OPI
PESARO
URBINO

Ordine delle Professioni Infermieristiche di Pesaro Urbino

REGOLAMENTO PER L'ATTUAZIONE DELLA NORMATIVA EUROPEA E NAZIONALE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI DELLE PERSONE FISICHE-OPI PESARO URBINO

Approvato con Delibera del Consiglio Direttivo n. 136/2022 del 12.05.2022

INDICE

Art. 1 - Oggetto del Regolamento

1. Il presente Regolamento ha per oggetto l'individuazione dei soggetti coinvolti a vario titolo nelle attività di trattamento, le loro precipue funzioni e le regole comportamentali e le misure fisiche, tecniche ed organizzative, atte all'ottenimento di una corretta attuazione del Regolamento Europeo 2016/679 (di seguito indicato solo con: Reg. UE 679), nonché del Codice per la tutela dei dati personali (D.lgs. 196/2003 e successive modificazioni ed integrazioni), con riguardo ai trattamenti dei dati personali delle persone fisiche attuati dall'Ordine delle Professioni Infermieristiche di Pesaro-Urbino (OPI) al fine di garantire i diritti e le libertà degli interessati (persone fisiche).

Art. 2 - Finalità e base giuridica dei trattamenti

1. Il trattamento è effettuato dall'Ordine per le seguenti finalità:
   - l'esercizio delle funzioni amministrative proprie;
   - l'erogazione dei servizi connessi all'esercizio delle funzioni amministrative o su domanda degli interessati;

2. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina, che ne costituisce la base giuridica, ed in particolare ai sensi dell'art. 6, comma 1, del REG. UE 679, alle lettere:
b) l'esecuzione di un contratto con i soggetti interessati;
c) l'adempimento di un obbligo legale al quale è soggetto l'Ordine;
e) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
f) l'interesse legittimo del titolare (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati biometrici, dati relativi alla salute o alla vita sessuale).
3. Il trattamento dei dati particolari di cui all'art. 9, comma 1, del Reg. UE 679, necessario per le specifiche finalità di cui ai precedenti punti, è lecito purché all'interessato sia stata fornita una puntuale informativa su tale categoria di dati, o si verta nelle casistiche di cui al comma 2, alle lettere b) e g).

Art. 3 – Informativa

1. Ogniqualvolta l'Ordine provvede alla raccolta dei dati personali, deve informare l'interessato in forma concisa, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro. L'informativa deve contenere:
   - il nominativo ed i dati di contatto del Titolare;
   - il nominativo ed i dati di contatto del Responsabile della Protezione dei dati;
   - le finalità e le modalità del trattamento cui sono destinati i dati richiesti;
   - la base giuridica del trattamento;
   - le categoria di dati personali trattati;
   - i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili;

- l’eventuale trasferimento dei dati in paesi terzi extra UE;
- il periodo di conservazione dei dati;
- l’esistenza di un eventuale processo decisionale automatizzato;
- i diritti dell’interessato di cui agli artt. 15-22 del Reg. UE 679, nonché di proporre reclamo all’Autorità di controllo.

2. L'informativa deve essere resa, di norma, per iscritto; può essere resa oralmente, o anche mediante affissione negli Uffici in cui gli interessati si recano per conferire i dati o con appositi moduli pubblicati sulle pagine *web* del sito istituzionale.
3. Se i dati personali non sono raccolti presso l’interessato, l’informativa è data al medesimo all’atto della registrazione dei dati o non oltre la prima comunicazione, eccetto nei seguenti casi: a) quando i dati sono trattati in base ad un obbligo previsto dalla legge o da un regolamento; b) quando i dati sono trattati per far valere o difendere un diritto dell’Ente in sede giudiziaria, sempre che siano trattati solo per tale finalità e per il periodo necessario al loro perseguimento; c) quando la comunicazione dell’informativa all’interessato comporti un impiego di mezzi sproporzionato rispetto al diritto tutelato.

Art. 4 - Titolare del trattamento

1. Il Titolare del trattamento dei dati personali è l’Ordine delle Professioni Infermieristiche di Pesaro-Urbino (OPI). L’ente è rappresentato ai fini previsti dal Reg. UE 679 dal Presidente pro-tempore.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall’art. 5, del Reg. UE 679: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza;
3. Il Titolare mette in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al Reg. UE 679;
4. Le suddette misure sono definite fin dalla fase di progettazione e sono messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l’esercizio dei diritti dell’interessato, stabiliti dal Capo III, Sezione I (articoli da 15 a 22), del Reg. UE 679, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio;
5. Gli interventi necessari per l’attuazione delle medesime misure sono considerati nell’ambito della programmazione operativa e le risorse necessarie sono allocate nel bilancio di previsione previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
6. Il Titolare adotta misure appropriate per fornire all’interessato:
a) le informazioni indicate dall’art. 13, del Reg. UE 679, qualora i dati personali siano raccolti presso lo stesso interessato;
b) le informazioni indicate dall’art. 14, del Reg. UE 679, qualora i dati personali non stati ottenuti presso lo stesso interessato;
7. 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 (nell’accezione inglese *Data Protection Impact Assessment*, di seguito indicata anche con “DPIA”) ai sensi dell’art. 35, del Reg. UE 679, considerati la natura, l’oggetto, il contesto

e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo articolo 18;
8. Il Titolare, inoltre, provvede:
a) ad individuare i Responsabili del trattamento nelle persone dei soggetti pubblici o privati eventualmente affidatari o concessionari di attività e servizi per conto dell'Ordine, relativamente alle banche dati gestite da soggetti esterni 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;
b) nominare il Responsabile della Protezione dei Dati (di seguito indicato anche con RPD) di cui al successivo art. 5;
c) nominare quali "Designati al trattamento" i soggetti che materialmente effettuano le operazioni di trattamento.
d) provvede alla formazione periodica di tutti i designati al compimento delle attività di trattamento dei dati personali;
9. I soggetti designati che richiedono i dati e li ricevono, o che eseguono un qualsiasi trattamento sono comunque vincolati al rispetto del dovere di riservatezza e sono tenuti ad eseguire tutte le misure di sicurezza per la protezione dei dati a loro trasmessi;
10. L'Ordine impronta le attività di trattamento secondo le regole deontologiche approvate dal Garante, per contribuire alla corretta applicazione del Reg. UE 679 e per dimostrarne il concreto rispetto da parte del Titolare. Il rispetto delle disposizioni contenute nelle regole deontologiche costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali.

Art. 5 - Responsabile esterno del trattamento

1. Il Titolare del trattamento può avvalersi, per il trattamento di dati, anche particolari, di soggetti pubblici o privati che, in qualità di responsabili esterni del trattamento, forniscano le garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure fisiche, tecniche e organizzative di cui all'art. 17, comma 3, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
2. I soggetti di cui al precedente comma 1, sono tenuti a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare;
3. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, del Reg. UE 679; tali atti possono anche basarsi su clausole contrattuali.
4. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
5. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, specificati per iscritto nell'atto di designazione o nel contratto ed in particolare provvede:

- alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
- all'adozione di idonee misure fisiche, tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;

- alla designazione del Responsabile per la Protezione dei Dati (RPD), se previsto;
- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati, fornendo allo stesso ogni informazione di cui è in possesso;
- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*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. 6 - Responsabile della Protezione dei Dati (RPD)

1. Il Responsabile della Protezione dei Dati (in seguito indicato solo con "RPD"), è designato dal Titolare. Il soggetto designato può essere un dipendente dell'Ordine individuato in funzione delle 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 cui all'art. 39 del Reg. UE 679, o un soggetto esterno all'Ente, in possesso delle qualità di cui sopra. I compiti attribuiti al RPD esterno sono indicati in apposito contratto di servizi.
2. Il RPD è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Titolare del trattamento;
3. Il RPD è incaricato dei seguenti compiti:
a) informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti designati al trattamento in merito agli obblighi derivanti dal Reg. UE 679 e dalle altre normative relative alla protezione dei dati.
b) sorvegliare l'osservanza del Reg. UE 679 e delle altre normative relative alla protezione dei dati, ferma restando le responsabilità del Titolare del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare del trattamento;
c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare del trattamento;
d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) di cui al successivo art. 12.
e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, del Reg. UE 679, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare del trattamento al Garante;
f) la revisione, in funzione della valutazione dell'impatto del registro di cui al successivo art. 10;
g) rispondere agli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal Reg. UE 679 e dal presente regolamento;
h) altri compiti e funzioni a condizione che il Titolare si assicuri che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.
4. Il Titolare del trattamento assicura che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti le decisioni

che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;

- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

5. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:
a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare del trattamento.
6. La figura del RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;

- il Responsabile esterno del trattamento;

- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

7. Il Titolare del trattamento fornisce al RPD le risorse necessarie per assolvere i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente. In particolare, è assicurato al RPD:

– supporto attivo per lo svolgimento dei suoi compiti da parte dei soggetti interni che operano nel campo della tutela dei dati personali;

– tempo sufficiente per l'espletamento dei compiti affidati al RPD;

– accesso garantito agli uffici dell'Ordine così da fornirgli supporto, informazioni e input essenziali;

8. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento, né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati;
9. Il RPD non può essere rimosso o penalizzato dal Titolare del trattamento per l'adempimento dei propri compiti;
10. Fermo restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare del trattamento;
11. Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il Reg. UE 679 e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare del trattamento.

Art. 7 - Amministrazione del Sistema informatico

1. Per il conseguimento degli obiettivi di sicurezza informatica previsti dal Codice Amministrazione Digitale (da ora solo CAD), di cui al successivo art. 17, comma 1, il Titolare, oltre al Responsabile per la transizione al digitale di cui all'art. 17, comma 1 *sexies* del C.A.D., si avvale di un dipendente dotato delle specifiche competenze informatiche, quale Designato per l'amministrazione del sistema informatico, con la precipua funzione di collaborare alla gestione e manutenzione dei sistemi informatici, con particolare riferimento alle misure tecniche predisposte dal Titolare atte a garantire un livello di sicurezza adeguato al rischio connesso ai trattamenti dei dati personali effettuati dall'Ente.
2. Il Designato, in particolare:
a) gestisce gli accessi condizionati al sistema informatico, attribuendo le credenziali ai soggetti autorizzati;
b) collabora con il Titolare per la predisposizione delle Istruzioni operative atte a garantire la sicurezza informatica;
c) propone al Titolare l'adeguamento periodico delle misure tecniche in relazione all'evoluzione tecnologica dei sistemi di ICT ed al rischio connesso al trattamento dei dati personali;
d) collabora con il Titolare e con i Designati al trattamento per verificare la corretta implementazione delle misure tecniche atte a garantire la sicurezza dei trattamenti dei dati personali;
e) assiste – se richiesto - il Titolare nell'esecuzione del DPIA.
3. Qualora l'Ente non sia dotato di personale con le specifiche competenze informatiche, o a cui non possa assegnare le attività elencate, potrà ricorrere o al personale di altro Ente pubblico, a mezzo apposita convenzione, o a personale esterno individuato nel rispetto della normativa sull'affidamento dei servizi.

Art. 8 - Designato al trattamento

1. Il Titolare del Trattamento può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connesse al trattamento dei dati personali siano attribuiti a persone fisiche espressamente designate che operano sotto la sua autorità.
2. Il Designato è tenuto a mettere in atto le adeguate misure fisiche, tecniche e organizzative di cui al successivo art. 17, comma 3, volte a garantire che i trattamenti siano effettuati in conformità al Reg. UE 679.

Art. 9 - Incaricati del trattamento

1. Il soggetto Designato al trattamento di cui al precedente articolo provvede, se del caso, a ono a nominare gli Incaricati del trattamento, da individuare, con apposito atto, tra le singole figure soggettive dei collaboratori e dipendenti cui affidare delle attività di trattamento dei dati personali nei procedimenti di rispettiva competenza, per le stesse finalità di cui all'art. 2-*quaterdecies*, comma 1, del d.lgs. 196/2003;
2. I soggetti Incaricati devono assicurare la legittimità delle attività di trattamento dei dati personali ponendo in essere le adeguate misure fisiche, tecniche e organizzative di sicurezza, nonché le istruzioni operative emanate dal Titolare.

Art.10 - Registro delle attività di trattamento

1. Il Titolare tiene un registro delle attività di trattamento ai sensi dell'art. 30, del Reg. UE 679.
2. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le

seguenti informazioni:
a) i dati di contatto del Titolare del trattamento e del soggetto Designato ai sensi del precedente art. 8, comma 1, nonché del RPD;
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 fisiche, tecniche ed organizzative del trattamento adottate come da successivo art. 17.
3. Il registro è tenuto dal Titolare presso gli uffici della struttura organizzativa dell'Ordine in formato digitale/cartaceo; nello stesso registro possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.
4. Il Titolare del trattamento, sotto la propria responsabilità, può delegare ad un soggetto Designato al trattamento di cui al precedente art. 8 il compito di tenere il Registro.
5. Il Titolare del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto alla tenuta del registro ogni elemento necessario alla regolare tenuta ed aggiornamento del registro stesso.

Art. 11 - Misure di sicurezza

1. Il Titolare e ciascun Designato al trattamento, adottano le opportune misure fisiche, tecniche ed organizzative atte a garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
2. Le misure fisiche, tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: 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. Costituiscono misure fisiche, tecniche ed organizzative:
   - 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 per garantire la continuità operativa;
   - istruzioni operative per i Designati al trattamento.

4. L'ordine si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per suo conto ed abbia accesso a dati personali;

5. I dati di contatto del Titolare, del Designato al trattamento e del RPD sono pubblicati sul sito internet istituzionale dell'Ente, sezione *Amministrazione trasparente> Altri contenuti,* oltre che nella apposita sezione "*privacy*".

Art. 12 - Valutazioni d'impatto sulla protezione dei dati (DPIA)

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 Reg. UE 679, 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'art. 35, punti n. 4-6, del Reg. UE 679.
3. L'Amministratore dei sistemi informativi fornisce supporto al Titolare per lo svolgimento della DPIA.
4. Il RPD 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.

Art. 13 - Violazione dei dati personali

1. Il Titolare in presenza di una violazione di dati personali (*Data breach)* ove ritenga probabile che dalla stessa possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy.
La notifica dovrà avvenire 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.
2. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al Considerando 75, del Reg. UE 679, per quel che riguarda il presente Ente sono i seguenti:

- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari, ecc.).

3. 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;

La notifica deve avere il contenuto minimo previsto dall'art. 33 del Reg. UE 679, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

4. 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 Reg. UE 679.

Art. 14 – Diritti dell'interessato

1. L'interessato ha diritto:
a) ai sensi degli articoli 13 e 14 del Reg. UE 679 di ricevere dal Titolare le informazioni, relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro;
b) ai sensi degli articoli da 15 a 22 del Reg. UE 679, di accedere, di chiedere la rettifica o la cancellazione in tutto o in parte, ai propri dati personali, nonché la loro portabilità in formato accessibile ed in autonomi supporti analogici o informatici qualora gli stessi non siano più necessari per la formazione, validità e/o efficacia del documento amministrativo informatico/analogico per il quale sono stati forniti; di essere informato sull'eventuale processo decisionale automatizzato, e di potervisi opporre;
c) ai sensi dell'art. 34 del Reg. UE 679 di ricevere dal Titolare la comunicazione della violazione dei dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
2. L'interessato può esercitare i propri diritti inviando una richiesta alla casella di PEC dell'Ordine. Nell'oggetto l'interessato dovrà specificare il diritto che si intende esercitare, per quale finalità sa o suppone che i suoi dati siano stati raccolti dal Comune e dovrà allegare, se la richiesta non proviene da una casella pec intestata all'interessato, la richiesta sottoscritta ed un proprio documento di identità;
3. L'interessato può contattare il RPD per segnalare le problematiche connesse all'esercizio dei propri diritti. Il RPD ricevuta la segnalazione dall' interessato circa la violazione dei propri diritti provvede sollecitamente a contattare il Titolare e/o il soggetto Designato al trattamento per assumere tutte le necessarie informazioni atte a verificare la fondatezza della segnalazione. In caso affermativo suggerisce al Titolare e/o al Designato al trattamento la soluzione alla problematica segnalata, dandone comunicazione all'interessato entro il termine di 30 giorni dal ricevimento della segnalazione;
4. L'interessato ha diritto, ai sensi all'articolo 77, del Reg. UE 679, di proporre reclamo a un'autorità di controllo, in caso ritenga illecito il trattamento dei propri dati personali per violazione delle norme previste dal Reg. UE 679 e dal Codice *Privacy*.

Art. 15 - Accesso ai documenti amministrativi e accesso civico

1. Fatto salvo quanto previsto dall'articolo 60 del Codice *privacy* (D.L.vo 30.06.2003 n. 196 aggiornato dal D.L.vo 10.08.2018 n. 101), i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241 e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i dati di cui agli articoli 9 e 10 del Reg. UE 679 e le operazioni di

trattamento eseguibili in esecuzione di una richiesta di accesso;

2. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dagli articolo 5 e 5-*bis*, del d.lgs. 33/2013.

Art. 16 Norme applicabili e conservazione degli effetti degli atti amministrativi

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni regolamentari, si applicano le vigenti disposizioni del Reg. UE 679 ed il d.lgs. 196/2003, nonché tutte le altre disposizioni speciali per gli enti pubblici;
2. Sono fatti salvi gli effetti giuridici di tutti gli atti amministrativi adottati dall'Ente secondo la normativa *privacy* previgente, purché rispettino sostanzialmente i principi e le finalità delle vigenti norme in materia di tutela dei dati personali e del presente regolamento.

GLOSSARIO

Ai fini del presente Regolamento si intende per:

Titolare del trattamento: l'autorità pubblica (l'Ordine professionale) che determina finalità e modalità del trattamento di dati personali;
Designato al trattamento: Il soggetto nominato da parte del Titolare del trattamento, ex art. 2 *quaterdecies* comma 1, Codice Privacy novellato;
Incaricato del trattamento: il soggetto nominato dal Designato al trattamento, quale collaboratore del proprio Settore che compie attività di trattamento dati personali;
Responsabile del trattamento: il soggetto pubblico/privato che per conto del Titolare ex art. 28 del Reg. UE 679 esegue il trattamento dei dati, la cui nomina spetta al Titolare con conseguente definizione puntuale degli obblighi dello stesso all'interno di apposito contratto/atto giuridico secondo quanto previsto dallo stesso art. 28 del Reg. UE 679.
Responsabile della Protezione Dati (RPD o DPO - Data Protection Officer nella accezione inglese): la figura professionale con funzioni di assistenza del Titolare nominato ai sensi dell'art. 37 Reg. UE 679 (cfr. considerando 97 del regolamento).
Registri delle attività o categorie di trattamento: elenchi dei trattamenti in forma cartacea o telematica;
DPIA - Data Protection Impact Assessment – Valutazione d'impatto sulla protezione dei dati: 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;
Garante Privacy: l'Autorità Garante per la protezione dei dati personali istituito dalla Legge 31/12/1996, n. 675, quale autorità amministrativa pubblica di controllo indipendente. L'organizzazione dell'ufficio del Garante per la *privacy* e le competenze sono individuate nel Codice Privacy (d.lgs. 196/2003).
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 interessati: cittadini residenti e non; minori di anni 16; elettori; contribuenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; soggetti portatori di interessi nei procedimenti amministrativi; destinatari di atti e provvedimenti; utenti di servizi generali o di prestazioni a domanda individuale;
Categorie di destinatari: persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.
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: adempimento di un obbligo legale al quale è soggetto l'Ordine; esecuzione di un contratto con i soggetti interessati; altre specifiche e diverse finalità;
Misure fisiche, 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; 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;
Dati particolari (sensibili): i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Violazione di dati personali (*Data breach*): si intende qualsiasi violazione di sicurezza dei dati personali 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.