ACCORDO

tra

PagoPA S.p.A., con sede legale in Roma, Piazza Colonna n. 370, c. f., P.I. e iscrizione al Registro delle Imprese di Roma n. 15376371009, in persona del suo legale rappresentante pro tempore, dott. Alessandro Moricca (di seguito, "**PagoPA**" o "**Società**")

e

l'Universita' degli Studi di Messina, con sede legale in Piazza Pugliatti N. 1, 98121, nella persona della Rettrice, Prof.ssa Giovanna Spatari, codice fiscale 80004070837, partita IVA 00724160833, Indirizzo PEC protocollo@pec.unime.it (di seguito **Ente**);

Ente e PagoPA, di seguito singolarmente "**Parte**" e congiuntamente "**Parti**"

PREMESSO CHE

a. PagoPA è una società per azioni interamente partecipata dallo Stato creata, ai sensi del Decreto Legge 14 dicembre 2018, n. 135, convertito con modificazioni dalla legge 11 febbraio 2019, n. 12, allo scopo di diffondere i servizi digitali in Italia, attraverso la gestione del punto di accesso telematico ai servizi della Pubblica Amministrazione ai sensi dell'articolo 64-bis del decreto legislativo 7 marzo 2005, n. 82 recante il codice dell' amministrazione digitale ("**CAD**") (di seguito, **Piattaforma IO**), come definito nelle linee guida sul punto di accesso telematico ai servizi della Pubblica Amministrazione ("**Linee Guida**") e attraverso la gestione di progetti innovativi legati ai servizi pubblici tra cui la piattaforma pagoPA per i pagamenti digitali verso la Pubblica Amministrazione di cui all'articolo 5 del CAD e la Piattaforma digitale nazionale dati (PDND) di cui all'articolo 50-ter del CAD;
b. al fine di ampliare l'offerta dei servizi digitali della pubblica amministrazione, è in corso di sperimentazione da parte di PagoPA una soluzione tecnologica che introduce una funzionalità utile al fine di sottoscrivere i documenti inviati dai soggetti di cui all'articolo 2, comma 2, del CAD ("**Enti**") ai cittadini mediante firma elettronica qualificata (di seguito, "**Firma con IO**");
c. più in particolare, Firma con IO consente agli Enti di inviare tramite messaggio su Piattaforma IO o call to action sul proprio sito web documenti per i quali è richiesta l'apposizione della firma da parte degli utenti destinatari ("**Utente/i**"), permettendo loro di apporre una firma elettronica qualificata attraverso la Piattaforma IO per la sottoscrizione di tali documenti, con una modalità semplice e interamente digitalizzata;
d. nell'ambito dell'esecuzione del servizio Firma con IO (di seguito anche "**Servizio**"), PagoPA si avvarrà di un prestatore di servizi fiduciari qualificati per l'erogazione della firma elettronica

qualificata ai sensi del Regolamento Europeo n. 910/2014 (" **Regolamento eIDAS**") autorizzato dall'Agenzia per l'Italia digitale ("**AgID**") ai fini dell'emissione del certificato qualificato di firma (il "**Prestatore di Servizi**");

e. il servizio Firma con IO è in fase di sperimentazione/beta testing, pertanto vi è la possibilità che durante detta fase le funzionalità del Servizio potrebbero essere depotenziate, presentare problematiche di funzionamento e/o di indisponibilità momentanea o definitiva oppure aspetti che richiedano interventi o miglioramenti;

f. in considerazione di quanto sopra, le Parti, con il presente accordo (di seguito, "**Accordo**"), intendono disciplinare i termini e le condizioni di utilizzo del servizio Firma con IO da parte dell' Ente, per l'espletamento di attività di interesse comune.

Tutto ciò premesso, le Parti, come sopra rappresentate

STIPULANO E CONVENGONO QUANTO SEGUE

Art. 1 - Valore delle premesse, degli Allegati, della Documentazione Correlata e disciplina applicabile

1. Le premesse, gli allegati di cui al comma 3 che segue, nonché la documentazione richiamata nell'Accordo e negli allegati stessi, ancorché non materialmente allegata al presente Accordo (di seguito, "**Documentazione Correlata**"), costituiscono parte integrante e sostanziale del presente Accordo, e vincolano le Parti al loro rispetto.
2. L'Accordo è stipulato in analogia alla modalità elettronica ai sensi dell'articolo 18, comma 1, del decreto legislativo 31 marzo 2023, n. 36 ("Codice dei contratti pubblici") e nel rispetto delle pertinenti disposizioni del CAD.
3. Sono allegati al presente Accordo i seguenti documenti:
   A. Trattamento di dati personali e nomina a responsabile del trattamento di nomina a responsabile del trattamento dei dati personali di PagoPA ai sensi dell' articolo 28 del Regolamento (UE) 2016/679 ("**DPA**");
   B. Allegato Tecnico reperibile al seguente link: https://docs.pagopa.it/manuale-operativo-di-firma-con-io/;
   C. Livelli di servizio.

Art. 2 - Oggetto finalità dell'Accordo

1. Il presente Accordo regola la licenza di utilizzo del servizio Firma con IO in corso di sperimentazione da parte di PagoPA in favore dell'Ente, alle condizioni ed ai termini ivi previsti, al fine di consentire all'Ente di offrire agli Utenti un metodo agevole, sicuro e certo di sottoscrizione dei documenti con firma elettronica qualificata tramite la Piattaforma IO.
2. La modalità tecnica con cui il servizio Firma con IO viene messa a disposizione dell'Ente è descritta nel dettaglio nell'Allegato Tecnico di cui all'art. 1, comma 3, lett. c) che precede.
3. A fronte di ogni utilizzo del servizio Firma con IO, l'Ente si impegna a pagare in favore di PagoPA il corrispettivo individuato al successivo articolo 7.
4. Ciascuna delle Parti è responsabile in via diretta ed esclusiva dell'esecuzione delle attività ad essa facenti capo nell'ambito delle prestazioni oggetto del presente Accordo.
5. L'Ente accetta e riconosce che, ai fini dell'esecuzione

delServizio a norma di legge PagoPA si avvarrà di un Prestatore di Servizi indicato nella lista fornitori di IO rinvenibile all'indirizzo https://io.italia.it/app-content/fornitori/.

6. L'Ente dichiara altresì di aver ricevuto tutte le informazioni necessarie per verificare che il Servizio corrisponda alle sue esigenze e si impegna a controllare tale corrispondenza in ragione dell'evolversi del Servizio in corso di sperimentazione; di conseguenza, PagoPA non può essere in alcun modo ritenuta responsabile di eventuali inidoneità del Servizio alle esigenze dell'Ente e resta altresì inteso che PagoPA non ha obblighi di verifica dei dati trasmessi dall'Utente e dall'/all'Ente.
7. L'Ente si impegna, ove necessario, ad informare gli Utenti che essi stanno partecipando a una fase di sperimentazione del Servizio e il loro ruolo è quello di contribuire alla stessa segnalando eventuali anomalie e problematiche riscontrate, senza alcuna garanzia in merito ad un ottimale funzionamento dei servizi.
8. Ai fini di cui al presente Accordo, PagoPA fornisce all'Ente una licenza limitata, non esclusiva per l'utilizzo del Servizio Firma con IO.

Art. 3 - Durata, recesso e cessione

1. Il presente Accordo è valido ed efficace a partire dalla data di sottoscrizione dello stesso da parte dell'Ente e per una durata di 24 mesi. Qualora nessuna delle Parti comunichi all'altra, ai sensi e con le modalità di cui all'art. 11 che segue, la disdetta entro 30 giorni rispetto alla data prevista per la scadenza il contratto si intenderà tacitamente rinnovato per il medesimo periodo.
2. PagoPA potrà recedere dal presente Accordo, in qualsiasi momento, senza obbligo di motivazione, con un preavviso minimo di 15 giorni, e senza alcun rimborso, risarcimento, indennizzo, costo, onere o altro corrispettivo, terminando la sperimentazione e/o l'erogazione del Servizio tramite comunicazione da inviare all'Ente per iscritto, tramite PEC, ai sensi dell'articolo 11 che segue.
3. L'Ente potrà recedere dal presente Accordo, in qualsiasi momento, senza obbligo di motivazione, con un preavviso minimo di 15 giorni, e senza alcun rimborso, risarcimento, indennizzo, costo, onere o altro corrispettivo tramite comunicazione da inviare a PagoPA per iscritto, tramite PEC, ai sensi dell'articolo 11 che segue.
4. Resta inteso che il recesso di una delle due Parti non libera quest'ultima dagli obblighi assunti e non ancora pienamente assolti.
5. E' fatto espresso divieto all'Ente di cedere, in tutto o in parte, il presente Accordo e/o trasferire i diritti e gli obblighi derivanti dallo stesso senza il preventivo consenso di PagoPA.

Art. 4 - Aggiornamento e modifica dell'Accordo, integrazione automatica e garanzie

3. Qualora si tratti di modifiche e/o integrazioni al presente Accordo che non richiedano delle implementazioni applicative e/o infrastrutturali da parte dell'Ente, tali modifiche e/o integrazioni entreranno in vigore trascorsi 90 (novanta) giorni a

partire dalla data di loro comunicazione a mezzo PEC all'Amministratore dell'Ente, fermo restando sempre il diritto di recedere da parte dell'Ente.

4. Qualora, invece, si tratti di modifiche e/o integrazioni agli allegati di cui all'art. 1 che precede e/o alla Documentazione Correlata che richiedano delle implementazioni applicative e/o infrastrutturali da parte dell'Ente, tali modifiche e/o integrazioni, entreranno in vigore trascorsi 180 (centottanta) giorni a partire dalla data di loro comunicazione a mezzo PEC all'Amministratore dell'Ente, fermo restando sempre il diritto di recedere da parte dell'Ente. A PagoPA è riconosciuta la facoltà di individuare e, se del caso, comunicare all'Ente due date prestabilite dell'anno per fare in modo che le modifiche di cui al presente comma possano entrare in vigore in tali due date prestabilite espressamente indicate all'Ente tramite apposita comunicazione.
5. In deroga al comma 4, le Parti si impegnano a realizzare gli interventi d'urgenza che si dovessero rendere necessari per assicurare la corretta funzionalità del Servizio.
6. Resta inteso tra le Parti che in nessun caso verranno introdotte modifiche relative all'oggetto, al pagamento del corrispettivo e in generale, modifiche sostanziali al presente Accordo per la fruizione del Servizio, senza accettazione espressa dalle Parti.

Art. 5 - Modalità di esecuzione del Servizio e obblighi delle Parti

1. PagoPA si impegna a fornire il Servizio in conformità ai termini e alle condizioni contenute nel presente Accordo, negli allegatie nella Documentazione Correlata.
2. L'Ente accetta, riconosce e garantisce che:
   - è responsabilità esclusiva dello stesso porre in essere, a propria cura e spese, tutte le attività necessarie all' integrazione tecnologica, come descritto nell'Allegato Tecnico e nella Documentazione Correlata;
   - per aderire al Servizio, deve preliminarmente completare il processo di accreditamento;

   pena l'impossibilità di fruire del Servizio.
3. Affinchè l'Ente possa usufruire del Servizio dovrà integrarsi secondo le modalità indicate all'Allegato B.
4. Ciascuna Parte si impegna a informare tempestivamente l'altra sulle principali criticità/anomalie operative riscontrate durante l'esecuzione del presente Accordo.
5. Resta inteso tra le Parti che, con la sottoscrizione del presente Accordo, l'Ente acquista il diritto di utilizzare il Servizio Firma con IO per farne ogni uso alla stessa consentito, con espresso divieto per l'Ente di utilizzare Firma con IO e/o i dati ottenuti in esecuzione del presente Accordo per scopi diversi da quelli previsti dall'Accordo stesso, per scopi illeciti e ulteriori rispetto alle proprie finalità istituzionali/ statutarie.
6. L'Ente accetta e riconosce che gravano esclusivamente sul Prestatore di Servizi di cui si avvarrà PagoPA nell'ambito dell' esecuzione del Servizio, gli obblighi di conservazione del certificato di firma qualificata nei modi e nei termini meglio descritti nell'Allegato Tecnico e che pertanto qualsiasi pretesa relativa all'ottenimento dello stesso dovrà essere

avanzata dall'Ente verso il Prestatore di Servizi.

7. L'Ente accetta e riconosce altresì che grava esclusivamente sullo stesso l'obbligo di conservazione del documento sottoscritto dall'Utente.
8. E',altresì, fatto esplicito divieto di, e l'Ente si impegna a non:
   - aggirare o manomettere i sistemi preposti al funzionamento del Servizio,
   - accedere al Servizio attraverso programmi o metodi diversi da quelli ufficialmente rilasciati e gestiti da PagoPA;
   - utilizzare il Servizio in violazione o in sovraccarico della capacità di rete, in conformità alle best practice del settore e agli indicatori contenuti nella Documentazione Correlata;
   - trasmettere virus, malware, o altro codice dannoso, violarne la sicurezza e/o effettuare interventi di hacking o reverse engineering.
9. L'Ente è tenuto ad avvisare PagoPA, entro e non oltre 24 (ventiquattro) ore dalla scoperta dell'evento, in caso di uso o accesso non autorizzato, e per proprio conto, al Servizio e alle relative funzioni, nonché in caso di qualsiasi violazione, malfunzionamento o incidente di sicurezza. PagoPA non potrà essere considerata responsabile per eventuali danni o disservizi derivanti da usi ed accessi non autorizzati effettuati dall'Ente.
10. Fermi restando gli altri rimedi a disposizione di PagoPA ai sensi dell'Accordo o della normativa applicabile, nel caso di violazioni gravi o sostanziali dell'Accordo, la Società si riserva il diritto di sospendere o limitare temporaneamente l'accesso dell'Ente al Servizio.
11. In nessuna circostanza PagoPA potrà essere considerata responsabile dall'Ente o dagli Utenti per atti e fatti di Terze Partie ad esse riconducibili.
12. PagoPA si impegna ad adottare il massimo livello di sicurezza per le infrastrutture hardware e di rete utilizzate per lo svolgimento del Servizio, e in particolare per la trasmissione delle informazioni e il trattamento dei dati personali, garantendo di avere adeguati presidi interni e adeguata organizzazione e competenze in ambito di sicurezza informatica e gestione del rischio.
13. PagoPA garantisce che il Servizio sarà erogato nel rispetto dei livelli di servizio previsti dall'Allegato C, a fronte del pagamento del corrispettivo dovuto ai sensi del presente Accordo.
14. L'Ente accetta e riconosce che PagoPA non fornisce alcuna assistenza agli Utenti con riferimento ai documenti sottoposti agli Utenti stessi per la sottoscrizione tramite Firma con IO nè al relativo contenuto. Qualunque informazione e/o assistenza che l'Utente dovesse richiedere con riferimento ai documenti da sottoscrivere (e al relativo contenuto) questa è di esclusiva responsabilità dell'Ente. PagoPA si riserva il diritto di re- indirizzare all'Ente ai recapiti di cui al successivo art. 11, co. 2 qualunque richiesta da parte di un Utente su un documento da sottoscrivere e/o sottoscritto.
15. L'Ente accetta e riconosce che Firma con IO e/o parte delle sue funzionalità sono o potrebbero essere in fase di sperimentazione/beta testing e dichiara di aver ricevuto

informazioni esaustive relative allo stato di detta fase di sperimentazione/beta testing. In tal caso aderendo a tale sperimentazione/beta testing, l'Ente accetta e riconosce che Firma con IO potrebbe presentare problematiche di funzionamento o indisponibilità, e/o potrebbero essere necessari ulteriori interventi, adempimenti o adeguamenti, inclusi i casi di cui all'art. 12.5 del presente Accordo. L'Ente si impegna, pertanto, ad informare gli Utenti delle predette circostanze, se del caso richiedendo la collaborazione di PagoPA.

16. In nessun caso PagoPA potrà rispondere ad alcun titolo dei danni causati direttamente o indirettamente a terzi attraverso l'utilizzo del Servizio da parte dell'Ente.
17. Fatte salve le ipotesi di dolo e colpa grave, l'Ente si impegna a manlevare e tenere indenne PagoPA da ogni perdita, contestazione, responsabilità, spese sostenute, nonché costi subiti - anche in termini di danno reputazionale - in relazione a eventuali contestazioni che dovesse ricevere da parte di Utenti o terzi danneggiati per qualsiasi causa e a qualsiasi titolo con riferimento alla fruizione del Servizio, inclusa, a titolo meramente esemplificativo e non esaustivo, ogni azione, domanda e/o istanza connessa e/o derivante da:
    a. un disconoscimento della firma da parte dell'Utente;
    b. problematiche di funzionamento o indisponibilitm del Servizio.

Art. 6 - Responsabilità

1. PagoPA si impegna a mantenere l'efficienza del servizio Firma con IO. Tuttavia, fermo restando il rispetto da parte di PagoPA degli obblighi assunti in tema di sicurezza e protezione dei dati in conformitm alla disciplina in materia, l'Ente accetta e riconosce che nel corso della durata dell'Accordo, anche al di fuori dei casi di sperimentazione/beta testing, potranno verificarsi malfunzionamenti, disservizi o interruzioni, anche conseguenti a interventi tecnici o di manutenzione correttiva e /o evolutiva, non preventivamente programmati, nonché modifiche alla Normativa Privacy (come definita nel DPA) in grado di generare nuovi requisiti e adempimenti. In tali casi PagoPA comunicherà la circostanza all'Ente e provvederm, non appena ragionevolmente praticabile alle azioni correttive, agli adempimenti necessari di sua competenza e al ripristino del Servizio.
2. Fatte salve le disposizioni inderogabili di legge, PagoPA non potrà essere ritenuta responsabile per danni diretti o indiretti provocati da malfunzionamenti, disservizi o interruzioni della infrastruttura di Firma con IO, dei Servizi né parte di essi e/o di una o più funzionalità, durante le fasi di sperimentazione/beta testing e/o i periodi di manutenzione e/o interruzione e, in ogni caso, salvo dolo o colpa grave, PagoPA sarà responsabile verso l' Ente, ai sensi delle norme di diritto comune, per un valore non superiore al corrispettivo pagato dall'Ente in esecuzione dell' Accordo.
3. Resta inteso tra le Parti che:
    i. in considerazione di quanto indicato all'art. 5, comma 6 che precede, il Prestatore di Servizi è il solo responsabile del rispetto di ogni normativa inerente l'attività di rilascio e conservazione dei certificati qualificati a norma di

legge, pertanto lo stesso è l'unico responsabile in caso di errori attinenti alla correttezza dei dati relativi a tali processi;

ii. grava su PagoPA l'obbligo di corretta esecuzione dell'attività di autenticazione e autorizzazione dell'Utente e di trasmissione dei relativi dati al Prestatore di Servizi, nonché delle ulteriori attività meglio dettagliate nell'Allegato Tecnico.

4. L'Ente è l'unico responsabile del documento sottoposto alla sottoscrizione dell'Utente, e ne garantisce la correttezza formale e sostanziale, nonché la conformità normativa e regolamentare (incluse le Linee Guida) e l'adempimento di qualsiasi obbligo connesso applicabile all'Ente, ivi inclusi gli obblighi informativi verso gli Utenti, il rispetto della Normativa Privacy (come definita nel DPA) e degli obblighi regolamentari imposti dalle autorità competenti, incluse le Linee Guida. L'Ente si impegna a manlevare e tenere indenne PagoPA da ogni perdita, contestazione, responsabilità, condanna o sanzione derivante o connessa al contenuto - formale e sostanziale - del documento sottoscritto dall'Utente, alla sua interpretazione e/o applicazione, nonché al mancato rispetto della normativa vigente.

Art. 7 - Pagamento del corrispettivo

1. Il corrispettivo che l'Ente deve corrispondere a PagoPA per il Servizio è basato su una tariffa a consumo (a scaglioni):
   - 0,50 Euro/firma oltre IVA da 1 a 25.000 firme;
   - 0,40 Euro/firma oltre IVA oltre 25.000 firme.

   Tali corrispettivi si applicano su base annuale, prendendo a riferimento il singolo anno solare a prescindere dalla data di sottoscrizione dell'Accordo.
2. I corrispettivi verranno fatturati da PagoPA all'Ente con cadenza trimestrale, sulla base dell'effettivo consumo.
3. Le fatture dovranno essere intestate come segue: Università degli Studi di Messina, Partita IVA. n. 00724160833 con la dicitura "Importi riconosciuti per l'erogazione del servizio Firma con IO" comprensivi dell'indicazione del periodo di riferimento - calcolati sulla base di quanto previsto al comma 1 del presente articolo - e dovranno essere inviate esclusivamente in formato xml, tramite il Sistema di interscambio, riportando nel campo Codice Destinatario il codice UFYJ26. L'Ente è soggetto al regime della scissione dei pagamenti di cui all'art. 17-ter del D.P.R. 633/1972, da indicare in fattura.
4. All'Ente spetterà l'onere di comunicare a PagoPA, ogni eventuale modifica dei dati di cui al comma che precede, utilizzando il seguente indirizzo mail: account@pagopa.it.
5. Il pagamento del corrispettivo sarà effettuato dall'Ente tramite bonifico bancario, oppure altra modalità indicata da PagoPA nella fattura di riferimento, ed alle coordinate bancarie ivi specificate, entro 30 (trenta) giorni dalla data di emissione della fattura da parte di PagoPA.
6. Le Parti convengono, ai sensi e per gli effetti dell'art. 1462 del codice civile, che l'Ente non potrà opporre eccezioni, al fine di evitare o ritardare il pagamento del corrispettivo di cui al precedente comma 4.
7. Il presente Accordo è soggetto ad imposta di registro ai sensi del D.P.R. n. 131/86 e ad imposta di bollo ai sensi del D.P.R. n. 642

/1972.

Art. 8 – Diritti di proprietà intellettuale e industriale

1. Tutti i diritti di proprietà intellettuale e industriale relativi al Servizio, restano nella esclusiva titolarità di PagoPA e/o dei danti causa della stessa, e nessuna loro parte può essere riprodotta in qualsiasi forma né con alcun mezzo, ad eccezione di quanto espressamente concesso ai sensi dell'Accordo. L'Ente accetta di non modificare, concedere in licenza, noleggiare, prestare, vendere, distribuire o creare opere derivate basate sul Servizio.
2. Ogni utilizzo da parte dell'Ente dei marchi, dei loghi, del nome commerciale e di qualsiasi altro segno distintivo relativo a PagoPA e/o al Servizio dovrà essere preventivamente richiesto dall'Ente a PagoPA e da quest'ultima espressamente autorizzato, in forma scritta.
3. L'Ente si obbliga a non realizzare progetti tali da costituire imitazione, anche parziale, dei marchi, dei loghi, del design, del nome commerciale e di qualsiasi altro segno distintivo relativo a PagoPA e/o al Servizio.
4. L'Ente accetta e riconosce che ai fini dell'erogazione del Servizio, PagoPA potrebbe utilizzare servizi, soluzioni e software pre-esistenti di titolarità di terzi (di seguito "**Terze Parti**") e messi nella disponibilità di PagoPA in forza di specifici accordi (di seguito "**Soluzioni di Terze Parti**"). A tal fine, PagoPA garantisce all'Ente di avere il diritto di utilizzare tali Soluzioni di Terze Parti per le finalità di cui all'Accordo e per tutta la durata dello stesso. L'Ente accetta e riconosce, altresì, che alle Soluzioni di Terze Parti potrebbero applicarsi termini e condizioni specifiche imposti da dette Terze Parti stesse, che potranno essere messi a disposizione dell'Ente, su richiesta di quest'ultimo anche tramite pubblicazione nelle pagine web esposte da PagoPA.

Art. 9 – Cancellazione dei dati dell'Ente, utilizzo di dati aggregati e pubblicità

1. In caso di cessazione per qualsiasi causa dell'Accordo, rispetto alla conservazione dei dati trattati in qualità di responsabile del trattamento per conto dell'Ente, si applicano le disposizioni contenute nell'Appendice 2 al DPA(di cui all'allegato A del presente Accordo). Tali dati saranno consultabili e scaricabili da parte dell'Ente unicamente entro i termini ivi indicati ed è onere e responsabilità esclusiva dell'Ente procedere al recupero di tali informazioni prima di tali termini, senza che PagoPA possa essere in alcun modo ritenuta responsabile per la mancata memorizzazione delle informazioni e dati di proprietà dell'Ente sui propri sistemi decorsi tali termini. In particolare, l'Ente accetta e riconosce che la cancellazione non avrà ad oggetto dati per i quali PagoPA ha autonomo titolo di trattamento o conservazione per il perseguimento dei propri interessi pubblici.
2. In caso di cessazione dell'Accordo, PagoPA e l'Ente concordano, prima della cancellazione dei dati, le modalità per portare a conoscenza degli Utenti, anche tramite l'invio di un messaggio concordato, da inviarsi prima della cessazione della fornitura

dei Servizi all'Ente, informazioni circa le conseguenze della cessazione dell'Accordo sui dati archiviati e le eventuali modalità per ottenerne una copia prima della cancellazione.

3. L'Ente autorizza PagoPA ad utilizzare il nome, i marchi, i loghi e gli altri segni distintivi dell'Ente per identificare l'Ente nell' ambito del Servizio e della sperimentazione, in documenti interni, sulla Piattaforma IO e su eventuali pagine web controllate da PagoPA:
    a. nelle comunicazioni provenienti dal Servizio ove riferite all'Ente;
    b. nella lista degli enti aderenti alla sperimentazione relativa al Servizio;
    c. in occasione degli eventi di comunicazione istituzionale relativi alla sperimentazione e al Servizio, comprese la documentazione prodotta a soggetti terzi ai fini di presentazione del Servizio e ad autorità competenti /vigilanti PagoPA per adempimenti normativi o finalità di reportistica;
    d. nelle comunicazioni ad uso interno, anche a fini di reportistica e gestione della sperimentazione.
4. Qualsiasi eventuale uso di nome, marchi, loghi e altri segni distintivi dell'Ente diverso da quelli sopra elencati al precedente comma 3, dovrà essere specificamente autorizzato per iscritto dall'Ente previa richiesta di PagoPA ai sensi e secondo le modalità di cui al successivo art. 11.

Art. 10 – D. Lgs. 231/2001, Modello organizzativo e codice etico

1. PagoPA si impegna a prendere visione del "Codice Etico e di comportamento interno" inviato dall'Ente unitamente al presente Accordo, o condiviso entro i 15 (quindici) giorni successivi alla sottoscrizione dello stesso. PagoPA si impegna per tutta la durata del rapporto contrattuale, ad attenersi a, e rispettare, quanto contenuto nel "Codice Etico e di comportamento interno". Si impegna, inoltre, a condividerlo ed assicurarne il rispetto anche da parte dei propri dipendenti e collaboratori che partecipino all'esecuzione del presente Accordo.
2. L'osservanza delle disposizioni di detti documenti è considerata parte essenziale, nell'interesse dell'Ente, anche ai sensi e per gli effetti dell'art. 1456 c.c., delle obbligazioni assunte da PagoPA con il presente Accordo. La violazione anche di uno solo degli obblighi indicati nei documenti sopracitati costituisce inadempimento, con ogni conseguenza di legge, anche in ordine alla facoltà di risoluzione del rapporto contrattuale, impregiudicato il diritto al risarcimento del danno.
3. L'Ente dichiara di aver preso e di prendere atto dei principi etici generali di onestà ed osservanza della legge, pluralismo, professionalità, imparzialità, correttezza, riservatezza, trasparenza, diligenza, lealtà e buona fede nonché del contenuto del Codice Etico, del Modello di Organizzazione, Gestione e Controllo (di seguito, congiuntamente, "**Modello**") e del Piano Triennale di Prevenzione della Corruzione e Trasparenza ("**PTPCT**") di PagoPA adottati ex D.Lgs. n. 231/2001 (di seguito "**Decreto**") ed ex L. n. 190/2012, avendone preso chiara, piena ed esatta visione nella sezione "Società Trasparente" del sito https://pagopa.

portaleamministrazionetrasparente.it/.

4. L'Ente dichiara e garantisce, inoltre, che quanto forma oggetto del presente Accordo sarà realizzato anche nel rispetto dei principi e delle previsioni previsti nel Modello e nel PTPCT e, per l'effetto, si impegna a far conoscere gli stessi, nonché tutta la normativa applicabile a chiunque, a qualsiasi titolo, prenderà parte alla realizzazione delle attività oggetto del presente Accordo.
5. In particolare, e senza limitare la generalità di quanto sopra, l' Ente garantisce che i suoi dipendenti e/o collaboratori e/o soci e /o amministratori e/o legali rappresentanti e/o chiunque partecipi, a qualsiasi titolo, alla realizzazione di quanto forma oggetto dell'Accordo e/o faccia parte della sua organizzazione non terrà comportamenti, omissivi e/o commissivi, che possano comportare la violazione, anche solo indiretta, dei principi, delle previsioni e delle norme del Modello, del PTPCT e/o di tutta la normativa applicabile e/o che risultino lesivi dell'immagine e, comunque, dei valori morali e materiali in cui PagoPA si riconosce e che applica nell'esercizio della propria attività, anche con riferimento ai rapporti con soggetti terzi.
6. L'effettivo rispetto delle dichiarazioni e garanzie ivi rilasciate, nonché la prevenzione, sotto ogni forma, delle criticità e dei rischi evidenziati dal Modello e dal PTPCT sono considerati parte essenziale, nell'interesse di PagoPA, anche ai sensi e per gli effetti dell'articolo 1456 c.c., delle obbligazioni assunte dall' Ente con il presente Accordo.
7. La violazione anche di una sola delle dichiarazioni e/o garanzie sopra previste costituisce grave inadempimento contrattuale con ogni conseguenza di legge, anche in ordine alla facoltà di PagoPA di risolvere il presente Accordo ai sensi e per gli effetti dell'art. 1456 c.c., salvo il risarcimento del danno ed ogni altro diritto e/o azioni previsti dalla legge e/o dal presente Accordo.
8. L'Ente dichiara di non essere a conoscenza di fatti rilevanti ai sensi del Decreto nel suo rapporto con PagoPA, in particolare nella fase delle trattative e della conclusione dell'Accordo e si impegna, per quanto di sua spettanza, a vigilare sull'esecuzione di esso in modo da scongiurare il rischio di commissione dei reati previsti dal succitato Decreto, nonché ad attivare, in tale ipotesi, tutte le azioni più opportune in conformità alla legge e ai propri strumenti di organizzazione interna.
9. Con specifico riferimento alla normativa anticorruzione, l'Ente dichiara e garantisce che quanto previsto nel presente Accordo costituisce esclusivamente il rimborso per la regolare esecuzione degli impegni assunti con il presente Accordo e che non porrà in essere atti omissivi e/o commissivi tra cui trasferimenti, diretti e/o indiretti, di somme, che possano comportare la violazione, anche solo indiretta, della normativa anticorruzione, ferme restando le garanzie e manleve rilasciate ai sensi del presente Accordo.
10. L'Ente assume le garanzie di cui sopra ai sensi dell'art. 1381 c.c., per ogni proprio dipendente, collaboratore, ausiliario nonché per chiunque, a qualsiasi titolo, prenderà parte alla realizzazione delle attività oggetto del presente Accordo.

Art. 11 - Comunicazioni e referenti dell'Accordo

1. Le Parti indicano quali referenti amministrativi ai fini dell' esecuzione del presente Accordo (di seguito "**Amministratore/i** ") i seguenti soggetti:
   - per l'Ente:

     Nome e Cognome: Giuseppe Mannino
     Codice Fiscale: MNNGPP65D01F158B
     Amm.ne/Ente/Società:
     Qualifica/Posizione:
     e-mail: mannino@unime.it
     PEC:

   - per PagoPA:

     Nome e Cognome: Giuseppe De Giorgi;
     Codice Fiscale: DGRGPP85H23E506X;
     Qualifica/Posizione: Product Management Lead;
     e-mail: giuseppe.degiorgi@pagopa.it
     PEC: pagopa@pec.governo.it;

Art. 12 - Trattamento dei dati personali

1. Con riferimento a quanto previsto dal Regolamento (UE) n. 2016 /679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché rispetto alla libera circolazione di tali dati (di seguito "**GDPR**"), l'Ente tratterà i dati personali cui avrà accesso ai fini dell'esecuzione del presente Accordo in qualità di titolare del trattamento, mentre PagoPA agirà per i trattamenti strettamente connessi all'esecuzione del presente Accordo in qualità di responsabile del trattamento, fatti salvi i casi in cui la Società agisce in qualità di titolare del trattamento ai sensi dell'art. 7.1 delle Linee Guida.
2. Con la sottoscrizione del DPA (allegato 1 al presente Accordo), PagoPA è nominata dall'Ente responsabile del trattamento dei dati, in conformità all'art. 28 del GDPR.
3. Le Parti si impegnano a trattare i dati nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione e integrità (Art. 5 GDPR), e comunque nel rispetto della Normativa Privacy (come definita nel DPA).
4. L'Ente si obbliga a manlevare e tenere indenne PagoPA da qualsiasi perdita, contestazione, responsabilità, condanna o sanzione, nonché altre spese sostenute o costi subiti - anche in termini di danno reputazionale - per effetto di un'azione, reclamo, procedura intrapresa dalla competente Autorità Garante per la protezione dei dati personali o da qualsiasi interessato qualora tale azione sia conseguenza anche di una sola violazione da parte dell'Ente, nonché eventualmente di suoi agenti e/o sub-contraenti, della Normativa Privacy (come definita nel DPA) e/o delle obbligazioni assunte ai fini dell' esecuzione del presente Accordo (ivi inclusi gli Allegati).
5. Durante l'esecuzione dell'Accordo, nell'eventualità di qualsivoglia modifica della Normativa Privacy (come definita nel DPA) che generi nuovi requisiti, le Parti si impegnano a sviluppare, adottare e implementare misure correttive di adeguamento ai nuovi requisiti.

Art. 13 - Riservatezza

1. Nel corso del presente Accordo, ciascuna Parte potrebbe avere accesso ad informazioni non pubbliche dell'altra Parte o di società del gruppo dell'altra Parte (in forma verbale, cartacea od elettronica) che siano relative ad attività passate, presenti o future riguardanti, a mero titolo esemplificativo: l'impresa, la ricerca, lo sviluppo, i prodotti, i servizi e le conoscenze tecniche (di seguito, "**Informazioni Riservate**").
2. Le Informazioni Riservate di una Parte (di seguito "**Parte Comunicante**") possono essere utilizzate dall'altra Parte (di seguito "**Parte Ricevente**") solo in relazione all'esecuzione del presente Accordo e potranno essere divulgate dalla Parte Ricevente esclusivamente ai propri dipendenti, società controllanti, società controllate, consulenti, fornitori e sub-fornitori che debbano conoscerle ai fini dell'esecuzione di quanto previsto nel presente Accordo. Ogni Parte riconosce che i menzionati soggetti sono obbligati al rispetto delle disposizioni contenute nel presente Accordo con riferimento alle Informazioni Riservate.
3. Ciascuna Parte s'impegna a proteggere la riservatezza delle Informazioni Riservate dell'altra Parte con la stessa cura con la quale protegge la riservatezza delle proprie Informazioni Riservate e comunque con il grado di diligenza che le compete.
4. Le Informazioni Riservate non potranno essere copiate o riprodotte senza il previo consenso scritto della Parte Comunicante. Le Informazioni Riservate messe a disposizione nel corso del presente Accordo, incluse eventuali loro copie, dovranno essere restituite alla Parte Comunicante o distrutte al verificarsi del primo tra i seguenti eventi:
    a. la cessazione, per qualsiasi causa, del presente Accordo;
    b. su richiesta della Parte Comunicante, a meno che la Parte Ricevente non sia autorizzata a trattenere tali Informazioni Riservate ad altro titolo.
5. In caso di inosservanza degli obblighi di riservatezza, ciascuna Parte, previa comunicazione inviata all'altra Parte mediante PEC della volontà di avvalersi della clausola risolutiva espressa, ha facoltà di dichiarare risolto di diritto il presente Accordo ai sensi dell'art. 1456 c.c., nonché di esigere il risarcimento di tutti i danni che dovessero derivarne.
6. Non grava sulla Parte Ricevente l'obbligo di mantenere riservate o comunque tenere confidenziali le Informazioni Riservate se:
    a. al momento in cui le Informazioni Riservate sono state per la prima volta divulgate dalla Parte Comunicante alla Parte Ricevente, la Parte Ricevente si trovava gim in possesso, lecitamente, delle Informazioni Riservate; o
    b. le Informazioni Riservate divengono pubbliche per causa diversa dalla negligenza o dalla violazione delle obbligazioni gravanti sulla Parte Ricevente contenute nel presente Accordo; o
    c. la divulgazione delle Informazioni Riservate è richiesta dalla legge o da un provvedimento di un'Autorità e, in detta eventualità, deve essere comunicata soltanto quella parte delle Informazioni Riservate la cui

divulgazione viene ordinata, usando le migliori cautele per ottenere un trattamento confidenziale per qualsiasi Informazione Riservata comunicata. Resta fermo che, in tale eventualità, la Parte Ricevente informerà immediatamente la Parte Comunicante dell'esistenza di tale obbligo.

7. Gli obblighi di riservatezza di cui al presente articolo si applicheranno per tutta la durata dell'Accordo e per i 5 (cinque) anni successivi alla scadenza di tutte le obbligazioni contrattuali connesse alla stipula del presente Accordo o alla eventuale risoluzione/recesso anticipato dello stesso.

Art. 14 - Risoluzione

1. Fermo restando le ipotesi di risoluzione previste da altre disposizioni del presente Accordo e dalla legge applicabile, ciascuna delle Parti si riserva la facoltà di risolvere il presente Accordo in presenza di violazione, a opera dell'altra Parte di uno o più obblighi nascenti dall'Accordo decorso inutilmente il termine di 15 (quindici) giorni lavorativi dal ricevimento dell' intimazione scritta ad adempiere di cui all'art. 1454 del codice civile.
2. Le Parti potranno risolvere il presente Accordo, ai sensi dell' articolo 1456 del codice civile, con effetto immediato con comunicazione scritta, ed in ogni caso fatto salvo l'eventuale risarcimento dei danni subiti e subendi, in caso di violazione degli artt. 5 - Modalità di esecuzione dei Servizi e obblighi delle Parti, 7 - Pagamento del Corrispettivo e 13 - Riservatezza.
3. Le Parti potranno risolvere l'Accordo ai sensi e per gli effetti dell' art. 1456 del codice civile, con effetto immediato, in caso di mutamenti dovuti a leggi, regolamenti, atti amministrativi, relativi alla normativa vigente applicabile al Servizio che rendano impossibile o difficoltosa la prosecuzione del rapporto.

Art. 15 – Legge applicabile e foro competente

1. Le norme applicabili al presente Accordo sono quelle previste nell'ordinamento italiano.
2. Ogni eventuale contestazione e/o controversia che dovesse insorgere fra le Parti in relazione all'interpretazione, alla validità e/o all'esecuzione del presente Accordo, che non venisse risolta bonariamente fra le Parti, sarà deferita in via esclusiva al Foro di Roma.

Art. 16 - Disposizioni finali

1. L'esecuzione del presente Accordo è regolata dalle disposizioni contenute nel presente Accordo, negli Allegati e nella Documentazione Correlata, che congiuntamente costituiscono la manifestazione unica e integrale di tutti gli accordi intervenuti tra l'Ente e PagoPA e sostituisce tutte le precedenti comunicazioni e gli accordi tra le Parti in merito ad esso. Il presente Accordo può essere oggetto di modifica o di rinuncia solo con il mutuo consenso scritto delle Parti.
2. Qualora uno o più articoli del presente Accordo dovessero essere ritenuti nulli, inefficaci o contrari a norme imperative, la

nullità, l'inefficacia o la contrarietà a norme imperative non si applicheranno agli altri articoli dell'Accordo stesso, che manterrà, a tutti gli effetti, la sua validità ed efficacia.

3. In caso di mancata o non puntuale applicazione di una qualsiasi delle previsioni del presente Accordo, la tolleranza dell' altra Parte non comporterà la rinuncia definitiva da parte della stessa alle facoltà o diritti connessi a tale disposizione o a farla valere o invocarne l'applicazione in futuro.

L'Ente Universita' degli Studi di Messina	PagoPA S.p.A. Il legale rappresentante pro tempore

A norma degli artt. 1341 e 1342 c.c., l'Ente, previa lettura delle norme contenute nel presente Accordo, con particolare riguardo agli articoli 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14 e 15 dichiara di approvarli, reietta fin d'ora ogni reciproca eccezione.

L'Ente Universita' degli Studi di Messina

Allegato A
Trattamento di dati personali e nomina a responsabile del trattamento di PagoPA ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 ("GDPR") ("DPA")

1. Ai fini del presente DPA:
   - per "**Dati Personali**", si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile del cui trattamento l'Ente è titolare del trattamento (o responsabile del trattamento qualora agisca per conto di altro Ente), e che risultano oggetto di trattamento da parte della Società in qualità di responsabile (o sub-responsabile) ai fini di dare esecuzione all'Accordo, ivi inclusi eventuali categorie particolari di dati personali. In particolare, i dati oggetto di trattamento sono i dati personali di volta in volta contenuti nel Servizio (vale a dire, ogni informazione che riguarda il destinatario del Servizio o ogni altra persona fisica identificata o identificabile tramite il contenuto del Servizio stesso), le preferenze espresse dagli Utenti con riguardo al Servizio, ivi incluse le modalità di ricezione dei Messaggi, nonché i dati personali trattati per le finalità connesse all'attuazione dell'Accordo;
   - Per "**Interessati**", si intendono gli Utenti e ogni altra persona fisica identificata o identificabile dei cui dati l' Ente è titolare del trattamento e che risultano oggetto di trattamento da parte della Società in qualità di responsabile (o sub-responsabile) per l'esecuzione all'

Accordo;

- Per "**Regolamento Privacy**", si intende il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- Per "**Codice Privacy**", si intende il Decreto Legislativo n. 196 del 30 giugno 2003 e successive modifiche e integrazioni;
- Per "**Normativa Privacy**", si intende il Regolamento Privacy, il Codice Privacy e ogni altro provvedimento emanato da un'autorità competente in attuazione degli stessi, ivi inclusi i provvedimenti del Garante per la protezione dei dati personali, le raccomandazioni e linee guida dell'EDPB/WP29;
- Per "**Documentazione Privacy e Sicurezza**", si intende quella Documentazione Correlata (come definita nell' Accordo) di volta in volta predisposta dalla Società, che descrive tutti gli adempimenti, le misure tecniche o organizzative e le misure di sicurezza adottate dalla Società, nonché la documentazione predisposta ai sensi della Normativa Privacy, ivi incluse le politiche di conservazione dei dati e di gestione delle richieste degli interessati;
- Per "**Linee Guida**", si intendono le Linee Guida per il punto di accesso telematico ai servizi della Pubblica Amministrazione, emanate da AgID il 3 novembre 2021;
- Per "**Società**", si intende PagoPA S.p.A., con sede legale in Roma, Piazza Colonna n. 370, c.f., P.I. e iscrizione al Registro delle Imprese di Roma n. 15376371009, in persona del suo legale rappresentante pro tempore, così come definita nell'Accordo.

2. Ogni altro termine usato in maiuscolo e non definito nel presente DPA avrà il significato attribuito nell'Accordo e nella Normativa Privacy. In caso di contrasto tra il presente DPA e l' Accordo e/o la Normativa Privacy, questi ultimi avranno prevalenza.
3. Fatti salvi i casi in cui la Società agisce in qualità di titolare del trattamento ai sensi dell'art. 7.1 delle Linee Guida, i Dati Personali sono di esclusiva titolarità dell'Ente e la Società si impegna a non farne alcun uso diverso da quelli previsti per l' adempimento dell'Accordo.
4. Fuori dei casi in cui la Società agisce in qualità di titolare del trattamento ai sensi dell'art. 7.1 delle Linee Guida, la Società agisce in qualità di responsabile o sub-responsabile dell'Ente ai sensi del presente DPA. Le categorie di Dati Personali oggetto di trattamento, come anche le finalità, la base giuridica, le categorie di interessati, tra gli Utenti, sono determinate, in via esclusiva, dall'Ente in quanto titolare del trattamento e unico soggetto responsabile dell'utilizzo della Piattaforma IO per l' offerta del Servizio. Qualora per la fornitura del Servizio, sia necessario il trattamento di particolari categorie di dati, sulla

base della valutazione dell'Ente stesso, quest'ultimo deve preventivamente informare la Società e conformarsi agli obblighi di cui alle Linee Guida (in particolare, art. 7.3).

5. Prima della conclusione dell'Accordo e su espressa richiesta dell' Ente, la Società si impegna a mettere a disposizione dell'Ente stesso la Documentazione Privacy e Sicurezza necessaria per le opportune valutazioni da parte dell'Ente stesso, ad esclusione delle eventuali parti confidenziali. Resta in ogni caso salva la facoltà, per l'Ente e la Società, di concordare misure aggiuntive, ove necessario, ai sensi delle Linee Guida (in particolare, art. 7.2).
6. L'Ente ha ritenuto la Società soggetto idoneo al trattamento e, per l'effetto, nomina la stessa responsabile del trattamento dei Dati Personali ai sensi dell'art. 28 del Regolamento Privacy, salvi i casi già menzionati in cui la Società agisce in qualità di titolare del trattamento.
7. Resta inteso che, nel caso in cui l'Ente agisca a sua volta come responsabile del trattamento, l'Ente dichiara e garantisce di aver concluso un valido accordo ai sensi dell'art. 28 del Regolamento Privacy, e in tal caso il presente DPA deve intendersi quale nomina a sub-responsabile del trattamento ai sensi dell'art. 28, comma 4, del Regolamento Privacy. L'Ente si impegna, nella misura massima consentita dalla legge, a manlevare e tenere indenne la Società da ogni danno diretto e indiretto e da tutte le spese, i costi nonché pretese e contestazioni da parte di terzi (incluse eventuali sanzioni del Garante per la protezione dei dati personali e spese legali) in caso di assenza di tale accordo o di non conformità dello stesso ai requisiti previsti per legge. Inoltre, l'Ente garantisce di essere espressamente autorizzato a nominare a propria volta la Società come responsabile del trattamento.
8. La Società dichiara di conoscere gli obblighi assunti con il presente DPA ai sensi dell'art. 28 del Regolamento Privacy e garantisce di possedere capacità, esperienza e competenze, anche tecniche, per ricoprire tale ruolo.
9. La Società e l'Ente adempiranno agli obblighi assunti con la predetta nomina nel rispetto della Normativa Privacy e delle Linee Guida.
10. In particolare, la Società si impegna a trattare i Dati Personali nel rispetto delle seguenti istruzioni e previsioni:
    a. non cederli o metterli a disposizione di terzi, in modo parziale o totale, temporaneo o definitivo, salvo specifica istruzione scritta dell'Ente in ossequio a legittima base giuridica;
    b. non farne uso ultroneo rispetto alle finalità indicate nelle Linee Guida, presente DPA e a quelle connesse all' attuazione dell'Accordo, salvo l'uso in forma aggregata;
    c. trattarli in modo adeguato, pertinente e nel rispetto del principio della minimizzazione dei dati, nonché in modo lecito, corretto e trasparente, secondo quanto previsto dalla Normativa Privacy;
    d. garantirne la riservatezza, l'integrità e la disponibilità, compreso ogni profilo relativo alla sicurezza così come

disciplinato dall'art. 32 del Regolamento Privacy, secondo quanto descritto nella Documentazione Privacy e Sicurezza e in ossequio alla Normativa Privacy e alle Linee Guida;

e. garantire un'adeguata tutela dei diritti dell'interessato, supportando l'Ente al fine di adempiere al proprio obbligo di dare seguito alle richieste degli interessati per l'esercizio dei propri diritti, anche qualora tali richieste siano ricevute dalla Società, (i) comunicando all'interessato di indirizzare la propria richiesta all'Ente; (ii) trasmettendo all'Ente la richiesta e/o (iii) mettendo a disposizione all'interno della Piattaforma IO strumenti a disposizione degli Interessati per la gestione dei propri diritti, come descritto nella Documentazione Sicurezza e Privacy.
f. avvalersi della propria struttura organizzativa, identificando e designando le persone autorizzate ad effettuare operazioni di trattamento dei Dati Personali, individuando contestualmente l'ambito autorizzativo, fornendo le dovute istruzioni sulle modalità di trattamento e provvedendo alla relativa formazione;
g. garantire che le persone autorizzate siano state preventivamente informate della natura confidenziale dei Dati Personali e, conseguentemente, siano soggetti a specifici obblighi di confidenzialità;
h. gestire tutti gli obblighi connessi alla nomina ad amministratore di sistema del proprio personale preposto alla gestione e alla manutenzione della Piattaforma IO;
i. garantire un livello di sicurezza adeguato al rischio, adottando misure di sicurezza tecniche e organizzative adeguate in linea con le disposizioni previste dalla Regolamento Privacy;
j. ove necessario, cooperare con l'autorità di controllo e mettere a disposizione di questa la documentazione eventualmente richiesta in occasione di controlli e/o accessi dell'autorità medesima, provvedendo altresì ad informare l'Ente;
k. istituire e mantenere il registro delle attività di trattamento ai sensi dell'art. 30 del Regolamento Privacy e renderlo disponibile all'Ente su sua richiesta;
l. mettere a disposizione dell'Ente il nominativo e le informazioni di contatto del proprio responsabile della protezione dei dati designato ai sensi degli artt. 37 e ss. del Regolamento Privacy;
m. per gli aspetti di propria competenza, fornire supporto tecnico all'Ente rispetto agli obblighi inerenti alla: (i) sicurezza del trattamento, (ii) notifica di una violazione dei dati personali all'autorità di controllo ai sensi dell'art. 33 del Regolamento Privacy, (iii) comunicazione di una violazione dei dati personali all'interessato ai sensi dell' art. 34 del Regolamento Privacy, (iv) valutazione d' impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento Privacy, (v) consultazione preventiva ai sensi dell'art. 36 del Regolamento Privacy;

n. in caso di violazione accidentale o illecita dei sistemi della Piattaforma IO che comporti la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l' accesso ai Dati Personali trasmessi, conservati o comunque trattati, procedere a: (i) informare l'Ente, senza ingiustificato ritardo a mezzo PEC inviata ai recapiti forniti dall'Ente stesso; (ii) fornire all'Ente le opportune informazioni circa la natura della violazione, le categorie ed il numero approssimativo di dati e di interessati coinvolti, nonché le probabili conseguenze della violazione e le misure adottate o di cui si propone l' adozione per porre rimedio alla violazione o attenuare gli effetti pregiudizievoli; (iii) qualora non sia possibile fornire le suddette informazioni specifiche nel termine previsto, indicare all'Ente i motivi del ritardo, fornendo comunque delle informazioni iniziali riferite alla violazione riscontrata ed utili all'Ente ai fini della relativa notifica;
o. fornire all'Ente, anche nel corso dell'esecuzione dell' Accordo, le informazioni relative alle misure tecniche, organizzative e di sicurezza adottate necessarie per il pieno rispetto della Normativa Privacy per il tramite della Documentazione Privacy e Sicurezza, ad esclusione delle eventuali parti confidenziali;
p. rendersi disponibile con riguardo alle attività ispettive e di audit che l'Ente vorrà effettuare, direttamente o per il tramite di un altro soggetto da questo incaricato, fermo restando che (i) tali attività non potranno essere effettuate dall'Ente con una frequenza superiore a 1 (una) volta all'anno e, in ogni caso, prima che siano decorsi 12 (dodici) mesi dall'ultima attività di audit svolta o commissionata dall'Ente (ii) tali attività dovranno essere concordate con la Società con un preavviso di almeno 10 (dieci) giorni lavorativi; (iii) tali attività dovranno essere svolte salvaguardando la normale operatività della Società; (iv) l'uso delle informazioni di cui l'Ente e l' eventuale soggetto incaricato dall'Ente dovessero venire a conoscenza nel corso dell'audit dovrà essere preventivamente regolamentato da un apposito accordo di confidenzialità; (v) tali attività non vengano svolte durante i periodi di beta testing e/o sulle componenti, applicativi, perimetri soggetti a beta testing; e (vi) qualora tali attività comportino un costo non ragionevole per la Società, le parti si accordino per un equo compenso che l'Ente corrisponda alla Società per lo svolgimento di tali attività. Per costi non ragionevoli per la Società si intendono, spese emergenti e lucro cessante che possano derivare da prolungate interferenze nella normale operatività della Società ovvero da richieste tecniche e organizzative che si rendano necessarie ai soli fini dello svolgimento dell'audit. La Società ad ogni modo condividerà su richiesta dell'Ente le risultanze degli audit e processi di certificazione cui si sottopone e l'Ente potrà richiedere di partecipare a tali attività di audit programmate dalla Società. In ogni caso, in deroga a

quanto previsto sopra nei punti (i) (ii) e (v), qualora sussistano circostanze eccezionali o di particolari problematiche dell'Ente (a titolo esemplificativo, violazioni di dati personali, ispezioni o richieste da parte del Garante per la Protezione dei dati personali), la Società si renderà pienamente disponibile ad attività ispettive e audit effettuate dall'Ente, direttamente o per il tramite di un altro soggetto da questo incaricato;

q. qualora dovesse riscontrare che un'istruzione impartita dall'Ente violi la Normativa Privacy, ad informare prontamente l'Ente stesso;
r. garantire che i Dati Personali siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, mediante l'adozione di idonee e preventive misure di sicurezza;
s. adottare misure atte a prevenire accessi fisici non autorizzati, danni e interferenze ai Dati Personali trattati nello svolgimento del proprio incarico, nonché un' adeguata e sicura operatività delle strutture di elaborazione dei dati, attraverso l'adozione di misure di sicurezza fisica e ambientale oltre ad idonei strumenti di protezione contro i malware e contro la perdita dei dati;
t. adottare procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

11. Con il presente DPA, l'Ente conferisce alla Società un' autorizzazione generale ad avvalersi di sub-responsabili nominati per iscritto, a condizione che la Società imponga agli stessi, mediante un contratto o altro atto giuridico, i medesimi obblighi in materia di protezione dei dati contenuti nel presente DPA, prevedendo, in particolare, garanzie adeguate in tema di misure tecniche e organizzative, per soddisfare i requisiti richiesti dalla Normativa Privacy, restando tuttavia la Società interamente responsabile verso l'Ente dell' adempimento degli obblighi dei sub-responsabili individuati ai sensi del presente articolo. La Società è autorizzata e si impegna, inoltre, a impiegare gli strumenti di trasferimento adeguati, compresa la conclusione di clausole contrattuali tipo ("Standard Contractual Clauses" o "SCC"), nonché ad ottemperare agli obblighi di notifica, informazione e comunicazione nei confronti dei titolari previsti dalla Normativa Privacy.
12. L'elenco dei sub-responsabili essenziali all'operatività della Piattaforma IO, con indicazione delle relative garanzie, è disponibile all'indirizzo io.italia.it/app-content/fornitori. Senza pregiudizio degli obblighi di riservatezza in capo alla Società, quest'ultima fornisce, su richiesta dell'Ente, gli approfondimenti necessari rispetto ai sub-responsabili a qualsiasi titolo coinvolti nei trattamenti rilevanti per l'Accordo e si impegna a informare

l'Ente di eventuali modifiche riguardanti l'aggiunta o la sostituzione dei sub-responsabili, dando così all'Ente l' opportunità di opporsi a tali modifiche.

13. La Società si impegna altresì a non eseguire alcun trasferimento di Dati Personali fuori dallo SEE e verso Paesi che non garantiscono un livello adeguato di tutela in assenza di garanzie adeguate e di effettuare tali trasferimenti unicamente nel pieno rispetto della Normativa Privacy e previa indicazione nella Documentazione Privacy e Sicurezza dello strumento utilizzato per garantire un livello adeguato di tutela. In relazione all'eventuale trasferimento di Dati Personali effettuato dalla Società, la Società stessa effettua ed aggiorna regolarmente la valutazione di impatto sui trasferimenti dei dati personali (Transfer Impact Assessment - "TIA"). Tale TIA è messa a disposizione dell'Ente su richiesta, con riserva delle informazioni confidenziali.
14. La Società conserverà i Dati Personali in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità di cui all'Accordo, e comunque nel rispetto del principio di limitazione della conservazione, ferma restando l'osservanza della normativa vigente per i documenti fiscali, contabili e legali. In particolare, la Società, al fine di garantire che il trattamento sia svolto nel rispetto del principio di limitazione della conservazione dei dati, provvederà a cancellare i Dati Personali allo scadere dei termini di conservazione indicati nell' informativa della Piattaforma IO, sempre disponibile in app e all' indirizzo io.italia.it/app-content/tos_privacy.html, e nella DPIA predisposta dalla Società. In caso di cessazione per qualsiasi causa dell'Accordo, rispetto alla conservazione dei dati trattati in qualità di responsabile del trattamento per conto dell'Ente con specifico riferimento al Servizio, si applicano le disposizioni contenute nell'Appendice 2 del presente DPA. Tali dati saranno consultabili e scaricabili da parte dell'Ente unicamente entro il termine sopra indicato ed è onere e responsabilità esclusiva dell' Ente procedere al recupero di tali informazioni prima di tali termini, senza che la Società possa essere in alcun modo ritenuta responsabile per la mancata memorizzazione delle informazioni e dati di proprietà dell'Ente sui propri sistemi decorso tale termine.
15. Il presente DPA potrà, ove necessario, costituire oggetto di accordi accessori e supplementari in forma scritta attraverso cui le Parti potranno stabilire misure di sicurezza e organizzative aggiuntive qualora esse, secondo la valutazione delle Parti, risultino più idonee ad assicurare la tutela dei principi *di privacy by design e by default* avendo riguardo alle caratteristiche del Servizio.
16. Il presente DPA ha durata pari alla durata dell'Accordo e si intenderà caducato in caso di cessazione per qualsiasi motivo dell'Accordo stesso, senza pregiudizio di quanto disposto al precedente art. 14 e salvo diverso accordo delle Parti.

APPENDICE 1

La presente appendice costituisce parte integrante delle clausole contrattuali e contiene i dettagli relativi al trattamento dei dati personali oggetto del DPA

Titolare del Trattamento

L'Ente, come identificato nell'Accordo.

Responsabile del Trattamento

PagoPA S.p.A., con sede legale in Roma, Piazza Colonna n. 370, c.f., P.I. e iscrizione al Registro delle Imprese di Roma n. 15376371009.

Interessati

I dati personali trattati interessano le seguenti categorie di persone: Utenti del Servizio

Categorie di dati oggetto di trattamento

I dati trattati interessano, a titolo esemplificativo, le seguenti categorie di dati:

- dati comuni (compresi dati anagrafici, es. nome, cognome, codice fiscale, dati di contatto, dati bancari/finanziari, dati relativi alla firma);
- eventuali altri dati, anche appartenenti a categorie particolari, eventualmente presenti nei documenti sottoposti a firma e determinati esclusivamente dall'Ente, oppure volontariamente comunicati dagli Utenti (ad esempio, nelle richieste di assistenza), e in ogni caso necessari per l'erogazione o la fruizione del Servizio.

Trattamento

I dati personali trasferiti saranno sottoposti alle seguenti attività principali di trattamento:

Tramite il Servizio Firma con IO, la Società consente agli Enti di inviare tramite messaggio su Piattaforma IO o call to action sul proprio sito web dell'Ente, documenti per i quali è richiesta l' apposizione della firma da parte degli Utenti, permettendo agli stessi, tramite la Piattaforma IO, di apporre una firma elettronica qualificata, con una modalità semplice e interamentedigitalizzata.

Durata del trattamento e Conservazione dei Dati Personali

Il trattamento avrà durata pari alla durata dell'Accordo. Si applicano i termini di conservazione indicati nell'informativa della Piattaforma IO, sempre disponibile in app e all'indirizzo io.italia.it /app-content/tos_privacy.html, e nella DPIA predisposta dalla Società, nonchè le regole dettate nell'Appendice 3.

APPENDICE 2

MISURE TECNICHE E ORGANIZZATIVE DI SICUREZZA

In PagoPA consideriamo una priorità assoluta la sicurezza dei nostri progetti e delle informazioni che trattiamo, in particolare i dati dei cittadini.

L'approccio che adottiamo per garantire livelli di sicurezza e protezione sempre crescenti si fonda sull'adozione di best practices riconosciute e certificabili. PagoPA, infatti, ha definito il proprio Sistema di Gestione della Sicurezza delle Informazioni (di seguito anche "SGSI") basandosi sul framework internazionale della ISO/IEC 27001, ottenendo alla fine del 2020 la certificazione dello stesso.

Il nostro SGSI implementa prassi e regole di sicurezza come di seguito sintetizzato.

POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

Nell'ambito della governance del proprio Sistema di Gestione della Sicurezza delle Informazioni PagoPA ha definito una Information Security Policy, diffusa a tutto il personale, al fine di proteggere dalle minacce le informazioni che costituiscono il patrimonio informativo di PagoPA, nonché i dati dei cittadini che sono gestiti nel ciclo di vita dei prodotti e servizi forniti.

Lo scopo della Information Security Policy è quello di definire:

- gli obiettivi generali di sicurezza, in linea con le strategie di business;
- i principi di azione per un'adeguata sicurezza.

In linea con la Information Security Policy, PagoPA si è dotata di norme e procedure mirate a mantenere nel tempo un costante ed elevato livello di sicurezza del proprio sistema informativo.

ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

La gestione della sicurezza delle informazioni comprende i processi e le misure volti a:

- preservare la sicurezza delle informazioni e dei beni aziendali;
- garantire che le risorse aziendali siano protette in termini di riservatezza, integrità e disponibilità in maniera appropriata e coerente lungo il loro intero ciclo di vita.

L'organizzazione della sicurezza di PagoPA prevede la figura di responsabile della sicurezza delle informazioni (o "CISO") che, in coordinamento con la Direzione Aziendale, definisce la strategia della sicurezza, la cui attuazione è assegnata ai manager di area.

Il CISO è supportato da un team con competenze relative a:

- Architecture & Product Security;
- Security Governance;
- Security Operations.

In ottemperanza agli obblighi normativi relativi al trattamento dei dati personali , inoltre, PagoPA si è avvalsa altresì della figura del Data Protection Officer (o "DPO").

SICUREZZA DELLE RISORSE UMANE

Al fine di assicurare che il personale e i collaboratori comprendano le proprie responsabilità e seguano i principi di sicurezza richiesti per i ruoli assegnati, è prevista la definizione e condivisione di policy, procedure istruzioni e linee guida, organizzative e tecniche, per diffondere la cultura e la consapevolezza sulle tematiche di Information security e compliance.

GESTIONE DEGLI ASSET

Nell'ambito dell'identificazione degli asset dell'organizzazione e della definizione di adeguate responsabilità per la loro protezione, ricadono non solo gli elementi fisici, ma anche i dati e le informazioni che fanno anch'essi parte a pieno titolo del patrimonio aziendale.

Tutte le categorie di asset sono inventariate, identificabili e aggiornate nel tempo. Il responsabile di ciascun asset assicura che lo stesso sia inventariato, appropriatamente classificato e protetto, definisce e riesamina periodicamente i privilegi di accesso e la classificazione, in particolare per gli asset più critici e, coerentemente con le linee guida stabilite per regolare le modalità di gestione e uso sicuro degli asset, assicura un corretto trattamento, la dismissione, la segnalazione e gestione nel caso di compromissione degli stessi.

CONTROLLO DEGLI ACCESSI

All'interno delle linee guida di security sono delineati i requisiti per la gestione e controllo degli accessi, secondo i principi di:

- necessità (need to know/need to do);
- limitazione dei privilegi (least privilege);
- separazione dei ruoli (SoD, Segregation of Duties).

Le linee guida di sicurezza prevedono che siano definiti e verificati (almeno una volta l'anno da parte del referente dei singoli sistemi) i ruoli sui sistemi, i privilegi associati ai ruoli e le regole per l' assegnazione dei ruoli ai singoli utenti (cosa è autorizzato di default e quali sono / come si gestiscono eventuali eccezioni) in maniera tale che sia sempre possibile risalire a "chi può fare cosa, dove". I singoli team hanno la responsabilità di applicare, in funzione dei rischi connessi, le regole di utilizzo e i sotto-processi per l'attribuzione, revisione e revoca dei diritti di accesso ai sistemi e alle applicazioni, nel rispetto dei suddetti principi.

L'accesso a sistemi e applicazioni avviene tramite credenziali che consentano di identificare e autenticare in maniera univoca gli specifici utenti.

Per tutti i sistemi critici è implementata l'autenticazione a 2 fattori.

CRITTOGRAFIA

Sono implementate misure per la protezione dei dati:

- 'in transito' (cifratura del canale, nel momento in cui si stabilisce la connessione, o del dato);
- 'a riposo' (cifratura di tutte le componenti per la conservazione / archiviazione dei dati).

L'approccio adottato tiene in considerazione la criticità dei dati, le minacce a cui sono esposti, gli obblighi normativi, la presenza di elementi a mitigazione dei rischi e gli impatti su performances e disponibilità dei servizi.

I servizi web Internet, al fine di garantire la riservatezza delle informazioni scambiate e permettere la verifica dell'attendibilità del sito (ad esempio in caso di phishing), sono esposti utilizzando un certificato SSL rilasciato da una Autorità di certificazione ufficialmente riconosciuta.

Anche la sicurezza dei sistemi di posta elettronica è garantita tramite l'uso di protocolli per tutelare l'azienda da utilizzo improprio (limitando tentativi di impersonificazione/spoofing del dominio, spam, phishing) e garantendo il corretto recapito dei messaggi.

SICUREZZA FISICA E AMBIENTALE

Sono definite:

- istruzioni per il personale sulle misure fisiche presenti e su comportamenti/pratiche da adottare per non diminuirne l'efficacia;
- regole e vincoli per l'utilizzo di attrezzature all'interno e all'esterno delle aree di lavoro, indicazione delle misure previste a protezione delle informazioni contenute e trattate tramite le stesse, dei comportamenti da adottare in pubblico, dei canali di comunicazione da utilizzare e delle pratiche da seguire in caso di furto o sospetta compromissione dell'apparecchiatura.

In linea con la Information Security Policy e con le relative linee guida di sicurezza è previsto che:

- ai dipendenti sia assegnato un badge con livelli di autorizzazione sufficienti a garantire accesso alle aree previste per il ruolo assegnato;
- l'accesso alle aree più critiche sia limitato e controllato;
- il personale esterno a cui sia concesso l'accesso venga registrato all'entrata e all'uscita, accompagnato da personale dipendente durante la permanenza nei locali, istruito sulle regole di sicurezza presenti e sulle sanzioni in caso di mancato rispetto delle stesse.

Altre misure per la protezione fisica e ambientale prevedono:

- sistemi di allarme antintrusione;
- prevenzione incendi;
- videosorveglianza.

SICUREZZA DELLE ATTIVITÀ OPERATIVE

Sono definite e implementate linee guida e misure di sicurezza a supporto delle attività e dei processi operativi (corretto e sicuro funzionamento dei sistemi, gestione dei dati; mitigazione dei rischi legati ad errori umani, furto, frode o uso improprio di dati e sistemi). Tra le misure di protezione e mitigazione, inoltre, vi sono:

- log management: registrazione degli eventi di sicurezza, delle attività degli utenti in file di log che consentano di risalire ad attività anomale, root cause di eventuali problemi, ecc.;
- separazione degli ambienti: gli ambienti di sviluppo e collaudo sono logicamente separati da quello di produzione;
- controlli di rete: monitoraggio delle intrusioni e verifica degli eventi registrati dai sistemi di sicurezza a protezione della rete;
- patch management: acquisizione, test e installazione di modifiche al codice (patches) per mantenere a livelli congrui la resilienza del sistema informatico, in particolar modo riguardo alla sicurezza;
- backup e restore: definite, testate e adottate procedure per il salvataggio dei dati e delle configurazioni e per il relativo ripristino in caso di necessità;
- penetration test e vulnerability assessment: attività effettuata almeno annualmente tramite società esterne su infrastruttura e sw;
- monitoraggio sistemi: controllo su disponibilità, raggiungibilità, health check di sistemi e applicazioni prevedendo gli opportuni processi di escalation a fronte di anomalie per garantire interventi rapidi e qualità del servizio;
- capacity planning: garantito tramite opportune valutazioni che derivano dalla costante analisi (monitoraggio di capacità, volumi, utilizzo, performance, ecc; rilevazione di eventuali failure, colli di bottiglia e altre possibili anomalie) delle risorse impiegate (rete, sistemi, ecc.) rispetto ai vari obiettivi, inclusi quelli per la sicurezza;
- antivirus: ogni personal computer assegnato ai dipendenti è dotato di un software antivirus, attivo, costantemente aggiornato e monitorabile centralmente, a protezione della navigazione internet e della posta elettronica.

SICUREZZA DELLE COMUNICAZIONI

Le reti di trasmissione dati sono configurate prevedendo opportuna separazione in base ai servizi offerti. L'accesso ai

sistemi all'interno della rete richiede un account di rete unico e univocamente associato all'utente. Non è consentito l'accesso anonimo alla rete.

Sono previste misure tecnico/organizzative volte a impedire l' interconnessione di reti esterne non autorizzate alla rete aziendale e controlli per impedire l'accesso non autorizzato in entrata/uscita.

Sono adottate misure per la protezione contro gli attacchi basati sulla rete (denial of service, intercettazioni, impersonificazione) e ulteriori controlli di network based intrusion detection / prevention.

Anche i tentativi (riusciti/non riusciti) di stabilire una connessione di rete sono loggati e tenuti sotto monitoraggio.

ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI

Sono definite linee guida e relativi approcci per migliorare l'efficacia della sicurezza lungo il ciclo di vita di sviluppo del software (Software Development Life Cycle - SDLC) e, più in generale, nel più ampio processo di Gestione del Cambiamento:

- identificazione e gestione dei requisiti di sicurezza e di conformità alla normativa (in particolare per la protezione della privacy dei cittadini) gim nelle fasi iniziali di sviluppo;
- definizione, in fase di progettazione, di opportuni threat model (identificazione, enumerazione e prioritizzazione delle potenziali minacce), per individuare adeguate misure per il rispetto dei requisiti e la mitigazione dei rischi, soprattutto per i cambiamenti più critici;
- analisi statica del codice e soluzione delle vulnerabilità, pianificata sulla base dei livelli di criticità rilevati.
- Qualsiasi modifica, prima di essere promossa in produzione, deve essere opportunamente testata ed approvata.
- Quando l'intero sviluppo, o singole fasi di sviluppo di sistemi /servizi sono assegnate a terze parti o in caso di acquisizione di strumenti / sistemi OTS, la sicurezza delle informazioni e l'adozione dei relativi requisiti è regolata tramite opportune clausole contrattuali di sicurezza; i fornitori sono quindi valutati nel tempo rispetto alla capacità di rispondenza ai requisiti ed al rispetto delle regole definite.

Per i trattamenti più critici, in ottemperanza con gli obblighi relativi alla protezione dei dati personali, sono condotte attività preliminari di valutazione dei possibili impatti sui cittadini interessati a cui si riferiscono i dati trattati (DPIA).

GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI

Sono definite linee guida e viene dato supporto per assicurare un approccio coerente ed efficace per la gestione degli incidenti

relativi alla sicurezza delle informazioni, incluse le indicazioni per efficaci comunicazioni interne e verso l'esterno (ad esempio in caso di Notifica alle Autorità di eventuali violazioni dei dati personali in ottemperanza agli obblighi previsti in tal senso dal GDPR), la registrazione di ogni incidente e il reporting. L'esperienza ricavata da ogni accadimento viene acquisita e documentata ai fini del miglioramento del processo stesso.

ASPETTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI NELLA GESTIONE DELLA CONTINUITÀ OPERATIVA

Sono identificate e indirizzate, nei confronti delle terze parti eventualmente impiegate in una o più fasi della catena di erogazione dei servizi, i livelli minimi di funzionamento e i normali regimi di operatività, fissando gli obiettivi di recupero della stessa (recovery time objectives (RTO) e recovery point objectives (RPO)). È richiesto che per i sistemi, i database, le infrastrutture e ogni altra iniziativa a copertura della continuità aziendale, sia nel day-by-day che durante un evento avverso, il livello di sicurezza sia mantenuto allineato con la produzione e i processi nella cosiddetta "normal operation". La continuità della sicurezza delle informazioni è garantita anche attraverso le necessarie attività sulle basi dati per assicurare la continuità del servizio.

APPENDICE 3

Data Retention Policy

Con riferimento agli specifici trattamenti effettuati in attuazione dell'Accordo, necessari per l'erogazione del Servizio, la Società applicherà i termini di conservazione seguenti, in virtù del suo ruolo di Gestore (come definito nelle Linee Guida) della Piattaforma IO, per il periodo in cui sarà in vigore l'Accordo nonché per i periodi successivi, salva in ogni caso la rivalutazione periodica effettuata dalle Parti al fine di garantire l'adeguatezza nel tempo dei termini stessi, e salvo in ogni caso diverso accordo delle Parti:

- Conservazione del documento (e dei Dati Personali in esso contenuti) in attesa di firma da parte dell'Utente (i.e. tempo massimo per cui il documento rimane a disposizione dell' Utente per consentirne la sottoscrizione): 90 (novanta) giorni, salvo diversa indicazione da parte dell'Ente.
- Conservazione del documento (e dei Dati Personali in esso contenuti) firmato dall'Utente (i.e. tempo massimo entro il quale l'Utente ha la possibilità di effettuare il download del documento sottoscritto sulla Piattaforma IO): 90 (novanta) giorni.
- Conservazione del certificato di firma e delle informazioni ex art. 32, comma 3, lett. j), CAD a cura del QTSP: 20 (venti) anni.

Allegato C

Livelli di servizio

Gli Enti che intendono avvalersi di Firma con IO possono richiamare le API di IO con un rate di invocazione di seguito riportato:

- fino a 150 chiamate API cumulative nell'intervallo dei 5 secondi. Nel conteggio sono comprese, a titolo esemplificativo e non esaustivo, le chiamate alle API per la creazione di un Dossier (Create-Dossier), la creazione di una Richiesta di Firma (Create-Signature-Request) e per la verifica dello stato di una richiesta (Get-Signature-Request). Di seguito i Service Level Indicators qualitativi di verifica delle API sopra indicate:

Descrizione indicatore	**Valore di Soglie (obiettivo)**	**Strumento di verifica**	**Unità temporale di calcolo**	**Penale**
Non disponibilità delle API	Il numero medio di risposte con esito negativo (classe di errore http 5xx) non superiori al 5% del totale delle richieste ricevute sulle API indicate La soglia può essere applicata ad un numero minimo di 3000 chiamate nel mese alle API	Le dashboard di monitoraggio statiche che consentono di rilevare gli esiti di risposta delle API sono disponibili, su richiesta dell' Ente, in caso di contestazione del mancato rispetto degli SLA	trimestrale	se >5% e < 7%: penale del 3% rispetto a quanto dovuto a titolo di corrispettivi dall'Ente nel trimestre di riferimento se > 7% penale del 4% rispetto a quanto dovuto a titolo di corrispettivi dall'Ente nel trimestre di riferimento
Tempi medi di risposta delle API	Il tempo medio di risposta delle API, rispetto al numero totale delle chiamate effettuate nell' intervallo di riferimento, è inferiore o uguale ad un	Le dashboard di monitoraggio statiche che consentono di rilevare gli esiti di risposta delle API sono disponibili , su richiesta	trimestrale	se > di 1 ,5 secondi e < 2 secondi: penale del 2% rispetto a quanto dovuto a titolo di corrispettivi dall'Ente nel

	1,5 secondi La soglia può essere applicata ad un numero minimo di 3000 chiamate nel mese alle API	dell'Ente, in caso di contestazione del mancato rispetto degli SLA.		trimestre di riferimento se >2 secondi: penale del 3% rispetto a quanto dovuto a titolo di corrispettivi dall'Ente nel trimestre di riferimento
Tempi medi di risposta dei job asincroni	Il tempo medio di esecuzione dei job asincroni (a titolo esemplificativo e non esaustivo i passaggi di stato e l' apposizione della firma) è inferiore o uguale a 3 minuti. La soglia può essere applicata ad un numero minimo di 3000 chiamate nel mese alle API	Le dashboard di monitoraggio statiche che consentono di rilevare gli esiti di risposta delle API sono disponibili , su richiesta dell'Ente, in caso di contestazione del mancato rispetto degli SLA.	trimestrale	se >3 minuti e <5 minuti: penale del 1% rispetto a quanto dovuto a titolo di corrispettivi dall'Ente nel trimestre di riferimento se >5 minuti: penale del 1,5% rispetto a quanto dovuto a titolo di corrispettivi dall'Ente nel trimestre di riferimento.

I livelli di servizio possono essere misurati e applicati dall'Ente solo nella fase di produzione, ossia in fase di consumo e fatturazione effettiva delle firme. In caso di svolgimento di un test gratuito del Servizio da parte dell'Ente non sono previsti livelli di servizio.