
j) fornire evidenza, entro e non oltre 3 (tre) giorni dalla richiesta da parte di InfoCert, di tutta la documentazione relativa alle Attività, qualora la richiesta derivi dall'Autorità di vigilanza;
k) sottoporre agli Utenti, siano esse persone fisiche o giuridiche che richiedono l'emissione dei Servizi Trust per conto dell'Utente, la documentazione contrattuale messa a disposizione da InfoCert, nonché concordare preventivamente con quest'ultima qualsiasi documento da rilasciare al Richiedente e/o Utente, relativamente all'attività di registrazione e/o di rilascio dei Servizi Trust;

l) mantenere strettamente riservate le credenziali ricevute da InfoCert per l'accesso alla Piattaforma con obbligo di custodia, per un utilizzo da parte di questi ultimi finalizzato all'espletamento delle attività precipue e nel rispetto delle obbligazioni ivi assunte;
m) obbligarsi ad un corretto utilizzo della Piattaforma, nelle modalità indicate da InfoCert;
n) provvedere ad un regolare caricamento/aggiornamento sulla Piattaforma di tutta la documentazione richiesta da InfoCert (a titolo meramente esemplificativo e non esaustivo: mandati, modulistica dei Servizi Trust), che dovrà essere fornita a quest'ultima entro i termini con essa convenuti, e in ogni caso qualora InfoCert ne faccia espressa richiesta;

3.3. La R.A. e il Master R.A.O. saranno solidalmente responsabili nei confronti di InfoCert per le attività previste nel presente Mandato.
3.4. La violazione di uno qualsiasi degli obblighi di cui al comma 3.1. e 3.2. del presente articolo costituirà giusta causa di revoca del presente Mandato da parte di InfoCert o della R.A., che sarà esercitata a mezzo di apposita comunicazione, fatto salvo il diritto al risarcimento dei danni eventualmente subiti e *subendi*. In caso di revoca, il Master R.A.O. è obbligato a cessare qualsiasi attività posta in essere in base al presente atto ed a restituire i materiali ricevuti al fine dell'espletamento dell'incarico.

4 CORRISPETTIVI E FORNITURA

4.1. La R.A. ed il Master R.A.O. per lo svolgimento dell'attività prevista nel Mandato non potranno pretendere il pagamento di alcun corrispettivo da parte di InfoCert né vantare alcuna esclusiva nei suoi confronti.
4.2. L'esclusione di cui al precedente comma è altresì valida con riferimento ai mezzi necessari per l'esecuzione del Mandato e alle anticipazioni e spese sostenute dal mandatario.

5 DURATA E DECORRENZA

5.1. Il Mandato avrà efficacia per il periodo di un anno dalla data della sua sottoscrizione e si rinnoverà tacitamente per periodi annuali, salvo disdetta di una delle Parti, da comunicarsi per iscritto almeno 3 (tre) mesi prima della scadenza del periodo annuale, a mezzo Posta Elettronica Certificata. Il Mandato perderà automaticamente efficacia, in ogni caso di cessazione della Convenzione in essere tra InfoCert e la R.A.
5.2. Durante il periodo di vigenza del Mandato, InfoCert avrà diritto, senza pagamento di alcun corrispettivo, di recedere da esso in qualsiasi momento, con comunicazione della volontà di esercitare tale diritto a mezzo Posta Elettronica Certificata o raccomandata A/R.
5.3. In caso di recesso e/o revoca, il Master R.A.O. non potrà vantare alcuna richiesta nei confronti della R.A. e/o di InfoCert, neanche per eventuali danni subiti in conseguenza dello stesso.
5.4. Resta salvo tra le Parti che in caso di risoluzione del presente Mandato, la Convenzione rimane valida ed efficace tra InfoCert e la R.A. fino a naturale vigenza della stessa.

6 PRIVACY

6.1. La R.A. e il Master R.A.O. si impegnano alla piena osservanza, per quanto di rispettiva competenza, del dettato del Regolamento (UE) 679/2016 e della normativa italiana compatibile con lo stesso.
6.2. Nell'espletamento del mandato, il Master R.A.O. sarà autorizzato al trattamento dei dati per lo svolgimento delle sole attività oggetto del presente Mandato, sotto la diretta autorità della R.A. e InfoCert attenendosi alle istruzioni impartite da quest'ultima.
6.3. In particolare, il Master R.A.O. metterà in atto le seguenti operazioni di trattamento:
a) verifica del documento di identità del richiedente, della relativa validità e della corrispondenza al soggetto richiedente;

b) trascrizione o verifica (in base alle indicazioni fornite in sede di formazione) delle informazioni inerenti alla persona fisica del richiedente;
c) produzione della documentazione che attesta l'avvenuto riconoscimento dell'Utente;
d) raccolta dei documenti firmati, se applicabile sulla base della procedura di identificazione messa in atto.

7 LEGGE APPLICABILE E FORO COMPETENTE

7.1. Il presente Mandato è soggetto alla legge italiana.

7.2. Qualsiasi controversia dovesse insorgere tra le Parti in ordine al presente Mandato, comprese quelle relative alla validità, interpretazione, esecuzione e risoluzione dello stesso, sarà devoluta in via esclusiva al Tribunale di Roma, con esclusione di qualsiasi altro foro competente.

Luogo _____, data _____

InfoCert S.p.A.	Ufficio di Registrazione	Master R.A.O.
_____	_____	_____

Si intendono espressamente approvati ai sensi e per gli effetti degli artt. 1341 e 1342, c.c., i seguenti articoli: 3 (Obblighi delle Parti); 4 (Corrispettivi e fornitura); 5 (Durata e decorrenza).

_____
(Ufficio di Registrazione)

_____
(Master R.A.O.)

MANDATO QUADRILATERALE PER LO SVOLGIMENTO DI ATTIVITA' DA PARTE DEL R.A.O. SUPPLIER

PER IL RILASCIO DI SERVIZI DI INFOCERT

tra

InfoCert S.p.A., con sede legale in Roma, Piazzale Flaminio 1/B, CF e P. IVA 07945211006, in persona dell'Amministratore Delegato e legale rapp.te *pro-tempore* dott. Danilo Cattaneo, società soggetta a direzione e coordinamento di Tinexta S.p.A. (di seguito "**InfoCert**")

e

XXXX, con sede in _____ n. _____, CF e P. IVA _____, in persona del legale rappresentante *pro tempore* _____ munito dei necessari poteri, come dichiara e garantisce (di seguito, anche "**Ufficio di Registrazione**" o "**R.A.**")

e

XXXX, con sede in _____ n. _____, CF e P.IVA_____, in persona del legale rappresentante *pro tempore* _____ munito dei necessari poteri, come dichiara e garantisce (di seguito, "**R.A.O. Supplier**")

e

XXXX, residente in _____ n. _____, CF _____, (di seguito, "**Operatore dell'Ufficio di Registrazione"** o "**R.A.O.**")

PREMESSO CHE:

a) L'Ufficio di Registrazione ed InfoCert, in data _____ hanno stipulato apposita convenzione (di seguito "**Convenzione"**), con la quale è stato conferito mandato alla prima di svolgere le funzioni di Ufficio di Registrazione, per il rilascio dei Certificati di firma, secondo quanto previsto dal Manuale Operativo ICERT-INDI-MO (di seguito il "**Manuale Operativo Certificati**") e/o per il rilascio dello SPID secondo quanto previsto dal Manuale Operativo ICERT-MO-SPID **("Manuale Operativo SPID");**
b) ai sensi della Convenzione, la R.A. ha facoltà di operare anche attraverso propri R.A.O. Supplier, che si impegneranno ad osservare gli obblighi meglio dettagliati nel prosieguo;
c) con il presente atto, si desidera conferire al R.A.O. Supplier apposito mandato per l'esecuzione delle attività di sua competenza ai sensi della Convenzione, da conferire a sua volta attraverso apposito mandato al R.A.O., nell'ambito dell'identificazione, autenticazione, registrazione e revoca degli utenti (gli "**Utenti**"), nonché quelle di rilascio ed erogazione dei servizi InfoCert ("**Servizi Trust**"), ai sensi del Manuale Operativo;
d) Il R.A.O. Supplier si è reso disponibile a svolgere le attività elencate al punto precedente e meglio dettagliate nel presente atto per il tramite dei propri Operatori di Registrazione, formalizzando l'apposito documento (il "**Mandato**");
e) le procedure di registrazione sono analiticamente esposte nel Manuale Operativo di InfoCert sopra citato, pubblicato sul sito Internet "*www.infocert.it"*, e nei provvedimenti legislativi e amministrativi eventualmente ivi richiamati.

TUTTO CIO' PREMESSO, le Parti convengono quanto segue:

1. PREMESSE

1.1. Le premesse, nonché il PDS e il Manuale Operativo Certificati e Manuale Operativo SPID disponibili sul sito InfoCert (https://www.firma.infocert.it/documentazione/), formano parte integrante del presente Mandato che sarà espletato secondo le specifiche condizioni ivi previste.

2. OGGETTO

2.1 InfoCert, la R.A. e il R.A.O. Supplier conferiscono mandato non esclusivo al R.A.O. a svolgere parte dell'attività di cui alla lett. c) delle premesse e, in particolare, gli obblighi previsti al successivo art. 3.1, esclusivamente attraverso sistemi autorizzati da InfoCert e secondo le modalità concordate da InfoCert e dalla R.A.

2.2 Per lo svolgimento delle attività previste nel presente Mandato, il R.A.O. Supplier si avvarrà di propri dipendenti e/o collaboratori e, in particolare e non in esclusiva, dell'Operatore di Registrazione che sottoscrive parimenti il presente Mandato.

3. OBBLIGHI DELLE PARTI

3.1. La RA, ferme rimanendo le obbligazioni di cui alla Convenzione, provvederà a:

a) supervisionare, per conto di InfoCert, l'attività di formazione e/o aggiornamento dei R.A.O. Supplier;
b) verificare che i destinatari della formazione rispettino i requisiti organizzativi necessari all'esercizio della suddetta attività, come da indicazioni di InfoCert;
c) fornire i beni ed i materiali da consegnare agli Utenti.

3.2 Il R.A.O. Supplier, con la diligenza del mandatario *ex* art. 1710, c.c., dovrà:

a) vigilare sui R.A.O., affinché questi svolgano le attività demandate ai sensi del precedente art. 2, nel rispetto del presente Mandato e della normativa vigente e, in particolare, affinché:
   i. informino gli Utenti sulle modalità di utilizzo del Servizio, con particolare riferimento alle modalità di revoca, sospensione e rinnovo dello stesso nonché su aspetti normativi e conseguenze giuridiche derivanti dall'utilizzo dello stesso;
   ii. interrompano l'attività di identificazione, qualora i documenti presentati dall'Utente o altre circostanze oggettive (es. scarsa qualità dell'audio e/o del video, in caso di identificazione a mezzo *webcam*), non consentano di formare il convincimento sull'identità del Richiedente;
b) far conseguire ai propri R.A.O. la formazione necessaria per le finalità del presente Mandato;
c) assumere gli obblighi descritti nei Manuali Operativi, nell'ultima versione tempo per tempo disponibile online sul sito di InfoCert, e garantire di possedere e mantenere già un'organizzazione di personale e di beni adeguata all'esercizio delle Attività;
d) rispettare le procedure operative di rinnovo, revoca o sospensione dei Servizi Trust come prescritte nei Manuali Operativi;
e) assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniqualvolta venga revocato il Mandato da InfoCert, qualora si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del R.A.O.), dandone tempestiva notizia per iscritto ad InfoCert entro 24 (ventiquattro) ore lavorative;
f) svolgere le Attività nel rispetto della normativa vigente, dei Manuali Operativi e delle istruzioni ricevute da InfoCert, con particolare riferimento all'identificazione personale certa degli Utenti che richiedono l'emissione dei Servizi Trust;

g) informare entro 12 (dodici) ore InfoCert di eventuali vizi, difetti, interruzioni o malfunzionamenti del sistema e/o di errori nello svolgimento delle attività di identificazione e registrazione;
h) consentire alle Autorità di vigilanza, nonché alle R.A. di InfoCert, di accedere nei propri locali per verificare il corretto espletamento delle Attività ed il rispetto delle procedure per lo svolgimento delle stesse;
i) fornire evidenza, entro e non oltre 3 (tre) giorni dalla richiesta da parte di InfoCert, di tutta la documentazione relativa alle Attività, qualora la richiesta derivi dall'Autorità di vigilanza;
j) sottoporre ai Richiedenti, siano esse persone fisiche o giuridiche che richiedono l'emissione dei Servizi Trust per conto dell'Utente, la documentazione contrattuale messa a disposizione da InfoCert, nonché concordare preventivamente con quest'ultima qualsiasi documento da rilasciare all'Utente, relativamente all'attività di registrazione del Certificato e/o di rilascio dei Servizi Trust;
k) mantenere strettamente riservate le credenziali ricevute da InfoCert per l'accesso alla Piattaforma;
l) obbligarsi ad un corretto utilizzo della Piattaforma, nelle modalità indicate da InfoCert;
m) provvedere ad un regolare caricamento/aggiornamento sulla Piattaforma di tutta la documentazione concordata con InfoCert, che dovrà essere fornita a quest'ultima entro i termini con essa convenuti, e in ogni caso qualora InfoCert ne faccia espressa richiesta;
n) impedire ai R.A.O. la prosecuzione delle attività e ritirare ogni materiale a tal fine in uso, qualora, per qualsiasi causa, si interrompa il rapporto in essere e darne tempestivamente notizia per iscritto alla R.A. e a InfoCert;
o) rispettare le istruzioni di cui al successivo art. 6, impartite ai sensi del Reg. (UE) 679/2016;
p) se prevista la sospensione e/o cessazione del Ruolo, così come definito nel Manuale Operativo ICERT-INDI-MO, inviare ad InfoCert la comunicazione di revoca e/o sospensione del Servizio;

3.3. Il R.A.O. con la diligenza del mandatario *ex* art. 1710, c.c., dovrà:

a) assumere gli obblighi descritti nei Manuali Operativi, nell'ultima versione tempo per tempo disponibile online sul sito di InfoCert, e garantire di possedere e mantenere già un'organizzazione di personale e di beni adeguata all'esercizio delle Attività;
b) rispettare le procedure operative di rinnovo, revoca o sospensione dei Servizi Trust definite da InfoCert;
c) assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniqualvolta venga revocato il Mandato da InfoCert o dalla R.A., qualora. si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del R.A.O.), dandone tempestiva notizia per iscritto ad InfoCert;
d) svolgere le Attività nel rispetto della normativa vigente, dei Manuali Operativi e delle istruzioni ricevute da InfoCert, con particolare riferimento all'identificazione personale certa degli Utenti che richiedono l'emissione dei Servizi Trust;
e) informare entro 8 (otto) ore InfoCert di eventuali vizi, difetti, interruzioni o malfunzionamenti del sistema e/o di errori nello svolgimento delle attività di identificazione e registrazione;
f) consentire alle Autorità di vigilanza, nonché agli incaricati di InfoCert, di accedere nei propri locali per verificare il corretto espletamento delle Attività ed il rispetto delle procedure per lo svolgimento delle stesse;
g) fornire evidenza, entro e non oltre 3 (tre) giorni dalla richiesta da parte di InfoCert, di tutta la documentazione relativa alle Attività, qualora la richiesta derivi dall'Autorità di vigilanza;
h) sottoporre agli Utenti, siano esse persone fisiche o giuridiche che richiedono l'emissione dei Servizi Trust per conto dell'Utente, la documentazione contrattuale messa a disposizione da InfoCert, nonché concordare preventivamente con quest'ultima qualsiasi documento da rilasciare all'Utente, relativamente all'attività di registrazione e/o di rilascio dei Servizi Trust;

i) mantenere strettamente riservate le credenziali ricevute da InfoCert per l'accesso alla piattaforma dedicata, propedeutica al caricamento e alla gestione di tutta la documentazione afferente al ciclo-vita della R.A. ("**Piattaforma**");
j) obbligarsi ad un corretto utilizzo della Piattaforma, nelle modalità indicate da InfoCert;
k) provvedere ad un regolare caricamento/aggiornamento sulla Piattaforma di tutta la documentazione richiesta da InfoCert (a titolo meramente esemplificativo e non esaustivo: mandati, modulistica dei Servizi Trust), che dovrà essere fornita a quest'ultima entro i termini con essa convenuti, e in ogni caso qualora InfoCert ne faccia espressa richiesta;
l) impedire ai R.A.O. la prosecuzione delle attività e ritirare ogni materiale a tal fine in uso, qualora, per qualsiasi causa, si interrompa il rapporto in essere e darne tempestivamente notizia per iscritto alla R.A. e a InfoCert;
m) rispettare le istruzioni di cui al successivo art. 6, impartite ai sensi del Reg. (UE) 679/2016;
n) se prevista la sospensione e/o cessazione del Ruolo, così come definito nel Manuale Operativo ICERT-INDI-MO, inviare ad InfoCert la comunicazione di revoca e/o sospensione del Servizio;

3.4 La R.A., il R.A.O. Supplier e il R.A.O. saranno solidalmente responsabili nei confronti di InfoCert per le attività previste nel presente Mandato, anche per eventuali danni patiti dagli Utenti e/o da terzi, direttamente conseguenti a propri comportamenti e/o omissioni colpevoli nonché per i comportamenti e/o le omissioni colpevoli dei propri R.A.O., nell'espletamento degli obblighi nascenti dal presente Mandato e dalla normativa vigente, senza possibilità di esonero neanche parziale e anche in deroga all'art. 1717, c. 2, c.c.
3.5. La violazione di uno qualsiasi degli obblighi di cui al comma 3.2. del presente articolo costituirà giusta causa di revoca del presente Mandato da parte di InfoCert o della R.A., che sarà esercitata a mezzo di apposita comunicazione, fatto salvo il diritto al risarcimento dei danni eventualmente subiti e *subendi*. In caso di revoca, il R.A.O. Supplier è obbligato a cessare qualsiasi attività posta in essere in base al presente atto ed a restituire i materiali ricevuti al fine dell'espletamento dell'incarico.

4. CORRISPETTIVI E FORNITURA

4.1. Il R.A.O. Supplier ed il R.A.O. per lo svolgimento dell'attività prevista nel Mandato non potranno pretendere il pagamento di alcun corrispettivo da parte di InfoCert né vantare alcuna esclusiva nei suoi confronti.
4.2. L'esclusione di cui al precedente comma è altresì valida con riferimento ai mezzi necessari per l'esecuzione del Mandato e alle anticipazioni e spese sostenute dal mandatario.

5. DURATA E DECORRENZA

5.1. Il Mandato avrà efficacia per il periodo di un anno dalla data della sua sottoscrizione e si rinnoverà tacitamente per periodi annuali, salvo disdetta di una delle Parti, da comunicarsi per iscritto almeno 3 (tre) mesi prima della scadenza del periodo annuale, a mezzo Posta Elettronica Certificata o lettera raccomandata A/R. Il Mandato perderà automaticamente efficacia, in ogni caso di cessazione della Convenzione in essere tra InfoCert e l'R.A..
5.2. Durante il periodo di vigenza del Mandato, InfoCert avrà diritto, senza pagamento di alcun corrispettivo, di recedere da esso in qualsiasi momento, con comunicazione della volontà di esercitare tale diritto a mezzo Posta Elettronica Certificata o raccomandata A/R.
5.3. In caso di recesso e/o revoca, il R.A.O. Supplier ed il R.A.O. non potranno vantare alcuna richiesta nei confronti della R.A. e/o di InfoCert, neanche per eventuali danni subiti in conseguenza dello stesso.
5.4. Resta salvo tra le Parti che in caso di risoluzione del presente Mandato, la Convenzione rimane valida ed efficace tra InfoCert e la R.A. fino a naturale vigenza della stessa.

6. PRIVACY

6.1. La R.A. e il R.A.O. Supplier e il R.A.O. si impegnano alla piena osservanza, per quanto di rispettiva competenza, del dettato del Regolamento (UE) 679/2016 e della normativa italiana compatibile con lo stesso.

6.2. Nell'espletamento del mandato, il R.A.O. Supplier e il R.A.O. saranno autorizzati al trattamento dei dati per lo svolgimento delle sole attività oggetto del presente Mandato, sotto la diretta autorità della R.A. e InfoCert attenendosi alle istruzioni impartite da quest'ultima.

6.3. In particolare, il R.A.O. Supplier e il R.A.O. metteranno in atto le seguenti operazioni di trattamento:

a) verifica del documento di identità dell'Utente, della relativa validità e della corrispondenza al soggetto richiedente;
b) trascrizione o verifica (in base alle indicazioni fornite in sede di formazione) delle informazioni inerenti alla persona fisica dell'Utente;
c) produzione della documentazione che attesta l'avvenuto riconoscimento dell'Utente;
d) raccolta dei documenti firmati, se applicabile sulla base della procedura di identificazione messa in atto.

7. LEGGE APPLICABILE E FORO COMPETENTE

7.1. Il presente Mandato è soggetto alla legge italiana.

7.2. Qualsiasi controversia dovesse insorgere tra le Parti in ordine al presente Mandato, comprese quelle relative alla validità, interpretazione, esecuzione e risoluzione dello stesso, sarà devoluta in via esclusiva al Tribunale di Roma, con esclusione di qualsiasi altro foro competente.

Luogo _____, data _____

InfoCert S.p.A.	Ufficio di Registrazione	R.A.O. Supplier	R.A.O.
_____	_____	_____	_____

Si intendono espressamente approvati ai sensi e per gli effetti degli artt. 1341 e 1342, c.c., i seguenti articoli: 3.2, 3.3. e 3.4. (obblighi e responsabilità delle Parti); 4 (Corrispettivi e fornitura); 5 (Durata e decorrenza).

_____
(Ufficio di Registrazione)

_____
(R.A.O. Supplier)

_____
(R.A.O.)

MANDATO TRILATERALE PER LO SVOLGIMENTO DI ATTIVITA' DA PARTE DEL R.A.O. PER IL RILASCIO DI SERVIZI TRUST DI INFOCERT

Tra

InfoCert S.p.A., con sede legale in Roma, Piazzale Flaminio 1/B, CF e P. IVA 07945211006, in persona dell'Amministratore Delegato e legale rapp.te *pro-tempore* dott. Danilo Cattaneo, società soggetta a direzione e coordinamento di Tinexta S.p.A. (di seguito "**InfoCert**")

e

XXXX, con sede in _____ n. _____, CF e P. IVA _____, in persona del legale rappresentante *pro tempore* _____ munito dei necessari poteri, come dichiara e garantisce (di seguito, anche "**Ufficio di Registrazione**" o "**R.A.**")

e

XXXX, residente in _____ n. _____, CF _____, (di seguito, "**Operatore dell'Ufficio di Registrazione"** o "**R.A.O.**")

PREMESSO CHE:

a) L'Ufficio di Registrazione ed InfoCert, in data _____ hanno stipulato apposita convenzione (di seguito "**Convenzione"**), con la quale è stato conferito mandato alla prima di svolgere le funzioni di Ufficio di Registrazione, per il rilascio dei Certificati di firma, secondo quanto previsto dal Manuale Operativo ICERT-INDI-MO (di seguito il "**Manuale Operativo Certificati**") e/o per il rilascio dello SPID secondo quanto previsto dal Manuale Operativo ICERT-MO-SPID **("Manuale Operativo SPID")**;
b) ai sensi della Convenzione, la R.A. ha facoltà di operare anche attraverso propri Operatori dell'Ufficio di Registrazione, che si impegneranno ad osservare gli obblighi meglio dettagliati nel prosieguo;
c) con il presente atto, si desidera conferire all'Operatore dell'Ufficio di Registrazione apposito mandato per l'esecuzione delle attività di sua competenza ai sensi della Convenzione, concernenti le fasi identificazione, autenticazione, registrazione e revoca degli utenti (gli "**Utenti**"), nonché quelle di emissione, revoca e sospensione dei certificati e consegna del dispositivo ("**Servizi Trust**"), ai sensi del Manuale Operativo;
d) l'Operatore dell'Ufficio di Registrazione si è reso disponibile a svolgere le attività elencate al punto precedente e meglio dettagliate nel presente atto (il "**Mandato**");
e) le procedure di registrazione sono analiticamente esposte nel Manuale Operativo di InfoCert sopra citato, pubblicato sul sito Internet "*www.infocert.it"*, e nei provvedimenti legislativi e amministrativi eventualmente ivi richiamati.

TUTTO CIO' PREMESSO, e Parti convengono quanto segue:

1. PREMESSE

1.1. Le premesse, nonché il PDS e il Manuale Operativo Certificati e Manuale Operativo SPID disponibili sul sito InfoCert (https://www.firma.infocert.it/documentazione/) formano parte integrante del presente Mandato che sarà espletato secondo le specifiche condizioni ivi previste.

2. OGGETTO

2.1. InfoCert e la R.A. conferiscono mandato non esclusivo all'Operatore dell'Ufficio di Registrazione a svolgere parte dell'attività di cui alla lett. c) delle premesse e, in particolare, a identificare gli Utenti con certezza, esclusivamente attraverso sistemi autorizzati da InfoCert e secondo le modalità concordate da InfoCert e dalla R.A.

3. OBBLIGHI DELLE PARTI

3.1. La R.A., ferme rimanendo le obbligazioni di cui alla Convenzione, provvederà a:

a) supervisionare, per conto di InfoCert, l'attività di formazione e/o aggiornamento dei R.A.O.;
b) verificare che gli Operatori dell'Ufficio di Registrazione eseguano con la dovuta diligenza le attività a loro assegnate;
c) monitorare costantemente che gli Operatori dell'Ufficio di Registrazione mantengano i requisiti di competenza, affidabilità, onorabilità ed esperienza ai sensi dell'art. 24 par. 2 lett. b) del Regolamento eIDAS;
d) assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniqualvolta venga revocato il Mandato da InfoCert o dalla R.A., qualora cessi il rapporto di dipendenza/collaborazione tra l'Ufficio di Registrazione e il R.A.O., ovvero si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del R.A.O.), dandone tempestiva comunicazione per iscritto ad InfoCert entro 24 (ventiquattro) ore lavorative;
e) fornire i beni ed i materiali ai R.A.O. da consegnare agli Utenti.

3.2 L'Operatore dell'Ufficio di Registrazione, con la diligenza del mandatario *ex* art. 1710, c.c., dovrà:

a) conseguire la formazione necessaria per le finalità del presente mandato, partecipando ai corsi di formazione come predisposti dal R.A. ai sensi dell'art. 3.1 lett. a);
b) prendere visione delle istruzioni contenute nei Manuali Operativi, nell'ultima versione tempo per tempo disponibile online sul sito di InfoCert, e garantire di possedere e mantenere in essere requisiti di onorabilità e professionalità necessari all'esercizio delle Attività;
c) rispettare le procedure operative di rinnovo, revoca o sospensione dei Servizi Trust definite da InfoCert;
d) esercitare le Attività nell'interesse di InfoCert e con la diligenza del mandatario, ex art. 1710, c.c.;
e) svolgere le Attività nel rispetto della normativa vigente, dei Manuali Operativi e delle istruzioni ricevute da InfoCert, con particolare riferimento all'identificazione personale certa degli Utenti che richiedono l'emissione dei Servizi Trust;
f) informare entro 12 (dodici) ore InfoCert di eventuali vizi, difetti, interruzioni o malfunzionamenti del sistema e/o di errori nello svolgimento delle attività di identificazione e registrazione;
g) consentire alle Autorità di vigilanza, nonché alle R.A. di InfoCert, di accedere nei propri locali per verificare il corretto espletamento delle Attività ed il rispetto delle procedure per lo svolgimento delle stesse;
h) fornire evidenza, entro e non oltre 3 (tre) giorni dalla richiesta da parte di InfoCert, di tutta la documentazione relativa alle Attività, qualora la richiesta derivi dall'Autorità di vigilanza;
i) sottoporre agli Utenti, siano esse persone fisiche o giuridiche che richiedono l'emissione dei Servizi Trust per conto dell'Utente, la documentazione contrattuale messa a disposizione da InfoCert, nonché concordare

preventivamente con quest'ultima qualsiasi documento da rilasciare al Richiedente e/o Utente, relativamente all'attività di registrazione del Certificato e/o di rilascio dei Servizi Trust;

j) mantenere strettamente riservate le credenziali ricevute da InfoCert per l'accesso alla piattaforma dedicata, propedeutica al caricamento e alla gestione di tutta la documentazione afferente al ciclo-vita della R.A. ("**Piattaforma**");
k) obbligarsi ad un corretto utilizzo della Piattaforma, nelle modalità indicate da InfoCert;
l) provvedere ad un regolare caricamento/aggiornamento sulla Piattaforma di tutta la documentazione richiesta da InfoCert (a titolo meramente esemplificativo e non esaustivo: mandati, modulistica dei Servizi Trust), che dovrà essere fornita a quest'ultima entro i termini con essa convenuti, e in ogni caso qualora InfoCert ne faccia espressa richiesta.

3.3. L' Operatore dell'Ufficio di Registrazione e la R.A. saranno solidalmente responsabili nei confronti di InfoCert per le attività previste nel presente Mandato.

3.4. La violazione di uno qualsiasi degli obblighi di cui al comma 3.2. e 3.3 del presente articolo costituirà giusta causa di revoca del presente Mandato da parte di InfoCert o della R.A., che sarà esercitata a mezzo di apposita comunicazione, fatto salvo il diritto al risarcimento dei danni eventualmente subiti e *subendi*. In caso di revoca, l'Operatore dell'Ufficio di Registrazione è obbligato a cessare qualsiasi attività posta in essere in base al presente atto ed a restituire i materiali ricevuti al fine dell'espletamento dell'incarico.

4. CORRISPETTIVI E FORNITURA

4.1. L' Operatore dell'Ufficio di Registrazione e la R.A. per lo svolgimento dell'attività prevista nel Mandato non potranno pretendere il pagamento di alcun corrispettivo da parte di InfoCert né vantare alcuna esclusiva nei suoi confronti.

4.2. L'esclusione di cui al precedente comma è altresì valida con riferimento ai mezzi necessari per l'esecuzione del Mandato e alle anticipazioni e spese sostenute dal mandatario.

5. DURATA E DECORRENZA

5.1. Il Mandato avrà efficacia per il periodo di un anno dalla data della sua sottoscrizione e si rinnoverà tacitamente per periodi annuali, salvo disdetta di una delle Parti, da comunicarsi per iscritto almeno 3 (tre) mesi prima della scadenza del periodo annuale, a mezzo Posta Elettronica Certificata o lettera raccomandata A/R. Il Mandato perderà automaticamente efficacia, in ogni caso di cessazione della Convenzione in essere tra InfoCert e la R.A..

5.2. Durante il periodo di vigenza del Mandato, InfoCert avrà diritto, senza pagamento di alcun corrispettivo, di recedere da esso in qualsiasi momento, con comunicazione della volontà di esercitare tale diritto a mezzo Posta Elettronica Certificata o raccomandata A/R.

5.3. In caso di recesso e/o revoca, l'Operatore dell'Ufficio di Registrazione non potrà vantare alcuna richiesta nei confronti della R.A. e/o di InfoCert, neanche per eventuali danni subiti in conseguenza dello stesso.

5.4. Resta salvo tra le Parti che in caso di risoluzione del presente Mandato, la Convenzione rimane valida ed efficace tra InfoCert e la R.A. fino a naturale vigenza della stessa.

6. PRIVACY

6.1. La R.A. e l'Operatore dell'Ufficio di Registrazione si impegnano alla piena osservanza, per quanto di rispettiva competenza, del dettato del Regolamento (UE) 679/2016 e della normativa italiana compatibile con lo stesso.

6.2. Nell'espletamento del mandato, l'Operatore dell'Ufficio di Registrazione sarà autorizzato al trattamento dei dati per lo svolgimento delle sole attività oggetto del presente Mandato, sotto la diretta autorità della R.A. e InfoCert attenendosi alle istruzioni impartite da quest'ultima.

6.3. In particolare, l'Operatore dell'Ufficio di Registrazione metterà in atto le seguenti operazioni di trattamento:

a) verifica del documento di identità del richiedente, della relativa validità e della corrispondenza al soggetto richiedente;
b) trascrizione o verifica (in base alle indicazioni fornite in sede di formazione) delle informazioni inerenti alla persona fisica del richiedente;
c) produzione della documentazione che attesta l'avvenuto riconoscimento dell'Utente;
d) raccolta dei documenti firmati, se applicabile sulla base della procedura di identificazione messa in atto.

7. LEGGE APPLICABILE E FORO COMPETENTE

7.1. Il presente Mandato è soggetto alla legge italiana.

7.2. Qualsiasi controversia dovesse insorgere tra le Parti in ordine al presente Mandato, comprese quelle relative alla validità, interpretazione, esecuzione e risoluzione dello stesso, sarà devoluta in via esclusiva al Tribunale di Roma, con esclusione di qualsiasi altro foro competente.

Luogo _____, data _____

InfoCert S.p.A.	Ufficio di Registrazione	Operatore dell'Ufficio di Registrazione
_____	_____	_____

Si intendono espressamente approvati ai sensi e per gli effetti degli artt. 1341 e 1342, c.c., i seguenti articoli: 3 (Obblighi delle Parti); 4 (Corrispettivi e fornitura); 5 (Durata e decorrenza).

_____

(Ufficio di Registrazione)

_____

(Operatore dell'Ufficio di Registrazione)

tinexta infocert

Requisiti di compliance

Registration Authority

1 INTRODUZIONE

SCOPO

I Clienti che svolgono l'attività di Registration Authority per conto di InfoCert, eventualmente anche integrando i loro servizi con componenti applicative, devono rispettare, nell'erogazione del servizio oggetto dell'Accordo, i seguenti principi e criteri, necessari a garantire una adeguata compliance alla normativa relativa ai servizi fiduciari:

- sicurezza informatica;
- erogazione dei servizi IT;
- qualità del servizio;
- requisiti ambientali;
- requisiti per la fornitura.

RIFERIMENTI

- ISO/IEC 27001 - Sistema di gestione sulla Sicurezza delle informazioni
- ISO 20000-1 - Requisiti sistema di gestione dei servizi IT
- ISO 9001 - Sistemi di gestione qualità
- ISO 14001 - Sistemi di gestione ambientale
- ETSI EN 319 401 – Policy di requisiti generali per i Fornitori di servizi fiduciari

2 REQUISITI

Sono qui di seguito delineati i **Requisiti** ai quali la Registration Authority deve garantire di essere conforme, al fine di rispettare i principi e criteri di compliance di cui alla normativa dei servizi fiduciari.

MISURE ORGANIZZATIVE

La Registration Authority deve:

- garantire, nell'erogazione del servizio contrattualizzato, personale, adeguatamente informato e formato sui requisiti minimi in ambito di information security. La Registration Authority deve anche conservare appropriate informazioni documentate quale evidenza delle competenze e della formazione effettuate sui temi di cui sopra;
- garantire che le figure degli Operatori dell'Ufficio di Registrazione (RAO) ovvero dei Master RAO abbiano compreso loro mansioni e responsabilità, siano costantemente aggiornati sulle stesse e che abbiano frequentato e concluso un corso adeguato nei processi di erogazione dei servizi fiduciari che li riguardano;
- definire e rispettare una procedura per la gestione, la protezione ed il monitoraggio degli accessi fisici agli spazi aziendali della Registration Authority, che consideri anche i locali adibiti alla conservazione delle informazioni correlate al servizio erogato (archivi cartacei, etc);
- definire le responsabilità in merito alla protezione dei dati personali all'interno dell'azienda, in coerenza con quanto sottoscritto in termini di Accordo e/o mandato con InfoCert;
- garantire conformità ai requisiti legislativi applicabili per la tutela della privacy: informative, trattamenti, cancellazione dati, gestione data breach, valutazione d'impatto, protezione dei dati memorizzati, protezione dei dati trasmessi, cancellazione sicura dei dati e modalità di conservazione dei dati personali, ecc;
- definire le proprie politiche/regolamenti relativi alla sicurezza informatica, garantendo che siano applicate all'interno di tutta l'Azienda;
- prevedere l'inserimento di analoghi requisiti di sicurezza, riservatezza, privacy nei contratti con gli eventuali sub-fornitori, qualora preventivamente autorizzati da InfoCert;
- garantire il monitoraggio della sicurezza informatica degli eventuali sub- fornitori con potenziale impatto sui servizi oggetto dell'Accordo e che possano pertanto pregiudicare gli SLA concordati;
- verificare le misure di sicurezza delle informazioni adottate da eventuali terze parte fornitrici di servizi cloud computing coinvolte nelle attività contrattualizzate e comunicarle ad InfoCert;
- comunicare un processo di gestione degli incidenti di sicurezza delle informazioni e, in caso di incidente significativo, garantirne la comunicazione ad InfoCert entro 8 ore

dall'avvenuta conoscenza dell'evento (si veda capitolo specifico "Comunicazione incidente di sicurezza informatica significativo");

- garantire la disponibilità alle attività di monitoraggio, annuale o ad evento significativo, dei requisiti suddetti da parte del Committente attraverso la somministrazione di questionari;
- garantire un processo di gestione delle emergenze per la sicurezza nei luoghi di lavoro;
- rispettare le normative vigenti in ambito ambientale applicabili all'oggetto della fornitura.

MISURE TECNOLOGICHE

La Registration Authority deve:

- definire e descrivere una modalità di utilizzo delle risorse informatiche aziendali condivisa all'interno dell'organizzazione sia per i dipendenti che per i collaboratori e che comprenda almeno:
  - una policy di generazione ed utilizzo delle password di dominio;
  - modalità di protezione degli endpoint aziendali (password del BIOS, cifratura disco, piattaforma MDM, etc);
  - l'utilizzo in tutte le postazioni di software antivirus/anti malware;
  - obblighi e limitazioni d'uso dei dispositivi informatici;
  - una procedura di gestione degli aggiornamenti software;
  - le tecniche di sicurezza implementate nei casi di utilizzo di reti wireless;
  - misure di sicurezza adottate nei casi di lavoro da remoto (es.VPN, crittografia delle comunicazioni, etc);
- garantire che le password di accesso ai sistemi e alle applicazioni utilizzate nell'erogazione della fornitura, siano univoche, personali, "forti" e non memorizzate su supporti logici/fisici.
  Di seguito alcuni esempi di buone pratiche nella creazione di password:
  - Almeno 1 lettera minuscola
  - Almeno 1 lettera maiuscola
  - Almeno 1 numero
  - Almeno 1 carattere speciale
  - Non deve contenere uno dei seguenti pattern = qwerty, asdf , 1234
  - Lunghezza di almeno 8 caratteri
  - Non è una parola di una qualunque lingua, dialetto o linguaggio specialistico
  - Non si basa su informazioni personali.

  Tali password dovranno essere gestite utilizzando esclusivamente un sistema di password manager;
- garantire di aver definito ed attuato un processo per l'assegnazione e la revoca dei diritti di accesso e delle abilitazioni degli operatori preposti. Deve essere verificato che l'accesso alle workstation da parte degli operatori preposti avvenga esclusivamente

tramite le credenziali personali;

- garantire che eventuali sistemi informativi coinvolti nei processi oggetto dell'Accordo siano stati periodicamente analizzati e scansionati al fine di individuare e risolvere eventuali vulnerabilità tecniche (almeno annualmente).
  Le attività di remediation devono rispettare le seguenti tempistiche: 0day/Early Warning 5gg, Critical/High 30 gg, Medium 90 gg, Low 120 gg, considerando come riferimento il risk score CVSS (Common Vulnerability Scoring System). Queste tempistiche devono essere rispettate anche nei casi di remediation chieste da InfoCert;
- garantire un flusso autorizzativo degli accessi logici ai sistemi ed alle applicazioni per gli utenti. Inoltre, la Registration Authority deve garantire un processo di gestione e monitoraggio degli amministratori di sistema;
- definire le misure di sicurezza informatica adottate per proteggere la rete (DMZ, firewall, etc.);
- garantire che le connessioni di rete siano sicure e protette con adeguate tecnologie di crittografia;
- assicurare che le informazioni ed i sistemi informativi siano protetti contro malware/antispam;
- garantire, nei casi di utilizzo di dispositivi fisici (smart card o business key) per il rilascio di certificati di firma, un processo di:
  - ✓ conservazione sicura di tali dispositivi (es. magazzino con protezioni antiallagamento, anti-danneggiamento, antincendio, etc);
  - ✓ gestione di un inventario di tali asset;
  - ✓ definizione di una lista di utenti autorizzati all'utilizzo e gestione di tali asset;
  - ✓ consegna ai clienti finali di tali asset;
  - ✓ gestione e smaltimento dei dispositivi obsoleti, che comprenda la definizione delle attività di utilizzo, conservazione e gestione dell'obsolescenza.

Inoltre, nei casi in cui la Registration Authority (RA), per la sua attività nel processo di erogazione di servizi fiduciari, utilizzi software o parti di esso sviluppati internamente, si aggiungono i seguenti requisiti:

- se sono presenti servizi di web running gestiti dalla RA, devono essere garantite misure di ridondanza dell'impianto di alimentazione elettrica (eventuali UPS, sistemi generazioni di emergenza, etc) e di sistemi di sicurezza fisica ove siano gestiti i dati (sistemi antincendio, sistemi videosorveglianza, etc);
- definire un processo di gestione delle richieste di change, incluse le proposte per aggiungere, rimuovere o trasferire servizi, che ne preveda la registrazione e la classificazione, l'approvazione formale, la verifica ed i test preliminari al rilascio della change stessa.
  Nei casi di change richieste da InfoCert, la Registration Authority deve garantire l'applicazione delle stesse nei tempi richiesti dalla Committente.
  Inoltre, prevedere una tempestiva comunicazione ad InfoCert nei casi di modifiche che

impattano la sicurezza dei sistemi applicativi utilizzati nell'erogazione del servizio contrattualizzato;

- definire e rispettare un processo di sviluppo sicuro del software che preveda dei test periodici di sicurezza e la formazione degli sviluppatori coinvolti;
- garantire che gli ambienti di sviluppo, collaudo e produzione siano segregati logicamente;
- gestire le fasi di release e deploy nel rispetto dei principi dello sviluppo sicuro che garantisca ad esempio:
    - ✓ la definizione dei requisiti di sicurezza in fase progettuale,
    - ✓ i requisiti di sicurezza devono garantire l'integrità, la riservatezza e la disponibilità dei dati gestiti dall'applicazione, tramite l'applicazione dei criteri di Software Development Life Cycle (SDLC),
    - ✓ la valutazione dei rischi emergente dalla combinazione tra la classificazione dei dati, trattati, gli eventuali impatti in tema di Data Protection e l'ambito di utilizzo,
    - ✓ l'assicurazione dell'integrità dei dati "at rest", "in transit" ed "end-to-end",
    - ✓ gli ambienti di sviluppo, test e produzione devono essere separati,
    - ✓ scansioni statiche del codice,
    - ✓ devono essere definite e documentate le modalità per tenere traccia del ciclo di vita dei dati personali (dalla raccolta alla conservazione, fino alla distruzione),
    - ✓ i cambiamenti ai sistemi all'interno del ciclo di vita devono essere tenuti sotto controllo attraverso l'utilizzo di procedure formali di controllo dei cambiamenti,
    - ✓ il prodotto/servizio non deve contenere vulnerabilità note
    - ✓ durante lo sviluppo devono essere effettuati test relativi alle funzionalità di sicurezza del prodotto/servizio.
- definire e rispettare una procedura per la gestione della configurazione;
- definire e rispettare un processo di gestione delle vulnerabilità infrastrutturali e delle applicazioni (coinvolte nell'oggetto della fornitura) che preveda sia delle scansioni periodiche, almeno annuali, che delle attività di remediation a valle di vulnerabilità riscontrate o degli aggiornamenti software.
  Le attività di remediation devono rispettare le seguenti tempistiche: 0day/Early Warning 5gg, Critical/High 30 gg, Medium 90 gg, Low 120 gg, considerando come riferimento il risk score CVSS (Common Vulnerability Scoring System). Queste tempistiche devono essere rispettate anche nei casi di remediation chieste da InfoCert;
- definire ed attuare un processo di risk management relativo alla sicurezza delle informazioni aziendali;
- definire e rispettare un processo di backup delle informazioni, che descriva metodi, retention, strumenti;
- monitorare il livello di conformità alla gestione della sicurezza delle informazioni.

COMUNICAZIONE INCIDENTE DI SICUREZZA INFORMATICA SIGNIFICATIVO

Gli incidenti di sicurezza, per tali intendendo qualsivoglia evento o insieme di eventi che sottintendono una violazione o anche solo la minaccia di violazione delle politiche di sicurezza ICT e per la quale si renda necessaria l'applicazione di misure di contrasto e/o contenimento da parte delle strutture preposte, possono essere di varia natura e con vari livelli di criticità associati.
Secondo la definizione della Direttiva (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022 (NIS2) un incidente è considerato significativo se:

- ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
- si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

L'identificazione di quali di essi possano essere identificati come significativi è lasciata alla discrezionalità del caso specifico, ma di seguito viene fornita una lista, non esaustiva, dei casi in cui un incidente è da ritenersi significativo e pertanto soggetto alla gestione descritta nel presente paragrafo:

- eventi che impattano negativamente sulle risorse infrastrutturali critiche o sui dati in esse contenuti;
- incidenti che impattano un elevato numero di clienti;
- incidenti che coinvolgono dati personali e/o sensibili e che potrebbero richiedere la notifica verso il garante e/o il cliente, come previsto dal GDPR;
- incidenti che diventano di pubblico dominio attraverso i media;
- incidenti che violino le normative e/o le leggi che regolano i servizi forniti da InfoCert;
- incidenti che potrebbero avere un impatto negativo sulla reputazione di InfoCert;
- tipologie di incidenti comprese negli adempimenti normativi InfoCert.

In caso di incidente di sicurezza significativo relativo al servizio contrattualizzato, la Registration Authority dovrà seguire la seguente procedura:

- Prima comunicazione ad InfoCert alla casella di posta cyber.security@infocert.it
  - ✓ SLA: in mancanza di specifica contrattuale, entro 8 ore dalla verifica dell'incidente
  - ✓ Oggetto della comunicazione: Segnalazione Incidente di Sicurezza
  - ✓ Corpo della comunicazione: Descrizione dell'evento
- Report Incident da inviare ad InfoCert contenente
  - ✓ SLA: in mancanza di specifica contrattuale, entro 5 giorni lavorativi dalla verifica dell'incidente
  - ✓ Oggetto della comunicazione: Report Incident di Sicurezza
  - ✓ Allegato della comunicazione: Report Incident con il contenuto relativo al seguente sommario:
    - Template Verbale Incident di sicurezza
    - 1.1 Novità introdotte rispetto alla precedente emissione

- 1.2 Scopo e campo di applicazione del documento
- 1.3 Termini e definizioni
- 2 Servizi cui il verbale si riferisce
- 3 Descrizione dell'incidente
- 4 Analisi delle cause dell'evento
- 5 Azioni completate/in corso per ridurre la probabilità del ripetersi dell'evento e mitigare gli impatti
- 6 Appendice – Estrazione log.

Provincia di Padova

Ufficio SPESA

Visto Contabile

Determina N. 816 del 18/07/2025

SERVIZIO SISTEMI INFORMATIVI

Proposta n° 2122 /2025

Oggetto: APPROVAZIONE SCHEMI CONTRATTUALI PER LO SVOLGIMENTO DI ATTIVITÀ DI UFFICIO DI REGISTRAZIONE E RILASCIO DI SERVIZI DI CERTIFICAZIONE DIGITALE E DELLA CARTA NAZIONALE DEI SERVIZI TRA LA PROVINCIA DI PADOVA (ENTE EMETTITORE) E INFOCERT SPA (CERTIFICATION AUTHORITY) .

Ai sensi dell' art. 183, c.7 del Decreto legislativo n. 267 del 18 agosto 2000, si appone il visto di regolarità contabile attestante la copertura finanziaria

Padova li,
21/07/2025

Sottoscritto dal Dirigente
(CREMONESE MASSIMO)
con firma digitale