REGOLAMENTO INTERNO PER LA PROTEZIONE DEI DATI PERSONALI (PRIVACY POLICY) DI AMIA

Approvato dal CdA in data 3 NOVEMBRE 2025 con Deliberazione n. 37/2025

Sommario

1. Scopo, campo di applicazione e governance del documento

Il presente Regolamento di AMIA (di seguito "la Società" o "AMIA") definisce il modello organizzativo e operativo per la protezione dei dati personali, in ottemperanza al Regolamento (UE) 2016/679 (GDPR), al D.Lgs. 196/03 (Codice Privacy) come novellato dal D.Lgs. 101/2018, e ai provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali. La protezione dei Dati Personali è considerata una priorità per tutelare i diritti e le libertà fondamentali degli interessati, tra cui utenti dei servizi e dipendenti. Il trattamento dei dati deve avvenire secondo le migliori prassi internazionali.

Gli obiettivi principali sono:

- definire il quadro normativo e organizzativo di riferimento;
- individuare ruoli, responsabilità e flussi informativi;
- stabilire linee guida generali e raccordo con i regolamenti tematici.

Il presente documento, unitamente ai regolamenti e alle procedure interne che disciplinano i processi correlati (ad es. esercizio dei diritti degli interessati, gestione delle violazioni dei dati personali – data breach, utilizzo degli strumenti informatici, conservazione/retention dei dati), costituisce la politica sulla protezione dei dati e si applica a tutti i trattamenti, automatizzati e non, effettuati dalla Società in qualità di Titolare o di Responsabile, inclusi quelli svolti tramite fornitori e altri soggetti terzi.

Il regolamento è approvato dal Consiglio di Amministrazione di AMIA, previa validazione del DPO. Il documento entra in vigore alla data di approvazione ed è vincolante per tutto il personale e per i soggetti che trattano dati per conto di AMIA.

2. Definizioni Chiave

Ai fini del presente Regolamento si applicano le seguenti definizioni, derivanti dal GDPR e dalle normative correlate.

Termine	**Definizione**
Autorità di Vigilanza	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR (ad es. in Italia il "Garante per la protezione dei Dati Personali").

Categorie Particolari di Dati Personali	Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale (art. 9 c. 1 GDPR).
Contitolare	Titolare del trattamento che determina congiuntamente ad altro Titolare del trattamento finalità e mezzi del trattamento dei Dati Personali (art. 26 GDPR).
Dati Giudiziari	Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza riferite a una persona fisica (art. 10 GDPR).
Dato personale	Qualsiasi informazione direttamente o indirettamente riguardante una persona fisica identificata o identificabile ("interessato")
GDPR (General Data Protection Regulation)	Regolamento (EU) 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/EC (Regolamento Generale sulla Protezione dei Dati)
Interessato	Persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a 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.
Persona autorizzata al Trattamento	Persona fisica che compie operazioni di trattamento sotto l'autorità diretta del Titolare o del Responsabile, tipicamente dipendenti o collaboratori.

Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali per valutare determinati aspetti personali (es. rendimento professionale, situazione economica, interessi, affidabilità, comportamento).
Pseudonimizzazione	Trattamento dei dati personali in modo che non possano più essere attribuiti a un interessato specifico senza l'uso di informazioni aggiuntive conservate separatamente e soggette a misure tecniche e organizzative.
Referente di area	Il soggetto individuato in ciascuna area che mantiene aggiornate le informazioni sui trattamenti di competenza e le trasmette al Referente Privacy e al DPO.
Referente Privacy	La figura designata dal Titolare che coordina, a livello operativo, l'attuazione del sistema privacy, cura il consolidamento del Registro dei trattamenti e i flussi informativi interni.
Responsabile del Trattamento	La persona fisica o giuridica che tratta i Dati Personali per conto del Titolare del Trattamento (art. 28 GDPR).
RPD/DPO	Responsabile per la Protezione dei Dati Personali (Data Protection Officer) della Società.
Titolare del Trattamento	La persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento dei Dati Personali.
Trattamento dei dati	Qualsiasi operazione o insieme di operazioni applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'uso, la comunicazione, la cancellazione o la distruzione.
Valutazione d'Impatto sulla	Valutazione d'impatto delle operazioni di Trattamento previste

protezione dei dati (DPIA)	sulla protezione dei Dati Personali (art. 35 GDPR)..
Violazione dei Dati Personali (Data Breach)	Una 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 (art. 4 c. 12 GDPR).

3. Principi Fondamentali del Trattamento dei Dati Personali

AMIA si impegna ad applicare i seguenti principi fondamentali che disciplinano il Trattamento dei Dati Personali, in ottemperanza all'Art. 5 GDPR:

- Liceità, Correttezza e Trasparenza: I dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Il trattamento è lecito quando è basato su una motivazione valida (es. consenso, adempimento contrattuale o obbligo legale). La trasparenza richiede che le comunicazioni siano facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro.
- Limitazione delle Finalità: I dati devono essere raccolti per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità.
- Minimizzazione dei Dati: I dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità. Vanno raccolti e trattati solo i Dati Personali necessari.
- Accuratezza (Esattezza): I dati devono essere precisi e, ove necessario, aggiornati. Le Società non devono trattare Dati Personali inesatti e devono adottare misure ragionevoli per correggerli o cancellarli.
- Limitazione della Conservazione: I dati 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.
- Integrità e Riservatezza: I dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei Dati Personali, mediante misure tecniche e organizzative adeguate, per evitare Trattamenti non autorizzati, illeciti, perdite accidentali, distruzione o danneggiamento.
- Responsabilizzazione (Accountability): Il Titolare del trattamento è responsabile della conformità ai principi sopra indicati e il rispetto degli stessi deve essere facilmente dimostrato in qualsiasi momento attraverso l'adozione di normative interne e processi adeguati (es. tenuta del registro dei trattamenti, DPIA).

4. Modello Organizzativo Privacy: Ruoli e Responsabilità

Il Modello Organizzativo Privacy di AMIA identifica chiaramente i ruoli e le responsabilità, sia in qualità di Titolare che in qualità di Responsabile del Trattamento per conto terzi.

4.1 Titolare del Trattamento

AMIA, nella persona del Legale Rappresentante, è il Titolare del Trattamento e ha la responsabilità ultima di determinare le finalità e i mezzi del trattamento. Il Consiglio di Amministrazione (CdA) o il soggetto da esso delegato, è titolare dei poteri decisionali e rappresentativi necessari per garantire il rispetto e la piena attuazione della normativa. Principali responsabilità del Titolare:

- Definire le finalità legittime e i mezzi del Trattamento di Dati Personali.
- Garantire che la protezione dei dati personali sia assicurata by design e by default fin dalle fasi di progettazione dei processi e dei sistemi.
- Mantenere un Registro delle attività di Trattamento dei Dati Personali svolte sotto la sua responsabilità.
- Attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.
- Notificare tempestivamente all'Autorità di controllo competente qualsiasi violazione dei dati personali (data breach) e, se del caso, informare gli interessati, nei termini previsti dal GDPR.
- Effettuare la Valutazione d'Impatto (DPIA) quando previsto o necessario.
- Nominare il DPO e assicurare la sua indipendenza nell'esercizio delle funzioni.

4.2 Responsabile della Protezione dei Dati (RPD/DPO)

Il DPO è nominato dal Consiglio di Amministrazione e funge da parte essenziale del sistema di controllo interno. Il DPO deve possedere un'approfondita conoscenza delle normative e delle pratiche nazionali ed europee sulla protezione dei dati, nonché delle operazioni di Trattamento svolte dalla Società. I suoi compiti includono:

- Informare il CdA, la Direzione e il personale riguardo agli obblighi del GDPR e delle normative applicabili.
- Monitorare la conformità al GDPR, anche promuovendo iniziative di sensibilizzazione e formazione specifica.
- Fornire consulenza in merito alla DPIA e monitorarne l'esecuzione.
- Fungere da punto di contatto per gli Interessati (ad esempio per l'esercizio dei diritti).

- Fungere da punto di contatto per l'Autorità di Vigilanza per questioni connesse al Trattamento, inclusa la consultazione preventiva.
- Essere coinvolto sistematicamente nella fase più precoce possibile di tutte le questioni riguardanti la protezione dei Dati Personali.
- Sottoporre a revisione la DPIA per verificare il corretto livello di rischio residuo e, se del caso, identificare ulteriori misure compensative.
- Fornire consulenza sui tempi di conservazione dei dati, in particolare quando il trattamento è basato sul legittimo interesse del Titolare.

4.3 Referente Privacy

Figura designata dal Titolare per coordinare, a livello operativo, l'attuazione del sistema di gestione privacy all'interno della Società.

In particolare:

- collabora con il DPO e con le diverse aree aziendali;
- cura l'aggiornamento e il consolidamento del Registro dei trattamenti;
- gestisce i flussi informativi interni (es. segnalazioni, aggiornamenti, data breach), secondo i regolamenti e le procedure interne;
- mantiene e aggiorna l'elenco dei Responsabili del trattamento (art. 28) e l'elenco delle persone autorizzate al trattamento (artt. 29 e 32, c. 4), assicurandone la coerenza con gli atti di nomina/istruzioni;
- supporta le funzioni competenti nell'allineamento tra regolamento generale e regolamenti/procedure tematiche.

Opera sulla base di specifico atto di designazione o incarico interno.

4.4 Referenti di area

I Referenti di area sono soggetti individuati all'interno di ciascuna area di AMIA, con il compito di garantire la corretta gestione dei trattamenti di dati personali nell'ambito delle attività di competenza.

In particolare, ciascun referente:

- mantiene e aggiorna le informazioni relative ai trattamenti della propria area, nel Registro dei Trattamenti;
- assicura la comunicazione periodica di eventuali modifiche o nuove attività di trattamento al Referente Privacy e al DPO, secondo le modalità definite nei regolamenti e procedure interne;

- collabora alla gestione di segnalazioni privacy, data breach e richieste di esercizio dei diritti che coinvolgano la propria area;
- promuove la corretta applicazione delle istruzioni e delle misure organizzative impartite dal Titolare o dal Referente Privacy;
- partecipa, se richiesto, alle attività di formazione e aggiornamento promosse dalla Società in materia di protezione dei dati.

I referenti di area sono individuati nell'organigramma aziendale; l'elenco aggiornato è conservato a cura del Referente Privacy.

4.5 Persone autorizzate al Trattamento (art. 29 e 32 c. 4 GDPR)

Il personale autorizzato comprende dipendenti, collaboratori e altri soggetti che, sotto l'autorità del Titolare, eseguono operazioni di trattamento o vi accedono. Tali persone devono essere adeguatamente istruite. Gli obblighi del personale autorizzato sono:

- Operare nel rispetto della normativa esterna e interna vigente e nell'ambito esclusivo dei profili di autorizzazione assegnati.
- Effettuare il trattamento nell'osservanza delle istruzioni fornite dal Titolare.
- Assicurare che i dati siano trattati in modo lecito, corretto, limitato alla finalità, esatto e sicuro.
- Assicurare la completa riservatezza sui dati di cui sia venuto a conoscenza.
- Comunicare tempestivamente al DPO o al referente Privacy (se presente) situazioni di anomalie sopravvenute.

4.6 Responsabili del Trattamento (art. 28 GDPR)

AMIA si avvale di Responsabili del trattamento esterni che offrono garanzie sufficienti (competenze, affidabilità, misure di sicurezza) per tutelare i dati personali. Il rapporto con ciascun Responsabile è regolato da un contratto scritto (Data Protection Agreement – DPA) che dettaglia materia, durata, natura, finalità del trattamento, tipologia dei dati trattati e obblighi delle parti. Il Responsabile tratta i dati solo su istruzione documentata del Titolare e deve ottenere l'autorizzazione scritta del Titolare per nominare sub-responsabili.

4.7 AMIA come Responsabile del Trattamento

La Società opera anche in qualità di Responsabile del Trattamento per conto di altri Titolari. Questa attività è regolata da un apposito atto di nomina. AMIA è Responsabile del Trattamento, in particolare, per i seguenti Enti Titolari: Cral Verona Verona, Comune di Verona (anche in veste di Ente di Bacino

di Verona Città), Consiglio di Bacino Verona Nord (Comuni di Villafranca di Verona (VR) e di Grezzana (VR)).

In virtù di tale ruolo, e nel rispetto della nomina, AMIA si impegna a:

- Trattare i Dati Personali in conformità ai principi del GDPR e alle istruzioni documentate ricevute dal Titolare.
- Mantenere un Registro delle attività di Trattamento specifico per ciascun Titolare per conto del quale sta agendo.
- Attuare adeguate misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio.
- Assistere il Titolare nell'adempimento dei suoi obblighi, inclusa la risposta alle richieste relative ai diritti degli Interessati e la conduzione di Valutazioni d'Impatto (DPIA) e consultazioni preventive.
- Dare immediata notifica al Titolare di eventuali violazioni dei Dati Personali (Data Breach) che coinvolgano i dati trattati per suo conto.
- Garantire che il personale autorizzato abbia un adeguato obbligo di riservatezza.
- Nominare un Sub-Responsabile con contratto scritto che imponga obblighi di protezione dei dati almeno equivalenti a quelli previsti nell'atto di nomina di AMIA.

Il processo di verifica ed eventuale accettazione della nomina a Responsabile da parte di terzi prevede l'analisi e il supporto del Referente Privacy, del DPO ed eventualmente dell'area IT/CED aziendale in relazione agli obiettivi di sicurezza.

4.8 Contitolarità del Trattamento (art. 26 GDPR)

Quando AMIA, operando come Titolare, determina congiuntamente ad altro Titolare le finalità e i mezzi del trattamento, deve stipulare un accordo scritto (DPA) che definisca le rispettive responsabilità. L'accordo deve essere formalizzato per iscritto e il contenuto essenziale deve essere messo a disposizione degli Interessati.

4.9 Flussi informativi e reporting

AMIA adotta un modello di gestione del Registro dei trattamenti suddiviso per area aziendale, in coerenza con la propria struttura organizzativa.

Ciascuna area, tramite il proprio referente interno, è responsabile del mantenimento e dell'aggiornamento delle informazioni relative ai trattamenti di competenza e garantisce la trasmissione

periodica degli aggiornamenti al Referente Privacy e al DPO, secondo le modalità definite nelle procedure interne.

Il Referente Privacy assicura il consolidamento dei registri delle singole aree nel Registro dei trattamenti del Titolare, curandone la coerenza complessiva e la trasmissione al DPO per le verifiche periodiche.

5. Requisiti Chiave del Titolare del Trattamento

5.1 Basi giuridiche del trattamento (art. 6 GDPR)

Il Titolare deve identificare una base legittima (fondamento di liceità) per il Trattamento prima che questo sia iniziato. Il Trattamento dei Dati Personali è lecito quando ricorre almeno una delle seguenti condizioni:

- È basato sul consenso accordato dall'interessato per una o più finalità specifiche. Il consenso deve essere libero, specifico, informato e inequivocabile.
- È necessario per l'esecuzione di un contratto di cui l'interessato è parte o di attività precontrattuali.
- È necessario per adempiere a un obbligo legale al quale è soggetta la Società.
- È necessario per il perseguimento del legittimo interesse della Società o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

5.2 Categorie particolari e dati giudiziari (artt. 9–10 GDPR; norme nazionali)

Il trattamento di Categorie Particolari di Dati Personali (dati sensibili) è vietato, eccetto quando si verifica uno dei casi specifici, come il consenso esplicito dell'Interessato o la necessità per motivi di interesse pubblico rilevante. Il trattamento di Dati Giudiziari è consentito solo se autorizzato da una norma di legge o di regolamento che preveda garanzie appropriate.

5.3 Informativa e diritti degli interessati

Gli interessati vengono adeguatamente informati in modo chiaro e comprensibile (informativa privacy) sulle caratteristiche del trattamento e sui loro diritti. L'informativa è concisa, trasparente, facilmente accessibile, in linguaggio semplice. Il Titolare facilita l'esercizio dei diritti degli interessati e risponde alle richieste entro un mese dal ricevimento (prorogabili di altri due mesi in casi complessi, previa comunicazione).

I diritti riconosciuti all'Interessato includono:

- Diritto di Accesso: Ottenere la conferma del trattamento e accedere ai dati personali e alle informazioni ad essi collegate (finalità, categorie, destinatari, periodo di conservazione).

- Diritto di Rettifica: Ottenere senza ingiustificato ritardo la rettifica dei dati inesatti o il completamento di quelli incompleti.
- Diritto alla Cancellazione (Diritto all'Oblio): Ottenere la cancellazione dei propri Dati Personali se non sono più necessari rispetto alle finalità, in caso di revoca del consenso (se non sussiste altra base giuridica) o di trattamento illecito.
- Diritto di Limitazione del Trattamento: Richiedere la limitazione delle attività di Trattamento in caso di contestazione dell'esattezza dei dati o trattamento illecito.
- Diritto alla Portabilità dei Dati: Ricevere i Dati Personali forniti in un formato strutturato, di uso comune e leggibile da dispositivo automatico e trasmetterli a un altro Titolare del Trattamento, se tecnicamente possibile.
- Diritto di Opposizione: Opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al Trattamento dei Dati Personali (inclusa la profilazione), in particolare se basato sul legittimo interesse del Titolare o per finalità di marketing diretto.
- Diritto di non essere sottoposto a decisioni basate unicamente sul Trattamento Automatizzato: Diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (compresa la profilazione) che produca effetti giuridici o incida significativamente sulla persona.
- Diritto di proporre reclamo all'Autorità di controllo (Garante): in caso di violazione della normativa sulla protezione dei dati personali, l'interessato può presentare reclamo al Garante per la Privacy.

5.4 Registro delle attività di trattamento

Ai sensi dell'art. 30 GDPR, la Società tiene un registro delle attività di trattamento dei dati personali sia come Titolare che come Responsabile. In particolare, AMIA mantiene:

- Un registro delle attività in qualità di Titolare, contenente per ciascuna attività le finalità del trattamento, le categorie di interessati e dei dati trattati, i destinatari, eventuali trasferimenti di dati verso paesi terzi e le misure di sicurezza adottate.
- Un registro delle attività svolte in qualità di Responsabile, per conto di ciascun Titolare, con indicazione delle categorie di trattamenti effettuati, dei dati e delle misure di sicurezza implementate.

Tali registri sono tenuti in forma scritta o elettronica e messi a disposizione dell'Autorità di controllo su richiesta. Nel registro sono inoltre indicati i tempi di conservazione previsti per le diverse categorie di dati.

Gli aggiornamenti delle singole sezioni del Registro sono curati dai referenti di ciascuna area aziendale, in conformità ai flussi informativi descritti nel presente documento o nei regolamenti e procedure interne.

5.5 Trasferimenti extra-UE/SEE

I trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali avvengono solo se conformi alle disposizioni del Capo V del GDPR (artt. 44-50). In generale, i trasferimenti al di fuori dello Spazio Economico Europeo (SEE) sono vietati a meno che non intervengano specifiche garanzie. In particolare:

- Trasferimento su base di adeguatezza (art. 45 GDPR): se un paese terzo è stato oggetto di decisione di adeguatezza da parte della Commissione Europea, il trasferimento può avvenire liberamente in virtù di tale decisione. Le decisioni di adeguatezza (art. 45) sono vincolanti e consentono trasferimenti di dati verso paesi con un livello di protezione equiparato a quello dell'UE.
- Trasferimento con garanzie adeguate (art. 46 GDPR): in assenza di decisione di adeguatezza, è possibile trasferire i dati mediante adeguate garanzie (clausole contrattuali standard, norme vincolanti d'impresa, codici di condotta approvati, ecc.), che assicurino un livello di protezione adeguato ai diritti degli interessati.
- Deroghe specifiche (art. 49 GDPR): in casi eccezionali, quando non è possibile adottare una decisione di adeguatezza o garanzie, si può ricorrere alle deroghe previste dall'art. 49 (ad es. consenso esplicito dell'interessato, trasferimento occasionale necessario per esecuzione contrattuale con l'interessato). Tali deroghe sono applicabili solo in situazioni particolari e vanno interpretate restrittivamente.

La Società verifica sempre la presenza di una decisione di adeguatezza o l'adozione di garanzie appropriate prima di effettuare un trasferimento extra-UE, garantendo in ogni caso i diritti degli interessati.

6. Gestione della Sicurezza e Misure Tecniche e Organizzative

AMIA adotta un approccio basato sul rischio ai sensi del GDPR (in particolare art. 32), predisponendo misure tecniche e organizzative adeguate al livello di rischio dei trattamenti di dati personali. Le misure devono essere proporzionate al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione.

6.1 Misure di Sicurezza Generali

- Misure Fisiche: documenti e atti cartacei contenenti dati personali devono essere conservati per il tempo strettamente necessario in luoghi accessibili solo a personale autorizzato, ad esempio in

armadi o cassetti chiusi a chiave o in locali chiusi quando non presidiati. Lo smaltimento dei documenti deve avvenire tramite trituratori (distruggi-documenti) che ne rendano illeggibile o impossibile la ricostruzione.

- Trasmissioni di dati: l'invio di informazioni personali per posta elettronica deve essere limitato allo stretto necessario. Per l'invio di email contenenti dati personali occorre verificare accuratamente l'indirizzo del destinatario e segnalare, nel messaggio in uscita, l'obbligo di riservatezza del contenuto.

6.2 Sicurezza Informatica e Postazione di Lavoro

Accesso logico: l'accesso ai sistemi informatici avviene tramite credenziali personali (user-id e password) fornite al personale autorizzato. Le credenziali sono strettamente personali e non cedibili. Le password devono avere almeno 8 caratteri, comprensivi di lettere, numeri e simboli, senza riferimenti diretti all'utente. Alla minima assenza dalla postazione (anche per brevi pause) il dispositivo deve essere protetto dal blocco schermo.

Uso di posta elettronica e Internet: gli strumenti informatici aziendali sono riservati esclusivamente a scopi lavorativi. È vietato inviare o ricevere messaggi di carattere personale non strettamente inerenti all'attività lavorativa. La navigazione internet deve avvenire unicamente per fini aziendali; l'utilizzo della rete per scopi personali non autorizzati è proibito.

Dispositivi portatili: laptop, tablet, smartphone aziendali devono essere custoditi con cura durante l'utilizzo e conservati in un luogo sicuro al termine della giornata lavorativa. I dispositivi non devono essere lasciati incustoditi. In caso di furto, smarrimento o accesso non autorizzato, l'Incaricato competente ne informa immediatamente il Titolare (e il DPO, se designato) per le opportune azioni di sicurezza.

6.3 Verifiche del Titolare

Il Titolare può svolgere verifiche, periodiche o straordinarie, sul rispetto:

- degli obblighi in materia di protezione dei dati personali;
- delle regole interne sull'uso degli strumenti aziendali e sulla sicurezza IT;
- degli ulteriori obblighi connessi al rapporto di lavoro e alle policy aziendali applicabili.

Le verifiche si svolgono nell'ambito del sistema di controllo interno e secondo i regolamenti e le procedure aziendali.
Le aree e le persone autorizzate collaborano fornendo tempestivamente informazioni ed evidenze.
I Responsabili del trattamento assicurano il diritto di audit del Titolare secondo quanto previsto negli atti di nomina.

Gli esiti sono tracciati e possono comportare azioni correttive con tempistiche proporzionate al rischio. I controlli sono effettuati nel rispetto della normativa vigente (inclusa quella in materia di controlli a distanza e tutela dei lavoratori), nonché dei principi di necessità, proporzionalità e trasparenza.

7. Processi Operativi Critici

7.1 Valutazione d'Impatto sulla Protezione dei Dati (DPIA)

La DPIA è obbligatoria quando un trattamento, per la sua natura, estensione, contesto o finalità, può presentare un rischio elevato per i diritti e le libertà degli interessati. In particolare, ai sensi dell'art. 35(3) del GDPR, la DPIA è richiesta per trattamenti quali la profilazione automatizzata con valutazione sistematica degli interessati, il trattamento su larga scala di categorie particolari di dati (art. 9) o di dati giudiziari, oppure la sorveglianza sistematica di vaste aree accessibili al pubblico.

La valutazione d'impatto deve contenere almeno:

- Una descrizione sistematica dei trattamenti previsti e delle finalità.
- La valutazione della necessità e proporzionalità dei trattamenti rispetto alle finalità.
- La valutazione dei rischi per i diritti e le libertà degli interessati.
- Le misure previste per mitigare tali rischi, incluse garanzie, misure di sicurezza e meccanismi per garantire la conformità al GDPR.

Il Titolare svolge la DPIA con il supporto del DPO, se designato (art. 35(2) GDPR). Se, a seguito della DPIA, il rischio residuo rimane elevato nonostante le misure adottate, il Titolare consulta preventivamente l'Autorità di controllo (cfr. art. 36 GDPR) prima di procedere.

7.2 Gestione della Violazione dei Dati Personali (Data Breach)

Il Titolare deve implementare un processo adeguato a garantire la corretta gestione delle Violazioni dei Dati Personali.

Fasi tipiche del Processo:

- Segnalazione e Identificazione: Raccogliere le segnalazioni di potenziali violazioni, coinvolgendo fin da subito la figura del DPO.
- Valutazione e Rimedio: Valutare l'incidente dal punto di vista del rischio (Basso, Medio, Alto, Molto Alto) e identificare le misure correttive da adottare. Il DPO è informato e rivede la valutazione del rischio e l'adeguatezza delle azioni di mitigazione.
- Notifica e Comunicazione:

    - Notifica all'Autorità Garante: Deve essere effettuata senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui se ne è venuti a conoscenza, a meno che la violazione sia improbabile che comporti un rischio per i diritti e le libertà delle persone fisiche.
    - Comunicazione agli Interessati: È obbligatoria se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica.
- Registro delle Violazioni: Il Titolare deve documentare qualsiasi violazione subita (anche se non notificata o comunicata), le relative circostanze, le conseguenze e i provvedimenti adottati. Tale registro è previsto all'art. 33(5) del GDPR per garantire trasparenza e consentire all'Autorità di controllo di verificare l'osservanza delle procedure.

7.3 Conservazione e Cancellazione dei Dati

I dati personali sono conservati per un periodo non superiore a quello necessario agli scopi per cui sono trattati, come previsto dal principio di limitazione della conservazione (art. 5 GDPR). La durata esatta è definita in funzione delle finalità, delle disposizioni di legge e dei regolamenti applicabili.

Al termine del periodo di conservazione, i dati sono resi non identificabili tramite cancellazione o anonimizzazione irreversibile.

Ove possibile AMIA adotta procedure automatizzate che garantiscono la cancellazione o l'anonimizzazione dei dati personali conservati in forma elettronica una volta scaduti i termini previsti.

8. Formazione e Aggiornamento

AMIA garantisce che tutto il personale autorizzato a trattare dati personali sia adeguatamente formato e informato sulle procedure e sulle regole interne. In particolare, il Titolare (o il Referente Privacy con il supporto delle risorse umane) definisce annualmente un piano di formazione volto a sensibilizzare il personale sulle tematiche della protezione dei dati personali. Il DPO ne sorveglia l'erogazione e ne verifica il completamento da parte dei destinatari. Tra i compiti del DPO, come previsto dall'art. 39 GDPR, vi sono la sensibilizzazione e la formazione del personale coinvolto nelle attività di trattamento.

Il Titolare assicura inoltre la revisione periodica di questo Regolamento. Qualsiasi modifica intervenuta viene tempestivamente comunicata a tutti i soggetti cui il Regolamento si applica. Il documento è oggetto di revisione almeno con cadenza annuale, così da garantire la continua conformità alle disposizioni di legge e alle best practice in materia di privacy.