PRIVACY POLICY DEL CONSORZIO STRADALE CENTRO RESIDENZIALE AXA

Per la protezione dei dati personali ai sensi del Regolamento (UE) 2016/679 - (GDPR)

ConsorzioStradale CentroResidenziale

PRIVACY POLICY

Sommario

PRIVACY POLICY

PRIVACY POLICY

1. PREMESSA

Il presente Documento Unico, redatto in conformità al Regolamento (UE) 2016/679 definisce il modello Privacy, ossia le disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dal Consorzio Stradale Centro Residenziale AXA (di seguito Consorzio AXA).

Al Consorzio AXA in quanto tale, nella sua qualità di Titolare del trattamento dei dati personali, competono, infatti, le decisioni in ordine alle finalità ed alle modalità del trattamento, compreso il profilo della sicurezza e della prevenzione da un potenziale Data Breach (violazione dei dati).

Più specificatamente, gli obiettivi primari del presente Documento Unico sono:

- migliorare la consapevolezza dei rischi insiti nel trattamento dei dati con l'ausilio di strumenti elettronici, con particolare riferimento alla gestione e all'utilizzo del sistema informativo;
- individuare e definire adeguate misure tecniche ed organizzative finalizzate alla salvaguardia, alla corretta gestione e al corretto utilizzo del patrimonio informativo consortile;
- adottare idonei presidi di controllo al fine di contenere i rischi, prevenendo le possibili situazioni di pericolo;
- fornire adeguate istruzioni comportamentali e procedurali ai soggetti coinvolti nella gestione dei singoli trattamenti.

Per il raggiungimento dei suddetti obiettivi il Consorzio AXA pone in essere, fra l'altro, le seguenti attività:

- interventi formativi degli incaricati del trattamento;
- censimento dei trattamenti effettuati e delle banche dati gestite dagli incaricati, al fine di individuare le diverse tipologie di dati trattati, i rischi potenziali e le conseguenti misure di sicurezza (art. 32 Reg.);
- predisposizione di una Privacy Policy per il trattamento dei dati personali con cui vengono fatte proprie le regole deontologiche e le misure minime di sicurezza previste dal nuovo Regolamento (UE) 2016/679, in materia di protezione dei dati personali;
- predisposizione di un apposito Registro delle attività del trattamento (art. 30 Reg.)

PRIVACY POLICY

Le attività di cui sopra hanno portato all'acquisizione e all'aggiornamento delle seguenti informazioni, trattate in modo approfondito nei successivi paragrafi del presente Documento:

- elenco dei trattamenti di dati personali;
- distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- misure da adottare per garantire l'integrità e la disponibilità dei dati e la protezione delle aree e dei locali;
- descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- descrizione dei criteri da adottare per garantire l'adozione delle misure di sicurezza in caso di trattamento di dati personali affidati all'esterno della struttura del titolare.

2. DEFINIZIONI IN MATERIA DI PRIVACY

Trattamento: qualsiasi operazione o insieme di operazioni compiute con o senza l'analisi di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, la conservazione, l'uso, la comunicazione mediante diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Titolare del trattamento: la persona fisica, l'impresa, l'ente, l'associazione, ecc. cui fa capo effettivamente il trattamento di dati personali e spetta assumere le decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza). Nei casi in cui il trattamento sia svolto da una società o da una pubblica amministrazione per titolare va intesa l'entità nel suo complesso e non l'individuo o l'organo che l'amministra o la rappresenta (presidente, amministratore delegato, sindaco, ministro, direttore generale, ecc.). I casi in cui il trattamento può essere imputabile ad un individuo riguardano semmai liberi professionisti o imprese individuali

Responsabile del trattamento: la persona, la società, l'ente, l'associazione o l'organismo cui il titolare affida, anche all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati. La designazione del responsabile è facoltativa.

Incaricato: il dipendente che è coinvolto materialmente nel trattamento dei dati (ad es. amministrazione del personale) e incaricato attraverso un'apposita lettera di incarico.

Dato Personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la 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 una o più

elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Esempi:

- codice fiscale e altri numeri di identificazione personale;
- nominativo, indirizzo o altri elementi di identificazione personale dati relativi alla famiglia e a situazioni personali
- dati bancari o postali carta identità
- istruzione formazione
- dati relativi ai familiari, anche minori, del lavoratore iscritto

Dati Particolari (sensibili): i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biomedici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Esempi:

- adesione ad un sindacato
- stato di salute
- origine razziale ed etnica
- convinzioni religiose filosofiche o di altro genere
- opinioni politiche
- organizzazioni a carattere religioso, filosofico, politico o sindacale

Modalità Del Trattamento: il regolamento sancisce che il trattamento deve sempre ispirarsi ai principi di liceità, correttezza, trasparenza, pertinenza, compatibilità con le finalità espresse con gli scopi dichiarati, minimizzazione, proporzionalità, limitazione alla conservazione, sicurezza e integrità

3. TRATTAMENTO DEI DATI DEL CONSORZIO NELL'ESERCIZIO DELL'ATTIVITÀ DI GESTIONE

3.1 Elenco dei Trattamenti di Dati Personali

Il Consorzio AXA esegue i trattamenti sia tramite strumenti elettronici, attraverso il proprio sistema informatico, sia attraverso strumenti tradizionali sia tramite i propri archivi cartacei.

3.2 Natura dei dati trattati dal Consorzio AXA

Il Consorzio AXA, nell'esercizio dell'attività di gestione, tratta i dati personali dei propri dipendenti, dei consorziati e di tutti coloro che, a qualunque titolo, sono titolari di diritti di godimento di beni immobili locati all'interno dell'area consortile (affitti, locazioni, comodati ecc…).

I dati trattati sono essenzialmente anagrafici/identificativi.

Non è possibile escludere a priori il trattamento di dati "**particolari**", soprattutto per quanto riguarda lo stato di salute dei propri dipendenti e l'adesione di quest'ultimi ad un sindacato, e "**giudiziari**", soprattutto per quanto riguarda le ipotesi di recupero degli oneri consortili nei confronti dei consorziati morosi.

Le tipologie di dati trattati sono meglio specificate nell'apposito registro dei trattamenti, unitamente alle finalità e a tutte le altre informazioni richieste dal Regolamento (All. 1).

3.3 Finalità del Trattamento

I dati personali forniti sono destinati esclusivamente alle finalità connesse all'attività di gestione del Consorzio ed al corretto adempimento del relativo mandato da parte del Consiglio di Amministrazione nominato dall'Assemblea Consortile, nel rispetto delle prescrizioni di legge.

In particolare il trattamento dei dati forniti è finalizzato:

- alla gestione del personale;
- alla elaborazione e tenuta del registro di anagrafe consortile contenente le generalità dei singoli proprietari e dei titolari di diritti reali e di diritti personali di godimento, comprensive del codice fiscale e della residenza o domicilio, i dati catastali di ciascuna unità immobiliare;

- alla elaborazione e organizzazione generale e particolare dei documenti, fiscali e non, nell'ambito dell'amministrazione e della gestione del Consorzio nel senso più ampio del termine compresa l'elaborazione dei dati contabili, del bilancio di esercizio, delle attestazioni, certificazioni e/o dichiarazioni fiscali oltre alla relativa presentazione/trasmissione telematica delle stesse;
- alla elaborazione dei dati necessari per l'adempimento di tutte le incombenze previste per Legge ovvero per ogni altro obbligo contabile, fiscale, previdenziale e/o civilistico compresa la gestione di pratiche assicurative e/o con istituti di credito, con la Pubblica Amministrazione o con diversi soggetti terzi in generale.

3.4 Modalità di Trattamento

Il trattamento dei dati è svolto nel rispetto di quanto previsto dall'art. 32 del GDPR 2016/679 e dall'Allegato B) del D.Lgs. n. 196/2003 (artt. 33-36 del Codice della Privacy) in materia di misure di sicurezza, ad opera di soggetti appositamente incaricati ed in ottemperanza a quanto previsto dall'art. 29 del GDPR 2016/679.

In particolare, il trattamento dei dati trattamento dei dati è svolto nel pieno rispetto delle libertà fondamentali senza ledere la riservatezza e dignità, adottando sempre principi ispirati alla correttezza, liceità e trasparenza nonché per scopi non eccedenti le finalità della raccolta, ed è realizzato per mezzo delle operazioni di cui all'art. 4, n.2), GDPR e precisamente: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'elaborazione, la selezione, il blocco, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Per il trattamento dei dati possono essere utilizzati sia mezzi informatici o telematici che strumenti manuali adottando tutte le misure di sicurezza idonee a garantire la riservatezza, l'integrità e l'esattezza dei dati.

Nel pieno rispetto dell'art. 5 del GDPR 2016/679, i dati personali saranno altresì adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono raccolti e trattati/conservati per il periodo di tempo strettamente necessario per il conseguimento delle finalità espresse.

3.5 Designazione degli incaricati

L'Art. 29 del Regolamento UE 2016/679 stabilisce che chiunque agisca sotto la autorità del titolare del trattamento e che abbia accesso a dati personali non può trattare gli stessi se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Orbene, ogni operatore che agisce sotto l'autorità del Consorzio AXA è **incaricato** al trattamento dei dati derivanti dall'espletamento delle proprie specifiche mansioni mediante un apposito atto di nomina, nonché preventivamente ed adeguatamente formato in materia privacy.

3.6 Attività degli incaricati

Gli incaricati, nel trattare i dati personali, dovranno operare garantendo la massima riservatezza delle informazioni di cui vengono in possesso, dovranno attenersi alle istruzioni impartitegli dal Titolare ed adottare tutte le misure di sicurezza che siano indicate, oggi o in futuro, da quest'ultimo.

Gli incaricati dovranno considerare tutti i dati personali come confidenziali, ad eccezione dei soli dati c.d. ordinari, ossia quelli contenuti in pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

3.7 Regole generali per gli incaricati

L'incaricato deve garantire l'integrità del dato, la sua disponibilità e la sua confidenzialità, operando con la massima diligenza ed attenzione in tutte le fasi di trattamento: dalla esatta acquisizione dei dati, all'eventuale loro aggiornamento; così per la conservazione, la custodia ed eventuale cancellazione o distruzione.

Gli incaricati, più specificatamente, sono tenuti al rispetto delle seguenti regole generali:

- non sono, in nessun caso, tenuti a comunicare dati personali richiesti telefonicamente;
- quando appositamente autorizzati all'accesso alle banche dati informatiche, custodire con attenzione le proprie credenziali di autenticazione ed ogni dispositivo che le contiene;
- non lasciare accessibile il sistema operativo in caso di allontanamento, anche temporaneo, dal posto di lavoro, al fine di evitare trattamenti non autorizzati;
- non operare su terminali altrui;

- trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
- conservare i supporti informatici e/o cartacei contenenti i dati personali, in modo da evitare che siano accessibili a persone non autorizzate al trattamento dei dati medesimi o siano facilmente oggetto di danneggiamenti intenzionali o accidentali;
- copie di dati personali oggetto di trattamento devono essere effettuate esclusivamente se necessario e soltanto previa autorizzazione del titolare del trattamento;
- in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al titolare del trattamento;
- in caso di richieste da parte dell'interessato (reclami, accesso, opposizione, ecc…) attenersi, per quanto di competenza, alla procedura stabilita e descritta nel presente documento;
- in caso di violazione di dati attenersi, per quanto di competenza, alla procedura stabilita e descritta nel presente documento;
- compiere tempestivamente quanto necessario per fornire al Titolare le informazioni necessarie per rispondere ad eventuali richieste di accesso ai dati personali da parte dell'interessato;
- compiere tempestivamente quanto necessario per fornire al Titolare le informazioni necessarie per rispondere ad eventuali richieste pervenute dal Garante o dall'Autorità Giudiziaria o, comunque, dalle Forze dell'Ordine;
- segnalare al titolare del trattamento eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- effettuare la comunicazione dei dati esclusivamente ai soggetti indicati dal titolare del trattamento e secondo le modalità stabilite dai medesimi;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;

- fornire al titolare del trattamento, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentirgli di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al Titolare al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico, nel rispetto della normativa vigente

4. ISTRUZIONI PER I TRATTAMENTI SVOLTI CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI

4.1 Istruzione per i trattamenti svolti

La presente sezione comprende le istruzioni operative generali relative a:

a) parola chiave per l'accesso ai dati
b) autonoma sostituzione della parola chiave per l'accesso ai dati
c) antivirus e protezione da programmi pericolosi
d) riutilizzo controllato dei supporti
e) autorizzazioni all'ingresso nei locali
f) controllo accesso ai locali
g) trattamenti per fini esclusivamente personali
h) ripristino dati

A. Parola chiave per l'accesso ai dati

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave conosciuta solamente dal medesimo. Il codice per l'identificazione non può essere assegnato ad altri incaricati, neppure in tempi diversi.

In particolare:

a) **La password:**
   - non deve essere divulgata e deve essere custodita con la massima diligenza;
   - deve essere modificata dall'assegnatario almeno ogni sei mesi;
   - deve essere composta da una combinazione di caratteri alfanumerici e non deve contenere riferimenti riconducibili all'assegnatario, come, ad esempio, la sua data di nascita;
   - dopo ogni modifica, le nuove credenziali devono essere consegnate, in busta chiusa firmata, al Presidente del Consorzio.

b) **Il nome utente** una volta generato non può essere mai utilizzato, neanche in momenti diversi, da altri incaricati che non siano l'assegnatario.

c) Le credenziali di autenticazione devono essere disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

d) Gli strumenti elettronici devono essere preferibilmente spenti ogni sera prima di lasciare gli uffici presidiando fino al corretto completamento dello spegnimento del sistema.

e) Nelle pause dal lavoro ogni incaricato deve salvare tutti i file, chiudere tutte le applicazioni aperte e bloccare lo schermo per evitare di lasciare incustodito l'accesso allo strumento.

f) L'operatore che dovrà effettuare la stampa dei dati è tenuto a ritirarla immediatamente dai vassoi delle stampanti comuni per evitare accessi da parte di persone non autorizzate.

g) È fatto assoluto divieto di consentire a terzi l'accesso agli archivi.

In caso di irreperibilità di un incaricato e della necessità di accedere al sistema informativo, il Presidente pro tempore del Consorzio può aprire la busta sigillata ed utilizzare le sue credenziali. Appena l'incaricato sarà di nuovo reperibile si provvederà ad avvisarlo dell'avvenuto intervento, invitandolo a provvedere con la massima sollecitudine alla modifica della password da consegnare al Presidente pro tempore del Consorzio.

B. Autonoma sostituzione della parola chiave per l'accesso ai dati

La parola chiave è autodeterminata dai singoli soggetti e, successivamente, modificata almeno ogni sei mesi.

La parola chiave, in ogni caso, non potrà essere comunicata ad altri soggetti per nessun motivo e non potrà essere trascritta o annotata in maniera evidente o visibile da altri. Nella generazione della parola chiave si dovranno adottare criteri di massima prudenza ad evitare che la stessa possa essere individuata per limitati tentativi.

Nel caso di utilizzo di più password queste dovranno essere diverse tra di loro.

C. Antivirus e protezione da programmi pericolosi

Tutti i PC del Consorzio AXA connessi in rete devono essere dotati di programmi, sempre attivi ed aggiornati, atti alla rilevazione di virus informatici, a prevenire la vulnerabilità di strumenti elettronici e a correggere difetti.

Più specificatamente:

- vi è divieto assoluto di installare programmi software senza la preventiva autorizzazione del Consorzio AXA;
- vi è divieto assoluto di scaricare software o applicativi da internet per un uso diverso da quello professionale;
- vi è divieto assoluto di aprire ed eseguire file in allegato alle e-mail ricevute da mittenti sconosciuti;
- vi è divieto assoluto di accedere a siti internet se non, esclusivamente, per consultazioni di natura professionale;
- la casella di posta elettronica è messa a disposizione per usi prevalentemente professionali.

D. Utilizzo dei supporti hardware

Gli incaricati debbono custodire e controllare i supporti magnetici sui quali sono conservati di dati personali in maniera che soggetti non autorizzati non possano venire a conoscenza, nemmeno occasionalmente o accidentalmente, del loro contenuto.

Al termine di ogni lavorazione i supporti dovranno essere custoditi in appositi contenitori e riposti in armadi o cassetti muniti di serratura e chiusi a chiave.

Se un supporto, quale un Hard Disk esterno, è condiviso tra più incaricati, ciascuno di essi dovrà accedere, esclusivamente, alle sole cartelle che riguardano il proprio incarico mediante l'utilizzo di una apposita password.

E. Autorizzazione all'ingresso nei locali

L'ingresso nei locali del Consorzio, fatta salva l'area di accesso riservata al pubblico, è riservato ai dipendenti e alle persone espressamente autorizzate.

F. Ripristino dati

Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a trenta giorni.

G. Corretto utilizzo delle caselle di posta elettronica

- devono essere immediatamente cancellati i messaggi che contengono allegati segnalati dall'antivirus;
- è preferibili evitare l'utilizzo delle caselle e-mail per l'invio di messaggi estranei al rapporto di lavoro, prediligendo l'utilizzo delle unità di rete piuttosto che allegare il documento ad un messaggio di posta elettronica;

Relativamente alla navigazione Internet è tassativamente proibito:

- effettuare qualsiasi genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati e con il rispetto delle normali procedure per gli acquisti;
- ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

5. ISTRUZIONI PER I TRATTAMENTI SVOLTI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI

5.1 Istruzione per i trattamenti svolti

A. Accesso ai soli dati necessari

Durante lo svolgimento di trattamenti di dati personali registrati su carta o altri supporti, i singoli incaricati delle diverse operazioni di trattamento devono operare solo su quei dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti previsti per le specifiche attività attribuite alla funzione ricoperta.

B. Conservazione in archivi ad accesso selezionato

L'accesso agli archivi contenenti atti e i documenti di dati personali di qualunque natura è riservato alle sole persone incaricate ed autorizzate a potervi accedere.

Censimento degli archivi cartacei:

1. Corrente	Localizzato presso le postazioni di lavoro, presso le scrivanie e appositi armadi nei quali a fine giornata viene riposta tutta la documentazione che è stata utilizzata.
2. Storico	Localizzato presso una struttura separata chiusa a chiave a cui vi hanno accesso soltanto gli incaricati che hanno il compito di gestire tale documentazione.
3. Documentazione riservata/personale	Localizzato presso la sede dove vengono custoditi i documenti di rilevante importanza costruito con materiale ignifugo. Questo archivio è costituito da una cassaforte sempre chiusa e vi hanno accesso soltanto gli incaricati che hanno il compito di gestire tale documentazione.

C. Custodia atti e documenti

Gli atti e i documenti contenenti dati personali di qualunque natura devono essere trattati con diligenza, custoditi e conservati in maniera che le persone non incaricate non possano venirne a conoscenza.

Gli incaricati abilitati al trattamento di dati provenienti (o direttamente tratti) da archivi ad accesso selezionato, devono conservare e custodire i dati trattati con diligenza e riservatezza evitando che vengano volontariamente o involontariamente conosciuti da soggetti privi della stessa qualificazione di incaricato.

D. Restituzione atti e documenti al termine delle operazioni

Gli atti e i documenti devono essere trattenuti solo per il periodo strettamente necessario allo svolgimento delle operazioni inerenti i propri compiti e al termine di dette operazioni devono essere restituiti o riposti nell'archivio dal quale erano stati prelevati (o presso il quale devono essere custoditi).

E. Macero e/o distruzione di supporti cartacei contenenti dati personali

Gli incaricati del trattamento hanno il compito di curare che l'inoltro al macero di supporti cartacei contenenti dati personali (es. tabulati contenenti: dati anagrafici) sia preceduto da idonei interventi ed accorgimenti atti ad evitare che altri soggetti vengano a conoscenza, anche accidentalmente, dei dati riportati sui supporti.

6. MISURE DI PROTEZIONE DEI DATI PERSONALI

6.1 Destinatari della comunicazione dei dati

Si rinvia al Registro dei trattamenti per l'individuazione dei nominativi dei terzi destinatari della comunicazione dei dati trattati dal Consorzio.

6.2 Protezione delle Aree e dei Locali

Il Titolare del Trattamento mette in atto misure tecniche e organizzative tese a:

- predisporre, e conservare in luogo chiuso e protetto, per ogni incaricato al trattamento una busta nella quale vengono riportati il codice di identificazione e la password;
- revocare tutte le password non utilizzate per un periodo superiore a sei mesi o comunque a soggetti non più autorizzati ad accedere ai dati;

- collocare l'hardware in locali non accessibili al pubblico e a persone non autorizzate;
- impedire l'intrusione nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate;
- impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia di dati nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate;
- conservare i documenti contenenti i dati in contenitori muniti di serratura;
- porre in essere dispositivi anti incendio e dispositivi anti intrusione.

6.7 Integrità dei dati

Le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile hanno accesso ai soli dati personali la cui conoscenza è strettamente necessaria per adempiere ai compiti loro assegnati e si attengono ad una serie di istruzioni.

6.8. Criteri e modalità di ripristino della disponibilità dei dati

- Backup completo giornaliero
- Copie periodiche degli archivi (una al mese) su supporti esterni con conservazione in apposita cassaforte

Nel locale dove è ubicato il server è presente un gruppo di continuità elettrico che garantisce l'integrità degli archivi in caso di sbalzi di tensione elettrica o black-out per un massimo di 30 minuti.

6.9 Misure di sicurezza

Di seguito sono elencate alcune notazioni riguardo l'adozione delle misure tecniche e organizzative di sicurezza così come previste nel Regolamento UE 2016/679.

A. Misure per trattamenti informatici

- tutti gli incaricati sono dotati di credenziali di autenticazione (codice identificativo personale e parola chiave). Il trattamento dei dati personali richiede il superamento di una o più procedure di autenticazione, per l'accesso alla rete e/o all'applicazione;

- l'Amministratore di sistema e/o il Responsabile interno del trattamento provvede ad operazioni periodiche di pulizia degli account per disattivare credenziali inutilizzate, o riferite ad incaricati che hanno perso le qualità per accedere ai dati personali;
- l'attività informatica del Consorzio nei locali interni prevede l'utilizzo di notebook e Pc Desktop collegati al server, in questo modo nessun dato viene utilizzato o memorizzato sui dischi locali ma ogni interazione avviene direttamente con il server dove sono installati tutti i mezzi di protezione dei dati (antivirus, firewall);
- l'evoluzione dei sistemi operativi viene monitorata regolarmente. Gli aggiornamenti del sistema operativo sono effettuati in modalità automatica.

B. Misure per trattamenti cartacei

- L'ingresso nei locali dell'Ente non aperti al pubblico è riservato ai dipendenti e alle persone espressamente autorizzate;
- nei locali in cui vengono svolti trattamenti di dati particolari possono accedere solo gli incaricati espressamente autorizzati;
- l'accesso alle stanze archivio è consentito alle sole persone incaricate ed autorizzate a potervi accedere e viene controllato dal Presidente pro tempore del Consorzio;
- gli incaricati del trattamento di dati personali, oltre a rispettare le norme generali previste per la custodia (diligenza), sono tenuti a conservare atti o documenti in contenitori (armadi e/o cassetti) muniti di serratura e chiusi;
- l'accesso a tali contenitori è consentito solo alle persone autorizzate a svolgere le operazioni di trattamento.

7.MISURE DI SICUREZZA IN CASO DI TRATTAMENTO DI DATI PERSONALI AFFIDATI AI TERZI

7.1 Responsabile esterno del trattamento

Qualora il trattamento dei dati debba essere effettuato per conto del titolare, quest'ultimo deve avere tutte le garanzie che il trattamento si svolga secondo i requisiti del Regolamento e garantisca la tutela degli interessati.

Più specificatamente, i trattamenti da parte del responsabile esterno sono disciplinati mediante una nomina attraverso la quale il soggetto cui le attività sono affidate si impegna a (art. 32 del Reg.):

1. curare che i dati personali oggetto del trattamento siano trattati in modo lecito e secondo correttezza, e comunque sempre nel pieno rispetto dell'attuale normativa vigente;
2. adottare preventive misure di sicurezza che, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, siano idonee a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta;
3. adottare tutte le misure di sicurezza e gli accorgimenti necessari al fine di garantirne la puntuale attuazione e, in particolare:
    a. provvedere alla eventuale nomina scritta delle persone fisiche (incaricati) autorizzati al trattamento, impartendo alle stesse le istruzioni necessarie ed opportune al fine di garantire la riservatezza dei dati e, in generale, il rispetto della normativa vigente;
    b. informare il Titolare, su richiesta, in merito alle misure di sicurezza e agli accorgimenti adottati per garantire il rispetto della normativa vigente ed in particolare delle istruzioni impartite dal Titolare nel presente atto di nomina;
    c. prevedere una specifica procedura di gestione delle violazioni dei dati;
    d. prevedere una specifica procedura di gestione delle richieste da parte dei soggetti interessati;

e. fornire al Titolare, a semplice richiesta e secondo le modalità indicate da quest'ultimo, i dati e le informazioni necessari per consentire allo stesso di svolgere una tempestiva difesa in eventuali procedure instaurate davanti al Garante o all'Autorità Giudiziaria e relative al trattamento dei dati personali;
f. compiere tempestivamente quanto necessario per fornire al Titolare le informazioni necessarie per rispondere ad eventuali richieste di accesso ai dati personali da parte dell'interessato;
g. compiere tempestivamente quanto necessario per fornire al Titolare le informazioni necessarie per rispondere ad eventuali richieste pervenute dal Garante o dall'Autorità Giudiziaria o, comunque, dalle Forze dell'Ordine;
h. in generale, prestare la più ampia e completa collaborazione al Titolare al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico, nel rispetto della normativa vigente.

Il Responsabile esterno è autorizzato ad operare per i tempi di erogazione del servizio, secondo i termini temporali contrattualmente previsti (data retention) decorsi i quali dovrà provvedere alla restituzione/distruzione di tutti i dati riconducibili all'incarico presenti sia in linea sia nelle copie di garanzia e backup.

8. PROCEDURA PER LA GESTIONE DELLE RICHIESTE DA PARTE DEGLI INTERESSATI AL TRATTAMENTO DEI DATI PERSONALI

A. **Referente privacy:**
   a. Presidente pro tempore del Consorzio
B. **Definizione "richiesta privacy":**
   a. qualsiasi comunicazione proveniente da un interessato;
C. **Presentazione "richieste privacy":**
   a. possono pervenire in qualsiasi modalità (cartacea, posta elettronica, telefono fax, *brevi manu*);
   b. è necessario assicurarsi dell'identità dell'interessato se questi non è già conosciuto;
   c. la richiesta va consegnata al referente privacy che provvederà alla sua registrazione;

d. non occorre fare fotocopie dei documenti identificativi;
e. nel caso la richiesta sia fatta da un legale ovvero altro rappresentante legale, occorre farsi consegnare copia della procura o delega.

D. Gestione della richiesta:

a. il referente privacy avvalendosi se necessario di consulenti esterni valuta la richiesta e predispone la documentazione relativa per dare "riscontro" allo stesso;
b. è necessario rispondere alla richiesta entro massimo 15 giorni.

E. Risposta all'interessato:

a. le risposte, sia positive che negative, vanno anticipate via email e inviate tramite posta elettronica certificata o, in mancanza, in forma scritta, tramite raccomandata A/R.

F. Chiusura richiesta:

a. dopo l'invio della risposta la procedura va chiusa utilizzando un codice o una terminologia opportuna (esito positivo o negativo).

9. PROCEDURA PER LA GESTIONE DI DATA BREACH

A. Normativa e documenti di riferimento:

a. Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34;
b. Guidelines on Personal data breach notification under Regulation 2016/679 – article 29 data protection working party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018)

B. Referente privacy:

a. Presidente pro tempore del Consorzio

C. Modalità e profili di notifica all'Autorità Garante Privacy:

a. ogni operatore autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di data breach, avvisa tempestivamente il referente privacy;
b. la segnalazione avviene tramite le consuete modalità di gestione dei flussi documentali già in uso nel consorzio;

c. il referente privacy effettua una valutazione dell'evento avvalendosi, nel caso, di eventuali altre professionalità necessarie per la corretta analisi della situazione;
d. ai fini di una corretta classificazione dell'episodio, il referente privacy utilizzerà lo schema di scenario di data breach di cui al punto F della presente sezione;
e. qualora si ritenga non necessario comunicare l'episodio all'Autorità garante, la scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del referente privacy;
f. se, invece, si intende comunicare l'evento all'Autorità Garante, il referente privacy predispone la comunicazione, a firma del titolare del trattamento, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali;
g. la notifica va trasmessa al Garante per la protezione dei dati personali, inviandola all'indirizzo: protocollo@pec.gpdp.it
h. oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo;
i. è comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi);[1]

D. Modalità di comunicazione agli interessati:

a. solo nel caso in cui dalla violazione dei dati personali si ritiene possa essere derivato o possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione;

[1] Per avere maggiori informazioni circa la notifica al Garante è possibile visitare la seguente pagina internet: https://www.garanteprivacy.it/regolamentoue/databreach

b. il referente privacy deve predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del titolare, da inviarsi nei tempi e nei modi che lo stesso, anche attraverso la consulenza di altri professionisti, individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

E. Registro delle violazioni:

a. il referente privacy cura l'aggiornamento del registro delle violazioni, ai sensi dell'art. 33, comma 5 del GDPR.

F. Schema di valutazione dei possibili scenari:

TIPO DI BREACH	ESTENSIONE MINIMA / SOGLIA DI SEGNALAZIONE	ESEMPI
DISTRUZIONE	Dati non recuperabili o provenienti da procedure non ripetibili. Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi che, quindi, non sono ripetibili.	Guasto non riparabile dell'hard disk contenente uno o più documenti che, in violazione al regolamento, erano salvati localmente.
PERDITA	Dati non recuperabili o provenienti da procedure non ripetibili. Rientrano tra i casi di segnalazione le sole tipologie di dato la cui disponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato.	Smarrimento di chiavetta USB contenente dati originali.
MODIFICA	Un insieme di dati personali che, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di	Azione involontaria, o fraudolenta, di un operatore che porta alla alterazione di dati

	richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	personali in modo non tracciato e irreversibile.
ACCESSO NON AUTORIZZATO	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione. Rientrano tra i casi di segnalazione le sole tipologie di dato la cui disponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente all'accesso non autorizzato possa ledere i diritti fondamentali dell'interessato.	▪ Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano la vulnerabilità di sistemi. ▪ Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso al sistema informatico