ALLEGATO 2 AL CONTRATTO

Accordo sul trattamento dei dati personali e misure di sicurezza

ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI E MISURE DI SICUREZZA

TRA

PagoPA S.p.A., istituita ai sensi del decreto legge 14 dicembre 2018, n. 135 (in Gazzetta Ufficiale - Serie generale -n. 290 del 14 dicembre 2018), coordinato con la legge di conversione 11 febbraio 2019, n.12 recante: «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione.» (GU n. 36 del 12-2-2019) , nel seguito indicata come "**PagoPA**", "**Società**" o "**Committente**", con sede legale e domicilio fiscale in Roma, piazza Colonna 370, c.a.p. 00187, società con socio unico e capitale sociale i.v. di euro 1.000.000, CF e P.IVA 15376371009 nella persona dell'Amministratore unico Giuseppe Virgone

E

la **SIA** s.p.a., nel seguito indicata come la "**SIA**", il "**Prestatore**" o il "**Fornitore**", con sede e domicilio fiscale in Milano, Via Gonin 36, c.a.p. 20147, codice fiscale e partita IVA n. 10596540152, nella persona del legale rappresentante in qualità dell'Amministratore Delegato p.t., Ing. Nicola Cordone

(congiuntamente la Società e SIA nel seguito indicate come le "**Parti**")

VISTO

- 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 e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), di seguito, per brevità, anche "**Regolamento**", e in particolare l'art. 4, nonché l'articolo 28 dello stesso;

PREMESSO E CONSIDERATO CHE

- in virtù del contratto sottoscritto tra PagoPA e SIA in data 20 dicembre 2019 e di cui il presente accordo costituisce l'allegato 2 (di seguito, "**Contratto**"), quest'ultima si assume l'obbligo di fornire a PagoPA i servizi oggetto del Contratto (di seguito, i "**Servizi**");
- la prestazione dei Servizi comporta il trattamento di informazioni configurabili quali dati personali ai sensi del Regolamento come meglio illustrate nell'Appendice 1 del presente accordo;
- nell'ambito delle suddette attività di trattamento a secondo che (i) PagoPA si qualifichi come: a) Titolare del trattamento o b) Responsabile del trattamento per conto di altri titolari (di seguito, "**Altri Titolari**"); (ii) SIA si qualifica rispettivamente come Responsabile o Sub Responsabile.

CIÒ PREMESSO E CONSIDERATO, l'intenzione delle Parti è di utilizzare il presente atto (di seguito anche solo "Accordo") quale accordo contrattuale per disciplinare il trattamento dei dati personali effettuato da SIA ai fini dell'esecuzione del Contratto con l'obiettivo di prestare garanzie sufficienti sulla tutela della vita privata, delle libertà e dei diritti fondamentali delle persone fisiche, ai sensi e per gli effetti dell'articolo 28 del Regolamento.

Nello specifico, è stato ritenuto che SIA, presenti - ai sensi dell'art. 28, paragrafo 1 e del considerando 81 del Regolamento - garanzie sufficienti, in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento, anche per la sicurezza, e garantisca la tutela dei diritti dell'interessato.

ARTICOLO 1
Premesse, considerato e appendici

1. Le premesse, i considerato e le appendici costituiscono parte integrante e sostanziale del presente Accordo.
2. Le Parti si danno atto che, in caso di discordanza tra gli Appendici e l'Accordo, prevarrà quanto disposto nell'Accordo.
3. 3. Qualunque termine definito nel presente Accordo avrà efficacia anche nelle Appendici allo stesso.

ARTICOLO 2
Definizioni

1. Ai fini del presente atto, trovano applicazione la terminologia e le definizioni utilizzate nel Regolamento, e in particolare i termini definiti qui di seguito:

a) **Dato Personale**	Qualsiasi informazione riguardante una persona fisica identificata o identificabile che SIA tratta al fine dell'erogazione dei Servizi, per il tramite delle attività di trattamento individuate 1 nell'Appendice 1 al presente Accordo.
b) **Interessato**	La persona fisica identificata o identificabile i cui Dati Personali sono trattati da SIA per rendere i Servizi. Le categorie di Interessati indicate con maggiore dettaglio nell'Appendice 1 al presente Accordo.
c) **Istruzioni**	Le istruzioni che PagoPA fornisce a SIA, per il tramite del presente Accordo e relativi Appendici, nonché per il tramite di ogni atto o documento previsto dal presente Accordo e/o comunicato da PagoPA a SIA nel corso della durata del del Contratto.
d) **Legge Applicabile**	Il Regolamento, nonché il d. lgs. 196/3003 recante il Codice in materia di protezione dei dati personali ("Codice Privacy") e i provvedimenti dal Garante per la protezione dei dati personali di volta in volta applicabili ai trattamenti oggetto del presente Accordo..
e) **Violazione di Sicurezza**	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai

	dati personali trasmessi memorizzati o comunque trattati che interessano i Dati Personali trattati ai sensi del Contratto e del presente Accordo.
f) **Altro Responsabile**	Qualunque ulteriore responsabile, stabilito all'interno o al di fuori dell'UE/SEE, di cui SIA si avvale ai sensi dell'articolo 28, comma 2 e 4 del Regolamento, al fine di prestare a PagoPA i Servizi o parte di essi.
g)Trattamento	Qualunque trattamento di Dati Personali effettuato da SIA in esecuzione del Contratto.

ARTICOLO 3
Obblighi delle Parti

1. Le Parti sono tenute a effettuare le attività di trattamento, ognuna per quanto di propria competenza, nel rispetto della Legge Applicabile in materia di protezione dei Dati Personali.

ARTICOLO 4
Obblighi di PagoPA

1. Nelle ipotesi in cui PagoPA si qualifica come: (i) Titolare, quest'ultima garantisce che i Dati Personali trattati dal Responsabile in relazione al presente accordo e al Contratto siano resi accessibili al Responsabile nel pieno rispetto della Legge Applicabile e si impegna altresì ad adempiere ai propri obblighi nei confronti degli Interessati ai sensi della Legge Applicabile, fatto salvo l'obbligo di assistenza di SIA ai sensi dell'Articolo 14 di cui al presente Accordo; (ii) Responsabile, quest'ultima garantisce che i Dati Personali trattati da SIA in relazione al Contratto e al presente Accordo sono resi accessibili a SIA previa autorizzazione, specifica o generale, da parte dell'Altro Titolare e nel pieno rispetto della Legge Applicabile.

ARTICOLO 5
Obblighi di SIA

1. SIA si obbliga a comunicare a PagoPA qualsiasi mutamento sostanziale delle garanzie di cui alle premesse e delle Appendici, che possa sollevare incertezze sul mantenimento delle stesse.

2. SIA conferma la sua diretta ed approfondita conoscenza degli obblighi che assume in relazione a quanto disposto dal Regolamento e si impegna a procedere al trattamento dei Dati Personali, attenendosi, ivi incluso in materia di sicurezza , oltre che al rispetto della Legge Applicabile, anche alle Istruzioni e si impegna a non effettuare alcun Trattamento dei Dati Personali al di fuori delle finalità e modalità indicate nel presente Accordo e/o nelle Istruzioni.
.
3. SIA – per quanto di propria competenza - si impegna a trattare i Dati Personali nel rispetto dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, in conformità a quanto disposto dall'art. 5 del Regolamento e di adottare le misure di sicurezza ritenute idonee

a garantire la riservatezza, l'integrità, la disponibilità dei Dati Personali in ogni fase dei Trattamenti..

4. Ove SIA rilevi la sua impossibilità a rispettare le Istruzioni, anche per caso fortuito o forza maggiore (danneggiamenti, anomalia di funzionamento delle protezioni e controllo accessi, ecc.) si impegna ad attuare, comunque, le possibili e ragionevoli misure di salvaguardia e ad avvertire senza ingiustificato ritardo PagoPA e concordare eventuali ulteriori misure di protezione.

5. SIA si impegna fin da ora a fornire su richiesta di PagoPA evidenza del rispetto di tutti gli obblighi in capo alla stessa ai sensi del presente Accordo e delle Legge Applicabile.

ARTICOLO 6
Persone autorizzate al trattamento

1. SIA si impegna ad individuare le modalità più opportune per autorizzare al Trattamento dei Dati Personali le persone che operano sotto la propria autorità diretta, scegliendole tra i soggetti reputati idonei ad eseguire le operazioni di Trattamento nel pieno rispetto della Legge Applicabile.

2. SIA garantisce, a norma dell'art. 28, paragrafo 3, lett. b) del Regolamento e articolo Art. 2-quaterdecies del Codice Privacy, che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza, nonché siano state istruite e adeguatamente formate al pieno rispetto della Legge Applicabile.

3. SIA si impegna ad avere in vigore per tutta la durata del Contratto un processo che garantisca la possibilità di conoscere le persone autorizzate al trattamento dei dati personali nell'ambito della propria organizzazione nonché i trattamenti ad essi affidati ed i relativi profili di autorizzazione.

4. SIA si impegna a provvedere, nell'ambito dei percorsi formativi predisposti per gli incaricati, alla formazione sulle modalità di gestione sicura e sui comportamenti prudenziali nella gestione dei dati personali, specie con riguardo all'obbligo legale di riservatezza cui sono soggette le persone autorizzate al trattamento dei dati.

5. SIA, considerato l'art. 32, paragrafo 4, del Regolamento, fa si che chiunque agisca sotto la propria autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso da SIA medesima, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

6. SIA si impegna fin da ora a fornire a PagoPA evidenza delle attività con le quale SIA ha istruito e tenuto costantemente aggiornate agli obblighi di cui al presente Accordo e/o alla Legge Applicabile le persone autorizzate al trattamento.

ARTICOLO 7
Amministratori di sistema

1. SIA si impegna a designare i propri "amministratori di sistema" ai sensi del Provvedimento Generale del Garante per la protezione dei dati personali del 27 novembre 2008 (pubblicato sulla G.U. del 24 dicembre 2008), modificato dal provvedimento dello stesso Garante del 25 giugno 2009 (pubblicato sulla G.U. del 30 giugno 2009), e successive modifiche, integrazioni e/o atti o provvedimenti sostitutivi ("Provvedimento AS") e dare attuazione e conformarsi a tutto quanto ivi indicato.
2. In particolare:
    a. al fine di individuare i soggetti da nominare amministratori di sistema, SIA deve far riferimento alla valutazione delle caratteristiche soggettive e alla definizione che di tali figure viene data nell'ambito del Provvedimento AS;
    b. SIA si impegna a nominare per iscritto e in modo individuale come Amministratori di sistemale persone fisiche incaricate della gestione e manutenzione del sistema informativo, indicando analiticamente i rispettivi ambiti di competenza e le funzioni attribuite a ciascuno;
    c. SIA deve conservare e mantenere aggiornato l'elenco degli Amministratori di sistema con l'indicazione delle funzioni ad essi attribuite e, qualora richiesto, tenere tale elenco disponibile in visione a Pago PA;
    d. SIA deve verificare, almeno annualmente, l'operato degli Amministratori di sistema al fine sia di accertare che le persone mantengano le caratteristiche soggettive richieste dal Provvedimento AS, e la rispondenza del loro operato alle misure organizzative, tecniche e di sicurezza poste in essere per i trattamenti dei dati personali.

ARTICOLO 8

Modalità di trattamento e di accesso ai Dati Personali, controllo e registrazione degli accessi

1. Il trattamento dei dati dovrà essere effettuato da SIA in modo tale da garantirne la sicurezza e la riservatezza e potrà essere attuato per il tempo e con logiche strettamente correlate alle finalità di cui in premessa, cui è obbligato, nel rispetto delle previsioni di cui all'art. 5 del Regolamento.

2. SIA adotta un idoneo sistema di identificazione, autenticazione, autorizzazione di qualsiasi tipo di accesso del personale autorizzato ai dati (diretto o tramite applicazione), nel rispetto di quanto previsto dall'art. 32 del Regolamento, adottando tutte le misure tecniche e organizza ive adeguate per garantire un livello di sicurezza adeguato al rischio, quali anche se del caso:
    a. tecniche di pseudonimizzazione e di cifratura dei dati personali;
    b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
    c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
    a. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Nel valutare l'adeguato livello di sicurezza, SIA dovrà tenere conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati.

4. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti richiesti; SIA si obbliga a rendere disponibile e a mantenere aggiornata la lista di tutte le certificazioni eventualmente ottenute e/o codici di condotta cui abbia eventualmente aderito.

5. L'accesso ai dati e le operazioni effettuate dalle persone autorizzate e dagli amministratori di sistema, debbono essere tracciate e risultare consultabili da SIA e, su eventuale motivata richiesta e in sede di audit, da Pago PA nell'ambito dei propri compiti di vigilanza.

6. Le registrazioni degli accessi ai Dati Personali devono:

    a. avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità;
    b. comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate;
    c. essere adeguate al raggiungimento dello scopo di verifica per cui sono state richieste;
    d. essere conservate per un congruo periodo, non inferiore a sei mesi.

7. Le registrazioni degli accessi ai sistemi non riconducibili ai Dati Personali, da parte degli Amministratori di Sistema seguono le indicazioni connesse al Provvedimento AS.

8. Le misure tecniche e organizzative di sicurezza devono essere in linea con lo stato dell'arte della tecnologia e gli standard di sicurezza riconosciuti dall'industria di settore, con particolare riferimento allo standard ISO / IEC 27001 e, ove applicabile, allo standard PCI DSS.

9. Le misure tecniche e organizzative implementate da SIA sono descritte nell'Appendice 2 al presente Accordo che costituisce parte integrante delle Istruzioni di PagoPA.

10. SIA può di volta in volta modificare le misure tecniche ed organizzative a condizione che le nuove misure garantiscano il medesimo ovvero più elevato livello di sicurezza nel trattamento dei Dati Personali.

11. SIA si impegna ad aggiornare semestralmente le misure di sicurezza applicate al Trattamento, fornendo a Pago PA una versione aggiornata dell'appendice 2 al presente Accordo.

ARTICOLO 9

Fornitura di dati al Titolare

1. PagoPA informa SIA circa i soggetto/i autorizzati a richiedere fornitura di Dati Personali con eventuali limitazioni di ambito.

2. Qualora SIA, o soggetto/funzione da esso incaricato, abbia necessità per lo svolgimento dei propri compiti istituzionali di accedere a Dati Personali non disponibili attraverso i servizi applicativi, li richiede per iscritto, esplicitando tipologia dei dati, tempistica e modalità di fornitura, a SIA il quale è tenuto a renderli disponibili, secondo modalità da concordare tra le Parti.

3. SIA tiene traccia in un apposito registro generale di tali richieste e dei dati movimentati.

ARTICOLO 10

Ricorso ad un Altro Responsabile

1. SIA non può ricorrere a un Altro Responsabile senza previa specifica autorizzazione scritta di PagoPA.

2. Nell'ipotesi in cui SIA, a seguito di specifica autorizzazione scritta da parte di PagoPA, ricorra ad un Altro Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto di PagoPA, (i) SIA dovrà scegliere quale tale Altro Responsabile società che diano adeguate garanzie in termini di esperienza, capacità e affidabilità in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza; e (ii) su tale Altro Responsabile del trattamento devono essere imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi o equivalenti obblighi – tenuto conto della natura delle attività di trattamento affidati all'Altro Responsabile - in materia di protezione dei dati contenuti nel presente atto giuridico , prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento.

3. Qualora l'Altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, SIA conserva – nei limiti di cui al presente Accordo - nei confronti di PagoPA l'intera responsabilità dell'adempimento degli obblighi dell'Altro Responsabile.

4. SIA si impegna ad impartire all'Altro Responsabile e di impartire o far impartire al personale di quest'ultimo autorizzato al trattamento le Istruzioni e indicazioni circa le modalità di Trattamento e si impegna a esercitare un costante controllo sul loro rispetto.

5. SIA si impegna a mantenere un apposito registro, anche eventualmente nel Registro dei trattamenti, correttamente aggiornato, degli Altri Responsabili, da rendere disponibile a PagoPA su richiesta.

ARTICOLO 11

Sostituzione e dismissione delle apparecchiature

1. L'eventuale sostituzione e dismissione delle apparecchiature utilizzate nell'erogazione del Servizio con conseguente distruzione dei relativi dati dovrà avvenire secondo quanto previsto dalle norme e dai provvedimenti vigenti.

ARTICOLO 12

Tenuta del Registro dei trattamenti e nomina del responsabile per la protezione dei dati

1. SIA deve tenere, in forma scritta, anche in formato elettronico, un registro di tutte le categorie di attività relative al trattamento svolte per conto di PagoPA, contenente le informazioni di cui al paragrafo 2 dell'art. 30 del Regolamento, da mettere, su richiesta, a disposizione dell'autorità di controllo e di PagoPA.

2. SIA designa, a norma degli articoli 37 e ss. del Regolamento, un responsabile della protezione dei dati (RPD), comunicandone gli estremi e i dati di contatto a PagoPA.

ARTICOLO 13

Attività di verifica e controllo

1. SIA è sottoposta al controllo da parte di PagoPA sullo svolgimento dell'attività e dei compiti ad esso affidati. Tale controllo potrà essere effettuato da SIA anche attraverso periodiche attività di audit, svolte, direttamente o tramite persona/funzione da essa delegata.

2. SIA si impegna ad informare per iscritto PagoPA, su sua esplicita richiesta, sullo stato di applicazione delle procedure ed Istruzioni impartite, fornendone evidenza a PagoPA secondo le modalità e periodicità concordate dalle Parti. Ciascuna Parte si impegna a cooperare con l'altra segnalando eventuali necessità di intervento e proponendo le migliori azioni da porre in essere.

3. SIA mette, in ogni caso, a disposizione di PagoPA tutte le informazioni ragionevolmente necessarie per dimostrare il rispetto degli obblighi di cui al presente Accordo e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate da PagoPA o da altro soggetto da questi incaricato.

4. SIA informa immediatamente PagoPA qualora, a suo parere, un'Istruzione violi il Regolamento, la Legge Applicabile o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

ARTICOLO 14

Obblighi di assistenza e collaborazione con PagoPA

1. SIA si impegna ad assistere PagoPA:

- tenendo conto della natura del Trattamento, con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo di PagoPA medesimo di fornire assistenza agli Altri Titolari e/o di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento in conformità alle procedura concordate dalle Parti "Procedura per la Gestione dei Diritti degli Interessati" e in conformità con il Servizio di Assistenza fornito da SIA nell'esecuzione del Contratto. Le Parti si impegnano alla definizioni della "Procedura per la Gestione dei Diritti degli Interessati"entro e non oltre 60 giorni dalla stipula del Contratto.;

- trattare i Dati Personali nel territorio dell'Unione Europea nonché dello Spazio Economico Europeo (SEE). Qualsiasi trasferimento verso Paesi al di fuori dall'Unione Europea nonché dallo SEE richiede il consenso esplicito, preventivo e in forma scritta di PagoPA e può avvenire solo se le condizioni di cui agli Artt. 44 del Regolamento e seguenti siano soddisfatte. Se SIA è tenuta al trasferimento verso Paesi al di fuori dall'Unione Europea nonché dallo SEE in base a norme inderogabili di legge dell'Unione Europea o dello Stato Membro a cui è soggetta SIA, quest'ultimo informerà PagoPA di tale obbligo legale prima che abbia inizio tale trasferimento, a meno che la legge non vieti a SIA di fornire tale informazione a PagoPA per rilevanti motivi di interesse pubblico.

- tenendo conto della natura del trattamento e delle informazioni a disposizione di SIA, nel garantire il rispetto di tutti gli obblighi di cui agli articoli da 32 a 36 del Regolamento. In particolare, conformemente all'art. 28, paragrafo 3, lett. f) del Regolamento, deve assistere SIA nell'esecuzione della valutazione d'impatto sulla protezione dei dati e fornire tutte le informazioni necessarie. SIA si impegna altresì a compilare e fornire a PagoPA, per quanto di propria competenza, annualmente o al verificarsi di sostanziali modifiche nelle attività di trattamento una valutazione di impatto del servizio relativa al rischio di sicurezza IT ..

- SIA si impegna, altresì, a norma dell'art. 33, paragrafo 2, del Regolamento ad informare PagoPA senza ingiustificato ritardo di una Violazione di Sicurezza e si impegna a fornire ragionevole assistenza a PagoPA nell'obbligo di informare l'Autorità di controllo e gli Interessati, laddove necessario, Successivamente, fornisce a PagoPA, oltre alle Informazioni indicate nell'allegato 1 e 1 bis del Contratto, le seguenti informazioni di dettaglio, salvo impossibilità di conoscerle:

    a) il tipo di violazione
    b) la natura, la categoria e il volume dei dati personali interessati;
    c) facilità di identificazione delle persone;
    d) la descrizione delle probabili conseguenze per gli interessati (ad esempio: danni fisici, disagio psicologico, umiliazione o danni alla reputazione);
    e) le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di record di dati personali interessati;

f) probabili conseguenze della violazione dei dati personali subita dal Responsabile e/o dai Sub-responsabili;
g) misure adottate o da adottare per affrontare la violazione dei dati personali, per attenuare gli effetti e ridurre al minimo i danni derivanti dalla Violazione della sicurezza.

2. Tutte le attività di SIA ai sensi del presente articolo e ai sensi del Contratto sono comprese nei Corrispettivi, fatta salva la possibilità per SIA di addebitare i costi sostenuti per fornire le informazioni o intraprendere l'azione richiesta, unicamente ove tali attività risultino particolarmente onerose in termini economici e non prevedibili al momento della stipula del presente Accordo e/o non riconducibili alle normali attività che ci si potrebbe attendere da SIA nell'esecuzione del Contratto e del presente Accordo. SIA è tenuta a comunicare a PagoPA preventivamente qualsiasi attività che comporti un tale maggior costo e attendere l'approvazione scritta di PagoPA prima di iniziare l'attività medesima.

3. SIA deve, inoltre, collaborare con PagoPA nei rapporti di quest'ultimo con il Garante per la protezione dei dati personali ("Garante") ed in particolare deve:

- tenersi sempre aggiornato sulle iniziative normative e, in genere, sulle attività del Garante;
- collaborare per l'attuazione di eventuali specifiche istruzioni;
- avvisare immediatamente in caso di ispezioni, di richiesta di informazioni e di documentazione da parte del Garante fornendo, per quanto di competenza, il supporto eventualmente richiesto, ove non altrimenti vietato dalla legge;
- rendere disponibile per tempo a PagoPA ogni informazione appropriata, in caso di contenzioso.

4. Il Responsabile coopera, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.

ARTICOLO 15

Istruzioni

Il presente atto e il Contratto costituiscono le istruzioni complete e finali di Pago PA.

Pago PA può fornire ulteriori istruzioni a SIA che dovranno rientrare nell'ambito delle istruzioni impartite nel Contratto e nel presente Accordo. In caso contrario, le ulteriori istruzioni che comportino Servizi Evolutivi da parte di SIA saranno quotati a parte e retribuiti sulla base dell'Allegato 3 b del Contratto.

ARTICOLO 16

Responsabilità

1. Le Parti si danno reciprocamente atto che (i) **a**i sensi dell'art. 82 del Regolamento, le responsabilità dei soggetti operanti in qualità di Titolare, Responsabile e Sub Responsabile è solidale per qualsiasi danno cagionato nei confronti degli Interessati nell'esecuzione del

trattamento. La Parte che abbia risarcito il danno per intero avrà diritto di rivalsa nei confronti dell'altra Parte, nei limiti di seguito contrattualmente convenuti nel seguente paragrafo.

2. Fatti salvi i casi di dolo o colpa grave, la responsabilità complessiva di SIA nei confronti di Pago PA per qualsiasi danno, che possa derivare a seguito di una violazione imputabile a SIA degli obblighi imposti dalla Legge Applicabile e/o delle Istruzioni e/o degli obblighi di cui al presente atto è limitata complessivamente e regolata dalle disposizioni in materia di responsabilità di cui al Contratto. Le Parti stabiliscono che il limite complessivo previsto per la responsabilità di SIA dovuta per le presenti violazioni è il medesimo di quello previsto nel Contratto.
3. In caso di violazioni accertate dall'autorità di controllo, ciascuna Parte sarà tenuta al pagamento dell'ammontare della sanzione contestata nei limiti della responsabilità rilevata a proprio carico dall'autorità di controllo.

ARTICOLO 17

Durata del trattamento

1. SIA è autorizzato al Trattamento per tutta la durata del Contratto e il presente Accordo cesserà di avere efficacia in caso di cessazione per qualsiasi ragione del Contratto, fatti salvi gli obblighi di assistenza di SIA nelle attività di migrazione e continuità del servizio pubblico ivi indicati..

2. SIA si impegna a restituire o cancellare, a scelta insindacabile di PagoPA, tutti i Dati Personali , una volta che sia terminata la prestazione dei Servizi relativi al Trattamento e siano state esaurite le lavorazioni per le quali gli stessi dati sono stati conosciuti e, in ogni caso, alla cessazione, per qualsiasi motivo del Contratto e a provvedere alla effettiva cancellazione dai supporti delle copie esistenti, fatti salvi eventuali specifici obblighi di legge che prevedano la conservazione dei dati nonché la conservazione dei Dati Personali imposta a SIA da leggi e regolamenti, ovvero qualora la conservazione sia necessaria a SIA per l'accertamento, l'esercizio e la difesa di un diritto in sede giudiziaria, previa informazione a PagoPA con riguardo ai Dati Personali conservati per tali ragioni e relativa durata della conservazione.

ARTICOLO 18

Disposizioni varie

1. L'inapplicabilità o l'invalidità di una o più disposizioni del presente Accordo non pregiudica le restanti parti dello stesso. La disposizione invalida o inapplicabile potrà all'occorrenza essere (i) modificata al fine di garantirne validità ed opponibilità, rispettando il più fedelmente possibile l'intenzione delle Parti o -qualora questo non sia possibile- (ii) interpretata come se la stessa non fosse mai stata parte del presente Accordo.

2. Per tutto quanto non espressamente disciplinato dal presente Accordo trovano applicazione le disposizioni del Contratto e del Regolamento. In caso di contrasto tra il Contratto e il Regolamento, quest'ultimo prevarrà.

Appendici:

Appendice 1 – Dettagli delle attività di trattamento dei dati personali da parte di SIA
Appendice 2 – Misure Tecniche e Organizzative di Sicurezza

per PagoPA S.p.A.

L'AMMINISTRATORE UNICO

Firmato digitalmente da:GIUSEPPE VIRGONE
Ruolo:AMMINISTRATORE UNICO
Organizzazione:PAGOPA S.P.A./15376371009
Data:23/12/2019 17:12:00

per SIA S.p.A:

IL LEGALE RAPPRESENTANTE

Nicola Cordone

Firmato digitalmente da
Nicola Cordone
Data: 2019.12.23 16:04:04
+01'00'

f.to digitalmente

Appendice 1 – Dettaglio dei Servizi che comportano un trattamento dei dati personali da parte di SIA in qualità di Responsabile o Sub Responsabile del trattamento

Responsabile per la protezione dei dati personali di SIA

Indicare i dati di contatto del Responsabile per la protezione dei dati personali

- email: dpo@sia.eu
- tel: 02.6084.1

SIA effettua, per conto di Pago PA, il trattamento dei dati personali necessario per lo svolgimento dei Servizi oggetto del Contratto.

In particolare, il trattamento dei dati personali è così individuato:

1. Nodo dei Pagamenti-SPC.

In esecuzione del Contratto, SIA è chiamata alla trasmissione tecnica delle richieste di pagamento telematiche e delle ricevute di pagamento telematiche funzionali all'esecuzione di operazioni di pagamento attraverso il sistema pagoPA. Pertanto, SIA. tratterà i dati personali contenuti nei tracciati standard delle richieste e delle ricevute di pagamento telematico. Tra i dati personali si segnalano, a titolo non esaustivo, tra gli altri, i dati del soggetto pagatore e del soggetto versante, il motivo del pagamento;

Durata: sino alla scadenza del Contratto;

Periodo di conservazione dei dati personali: I Dati Personali sono trattati per il periodo strettamente necessario al perseguimento delle finalità di cui al Contratto, tenuto conto degli obblighi di legge e comunque per il periodo necessario all'esercizio, l'accertamento o la difesa di un diritto di SIA in sede giudiziaria.

Finalità: esecuzione del Contratto;

Categorie di interessati: cittadini che eseguono le operazioni di pagamento attraverso il sistema pagoPA.

Categorie di dati personali trattati: dati personali comuni e potenzialmente Categorie Particolari di Dati (es. nel caso in cui la causale di pagamento includa tali tipi di dati), e in particolare:

- - Nome
- - Cognome
- - Codice Fiscale
- - Indirizzo
- - Civico
- - Provincia
- - Nazione
- - Causale Pagamento
- - Importo

- - IBAN utente se necessario
- - Esito Pagamento
- - ID Riscossione
- - Dati specifici Riscossione
- - RRN
- - Codice Autorizzativo

2. Portale delle Adesioni pagoPA.

In esecuzione del Contratto, SIA è chiamata alla gestione del Portale delle Adesioni al sistema pagoPA. Pertanto, SIA. tratterà i dati personali acquisiti tramite tale Portale. Tra i dati personali si segnalano, a titolo non esaustivo tra gli altri, i dati dei Referenti tecnici e dei Referenti dei Pagamenti dei soggetti aderenti;

Durata: sino alla scadenza del Contratto;

Periodo di conservazione dei dati personali: I Dati Personali sono trattati per il periodo strettamente necessario al perseguimento delle finalità di cui al Contratto, tenuto conto degli obblighi di legge e comunque per il periodo necessario all'esercizio, l'accertamento o la difesa di un diritto di SIA in sede giudiziaria.

Finalità: esecuzione del Contratto;

Categorie di interessati: utenti del Portale delle Adesioni al sistema pagoPA, dipendenti del Titolare, Dati dei referenti degli Enti Creditori e degli PSP;

Categorie di dati personali trattati: dati personali comuni:

- email
- firstname
- fiscalcode
- mobilephone
- phone
- position
- secondname
- username
- company
- address
- cap
- city
- province

3. Payment Manager / WISP (Wizard Interattivo per la Scelta del PSP). In esecuzione del Contratto, SIA è chiamata all'erogazione del servizio di registrazione degli utenti pagatori e al relativo servizio di memorizzazione delle modalità di pagamento e dei relativi strumenti di pagamento indicati dallo stesso utente pagatore che debba eseguire delle operazioni di pagamento attraverso il sistema pagoPA. Pertanto, SIA tratterà i dati personali acquisiti dagli utenti pagatori in sede di registrazione e successivamente alla stessa. Tra i dati personali si segnalano, a titolo non esaustivo tra gli altri, i dati del pagatore, i dati che consentono il riconoscimento e/o

l'identificazione del pagatore registrato e il successivo accesso, nonché i dati degli strumenti di pagamento memorizzati dal pagatore e i dati dell'eventuale soggetto versante ove non coincidente con il pagatore;

Durata: sino alla scadenza del Contratto;

Periodo di conservazione dei dati personali: I Dati Personali sono trattati per il periodo strettamente necessario al perseguimento delle finalità di cui al Contratto, tenuto conto degli obblighi di legge e comunque per il periodo necessario all'esercizio, l'accertamento o la difesa di un diritto di SIA in sede giudiziaria.

Finalità: esecuzione del Contratto.

Categorie di interessati: cittadini che eseguono le operazioni di pagamento attraverso il sistema pagoPA.

Categorie di dati personali trattati: dati personali comuni e potenzialmente Categorie Particolari di Dati (es. nel caso in cui la causale di pagamento includa tali tipi di dati), e in particolare:

- Nome
- Cognome
- Codice Fiscale
- Indirizzo
- Indirizzo mail
- Civico
- Provincia
- Nazione
- Causale Pagamento
- Importo
- IBAN utente se necessario
- Esito Pagamento
- ID Riscossione
- Dati specifici Riscossione
- PAN
- Data scadenza
- CVC
- IdOrdine
- RRN
- Codice Autorizzativo

4. Servizio di Assistenza: In esecuzione del Contratto, SIA è chiamata all'erogazione del Servizio di Assistenza come meglio descritto nel Contratto e, in particolare, nell'allegato 1 bis dello stesso. Pertanto, SIA tratterà i dati personali di chiunque richieda assistenza tramite i canali di assistenza gestiti dalla SIA ai sensi del Contratto. Tra i dati personali si segnalano, a titolo non esaustivo tra gli altri, i dati degli utenti pagatori, degli utilizzatori del Sistema PagoPA, di cittadini non utilizzatori del Sistema PagoPA ma che desiderano ottenere informazioni, personale dei Prestatori di servizi di pagamento abilitati alla Piattaforma PagoPA o che desiderano abilitarsi alla stessa, nonché personale degli enti e pubbliche amministrazioni aderenti alla Piattaforma o che desiderano aderire alla stessa.

Durata: sino alla scadenza del Contratto;

Periodo di conservazione dei dati personali: I Dati Personali sono trattati per il periodo strettamente necessario al perseguimento delle finalità di cui al Contratto, tenuto conto degli obblighi di legge e comunque per il periodo necessario all'esercizio, l'accertamento o la difesa di un diritto di SIA in sede giudiziaria.

Finalità: esecuzione del Contratto.

Categorie di interessati: qualunque persona fisica che si rivolge al servizio di assistenza.

Categorie di dati personali trattati: dati personali comuni e potenzialmente Categorie particolari di Dati (es. informazioni relative allo stato di salute dell'Interessato spontaneamente fornite dallo stesso al momento della richiesta di assistenza).

Appendice 2 – Misure Tecniche e organizzative di Sicurezza

1. Prefazione

Il presente allegato specifica le misure di sicurezza tecniche e organizzative implementate da SIA volte a proteggere i dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale, dall'alterazione, dalla divulgazione non autorizzata o dall'accesso ai dati trasmessi, archiviati o altrimenti trattati e contro tutte le ulteriori forme illecite di trattamento.
Le misure di sicurezza sono state selezionate utilizzando un approccio basato sul rischio dal punto di vista della sicurezza e della protezione dei dati, tenuto conto degli standard e delle leggi applicabili.
SIA, per le attività di propria competenza, mantiene, monitora e aggiorna regolarmente la conformità a alle predette misure in base alle disposizioni delle norme ISO / IEC 27001, ISO 22301 e, ove applicabile, lo standard PCI DSS; inoltre, saranno condotte certificazioni e audit di terze parti.
Le misure tecniche e organizzative saranno mantenute durante il periodo dell'accordo e potranno essere riviste e aggiornate per adattarle ai cambiamenti avvenuti nel panorama normativo e delle minacce di sicurezza.

2. Struttura del documento di misure tecniche e organizzative

L'applicabilità delle misure di sicurezza deve essere determinata come pertinente nell'ambito dell'Accordo in relazione alle attività e ai servizi offerti dal Fornitore.
Le misure tecniche e organizzative sono organizzate come segue:

2.1 Controllo degli accessi logici Il controllo dell'accesso logico comprende l'accesso ai sistemi, alle applicazioni e ai dati. Lo scopo di tale attività è:

- impedire a persone non autorizzate di utilizzare sistemi di trattamento dei dati in cui sono archiviati, elaborati o utilizzati dati personali;
- garantire che le persone autorizzate ad utilizzare un sistema di elaborazione dei dati abbiano accesso solo ai dati per cui sono autorizzati ad accedere e che i dati personali non possano essere letti, copiati, alterati o rimossi, senza previa autorizzazione, durante l'elaborazione, l'uso e dopo la memorizzazione del dato.

2.2 Controllo degli accessi fisici
Lo scopo di tale attività è impedire a persone non autorizzate di accedere ai locali dove avviene l'elaborazione dei dati.

2.3 Protezione del ciclo di vita dei dati
Lo scopo di tale attività è garantire una protezione adeguata durante il ciclo di vita dei dati.

2.4 Gestione delle operazioni in sicurezza
Lo scopo di tale attività è assicurare la gestione di operazioni sicure delle strutture di elaborazione delle informazioni.

2.5 Disponibilità

Lo scopo di tale attività è garantire che i dati personali siano protetti contro la distruzione o la perdita accidentale.

2.6 Separazione dei dati

Lo scopo di tale attività è garantire che i dati raccolti per scopi diversi possano essere elaborati separatamente.

2.7 Controllo organizzativo

Lo scopo di tale attività è:

- garantire che vengano assegnate le responsabilità di sicurezza al personale di cui SIA si avvale;
- garantire che il sistema di gestione della sicurezza sia mantenuto in linea con lo standard ISO/IEC 27001;
- garantire che personale di cui SIA si avvale siano consapevoli delle proprie responsabilità nelle attività di trattamento e che vengano adeguatamente formati.

2.8 Controllo degli accessi logici

SIA stabilisce, documenta, implementa e mantine una procedura che regolamenta il ciclo di vita delle utenze di SIA (e.g. dal provisioning delle utenze in caso di assunzione al de-provisioning in caso di termine del lavoro); include anche revisione e revoca dell'accesso utente.
Tramite una piattaforma di Identity Manager, le notifiche pervenute dal personale (nuovo dipendente, rotazione del lavoro, cessazione del rapporto di lavoro) sono immediatamente:

- gestite su sistemi di destinazione direttamente connessi alla piattaforma di Identity Management
- notificate agli amministratori di sistema dei sistemi o delle applicazioni di destinazione che non sono direttamente collegati alla piattaforma di Identity Management.

In particolare, per quanto riguarda:

- identificazione utente, sono implementati i seguenti requisiti:
  - assegnazione identificativo unico; non sono consentiti account di gruppo o condivisi, gli account di fornitori e del fornitore di servizi vengono rilasciati solo a singoli utenti, con la sola eccezione degli account autorizzati ed utilizzati per fini tecnici;
  - assegnazione di un nome utente univoco prima di consentire all'utente gli l'accesso al sistema;
  - verifica dell'identità dell'utente prima della creazione dell'account o dell'esecuzione delle richieste di reimpostazione della password;
  - disabilitazione dei profili utente predefiniti (amministratore, SA, public, ecc.);
  - disabilitazione automatica dei profili utente assegnati a persone esterne dopo un periodo massimo di validità, se necessario rinnovabile;
  - disabilitazione immediata al termine dello stato di autorizzazione (cessazione dei dipendenti, fine della collaborazione, scadenza del contratto, ecc.).

- autenticazione utente, sono implementati i seguenti requisiti:

- L'autenticazione dell'utente per un sistema si verifica mediante l'utilizzo di una password e, laddove applicabile per i sistemi più critici, mediante l'utilizzo di strumenti di autenticazione strong (come token, smart card, ecc.);
- La politica della password è definita in linea con gli standard e soddisfa i seguenti requisiti:
    - lunghezza minima di 8 caratteri;
    - supporta almeno tre dei quattro requisiti come caratteri maiuscoli, minuscoli, numerici e speciali;
    - contiene almeno una lettera e almeno un numero;
    - non è facilmente correlata all'assegnatario;
    - è generata in modo univoco per ciascun utente ed è pre-scaduta (il profilo utente non può essere utilizzato se l'assegnatario non ha precedentemente modificato la password iniziale);
    - ha una validità massima di 90 giorni;
- alla scadenza, non può essere sostituita con una delle quattro password precedenti utilizzate; l'accesso remoto è concesso solo dopo un'autorizzazione formale e viene eseguito tramite autenticazione a 2 fattori; in caso di autenticazione a più fattori, oltre all'ID utente vengono scelti altri due fattori tra i seguenti:
    - qualcosa che l'utente conosce (e.g. Password, PIN, etc.);
    - qualcosa che l'utente possiede (e.g. smartcard, token, etc.);
    - qualcosa che l'utente è (e.g. parametri biometrici);
- Le credenziali di autenticazione (come ID utente e password) non vengono mai trasmesse in modo non protetto sulla rete;

- autorizzazione utente, sono implementati i seguenti requisiti:
    - la definizione dei diritti di accesso dell'utente garantisce che l'accesso ai dati nel sistema sia consentito solo nella misura richiesta all'utente per effettuare le attività di sua pertinenza e nel rispetto della separazione dei compiti lo scopo delle autorizzazioni è limitato al minimo necessario per svolgere i compiti e le funzioni della persona autorizzata;
    - viene implementato un approccio di controllo degli accessi basato sui ruoli assicurando allineamento tra i ruoli e i relativi profili di accesso;
    - ruoli e privilegi sono assegnati seguendo il principio di separazione dei compiti;
    - la revisione dei diritti di accesso dei dipendenti e degli appaltatori di SIA viene eseguita almeno una volta all'anno. Sono in atto procedure per garantire che i diritti di accesso siano revocati se le persone non soddisfano più le condizioni per ricevere l'accesso (ad es. perché cambiano posizione o cessazione del rapporto di lavoro).

Per l'accesso ai sistemi e alle applicazioni, sono implementati i seguenti requisiti:

- l'accesso dell'utente è configurato attraverso procedure di accesso che implementano soluzioni di autenticazione appropriate;
- in caso di errore di accesso, non viene visualizzata alcuna indicazione sulla causa dell'errore;
- i tentativi di accesso sono limitati;
- le sessioni che sono rimaste inattive per più di 15 minuti richiedono all'utente di ri-autenticarsi per riattivare il terminale o la sessione;
- le sessioni remote vengono disconnesse dopo 15 minuti di inattività.

Gli account degli utenti privilegiati possono essere richiesti solo da responsabili o supervisori e sono appropriatamente approvati.
Per taluni servizi SIA ha implementato misure di registrazione (e.g. come la registrazione delle sessioni); sono documentate le istruzioni al personale che ha account privilegiati sulla criticità del proprio ruolo.

I sistemi in ambito PagoPa sono:

- il nodo dei pagamenti: il cui accesso è regolamentato come indicato sopra
- il payment manager: il cui accesso è regolamentato come indicato sopra
- il portale delle adesioni:
- il tool di assistenza per il nodo:
- il tool di assistenza per il payment manager:

2.9 Controllo degli accessi fisici

È stabilita, documentata, implementata e mantenuta una politica di controllo degli accessi fisici, nonché sono in essere presidi di sicurezza fisica a protezione dei locali in cui si svolgono attività di trattamento dei dati.

2.10 Accesso ad edifici e locali

L'accesso ai locali di SIA, sia la sede centrale che i datacenter, è consentito solo al personale autorizzato. L'accesso alle sale è gestito tramite lettore badge, tornelli all'ingresso principale e lettori badge in ogni stanza.
In particolare, il sistema di controllo degli accessi fisici permette l'accesso ai soli utenti forniti di predefiniti profili autorizzativi ed è applicato sui varchi delle aree fisiche, in altre parole sui tratti del perimetro di un'area che consentono di accedere all'interno della stessa.
Il sistema di controllo degli accessi fisici:

- è progettato per non essere superabile senza specifica autorizzazione;
- gestisce diversi profili autorizzativi;
- è applicato a tutte le aree aziendali che, sulla base di specifica valutazione dei rischi, devono garantire un adeguato livello di protezione delle informazioni;
- registra tutte le operazioni di transito tentate o riuscite imputandole al soggetto a cui è stato concesso un certo profilo autorizzativo con il quale viene compiuta l'azione;
- segnala immediatamente eventuali violazioni delle regole o tentativi di forzare il controllo;
- custodisce per un tempo prefissato le informazioni registrate;
- adotta un sistema di autenticazione basato sul possesso di un elemento di autenticazione personale (badge o chiave) e per l'accesso in alcune aree di custodia da un PIN (personal identification number).

Nel datacenter tutte le porte interne sono collegate a una sala di controllo centrale che riceve allarmi da ciascuna porta nel caso rimanga aperta. La sala di controllo centrale ha una connessione diretta con il dipartimento di Polizia. Il datacenter è dotato di misure di sicurezza perimetrale e non e di seguito si citano tra le altre a titolo esemplificativo e non esaustivo: telecamere (ad esempio sistemi

di rilevamento del movimento e telecamere CCTV), sistemi di allarme antifurto, meccanismi di controllo degli accessi utilizzati per monitorare i punti di ingresso / uscita in aree sensibili.
L'accesso fisico ai locali di SIA per il personale non dipendente SIA (es. consulenti esterni) è consentito solo ed esclusivamente alle persone autorizzate, previa identificazione, assegnazione di un badge di accesso temporaneo e se accompagnate da personale interno di SIA durante la loro permanenza all'interno dell'edificio.
La reception della sede degli uffici è presidiata h24 da uno staff dedicato. Lo staff gestisce i sistemi di allarme centralizzati e una sala di controllo ridondata rispetto a quella del datacenter.

2.11 Aree di sicurezza

Le aree fisiche hanno un resposabile di riferimento che ha il compito di classificarle in relazione alla criticità delle informazioni che vengono trattate al loro interno e tenendo conto degli obblighi introdotti dalle normative.
La disposizione delle sale e delle strutture al loro interno tiene conto dei rischi connessi ad eventuali accessi non autorizzati. Per questo motivo, le strutture di elaborazione delle informazioni sono ospitate all'interno di locali più protetti e lontani dall'accesso al pubblico. L'accesso è strettamente controllato da un sistema di registrazione; le registrazioni degli accessi fisici vengono archiviate e controllate regolarmente.
Tutti gli utenti sono adeguatamente informati e resi consapevoli delle regole in vigore all'interno delle aree fisiche di SIA. Tutto il personale è formato per segnalare, attraverso il servizio di sicurezza e il diretto superiore, la presenza di persone non identificate all'interno dei locali di SIA.

3. Protezione del ciclo di vita dei dati

Proteggere il ciclo di vita dei dati significa raccogliere, conservare, processare, smaltire e distruggere i dati in modo sicuro. Al fine di garantire una protezione adeguata, è necessaria la classificazione dei dati.
SIA ha definito, documentato e comunicato le regole di classificazione dei dati ai dipendenti al fine di garantire che, in conformità con la criticità dei dati, vengano applicate procedure di gestione adeguate.
I controlli crittografici sono adottati in base alla triade di classificazione riservatezza, integrità e disponibilità; i sistemi crittografici vengono implementati in base alle best practice riconosciute e standard del settore (come ad esempio gli algoritmi crittografici raccomandati da FIPS o NIST).
I criteri per la lunghezza minima delle chiavi di crittografia sono definiti in linea con gli standard approvati e riconosciuti come lo standard PCI DSS.
Le procedure di gestione delle chiavi simmetriche sono documentate, implementate e mantenute. Esse sono progettate per assicurare i criteri del "dual control" e dello "split knowledge" durante il loro intero ciclo di vita.

Durante il loro intero ciclo di vita, i dati sono protetti in ogni fase.

3.1 Dati memorizzati

I dati memorizzati sono protetti da un meccanismo di crittografia integrato a livello di archiviazione (ad esempio, le strutture di backup sono crittografate).

Se si utilizza la cifratura del disco anziché la cifratura di tabelle, colonne o file, le tabelle nei database contenenti informazioni sensibili vengono protette utilizzando altri meccanismi di sicurezza quali il

controllo di accesso logico gestito indipendentemente dal controllo di accesso del sistema operativo nativo.

3.2 Dati in transito

I dati scambiati su reti c.d. *untrusted* sono protetti mediante meccanismi di cifratura che, come elenco non esaustivo, includono:

- Transport Layer Security (TLS) in combinazione con certificati digitali validi che utilizzano la crittografia a chiave pubblica per impedire intercettazioni, manomissioni e falsificazioni;
- Secure Shell;
- TLS-VPN;
- Secure FTP (SFTP);
- IPSec.

3.3 Dati in uso

I dati in uso sono protetti mediante misure di controllo di accesso logico come previsto nel precedente Capitolo 1 "Controllo degli accessi logici"; inoltre, per taluni servizi le workstation in uso per elaborare o accedere ai dati critici, ove trattati, sono dotate di una soluzione che intercetta e previene la perdita di dati dalle workstation (end-point DLP). La soluzione è gestita centralmente dal personale di SIA ed è implementata come segue:

- è basato su agenti intallati sulle singole macchine; le workstation e gateway per le reti esterne rientrano nell'ambito di questo controllo;
- è configurato per bloccare le azioni critiche sui dati sensibili; è stato inoltre definito un processo di eccezione temporaneo.

3.4 Smaltimento sicuro

Viene stabilita e documentata una procedura per lo smaltimento e/o la distruzione di supporti fisici (ad es. documenti cartacei, CD, DVD, nastri, unità disco, ecc.); i meccanismi di smaltimento variano in base alla classificazione dei dati contenuti e al tipo di supporto.
Lo smaltimento sicuro dei dati cartacei contenenti dati critici viene eseguito utilizzando una trituratrice con un impianto di taglio trasversale; in alternativa, i documenti possono essere inceneriti. La triturazione è anche il meccanismo utilizzato per la distruzione dei supporti ottici.

In caso di disco rigido, supporti magnetici o altri supporti equivalenti che contengono dati critici, la procedura di smaltimento prevede meccanismi di cancellazione sicura per rendere i dati irrecuperabili utilizzando ad esempio:

- l'esecuzione di un programma di cancellazione sicura in conformità con gli standard accettati dal settore (e.g. wiping)
- la distruzione fisica dei supporti.

Vengono mantenuti i registri dello smaltimento dei supporti.

4. Gestione delle operazioni in sicurezza

SIA ha stabilito, documentato, implementato e mantenuto una serie di istruzioni operative relative alle procedure di sicurezza per garantire la corretta operatività delle comunicazioni e delle infrastrutture di elaborazione delle informazioni.

4.1 Registrazione e monitoraggio

I sistemi, applicazioni e componenti di rete sono configurati per generare eventi relativi alla sicurezza che sono conservati in appositi registri (log). Tali registri vengono inviati e correlati da una piattaforma centrale di sicurezza doniminata SIEM (information event management).
La piattaforma SIEM è gestita da personale dedicato di SIA che gestisce le attività di monitoraggio.
Vengono definiti gli eventi da registrare e la verbosità del registro in linea con gli standard di settore; i log prodotti includono un livello di dettaglio adatto per una corretta rilevazione.
La protezione dei file di log è garantita al fine di garantire la loro integrità ed evitare modifiche da parte di personale non autorizzato.
I registri vengono conservati per 2 anni in conformità con le leggi e gli standard applicabili.
Le attività degli amministratori di sistema e degli operatori di sistema vengono registrate e i log sono protetti e sottoposti a backup.

4.2 Protezione Anti-malware

SIA al fine di prevenire attacchi relativi a *malware* utilizza un approccio costituito da diverse tecnologie di rilevamento utilizzate perimetralmente sia su server sia su PC.

I prodotti antivirus e IDS vengono utilizzati per proteggere i sistemi informatici da codice malevolo.

Le workstation sono protette secondo lo standard PCI-DSS e, per taluni servizi, secondo misure aggiuntive quali APT e DLP (prevenzione della fuga dei dati).

Per fronteggiare le minacce avanzate, sono state implementate soluzioni aggiuntive come l'esecuzione di sandboxing degli allegati e-mail, l'agente EDR (Endpoint Detection and Response) e la protezione DNS.

4.3 Gestione delle configurazioni

Sono definite, documentate e implementate le configurazioni dei sistemi di informazione (ad es. sistemi operativi, prodotti software, dispositivi di rete).
Esse sono progettate in linea con le migliori pratiche pertinenti e includono opzioni di configurazione rilevanti per la sicurezza.

4.4 Gestione dei cambiamenti

Vengono definite le responsabilità per la gestione e il controllo dei cambiamenti applicativi e tecnologici, garantendo la segregazione dei compiti tra le strutture di sviluppo, di test e operative al fine di ridurre i rischi di accessi o cambiamenti non autorizzati ai sistemi in funzione.
Per quanto riguarda i cambiamenti, le procedure interne prevedono:

- documentazione sull'impatto;
- approvazione documentata da parte di soggetti autorizzati;
- test di funzionalità per verificare che il cambiamento non abbia effetti negativi sulla sicurezza dell'intero sistema.

Vengono fornite procedure adeguate per il ripristino dei sistemi in caso di fallimento della modifica operativa, al fine di tornare ad uno stato stabile precedente (rollback).

Le modifiche applicative / tecnologiche nell'ambiente operativo di SIA sono adeguatamente comunicate a tutto il personale coinvolto e, ove necessario, anche ai clienti.

4.5 Test di sicurezza e gestione delle vulnerabilità

Sono state stabilite, documentate, implementate e mantenute le procedure per i test di sicurezza e per la gestione delle vulnerabilità.
I test di sicurezza (a livello applicativo o infrastrutturale) sono eseguiti sulla base delle *best pratice* e gli standard pertinenti (PCI-DSS) nonché secondo gli accordi tra SIA e la propria clientela.
SIA adotta un processo di gestione delle vulnerabilità per identificare vulnerabilità di sicurezza che integra fonti esterne attendibili per trarre informazioni ed assegnare una classificazione del rischio basata sugli standard riconosciuti (ad esempio, classificazione CVE).
Questo processo consente il monitoraggio e la gestione delle vulnerabilità dei sistemi e delle applicazioni; i tempi per la riparazione in caso di vulnerabilità sono definiti in conformità con la classificazione della vulnerabilità e gli standard pertinenti.

4.6 Sicurezza delle workstation

Le workstation sono protette adottando una serie di misure di sicurezza che includono tra le altre a titolo esemplificativo e non esaustivo: antivirus, cifratura del disco, sistemi di filtraggio della navigazione, sistemi di detection di minacce avanzate (e.g. EDR), data loss prevention. Tali misure sono gestite centralmente e sono logicamente amministrate dal team di sicurezza che opera l'analisi degli eventi e degli allarmi prodotti dalle piattaforma centrale SIEM.
Agli utenti non sono concessi diritti amministrativi sulle loro workstation.
I dispositivi mobili sono protetti, controllati e gestiti tramite una soluzione MDM specifica.
Secondo le politiche SIA, attualmente il BYOD non è consentito.

5. Disponibilità

5.1 Back up, Business Continuity & Disaster Recovery

SIA si impegna a predisporre e gestire adeguate procedure di back up per la ripartenza del servizio in caso di anomalie/interruzioni. In particolare si impegna a garantire, nei tempi minimi consentiti dai vincoli tecnici/operativi e con l'obiettivo di limitare il disservizio, il ripristino dell'ultima situazione consolidata prima del verificarsi dell'anomalia/interruzione; in ogni caso tale situazione non deve essere anteriore al giorno lavorativo precedente, salvo diverse modalità temporali precisate in altri allegati al presente contratto. Le copie di dati applicativi, programmi e immagini di sistema sono effettuate regolarmente al fine di preservare la loro disponibilità a seguito di uno stop programmato o inaspettato causato da eventi esterni (manutenzione ordinaria, manutenzione straordinaria, Business Continuity / Disaster Recovery) in linea con le disposizioni di requisiti aziendali. SIA infatti gestisce - ove previsto - procedure di back up per la ripartenza dei servizi medesimi in caso di anomalie/interruzioni.

6. Separazione dei dati

SIA ha implementato una serie di misure atte a garantire l'elaborazione separata ovvero la segregazione logica dei dati raccolti per scopi diversi; come da elenco a titolo esemplificativo e non esaustivo, esso comprende:

- l'accesso ai dati personali è gestito adottando il criterio "need-to-know";

- le risorse IT (in termini di ambienti di elaborazione, architetture, sistemi, applicazioni, archivi, reti e dati) sono classificate in base al livello di rischio delle attività svolte e al livello di criticità dei dati trattati, garantendo un approccio di difesa in profondità; ciò assicura che gli ambienti di produzione siano separati dagli ambienti non di produzione e il software o il trasferimento dei dati tra ambienti con criticità diverse sia regolato;
- applicazioni, interfacce, processi batch e report sono progettati solo per scopi e funzioni specifici, pertanto i dati raccolti per scopi diversi vengono elaborati separatamente.

7. Controllo organizzativo

SIA ha adottato un sistema di gestione della sicurezza delle informazioni certificato ISO / IEC 27001 che include la definizione di ruoli, responsabilità, procedure e controlli.
É stato nominato un responsabile della sicurezza ed è presente una funzione di Cybersecurity che gestisce i presidi più critici di sicurezza, indirizza e controlla le attività di sicurezza in ambito ICT.
Le politiche di sicurezza sono approvate dalla direzione, pubblicate e comunicate ai dipendenti e alle parti esterne interessate e sono disegnate per includere controlli di sicurezza rilevanti per le attività aziendali di business e interne.
Le politiche e gli standard di sicurezza vengono rivisti periodicamente in ottica di un miglioramento continuo, tenendo conto delle risultanze dell'analisi dei rischi, dei cambiamenti di scenario nel contesto aziendale, di business e normativo, così come di nuove minacce o vulnerabilità.
Il sistema di gestione della continuità operativa SIA è certificato ISO 22301 e garantisce che l'organizzazione:

- sviluppa e mantiene piani, istruzioni e processi aggiornati che consentono di gestire tempestivamente emergenze e crisi;
- crea una struttura di documenti contenente la serie di piani predefiniti che descrivono in dettaglio come l'organizzazione gestisce un evento dannoso e in che modo garantisce la continuità delle sue attività in caso di un evento di emergenza;
- organizza regolari corsi di formazione sulla Business Continuity;
- pianifica regolari test di Business Continuity e Disaster Recovery;
- effettua periodicamente una revisione dell'intero sistema di gestione della continuità operativa per garantirne la conformità e l'adeguatezza in relazione a modifiche normative, organizzative, strategiche e legislative.

Vengono eseguiti controlli di base appropriati, compresi gli screening in fase di assunzione, per tutti i dipendenti. In tema di sicurezza del personale, SIA si impegna a promuovere la cultura della sicurezza attraverso un processo continuativo di formazione e aggiornamento. Tutto il personale riceve una formazione periodica sulla sicurezza delle informazioni adeguata alle proprie attività quotidiane e alla loro funzione.

Firmato digitalmente da:GIUSEPPE VIRGONE
Ruolo:AMMINISTRATORE UNICO
Organizzazione:PAGOPA S.P.A./15376371009
Data:23/12/2019 17:11:16