

TRATTAMENTO DATI PERSONALI POLICY AZIENDALE

Premessa

Il presente documento stabilisce le misure di sicurezza da adottare affinché siano rispettati gli obblighi relativi la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, nel rispetto dei principi di: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione, di cui al Regolamento Europeo 2016/679, disciplinante la suddetta materia.

Eventuali trattamenti difformi rispetto a quanto precisato nel presente documento e nei Registri delle attività di trattamento afferenti ciascuna area aziendale o, comunque, effettuati per finalità diversa da quella per la quali i dati personali sono stati raccolti, dovranno essere ricondotti a stato di liceità nel più breve tempo possibile.

Oggetto e Finalità

Il presente documento definisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché quelle relative la libera circolazione degli stessi.

Nel rispetto del Regolamento Europeo 2016/679, Padania Acque S.p.A. si impegna a proteggere il diritto alla protezione dei dati personali trattati interamente o parzialmente in modo automatizzato e/o non automatizzato, contenuti in un archivio o destinati a figurarvi, dei soggetti con i quali si rapporta nell'ambito dell'espletamento delle proprie attività, nell'esatto adempimento del proprio servizio.

Il documento detta regole comportamentali comuni, alle quali tutto il personale di Padania Acque S.p.A. dovrà uniformarsi, rispettando quanto ivi indicato, al fine di;

- a) assicurare il rispetto delle norme di protezione dei dati personali;
- b) impedire la violazione dei medesimi dati e/o la perdita del controllo degli stessi;
- c) non limitare i diritti degli interessati;
- d) non consentire la discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifrazione non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Definizioni

Per creare maggiore consapevolezza nel personale operante e meglio comprendere le attività e comportamenti capaci di garantire il rispetto delle disposizioni in materia di trattamento dati, vengono rese note le seguenti definizioni:

- 1) **«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 uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- 2) **«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;

- 3) **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- 4) **«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;
- 5) **«pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- 6) **«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;
- 7) **«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 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 o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- 8) **«responsabile del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- 9) **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- 10) **«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 trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- 11) **«consenso dell'interessato»**: qualsiasi manifestazione di volontà libera, specifica, informata e 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;
- 12) **«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;
- 13) **«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;
- 14) **«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;

15) **«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;

16) **«impresa»:** la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

17) **«norme vincolanti d'impresa»:** le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune.

Titolare, responsabili, incaricati

- ❖ **Titolare del trattamento:** *Marco Lombardi* – Direttore Generale;
- ❖ **Responsabile della protezione dei dati (DPO):** *Maria Costarella*;
- ❖ **Responsabile del trattamento:** come da Registri delle attività di trattamento.
- ❖ **Responsabile della sicurezza informatica:** *Michele Ardigò* – Responsabile Sistemi Informativi
- ❖ **Incaricati del trattamento dei dati:** tutti i dipendenti preposti al trattamento da parte dei Responsabili delle aree aziendali, così come individuati nei Registri di trattamento.
- ❖ **Amministratore di sistema:** *Michele Ardigò*– Responsabile Sistemi Informativi.

L'Amministratore di sistema è individuato con apposito atto scritto della Direzione aziendale.

Ha il compito di generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, la parola chiave ed i codici di accesso personali da assegnare agli incaricati del trattamento dei dati, nel rispetto delle massime misure di sicurezza.

Dovrà adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza, nel rispetto delle disposizioni normative in materia di privacy, utilizzando le conoscenze acquisite in base al progresso tecnico di software e hardware.

Avrà il compito, altresì, di controllare periodicamente l'efficienza dei sistemi tecnici adottati e di redigere apposita relazione, da consegnare al titolare, riportante i riscontri e le verifiche effettuate, i parametri adottati e gli accorgimenti proposti per migliorare la sicurezza.

Inoltre, dovrà:

- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di backup;
- assicurarsi della qualità delle copie di backup dei dati e della loro conservazione in luogo adatto e sicuro;
- fare in modo che sia prevista la disattivazione dei Codici identificativi personali (USERID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso ai sistemi, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre sei mesi;
- garantire il rispetto di tutte le misure di sicurezza per i trattamenti elettronici specificate nel prosieguo;
- istruire il personale competente – o provvedere direttamente - alla distruzione o allo smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego.

Criteria per l'esecuzione del trattamento dei dati personali

Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto del diritto di riservatezza e della dignità dell'interessato.

Oggetto del trattamento devono essere i soli dati personali necessari per lo svolgimento delle attività istituzionali.

I dati personali devono essere trattati in modo lecito e corretto, raccolti e registrati secondo fini legittimi. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti e trattati.

Nei trattamenti è autorizzata solo l'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

È compito del Responsabile per la protezione dei dati, ma anche dei Responsabili del trattamento, verificare, per delega del Titolare del trattamento, la liceità e la correttezza dei trattamenti, l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite per compiti istituzionali.

I dati che, anche a seguito di verifiche, risultassero eccedenti, non pertinenti o non necessari, non potranno essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.

I trattamenti di dati effettuati attraverso l'accesso in banche dati, facenti capo a Titolari diversi dall'Azienda (interconnessione di banche dati), sono espletati in base ad espressa disposizione di legge o approvata regolamentazione. In ogni caso devono essere adottate misure tali da garantire che i dati personali, soprattutto quelli rientranti in categorie particolari, siano accessibili ai soli incaricati del trattamento e nella misura strettamente necessaria allo svolgimento delle proprie mansioni.

Valutazione di impatto sulla protezione dei dati (accountability)

Padania Acque S.p.A. tratta categorie di dati personali che rientrano nelle casistiche "particolari" di cui all'articolo 9, paragrafo 1 e articolo 10 del GDPR. In considerazione di ciò, nel rispetto delle disposizioni comunitarie, è stata effettuata una valutazione di impatto sulla protezione dei dati trattati.

In particolare, nelle informazioni di cui ai Registri dei trattamenti sono state valutate ed inserite le relative descrizioni dei trattamenti medesimi, delle finalità per cui tali trattamenti vengono effettuati, una valutazione dei rischi, nonché le misure previste per affrontarli, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità alla regolamentazione europea, tenuto conto dei diritti e degli interessi legittimi degli interessati.

In ragione delle misure di sicurezza adottate, delle responsabilità professionali dei collaboratori, della formazione dei dipendenti e dell'organizzazione aziendale, si ritiene di poter valutare **basso il profilo di rischio** per:

- i dati del personale dipendente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali);
- i dati personali dei clienti (dagli stessi forniti per l'espletamento di quanto previsto dalle relazioni commerciali esistenti, compresi i dati sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi);
- i dati personali dei fornitori (concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali e quelli necessari ai sensi della normativa sulla contrattualistica pubblica);
- i dati personali dei professionisti cui Padania Acque S.p.A. affida incarichi;

- i dati personali delle categorie di soggetti sopra elencati ricavati da albi, elenchi pubblici, visure camerali e/o documentazione accessibile ai sensi della normativa sull'accesso civico e sulla trasparenza.

Parimenti, si ritiene di poter determinare **basso il profilo di rischio per il trattamento delle categorie particolari di dati personali dei dipendenti**, in quanto l'accesso (fisico e informatico) ai dati è perfettamente tutelato.

I dati vengono trattati e conservati in fascicoli riposti in armadi dotati di chiusura, nonché trattati tramite computer in rete, in modalità protetta, con accesso ad Internet, per poi essere archiviati al termine della pratica.

Gli uffici della Società Padania Acque S.p.A., presso i quali si espletano le attività di trattamento dei dati, sono ubicati in due palazzine a due piani in Via del Macello n. 14 - Cremona e in un magazzino a fianco; in una palazzina in zona Via Colombo, in Crema e in due ulteriori immobili siti in Via del Depuratore – Cremona. Tutti gli immobili hanno accessi controllati da citofoni e sistemi di autenticazione tramite badge; le sedi centrali sono dotate di un sistema di videosorveglianza con lo scopo di preservare i locali da atti di vandalismo e da eventuali furti.

Gli uffici sono separati dalla zona front-office. Il personale esterno non può accedere a documenti cartacei e sistema informatico senza autorizzazione e senza controllo.

La sala server si trova presso la palazzina di Via del Macello, in Cremona, opportunamente separata e con accesso tramite badge.

Le strutture esterne delle palazzine prevedono cancelli e recinzione dei fabbricati, sorveglianza notturna, sistema di allarme volumetrico interno per la sala CED e telecontrollo ambientale.

Gli uffici sono dotati di porte con chiusura a chiave.

Padania Acque S.p.A. gestisce diversi impianti nei vari comuni serviti, dove viene effettuato telecontrollo, essendo queste di proprietà. In tali sedi non esiste alcuna documentazione contenente dati personali e l'accesso alla rete interna non è permessa, se non per scambio di dati informatici.

Sono presenti, inoltre, presso il territorio comunale di Soncino, Pandino, Soresina, Castelleone e Casalmaggiore, sedi distaccate dell'area front-office per la gestione delle pratiche clienti e, comunque, a servizio dell'utenza. Tali sportelli vengono gestiti da personale, avente comprovate qualità professionali, a tal fine preposto da parte dei Comuni soci interessati dall'attività e/o dalle rispettive società di servizi pubblici, in forza di negozi giuridici atti a regolamentarne l'attività. I soggetti rispettivamente coinvolti sono stati tutti assoggettati agli obblighi di riservatezza.

L'accesso ai sistemi è assoggettato all'inserimento di credenziali rilasciate dalla stessa Padania Acque S.p.A., le quali consentono l'accesso tramite collegamento VPN al server di Padania Acque S.p.A. ed al relativo applicativo Esperta per la gestione dei clienti.

I dati inseriti nelle anagrafiche dei clienti/utenti sono condivisi in rete con gli incaricati esterni e le informazioni a sistema, tra la sede aziendale e le sedi distaccate, viaggiano in modalità crittografata.

Le apparecchiature informatiche critiche (server di rete, apparecchiature di telecomunicazione e dispositivi di copia) sono situati in locali ad accesso controllato; i locali ad accesso controllato sono chiusi anche se presidiati; i dispositivi di accesso sono custoditi a cura del Responsabile dei Servizi Informativi, quale Amministratore di Sistema informatico.

I Responsabili dei trattamenti indicati nei registri dei trattamenti sono anche responsabili dell'area in cui si trovano i dati oggetto di attenzione.

L'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate; il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità; i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato.

Attività propedeutica ed indispensabile per un corretto e prudente trattamento dei dati personali da parte dei molteplici incaricati e responsabili dei trattamenti presso la Società, è la realizzazione di un adeguato Piano di formazione.

La formazione degli incaricati viene effettuata al momento dell'ingresso in servizio, in caso di installazione di nuovi strumenti per il trattamento dei dati e, comunque, in tutti i casi di aggiornamento normativo.

L'entrata in vigore del nuovo Regolamento Europeo n. 2016/679 è stata affrontata dall'azienda in modo responsabile ed attento; è stata garantita la formazione del personale in merito agli obblighi discendenti dalla normativa inerente la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché della circolazione di tali dati; sono stati chiariti ed attenzionati i principi sanciti dalla normativa europea, applicabili al suddetto trattamento, nonché i diritti dell'interessato ed i comportamenti ed attività da porre in essere in presenza di eventuali violazioni discendenti da trattamenti non idonei.

La formazione, che viene periodicamente rinnovata ed aggiornata, persegue le finalità di sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali; proporre buone pratiche di utilizzo sicuro della rete; riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

Art. 35 GDPR: Valutazione di impatto sulla protezione dei dati: Videosorveglianza

Nell'esercitare attività di videosorveglianza, viene rispettato il principio di proporzionalità tra i mezzi impiegati ed i fini perseguiti. In particolare, si precisa che:

- il trattamento dei dati avviene secondo correttezza e per scopi determinati, espliciti e legittimi;
- l'attività è svolta per la prevenzione di un pericolo concreto o di specifici reati;
- oltre al Titolare del Trattamento ed all'Amministratore di sistema, solo le autorità competenti sono legittimate ad accedere alle informazioni raccolte.

Inoltre, l'attività di videosorveglianza è esercitata osservando le seguenti indicazioni:

- alle persone che possono essere riprese sono fornite indicazioni chiare, anche se sintetiche, circa la presenza di impianti di videosorveglianza;
- è scrupolosamente rispettato il divieto di controllo a distanza dei lavoratori;
- sono raccolti i dati strettamente necessari per il raggiungimento delle finalità perseguite;
- vengono registrate le sole immagini indispensabili, avendo limitato l'angolo di visuale delle riprese;
- vengono evitate, salvo siano indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti;
- il periodo di conservazione dei dati è limitato allo stretto necessario e non eccede mai i termini di conservazione previsti dalle disposizioni normative di volta in volta vigenti;
- la conservazione dei dati oltre il termine previsto è possibile solo in relazione al verificarsi di illeciti o quando siano in corso indagini giudiziarie.
- I dati raccolti per fini determinati non sono utilizzati per finalità diverse o ulteriori, fatte salve le esigenze di polizia o di giustizia e non sono diffusi o comunicati a terzi.

Art. 35 GDPR: Valutazione di impatto sulla protezione dei dati: Dati relativi alla salute

I dati personali idonei a rivelare lo stato di salute dell'interessato vengono trattati nell'ambito delle attività gestite dal Servizio Personale, ai fini della tenuta, aggiornamento ed archiviazione del fascicolo personale di ogni dipendente in servizio e, per i tempi individuati ed indicati nel relativo registro dei trattamenti, dopo lo stato di quiescenza del lavoratore medesimo e/o, comunque, anche dopo il venir meno del rapporto di lavoro. Vengono, trattati, altresì, ai fini noti ad ogni lavoratore, per il tramite del medico dell'Azienda, competente in relazione ai provvedimenti organizzativi aziendali, ovvero per il tramite del medico di fiducia dell'interessato da lui designato, o del medico che ha prescritto eventuali accertamenti.

Parimenti, per i fini giuridicamente rilevanti, ai sensi delle norme sulla sicurezza (D.lgs. 81/08), vengono trattati, ma nei limiti della pertinenza, e - per quanto di sua competenza - secondo il principio della minimizzazione dei dati, dalla RSPD aziendale, nonché dal responsabile del lavoratore che viene assoggettato ad eventuali restrizioni e prescrizioni dal medico competente, in relazione alla mansione svolta.

Dati relativi alla salute dei dipendenti possono essere trattati anche dal personale preposto all'esercizio delle attività assicurative e dall'intermediario (broker) aziendale, nell'ambito della trasmissione, verifica e perfezionamento delle pratiche afferenti agli infortuni e/o le pratiche di responsabilità civile autoveicoli (RCA). Per il trattamento di tali dati è assicurata massima riservatezza e massima garanzia da un punto di vista tecnico-organizzativo. Il settore preposto al servizio assicurativo gode di un accesso riservato per le scansioni ed archiviazioni dei documenti da trasmettere all'intermediario assicurativo e le stesse comunicazioni ed aggiornamenti relativi lo stato delle pratiche aperte risiedono su un portale dedicato, con accesso riservato – mediante credenziali di accesso segrete – al solo personale preposto del settore legale che segue l'area "assicurazioni".

Art. 35 GDPR: Valutazione di impatto sulla protezione dei dati: dati relativi a condanne penali e a reati

Per quanto riguarda Amministratori e dipendenti, i dati personali atti a rivelare eventuali carichi pendenti e/o riscontri positivi presso i casellari giudiziari, sono trattati dalla Direzione Generale, che li conserva in armadi chiusi a chiave o in propri archivi informatici protetti da password.

Per quanto riguarda i fornitori, i dati personali atti a rivelare eventuali carichi pendenti e/o riscontri positivi presso i casellari giudiziari, vengono trattati dal personale preposto all'espletamento delle attività d'appalto, nell'ambito delle procedure di aggiudicazione di lavori, servizi o forniture, secondo il disposto normativo di cui al Codice dei contratti pubblici (D.lgs. 50/2016).

Il trattamento è autorizzato/imposto dalla normativa sopra riportata, ai fini delle verifiche di idoneità morale degli operatori economici partecipanti alle procedure di gara bandite da Padania Acque S.p.A., nella sua veste di Stazione Appaltante.

Il trattamento dei dati viene effettuato in modo riservato e responsabile dal personale autorizzato e gli stessi dati vengono conservati per il tempo strettamente necessario al trattamento, per poi essere distrutti al termine del medesimo.

La conservazione dei dati, nelle more dei tempi di aggiudicazione ed esecuzione contrattuale, avviene in modalità protetta presso l'Ufficio appalti, il quale detiene i dati in armadi chiusi a chiave. Lo stesso Ufficio rimane chiuso a chiave durante le ore in cui il personale non è presente in azienda.

Tipologia dei dati trattati

Padania Acque S.p.A., ai fini ed in considerazione delle attività oggetto del servizio di cui la stessa è Gestore, tratta i seguenti dati:

- dati personali di clienti/utenti, dichiarati in sede di stipula contratto di fornitura e/o in fase di perfezionamento dei negozi giuridici legati al servizio idrico integrato in genere, compresi i dati sul patrimonio e sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;
- dati personali, anche particolari, dei dipendenti, quali quelli necessari al rapporto di lavoro, alla reperibilità, alla corrispondenza con gli stessi o richiesti ai fini fiscali, previdenziali ed assistenziali; dati di natura bancaria; adesione alle organizzazioni sindacali; dati sullo stato di salute;
- dati personali di terzi, forniti dai clienti per l'espletamento delle attività derivanti dalle relazioni commerciali in essere, compresi i dati sul patrimonio e sulla situazione economica, o necessari ai fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;
- dati personali dei fornitori (in caso di persona giuridica, i dati afferiscono la persona del rappresentante legale), concernenti anche quelli rilevanti ai fini fiscali o relativi i dati di natura bancaria;
- dati personali di liberi professionisti cui Padania Acque affida incarichi o si rivolge per consulenze;
- dati particolari degli operatori economici partecipanti alle procedure di gara bandite da Padania Acque ai fini dell'acquisizione di lavori, servizi o forniture, quali i carichi pendenti ed il casellario giudiziale, ai sensi della normativa vigente (D.lgs. 50/2016).

Analisi dei rischi

➤ Minacce a cui sono sottoposte le risorse hardware

Le risorse hardware sono sottoposte alle seguenti minacce:

- malfunzionamenti dovuti a guasti;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica.

➤ Minacce a cui sono sottoposte le risorse connesse in rete

Le principali minacce alle risorse connesse in rete possono provenire dall'interno, dall'esterno o da una combinazione interno/esterno e riguardano:

- l'utilizzo della LAN/Intranet (interne);
- i punti di contatto con il mondo esterno attraverso Internet (esterne);
- lo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o le operazioni di download eseguite tramite il browser (interne/esterne).

➤ Minacce a cui sono sottoposti i dati trattati

Le principali minacce cui sono sottoposti i dati trattati vengono individuate in:

- accesso non autorizzato ai documenti contenenti le informazioni riservate (modifica, estrazione, consultazione, uso, cancellazione, distruzione, comunicazione mediante trasmissione, diffusione o qualsiasi altra messa a disposizione) da parte di soggetti autorizzati, interni e/o esterni;
- modifiche accidentali (errori, disattenzioni,) da parte di soggetti autorizzati;
- modifica, estrazione, uso, cancellazione, distruzione, comunicazione mediante trasmissione e/o divulgazione non autorizzata dei dati da parte dei soggetti non autorizzati.

➤ Minacce a cui sono sottoposti i supporti di memorizzazione

Le principali minacce ai supporti di memorizzazione possono essere così individuate:

- distruzione e/o alterazione a causa di eventi naturali;
- imperizia degli utilizzatori;

- sabotaggio;
- deterioramento nel tempo (invecchiamento dei supporti);
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

Misure di sicurezza tecnico-organizzative e garanzie adeguate

Padania Acque S.p.A., per assicurare un elevato grado di *compliance* rispetto alle misure di sicurezza tecnico-organizzative necessarie ed offrire garanzie adeguate e conformi alla normativa vigente, al fine di far fronte a potenziali violazioni di dati personali trattati, attua una serie di attività, preventive/cautelative e, più nel dettaglio:

- esegue un backup giornaliero dei dati e dei sistemi installati sul server tramite un servizio di MANAGED BACKUP SERVICES che permette un salvataggio con le seguenti caratteristiche:
 - Copertura per 7 TB /scalabile;
 - Copertura per 31 Virtual Machine/Server;
 - Short Retention c/o cliente 30 giorni;
 - Retention standard su nastro di 12 mesi/anni;
 - Infrastruttura servizio c/o Datacenter Elmec e Cliente;
 - Licensing a servizio Elmec;
 - Archiviazione nastri c/o Datacenter di Backup Elmec;
 - Connettività Elmec (dedicata) in Upload per ricezione dati;
 - 10 Mbps - 24x7;
 - Monitoraggio dei sistemi a perimetro di backup eseguito da personale Elmec in modalità 24x7;
 - Gestione Trasferimento dati da Datacenter Cliente verso Elmec;
 - Change Management.
- Ha disposto che non siano lasciati incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e classificatori contenenti dati personali, ma che gli stessi vengano prelevati per il tempo necessario al trattamento, per poi essere riposti negli appositi armadi.
- Quando è dato un ordine di stampa, il documento stampato dovrà essere prontamente prelevato e consegnato all'interessato.
- Il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti deve essere reso illeggibile prima di essere riposto negli appositi sacchi di plastica chiusi in modo che i documenti contenuti non possano accidentalmente fuoriuscire.
- Per la navigazione Internet Padania Acque S.p.A. utilizza Internet Explorer e/o Google Chrome aggiornato in occasione di ogni rilascio di *patch* od aggiornamenti da parte della casa produttrice.
- La società si è dotata di un sistema Web *filtering* (Sophos) e di un sistema di *antispam* (Office 365), che servono a proteggere la rete contro spam, virus, attacchi a livello di connessione e altre minacce per la sicurezza mirate all'infrastruttura. Il sistema Informativo Aziendale è protetto da intrusioni esterne tramite *firewall* Sophos.
- È stato programmato un controllo delle vulnerabilità esterne tramite sistema di controllo di vulnerabilità che, appoggiandosi a motori di scansione sicuri, riconosciuti a livello mondiale, attacca il sistema nello stesso modo e con gli stessi accorgimenti che utilizzerebbe un *hacker*.
- Per lo scambio di posta elettronica interna ed esterna Padania Acque S.p.A. utilizza Outlook 365 ad ogni rilascio di *patch* od aggiornamenti da parte della casa produttrice.

- Ogni ufficio che tratta dati personali è munito di indirizzo PEC riservato per la trasmissione delle comunicazioni necessarie e collegate al perfezionamento delle pratiche che richiedono il trattamento dei suddetti dati.
- Le aree aziendali che trattano dati particolari usufruiscono di scansioni riservate il cui accesso in rete è consentito solo ai preposti al trattamento.
- Tutti gli uffici sono dotati di armadi muniti di idonea serratura per permettere la conservazione sicura e protetta della documentazione contenente dati personali, con particolare attenzione agli orari in cui in azienda non è presente personale autorizzato al trattamento.
- Tutti gli uffici sono muniti di porte con serratura e chiavi, per assicurare la chiusura di quegli stessi uffici di particolare importanza per i trattamenti posti in essere, al termine dell'orario di lavoro o, comunque, durante le ore di pausa pranzo.
- Gli immobili societari sono assoggettati a sistema di videosorveglianza ed allarmati durante le ore non lavorative.
- Ogni dipendente gode di un accesso riservato in rete, ai fini della conservazione e successiva archiviazione dei documenti, assoggettato a *backup* quotidiano.
- Le comunicazioni trasmesse tra le sedi aziendali e le sedi del *call center* esterno sono crittografate.

Possono essere definiti, altresì, **bassi i seguenti rischi:**

- il rischio di accesso ai locali dell'azienda, atteso che l'ingresso è controllato e che è presente un citofono e personale di reception; dalla stessa area *front-office* non è possibile immettersi nelle restanti aree aziendali, in quanto è presente una porta che si apre con il solo *badge* aziendale;
- il rischio di accesso ai singoli uffici, atteso che tutti sono dotati di porte con chiusura e l'ingresso di terzi estranei può avvenire solo previa accettazione e controllo;
- il rischio di accesso ai singoli strumenti da parte di persone non autorizzate, essendo controllato l'accesso da parte di terzi; la zona di attesa è distanziata dagli strumenti;
- il rischio che riguarda gli strumenti elettronici, essendo state adottate da Padania Acque S.p.A. le misure di sicurezza tendenti a ridurre il rischio gravante sui dati e derivante dalla gestione di detti strumenti;
- il rischio relativo la documentazione cartacea, in quanto la stessa viene conservata/archiviata singolarmente da ogni incaricato preposto all'espletamento della pratica, in armadi chiusi a chiave e ubicati presso lo stesso ufficio del preposto/responsabile. È fatta eccezione, ovviamente, per gli eventi naturali.

Di fatti, le aree ed i locali potrebbero essere interessati da eventi naturali, quali incendi, allagamenti e corto circuiti. Ovviamente Padania Acque S.p.A. ha provveduto ad adottare le disposizioni di sicurezza stabilite dalla legge (81/08). Essendo, poi, l'azienda dotata di dispositivi salvavita, il rischio può comunque definirsi basso.

- Il rischio di deterioramento dei dati presenti nei supporti di memorizzazione, attesi i frequenti *backup*. Essi, inoltre, sono conservati in luogo chiuso a chiave, così come i dischi di installazione dei programmi software adottati.
- Il rischio afferente la riservatezza o la distrazione, o l'incuria degli incaricati al trattamento dei dati, considerando che gli stessi sono qualificati ed affidabili e dimostrano riservatezza ed attenzione nella gestione dei dati medesimi.

Di seguito, vengono elencate anche le misure di carattere elettronico/informatico adottate:

- utilizzo di una configurazione ridondante di DC (domain controller);
- presenza di un gruppo di continuità elettrica per la sala CED;
- attivazione di un sistema di backup centralizzato e automatizzato, con periodicità giornaliera e settimanale;
- installazione di un firewall con hardware dedicato, per proteggere la rete dagli accessi indesiderati attraverso internet;
- installazione di un sistema antivirus su tutte le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico, con frequenza giornaliera;
- definizione delle regole per la gestione di strumenti elettronico/informatico;
- definizione delle regole di comportamento per minimizzare i rischi da virus.
- Effettuazione di tutte le operazioni di manutenzione on-site, con la supervisione dell'incaricato del trattamento o di un suo delegato.
- Divieto di lasciare incustodito, o accessibile, lo strumento elettronico. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- Divieto di memorizzazione di dati personali non inerenti alla funzione svolta.
- Divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati personali, senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- Divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.

La stampa di documenti contenenti dati personali è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Piano formale di *Incident Response*

Tutti gli incaricati del trattamento dei dati hanno l'obbligo di avvisare tempestivamente il Responsabile della sicurezza informatica o l'Amministratore di sistema o il Responsabile del trattamento dei dati o il Responsabile per la protezione dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli *user-id*;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli *hard disk* originali a partire dalle ultime copie di *backup* ritenute valide. Altrimenti il Titolare del trattamento, il Responsabile del trattamento e l'Amministratore di Sistema coinvolgeranno esperti e/o autorità competenti.

La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di *incident response*, tenendo presente quanto sotto indicato:

- dovrà essere eseguita una copia *bit to bit* degli *hard disk* del sistema compromesso;

- se l'incidente riguarda i dati, il restore dei dati può avvenire sulla copia di cui al punto precedente, a partire dalle ultime copie di *backup* ritenute valide.

In caso di violazione di dati contenuti in documentazione cartacea, archiviata o ancora in fase di trattamento, ogni incaricato dovrà avvisare tempestivamente il Titolare del trattamento e/o il Responsabile del trattamento dei dati e il Responsabile per la protezione dei dati, al fine di permettere a questi ultimi il compimento di tutte le azioni necessarie ai sensi degli artt. 33 e 34 del Regolamento 2016/679 e, precisamente, laddove necessario, la notifica della violazione dei dati personali all'autorità di controllo e la comunicazione della medesima violazione all'interessato.

Trattamento dei dati da parte di Responsabili e "incaricati/preposti"

La Società ha provveduto a nominare Responsabili del trattamento i dipendenti che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento, effettuato da ognuno di loro per conto del Titolare del trattamento, garantisca la tutela dei diritti dell'interessato.

Di tali Responsabili dei trattamenti è data evidenza in seno ai Registri dei trattamenti, redatti ai sensi dell'articolo 30 del GDPR. Nei medesimi registri viene individuato ed indicato il nome del Titolare del trattamento e del Responsabile della protezione dei dati (DPO), nominati dall'Organo amministrativo societario.

I Responsabili del trattamento dovranno/potranno trattare esclusivamente i dati personali necessari per l'espletamento delle attività afferenti alla propria area, così come da istruzione documentata del Titolare del trattamento, nonché elencazione di cui al registro dei trattamenti.

Il Responsabile del trattamento deve garantire che la stessa riservatezza a lui richiesta ai fini delle attività di trattamento dati personali, venga applicata e rispettata dai soggetti dallo stesso incaricati al medesimo trattamento.

Qualsiasi violazione di trattamento andrà notificata all'autorità di controllo e comunicata all'interessato, laddove ricorrano le condizioni di cui agli artt. 32 e 33 del Regolamento Europeo.

Trattamento di dati affidati all'esterno

Agli Enti, agli organismi, agli altri soggetti pubblici e privati esterni all'Azienda, agli operatori economici con i quali Padania Acque S.p.A. ha contratti per l'acquisizione di servizi di manutenzione sui sistemi e sui software gestiti esternamente e/o a tutti i soggetti ai quali siano affidati attività o servizi, con esclusivo riferimento alle connesse operazioni di trattamento dei dati, viene loro attribuita la funzione di Responsabile del trattamento, ai sensi dell'articolo 28 del Regolamento 2016/679.

Nei contratti di affidamento di attività o di servizi a soggetti esterni all'Azienda, è inserita apposita clausola di garanzia, con la quale il soggetto affidatario si impegna, per i trattamenti di dati effettuati in forza del rapporto contrattuale, all'osservanza delle norme di legge sulla protezione dei dati personali, assumendosi la relativa responsabilità in caso di violazione di trattamento.