



**MODELLO ORGANIZZATIVO IN MATERIA DI  
PROTEZIONE DI DATI PERSONALI**

Rev. 0  
del 26-05-2022

0	26-05-2022	Prima stesura del modello
<b>Rev.</b>	<b>Data</b>	<b>Descrizione modifica</b>

Approvato dal Consiglio di Amministrazione in data 26-05-2022

## Indice:

1. Oggetto e Finalità .....	3
2. Definizioni .....	4
3. Titolare, responsabili, incaricati.....	6
4. Amministratore di sistema.....	6
5. Criteri per l'esecuzione del trattamento dei dati personali.....	8
6. Tipologia dei dati trattati .....	9
7. Accountability .....	9
8. Videosorveglianza .....	11
9. Geolocalizzazione mezzi e persone .....	12
10. Dati relativi alla salute .....	13
11. Dati relativi a condanne penali e a reati.....	13
12. Analisi dei rischi, misure di sicurezza tecnico-organizzative e garanzie adeguate .....	14
13. Piano formale di Incident Response e data breach .....	15
14. Trattamento dei dati da parte di Responsabili e “incaricati/preposti”.....	16
15. Trattamento di dati affidati all'esterno .....	16
16. Allegati .....	17

## **1. Oggetto e Finalità**

Il presente Modello Organizzativo in materia di protezione di dati personali – nel definire regole relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché quelle relative la libera circolazione degli stessi 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 e del D.lgs. 196/03, così come modificato e integrato dal D.lgs. 101/2018 – si prefigge l’obiettivo di permettere a tutti i potenziali interessati di individuare le generali linee di azioni adottate in materia da Società Acqua Lodigiana S.r.l., fermo restando che i dettagli operativi e analitici impiegati sono stati trattati in specifici documenti/procedure interne all’uopo richiamati nel presente documento.

Resta inteso che eventuali trattamenti difformi rispetto a quanto precisato nel presente documento e/o negli specifici documenti/procedure interne sopra richiamati e/o nel registro dei trattamenti o, comunque, effettuati per finalità diverse da quelle per le quali i dati personali sono stati raccolti, dovranno essere ricondotti a stato di liceità nel più breve tempo possibile.

Fermo quanto sopra, nel rispetto del Regolamento Europeo 2016/679, Società Acqua Lodigiana S.r.l. 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 Società Acqua Lodigiana S.r.l. 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.

## 2. 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.

### **3. Titolare, responsabili, incaricati**

- ❖ **Titolare del trattamento**: Rappresentante Legale pro-tempore;
- ❖ **Responsabile della protezione dei dati (DPO)**: *ing. Fabio Grassani*;
- ❖ **Responsabile del trattamento**: come da Registro trattamento;
- ❖ **Incaricati del trattamento dei dati**: tutti i dipendenti preposti al trattamento da parte dei Responsabili delle aziendali;
- ❖ **Amministratore di sistema**: *ing. Fabio Grassani* – Responsabile Ufficio Sistemi Informatici.

### **4. Amministratore di sistema**

L'Amministratore di sistema è stato individuato con apposito atto di nomina del 22.2.2013 che individua, tra l'altro, i compiti affidati al medesimo.

Ad esso, in particolare, sono assegnati i seguenti compiti, come riportati nel precitato atto di nomina:

“

- *impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali eseguiti tramite strumenti informatici, secondo quanto previsto dal punto 1 al punto 10 del Disciplinare Tecnico Allegato B) al D.Lgs. 196/2003. A tale proposito, sarà suo compito predisporre:*
  - *un sistema di autenticazione ed accesso al sistema tramite Userld e Password (con almeno otto caratteri);*
  - *una procedura per disattivare Userld se non utilizzato da almeno sei mesi (salvo diversa autorizzazione);*
  - *una procedura di autorizzazione per l'accesso alle applicazioni software.*

- *impostare e gestire un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 12 a 14 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;*
- *verificare costantemente che la nostra Società abbia adottato le misure minime di sicurezza per il trattamento dei dati personali, previste dall'art. 34 del D. Lgs. n. 196/2003, e dal Disciplinare tecnico, allegato B) al decreto legislativo medesimo, provvedendo senza indugio agli adeguamenti eventualmente necessari;*
- *suggerire al titolare del trattamento l'adozione e l'aggiornamento delle più ampie misure di sicurezza atte a realizzare quanto previsto dall'art. 31 del D. Lgs. n. 196/2003, che dispone che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;*
- *curare, su incarico del titolare del trattamento, l'adozione e l'aggiornamento delle misure "idonee" di cui al punto precedente;*
- *attivare e aggiornare con cadenza almeno semestrale idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaboratori del sistema informativo a Lei affidato, contro il rischio di intrusione e contro l'azione dei virus informatici. A tale proposito, predisposizione di idonei strumenti elettronici (antivirus, firewall, etc.) da aggiornare almeno con cadenza semestrale per la protezione dei dati personali dal rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale.*
- *predisporre idonei strumenti di controllo degli accessi alla rete informatica aziendale e ai singoli terminali o elaboratori affinché non possano essere messe in atto, da parte di soggetti interni all'organizzazione o da parte di terzi, in via accidentale o intenzionale, azioni che possano portare alla perdita o al danneggiamento dei dati;*
- *impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedono il salvataggio dei dati, con frequenza almeno settimanale, su supporti permanenti oppure su supporti di rete sottoposti automaticamente a backup;*
- *adottare e mantenere efficienti le procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;*

- *predisporre ed aggiornare, ogni qualvolta lo si ritenga necessario e comunque entro il 31 marzo di ogni anno, il documento programmatico sulla sicurezza previsto dal punto 19 del Disciplinare tecnico, allegato B) al D.Lgs. n. 196/2003;*
- *predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza adottate in azienda.*

*Sarà incaricato di riferire periodicamente al Direttore Generale e, su richiesta, al Titolare del trattamento dei dati sullo svolgimento dei Suoi compiti, dando loro inoltre piena collaborazione nello svolgimento delle verifiche periodiche circa il rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate aziendalimente”.*

## **5. Criteri per l'esecuzione del trattamento dei dati personali**

Il trattamento dei dati deve essere effettuato così che venga assicurato 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.

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.



## **6. Tipologia dei dati trattati**

Società Acqua Lodigiana S.r.l., 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 alla persona del rappresentante legale), concernenti anche quelli rilevanti ai fini fiscali o relativi i dati di natura bancaria;
- dati personali di liberi professionisti cui vengono affidati incarichi o si rivolge per consulenze;
- dati particolari degli iscritti all'Albo fornitori e degli operatori economici partecipanti alle procedure di gara bandite 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).

## **7. Accountability**

Come sopra accennato, non è da escludersi che Società Acqua Lodigiana S.r.l. tratti categorie di dati personali che rientrano nelle casistiche "particolari" di cui all'art. 9, paragrafo 1 e art. 10 del GDPR. In considerazione di ciò, nel rispetto delle disposizioni comunitarie, è stata effettuata una valutazione di impatto sulla protezione dei dati trattati.

Per questo Società Acqua Lodigiana S.r.l. ha valutato le relative descrizioni dei trattamenti medesimi, le finalità per cui tali trattamenti vengono effettuati, oltre ad aver effettuato 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 Società Acqua Lodigiana S.r.l. 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. Di fatti, 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 di Società Acqua Lodigiana S.r.l., presso i quali si espletano le attività di trattamento dei dati, sono ubicati presso la sede legale sita in Lodi, via dell'Artigianato, 1/3, Località San Grato, il laboratorio di analisi sito in Lodi, via dell'Industria, 3/5, Località San Grato e presso il Centro Operativo sito in Casalpusterlengo, via Galimberti, 17. Tutti gli immobili hanno accessi controllati da citofoni e sistemi di autenticazione tramite badge; le sedi sono dotate di un sistema di videosorveglianza e/o di allarme 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 sede legale sita in Lodi, via dell'Artigianato, 1/3 e risulta opportunamente separata e inibita all'accesso.

Società Acqua Lodigiana S.r.l. 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.

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 alla 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.

## **8. Videosorveglianza**

Nell'esercitare attività di videosorveglianza, viene rispettato, come emergente dall'informativa all'uopo predisposta e affissa nei luoghi soggetti a videosorveglianza, 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.

## **9. Geolocalizzazione mezzi e persone**

Per esigenze logistiche ed al contempo assicurare una più efficiente gestione e manutenzione del parco veicoli, nonché per garantire la sicurezza e l'incolumità dei lavori ed infine per prevenire e contrastare eventi criminosi e ai danni dei beni aziendali, Società Acqua Lodigiana S.r.l. ha installato sul proprio parco veicoli un sistema di localizzazione denominato "LoJack".

Di ciò ne è stata data notizia ai lavoratori dipendenti ai quali è stata altresì fornita l'informativa all'uopo dedicata qui da intendersi espressamente richiamata.

Società Acqua Lodigiana S.r.l. ha altresì provveduto, in data 2.8.2017, a stipulare un verbale di accordo ex art. 4 della l. n. 300/1970.

Oltre a quanto sopra, è opportuno dar conto del fatto che Società Acqua Lodigiana S.r.l. ha altresì fornito ai propri dipendenti che prestano la propria attività in luoghi isolati, diversi dall'azienda, in assenza di almeno un collega, di un dispositivo di sicurezza personale collegato ad una centrale operativa attiva h24. Detto dispositivo è stato fornito per garantire la sicurezza e l'incolumità dei lavoratori dipendenti, ai quali è stata anche fornita specifica informativa al trattamento dati.

Anche in questo caso Società Acqua Lodigiana S.r.l. ha altresì provveduto, in data 9.7.2015, a stipulare apposito verbale di accordo sindacale.

## **10. 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 (Titolare trattamento dati autonomo), 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 RSPP aziendale, nonché dal responsabile del lavoratore che viene assoggettato ad eventuali restrizioni e prescrizioni dal medico competente, in relazione alla mansione svolta.

## **11. 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 Società Acqua Lodigiana S.r.l., 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 in conformità alla normativa vigente in materia, 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

o in archivi informatici protetti. Lo stesso Ufficio rimane chiuso a chiave durante le ore in cui il personale non è presente in azienda.

## **12. Analisi dei rischi, misure di sicurezza tecnico-organizzative e garanzie adeguate**

In via preliminare si ricorda che Società Acqua Lodigiana S.r.l. ha adottato un regolamento interno recante “regolamento per l’utilizzo sistemi informatici e di telecomunicazioni” con l’obiettivo, tra l’altro, di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Si tratta di un regolamento che è stato consegnato a ciascun dipendente e collaboratore, che possibile consultare presso l’ufficio del Responsabile Sistemi Informatici, l’Ufficio Qualità Sicurezza e Ambiente e in una apposita cartella della intranet aziendale e che si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell’Azienda, a prescindere dal rapporto contrattuale con la stessa intrattenuto (consulenti, lavoratori somministrati, collaboratori a progetto, tirocinanti, ecc.).

Detto regolamento è parte integrante della privacy policy di Società Acqua Lodigiana S.r.l.

Oltre a ciò, ancorché non materialmente allegati alla presente per ragioni di riservatezza, è parte integrante del presente modello anche il documento denominato “piano di continuità operativa”.

In aggiunta a quanto precisato al precedente paragrafo 7. e a quanto recato nel documento “analisi dei rischi”, Società Acqua Lodigiana S.r.l. ritiene altresì di poter definire 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;
- 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 Società Acqua Lodigiana S.r.l. le misure di sicurezza sopra richiamate 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.

- Società Acqua Lodigiana S.r.l. 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 opportuni archivi informatici protetti da accessi non autorizzati, così come i dischi di installazione dei programmi software adottati.
- Il rischio afferente alla riservatezza o alla distrazione, o all'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.

### **13. Piano formale di Incident Response e data breach**

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, ai sensi della adottata procedura di data breach, 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*.

In caso di violazione di dati contenuti in documentazione cartacea, archiviata o ancora in fase di trattamento, ogni incaricato dovrà avvisare tempestivamente, ai sensi della procedura di data breach, 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.

#### **14. 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, laddovericorrano le condizioni di cui agli artt. 32 e 33 del Regolamento Europeo.

#### **15. 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 Società Acqua Lodigiana S.r.l. 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.



## **16. Allegati**

Ancorché non materialmente allegati al presente Modello Organizzativo in materia di protezione di dati personali, costituiscono parte integrante dello stesso il registro trattamenti, le informative privacy specificamente adottate dalla Società, la procedura di data breach, il Regolamento per l'uso dei sistemi informatici, il piano di continuità operativa (ovvero, in sua vece, il documento programmatico per la sicurezza ex allegato B) al D.lgs. 196/2003) e il PR. 10 allegato al Modello 231.