REGOLAMENTO GENERALE AZIENDALE PRIVACY

(per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali)

(approvato con Delibera CdA n. 39 del 12/12/2019)

Sommario

Art. 1 - Oggetto del regolamento

1. Il presente regolamento disciplina il trattamento dei dati personali contenuti nelle banche dati organizzate, gestite od utilizzate dalla Società in relazione allo svolgimento delle proprie finalità istituzionali, in attuazione:

- *del Regolamento UE 2016/679 del 27 aprile 2016 relativo alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" e che abroga la direttiva 95/46/CE (di seguito GDPR);*
- *del D.Lgs. 196/2003 così come rinovellato dal D.Lgs. 101/2018.*

Art. 2 - Finalità

1. La Società, nell'assolvimento delle proprie finalità istituzionali secondo i principi di trasparenza, efficacia ed economicità, garantisce che il trattamento dei dati personali si svolga con modalità che assicurino il rispetto del diritto alla riservatezza ed all'identità personale nonché delle norme vigenti in materia di protezione e gestione dei dati.

2. In adempimento dell'obbligo di comunicazione interna ed esterna e di semplificazione dell'azione amministrativa, favorisce la trasmissione di dati e documenti tra le banche dati e gli archivi aziendali, degli enti territoriali, degli enti pubblici, dei gestori e degli incaricati di pubblico servizio, operanti nell'ambito dell'Unione Europea.

3. La trasmissione dei dati può avvenire anche attraverso l'utilizzo di sistemi informatici e telematici, reti civiche e reti di trasmissione di dati ad alta velocità;

4. Ai fini del presente regolamento, per finalità istituzionali della Società si intendono le funzioni ad essa attribuite dalle leggi, dallo statuto e dai regolamenti o per effetto di accordi e/o convenzioni.

5. I trattamenti sono compiuti dalla Società per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico.
b) l'adempimento di un obbligo legale al quale è soggetta la Società.
   La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
c) l'esecuzione di un contratto con soggetti interessati;
d) le specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 3 - Definizioni

Ai fini del presente regolamento si intende per:

*a) "**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;*

*b) "**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;*

*c) "**dati identificativi**": i dati personali che permettono l'identificazione diretta dell'interessato;*

*d) "**dati sensibili e giudiziari**": dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché* la trattazione di *dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*

*e) "**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;*

*f) "**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;

g) ***"sub-responsabile del trattamento":*** *l'incaricato dal Responsabile del trattamento, per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento (elabora o utilizza materialmente i dati personali).*

h) ***Responsabile per la protezione dati (RPD) o Data Protection Officer (DPO):*** *tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali hanno l'obbligo di nominare il DPO che dovrà svolgere i compiti di cui all'art. 39 del GDPR;*

i) ***"Data Protection Impact Assessment (DPIA) o Valutazione d'impatto sulla protezione dei dati":*** *è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.*

j) ***"Garante privacy":*** *il Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente.*

k) *"**incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;*

l) *"**interessato**", la persona fisica, cui si riferiscono i dati personali;*

m) *"**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;*

n) *"**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;*

o) *"**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;*

p) *"**banca di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;*

q) *"**violazione di dati personali**": violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico.*

r) "***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;*

s) "***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.*

t) ***"Registri delle attività di trattamento":*** *elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Responsabile del trattamento secondo le rispettive competenze.*

Ai fini delle proposte dei registri, si intende per:

- **Categorie di trattamento**
  Raccolta; registrazione; organizzazione; strutturazione; conservazione; adattamento o modifica; estrazione; consultazione; uso; comunicazione mediante trasmissione; diffusione o qualsiasi altra forma di messa a disposizione; raffronto od interconnessione; limitazione; cancellazione o distruzione; profilazione; pseudonimizzazione; ogni altra operazione applicata a dati personali.
- **Categorie di dati personali**
  Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi

caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale. Dati inerenti lo stile di vita. Situazione economica, finanziaria, patrimoniale, fiscale. Dati di connessione: indirizzo IP, login, altro. Dati di localizzazione: ubicazione, GPS, GSM, altro.

- **Finalità del trattamento**
  Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: funzioni amministrative inerenti la popolazione ed il territorio, nei settori organici dei servizi alla persona, alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico.
  Adempimento di un obbligo legale al quale è soggetta l'Azienda.
  Esecuzione di un contratto con i soggetti interessati.
  Altre specifiche e diverse finalità.
- **Misure tecniche ed organizzative**
  Pseudonimizzazione; minimizzazione; cifratura; misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi.
  Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro) - adottati per il trattamento di cui trattasi ovvero dalla Società nel suo complesso.
  Misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature; sistemi di copiatura e conservazione archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico - adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso.
  Procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
- **Categorie interessati**
  Cittadini residenti; minori di anni 14; contribuenti; utenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; altro.
- **Categorie destinatari**
  Persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.

Art. 4 – Soggetti

Art. 4.1 Titolare

1. **Salerno Energia Holding S.p.A**. , rappresentata, in ossequio al Regolamento UE 2016/679, dal ***L e g a l e R a p p r e s e n t a n t e*** pro tempore ai fini privacy, è il **Titolare** del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "***Titolare***").
2. Il ***Titolare*** è responsabile del rispetto dei principi contenuti nell'art. 5 del Regolamento UE 2016/679:
   - ✓ ***Liceità;***
   - ✓ ***correttezza e trasparenza;***
   - ✓ ***limitazione della finalità;***
   - ✓ ***minimizzazione dei dati;***
   - ✓ ***esattezza;***
   - ✓ ***limitazione della conservazione;***
   - ✓ ***integrità e riservatezza.***
3. Il Titolare adotta misure appropriate per fornire all'interessato:
   a) *le informazioni indicate dall'art. 13 del Regolamento UE 2016/679 (GDPR), qualora i dati personali siano raccolti presso lo stesso interessato;*
   b) *le informazioni indicate dall'art. 14 del Regolamento UE 2016/679 (GDPR), qualora i dati personali non stati ottenuti presso lo stesso interessato.*
4. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, del Reg. citato, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.
5. Il Titolare, inoltre, provvede a:
   a) ***Identificare i designati al trattamento*** *in funzione della articolazione dell'organizzazione aziendale. I designati al trattamento sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il titolare può avvalersi anche di soggetti pubblici o privati;*
   b) ***Designare gli incaricati:*** *gli incaricati devono seguire le istruzioni impartite dal Titolare nell'atto di designazione;*
   c) ***Designare un Referente Privacy*** *che coordini il Team privacy a supporto delle attività aziendali per la gestione del trattamento dei dati personali;*
   d) ***Nominare*** *il Responsabile della protezione dei dati (RPD o DPO);*
   e) ***Nominare*** *quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto della Società, relativamente alle banche dati gestite da soggetti esterni alla Società in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;*
   f) ***Nominare*** *un Amministratore di Sistema a cui spetta il compito di supportare il Titolare e/o i designati al trattamento nel mettere in atto le misure tecniche per garantire un livello di sicurezza adeguato al rischio (art. 32 del GDPR).*
6. I designati al trattamento, provvedono, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidati dal Titolare, analiticamente specificati per iscritto nell'atto di designazione ed in particolare a:
   a) *tenere il registro delle categorie di attività di trattamento svolte per conto del Titolare;*
   b) *adottare idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;*
   c) *assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati fornendo allo stesso ogni informazione di cui è in possesso;*
   d) *informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali c.d. "data breach", per la successiva notifica della violazione al Garante*

Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art. 4.2 Team Privacy

A supporto delle attività aziendali per la gestione del trattamento dei dati personali ai sensi del Regolamento UE 2016/679 e della normativa nazionale di riferimento, è costituito uno specifico gruppo di lavoro formato da:

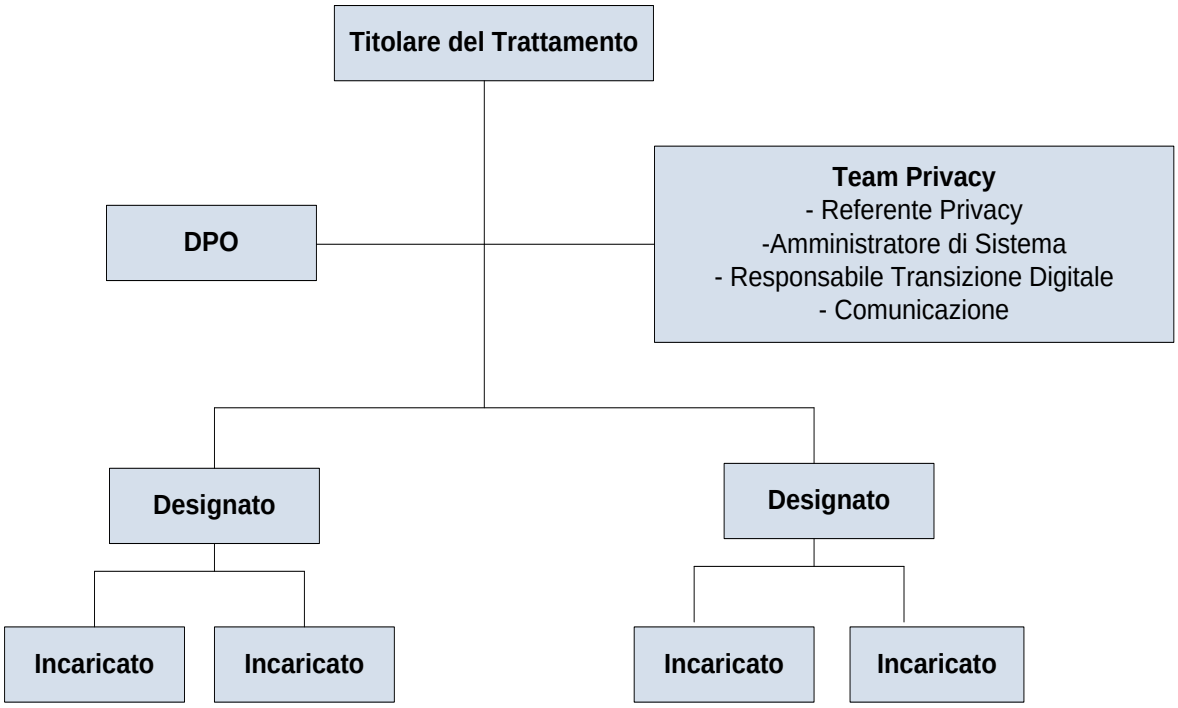
- ✓ *Referente Privacy;*
- ✓ *Responsabile Transizione Digitale;*
- ✓ *Amministratore di Sistema.*
- ✓ *Comunicazione*

Il gruppo di lavoro dovrà offrire ai vertici aziendali, confrontandosi anche con il Responsabile della protezione dei dati, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, curando l'adozione di un complesso di misure di sicurezza finalizzate alla tutela dei dati che soddisfino i requisiti di legge e assicurino sicurezza e riservatezza.
Il Team Privacy sarà coordinato dal Referente Privacy, figura professionale con competenze giuridiche, informatiche e gestionali, la cui responsabilità principale sarà, oltre al coordinamento del team, quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno della Società, affinché questi siano trattatati in modo lecito e pertinente, nel rispetto delle normative vigenti. A motivo dei compiti che deve svolgere, il Referente Privacy dovrà possedere un'adeguata conoscenza della normativa che regolamenta la gestione dei dati personali.

Art. 5 - Responsabile della protezione dei dati

1. Il Titolare, con suo provvedimento, nomina il Responsabile della protezione dei dati, in funzione delle sue qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di controllo a lui affidati.
2. Il Responsabile della protezione dei dati è un incaricato che potrà assolvere i suoi compiti in base a un contratto di servizio.
3. L'atto di nomina ed i dati di contatto del Responsabile della protezione dei dati sono pubblicati sul sito istituzionale della Società nella sezione *"Privacy"* e comunicati al Garante della protezione dei dati personali.
4. Il Responsabile della protezione dei dati deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e gli vanno fornite le risorse necessarie per assolvere tali compiti, accedere ai dati personali, ai trattamenti e per mantenere la propria conoscenza specialistica.
5. Riferisce e dipende direttamente dal Titolare.
6. Gli interessati possono contattare il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
7. Il Responsabile della protezione dei dati è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri deve svolgere almeno le seguenti funzioni:
   a) *sorvegliare l'osservanza del presente regolamento nonché della normativa nazionale e comunitaria da parte dei titolari del trattamento o dei designati al trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;*
   b) *fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;*
   c) *cooperare con l'Autorità garante per la protezione dei dati personali e fungere da punto di contatto per questioni connesse al trattamento dei dati personali;*
   d) *informare e fornire consulenza al Titolare ed ai designati al trattamento in merito agli obblighi derivanti dal presente regolamento nonché dalla normativa nazionale e comunitaria;*
8. I compiti attribuiti al DPO sono indicati in apposito contratto di servizi.

Figura 1 – Organigramma Privacy



Art. 6 - Adozione "Registro delle attività di trattamento e delle misure di sicurezza adottate per la corretta gestione delle banche dati aziendali e valutazione di impatto sulla protezione dei dati"

1. Al fine di coordinare le attività oggetto di trattamento, è adottato il "*Registro delle attività di trattamento e delle misure di sicurezza adottate per la corretta gestione delle banche dati aziendali e valutazione di impatto sulla protezione dei dati*".
2. Il Titolare, una volta compilato e aggiornato il Registro di cui al punto precedente, può provvede alla sua pubblicazione sul sito istituzionale nella sezione di "*Società Trasparente*".
3. La conformità del trattamento dei dati al Regolamento in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

Art. 7 - Trattamento dei dati personali

1. Le disposizioni del presente regolamento si intendono riferite al trattamento, alla diffusione e alla comunicazione dei dati all'esterno. L'accesso ai dati personali da parte delle strutture e dei dipendenti della Società, comunque limitato ai casi in cui sia finalizzato al perseguimento dei fini istituzionali, è ispirato al principio della circolazione delle informazioni, secondo il quale la Società provvede alla organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitare l'accesso e la fruizione, anche presso le strutture dipendenti.
2. Ogni richiesta di accesso ai dati personali da parte delle strutture e dei dipendenti, debitamente motivata, deve essere soddisfatta nella misura necessaria al perseguimento dell'interesse istituzionale.
3. Il Designato al Trattamento dei dati, specie se la comunicazione concerne dati sensibili, può tuttavia disporre, con adeguata motivazione, le misure ritenute necessarie alla tutela della riservatezza delle persone.

Art. 8 - Coordinamento con "Società Trasparente", procedimenti di accesso civico e generalizzato

Costituisce onere sia del ***Responsabile della protezione dei dati personali*** che del ***Responsabile per la prevenzione della corruzione e della trasparenza***, coordinare la loro attività al fine di semplificare e minimizzare l'impatto degli adempimenti sull'attività degli uffici e garantire la massima protezione dei dati

personali ogniqualvolta procedimenti di ufficio o attivati su istanza di soggetti esterni comportino attività di pubblicazione dei dati personali in "Società Trasparente", il rilascio di dati personali in occasione di istanze di accesso civico e generalizzato.
In tali ultime ipotesi dovranno essere adottate misure di sicurezza adeguate compresa la pseudonimizzazione, la minimizzazione e la cifratura dei dati personali.

Art. 9 - Procedimenti di accesso documentale

Costituisce onere sia dei singoli ***Responsabili*** sia del ***Responsabile della protezione dei dati personali***, coordinare la loro attività al fine di semplificare e minimizzare l'impatto degli adempimenti sull'attività degli uffici e garantire la massima protezione dei dati personali ogniqualvolta procedimenti di ufficio o attivati su istanza di soggetti esterni comportino attività di accesso agli atti amministrativi ai sensi della Legge n. 241/90 e ss.mm.ii.

Art. 10 - Formazione del personale

1. Costituisce onere sia del ***Responsabile della protezione dei dati personali*** che del ***Responsabile per la prevenzione della corruzione e della trasparenza***, coordinare la loro attività al fine di attuare misure di formazione del personale, anche con riscontro dell'acquisizione di abilità e competenze, al fine di garantire, nell'attività degli uffici, il rispetto delle norme in materia di trasparenza e l'assolvimento degli adempimenti atti a tutelare i diritti di riservatezza dei dati personali dei cittadini e dipendenti.

Art. 11 - Trattamenti consentiti

1. La Società, di norma, non è tenuta a chiedere il consenso al trattamento dei dati da parte degli interessati.
2. La pubblicazione e la divulgazione di atti e documenti che determinano una "diffusione" dei dati personali, comportando la conoscenza dei dati da parte di un numero indeterminato di persone, è legittima solo se la diffusione è prevista da una norma di legge o di regolamento.
3. Prima della pubblicazione di dati personali deve essere valutato se le finalità di trasparenza e di comunicazione possono essere perseguite senza divulgare dati personali.
4. Se risulta possibile occorre citare i dati personali solo negli atti a disposizione degli uffici, richiamati quale presupposto della compilazione di atti interni e consultabili solo da interessati e controinteressati oppure utilizzare espressioni di carattere generale, soprattutto nel caso in cui si debbano valutare circostanze e requisiti personali che attengono a situazioni di particolare disagio.
5. Deve essere valutato anche la possibilità di rendere pubblici atti e documenti senza indicare i dati che portino all'identificazione degli interessati.
6. Per attività di comunicazione istituzionale che contemplino l'utilizzo di dati personali, andrà posta particolare attenzione alla necessità di fornire un'adeguata informativa relativa al trattamento e soprattutto andrà valutato se risulti necessaria l'acquisizione, anche successiva, del consenso al trattamento.

Art. 12 - Principi

1. Negli atti destinati alla pubblicazione o divulgazione i dati che permettono di identificare gli interessati sono riportati solo quando è necessario ed è previsto da una norma di legge, rispettando il principio di proporzionalità, mediante la verifica che tale pubblicazione a fini di trasparenza concerne solo dati pertinenti e non eccedenti rispetto alle finalità perseguite.
2. I sistemi informativi ed i programmi informatici devono essere configurati per ridurre al minimo l'utilizzazione di dati personali e devono prevedere la possibilità di estratti degli atti con l'esclusione dei dati personali in essi contenuti.

Art. 13 - Attività amministrativa

1. L'attività amministrativa si svolge, principalmente, con l'emissione, la elaborazione, la riproduzione e la trasmissione di dati, compresi i procedimenti per la emanazione di provvedimenti, mediante sistemi informatici o telematici.
2. Per l'attività informatica di cui al comma precedente sono rigorosamente rispettate le norme di cui al codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, e successive

modificazioni.

3. La sicurezza dei dati personali è assicurata anche mediante adeguate soluzioni tecniche connesse all'utilizzo della firma digitale, chiavi biometriche o altre soluzioni tecniche.

Art. 14 - Fascicolo personale dipendenti e amministratori

1. I dati sullo stato di salute dei dipendenti e degli amministratori devono essere conservati separatamente rispetto alle altre informazioni personali. Il fascicolo, che raccoglie tutti gli atti relativi alla loro nomina, al percorso professionale e ai fatti più significativi che li riguardano, possono mantenere la loro unitarietà, adottando accorgimenti che impediscano un accesso indiscriminato, quali l'utilizzo di sezioni o fascicoli dedicati alla custodia di eventuali dati sensibili, da conservare chiusi o comunque con modalità che riducano la possibilità di una indistinta consultazione nel corso delle ordinarie attività amministrative.

Art. 15 - Sicurezza dei dati – Misure di sicurezza – Verifiche e controlli e relativi Regolamenti

1. **<u>Tutta l'attività di gestione è finalizzata a:</u>**
   a) ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati memorizzati;
   b) evitare l'accesso, non autorizzato, alle banche dati, alla rete e, in generale, ai servizi informatici aziendali;
   c) prevenire:
   - ✓ trattamenti dei dati non conformi alla legge o ai regolamenti;
   - ✓ la cessione o la distribuzione dei dati in caso di cessazione del trattamento.

2. I designati al trattamento dei dati garantiscono, anche in relazione alle conoscenze acquisite in base al progresso tecnologico, l'adozione e lo sviluppo di misure di sicurezza adeguate come:
   - ✓ *la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*

3. Nella gestione dei dati personali con il sistema informatizzato dovrà essere assicurato il puntuale e scrupoloso rispetto di tutte le norme vigenti.
4. Gli stessi Designati al Trattamento dei dati si attiveranno periodicamente con controlli, anche a campione, al fine di garantire la sicurezza delle banche dati e la esattezza e completezza dei dati inseriti.
5. Costituiscono misure tecniche ed organizzative che possono essere adottate:
   - ✓ *sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);*
   - ✓ *misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.*

6. Ogni ulteriore misura idonea a tutela delle banche dati personali informatiche o cartacee andrà adottata secondo un principio di proporzionalità tra le risorse disponibili e i diritti da tutelare.
7. In merito sono stati redatti specifici Regolamenti: "Regolamento per l'utilizzo dei sistemi e degli strumenti informatici", "Regolamento aziendale per il servizio di posta elettronica certificata e istituzionale" e "Regolamento Videosorveglianza".

Art. 16 - Trattamento e accesso ai dati sensibili e giudiziari

1. Per l'accesso ai dati sensibili e giudiziari, con determinazione del Titolare, sono rilasciate autorizzazioni singole o a gruppi di lavoro per il trattamento dei dati e la manutenzione.
2. L'autorizzazione è limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni assegnate all'incaricato.
3. In attuazione del Regolamento UE 2016/679 nel ***Registro dei Trattamenti*** sono identificati i tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità perseguite.

4. I dati sensibili e giudiziari individuati dal presente regolamento sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie nel caso in cui la raccolta non avvenga presso l'interessato.
5. I dati sensibili o giudiziari non indispensabili, dei quali la Società, nell'espletamento della propria attività istituzionale, venga a conoscenza, ad opera dell'interessato, comunque, non a richiesta della stessa, non sono utilizzati in alcun modo, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Art. 17 - Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:
   a) il nome ed i dati di contatto della Società, del Titolare, del Legale Rappresentante, del DPO;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.
2. Il Registro è tenuto dal Titolare presso gli uffici della struttura organizzativa della Società in forma digitale/cartacea, secondo quanto previsto dal Regolamento UE; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative della Società.

Art. 18 - Diritti dell'interessato e relativo Regolamento

1. I soggetti, i cui dati sono contenuti in una banca dati della Società, hanno il diritto di ottenere, senza indugio:
   a) la conferma dell'esistenza o meno di trattamenti di dati che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità del trattamento;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
   c) l'aggiornamento, la rettificazione, ovvero, qualora vi abbia interesse, l'integrazione dei dati;
   d) l'attestazione che le operazioni di cui ai successivi commi 2 e 3 sono state portate a conoscenza dei terzi;
2. L'interessato ha, inoltre, il diritto di opporsi, per motivi legittimi, al trattamento dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta.
3. L'interessato può esercitare tali diritti con una richiesta al DPO.
4. L'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.
5. In merito è stato redatto specifico "Regolamento per l'Esercizio dei Diritti degli Interessati in materia di protezione dei dati personali.

Art. 19 - Valutazione d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (**DPIA**) ai sensi dell'art. 35 del Regolamento UE, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'at. 35 del Regolamento UE.
3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, del Regolamento UE, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a. *trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;*
b. *decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;*
c. *monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;*
d. *trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, Regolamento UE;*
e. *trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico* dell'attività di *trattamento;*
f. *combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;*
g. *dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;*
h. *utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;*
i. *tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.*

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno alla Società. Il Titolare deve consultarsi con il DPO anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il DPO monitora lo svolgimento della DPIA. Il designato al trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. L'Amministratore di Sistema fornisce supporto al Titolare per lo svolgimento della DPIA.
5. Il DPO può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.
6. L'Amministratore di Sistema può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.
7. La DPIA non è necessaria nei casi seguenti:
   - ✓ *se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, Regolamento UE;*
   - ✓ *se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;*
   - ✓ *se il trattamento è stato sottoposto a verifica da parte del Garante Privacy in condizioni specifiche che non hanno subito modifiche;*
   - ✓ *se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.*

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un DPO e che proseguano con le stesse modalità oggetto di tale verifica.

8. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
   a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati.
      Sono altresì indicati:
      i. i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
   b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
      - ✓ *delle finalità specifiche, esplicite e legittime;*
      - ✓ *della liceità del trattamento;*
      - ✓ *dei dati adeguati, pertinenti e limitati a quanto necessario;*
      - ✓ *del periodo limitato di conservazione;*
      - ✓ *delle informazioni fornite agli interessati;*
      - ✓ *del diritto di accesso e portabilità dei dati;*
      - ✓ *del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;*
      - ✓ *dei rapporti con i responsabili del trattamento*
      - ✓ *delle garanzie per i trasferimenti internazionali di dati;*
      - ✓ *consultazione preventiva del Garante privacy;*
   c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
   d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il Regolamento UE, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
9. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
10. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

Art. 20 - Violazione dei dati personali e relativo Regolamento

1. Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Azienda.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire al più entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:
   - ✓*danni fisici, materiali o immateriali alle persone fisiche;*
   - ✓*perdita del controllo dei dati personali;*
   - ✓*limitazione dei diritti, discriminazione;*
   - ✓*furto o usurpazione d'identità;*
   - ✓*perdite finanziarie, danno economico o sociale.*
   - ✓*decifratura non autorizzata della pseudonimizzazione;*
   - ✓*pregiudizio alla reputazione;*

- ✓ *perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).*

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
   - ✓ *coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;*
   - ✓ *riguardare categorie particolari di dati personali;*
   - ✓ *comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);*
   - ✓ *comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);*
   - ✓ *impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).*
5. La notifica deve avere il contenuto minimo previsto dall'art. 33 del Regolamento, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.
7. Il Titolare o il Responsabile deve informare tempestivamente il responsabile della protezione dei dati dell'esistenza di una violazione e coinvolgerlo nella gestione delle violazioni e nel processo di notifica.
8. In merito è stato redatto specifico "Regolamento Data Breach - Disposizioni operative in materia di incidenti di sicurezza e di violazione dei dati personali (Data Breach)".

Art. 21 - Entrata in vigore e normativa applicabile

1. Il presente regolamento entra in vigore il primo giorno del mese successivo a quello di esecutività della delibera di approvazione.
2. Per quanto non previsto nel presente regolamento trovano applicazione:
   a) le direttive ed i regolamenti comunitari, le leggi nazionali e regionali;
   b) lo statuto aziendale;
   c) il Modello di Organizzazione e Gestione ai sensi del D.Lgs. 231/01 (MOG).

Art. 22 - Rinvio dinamico

1. Le norme del presente regolamento si intendono modificate per effetto di sopravvenute norme vincolanti comunitarie per la parte direttamente applicabile, statali e regionali.
2. In tali casi, in attesa della formale modificazione del presente regolamento, si applica la normativa sopraordinata.

Art. 23 - Norme abrogate

1. Con l'entrata in vigore del presente regolamento sono abrogate tutte le norme regolamentari con esso contrastanti.

Art. 24 - Pubblicità del regolamento

1. Copia del presente regolamento può essere pubblicato nell'apposita sezione di *Società Trasparent*e del sito internet istituzionale.