Approvato con Delibera n. 19 del 25/05/2018

REGOLAMENTO PER LA PROTEZIONE DEI DATI PERSONALI
REGOLAMENTO U.E. 679/2016

INDICE

GLOSSARIO

RGPD = Regolamento Generale sulla Protezione dei Dati Personali , Regolamento UE n. 679/2016

RPD = Responsabile della Protezione dei dati (in inglese DPO Data Protection Officer)

Data breach = "riuscire a fare breccia", qualunque violazione dei dati personali

DPIA = Valutazione di impatto sulla protezione dei dati

Privacy by design = Privacy dal momento della sua progettazione. Implica che qualsiasi progetto va realizzato assumendo dalla fase iniziale di ideazione misure di protezione di dati personali

Privacy by default = protezione dei dati per impostazione predefinita, ovvero, misure tecniche ed organizzative che assicurano solo i dati personali necessari per ogni specifica finalità di trattamento

Audit Privacy è una valutazione dei processi interni adottati sul grado di rispetto della normativa vigente del Reg. UE n. 679/2016

GEPD = Garante Europeo della protezione dei dati

Accountability = letteralmente "rendere conto", ovvero, il Titolare del trattamento si deve responsabilizzare autonoma-
mente nella gestione ed organizzazione della Privacy. Il principio nasce nella legislazione europea e statunitense ed è inteso come la responsabilità dell'amministrazione ha verso chi l'ha scelta e s fonda su: trasparenza intesa come informazioni dell'attività di governo; parteciazione di chiunque al miglioramento delle politiche ubbliche e collaborazione intesa come efficacia dell'azione amministrativa attraverso la cooperazione tra tutti i livelli di governo

WP 29 = Warking Party Art. 29 (c.d. Gruppo di lavoro art. 29) Organismo consultivo ed indipendente composto da un rappresentante dei Garanti dei dati personali di ogni stato membro, da un rappresentante della Commissione UE e dal Garante europeo della protezione dei dati

TITOLO I
PRINCIPI
Art. 1
Finalità

1. Il presente regolamento disciplina le misure organizzative ed i processi interni di attuazione del Regolamento UE n. 679/2016 (R.G.P.D.) ai fini del trattamento di dati personali per finalità istituzionali nello Istituto Autonomo Case Popolari Di Catania.

2. Ai fini del presente regolamento, per funzioni istituzionali si intendono quelle:

a) previste dalla legge, dallo statuto comunale e dai regolamenti;
b) esercitate in attuazione di convenzioni, accordi/intese nonché sulla base degli strumenti di programmazione e pianificazione previsti dalla legislazione vigente;
c) svolte per l'esercizio dell'autonomia organizzativa, amministrativa e finanziaria dell'ente locale;
d) in esecuzione di un contratto con i soggetti interessati;
e) per finalità specifiche e diverse dai punti precedenti purché l'interessato esprima il consenso al trattamento.

3. Il presente regolamento è conforme alle norme e principi costituzionali nonché alle altre disposizioni vigenti sulla materia, incluse le norme non incompatibili del Codice della Privacy, D.Lgs. n. 196/2003.

Art. 2
Principi del trattamento

1. Per le finalità indicate all'art. 1, l'Ente effettua il trattamento dei dati personali nel rispetto dei diritti e libertà fondamentali delle persone fisiche nonché del diritto alla riservatezza ed all'identità di persone fisiche e giuridiche.

2. In attuazione del comma 1, i dati personali sono:

– trattati in conformità delle norme di legge, cioè in modo lecito e con trasparenza nei confronti dell'interessato;
– corretti, esatti ed aggiornati a seguito di intervenute variazioni;
– solo quelli necessari e pertinenti allo scopo specifico, con la riduzione al minimo delle informazioni identificative; il trattamento va evitato laddove lo scopo specifico può essere raggiunto tramite dati anonimi;
– trattati con adeguate misure di sicurezza in modo da evitare abusi o illeciti o perdita, distruzione o danno accidentale, in conformità del principio di integrità e riservatezza.
- trattati al fine di porli a esclusiva disposizione del soggetto a cui si riferiscono e nel cui interessi ed entro i termini previsti dal presente regolamento, possano essere suscettibili di modifica, integrazione e/ o cancellazione.

3. Relativamente al trattamento di dati personali di persone decedute, il diritto alla riservatezza si estingue con la morte del titolare. I diritti di cui al Titolo V del presente regolamento , in tali casi, possono essere esercitati da chi agisce per la tutela del defunto o per motivi familiari meritevoli di tutela.

Art. 3
Definizioni

Ai fini del presente regolamento si adottano le seguenti definizioni:

– Dati personali: qualunque informazione riguardante una persona fisica identificata o identificabile;
– Trattamento: qualsiasi operazione compiuta con o senza processi automatizzati che prevede la raccolta, la registrazione, l'organizzazione, la strutturazione, conservazione, adattamento o modifica, l'estrazione, consultazione, utilizzo, trasmissione diffusione o altra forma di messa a disposizione di dati personali;

- Profilazione: trattamento automatizzato di dati personali per valutare determinati aspetti personali relativi ad una persona fisica come a titolo esemplificativo, rendimento professionale, situazione economica;
- Archivio: insieme strutturato di dati personali accessibili secondo criteri determinati;
- Pseudonimizzazione: trattamento di dati in modo che non si possa risalire all'identificazione dell'interessato senza informazioni aggiuntive conservate separatamente e soggette a misure di sicurezza;
- Titolare del trattamento: ente locale che anche congiuntamente determina e decide le finalità ed i mezzi del trattamento;
- Responsabile del trattamento: persona fisica o giuridica o ente pubblico che tratta i dati per conto del Titolare del trattamento;
- Destinatario: persona fisica o giuridica, ente pubblico che riceve comunicazione di dati personali;
- Terzo: chiunque (persona fisica, giuridica, ente pubblico) diverso dall'interessato, dal titolare del trattamento, dal responsabile del trattamento, da ogni incaricato.
- Consenso dell'interessato: ogni manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato con cui viene manifestato il suo assenso e viene conferita legittimità al trattamento dei propri dati personali;
- Violazione dei dati personali: ogni diffusione, trasmissione, accesso, comunicazione non autorizzata;
- Dati relativi alla salute: dati personali sensibili sullo stato di salute fisica e mentale di una persona fisica, inclusa la prestazione di servizi di assistenza sanitaria, inclusi i dati genetici e biometrici;
- Dati giudiziari: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

TITOLO II
SOGGETTI DEL TRATTAMENTO DEI DATI

Art. 4
Titolare del trattamento

1. Il Titolare del trattamento dei dati personali è lo Istituto Autonomo Case Popolari di Catania, rappresentato ai fini legali previsti dal Regolamento UE n. 679/2016, dal Presidente del Consiglio di Amministrazione, o dall'organo di rappresentanza commissariale, fino alla regolarizzazione della Giunta e dal Presidente della Regione Sicilia. Esso è il Responsabile per tutte le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati e può agire tramite un suo delegato per le competenze attribuite dal presente regolamento.

2. l'Istituto Autonomo Case Popolari di Catania adotta tutte le misure tecniche ed organizzative idonee a garantire che il trattamento è conforme ai principi di cui all'art. 2 e ciò deve essere dimostrabile.

3. Tramite verifiche periodiche deve vigilare sulla osservanza delle istruzioni scritte impartite ai Responsabili e sul pieno rispetto delle vigenti disposizioni in materia di trattamento dati.

4. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata allo Istituto da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato.

Art. 5 *Responsabili del trattamento*

I Responsabili del Trattamento dei dati personali dell'Ente sono i dirigenti responsabili delle singole Aree. Hanno competenza di redigere, formare e approvare il Regolamento per la protezione dei dati e di indicare eventuali responsabili sostitutivi delle singole aree.

Il nominativo nonché indirizzo Pec dei Responsabili va pubblicato nel sito dell'Ente alla sezione Amministrazione trasparente.

I Responsabili di trattamento dovranno svolgere i compiti specificati nel provvedimento di nomina, precisamente:

– garantire la presenza di altro incaricato, autorizzato al trattamento e alla riservatezza, nonché sia in possesso di apposita formazione;
– riferire al Titolare del trattamento e al RPD ogni violazione di dati personali di cui viene a conoscenza senza ritardo ed assisterlo nel procedimento di notifica al Garante ai sensi del successivo art. 37;
– fornire assistenza al Titolare del trattamento e al RPD per le comunicazioni all'interessato di violazione dei dati personali ai sensi del successivo art. 38;
– collaborare alla gestione del registro delle attività di trattamento dell'Ente come da successivo art. 16.
– collaborare alle richieste di accesso, di limitazione ed opposizione degli interessati relative a trattamenti di dati personali;
– attuare, insieme al Titolare del trattamento e al RPD, misure organizzative e tecniche adeguate per garantire il livello di sicurezza come da successivo art. 30, nonché alla procedura di valutazione di impatto sulla protezione dei dati (D.P.I.A.).

Art. 6

Sub-responsabili del trattamento

1. il Responsabile del Trattamento e / o ogni Responsabile del trattamento è autorizzato a nominare eventuali sostituti, responsabili del trattamento per settori specifici con determina che:

– individua e delimita specificatamente l'ambito del trattamento consentito, contiene specifiche istruzioni ed individua le competenze del sub-responsabile tra le quali in particolare:
  - la comunicazione agli interessati dell'informativa relativa al trattamento dei dati e alla loro diffusione;
  - la collaborazione alle richieste di accesso, di limitazione ed opposizione degli interessati relative a trattamenti di dati personali effettuati dal settore di propria competenza.

2. La nomina va comunicata al Rappresentante dell'Ente cui va anche informato di ogni variazione o sostituzione di sub-responsabili di trattamento.

3. I sub-responsabili operano sotto la diretta responsabilità del proprio Responsabile che li ha nominati; in caso di loro inadempimento risponde verso lo Istituto il Responsabile di trattamento di riferimento.

Art. 7

Responsabili esterni di trattamento

1. lo Istituto può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, 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. A tali Responsabili esterni si applicano le disposizioni dell'articolo 5 in quanto compatibili.

Art. 8

Responsabile della protezione dei dati

1. Il Rappresentante legale pro tempore nomina, con provvedimento motivato, il Responsabile della protezione dei dati (R.P.D.) che deve essere una figura dirigenziale interna all'ente locale che abbia conoscenza o comunque sia formata sulla disciplina della protezione dei dati e che è in posizione di autonomia nei confronti del Titolare del trattamento. Il Responsabile della protezione dei dati può assumere altre competenze interne all'ente che non generino conflitti di interesse con il suo ruolo principale. In particolare la sua figura è incompatibile con quella del Responsabile anticorruzione laddove non coincidono.

2. Il Responsabile della protezione è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti; egli riferisce direttamente al Direttore Generale e all'Organo di Rappresentanza politica o suo delegato o al Responsabile di trattamento

3. Il Titolare del trattamento ed il Responsabile del trattamento forniscono al Responsabile della

protezione dei dati le risorse organizzative e finanziarie necessarie per assolvere i propri compiti, anche considerando l'attuazione delle attività nell'ambito della programmazione operative del DUP, e del bilancio.

4. La nomina del RPD va comunicata al Garante privacy ed a tutto il personale in modo che la sua presenza e le sue funzioni del Responsabile siano note a tutti i dipendenti.

5. Il nominativo nonché indirizzo Pec del RPD va pubblicato nel sito dello Istituto alla sezione Amministrazione trasparente.

Il Raprresentante legale pro tempore, ove non potesse indicare la figura del R.P.D. all'interno delle Aree dirigenziali può ricorrere alla nomina di un Responsabile esterno, attraverso procedure ad evidenza pubblica, tra professionisti di comprovata professionalità e preparazione specifica, esperto sulla materia, che agisce in posizione di autonomia rispetto al Titolare del trattamento e non ha ulteriori incarichi nell'ente che possano dare adito a conflitti di interesse. Il Responsabile svolge le competenze espressamente attribuite con apposito contratto di servizi.

Art. 9

Competenze del Responsabile della protezione dei dati

1. Il Responsabile della protezione dei dati va tempestivamente informato di tutte le questioni riguardanti la protezione dei dati personali e, nell'eseguire i propri compiti, considera i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. In particolare:

– informa e fornisce consulenza al Titolare del trattamento o al Responsabile nonché agli altri dipendenti sub-responsabili;
– verifica l'applicazione corretta della disciplina sul trattamento dei dati personali e del RGPD, ferma restando la responsabilità del Titolare e del Responsabile di trattamento; sorveglia le attribuzioni di responsabilità, le attività di formazione e controllo effettuate dal Titolare e del Responsabile del trattamento;
– collabora in sede di audit nella mappatura dei processi e nella individuazione delle non conformità per le quali suggerisce misure correttive. Successivamente sovrintende i monitoraggi periodici delle soluzioni adottate per verificare la necessità di eventuali riesami o sostituzione delle misure, ai sensi dei successivi artt. 33-35;
– fornisce ai sensi dell'art. 27 il parere sulla necessità di procedere alla valutazione di impatto sulla protezione dei dati personali;
– funge da tramite con il Garante per la consultazione preventiva ai sensi dell'art. 29, in caso residuino rischi elevati in un trattamento, dopo l'adozione della valutazione di impatto sulla protezione dei dati personali;
– fornisce parere al Titolare del trattamento in caso di violazione dei dati personali per la valutazione della gravità del data breach.

Eventuali altri compiti attribuiti dal Titolare come per es. la tenuta del registro di trattamento che non origino conflitti di interesse.

2. Il Responsabile esprime parere non vincolante; l'eventuale adozione di condotta difforme da quella da lui suggerita va motivata.

3. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; 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. Il RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

TITOLO III
TRATTAMENTO DEI DATI PERSONALI

Art. 10

Trattamento dati particolari

1. Gli uffici trattano i dati particolari, sensibili ai sensi dell'art. 9 RGPD, che rivelino l'origine

razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, biometrici, relativi alla salute, alla vita sessuale ed i dati giudiziari:

– per motivi di interesse pubblico rilevante come specificati nel successivo art. 12;
– per un interesse vitale dell'interessato o di altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
– se l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati per una o più finalità specifiche;
– per diritti dell'interessato in materia di diritto del lavoro e sicurezza sociale e protezione sociale autorizzato da norma di legge o contratto collettivo;
– il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
– il trattamento è necessario ai fini di archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici ed è proporzionato alla finalità perseguita;

2. In tutti i casi indicati vanno sempre previste misure di garanzia appropriate e specifiche per tutelare i diritti fondamentali e gli interessati. A tal fine si applicano le misure di sicurezza previste nei successivi artt. 26 e ss.

3. I dati particolari riguardanti lo stato di salute non devono essere divulgati.

Art. 11

Principi del trattamento dei dati particolari e giudiziari

1. I dati particolari di cui all'articolo precedente sono trattati sempre nel rispetto dei principi indicati nell'art 2, ovvero devono essere esatti, pertinenti, non eccedenti ed indispensabili rispetto alle finalità perseguite e sono aggiornati periodicamente.

2. I raffronti e le interconnessioni con altre informazioni sensibili e giudiziarie detenute dallo Istituto sono consentite soltanto previa verifica della loro stretta indispensabilità nei singoli casi ed indicazione scritta dei motivi che ne giustificano l'effettuazione. Lo stesso vale se le predette operazioni sono effettuate utilizzando banche dati di diversi titolari del trattamento, nonché la diffusione di dati sensibili e giudiziari, sono ammesse esclusivamente previa verifica nel rispetto dei limiti e con le modalità stabiliti dalle disposizioni legislative che le prevedono.

3. Sono inutilizzabili i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali (e consigliato per non tenere separato il regolamento per i dati sensibili e giudiziari). Al presente regolamento sono direttamente indicati le schede per il trattamento dei dati particolari, sensibili e

4. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o dello Stato che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Art. 12

Individuazione di interesse pubblico rilevante

I trattamenti di interesse pubblico rilevante effettuati dallo Istituto sono i seguenti:

RAPPORTI DI LAVORO

Sono considerate di rilevante interesse pubblico le attività finalizzate all'instaurazione ed alla gestione dei rapporti di lavoro sia in ordine all'espletamento degli adempimenti previsti in relazione al trattamento economico e giuridico, sia in materia sindacale che i igiene e sicurezza del lavoro.

ATTIVITÀ DI PREDISPOSIZIONE DI ELEMENTI DI TUTELA IN SEDE AMMINISTRATIVA O GIURISDIZIONALE

Sono di rilevante interesse pubblico i trattamenti di dati effettuati in conformità di leggi o di regolamenti per l'applicazione della disciplina sull'accesso ai documenti amministrativi.

Art. 13

Pubblicazione web per obblighi di trasparenza

1. lo Istituto Autonomo Case Popolari di Catania effettua il trattamento di dati personali, contenuti in atti e documenti amministrativi, che devono essere pubblicati sul web per obblighi di trasparenza previsti dal D.Lgs. n. 33/2013.

2. I documenti di cui al comma 1 sono pubblicati tempestivamente sul sito istituzionale dell'amministrazione e vanno mantenuti aggiornati.

3. Non possono essere resi intellegibili i dati non necessari, eccedenti o non pertinenti con la finalità di pubblicazione.

4. I dati particolari idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale possono essere diffusi solo se indispensabili; i dati particolari relativi alla vita sessuale non possono essere diffusi per finalità di trasparenza.

5. I dati particolari idonei a rivelare lo stato di salute non devono essere diffusi.

6. I dati vanno pubblicati in formato di tipo aperto ai sensi dell'art. 68, D.Lgs. n. 82/2005 e sono liberamente riutilizzabili secondo la normativa vigente. I dati personali diversi dai dati sensibili e dai dati giudiziari, possono essere diffusi attraverso siti istituzionali, nonché trattati secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web.

7. I dati, le informazioni e i documenti di cui al comma 1, sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello dell'obbligo di pubblicazione.

8. Deroghe alla predetta durata temporale quinquennale sono previste:

a) nel caso in cui gli atti producono ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della produzione degli effetti;
b) per alcuni dati e informazioni riguardanti i titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale regionale e locale ai sensi dell'art. 14, comma 2, D.Lgs. n. 33/2013 e i titolari di incarichi dirigenziali e di collaborazione o consulenza che devono rimanere pubblicati online per i tre anni successivi dalla cessazione del mandato o dell'incarico ai sensi dell'art. 15, comma 4, D.Lgs. n. 33/2013;
c) nel caso in cui siano previsti diversi termini dalla normativa in materia di trattamento dei dati personali.

9. I dati personali devono essere conservati, in ogni caso, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati; l'interessato ha sempre diritto di ottenere la cancellazione dei dati personali di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati.

Art. 14

Pertinenza delle informazioni contenenti dati personali

1. Non possono essere disposti filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione trasparente".

2. Qualora i dati personali contenuti nei documenti non siano pertinenti o siano eccedenti rispetto all'interesse manifestato dal richiedente nell'istanza di ostensione, al fine di salvaguardare la riservatezza di terzi, l'accesso agli atti può essere limitato, su valutazione del Responsabile del procedimento, mediante l'occultamento di alcuni contenuti.

Art. 15

Trattamento dei dati personali effettuato con sistemi di videosorveglianza

1. Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza richiede apposita informativa agli interessati e questa può essere rilasciata in forma semplificata come indicato al successivo art. 24.

2. Per finalità di tutela della sicurezza urbana, la durata della conservazione dei dati è limitato "*ai* sette giorni successivi[1] alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione in conformità dell'art. 6, co. 9, D.L. n. 11/2009. Tempi di durata maggiore della conservazione dei dati necessitano di richiesta al Garante adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti (es. collaborazione con l'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso).

3. Ai dati raccolti mediante sistemi di videosorveglianza, vanno applicate misure di sicurezza adeguate ai sensi del successivo art. 33.

Art. 16
Registro unico del trattamento

1. Il Titolare del trattamento istituisce e tiene aggiornato, in forma scritta ed in formato elettronico tramite il Responsabile del trattamento un registro delle attività di trattamento svolte sotto la propria responsabilità.

2. Il Registro delle categorie di attività trattate da ciascun Responsabile, reca le seguenti informazioni:

– estremi identificativi e di contatto dello Istituto Autonomo Case Popolari di Catania;
– estremi identificativi e di contatto Responsabile della protezione dei dati o dei responsabili d'Area dirigenziale;
– finalità del trattamento;
– descrizione delle categorie di interessati;
– descrizione delle categorie di dati personali;
– le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
– eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale con documentazione delle garanzie in materia di privacy;
– termini ultimi previsti per la cancellazione delle diverse categorie di dati;
– descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

3. In caso di richiesta del Garante, il Registro privacy è messo immediatamente a disposizione.

È affidato al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Responsabile.

TITOLO IV
DIRITTI DELL'INTERESSATO

Art. 17
Diritto di accesso ed alla portabilità dei dati

1. L'interessato ha sempre diritto di ottenere dal Titolare del trattamento la conferma che sia in corso un trattamento dei dati personali che lo riguardano, di averne accesso e di acquisire le seguenti informazioni:

a) finalità del trattamento;
b) categoria di dati trattati;
c) i destinatari a cui i dati personali sono comunicati;

[1] Cfr. Garante privacy, Provvedimento 8 aprile 2010, n. 1712680, par. 3.4. Negli altri casi i tempi di conservazione sono 24 ore dalla rilevazione dei dati.

d) il periodo di conservazione dei dati previsto o se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del proprio diritto a richiedere la rettifica o cancellazione del dato o la limitazione dei dati o di opporsi al loro trattamento;

f) l'esistenza di un processo automatizzato e della profilazione dei dati nonché informazioni sulla logica utilizzata.

2. La richiesta va inoltrata in forma scritta dall'interessato senza particolari formalità; in caso sia inoltrata con mezzi elettronici, salvo contraria indicazione dell'interessato, le informazioni sono fornite in formato elettronico di uso comune.

3. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.

4. Il Responsabile del trattamento ed i sub-responsabili come individuati dall'art. 6, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, anche al se necessarie, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole. In tale ipotesi, va rilasciata copia del documento richiesto.

4. Il rilascio della copia è gratuito; in caso di richiesta di copie ulteriori il rilascio può essere subordinato al pagamento di un contributo per costi amministrativi.

5. Il diritto alla portabilità dei dati di cui all'articolo 20 del R.G.P.D. non si applica ai trattamenti svolti dallo Istituto necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito lo stesso ente.

Art. 18

Diritto di limitazione

1. L'interessato, previa richiesta scritta, ha diritto ad ottenere la limitazione del trattamento:

– in caso sia contestata l'esattezza dei dati personali, per il periodo necessario alla verifica da parte dello Istituto;

– in caso di trattamento illecito, se si oppone alla cancellazione dei dati chiedendo invece che ne sia limitato l'utilizzo;

– in caso di esercizio di opposizione nell'attesa della verifica dei presupposti del relativo diritto.

2. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.

3. Il Responsabile del trattamento ed i sub-responsabili come individuati dall'art. 6, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, anche al se necessarie, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole.

4. In caso di riscontro favorevole va comunicato all'interessato che ha ottenuto la limitazione del trattamento, senza ritardo e prima che la limitazione sia revocata nei casi 1 e 3. Vanno altresì avvisati i destinatari della limitazione dei dati, salvo ciò non sia impossibile o richieda uno sforzo sproporzionato.

Art. 19

Diritto all'oblio

1. L'interessato ha diritto a chiedere previa richiesta scritta, al Titolare del trattamento la cancellazione dei dati personali che lo riguardano:

– se non sono più necessari per le finalità per le quali sono stati raccolti o trattati;

– se si oppone al trattamento e non sussiste motivo legittimo prevalente per procedere al trattamento;

– se i dati sono illecitamente trattati.

2. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.

3. Il Responsabile del trattamento ed i sub-responsabili come individuati dall'art. 6, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, anche al se necessarie, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole.

4. In caso i dati siano stati diffusi pubblicamente anche su siti web, il Titolare del trattamento, tenendo conto dei costi di attuazione, è tenuto ad informare altri titolari che trattano i medesimi dati, della richiesta di cancellazione di qualsiasi link, copia o riproduzione.

5. In caso in cui i dati non siano diffusi pubblicamente e su siti web il Titolare del trattamento è tenuto ad avvisare i destinatari della cancellazione dei dati, salvo ciò non sia impossibile o richieda uno sforzo sproporzionato.

Art. 20

Diritto alla rettifica dei dati

1. L'interessato ha diritto a chiedere previa richiesta scritta, la rettifica da parte del lo Istituto, senza ingiustificato ritardo, dei dati personali inesatti che lo riguardano. La rettifica include anche la possibile integrazione dei dati avuto riguardo alla finalità del trattamento.

2. Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.

3. Il Responsabile del trattamento ed i sub-responsabili come individuati dall'art. 6, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, anche al se necessarie, anche al fine di identificarlo e, successivamente, per dare seguito all'esercizio del diritto dell'interessato.

Art. 21

Diritto di opposizione

1. L'interessato può presentare per iscritto richiesta di opposizione al trattamento dei dati personali che lo riguardano per motivi connessi alla sua situazione particolare, inclusa la profilazione.

2. Il Titolare del trattamento entro trenta giorni fornisce risposta all'interessato a seguito della valutazione della situazione: è consentito l'esercizio del diritto se non esistano comprovati motivi basati su norma di legge per procedere al trattamento prevalenti sugli interessi del richiedente o se si tratta di esercizio o accertamento di un diritto in sede giudiziaria.

3. Il termine di cui al precedente comma può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.

4. Il Responsabile del trattamento ed i sub-responsabili come individuati dall'art. 6, sono tenuti a collaborare nel procedimento interno di verifica dei presupposti del diritto di opposizione.

5. In ogni comunicazione all'interessato deve essere inserito l'avviso in modo chiaro e separato dal restante contenuto dell'atto che questi può esercitare il diritto all'opposizione.

Art. 22

Obbligo di informativa

1. Prima che inizi qualunque trattamento di dati personali il Titolare del trattamento fornisce all'interessato le informazioni necessarie per consentirgli l'esercizio dei propri diritti.

2. L'informativa privacy deve essere fornita per iscritto in formato cartaceo o elettronico, o qualora l'interessato lo richieda espressamente, anche oralmente, previa verifica dell'identità dell'interessato.

3. Essa va effettuata:

– in caso di dati personali raccolti presso l'interessato prima dell'inizio del trattamento, nel momento della raccolta dei dati;
– in caso di dati personali non ottenuti presso l'interessato:
  - entro un termine ragionevole, massimo di un mese dalla raccolta (non registrazione) dei dati;
  - nel caso in cui i dati vadano comunicati all'interessato alla prima comunicazione;
  - se i dati personali devono essere comunicati ad un altro destinatario, non oltre la prima comunicazione.

4. Non è necessario fornire l'informativa:

– nel caso in cui l'interessato disponga già di tutte le informazioni necessarie;
– nel caso in cui la comunicazione risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi il Titolare del trattamento adotta misure comunque appropriate per tutelare i diritti dell'interessato anche con pubbliche informazioni.

5. In presenza di un obbligo di legge che impone la riservatezza e segretezza dei dati personali.

Art. 23

Contenuto dell'informativa

1. L'informativa è gratuita e deve essere sintetica, presentare un linguaggio chiaro e semplice ed essere in ogni caso comprensibile per l'interessato.

2. Essa presenta il seguente contenuto:

– indicazione del Titolare del Trattamento e del Responsabile del trattamento;
– indicazione del Responsabile della protezione dei dati;
– indicazione di ogni finalità istituzionale di trattamento e della norma giuridica di riferimento;
– indicazione di finalità aventi fondamento in contratto o in richiesta dell'interessato;
– indicazione delle modalità di trattamento distinte anche in base all'ufficio che lo effettua evidenziando se sia un trattamento automatizzato (con eventuale possibilità di profilazione e della sua logica) o se sia un trattamento cartaceo;
– indicazione dei destinatari;
– il periodo di conservazione dei dati personali e, se non è previsto da norma di legge, il criterio utilizzato dal Titolare per la durata del trattamento;
– l'indicazione dei diritti che l'interessato può esercitare, ovvero: accesso, integrazione e rettifica, eventuale revoca, portabilità, oblio opposizione e reclamo;
– le conseguenze in caso di rifiuto del trattamento o di omessa comunicazione di dati.

3. Il Titolare del trattamento può di volta in volta aggiungere ogni ulteriore informazione che si ritiene necessaria al caso concreto.

Art. 24

Informativa per utilizzo di sistemi di videosorveglianza

1. Nel caso di utilizzo di sistemi di videosorveglianza per finalità di sicurezza urbana, gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).

2. A tal fine può essere utilizzato un modello di informativa semplificata (all. 1) che poi rinvii a un testo contenente tutti gli elementi completi di cui all'articolo precedente, disponibile agevolmente senza oneri per gli interessati, sia nel sito internet dell'amministrazione comunale sia affisso nella sede della polizia municipale *(indicare la soluzione scelta dall'ente locale come indicato in nota)*.

3. In ogni caso il Titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'articolo precedente.

4. Il supporto con l'informativa:

– deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
– deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
– può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Art. 25
Consenso

1. Il consenso al trattamento dei dati non è richiesto allo Istituto Autonomo Case Popolari di Catania in quanto pubblica amministrazione se agisce per finalità istituzionali.

2. Il consenso può essere richiesto se lo Istituto agisce per specifiche finalità diverse da quelle istituzionali ai sensi dell'art. 1, comma 1, lett. e). In tal caso il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.

3. La richiesta di consenso deve essere comprensibile, facilmente accessibile, chiara e semplice.

4. Il consenso può essere revocato ed in tal caso la revoca non pregiudica la liceità del trattamento già effettuato.

TITOLO VI
MISURE DI SICUREZZA

Art. 26
Misure di sicurezza preventive

1. Lo Istituto deve adottare misure che soddisfino la protezione dei dati fin dalla progettazione e della protezione dei dati di default; ovvero, mette in atto misure tecniche ed organizzative adeguate sia prima del trattamento, sia nell'atto del trattamento stesso indicate nel presente titolo.

2. In particolare:
– utilizza le tecniche di pseudonimizzazione dei dati personali;
– tratta i soli dati necessari per ogni specifica finalità al fine di garantire la massima protezione dei dati attraverso il loro minimo trattamento;
– custodisce e controlla i dati personali in modo da ridurre al minimo, mediante l'adozione di misure di sicurezza preventive, i rischi di distruzione, perdita, anche accidentale, de dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità pubbliche di raccolta;
– provvede a formare il personale sugli obblighi in materia di protezione dei dati personali in relazione alle specifiche competenze rivestite dai singoli dipendenti e dai rispettivi uffici in cui sono inseriti.

3. favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 27
D.P.I.A.

1. Oltre le misure preventive di cui all'articolo precedente, lo Istituto Autonomo Case Popolari, quando un trattamento presenta a seguito di analisi, rischi elevati per i diritti e le libertà degli interessati, procede alla valutazione di impatto sulla protezione dei dati (D.P.I.A.).

2. La D.P.I.A. può riguardare una singola operazione di trattamento o due o più trattamenti simili che presentano rischi elevati analoghi.

3. Ricorrono rischi elevati ai sensi dell'art. 35, par. 3, lett. a)-c) Reg. UE 679/2016 in presenza di:

– una valutazione sistematica di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione e sulla quali si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su tali persone fisiche;
– trattamento su larga scala, di categorie particolari di dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, relativi alla salute, alla vita sessuale o condanne penali, a reati e misure di sicurezza;
– sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. In caso ricorra uno dei tre indici di cui al comma precedente l'ente deve procedere nella D.P.I.A.

5. lo Istituto altresì redige una valutazione di impatto del rischio se ricorrono due dei seguenti indici forniti dal Garante:

– valutazione o assegnazione di un punteggio inclusiva di profilazione, in particolare in considerazione di 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;
– dati sensibili o di carattere altamente personale;
– trattamento di dati su larga scala;
– creazione di corrispondenze o combinazione di insiemi di dati;
– dati relativi a interessati vulnerabili considerato lo squilibrio di potere tra gli interessati e l'ente;
– uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative quando il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

6. Il Titolare se lo ritiene opportuno può procedere anche alla D.P.I.A. in caso ricorra anche uno solo dei requisiti sopra indicati e può individuare anche altri criteri di riscontro del rischio elevato in base alla specifica circostanza.

Art. 28

Procedimento

1. Qualora ricorra un rischio elevato il Titolare del trattamento, chiede il parere del Responsabile della Protezione dei dati e, se lo ritiene opportuno, degli stessi interessati.

2. La D.P.I.A. deve presentare il seguente contenuto minimo:

– una descrizione dei trattamenti previsti e delle finalità del trattamento;
– una valutazione della necessità e proporzionalità dei trattamenti;
– una valutazione dei rischi per i diritti e le libertà degli interessati;
– le misure previste per affrontare i rischi.

3. La D.P.I.A. può essere effettuata anche dal Responsabile del trattamento ma la responsabilità finale è del Titolare del trattamento.

4. In caso la D.P.I.A. non riesca a trattare in maniera sufficiente i rischi individuati, per quelli residui va effettuata, per tramite del Responsabile della protezione dei dati, la consultazione del Garante.

5. *(eventuale)* La D.P.I.A. in sintesi va menzionata all'interno dei procedimenti amministrativi nei quali si inserisce (procedure concorsuali, appalti) e va riportata in sintesi nei documenti pertinenti.

Art. 29

Consultazione preventiva del Garante della privacy

1. Nei casi in cui si è proceduto nella valutazione di impatto sulla protezione dei dati ed è emerso che l'ente non riesce a trattare in maniera sufficiente tutti i rischi elevati, poiché ne restano ancora alcuni per questi ultimi residui, va consultato preventivamente il Garante per la privacy.

2. lo Istituto Autonomo Case Popolari di Catania, tramite il Responsabile della protezione dei dati ai sensi degli artt. 36 e 39, par. 1, lett. e), Regolamento UE n. 679/2016, invia richiesta di consultazione al Garante comunicando:

– i dati dell’ente locale in quanto Titolare del trattamento ed i propri dati in quanto punto di contatto e referente per la consultazione;
– le finalità ed i mezzi di trattamento previsti;
– le misure di garanzia previste per proteggere i diritti e le libertà fondamentali degli interessati;
– la valutazione di impatto sulla protezione dei dati in versione completa;
– ogni altra informazione ritenuta necessaria.

3. Il Garante formula parere scritto entro otto settimane dal ricevimento della richiesta di consultazione nel caso in cui ritenga che il trattamento comunicato violi le norme sulla protezione dei dati ed in particolare qualora ritenga che l’ente non abbia sufficientemente attenuato o identificato il rischio. In base alla complessità del trattamento previsto il Garante può prorogare la sua risposta di un termine aggiuntivo di sei settimane informando il Responsabile della protezione dei dati, entro un mese dal ricevimento della richiesta di consultazione.

4. In caso sia necessario il Garante può richiedere al Responsabile della protezione dei dati informazioni aggiuntive a quelle già comunicate e può sospendere la decorrenza dei termini di cui al comma 3 in attesa della loro trasmissione.

5. In assenza di parere espresso del Garante entro le otto settimane dal ricevimento della richiesta di consultazione, l’ente può procedere nel trattamento dei dati.

Art. 30

Misure di sicurezza minime per trattamenti con strumenti elettronici ed informatici

1. Il Titolare del trattamento insieme al Responsabile della sicurezza ed al Responsabile della Protezione dei dati, controlla le banche dati organizzate in archivi elettronici e fornisce a tutto il personale che le utilizza direttive per garantire che le operazioni informatiche di trattamento siano svolte senza rischi per gli interessati. In particolare vengono adottate le seguenti misure di sicurezza:

– attribuzione agli incaricati di codici identificativi (parola chiave) composti di almeno otto caratteri, oppure, nel caso lo strumento elettronico non lo consenta, da un numero di caratteri pari al massimo consentito;
– modifica della parola chiave da parte dell’incaricato al primo utilizzo e successivamente, almeno ogni tre/sei mesi;
– disattivazione dei codici identificativi in caso di perdita della qualità degli stessi o di mancato utilizzo per un periodo superiore a sei mesi;
– protezione degli elaboratori contro i rischi di intrusioni, mediante l’utilizzo di appositi programmi;
– verifica dell’efficacia e dell’aggiornamento del software antivirus, almeno con cadenza semestrale/mensile/quindicinale;
– distruzione dei supporti di memorizzazione nel caso non siano riutilizzabili;
– applicazione di tecniche di pseudonimizzazione ai dati personali trattati;
– sistemi antintrusioni e di protezione (firewall, antivirus ecc.), misure antincendio;
– sistemi di copiatura e conservazione di archivi elettronici, misure idonee a ripristinare tempestivamente la disponibilità e l’accesso ai dati in caso di incidente fisico o tecnico.

2. Sono inoltre impartite con circolari interne le istruzioni agli incaricati per non lasciare incustodito ed accessibile il proprio strumento elettronico durante una sessione di trattamento.

3. *(in caso di avvilimento di soggetti esterni per l’adozione di misure di sicurezza)* l’ente deve ricevere dall’installatore, per iscritto, la descrizione dell’intervento effettuato conforme alle misure disposte alla normativa sulla protezione dei dati personali.

Art. 31

Misure per trattamenti non automatizzati

1. l’ente fornisce istruzioni scritte agli incaricati anche per i trattamenti di dati personali effettuati senza l’ausilio di strumenti elettronici, in particolare, per il controllo e la custodia, per intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

2. I documenti che contengano dati sensibili e giudiziari, sono controllati fino alla restituzione in modo che non accedano ad essi persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

3. L’accesso agli archivi contenenti dati sensibili o giudiziari è controllato.

4. Le persone ammesse, dopo l’orario di chiusura, sono identificate e registrate e se mancano strumenti elettronici di controllo degli accessi agli archivi, questi vanno preventivamente autorizzati.

Art. 32

Misure per dati raccolti con sistemi di videosorveglianza

1. I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.

2. Occorre rispettare i princìpi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l’angolo visuale delle riprese, evitando – quando non indispensabili – immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.

3. Devono quindi essere adottate almeno le seguenti specifiche misure tecniche ed organizzative:

– in presenza di differenti competenze attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, Responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
– laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
– nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
– qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo.

4. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza predisponendo apposita informativa di cui all’art. 24 del presente regolamento nonché va determinato con precisione il periodo di eventuale conservazione delle immagini, prima della loro cancellazione ai sensi dell’art. 15 del presente regolamento.

Art. 33

Sistema e politica di audit

1. l’ente mette in atto misure tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è conforme al Regolamento UE 679/2016 e, a tal fine, adotta il procedimento di audit in conformità anche delle politiche della qualità.

2. l’ente tramite il Responsabile della protezione dei dati, valuta, mediante audit, i processi interni all’ente locale per:

– verificare il grado di conformità del trattamento dei dati personali effettuato da tutti gli uffici alla normativa vigente;
– verificare che tutti i dipendenti osservino le regole per la liceità e la sicurezza del trattamento di dati personali;
– verificare l'efficacia di azioni correttive a seguito di "non conformità".

3. Il processo consiste:

– in una prima mappatura delle possibili situazioni di rischio che si verificano nell'ente in base alla sua organizzazione interna, agli uffici ed al trattamento dei dati di ciascuno;
– nell'individuare situazioni di non conformità del trattamento agli standard minimi di sicurezza come anche previsti nel presente titolo;
– nel porre in essere azioni correttive.

4. Il processo del comma precedente, dopo la prima volta che è stato effettuato, si sviluppa in monitoraggi periodici di verifica dell'applicazione delle misure stabilite e nella sostituzione o riesame delle misure per il miglioramento dei trattamenti da parte dei vari uffici dell'ente.

Art. 34

Procedimento di audit

1. l'ente, ed insieme al Responsabile della protezione dei dati, anche avvalendosi di esperti, procede nell'audit concretamente mediante:

– somministrazione di questionari ed interviste dirette al Responsabile, ai sub-responsabili di trattamento ed agli incaricati;
– consultazione delle banche dati ed archivi informatici e cartacei dell'ente;

2. A seguito dell'attività di cui al comma precedente, vengono analizzati i risultati emersi che possono consistere in:

– situazioni di conformità;
– raccomandazioni per il miglioramento;
– situazioni di non conformità.

3. Tali risultati vengono formalizzati in un rapporto di Audit che da atto di tutte le fasi del procedimento svolto e fornisce all'ente l'indicazione delle eventuali azioni correttive da porre in essere.

Art. 35

Monitoraggio semestrale

1. lo Istituto Autonomo Case Popolari di Catania, tramite il Responsabile di trattamento, verifica almeno ogni sei mesi che vengano applicate le procedure interne e delle misure di sicurezza adottate in sede di audit e, precisamente che:

– venga fatto un uso corretto di mezzi informatici ai fini del trattamento dei dati personali, in particolare monitorando l'utilizzo delle password e gli accessi agli archivi elettronici contenenti dati personali con particolare attenzione ai dati sensibili;
– venga fatto un corretto utilizzo degli archivi cartacei che conservano i dati personali con particolare riguardo alla conservazione dei dati sensibili;
– vengano adeguatamente formati i dipendenti in modo diversificato in base alla modalità di trattamento cui sono preposti;
– ogni ufficio comunale tratti i dati secondo il principio di minimizzazione, ovvero, solo a ciò che sia strettamente necessario, si accerti dell'esattezza e correttezza dei dati e che conservi i dati nel rispetto dei termini indicati dalle norme, laddove presenti, o, in subordine per il tempo strettamente necessario al raggiungimento della finalità di trattamento;
– in caso di incidenti o violazioni come descritte al titolo successivo, siano applicate le misure correttive per porre riparo agli effetti negativi;

– che siano garantiti i diritti degli interessati e correttamente curate le istanze di accesso, cancellazione, limitazione del trattamento, rettifica nonché siano verificate le istanze di opposizione nonché i reclami eventualmente presentati al Garante;
– che vengano tenuti sempre aggiornati i contenuti delle informative e siano adattate alle esigenze dei differenti uffici e differenti trattamenti;
– che i documenti contenenti dati personali, presenti nel sito internet dell'ente con particolare riferimento alla pubblicazione all'albo pretorio ed alla sezione Amministrazione Trasparente siano conformi ai tempi di pubblicazione previsti dall'art. 124, D.Lgs. n. 267/2000 e D.Lgs. n. 33/2013;
– che nelle ipotesi di utilizzo di sistemi di videosorveglianza vengano rispettate le specifiche misure di sicurezza come indicate negli artt. 24, 33, 32 del presente regolamento.

2. In caso di riscontro di non corretta applicazione del sistema di audit predisposto e delle norme sul trattamento dei dati personali, il Responsabile di trattamento insieme al Responsabile della Protezione dei dati predispone l'adozione di misure nuove correttive.

3. Se in sede di monitoraggio semestrale, insieme alla collaborazione del Responsabile della protezione dei dati, si riscontri la possibilità di migliorare ulteriormente il trattamento dei dati effettuato dai vari uffici comunali nell'ottica di obiettivi di efficienza, il Responsabile del trattamento procede nel riesame e nella sostituzione delle misure già applicate.

TITOLO VI
DATA BREACH O VIOLAZIONE DEI DATI PERSONALI
Art. 36
Definizione di violazione dati personali

1. La violazione dei dati personali è una violazione di sicurezza che comporta accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali.

2. Per ***distruzione non autorizzata*** è da intendersi un'azione che rende irreversibile il processo di ricostruzione del dato personale determinando la sua esatta e totale eliminazione in rerum natura.

3. Per ***perdita*** è da intendersi la fuoriuscita del dato trattato ai fini di privacy dalla sfera del legittimo detentore in modo del tutto incontrollato e non tracciato.

4. Per ***modifica non autorizzata*** è da intendersi una deficienza organizzativa o fatti illeciti che, incidendo sulla conformazione del dato, è capace di arrecare danni fisici e morali agli interessati (es. si pensi nel mondo della sanità a casi di sostituzioni errate di terapie).

5. Per ***rivelazione non autorizzata*** è da intendersi la comunicazione di un segreto professionale.

6. Per ***accesso non autorizzato*** è da intendersi l'illecita attività di terzi (hacker) capaci di sottrarre e disporre di dati di un sistema attaccato grazie a particolari tecniche elusive di protezione.

7. Per ***soggetto non autorizzato*** è da intendersi ogni persona diversa da quella competente nell'ente a possedere e trattare i dati.

Art. 37
Procedimento in caso di data breach

1. Il Responsabile del trattamento in caso venga a conoscenza della violazione informa senza ingiustificato ritardo il Titolare del trattamento e richiede immediato parere al Responsabile della protezione dei dati sulla gravità della violazione, ovvero:

– se questa sia inoffensiva per le misure di sicurezza già presenti in questo ente;
– se può comportare rischi per gli interessati al trattamento ed il grado dei rischi;
– le misure di sicurezza eventualmente da adottare per porre rimedio alla violazione.

2. Il Responsabile del trattamento relaziona immediatamente al Titolare del trattamento la violazione indicando la categoria di dati violati ed allega il parere del Responsabile della protezione dei dati in cui viene indicato se le misure presenti nell'ente rendono la violazione inoffensiva o, se invece, vanno integrate.

3. Al Titolare del trattamento compete la valutazione finale sulla gravità o meno della violazione. In caso venga riscontrata la presenza di rischi per le persone fisiche va effettuata via Pec la notifica del data breach al Garante per la privacy entro 72 ore dal momento in cui ne è venuto a conoscenza o, se in un momento successivo, nel provvedimento vanno indicati i motivi del ritardo.

Art. 38

Notifica al Garante della privacy

1. La Notifica al Garante non è necessaria se la violazione è inoffensiva, cioè vi è assenza di rischio per interessati e persone fisiche e ciò si verifica se l'ente al momento in cui essa si è verificata aveva misure di sicurezza che hanno reso i dati inintellegibili perché per esempio anonimi o cifrati in modo sicuro attraverso un algoritmo standardizzato o mediante schemi di cifratura a chiave simmetrica.

2. Non ricorre l'inintellegibilità se la violazione ha portato la distruzione o perdita dei dati personali.

3. La notifica al Garante deve presentare il seguente contenuto minimo:

– la natura della violazione dei dati personali le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
– il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
– le probabili conseguenze della violazione dei dati personali;
– le misure adottate o di cui si propone l'adozione da parte dell'ente per porre rimedio alla violazione dei dati personali.

A questo contenuto minimo è possibile aggiungere ogni altra informazione che il Titolare ritiene necessaria.

4. In caso non si sia in possesso delle informazioni di cui al comma 3 il Titolare procederà a comunicare entro 72 ore quelle di cui è a conoscenza e successivamente, appena verrà in possesso dei dati mancanti effettuerà una comunicazione integrativa senza ingiustificato ritardo.

5. Il Garante può indicare l'adozione di misure integrative a quelle già descritte nella notifica, oltre che fornire osservazioni per porre rimedio alla violazione e può anche imporre la comunicazione all'interessato di cui al successivo articolo, qualora non sia stata ritenuta necessaria dall'ente.

Art. 39

Comunicazione all'interessato

1. Il Titolare del trattamento comunica, senza giustificato ritardo, all'interessato la violazione in presenza solo di rischio elevato per i diritti e le libertà delle persone fisiche. Quanto più attuale è il dato violato tanto maggiore è la probabilità di rischio elevato, intendendosi per attualità il tempo trascorso dall'acquisizione/raccolta del dato.

2. La comunicazione all'interessato va effettuata con un linguaggio semplice e chiaro e deve presentare anch'essa un contenuto minimo rappresentato da:

– il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
– le probabili conseguenze della violazione dei dati personali;
– le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali

3. In caso non ricorrano i presupposti per la notifica al Garante come indicati dall'articolo precedente, non si procede nemmeno alla comunicazione all'interessato.

Questa inoltre non è necessaria se:

– i dati violati erano soggetti a misure di protezione tali da renderli incomprensibili, perché per es. sottoposti a cifratura;
– il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

– la comunicazione ad personam richiederebbe sforzi sproporzionati per l'elevato numero di interessati. In tal caso, l'ente può procedere ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia; es. tramite web o giornale locale.

Art. 40

Documentazione della violazione - Registro della violazione

1. Il Titolare del trattamento documenta ogni violazione dei dati personali, la procedura avviata internamente all'ente locale ed i provvedimenti per porvi rimedio. A tal fine redige apposita scheda tecnica cui sono allegati la relazione del Responsabile del trattamento ed il parere del RPD.

2. Il Titolare del trattamento annota la violazione nel *Registro delle violazioni*, che contiene tra le altre informazioni: l'ufficio dell'ente locale competente al trattamento dei dati violati, la descrizione e la gravità del data breach, l'indicazione dei dispositivi cartacei o automatizzati coinvolti, la categoria dei dati violati e dei destinatari, le misure di sicurezza presenti ed applicate ai dati violati e le ulteriori eventuali misure adottate.

3. La documentazione è a disposizione di eventuali ispezioni e verifiche da parte del Garante privacy.

TITOLO VI

MEZZI DI TUTELE E RESPONSABILITÀ

Art. 41

Soggetti responsabili ed azione risarcitoria

1. lo Istituto Autonomo Case Popolari di Catania è Responsabile per ogni danno materiale o immateriale causato da una violazione dei dati personali trattati ed è tenuto a risarcire l'interessato o la persona fisica e giuridica danneggiata.

2. All'obbligazione risarcitoria è tenuto verso il danneggiato anche il Responsabile del trattamento se il danno è stato causato da un suo inadempimento nell'ambito dei compiti a cui è stato preposto.

3. Il Titolare del trattamento ed il Responsabile del trattamento vanno esenti da responsabilità se provano che l'evento dannoso non è loro imputabile.

4. L'azione risarcitoria va proposta dinanzi all'autorità giudiziaria ordinaria secondo le norme dell'ordinamento interno.

5. Il Responsabile della Protezione dei dati non risponde nei confronti dei danneggiati ma solo nei confronti dell'entee Titolare del trattamento ed in relazione alle specifiche competenze attribuite al momento del conferimento dell'incarico e con successivi accordi scritti.

Art. 42

Reclamo

1. Fatta salva la tutela giurisdizionale l'interessato può presentare reclamo al Garante se ritiene che l'ente abbia violato la riservatezza dei propri dati.

2. Il reclamo è presentato in forma scritta senza particolari formalità al Garante e contiene la documentazione utile per la valutazione nonché le informazioni sull'ente e sul Responsabile di trattamento oltre che dell'interessato.

3. Il Garante effettua un'istruttoria preliminare in cui può richiedere informazioni all'ente ed all'esito del procedimento può imporre allo stesso di adottare i provvedimenti necessari per rendere il trattamento dei dati conforme alla disciplina vigente.

4. Il Garante informa l'interessato dello stato o dell'esito di reclamo.

Art. 43

Trattamento illecito dei dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione delle norme sulla protezione dei dati personali, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione delle norme sulla materia è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni e la pena accessoria della pubblicazione della sentenza ai sensi degli artt. 167 e 172, D.Lgs. n. 196/2003.

Art. 44

Falsità nelle dichiarazioni e notificazioni al Garante della privacy

Il Responsabile del trattamento o il Responsabile della protezione dei dati che in esecuzione delle rispettive competenze procedono per conto dell'ente con notificazioni, comunicazioni al Garante, qualora forniscano false dichiarazioni o attestazioni o producono documenti falsi, salvo che il fatto costituisca reato più grave, sono puniti con la reclusione da sei mesi a tre anni e la pena accessoria della pubblicazione della sentenza ai sensi degli artt. 168 e 172, D.Lgs. n. 196/2003.

Art. 45

Omessa predisposizione di misure di sicurezza

Il Titolare del trattamento e le persone fisiche che agiscono per suo conto che non adottino le misure di sicurezza minime sono penalmente responsabili e sono puniti con arresto fino a due anni dalle autorità giudiziarie competenti, oltre con la pena accessoria della pubblicazione della sentenza ai sensi degli artt. 169 e 172, D.Lgs. n. 196/2003.

TITOLO VII

ENTRATA IN VIGORE

Art. 46

Abrogazioni

1. Il presente regolamento sostituisce il precedente adottato prima dell'entrata in vigore del Regolamento UE 679/2016; per quanto non previsto si applicano direttamente le norme del regolamento europeo.

2. Il presente regolamento fa riferimento alle sole norme del Codice della privacy ancora oggi vigenti.

Art. 47

Entrata in vigore del regolamento

1. Il presente regolamento entra in vigore il giorno in cui diviene esecutiva la relativa delibera di approvazione.

2. Il regolamento e la relativa modulistica per l'esercizio dei diritti sono resi pubblici mediante pubblicazione sul sito internet dell'ente, nella Sezione Amministrazione Trasparente.

3. Copia del regolamento va inoltrata ai dirigenti, al RPD, al Responsabile del trattamento, ai sub-responsabili ed ogni altro dipendente che tratta dati personali nell'Ente.