Centro Servizi Anziani “U. Bagarella”

REGOLAMENTO POLICY PRIVACY

Allegato “A” alla delibera n. 40 del 19/09/2024

SOMMARIO

PARTE PRIMA: INTRODUZIONE

1. PREMESSA DI CARATTERE NORMATIVO

Il presente Regolamento in materia di protezione dei dati personali (così detta “privacy”) è uno strumento di applicazione del vigente Decreto Legislativo 30 giugno 2003, n. 196 (cosiddetto "Codice sulla privacy”) e, in particolare, del nuovo Regolamento Europeo n. 2016/679, nell'ambito dell'organizzazione dell’Ente Centro Servizi Umberto Bagarella di Dueville (VI).

Dal 25 maggio 2018 ha trovato diretta applicazione, sul territorio nazionale, il nuovo Regolamento Europeo sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell’Unione Europea il 04 maggio 2016.

Il Regolamento disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati. Esso abroga la precedente Direttiva 95/46/CE.

In data 19/09/2018 è entrato in vigore il Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679.

E’ necessario pertanto, come Ente, dotarsi sin da ora di un apposito “Regolamento” che disciplini compiti, attività e *policy* interne che garantiscano l’assolvimento degli adempimenti imposti dalle norme europee, in linea con la forte sanitarizzazione degli interventi e l’aumento considerevole di dati sensibili non sono degli ospiti ma anche dei dipendenti.

Il presente Regolamento del Centro Servizi Anziani U. Bagarella di Dueville, che sostituisce e aggiorna quello deliberato in data 07/08/2018 rubricato al num. 83 di repertorio, si rende inoltre necessario per recepire al meglio non solo, in un unico testo, i precetti normativi di maggior rilevanza, sia di carattere aziendale che nazionale in tema di trattamento dei dati personali *(D.lgs. 196 del 30/06/2003 e ss.mm., regolamenti e codici deontologici succeduti negli ultimi anni, direttive e linee guida del Garante, Direttiva dell'UE 2000/58 sulla riservatezza nelle comunicazioni elettroniche e soprattutto Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati),* ma anche di affrontare nuove tematiche come ad esempio la portabilità dei dati, la profilazione degli stessi, il diritto all’oblio e le limitazioni al trattamento, le quali dovranno essere armonizzate anche negli allegati presenti.

Il presente Regolamento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

2. PREMESSA DI CARATTERE ORGANIZZATIVO

Un’ attenta disamina della normativa vigente in materia di privacy ha fatto emergere una necessità imprescindibile di cambiamento della mentalità che porti alla piena tutela della stessa, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino-utente che si rivolge all’Ente, di una completa riservatezza sotto il profilo sostanziale.

Il diritto alla privacy costituisce, anche secondo il Legislatore europeo, un vero e proprio diritto inviolabile dell'essere umano, che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali nonché dignità del singolo individuo. Per questi motivi, la "cultura della privacy" necessita di divenire un vero e proprio elemento cardine dell'organizzazione di questo Ente. A tale scopo è necessario che il Centro Servizi Umberto Bagarella di Dueville (VI) per mezzo del proprio personale si adoperi affinchè possa crescere e rafforzarsi una maggiore consapevolezza in materia e ciò, non solo con una conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa nel trattamento dei dati, ma anche ponendo in essere tutti gli adempimenti di carattere tecnico ed organizzativo per contribuire concretamente al miglioramento della qualità del rapporto con l'utenza ed implementare il "processo di umanizzazione" in corso di realizzazione, nell'ambito di questo Ente, oramai da molti anni.

3. PREMESSA DI CARATTERE METODOLOGICO

Si intendono parte integrate di tale Regolamento una serie di documenti tecnici atti a dare compiuta attuazione ai dettami della nuova "privacy europea".

Tali documenti, ai quali viene data massima pubblicità e diffusione tramite la pubblicazione sul sito *internet* dell'Ente, sono richiamati all'interno del presente documento quali allegati.

Si sottolinea come il principio cardine della "responsabilizzazione" (accountability nell'accezione inglese), introdotto dal nuovo Regolamento UE, imponga al Titolare del trattamento dei dati l'obbligo di attuare delle politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della **"conformità"** o ***compliance*** nell'accezione inglese); e ciò anche attraverso dei comportamenti proattivi, atti a dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

La normativa vigente lascia al Titolare ampia autonomia decisionale in merito alle modalità, alle garanzie e ai limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Pertanto questo ente si sta impegnando, a far proprio i dettami del Legislatore europeo relativo all'*accountability* ed alla *compliance*. anche attraverso la predisposizione di questo documento.

PARTE SECONDA: DISPOSIZIONI GENERALI

4. OGGETTO DEL REGOLAMENTO

Il presente Regolamento disciplina, all'interno dell'Ente, la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali (Decreto Legislativo del 30/06/2003 n. 196 e ss.mm.) ed in conformità all'emanazione della nuova normativa sovranazionale, il Regolamento UE n. 679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

5. FINALITÀ' DEL REGOLAMENTO

Il Centro Servizi Anziani U. Bagarella di Dueville garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (articolo 8, paragrafo 1, della *Carta dei diritti fondamentali* dell'Unione Europea.)

6. SENSIBILIZZAZIONE

Il Centro Servizi Umberto Bagarella di Dueville (VI) sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto agli ospiti e ai loro familiari.

A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale le e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Ente.

Per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento europeo, e di conseguenza contenute nel presente Regolamento dell'Ente, al momento dell'ingresso in servizio è fornita, a cura dell'Ufficio Personale, ad ogni dipendente *(oltre che ad ogni collaboratore, consulente o tirocinante)* una specifica comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro *(o nella lettera di incarico per i soggetti non dipendenti poc'anzi citati)*, con la quale detti soggetti (dipendenti e non dipendenti) sono nominati quali **"autorizzati al trattamento dei dati"** e **"responsabili al trattamento"** ai sensi del Regolamento UE 2016/679.

Il Regolamento, pubblicato sul sito dell'Ente, contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di incarico), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

7. DEFINIZIONI

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare aziendale si intende per:

a) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può esser identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

b) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

c) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

d) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

e) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

f) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

g) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

h) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

i) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

j) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

k) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

l) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

m) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; a proposito delle tipologie di "dati" sopra indicate, si fa presente che il Regolamento europeo non utilizza la definizione ***"dati sensibili"*** per la quale, quanto meno sino all'emanazione della legge italiana di revisione del D.lgs. 196/20013, si fa espresso rinvio all'articolo n. 4 del vigente Codice della privacy (D.lgs. 196/2003): definizione che, quindi, al momento rimane nell'utilizzo e nel linguaggio corrente per la materia di cui si tratta.

n) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

Quelle sopra riportate, di cui si è data evidenza, rappresentano le "definizioni" su cui ha inciso maggiormente il nuovo Regolamento europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'articolo n. 4 del Regolamento Europeo n. 2016/679.

8. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 5 del Regolamento Europeo n. 2016/679, i dati personali sono:

a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato *(«**liceità, correttezza e trasparenza**»);*

b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico

interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali *(«**limitazione della finalità**»);*

c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati *(**«minimizzazione dei dati»**).* A tale proposito, il Regolamento UE ricalca i principi sostanziali di ***"necessità, pertinenza, indispensabilità e non eccedenza"*** (rispetto alle finalità del trattamento) contenuti negli articoli 4 e 11 del D.lgs. 196/2003.

d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati *(«**esattezza**»);*

e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato *(«**limitazione della conservazione**»);*

f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali *(«**integrità e riservatezza**»).*

Come stabilito dal Regolamento UE, il Titolare del trattamento è competente per il rispetto di quanto sin qui esposto ed è in grado di comprovarlo verso l'esterno (principio europeo dell'*«**accountability**»* o *«**responsabilizzazione**»).*

9. TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI)

Come stabilito dall'articolo n. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino l'*origine razziale o etnica*, le *opinioni politiche,* le *convinzioni religiose* o *filosofiche*, o *l'appartenenza sindacale*, nonché trattare *dati genetici, dati biometrici* intesi a identificare in modo univoco una persona fisica, *dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*.

Detta disposizione non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato articolo n. 9, tra le quali si evidenzia quella di cui alla lettera "g" applicabile a questo Ente, ai sensi della quale "*il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*", nonché quella di cui alla lettera "h", applicabile a questo Ente, ai sensi della quale *"il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero* ***gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri*** *o conformemente al contratto con un professionista della sanità (..)"*.

Si fa presente, inoltre, che il Regolamento UE consente di *"mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute"* (articolo n. 9, paragrafo n. 4).

Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati sensibili, biometrici e genetici e in particolare al "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art.21, comma 1 del D.Lgs 10 Agosto 2018, n. 101" del Garante della Privacy, pubblicato in Gazzetta Ufficiale il 05 Giugno 2019.

10. TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'articolo n. 10 del Regolamento Europeo n. 2016/679, *"il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica."*

Il Regolamento UE 2016/679 pertanto ravvisa quali condizioni necessarie per il trattamento su detto la presenza di una base giuridica che lo giustifichi (l'art. 6, paragrafo 1 del GDPR) ed altresì il controllo dell'autorità pubblica l'autorizzazione del diritto dell'Unione o degli Stati membri, nel rispetto delle garanzie appropriate per i diritti e le libertà degli interessati.

La dottrina prevalente, in merito al fondamento giuridico che consenta di trattare i dati relativi a condanne penali e reati per valutare l'attitudine lavorativa, ha ritenuto che l'autorizzazione da parte del diritto nazionale già risulti presente ai sensi dell'art. 8 del c.d. "Statuto dei Lavoratori" (L. 300/1970) che ne prevede il trattamento nell'ambito della valutazione dell'attitudine lavorativa.

11. COMUNICAZIONE DI DATI VERSO L'ESTERNO

La comunicazione a soggetti terzi di dati di carattere personale e particolare, detenuti dal Titolare del Trattamento, deve avvenire unicamente in ragione delle finalità per le quali gli stessi sono stati acquisiti e di cui si è data contezza nell'informativa privacy consegnata e sottoscritta dagli interessati.

La diffusione di dati che ecceda quanto su indicato, deve considerarsi illecita.

L'eventuale **comunicazione di dati particolari e giudiziari tra soggetti pubblici,** è ammessa solo in presenza di una normativa o di un regolamento che la giustifichino e, in ogni caso, qualora risulti necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi.

12. CARTELLA SOCIO SANITARIA

Nella sua forma tradizionale (cartella clinica cartacea) la cartella clinica costituisce il documento ufficiale e legalmente riconosciuto per la raccolta organica e funzionale dei dati sulla storia clinica di un assistito.

In generale, la funzione fondamentale della cartella clinica è quella di raccogliere le informazioni sulla storia sociale e clinica dell'ospite per poter così fungere da un lato come supporto alla comunicazione multidisciplinare tra i professionisti, dall'altro come supporto decisionale.

Le funzioni che essa assolve sono molteplici e si possono sintetizzare nei seguenti punti:

- fornire una base informativa per scelte assistenziali razionali e per garantire continuità di cura all'ospite, documentando non solo il quadro clinico, ma soprattutto la storia di vita propria e della rete famigliare, attraverso il percorso ed i risultati conseguiti nel corso dell'assistenza;
- costituire un mezzo di comunicazione tra tutti gli attori responsabili nel tempo dell'assistenza all'ospite, che possono così comunicare e assistere l'ospite con continuità, grazie alle annotazioni riportate, si tratta, in effetti, di uno spazio di lavoro condiviso;
- facilitare l'integrazione di competenze multi professionali nel processo di valutazione multidimensionale, favorendo la costituzione di un'informazione completa e organica,
- consentire la tracciabilità delle diverse attività svolte, in termini di responsabilità delle azioni intraprese dal personale medico, infermieristico e assistenziale nonché ludico riabilitativo, attraverso la loro cronologia e le modalità d'esecuzione delle stesse;
- trattandosi di documentazione pubblica di fede privilegiata, permette l'esercizio di diritti e la tutela degli interessi sia dell'ospite sia dell'Ente erogante l'assistenza;

Da quanto appena scritto emerge la centralità della Cartella Socio Sanitaria e la sua importanza per l'erogazione del servizio, essa viene definita nel presente documento come: "Un sistema informatico, ottimizzato per l'uso da parte del personale clinico e di assistenza, che durante la permanenza dell'ospite:

- raccoglie i dati inerenti lo stato di salute e di cura individuale, attività ed eventi legati al paziente;
- supporta tutte le attività e integra dati provenienti da multiple fonti, interne ed esterne, ed i processi di diagnosi e di erogazione delle cure assistenziali, sanitarie e infermieristiche (compresa la gestione di prescrizioni e somministrazioni);

Essa si configura quindi come un sistema informatico integrato aziendale, da intendersi come trasversale alle varie tipologie di processi sanitari, assistenziali e riabilitativi in sostituzione della cartella cartacea, che da un lato ne rispetti i requisiti e le funzioni, e dall'altro risolva alcune criticità ad essa legate, offrendo opportunità di aumentare il valore attraverso l'integrazione con altri strumenti informatici.

Nella Cartella Socio Sanitaria (CSS) una volta adottata, confluiscono quindi **tutte le informazioni dell'ospite e della sua rete famigliare.**

La CSS è consultabile esclusivamente dal personale della struttura, abilitato da apposita password con livelli di interrogazione e visione proporzionali al ruolo.

In uno scenario a regime, al fine di ottimizzare la fruizione e la completezza della CSS, l'Ente dovrà acquisire tramite scanner l'intera documentazione cartacea afferente alla cartella clinica che non possa essere

informatizzata (ad es. consensi informati e referti cartacei di strutture sanitarie terze), così da poterla gestire tramite l'applicativo di CSS come per tutti gli altri documenti di origine elettronica.

Criteri di profilazione degli utenti: per la protezione dei dati personali dell'ospite da specifici rischi di accesso non autorizzato e di trattamenti non consentiti, il personale sanitario *"Autorizzato al Trattamento"* è in possesso di una propria *password* che consente la tracciabilità degli accessi e delle modifiche effettuate, garantendo così anche l'esattezza e l'integrità dei dati.

I server presso cui sono custoditi i dati sono inoltre dotati di sistemi di *Back-up* e di sistemi antivirus e anti intrusione.

I dati personali utilizzati per la costituzione della CSS vengono trattati rispettando i **principi di correttezza, liceità, necessità e finalità** stabiliti dal Regolamento EU e osservando le misure di sicurezza.

L'Ospite, in sede di nota informativa, è anche informato del fatto che in qualsiasi momento, rivolgendosi al *Titolare del Trattamento dei dati,* è in grado di (così come previsto dall'articolo 7 del Decreto Legislativo 196/2003):

- esercitare la **facoltà di oscurare** eventi clinici che lo riguardano *("istanza di oscuramento")*;
- **esercitare il diritto di accesso ai dati personali** contenuti nella Cartella Sanitaria Elettronica *("istanza di esercizio dei diritti");*
- **visionare gli accessi** che sono stati effettuati sulla propria CSS da parte dei soggetti abilitati alla consultazione *("istanza di accesso")*;

PARTE TERZA: DIRITTI DELL'INTERESSATO

13. INFORMATIVA SUL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti **informazioni:**

a. l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b. i dati di contatto del Responsabile della protezione dei dati (D.P.O.);
c. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d. qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f. ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti **ulteriori informazioni necessarie** per garantire un trattamento corretto e trasparente:

a. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b. l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al *diritto alla portabilità* dei dati;
c. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d. il diritto di proporre reclamo a un'autorità di controllo;
e. se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f. l'eventuale esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Per quanto concerne il periodo di conservazione dei dati personali raccolti da questo Ente, i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una **finalità** diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.

14. CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI

Il Regolamento UE conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di **liceità del trattamento** sono indicati all'art. 6 del Regolamento.

In particolare:

- **il consenso deve essere "esplicito"** o il trattamento deve basarsi sul verificarsi dei casi previsti dal GDPR;
- deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile** e non è ammesso il consenso tacito o presunto (non è quindi possibile utilizzare "caselle pre-spuntate" su un modulo);
- deve essere manifestato attraverso **"dichiarazione o azione positiva inequivocabile"** (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Il Regolamento EU prevede tuttavia, sempre all'art. 6, ulteriori fattispecie in cui il trattamento è lecito, senza dover ricorrere al consenso. In particolare:

- il trattamento è necessario all'**esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; la sussistenza tra le parti di un contratto o di una fase pre-contrattuale rappresenta un rapporto basato su uno scambio di volontà tale da implicare tacitamente la volontà necessaria per il trattamento dati; tale presupposto legittimante il trattamento va interpretato in senso restrittivo, solo qualora il trattamento sia una condizione necessaria alla corretta esecuzione degli adempimenti contrattuali e pre-contrattuali;
- il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento: si intende a prescindere dalla natura giuridica dell'Ente (pubblica o privata), purchè il compito sia di interesse della collettività.
- **Interesse legittimo prevalente di un titolare o di un terzo** presuppone invece che sia il titolare stesso ad effettuare un bilanciamento fra il legittimo interesse suo o del terzo e i diritti e libertà dell'interessato e non sia più compito dell'Autorità. Pertanto l'interesse legittimo del titolare o del terzo deve risultare prevalente sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità. Il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

15. DIRITTO DI ACCESSO DELL'INTERESSATO

Come stabilito dall'articolo n. 15 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.
Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.
In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Per quanto riguarda, inoltre, le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo ed organizzativo, il diritto di accesso, si fa rinvio alle vigenti diposizioni normative e regolamentari emanate, negli anni, dal Legislatore statale nonché dal Garante per la privacy.
In questo Ente, la competenza sulla materia *de quo* è affidata al Responsabile aziendale della Trasparenza e della Prevenzione della Corruzione dott. Stefano Garbin Segretario Direttore dell'Ente.
A tale riguardo, nel rinviare a quanto pubblicato al sito web dell'Ente, si fa presente che:

a. per ***accesso documentale*** si intende la domanda di accesso (richiesta di presa visione o di rilascio copia) a delibere o provvedimenti dell'Ente, oppure a documenti di un processo amministrativo, nei termini e alle modalità previste dalla normativa vigente (Legge 07 agosto 1990 n. 241 e ss.mm.ii. e D.P.R. 12 aprile 2006 n. 184). Possono fare domanda tutti i cittadini portatori di un interesse *"diretto, concreto e attuale,*

corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso" (art. 22, Legge 241/1990). Per presentare domanda, è necessario utilizzare la procedura presente nel sito istituzionale. I costi di ricerca, visura e riproduzione fotostatica, e le spese di spedizione, sono quelle previste dal *tariffario dell'Ente* giusta delibera n.27 del 06/12/2022. Il procedimento di accesso si conclude entro 30 giorni, decorrenti dalla presentazione della richiesta all'ufficio competente (art. 6 del D.P.R. 184 del 2006);

b. per ***accesso civico*** si intende il diritto di chiunque di richiedere documenti, informazioni o dati che le pubbliche amministrazioni non hanno pubblicato pur avendone l'obbligo (Decreto Legislativo 97 del 17/5/2016 *"Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza delle Amministrazioni Pubbliche*", e Decreto Legislativo 33 del 14/03/2013: *"Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*"). La richiesta viene presentata al Responsabile della Prevenzione della Corruzione e della Trasparenza dell'Ente utilizzando la procedura presente nel sito istituzionale. L'Ente, entro 30 giorni, procede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto. Se il documento, l'informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente, l'Ente indica al richiedente il relativo collegamento ipertestuale. Nei casi di ritardo o mancata risposta il richiedente può ricorrere al titolare del potere sostitutivo (indicato sul sito web adell'Ente) che, verificata la sussistenza dell'obbligo di pubblicazione, provvede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto;

c. per ***accesso generalizzato*** si intende il diritto di chiunque di accedere ai dati e ai documenti detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del Decreto Legislativo 33/2013 ('Decreto Trasparenza') e del D.lgs. 97/2016 (così detto *Freedom of Information Act* o "FOIA"), nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico. La richiesta viene presentata attraverso la procedura presente nel sito istituzionale.

Il procedimento di accesso generalizzato deve concludersi con provvedimento espresso e motivato nel termine di 30 giorni dalla presentazione dell'istanza, con la comunicazione dell'esito al richiedente e agli eventuali contro interessati. Tali termini sono sospesi (fino ad un massimo di 10 giorni) nel caso di comunicazione della richiesta al controinteressato. Se il documento risulta già pubblicato nel sito dell'Ente nel rispetto della normativa vigente, l'Ente indica al richiedente il relativo collegamento ipertestuale. Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine indicato, il richiedente può presentare richiesta di riesame al Responsabile

della Prevenzione della Corruzione e della Trasparenza, che decide con provvedimento motivato, entro il termine di 20 giorni. Se l'accesso è stato negato o differito il suddetto Responsabile provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di 10 giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del Responsabile è sospeso fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti 10 giorni. Avverso la decisione dell'amministrazione competente o, in caso di richiesta di riesame, avverso quella del Responsabile della Prevenzione della Corruzione e della Trasparenza, il richiedente può proporre ricorso al tribunale amministrativo regionale (TAR).

16. DIRITTO DI RETTIFICA

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

17. DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 2016/679, in capo all'interessato è riconosciuto il **diritto "all'oblio",** che si configura come un diritto alla cancellazione dei propri dati personali **in forma rafforzata.** Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del Regolamento UE).

18. DIRITTO DI LIMITAZIONE AL TRATTAMENTO

Si tratta di un diritto diverso e più esteso rispetto al previgente "blocco" del trattamento di cui all'art. 7, comma 3, lettera b), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì **anche se l'interessato chiede la rettifica dei dati** *(in attesa di tale rettifica da parte del titolare)* **o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento** *(in attesa della valutazione da parte del titolare).*

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la **limitazione** è vietato a meno che ricorrano determinate circostanze *(consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).*

Il diritto alla limitazione prevede che il dato personale sia **"contrassegnato"** in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

19. DIRITTO ALLA PORTABILITA' DEI DATI

Si tratta di uno dei nuovi diritti previsti dal regolamento.

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste **specifiche condizioni per il suo esercizio**; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al Titolare (si veda il considerando 68 del Regolamento UE).

Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

20. DIRITTO DI OPPOSIZIONE

Come stabilito dall'articolo n. 21 del Regolamento Europeo n. 2016/679, l'interessato ha il **diritto di opporsi in qualsiasi momento,** per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni.

Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

21. PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)

Come stabilito dall'articolo n. 22 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul **trattamento automatizzato**, compresa la **profilazione,** che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.

PARTE QUARTA: TITOLARE E RESPONSABILE DEL TRATTAMENTO

22. TITOLARE DEL TRATTAMENTO

Il ***"Titolare"*** del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti del vigente Codice della privacy, è il Centro Servizi Anziani Umberto Bagarella, via IV Novembre 11, Dueville (VI), rappresentato dal Legale Rappresentante il Presidente pro tempore.

Il Titolare, avvalendosi della supervisione e collaborazione del ***Data Protection Officer***, provvede:

a. a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;
b. a nominare con atto deliberativo i *Responsabili del trattamento dei dati personali,* impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy e all'articolo 12 del Regolamento UE, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
c. a nominare il Data Protection Officer, come stabilito dall'articolo 37 del Regolamento UE;
d. a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
e. a mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.

Si dà evidenza, inoltre, del fatto che il Regolamento UE pone con forza l'accento sulla **"responsabilizzazione"** (***accountability*** nell'accezione inglese) di titolari e responsabili, ovverossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del Regolamento).

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Questa Ente sta lavorando attivamente per far proprio l'approccio del Legislatore europeo relativo all'*accountability*.

23. CONTITOLARI DEL TRATTAMENTO

Come stabilito dall'articolo n. 26 del Regolamento Europeo n. 2016/679, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono **contitolari del trattamento.** Essi determinano in modo trasparente, mediante un *accordo interno,* le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

24. DESIGNATO DEL TRATTAMENTO DEI DATI

Secondo il D.lgs. 196/2003, s'intende per Responsabile del trattamento dei dati, *"la persona fisica, giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione ed Organismo preposti dal Titolare al trattamento di dati personali".*

Anche se il Regolamento Europeo (art. 28) disciplina i compiti del Responsabile "esterno" senza contemplare espressamente la figura ed i compiti del Responsabile "interno", questo Ente, in considerazione della complessità e della molteplicità delle proprie funzioni istituzionali e della necessità di continuare a garantire, a tutti i livelli, la più efficace applicabilità dei precetti in materia di privacy, reputa necessario, come sempre avvenuto in passato, continuare a designare in ambito aziendale i ***Designati del trattamento dei dati personali,*** conferendo l'incarico a quei dirigenti apicali che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

Nell'ambito del Centro Servizi Anziani Umberto Bagarella di Dueville (VI) in base all'organizzazione vengono specificamente individuati i **Designati del trattamento dei dati personali.**

Il Titolare del trattamento dei dati deve informare ciascun soggetto, così come individuato dal presente Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti.

Tali figure rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente.

Il Designato del trattamento deve:

1) trattare i dati personali, anche sensibili, osservando le disposizioni del presente Regolamento dell'Ente nonché le specifiche istruzioni impartite dal Titolare;
2) garantire che, presso la propria struttura, le persone autorizzate (incaricate) al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza;

3) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso la propria struttura, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;
4) tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;
5) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel presente Regolamento;
6) contribuire alle attività di verifica del rispetto del regolamento, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

Il Designato, nell'espletamento della sua funzione, deve inoltre collaborare con il Data Protection Officer (DPO) dell'Ente al fine di:

a) comunicare al DPO, quando questi ne faccia richiesta, ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento UE 2016/679 riguardanti: *l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato, la predisposizione del Registro dei trattamenti*.
b) utilizzare la documentazione adottata dall'Ente, verificandone il rispetto e fornendo al DPO, quando questi ne faccia richiesta, le informazioni utili per l'aggiornamento del registro dei trattamenti;
c) rispondere e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
d) contribuire a far sì che tutte le misure di sicurezza riguardanti i dati dell'Ente siano applicate all'interno dell'Ente stesso ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;
e) informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

25. RESPONSABILE DEL TRATTAMENTO DEI DATI

Nell'ambito di questo Ente, sono inoltre individuati quali Responsabili del trattamento dei dati personali, tutti i soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto sottoscritto con l'Ente, trattino dati di cui è titolare l'Ente medesimo e qualora siano in possesso dei requisiti previsti dall'articolo 28 del Regolamento EU (esperienza, capacità ed affidabilità).

In ottemperanza all'articolo 28 del Regolamento Europeo 2016/679, i Responsabili hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa (nazionale ed europea) in materia di privacy;

- trattare i dati personali, anche di natura sensibile e giudiziaria, degli ospiti (o di altri interessati) esclusivamente per le finalità previste dal contratto stipulato con la ditta CBA Informatica di Rovereto (TN) e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;
- rispettare i principi in materia di sicurezza dettati dalla normativa vigente (nazionale ed europea) in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
- adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento Europeo 2016/679 rubricato "Sicurezza del trattamento" che possono anche essere definite dal Titolare del Trattamento;
- nominare, al loro interno, i soggetti autorizzati / incaricati del trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;
- attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a) del Regolamento Europeo;
- specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati;
- assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo *(sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati),* tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;
- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento Europeo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

La designazione del Responsabile viene effettuata mediante "accordo di nomina" sottoscritto da parte del Titolare del trattamento e controfirmato per accettazione da parte del Responsabile esterno: il documento deve

essere richiamato dagli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente all'Ente.

26. AUTORIZZATO AL TRATTAMENTO DEI DATI

Il Regolamento Europeo non fornisce rilievo autonomo alla figura dell'*incaricato* al trattamento dei dati, seppure si soffermi sul fatto che chi tratta dati, ricevendo istruzioni e formazione da parte del Titolare del trattamento debba da questi essere *"autorizzato"* al trattamento (articoli 4 e 10 del Regolamento).

Come già stabilito all'articolo 6 del presente Regolamento, al momento dell'ingresso in servizio è fornita, a cura a cura del personale/ufficio preposto, ad ogni dipendente *(oltre che ad ogni collaboratore, consulente o titolare di borsa di studio)* una specifica comunicazione in materia di privacycon la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali **"autorizzati al trattamento dei dati"** ai sensi del Regolamento UE 2016/679.

Contestualmente alla nomina dovrà essere data copia del presente Regolamento o, in alternative, indicazioni per poterla scaricare dal sito internet dell'Ente.

Il Regolamento contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di autorizzato), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

Analoghe considerazioni valgono per la figura dell'**autorizzato "esterno"**: tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito di questo Ente, pur non essendo dipendenti e neppure titolari di incarichi conferiti dalla medesima Azienda *(quali consulenze, collaborazioni o borse di studio),* devono essere designati da parte del Titolare tramite una lettera (o una nota) di nomina come *autorizzati*.

Ci si riferisce, a titolo esemplificativo, al *personale tirocinante* o al *personale volontario* che opera temporaneamente all'interno dell'Ente in virtù di un accordo o di una convenzione per lo svolgimento, appunto, di tirocini formativi piuttosto che di attività di volontariato a sostegno degli ospiti residenti in struttura.

Il personale di cui si parla è soggetto agli stessi obblighi cui sono sottoposti tutti gli autorizzati "interni", in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.

Nel caso di Autorizzati "esterni", l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività.

27. RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

Il Regolamento Europeo impone la nomina del ***Data Protection Officer*** (DPO, in italiano: Responsabile della protezione dei dati o 'RDP'), nei termini di cui all'articolo 37, 38 e 39 del Regolamento medesimo.

La nomina del RDP è obbligatoria in tutte le organizzazioni, anche pubbliche, che trattano come **attività principali i dati sensibili su larga scala**, come ospedali, assicurazioni e istituti di credito.

Chi svolge la funzione di RPD, quindi, deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. Non deve, inoltre, essere in **conflitto di interessi** in quanto il Regolamento UE vieta di nominare RDP anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi.

Si tratta di una figura di alta professionalità, a metà tra il *consulente* ed il *revisore* e non dovrebbe ricoprire ruoli gestionali rispetto all'attività dell'Ente o ai fini istituzionali della Pubblica Amministrazione.

Anche il Centro Servizi Anziani Umberto Bagarella provvede al conferimento dell'incarico di cui si tratta, tenendo conto delle prescrizioni sin qui descritte.

Ai sensi dell'articolo 39 del Regolamento UE, i suoi compiti sono:

- **sorvegliare l'osservanza del Regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione e delle finalità;
- **fornire consulenza e pareri** al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;
- collaborare con il titolare, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA);**
- **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- **cooperare con il Garante e fungere da punto di contatto per il Garante** su ogni questione connessa al trattamento;
- **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento**.

Ai sensi dell'articolo 37 del Regolamento UE, Egli deve:

- **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;
- **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse.** In linea di principio, ciò significa che il RPD non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;
- **operare alle dipendenze del titolare oppure sulla base di un contratto di servizio** (RPD esterno);
- **disporre di risorse umane e finanziarie**, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Il Regolamento UE prevede la pubblicazione *on line* del curriculum del RDP, nonché la pubblicazione sul sito istituzionale dell'Ente dei **"dati di contatto" del RDP**: dati che debbono essere inseriti anche nell'informativa dell'Ente sul trattamento dei dati, così che il RDP sia agevolmente contattabile dai cittadini-utenti ma anche dal Garante per la privacy.

Sia che il RDP sia interno che esterno, è necessario stipulare con il medesimo un **contratto ad hoc.** Nel caso in cui il RDP sia un "esterno" (persona o società) tutte le clausole, oltre che il compenso per l'incarico, dovranno essere inserite in un apposito contratto di servizi, ove siano anche previste le risorse necessarie a far funzionare l'ufficio del RDP.

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI - MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

28. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

L'articolo n. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese ***"data protection by default and by design"***, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (*"sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso",* secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

29. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda l'articolo 30, paragrafo 5 del Regolamento UE), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'Ente o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro deve essere esibito su richiesta del Garante.

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.

30. PROTEZIONE E SICUREZZA DEI DATI PERSONALI

Le misure di sicurezza devono ***"garantire un livello di sicurezza adeguato al rischio***" del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Per lo stesso motivo, secondo il Regolamento UE non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Il 05 Giugno 2019 il Garante della Privacy ha emanato il "*Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D.Lgs 10 agosto 2018 n.101*" contenente le indicazioni specifiche per alcune fattispecie di trattamenti.

31. NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO

A partire dal 25 maggio 2018, tutti i titolari dovranno **notificare all'Autorità di controllo le violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque *"senza ingiustificato ritardo",* ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del Regolamento UE); questa procedura va sotto il nome di ***"Data Breach".***

Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre *"senza ingiustificato ritardo";* fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento, nonché dalle "*Linee Guida in materia di notifica delle violazioni di dati personali – WP250, definite in base alle previsioni del Regolamento UE 2016/679*" adottate dal Gruppo di Lavoro Art.29 il 03 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) e dal Provvedimento del Garante sulla notifica delle violazioni dei dati personali del 30 Luglio 2019.

Il Titolare del trattamento, sentito il Data Protection Officer dell'Ente, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

32. VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI

Le misure di sicurezza devono ***"garantire un livello di sicurezza adeguato al rischio***" del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Fondamentali fra tali attività correlate alla sicurezza sono quelle connesse al secondo criterio individuato nel Regolamento UE rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento.**

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77 del GDPR); tali impatti dovranno essere analizzati attraverso un apposito **processo di valutazione** (si vedano artt. 35-36 del GDPR) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

All'esito di questa valutazione di impatto il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del

titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

33. TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Si fa rinvio ai principi dettati dal Regolamento Europeo agli articoli 44 e seguenti, nonché alle indicazioni che fossero dettate, in materia, dal Legislatore nazionale e dal Garante per la protezione dei dati personali.

PARTE SESTA: ATTUAZIONE IN AMBITO AZIENDALE DEGLI ADEMPIMENTI EUROPEI

34. ENTRATA IN VIGORE E PUBBLICITA'

Il presente Regolamento entrerà in vigore dalla data di adozione con atto deliberativo del Consiglio di Amministrazione.

Il Regolamento verrà pubblicato sul sito internet dell'Ente ed in Amministrazione Trasparente, nonché sul portale dei dipendenti CBA.

35. DISPOSIZIONE FINALE RELATIVA AGLI 'ALLEGATI TECNICI'

Il testo del presente Regolamento potrà essere aggiornato con atto deliberativo del CdA, a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa, sia nazionale che regionale, in materia di protezione dei dati personali.

Quanto, invece, ai n. [NR] ([NR IN LETTERA) Allegati tecnici al presente Regolamento, si stabilisce quanto segue: poiché si tratta di "strumenti di lavoro quotidiano", essi saranno inevitabilmente oggetto di continue, quanto rapide integrazioni, modifiche e revisioni, in virtù sia delle necessità dell'Ente che delle esigenze imposte da una realtà normativa ed organizzativa tuttora in rapidissima evoluzione.

Gli eventuali aggiornamenti ai *documenti tecnici allegati* verranno, pertanto, inseriti in tempo reale sul portale del personale.

A. REGOLE PER L'ADOZIONE DELLE MISURE DI SICUREZZA

La valutazione delle misure di sicurezza da adottare deve essere vista nel contesto del rischio a cui è rivolta. Pertanto le misure di sicurezza vanno viste nel loro senso più ampio del termine partendo dal principio che l'art. 32 del Regolamento EU recita "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*".

Di seguito vengono riportate ad esempio alcune regole e principi di base per diverse misure di sicurezza che verranno implementate nel tempo.

Misure	Regole / Principi da osservare
Custodia dei dati in armadi blindati e/o ignifughi	E' importante che gli uffici che trattano dati sensibili e giudiziari possano disporre di queste strutture per archiviare in modo consono tali informazioni.
Sistemi UPS e Generatori di corrente che garantiscano la continuità elettrica	Fondamentale a tutela delle attività soprattutto per gli strumenti elettronici. Da adottare necessariamente per tutti i server e per quei pc locali che non archiviano le informazioni sul server. Infatti questi ultimi non hanno delle procedure pianificate di backup e quindi è importante ridurre al minimo i rischi che gli sbalzi di tensione possono provocare sugli hard disk.
Manutenzione programmata degli strumenti	Come tutte le macchine che si rispettano anche il sistema informativo va manutenzionato periodicamente sia attraverso l'aggiornamento dei suoi componenti sia con la pulizia periodica delle macchine stesse.
Presenza di un sistema di autenticazione delle credenziali per tutti gli accessi agli archivi elettronici	Si intende con questa misura l'adozione di un server di dominio che consenta l'autenticazione dell'utente.
Disattivazione delle credenziali di autenticazione nel caso di inutilizzo per 6 mesi	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Aggiornamento periodico di programmi per il controllo della vulnerabilità	E' importante che ogni pc sia periodicamente aggiornato sulle proprie vulnerabilità con gli appositi software.

Istruzioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durante le sessioni di lavoro	E' importante che l'operatore conosca il regolamento per quanto concerne l'assenza dal posto di lavoro con il PC acceso.
Disattivazione delle credenziali di autenticazione in caso di perdita di qualità dell'incarico	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Aggiornamento periodico, con cadenza almeno annuale, della lista degli incaricati e dei profili di autorizzazione	Tutte le persone che operano all'interno degli uffici devono essere autorizzate dal Titolare
Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione	Rientra nel concetto della formazione del personale
Aggiornamento periodico delle credenziali di autenticazione	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Procedure di verifica sull'operato degli incaricati	E' un compito ispettivo che il Responsabile della sicurezza dei dati personali può demandare anche a società esterne
Adozione di procedure per le copie di sicurezza, la loro custodia ed il ripristino della disponibilità dei dati	Il backup deve essere metodico, non affidato alle singole volontà. E' per questo importante nominare l'Incaricato delle copie di sicurezza delle banche dati
Distruzione del cartaceo	E' importante nel limite del possibile incentivare la distruzione del cartaceo rendendolo illeggibile usando dei comodi distruggi documenti
Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati	Il salvataggio dei dati è fondamentale in qualsiasi organizzazione

B. DISCIPLINARE PER L'AUTORIZZATO AL TRATTAMENTO

Per i trattamenti di dati personali gli Autorizzati al trattamento dei dati personali debbono osservare le seguenti disposizioni.

Gli Incaricati del trattamento dei dati personali sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali.

II trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati.

L'Autorizzato al trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente

Ogni Autorizzato al trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

Gli Autorizzati al trattamento dei dati personali che hanno ricevuto le credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.

La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.

La componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'Autorizzato.

L'Autorizzato del trattamento dei dati personali deve modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.

Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

I documenti contenenti dati personali trattati non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.

Per tutto il periodo in cui i documenti contenenti dati personali sono al di fuori dei locali individuati per la loro conservazione, l'Autorizzato del trattamento non dovrà lasciarli mai incustoditi.

L'Autorizzato del trattamento deve inoltre controllare che i documenti contenenti dati personali, composti da numerose pagine o più raccoglitori, siano sempre completi e integri.

Al termine dell'orario di lavoro l'Autorizzato del trattamento deve riportare tutti i documenti contenenti dati personali nei locali individuati per la loro conservazione.

I documenti contenenti dati personali non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.

Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali.

Per evitare il rischio di diffusione dei dati personali si deve limitare l'utilizzo di copie fotostatiche.

Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro Autorizzato debitamente autorizzato.

Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.

È inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.

Documenti contenenti dati personali che, per una qualunque ragione, siano da cestinare, devono assolutamente essere distrutti in modo da risultare illeggibili a soggetti terzi non autorizzati che ne potrebbero entrare in possesso (es. addetti alle pulizie).

Quando i documenti devono essere trasportati essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'Autorizzato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.

L'Autorizzato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.

È proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un autorizzato a potere trattare i dati in questione.

Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.

Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico o aperto al pubblico.

C. PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI – DATA BREACH

Si fa rinvio alle disposizioni di cui alla procedura dell'Ente tempo per tempo vigente, che disciplina la materia di cui si tratta.

D. DISCIPLINA DELL'ENTE SULLA VIDEOSORVEGLIANZA

Si fa rinvio alle disposizioni di cui al *Regolamento dell'Ente* tempo per tempo vigente, che disciplina la materia di cui si tratta.

E. DISCIPLINA DELL'ENTE SULL'UTILIZZO DEI MEZZI INFORMATICI E TELEMATICI

Si fa rinvio alle disposizioni di cui al *Regolamento dell'Ente* tempo per tempo vigente, che disciplina la materia di cui si tratta.