Accordo sul trattamento di dati personali e designazione a responsabile del trattamento ai sensi dell'articolo 28 del Regolamento (UE) 2016/679

("DPA")

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", con sede legale e domicilio fiscale in Roma, piazza Colonna 370, c.a.p. 00187, sede operativa in Roma, Via Sardegna 38, CAP 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, Alessandro Moricca, in qualità di "**Responsabile del trattamento** "

e

L'**Ente Creditore** (di seguito, "EC" o "Titolare del trattamento"), meglio identificato nella Lettera di Adesione alla piattaforma PagoPA già sottoscritta.

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 CHE

1) nell'esecuzione delle proprie attività PagoPA effettua il trattamento ("Trattamento") di dati, ivi compresi dati personali ai sensi del regolamento generale sulla protezione dei dati (2016/679/UE) (nel prosieguo denominati "Dati personali");
2) PagoPA agirà quale Responsabile del trattamento dei Dati personali ai sensi della "Normativa sulla protezione dei dati" e per quanto previsto delle Linee Guida AgID;
3) L'Ente Creditore ha sottoscritto con PagoPA la lettera di Adesione alla piattaforma PagoPA e conosce le Specifiche Attuative del Nodo dei Pagamenti ("SANP");

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

4) Le Parti intendono formalizzare nel presente documento sul trattamento dei dati ("Trattamento di dati personali e nomina a responsabile del trattamento" o "DPA") le condizioni in base alle quali condurrà le attività di trattamento sui Dati personali dalla stessa trattati.

CIÒ PREMESSO SI CONVIENE QUANTO SEGUE:

Definizioni

I termini utilizzati nel presente DPA hanno lo stesso significato di quelli definiti all'articolo 4 del Regolamento Generale sulla Protezione dei Dati (2016/679/UE) ("GDPR"), ad es. "Dati personali", "Trattamento", "Responsabile", "Violazione dei dati personali" e "Autorità di controllo".

I seguenti termini hanno il significato loro attribuito nel presente articolo:

(a) "Normativa sulla protezione dei dati" indica il GDPR, le leggi di adeguamento al GDPR e tutte le leggi, le normative e le raccomandazioni settoriali applicabili in relazione al trattamento dei dati personali.

Ogni altro termine usato con iniziale maiuscola e non definito nel presente DPA avrà il significato attribuito nel presente Accordo.

I Dati Personali trattati sono di esclusiva titolarità dell'EC e PagoPA si impegna a non farne alcun uso diverso da quello previsto nel presente atto di designazione.

1. Istruzioni seguite da PagoPA S.p.A. in qualità di Responsabile

1.1 La Appendice 1 (Dettagli del Trattamento) stabilisce: la natura, la finalità e l'oggetto del Trattamento previsto, le categorie di interessati coinvolte e il tipo di dati, e costituisce parte integrante del DPA.

1.2 Nello svolgimento delle attività di Trattamento, PagoPA agisce in conformità alla normativa sulla protezione dei dati.

1.3 PagoPA si impegna a dare immediata comunicazione all'EC se (a) a suo parere, intervengono violazioni sulla Normativa sul trattamento dei dati, se (b) PagoPA viene a conoscenza di una circostanza o di una modifica della Normativa sul trattamento dei dati applicabile che è probabile abbia sostanziali effetti negativi sulla capacità di PagoPA di adempiere ai propri obblighi di cui al presente DPA.

1.4 In particolare, ai sensi dell'art. 28 del GDPR, l'EC, avendo ritenuto PagoPA soggetto idoneo, nomina la stessa, la quale accetta, Responsabile del trattamento dei Dati Personali.

2. Divieto di divulgazione e riservatezza

2.1 PagoPA manterrà la riservatezza dei Dati personali e non li comunicherà in alcun modo a Terzi, né li diffonderà, salvo i casi in cui (i) ciò sia richiesto per

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

l'esecuzione del Trattamento, o (ii) ciò sia necessario per rispondere ad una richiesta di un'autorità pubblica competente e/o per rispettare un obbligo di legge o un interesse pubblico prevalente

2.2 PagoPA darà accesso ai Dati personali ai propri dipendenti solo nella misura necessaria per l'esecuzione dei trattamenti. PagoPA garantisce che ogni dipendente autorizzato ad avere accesso ai Dati personali trattati abbia ricevuto un'adeguata formazione in materia di protezione dei dati. Inoltre, PagoPA intraprende misure volte a garantire che qualsiasi dipendente che abbia accesso ai Dati personali esegua il trattamento di tali Dati personali nel pieno rispetto della normativa sulla protezione dei dati.

3. Sicurezza

3.1 Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, PagoPA mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: (a) la pseudonimizzazione e/o anonimizzazione e la 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; (d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Nel valutare l'adeguato livello di sicurezza, si tiene 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, a dati personali trasmessi, conservati o comunque trattati.

3.2 PagoPA garantisce, in particolare in termini di conoscenza specialistica, affidabilità e risorse, di mettere in atto misure tecniche e organizzative che soddisfino i requisiti della Normativa sulla protezione dei dati, anche per la sicurezza del trattamento. Le misure adottate da PagoPA sono specificate nella Appendice 2, che PagoPA dovrà rivedere qualora ciò sia richiesto da standard di settore o al fine di (ri-)assicurare un livello di sicurezza adeguato al rischio. Le misure tecniche e organizzative sono soggette a progresso e sviluppo tecnologico, e PagoPA ha facoltà di mettere in atto misure alternative adeguate. Queste non devono tuttavia avere un livello di sicurezza inferiore a quello fornito dalle misure specificate. Eventuali variazioni rilevanti devono essere documentate.

3.3 PagoPA attesta di aver conseguito la certificazione secondo lo standard di settore ISO/IEC 27001:2013 per la conformità del proprio Sistema di Gestione per la Sicurezza delle Informazioni. PagoPA si impegna a garantire la conformità ai controlli previsti dallo standard stesso durante l'intera durata del presente DPA ed a garantire di sottoporsi a revisioni ai sensi delle best practice di settore almeno con cadenza annuale. PagoPA su richiesta fornirà una copia del certificato conseguito.

3.4 E' onere esclusivo dell'EC valutare preventivamente se le misure di sicurezza

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

implementate da PagoPA sono idonee al trattamento di Dati personali. Nel caso in cui l'EC ritenga necessario adottare e/o implementare particolari misure di sicurezza per il trattamento di tali dati, l'EC informerà prontamente PagoPA. In particolare, è onere dell'EC informare preventivamente PagoPA in caso trattamento di Categorie Particolari di Dati Personali.

4. Sub Responsabili

4.1 Con il presente DPA, l'EC conferisce a PagoPA un'autorizzazione generale ad avvalersi di propri sub-responsabili nominati per iscritto, a condizione che PagoPA imponga loro, mediante un contratto o altro atto giuridico, i medesimi obblighi in materia di protezione dei dati contenuti nel presente DPA, prevedendo in particolare garanzie sufficienti della messa in atto di misure tecniche e organizzative adeguate per soddisfare i requisiti richiesti dalla Normativa sulla protezione dei dati, restando tuttavia PagoPA interamente responsabile verso l'EC dell'adempimento degli obblighi dei propri sub-responsabili. PagoPA è autorizzata, inoltre, a concludere clausole contrattuali tipo per conto dell'EC.

4.2 PagoPA si impegna a mettere a disposizione dell'EC l'elenco dei sub-responsabili nominati e a informare l'EC stesso di eventuali modifiche riguardanti l'aggiunta o la sostituzione dei soggetti a tal scopo individuati, dando così all'EC l'opportunità di opporsi a tali modifiche.

5. Trasferimento di dati personali in paesi terzi

5.1 PagoPA si impegna altresì a non eseguire alcun trasferimento di Dati Personali fuori dall'UE 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 sulla protezione dei dati (es mediante clausole contrattuali tipo).

5.2 Se e nella misura in cui l'eventuale meccanismo di trasferimento diventi parzialmente o integralmente non valido, PagoPA applicherà un'altra soluzione valida per il trasferimento dei dati al fine di evitare un trasferimento illecito. Nel caso in cui non sia disponibile alcun meccanismo di trasferimento valido, PagoPA non trasferirà dati personali.

6. Violazione della sicurezza dei Dati

6.1 PagoPA in caso di violazione accidentale o illecita dei sistemi dalla stessa gestiti che comporti la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati, procederà a: (i) informare l'EC, senza ingiustificato ritardo, e comunque entro 48 (quarantotto) ore dall'avvenuta conoscenza, a mezzo PEC dell'EC, come fornita dallo stesso; (ii) fornirà all'EC 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

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

porre rimedio alla violazione o attenuarne gli effetti pregiudizievoli; (iii) qualora non sia possibile fornire le suddette informazioni specifiche nel termine previsto, indicare all'EC i motivi del ritardo, fornendo comunque delle informazioni iniziali riferite alla violazione riscontrata ed utili all'EC ai fini della relativa notifica.

7. Assistenza

7.1 PagoPA per gli aspetti di propria competenza, fornirà supporto tecnico all'EC 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 GDPR, (iii) comunicazione di una violazione dei dati personali all'interessato ai sensi dell'art. 34 del GDPR, (iv) valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del GDPR, (v) consultazione preventiva ai sensi dell'art. 36 del GDPR.

7.2 PagoPA si impegna inoltre a garantire un'adeguata tutela dei diritti dell'interessato, supportando l'EC 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 da PagoPA, (i) comunicando all'interessato di indirizzare la propria richiesta al Titolare del trattamento; (ii) trasmettendo al Titolare del trattamento la richiesta.

8. Durata e scioglimento

8.1 Il Presente DPA ha durata pari alla durata del servizio SRTP – Service Provider del Creditore e cesserà all'atto del recesso dallo stesso. Per qualsiasi causa ciò avvenga, i Dati Personali, nonché le copie degli stessi eventualmente detenute da PagoPA, saranno eliminati definitivamente dal sistemi gestiti da PagoPA, salvo non siano necessari per ulteriori finalità legittime e salvi gli obblighi di legge ulteriori o diverso accordo tra le parti. La prosecuzione del trattamento sarà comunque oggetto di valutazione alla luce dell'art. 28 par. 3 lett. g) del Regolamento.

8.2 Il presente DPA potrà, ove necessario, costituire oggetto di accordi accessori e supplementari in forma scritta attraverso cui si potranno stabilire misure di sicurezza e organizzative aggiuntive qualora esse, risultino più idonee ad assicurare la tutela dei principi di privacy by design e by default avendo riguardo alle caratteristiche specifiche dell'EC.

9. Audit

9.1 PagoPA si rende disponibile con riguardo alle attività ispettive e di audit che l'EC 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'EC 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'EC (ii) tali attività dovranno essere concordate con PagoPA con un preavviso di almeno 10 (dieci) giorni lavorativi; (iii) tali attività dovranno essere svolte salvaguardando la normale operatività di PagoPA; (iv) l'uso delle informazioni di cui l'EC e l'eventuale soggetto incaricato dall'EC dovessero venire a conoscenza nel corso dell'audit dovrà

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

essere preventivamente regolamentato da un apposito accordo di confidenzialità; (v) e qualora tali attività comportino un costo non ragionevole per PagoPA, le parti si accordino per un equo compenso che l'EC corrisponda a PagoPA per lo svolgimento di tali attività. Per costi non ragionevoli per PagoPA si intendono, spese emergenti e lucro cessante che possano derivare da prolungate interferenze nella normale operatività di PagoPA ovvero da richieste tecniche e organizzative che si rendano necessarie ai soli fini dello svolgimento dell'audit.

9.2 PagoPA ad ogni modo condividerà su richiesta dell'EC le risultanze degli audit e processi di certificazione cui si sottopone e l'EC potrà richiedere di partecipare a tali attività di audit programmate da PagoPA. In ogni caso, in deroga a quanto previsto sopra nei punti (i) (ii) e, qualora sussistano circostanze eccezionali o di particolari problematiche dell'EC (a titolo esemplificativo, violazioni di dati personali, ispezioni o richieste da parte del Garante per la Protezione dei dati personali), PagoPA si renderà pienamente disponibile ad attività ispettive e audit effettuate dal EC, direttamente o per il tramite di un altro soggetto da questo incaricato.

10. Risarcimento

10.1 L'EC si impegna, nella misura massima consentita dalla legge, a manlevare e tenere indenne PagoPA da ogni danno diretto e indiretto, 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 da un'Autorità di controllo o da un'altra autorità pubblica competente e/o da un interessato qualora tale azione sia conseguenza anche di una sola violazione da parte dell'EC e/o suoi agenti e/o sub-contraenti della normativa in materia di trattamento dei dati personali.

10.2 L'EC sosterrà tutti i costi legati a una Violazione della sicurezza dei dati, qualora tale violazione sia causata da, o attribuibile a, un inadempimento dello stesso.

10.3 Allo stesso modo PagoPA terrà indenne l'EC in relazione a tutte le pretese, i procedimenti o le azioni promossi da un'Autorità di controllo o da un'altra autorità pubblica competente e/o da un interessato in relazione al Trattamento condotto da PagoPA e/o dai suoi Sub Responsabili.

10.2 PagoPA sosterrà tutti i costi legati a una Violazione della sicurezza dei dati, qualora tale violazione sia causata da, o attribuibile a, un inadempimento della stessa.

11. Conservazione e cancellazione

11.1 PagoPA 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 al DPA e comunque nel pieno rispetto del principio di limitazione della conservazione, ferma restando l'osservanza della normativa vigente per i documenti fiscali, contabili e legali, nonché le Linee Guida AgID.

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

11.2 Al termine del periodo di conservazione, PagoPA provvederà a distruggere in modo sicuro i Dati personali in suo possesso (e.g. macero certificato e/o cancellazione digitale), salvo nella misura il diritto applicabile preveda altrimenti.

12. Obbligo di rinegoziazione, modifiche e recesso

12.1 PagoPA informerà tempestivamente i soggetti coinvolti nel trattamento su qualsiasi circostanza rilevante, ivi compresi a titolo esemplificativo e non esaustivo variazioni significative nei servizi di Trattamento erogati da PagoPA;

12.2 PagoPA è libera in ogni momento di modificare in via unilaterale il presente DPA, dandone comunicazione all'EC a mezzo pec. Tali modifiche avranno efficacia a partire dal giorno novantesimo successivo a quello in cui le modifiche saranno comunicate o rese note, fermo restando in capo all'EC il diritto di recesso a seguito di una tale modifica unilaterale da parte della Società.

13. Informazioni generali

13.1 Tutte le comunicazioni, le conferme e le altre dichiarazioni rese in relazione al presente DPA rivolte alla Società devono essere inviate in forma scritta a mezzo PEC all'indirizzo dpo@pec.pagopa.it.

13.2 Ogni qual volta il presente DPA faccia riferimento alla forma scritta, sarà sufficiente la forma elettronica, come ad esempio la posta elettronica certificata.

13.3 Il presente DPA è disciplinato e interpretato secondo il diritto italiano.

13.4 Eventuali controversie sorte dal presente DPA o in relazione allo stesso devono essere demandate al foro di Roma, Italia.

[segue, Appendice 1 / Appendice 2]

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

APPENDICE 1 DETTAGLI DEL TRATTAMENTO

1. Natura, finalità e oggetto del trattamento

PagoPA tratta i Dati personali per l'esecuzione del Servizio SRTP – Service Provider del Creditore.
Inoltre, PagoPA tratta i Dati personali per prevenire o risolvere problemi tecnici, nonché fornire assistenza all'EC. Tutte le altre forme di Trattamento dei Dati personali avverranno in conformità al presente DPA.

Sono incluse le seguenti attività di trattamento:

- Conservazione dei dati (registrazione, inserimento in registri, archiviazione o altrimenti conservazione dei Dati personali);
- Accesso ai dati (copia, estrazione, visualizzazione, comunicazione o altrimenti accesso ai Dati personali);
- Analisi dei dati (investigazione, test, studio, interpretazione, organizzazione o altrimenti analisi dei Dati personali).

2. Categorie di Interessati

Cittadini

3. Tipologia di Dati personali trattati

Dati personali comuni (dati anagrafici e relativi alla posizione debitoria)

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

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

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,

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

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

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

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;

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

- 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) già nelle fasi iniziali di sviluppo;

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

- 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.

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009