POLITICA IN MATERIA DI TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI

Revisione 06 del 26/05/2026

	EMESSO	APPROVATO
Funzione	**Responsabile Trattamento Dati Personali**	**Amministratore Delegato**
Data	26/05/2026	26/05/2026
Firma		

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

PA Digitale SpA

POLITICA IN MATERIA DI TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI

Revisione 06 del 26/05/2026

INDICE

1. OBIETTIVO 4
2. NORMATIVA DI RIFERIMENTO 4
3. DEFINIZIONI 4
4. CAMPO DI APPLICAZIONE 6
5. ORGANIZZAZIONE PER LA PROTEZIONE E IL TRATTAMENTO DEI DATI PERSONALI 7
   5.1 Titolare del trattamento dei dati personali 7
   5.2 Incaricati/Soggetti autorizzati al trattamento 8
   5.3 Responsabile esterno del trattamento 9
   5.4 Amministratori di Sistema 11
   5.5 Area Compliance 12
   5.6 Data Protection Team di Gruppo 13
   5.7 Responsabile della Protezione dei Dati (DPO) 13
   5.8 Funzioni aziendali (in corso di definizione) 14
6. POLITICA PER LA PROTEZIONE DEI DATI PERSONALI 14
   6.1 Raccolta e trattamento delle informazioni 14
   6.2 Registro dei trattamenti 15
      6.2.1 Registro del Titolare 15
      6.2.2 Registro delle categorie di attività trattate 15
   6.3 Informative 16
   6.4 Scelta e consenso 16
   6.5 Trasferimento di dati personali 17
   6.6 Integrità dei dati 17
   6.7 Sicurezza dei dati 18
      6.7.1 Sistemi di autenticazione informatica 18
      6.7.2 Segretezza e custodia delle credenziali di autenticazione 19
      6.7.3 Password 19
      6.7.4 Disattivazione delle credenziali di autenticazione 19
      6.7.5 Sospensione delle sessioni di lavoro 19
      6.7.6 Firewalling e software antivirus 19
      6.7.7 Aggiornamento dei programmi per elaboratore 19
      6.7.8 Backup e ripristino dei dati 19
      6.7.9 Business Continuity in HA 19
      6.7.10 Strumenti elettronici per la protezione da accessi abusivi 20
      6.7.11 Supporti removibili 20
      6.7.12 Controllo e custodia degli atti e dei documenti 20

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

6.7.13 Controllo e custodia degli atti e dei documenti contenenti dati particolari 20
6.7.14 Controllo degli accessi agli archivi contenenti dati particolari 20
6.7.15 Controllo degli accessi alle sedi della Società.....20
6.7.16 Controllo degli accessi ai Data Center 21
6.8 Analisi dei rischi 21
6.9 Conservazione dei dati.....21
6.10 Violazione dati personali 21
7. DIRITTI DEGLI INTERESSATI.....22
7.1 I diritti subordinati a una richiesta espressa dell'interessato (Artt. 15-21 GDPR) 22
7.2 I diritti non subordinati a una richiesta dell'interessato.....23
7.3 Esercizio dei diritti dell'Interessato e tempi di riscontro 23
8. CONTROLLO E CONFORMITÀ.....24
9. DATI DI CONTATTO 24
10. FUNZIONIGRAMMA PA DIGITALE SPA 25

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

PA Digitale SpA

POLITICA IN MATERIA DI TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI

Revisione 06 del 26/05/2026

1. OBIETTIVO

Il documento della Politica in materia di trattamento e protezione dei dati personali (di seguito "*Policy*") viene redatto da PA Digitale S.p.A. (di seguito PA Digitale) per rappresentare l'applicazione delle regole e dei principi in ossequio a quanto stabilito dalla Normativa di riferimento (vedi Punto 2), per:

- proteggere e salvaguardare i dati personali e confidenziali;
- disciplinare il trattamento dei dati personali e confidenziali;
- stabilire i principi di buona gestione per i dati personali e confidenziali;
- garantire che tutti i trattamenti avvengano nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche;
- assicurare la riservatezza delle informazioni riferite alla gestione del personale e dei collaboratori;
- assicurare la riservatezza delle informazioni riferite ai clienti, ai fornitori e a tutti coloro che hanno rapporti con PA Digitale.

2. NORMATIVA DI RIFERIMENTO

- Regolamento UE n. 679/2016 Regolamento Generale sulla Protezione dei dati (di seguito anche "Regolamento");
- Decreto Legislativo n. 196/2003 "Codice in materia di protezione dei dati personali" (di seguito "Codice Privacy"), dagli allegati al Codice così come modificati dalla Legge 25 ottobre 2017, n. 163 Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017;
- Decreto Legislativo 101/2018 di adeguamento della normativa nazionale
- Provvedimenti, Linee Guida e Pareri emessi dall'Autorità Garante per la protezione dei dati personali (di seguito "Garante Privacy"), dal Comitato Europeo per la Protezione dei Dati e dal Garante Europeo della Protezione dei Dati (GEPD);
- Norma ISO/IEC 27001:2022 "Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni - Requisiti";
- Norma ISO/IEC 27018:2019 "Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors".
- Norma UNI EN ISO 9001:2015 "Sistemi di Gestione per la Qualità – Requisiti"

3. DEFINIZIONI

Ai fini di una agevole comprensione il documento della *Policy*, si riportano alcune delle definizioni contenute nell'art. 4 del GDPR:

- "**dato personale**" anche definito come **"Informazioni Personali Identificabili (PII)"**: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato", anche definito come "PII Principal"); si considera

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

- "**trattamento**": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- "**limitazione di trattamento**": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- "**profilazione**": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- "**pseudonimizzazione**": il trattamento dei dati personali in modo tale che gli stessi non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, purché le medesime siano conservate separatamente e soggette a misure tecniche e organizzative tali da assicurare che i dati non siano attribuiti ad una persona fisica identificata o identificabile;
- "**archivio**": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- "**titolare del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento dei dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri
- "**responsabile del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare;
- "**destinatario**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi (non sono considerati destinatari quelle autorità pubbliche che possono ricevere comunicazioni nell'ambito di una specifica indagine conformemente al diritto dell'Unione Europea);
- "**terzo**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

trattamento e le persone autorizzate al trattamento dei dati personali che operano sotto l'autorità diretta del titolare o del responsabile;

- "**consenso dell'interessato**": qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- "**violazione dei dati personali**": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
- "**autorità di controllo**": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 GDPR;
- "**dati genetici**": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- "**dati biometrici**": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- "**dati relativi alla salute**": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

4. CAMPO DI APPLICAZIONE

La presente *Policy* si applica a tutti i dati personali di persone fisiche (tra cui, a titolo esemplificativo e non esaustivo, quelli afferenti a dati dei dipendenti, dei clienti, dei fornitori e dei soggetti terzi che operano in qualità di persona fisica) nonché a qualsiasi informazione di carattere personale o con le caratteristiche di dato personale ricevute da Partners Tecnici e Commerciali. Particolare riguardo viene riservato al trattamento delle informazioni personali identificabili (PII). Il documento si applica ai dati personali trattati da PA Digitale e ha lo scopo di garantire che il trattamento analogico, automatizzato o cartaceo di dati personali, effettuato da PA Digitale anche per il tramite di soggetti autorizzati ai sensi degli articoli 28 e 29 del GDPR, avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché, della dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale, secondo le disposizioni vigenti in materia di protezione dei dati e in materia di amministrazione digitale.
PA Digitale adotta tutte le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato, così da assicurare il rispetto dei principi di liceità, correttezza e trasparenza nel trattamento dei dati personali e assicura l'adozione di adeguate e preventive misure di sicurezza, idonee ad evitare situazioni di rischio e di non conformità o di alterazione dei dati.

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

5. ORGANIZZAZIONE PER LA PROTEZIONE E IL TRATTAMENTO DEI DATI PERSONALI

All'interno di PA Digitale sono individuati i ruoli e i compiti dei soggetti autorizzati a trattare i dati personali, attività consentita esclusivamente ai Designati, Incaricati/Soggetti autorizzati, Responsabili del trattamento, eventuali Sub-Responsabili del trattamento e Amministratori di Sistema.
Il trattamento effettuato da soggetti a ciò non preventivamente e formalmente autorizzati è illecito.
PA Digitale ha altresì nominato un Responsabile della Protezione dei Dati (Data Protection Officer - di seguito DPO) esterno, di comprovata esperienza e in possesso di competenze giuridiche e informatiche, di risk management e di analisi dei processi.
Infine, per una più attenta ed efficace gestione della Privacy, il modello identifica ulteriori ruoli all'interno dell'Organizzazione Privacy, sebbene non espressamente previsti dal Regolamento (Data Protection Team, Delegati Privacy, Privacy SPOC, ecc.).

5.1 Titolare del trattamento dei dati personali

È considerato Titolare del trattamento ai sensi della presente *Policy*, l'ente giuridico nel suo complesso, stante la sua autonomia decisionale in merito alle finalità e ai mezzi del trattamento dei dati personali degli Interessati.
Il Titolare del trattamento è colui che determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
In funzione dell'Organizzazione aziendale di riferimento e ai fini specifici dell'Organizzazione Privacy, Il Rappresentante Legale è il "Data Controller" identificabile a livello di Presidente del Consiglio di Amministrazione o Amministratore Delegato.
PA Digitale adotta tutte le misure tecniche e organizzative atte a garantire che il trattamento dei dati personali sia effettuato conformemente alla normativa vigente.
PA Digitale, tramite il supporto del DPO e dell'Area Compliance, nei casi previsti dalla legge, provvede a:

- assolvere ogni obbligo di comunicazione, interpello o notificazione all'Autorità Garante per la Privacy;
- cooperare, su richiesta, con l'Autorità Garante per la Privacy nell'esecuzione dei suoi compiti ai sensi dell'art. 31 GDPR;
- richiedere a tale Autorità ogni necessaria autorizzazione al trattamento dei dati personali, ove necessario;
- adottare, per quanto di competenza, le misure necessarie a garantire la protezione dei dati personali, anche per quanto riguarda il processo di digitalizzazione;
- adottare una procedura di valutazione d'impatto privacy (Data Privacy Impact Assessment) per le attività di trattamento dati al fine di attivare e mantenere

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

aggiornato il Registro delle attività di trattamento effettuate all'interno di PA Digitale - in formato cartaceo o elettronico - svolte sotto la propria responsabilità, conformemente a quanto prescritto dall'art. 30 n. 1 del GDPR;
- assicurare l'informazione e la formazione del personale sul tema della tutela della protezione dei dati personali;
- nominare i Designati, Incaricati autorizzati, Responsabili del trattamento dati personali impartendo loro le necessarie istruzioni per la corretta gestione e protezione dei dati personali.

Il Titolare del trattamento è tenuto a effettuare, nei confronti di tutti coloro che svolgono per suo conto attività di trattamento, le verifiche e i controlli atti a garantire il rispetto degli obblighi previsti dalle disposizioni vigenti in materia.

5.2 Incaricati/Soggetti autorizzati al trattamento

Ai sensi dell'art. 29 GDPR, il Titolare individua - con apposite nomine e quali persone autorizzate al trattamento medesimo - tutti i dipendenti, collaboratori e consulenti, che intervengono, in relazione all'esercizio delle rispettive mansioni e competenze, nell'esecuzione dei trattamenti. Le persone "autorizzate al trattamento" dei dati personali agiscono, dunque, sotto l'autorità del Titolare del trattamento. ***Gli Incaricati/Soggetti autorizzati al trattamento hanno livelli di accesso ai dati differenziato rispetto al ruolo responsabilità ricoperto (need to know need to use) e garantito dal sistema di identificazione del profilo utente e riconoscimento password gestito dai Sistemi Informativi (minimo privilegio).***
Ogni persona autorizzata (che viene debitamente nominata in fase di assunzione e ciclicamente formata), opera in base alle istruzioni ricevute e comunque non deve divulgare, trasmettere, comunicare o diffondere a terzi dati personali oggetto di eventuali trattamenti operati, se non nei limiti delle istruzioni specificamente impartite.
Pertanto, al fine della corretta gestione dei dati in trattamento, l'Incaricato Autorizzato dovrà:
- trattare i dati in modo lecito e secondo correttezza e secondo le prescrizioni nel Regolamento UE 679/16 e nella normativa nazionale;
- verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Responsabile del trattamento dei dati; attenersi alle procedure operative e alle istruzioni di lavoro impartite dal Responsabile del Trattamento dei dati del Settore.
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza esplicita autorizzazione del Titolare e del Responsabile del trattamento;
- mantenere la massima riservatezza sui dati oggetto di trattamento;
- osservare ai sensi dell'art. 32 del Regolamento UE 679/16 che il trattamento dei dati avvenga mediante l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio;

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

- informare tempestivamente il Responsabile del Trattamento dei dati del Settore di appartenenza in caso di incidenti o problematiche relative alla sicurezza dei dati trattati.

5.3 Responsabile esterno del trattamento

Per Responsabili esterni si intendono tutti i soggetti "non dipendenti" da PA Digitale, che effettuano trattamenti sulle banche dati dello stesso, per suo conto e nel suo interesse. I trattamenti effettuati da parte del Responsabile esterno del trattamento sono disciplinati, ai sensi dell'art. 28 GDPR, da un contratto o altro atto giuridico che individui la durata, la natura, la finalità del trattamento, il tipo di dati personali e le categorie degli interessati, le responsabilità affidate al Responsabile, gli obblighi e i diritti del Titolare. In particolare, il Responsabile, sebbene non in via esaustiva, avrà questi compiti e attribuzioni:

- garantire che il trattamento dei dati personali di cui è Titolare del Trattamento la Società e di cui venga a conoscenza con l'attività svolta avvenga in conformità a quanto previsto dalla vigente normativa e dalle presenti istruzioni;
- aggiornare periodicamente l'elenco dei trattamenti dei dati personali; tenere il Registro delle attività di trattamento dei dati, come previsto da art. 30 del GDPR, in formato elettronico, di tutte le categorie di attività relative al trattamento svolte per conto della Società;
- mettere in atto, ai sensi dell'art. 32 del GDPR, tutte le misure tecniche e organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento effettuato in esecuzione del Contratto;
- provvedere affinché vengano rigorosamente adottate tutte le misure idonee a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati con l'attività di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per le quali i dati sono stati raccolti;
- verificare periodicamente lo stato di applicazione del Regolamento Europeo 2016/679, nonché la corretta applicazione, il buon funzionamento dei sistemi e, ai sensi dell'art.32 del GDPR, delle adeguate misure tecniche e organizzative adottate per la tutela dei dati personali e la conformità alle indicazioni dell'Autorità Garante e del Titolare del Trattamento;
- tenere i dati personali, trattati in esecuzione del Contratto, separati rispetto a quelli eventualmente trattati per conto di altre terze parti applicando una segregazione fisica e logica, ove possibile;
- garantire la stretta osservanza dell'incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati personali di titolarità della Società non coerente con gli specifici trattamenti svolti in adempimento del Contratto e le relative suddette finalità;
- garantire la portabilità dei dati personali trattati in esecuzione del Contratto, ai sensi dell'art. 20 del GDPR, assicurando che gli stessi possano essere trasmessi in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo automatico;

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

- assistere il Titolare del Trattamento per quanto concerne gli obblighi di notifica e ogni altra comunicazione verso il Garante, ove dovute;
- tenendo conto della natura del trattamento, assistere il Titolare del Trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del Trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento Europeo 2016/679;
- mettere a disposizione del Titolare del Trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa vigente in particolare l'adozione delle adeguate misure organizzative e di sicurezza ai sensi art. 32 del GDPR;
- comunicare al Titolare del Trattamento qualsiasi variazione della situazione oggettiva o delle sue proprie caratteristiche soggettive, tali da compromettere il corretto espletamento dei compiti descritti nella presente;
- provvedere alla nomina del/i proprio/i amministratore/i di sistema, in adempimento a quanto previsto dal provvedimento del Garante della Privacy del 27/11/2008, pubblicato in G.U. n. 300 del 24/12/2008, ove ne ricorrano i presupposti, curando, altresì, l'applicazione di tutte le ulteriori prescrizioni contenute nel suddetto provvedimento;
- Informare il Titolare del Trattamento senza ingiustificato ritardo e comunque non oltre le 72 ore dal momento in cui ne è venuto a conoscenza (art. 33 del GDPR), eventuali violazioni dei dati personali (data breach) adottando, di concerto con lo stesso, nuove adeguate misure di sicurezza atte a circoscrivere gli effetti negativi dell'evento e a ripristinare la situazione precedente;
- Predisporre e aggiornare un registro che dettagli, in caso di eventuali data breach, la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze e le nuove misure di sicurezza implementate;
- supportare il Titolare del Trattamento durante la stesura della valutazione dell'impatto (ove prevista) dei trattamenti stabiliti sulla protezione dei dati personali, nei casi in cui un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- supportare il Titolare del Trattamento durante le fasi di consultazione con l'autorità di controllo, qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento possa presentare un rischio elevato in assenza di misure adottate dal Titolare del Trattamento per attenuare il rischio;
- ottemperare tempestivamente alle eventuali richieste inoltrate dal Titolare del Trattamento al fine di rendere conforme il trattamento dei dati posto in essere in esecuzione del Contratto, agli eventuali provvedimenti emessi dal Garante Privacy in materia di trattamento di dati personali;
- avvertire prontamente la PA Digitale, entro tre (3) giorni lavorativi, in merito alle eventuali richieste degli interessati che dovessero pervenire al Responsabile, inviando copia delle istanze ricevute all'indirizzo PEC: privacy.pec.padigitalespa@legalmail.it e collaborare al fine di garantire il pieno esercizio da parte degli interessati di tutti i diritti previsti dall'articolo 7 del Codice;

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

- avvisare immediatamente, e comunque entro tre (3) giorni lavorativi, il Titolare del Trattamento di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante o di quella Giudiziaria o di Pubblica Sicurezza eventualmente ricevuta, inviando copia delle istanze all'indirizzo PEC: privacy.pec.padigitalespa@legalmail.it per concordare congiuntamente il riscontro.

5.4 Amministratori di Sistema

PA Digitale designa, tra gli autorizzati al trattamento dei dati personali, i propri Amministratori di Sistema, con un apposito atto corredato di specifiche istruzioni operative, la cui copia viene conservata dall'Area Compliance. ***Gli Amministratori di Sistema sono dunque quelle persone autorizzate al trattamento a cui è stato conferito il compito di sovrintendere alle risorse del Sistema Informativo e di consentirne l'utilizzazione. Il ruolo ricoperto da tali soggetti li pone nella condizione di avere accesso ad ampie categorie di dati personali, per l'espletamento dei loro compiti. L'amministratore di sistema è la figura chiave nella gestione, manutenzione e protezione dei sistemi informativi: l'attività di audit del suo operato assume pertanto grande importanza per verificare che svolga la sua funzione secondo quanto richiesto dalla norma.***
Le attività di audit si differenziano e si adattano in funzione dei processi organizzativi da controllare e delle strutture informative esistenti.
L'Amministratore di Sistema ha dunque il compito di:

- porre in atto le adeguate misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio con riferimento all'adeguatezza della sicurezza informatica dei sistemi informativi e informatici nel trattamento dei dati.
- sovrintendere al sistema operativo e agli elaboratori e sistemi di base dati e di consentirne l'utilizzo.
- classificare le banche dati e impostare/organizzare un sistema complessivo di trattamento dei dati delle operazioni richiamate dall'art. 4 comma 2 del Regolamento UE 679/16 che riguardi esclusivamente la sola registrazione (intesa come memorizzazione su dispositivi hardware) e la cancellazione;
- attenersi alle Procedure / Istruzioni (previste nei sistemi di gestione certificati) per la tutela dei dati e del loro trattamento come stabilito dall'art. 22, 24, 25 e 32 del Regolamento UE 679/16 e dal Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (e ss. mm. ii.);
- operare in stretta sinergia con il Responsabile del trattamento nominato dal Titolare del trattamento;
- predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte Sua (nella sua qualità di "amministratore di sistema"); tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni dovranno comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e dovranno essere conservate per un congruo periodo, non inferiore a sei mesi;

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

- segnalare tempestivamente al Titolare del Trattamento e al Responsabile del trattamento eventuali violazioni o presunte irregolarità per la successiva segnalazione al Garante entro 72 ore (data breach);
- stilare periodicamente, almeno su base annuale, una Relazione in merito alla sicurezza del trattamento informatico dei dati, segnalando eventuali punti di miglioramento con riguardo all'adeguatezza delle misure tecniche e organizzative ai sensi dell'art. 32 del GDPR.

5.5 Area Compliance

L'Area Compliance è un'Area di Staff che, tra le altre, ricopre le funzioni esclusivamente operative di Ufficio Privacy e opera in stretta collaborazione con il Titolare, ***con il Data Protection Team*** e con il DPO, coordinando le attività volte a garantire la corretta osservanza della normativa vigente, nonché il documento della Policy. Ha il compito di segnalare le problematiche relative alla protezione dei dati personali, fornendo quando possibile la prima necessaria consulenza in tema di protezione dei dati per le eventuali segnalazioni ai soggetti competenti, in un'ottica di debita valutazione preliminare dei rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. L'Area Compliance coordina le attività relative alle misure necessarie a favorire l'osservanza della *Policy* e delle altre disposizioni vigenti relative alla protezione dei dati e svolge i seguenti compiti:

- cura l'aggiornamento del programma software utilizzato per gestire l'organizzazione e le attività necessarie a garantire la protezione dei dati personali e l'adeguamento alla normativa di riferimento e a produrre e gestire la documentazione relativa (Registri dei trattamenti, nomine, analisi dei rischi, ecc.);
- rileva l'eventuale bisogno formativo o informativo in tema di normativa sulla protezione dei dati personali e, quando necessario, predispone specifici piani formativi;
- opera a stretto contatto con il DPO, fornendogli tutto il supporto necessario all'espletamento delle attività in carico a quest'ultimo.

Nei confronti del DPO e del Data Protection Team, il Responsabile dell'Area Compliance assume il ruolo di Referente Privacy Aziendale. È persona formata, almeno per gli elementi essenziali e fondamentali, sulla normativa privacy e relativi obblighi e responsabilità. Si occupa di curare la costruzione di processi di Privacy. Le attività sono:

- ***Raccolta di informazioni utili a riscostruire le varie attività;***
- ***Gestione dei registri dei trattamenti;***
- ***Aggiornamento delle policy aziendali in materia di privacy***
- ***Gestione del rischio***
- ***Supporto all'esecuzione delle analisi di impatto (DPIA)***
- ***Esecuzione delle attività di audit interno, per quanto di competenza***
- ***Cura l'aggiornamento costante del Privacy Dive della sua Azienda***

Per eventuali necessità, consulta il Data Protection Team di Gruppo.

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

5.6 Data Protection Team di Gruppo

Svolge le attività di Ufficio Privacy di Gruppo, collabora per le attività di gestione dei processi di privacy di Gruppo, cura le attività di front-office e back-office relativa alle richieste delle aziende del gruppo, analizza e condivide i processi di Privacy di Gruppo. Si occupa di:

- ***Essere il punto di contatto tra le aziende ed il DPO di gruppo***
- ***Identificare le scoperture e definire le aree di miglioramento in ambito Privacy***
- ***Valutare i rischi e analizzare le priorità di intervento***
- ***Pianificare le azioni di mitigazione in base alle priorità***
- ***Effettuare check periodici sulla conformità ai requisiti normativi (GDPR)***
- ***Supportare i referenti nei processi di raccolta informativa, nelle attività di gestione dei trattamenti, di gestione del rischio;***
- ***Supervisionare e curare l'aggiornamento delle policy e delle informative in materia di Privacy di Gruppo;***
- ***Supportare l'esecuzione delle analisi di impatto (DPIA);***
- ***Supportare i referenti nelle attività di audit interno***

5.7 Responsabile della Protezione dei Dati (DPO)

Il Responsabile della Protezione dei Dati (DPO) è un organo di Staff che opera in stretta collaborazione con il Titolare coordinando le attività volte a garantire la corretta osservanza della normativa vigente, nonché il documento della Policy. La sua responsabilità principale è quella di valutare e organizzare la gestione del trattamento di dati personali in azienda, affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali. Secondo l'art. 39 del Regolamento europeo sulla protezione dei dati personali, i principali compiti del DPO sono:

- ***informare e fornire consulenza al titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;***
- ***sorvegliare l'osservanza del Regolamento, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;***
- ***fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;***
- ***cooperare con l'autorità di controllo;***
- ***fungere da punto di contatto con l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a***

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

qualunque altra questione;

- ***monitorare l'evoluzione del quadro normativo in materia di privacy***

Il DPO è anche l'Organo di PA Digitale designato a ***poter*** ricevere e gestire le segnalazioni di violazione o presunta violazione dei dati personali ed eventualmente a notificare la violazione al Garante (nel caso in cui PA Digitale sia Titolare del trattamento) o al Cliente Titolare del Trattamento (nel caso in cui PA Digitale sia stato nominato Responsabile esterno del trattamento) entro i termini stabili dal GDPR. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

5.8 Funzioni aziendali (in corso di definizione)

Nell'ambito dell'attuazione delle misure previste dal Gruppo controllante, allo stato attuale sono in corso di definizione i seguenti ruoli:

- ***I Delegati Privacy, quali soggetti incaricati della gestione interna e "decentralizzata" del trattamento dei dati personali, coerentemente agli incarichi ricoperti e alle mansioni che svolgono e operano sulla base di specifiche istruzioni.***
- ***I Privacy SPOC, quali figure operative interne a ogni Area, individuate e nominate dal Delegato Privacy come unici interlocutori per garantire l'effettiva applicazione delle disposizioni in materia di protezione dei dati personali per le attività svolte nella propria Area***

6. POLITICA PER LA PROTEZIONE DEI DATI PERSONALI

6.1 Raccolta e trattamento delle informazioni

PA Digitale adotta le misure e le precauzioni per verificare che le informazioni contenenti dati personali siano pertinenti, accurate, complete e attuali come è necessario per gli scopi per i quali devono essere utilizzate.
I trattamenti di dati personali effettuati si conformano al principio di minimizzazione dei dati ai sensi dell'art. art. 5, co. 1, lett. c), del Regolamento in base al quale la raccolta e il successivo trattamento di dati personali avvengono in maniera da ridurre al minimo indispensabile l'utilizzo di dati personali identificativi degli Interessati.
Il trattamento deve essere attuato in modo da assicurare il rispetto dei diritti e della dignità dell'interessato.
Qualora alcune operazioni di trattamento, ovvero processi o fasi di processo, non necessitino la visualizzazione in chiaro di dati personali e identificativi degli Interessati, le medesime operazioni di trattamento devono essere effettuate mediante dati resi anonimi o, quantomeno, codificati.
I dati che, anche a seguito di verifica, risultino eccedenti o non pertinenti o non necessari, non possono essere utilizzati salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.
I soggetti autorizzati delegati al trattamento sono tenuti a verificare periodicamente

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

l'esattezza e l'aggiornamento dei dati personali, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'Interessato fornisce di propria iniziativa.

6.2 Registro dei trattamenti

PA Digitale individua, come elementi fondamentali delle politiche di protezione dei dati personali, l'analisi dei trattamenti e la distribuzione dei compiti e delle responsabilità attribuite a coloro che sono incaricati di trattare dati personali. PA Digitale tiene un Registro delle attività di trattamento dei dati personali di riferimento, costantemente aggiornato, che evidenzia i diversi livelli di responsabilità attribuiti nell'ambito del trattamento. In particolare, PA Digitale ha predisposto e mantiene aggiornato:

- un Registro delle "attività di trattamento" svolte in quanto Titolare del trattamento
- un Registro delle "categorie delle attività di trattamento" svolte in quanto Responsabile esterno del trattamento, formalmente incaricato dai Clienti Titolari del trattamento.

I Registri sono tenuti dal Titolare, con uno specifico programma software, disponibile on-line e accessibile mediante credenziali di autenticazione, in possesso unicamente dall'Area Compliance e dal Titolare del trattamento.

6.2.1 Registro del Titolare

Il Registro delle attività trattate dal Titolare del trattamento reca le seguenti informazioni:

- il nome e i dati di contatto del Titolare, Responsabile, eventuali Incaricati autorizzati;
- le finalità del trattamento;
- la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- le eventuali categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- l'eventuale trasferimento di dati personali verso un Paese terzo o una organizzazione internazionale;
- ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- il richiamo alle misure di sicurezza tecniche e organizzative del trattamento adottate.

6.2.2 Registro delle categorie di attività trattate

Il Registro delle categorie di attività trattate svolte in quanto Responsabile esterno del trattamento, reca le seguenti informazioni:

- il nome e i dati di contatto del Responsabile del trattamento e degli Incaricati autorizzati;
- le categorie di trattamenti effettuati per ciascun Titolare;
- l'eventuale trasferimento di dati personali verso un Paese terzo o una organizzazione internazionale;
- il richiamo alle misure di sicurezza tecniche e organizzative del trattamento adottate.

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

Il Registro è tenuto sia in forma scritta che in formato elettronico e viene messo, su richiesta, a disposizione dell'Autorità Garante Privacy.

6.3 Informative

PA Digitale si adopera affinché tutte le operazioni di trattamento avvengano conformemente a quanto richiesto dall'art. 13 del Regolamento. L'Informativa deve essere sempre resa agli interessati all'atto della raccolta dei dati, anche quando non è necessario richiedere il loro consenso al trattamento. Per il rispetto di quanto indicato nell'Informativa devono essere adottati i seguenti principi:

- non è consentito effettuare trattamenti di dati personali senza aver fornito preventivamente l'Informativa;
- non è consentito effettuare trattamenti di dati personali per finalità diverse da quelle indicate nell'Informativa già resa agli interessati; ulteriori finalità possono essere integrate nell'Informativa previa condivisione con i Responsabili del trattamento;
- non è consentita la comunicazione dei dati alle categorie dei soggetti terzi diverse da quelle indicate nell'Informativa. Eventuali ulteriori categorie di soggetti ritenute necessarie ai fini del trattamento dei dati possono essere inserite nell'Informativa previa condivisione con i Responsabili del trattamento.

PA Digitale si impegna affinché sia previsto un aggiornamento periodico e/o una review delle varie informative sia cartacee (i.e. informativa dipendenti, informativi clienti, informativi fornitori, etc.) sia elettroniche (i.e. informative siti web).

6.4 Scelta e consenso

PA Digitale s'impegna a rispettare l'obbligo di raccolta del consenso come stabilito dagli artt. 6 e 7 del Regolamento. Il consenso è validamente prestato quando:

- è preceduto da un'Informativa corretta e completa;
- è espresso liberamente;
- è riferito univocamente a un determinato trattamento;
- è documentato per iscritto in relazione al tipo di dati raccolti (ad es. uso di dati sensibili).

Ai sensi dell'art. 6, comma 1, lett. b) – f), del Regolamento, il consenso non è dovuto quando:

- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- il trattamento è necessario per il perseguimento del legittimo interesse del Titolare

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei dati personali, in particolare se l'Interessato è un minore.

6.5 Trasferimento di dati personali

PA Digitale s'impegna ad adottare le misure necessarie per garantire che i trasferimenti di dati personali siano conformi con la normativa applicabile anche nel caso in cui questo dovesse avvenire da parte di soggetti terzi che agiscono in qualità di sub-appaltatori. Il trasferimento di Dati personali all'esterno dell'Unione Europea può avvenire, in presenza di almeno una delle seguenti condizioni (Artt. 44, 45 e 46 GDPR):

- una decisione di adeguatezza della Commissione Europea;
- clausole tipo di protezione ("Model Contract Clauses") dei dati adottate dalla Commissione Europea;
- clausole contrattuali tra il Titolare del trattamento e il Titolare/Responsabile destinatario dei Dati personali nel paese terzo approvate dall'autorità di controllo;
- adozione di un codice di condotta o meccanismo di certificazione e contestuale impegno del Titolare/Responsabile destinatario dei Dati personali di applicare le garanzie adeguate.

Il trasferimento di Dati personali verso un paese terzo o un'organizzazione internazionale sarà inoltre possibile nel caso in cui:

- l'interessato abbia prestato esplicitamente il consenso dopo essere stato informato dei possibili rischi;
- il trasferimento sia necessario per l'esecuzione di un contratto concluso tra l'interessato e il titolare ovvero di misure precontrattuali adottate su istanza dell'interessato;
- il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare e un terzo a favore dell'interessato;
- il trasferimento sia necessario per importanti motivi di interesse pubblico.

6.6 Integrità dei dati

PA Digitale, ai sensi dell'art. 5 del Regolamento, effettua i trattamenti di dati personali adeguando il loro operato ai seguenti criteri generali:

- ciascun trattamento deve avvenire in modo lecito, trasparente e secondo correttezza;
- i dati trattatati devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, e utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
- i dati trattati devono essere esatti e, se necessario, aggiornati;
- i dati trattati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- i dati trattati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

- i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («disponibilità, integrità e riservatezza»).

6.7 Sicurezza dei dati

PA Digitale s'impegna ad adottare, nei limiti del possibile, le misure di sicurezza necessarie e adeguate affinché i dati e le informazioni personali siano protetti da perdita, uso improprio, accesso non autorizzato, divulgazione, alterazione o distruzione oltre che le ragionevoli verifiche affinché tali misure risultino costantemente aggiornate.
In base a quanto disposto dagli articoli 24 e 32 del Regolamento, PA Digitale ha adottato un programma di sicurezza che prevede l'adozione di misure in linea con i seguenti principi:

- garantire che siano trattati i dati personali per impostazione predefinita necessari per ogni specifica finalità del trattamento (Security e Privacy by Default - art. 25 GDPR);
- attuare in modo efficace i principi di protezione dei dati e integrare nel trattamento fin dalla progettazione le necessarie garanzie al fine di tutelare i diritti degli interessati (Security e Privacy by Design - art. 25 GDPR);
- assicurare, in caso di violazione dei dati personali, la comunicazione verso gli interessati e il Garante Privacy nei modi e nei tempi del Regolamento;
- effettuare per quei trattamenti che presentano rischi elevati per i diritti e la libertà degli interessati la valutazione d'impatto nei modi e nei tempi previsti dal Regolamento;
- garantire adeguata formazione specialistica sulle tematiche di sicurezza IT;
- adottare misure tecniche, organizzative e di sicurezza adeguate, nonché adeguati meccanismi di controllo della costante conformità di tali misure nel tempo e ne dispone il costante aggiornamento (Accountability - Art. 5 GDPR);
- documenta le attività svolte per garantire che i trattamenti siano effettuati in conformità alla normativa applicabile e tiene tale documentazione a disposizione per eventuali accessi del Garante (Accountability - Art. 5 GDPR).

Ciò premesso, e in aggiunta a quanto precede, PA Digitale si impegna a trattare i dati personali solo qualora siano implementati i presidi di seguito descritti, gestiti con il Sistema di Gestione per la Sicurezza delle Informazioni di PA Digitale, secondo quanto previsto dalla Norma ISO/IEC 27001:2022.

6.7.1 Sistemi di autenticazione informatica

PA Digitale adotta credenziali di autenticazione che consistono in un codice per l'identificazione dell'utente (UserID) associato a una parola chiave riservata conosciuta solamente dal medesimo (password). A ogni utente sono assegnate e associate individualmente una o più credenziali per l'autenticazione.

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

6.7.2 Segretezza e custodia delle credenziali di autenticazione

PA Digitale invita gli utenti a conservare con la massima riservatezza le proprie credenziali di autenticazione e a non condividerle con altri utenti. Tutti gli utenti sono responsabili del corretto e lecito utilizzo delle di credenziali di autenticazione assegnate.

6.7.3 Password

PA Digitale utilizza password composte almeno da un numero di caratteri non inferiore da quello richiesto, volta per volta, per legge e con caratteristiche tali da rendere difficoltoso l'eventuale tentativo di individuazione. La password è modificata con cadenza periodica in funzione della tipologia di dati trattati (i.e. dati particolari: sensibili, giudiziari, etc.), al fine di ridurre il rischio che utenti non autorizzati o malintenzionati riescano a individuarla.

6.7.4 Disattivazione delle credenziali di autenticazione

PA Digitale assicura che le credenziali di autenticazione sono disattivate in caso di mancato utilizzo per un periodo temporale di almeno 6 (sei) mesi. La disattivazione delle credenziali avviene anche nel caso in cui il possessore non abbia più necessità di utilizzarle a causa del cambiamento delle proprie mansioni lavorative ovvero dell'interruzione del rapporto di lavoro.

6.7.5 Sospensione delle sessioni di lavoro

PA Digitale obbliga gli utenti ad attivare il blocco del proprio computer quando si allontanano dalla propria postazione di lavoro anche per periodi di tempo limitati. Il blocco avviene comunque in maniera automatica dopo un lasso temporale di inattività prestabilito.

6.7.6 Firewalling e software antivirus

Il sistema informativo di PA Digitale e le Procedure Software messe a disposizione dei propri clienti e Partners come servizio (Cloud Computing in modalità SaaS) sono protetti contro gli accessi abusivi provenienti da reti pubbliche di comunicazioni. Tutti gli elaboratori sono dotati di software antivirus aggiornato allo scopo di limitare il rischio di intrusione di virus e di programmi dannosi.

6.7.7 Aggiornamento dei programmi per elaboratore

PA Digitale provvede periodicamente all'installazione degli aggiornamenti (release) per risolvere le problematiche emerse nel rispetto delle indicazioni e delle politiche in uso.

6.7.8 Backup e ripristino dei dati

PA Digitale attua azioni in grado di garantire la disponibilità delle informazioni in linea con le prescrizioni di legge, nonché verifiche periodiche dell'effettiva leggibilità e integrità delle informazioni salvate.

6.7.9 Business Continuity in HA

PA Digitale garantisce un servizio di Business Continuity in HA completamente automatizzato in tutti i suoi processi e monitorato da personale tecnico specializzato 24

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

ore su 24, 7 giorni su 7, 365 giorni all'anno. Attività di verifica e test di funzionamento dei sistemi sono svolte regolarmente per la massima sicurezza di dati e sistemi.

6.7.10 Strumenti elettronici per la protezione da accessi abusivi

La rete informatica utilizzata da PA Digitale, sia internamente che per il collegamento al Data Center ove risiedono gli strumenti elettronici di trattamento dei dati, sia di PA Digitale stessa che dei propri clienti, è protetta da specifici strumenti quali firewall, sistemi di Intrusion prevention e detection, in grado di ridurre il rischio di accessi abusivi.

6.7.11 Supporti removibili

PA Digitale adotta specifici protocolli per la custodia, cancellazione e distruzione sicura sia dei supporti removibili utilizzati per il salvataggio o il trasferimento di dati personali sia degli elaboratori, fissi e portatili, dismessi o non più utilizzati.

6.7.12 Controllo e custodia degli atti e dei documenti

PA Digitale impartisce indicazioni affinché gli atti e i documenti cartacei contenenti dati personali siano controllati e custoditi dagli utenti durante tutte le operazioni di trattamento. Tutto il personale di PA Digitale è, in ogni caso, sempre responsabile dell'utilizzo e della custodia degli atti e dei documenti contenti dati personali. Al termine delle operazioni di trattamento, gli atti e i documenti cartacei devono essere archiviati in armadi/cassetti muniti di serratura. Ove possibile, analoghe misure vanno adottate nel caso in cui l'utente si allontani temporaneamente dalla propria postazione.

6.7.13 Controllo e custodia degli atti e dei documenti contenenti dati particolari

PA Digitale impartisce indicazioni, affinché gli atti e i documenti cartacei contenenti dati particolari siano utilizzati esclusivamente da personale espressamente incaricato al loro trattamento. Tali incaricati sono responsabili dell'utilizzo e della custodia degli atti e dei documenti che contengono tali categorie di dati, in particolare, devono garantire che altri Incaricati non autorizzati non abbiano accesso a informazioni che esulino dal proprio ambito di trattamento. Al termine delle operazioni di trattamento, gli atti e i documenti cartacei devono essere archiviati in armadi muniti di serratura.

6.7.14 Controllo degli accessi agli archivi contenenti dati particolari

Solamente gli incaricati a ciò autorizzati hanno la possibilità di accedere agli archivi per lo svolgimento delle proprie mansioni lavorative. Al termine della giornata lavorativa e dopo l'orario di chiusura degli uffici, l'accesso agli archivi deve avvenire previa identificazione, anche mediante strumenti elettronici (ad es. badge).

6.7.15 Controllo degli accessi alle sedi della Società

L'accesso alle sedi di PA Digitale è consentito al solo personale dipendente/collaboratori o a personale esterno autorizzato. L'accesso alle Sedi, da parte dei dipendenti è possibile solo mediante strumenti elettronici (ad es. badge) di identificazione, ovvero attraverso identificazione da parte degli addetti alla sorveglianza, o del personale preposto alla

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

reception. Particolare restrizione è riservata all'accesso ai locali contenenti infrastrutture per l'elaborazione delle informazioni (Sale CED).

6.7.16 Controllo degli accessi ai Data Center

Solamente gli utenti autorizzati dalla Direzione di PA Digitale possono accedere ai Data Center ove risiedono gli strumenti elettronici di trattamento e le banche dati contenenti dati personali, di cui PA Digitale è Titolare e/o Responsabile del trattamento.

6.8 Analisi dei rischi

L'adeguatezza delle misure di sicurezza adottate e riportate al paragrafo precedente è stata valutata mediante una specifica procedura di analisi dei rischi, la quale prevede di fare una valutazione del livello di rischio al quale ogni trattamento incluso nel Registro dei trattamenti, è soggetto, sulla base delle possibili minacce e dei relativi impatti. L'analisi dei rischi è stata implementata con uno specifico applicativo software, prodotto da una Società riconosciuta sul mercato, che ha scelto, come modello per l'implementazione, le linee guida rivolte alle Piccole e Medie Imprese, in materia di sicurezza per il trattamento dati personali, emesse da parte di *ENISA - Agenzia Europea per la sicurezza delle reti e delle informazioni*.

6.9 Conservazione dei dati

PA Digitale adotta le misure per conservare le informazioni personali solo ed esclusivamente per il tempo necessario a soddisfare gli scopi per cui sono stati raccolti e comunque in maniera non eccedente rispetto a quanto richiesto da obblighi di legge. I dati personali pertanto possono essere oggetto di conservazione, sia analogica che digitale, solo ed esclusivamente per il tempo previsto dalla normativa vigente e successivamente sottoposti a scarto d'archivio e distruzione, secondo quanto definito dalla specifica istruzione di lavoro aziendale in materia. I tempi di conservazione saranno regolati da idonee procedure operative e comunicati agli Interessati da apposite informative e secondo le indicazioni contenute in Provvedimenti del Garante ovvero indicate dalla normativa in vigore.

6.10 Violazione dati personali

PA Digitale, qualora ritenga che sia avvenuta una violazione di dati personali e che sia probabile che da tale violazione possano derivare rischi per i diritti e le libertà degli interessati, seguendo quanto disciplinato dalla Procedura Operativa Interna "Procedura per Data Breach", provvede alla notifica della violazione:

- al Garante Privacy, nel caso in cui PA Digitale sia Titolare del trattamento
- al Titolare del trattamento, nel caso in cui PA Digitale sia stata quest'ultimo nominata Responsabile del trattamento dati.

La notifica avviene senza ingiustificato ritardo, entro i tempi previsti dal Regolamento e secondo una specifica procedura operativa interna.
Per violazione dei dati personali si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dalla società. I principali rischi per i diritti e le libertà degli interessati conseguenti a una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale;
- decifratura non autorizzata della pseudonimizzazione (quando prevista);
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (dati doganali).

7. DIRITTI DEGLI INTERESSATI

I diritti attribuiti dal GDPR agli interessati si dividono in due categorie: (1) i diritti che necessitano di una richiesta espressa dell'interessato; (2) i diritti ai quali la normativa collega un obbligo del titolare in modo autonomo dalla ricezione di una previa richiesta dell'interessato.

7.1 I diritti subordinati a una richiesta espressa dell'interessato (Artt. 15-21 GDPR)

Il processo per la gestione dei diritti esercitati dagli Interessati mediante espressa richiesta è riconducibile alle seguenti fasi principali, indicate nel dettaglio all'interno della Procedura Operativa Interna "Procedura per gestione richieste degli Interessati":

- ricezione della richiesta;
- gestione della richiesta;
- riscontro all'interessato e archiviazione.

Le modalità di gestione del predetto processo sono disciplinate nell'apposita Procedura tempo per tempo aggiornata e pubblicata nel Documentale.
I principali diritti che il GDPR garantisce all'interessato e che lo stesso può esercitare mediante richiesta sono i seguenti:

- **Diritto di Accesso**: l'Interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di Dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai Dati personali che comprendono i Dati personali conferiti dall'Interessato, i Dati personali osservabili generati in esecuzione del contratto, i termini del trattamento compreso il periodo di conservazione previsto.
- **Diritto di Rettifica**: l'Interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei Dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei Dati personali incompleti, anche fornendo una dichiarazione integrativa.

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

- **Diritto di Cancellazione**: l'Interessato ha il diritto di ottenere dal titolare del trattamento, se sussistono i motivi indicati dal GDPR, la cancellazione dei Dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i Dati personali, salvo che ne sia impedito dall'obbligo di espletamento di tutti gli adempimenti di legge.
- **Diritto di Limitazione di trattamento**: l'Interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento quando si verificano le ipotesi previste dall'art. 18 del GDPR;
- **Diritto di Opposizione / Revoca**: l'Interessato ha il diritto di opporsi o revocare il consenso in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei Dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del GDPR, compresa la profilazione. Il Titolare del trattamento si astiene dal trattare ulteriormente i Dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
- **Diritto alla Portabilità**: L'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i Dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali Dati a un altro titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti qualora il trattamento è effettuato con mezzi automatizzati.

Infine, nel caso di esercizio dei diritti di rettifica, cancellazione e/o limitazione del trattamento da parte dell'Interessato, il Titolare provvede anche a effettuare la comunicazione ai destinatari interessati prevista dall'articolo 19 del GDPR.

7.2 I diritti non subordinati a una richiesta dell'interessato

Pur in assenza di richiesta da parte dell'Interessato, il Titolare garantisce che allo stesso sia fornita idonea informativa al momento della raccolta dei suoi Dati personali presso lo stesso o, se i Dati non sono raccolti direttamente presso l'Interessato, entro i seguenti termini:

- entro un termine ragionevole dall'ottenimento dei Dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i Dati personali sono trattati;
- nel caso in cui i Dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;
- nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei Dati personali.

7.3 Esercizio dei diritti dell'Interessato e tempi di riscontro

L'Interessato ha la facoltà di esercitare i propri diritti secondo le modalità e nei limiti previsti dal GDPR. PA Digitale si impegna a fornire all'Interessato le informazioni relative all'azione intrapresa riguardo a una richiesta senza ingiustificato ritardo e, comunque, al

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

più tardi entro 30 giorni dal ricevimento della richiesta stessa. Se la richiesta dell'Interessato sarà presentata mediante mezzi elettronici, le informazioni saranno fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'Interessato.
Tali diritti possono essere esercitati dall'Interessato attraverso l'invio di mail/PEC all'indirizzo privacy.pec.padigitalespa@legalmail.it oppure tramite comunicazione scritta a PA Digitale S.p.A., specificando l'oggetto della richiesta, domiciliato presso la sede della Società sita in Via Leonardo da Vinci 13 - 26854 Pieve Fissiraga (Lodi) oppure utilizzando i meccanismi previsti dai sistemi di mail marketing.
Una volta ricevuta la richiesta, Il Titolare del trattamento dati (tramite l'Area Compliance) non può rifiutarsi di soddisfare la richiesta dell'Interessato, salvo che dimostri di non essere in grado di identificare l'interessato.

8. CONTROLLO E CONFORMITÀ

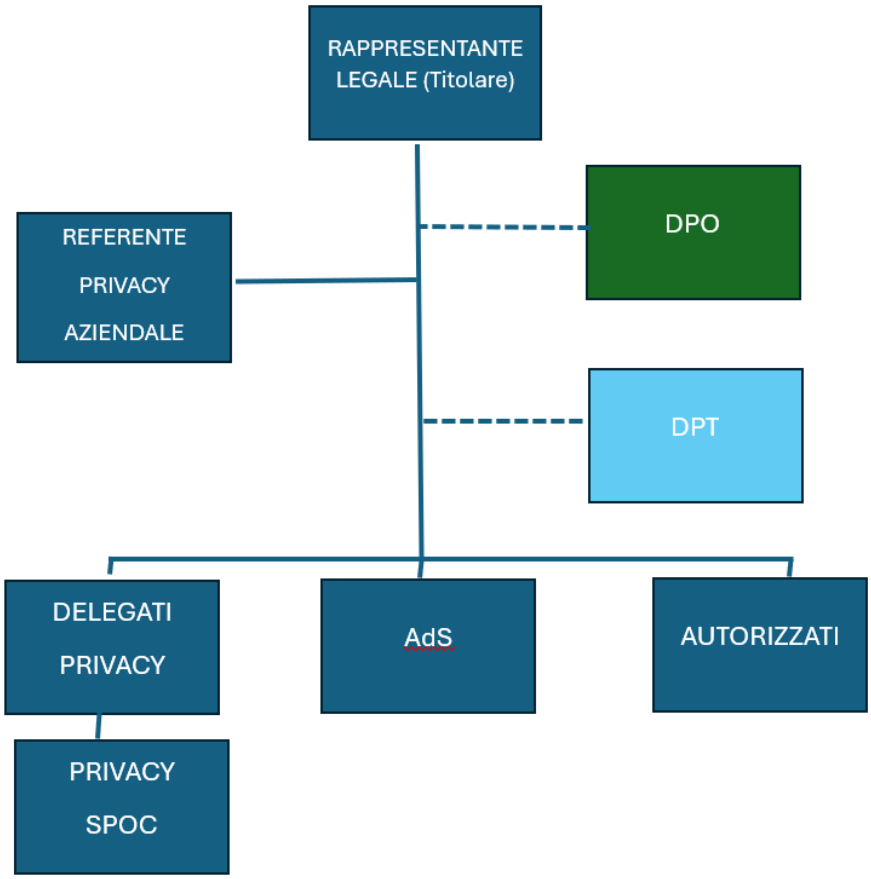
PA Digitale ha stabilito procedure per controllare il rispetto dei principi previsti dal Regolamento. È responsabilità di tutto il personale di PA Digitale conoscere, comprendere e rispettare questa Politica e i suoi contenuti. La mancata osservanza potrebbe comportare rischi significativi per PA Digitale e può subordinare ciascun individuo ad azioni disciplinari, fino al licenziamento o all'interruzione del rapporto professionale.

9. DATI DI CONTATTO

Domande o dubbi sull'interpretazione o sulle modalità di applicazione della presente Policy possono essere rivolti scrivendo a Area Compliance, al seguente indirizzo PEC: privacy.pec.padigitalespa@legalmail.it. Più in generale, i dati di contatto di PA Digitale sono riportati sul sito www.padigitale.it/privacy. In merito al Responsabile della protezione dei dati (DPO), quest'ultimo potrà essere contattato ai seguenti indirizzi:
e-mail: dpo@padigitale.it

PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.

10. FUNZIONIGRAMMA PA DIGITALE SPA



PA DIGITALE Spa – Autore Pa Digitale – È fatto divieto la copia, la riproduzione e qualsiasi uso di questo documento che non sia stato espressamente autorizzato - PA Digitale non sarà pertanto ritenuta responsabile di eventuali imprecisioni, errori od omissioni contenute all'interno del presente documento.