

**REGOLAMENTO AZIENDALE IN MATERIA DI PROTEZIONE DEI
DATI PERSONALI
AZIENDA SANITARIA LOCALE BT**

**Relativo alla protezione ed al trattamento dei dati personali,
nonché alla libera circolazione di tali dati**

COPIA TRATTA DAL SITO WEB ASLBAT.IT

Parte I

Disposizioni generali

Articolo 1 — Oggetto

Il presente regolamento dell'Azienda Sanitaria Locale BT contiene disposizioni organizzative ed attuative del Regolamento UE 2016/679, delle linee guida emanate dal Comitato Europeo per la protezione dei dati, dal vigente D. Lgs. n. 196/03 come modificato dal D.Lgs. 101/2018 e da tutte le pronunce dell'Autorità Garante per la Privacy, nell'ambito delle strutture, servizi e presidi della medesima azienda, con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con la stessa.

Secondo il considerando numero 1 del Regolamento UE 2016/679:

"La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano."

Secondo il considerando numero 2 del Regolamento UE 2016/679:

"I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche."

L'articolo numero 1 del Regolamento UE 2016/679

"... stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati." Il suddetto regolamento inoltre "... protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per

motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali."

L'Azienda Sanitaria Locale BT assicura l'adozione di misure di sicurezza anche preventive idonee ad evitare situazioni di rischio e non conformità o di alterazione di dati.

L'Azienda Sanitaria Locale BT adotta, altresì, le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi degli articoli 12 -23, contenuti nel Capo III del Regolamento UE 2016/679.

Articolo 2 – Definizioni

Dato Personale - dati genetici - dati biometrici – dati relative alla salute – categorie particolari di dati personali

Per **dato personale** ai sensi dell'articolo 4 paragrafo 1 numero 1) del Regolamento Ue 2016/679 si intende: *qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (C26, C27, C30)*

Per **dati genetici** ai sensi dell'articolo 4 paragrafo 1 numero 13) Regolamento Ue 2016/679 si intendono: *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; (C34)*

Per **dati biometrici** ai sensi dell'articolo 4 paragrafo 1 numero 14) Regolamento Ue 2016/679 si intendono: *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; (C51)*

Per **dati relativi alla salute** ai sensi dell'articolo 4 paragrafo 1 numero 15) Regolamento Ue 2016/679 si intendono: *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;* (C35)

Per **categorie particolari di dati personali** ai sensi dell'articolo 9 paragrafo 1 si intendono: *dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale nonché 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.* (C51) Tale trattamento di dati personali è vietato.

Sono previste delle specifiche esenzioni al cennato divieto, infatti i suddetti dati sono trattati principalmente nell'Azienda Sanitaria Locale BT in base al combinato disposto dell'articolo 9 paragrafo 2 lettera h) del Regolamento Ue 2016/679 con l'articolo 9 paragrafo 3 del Regolamento Ue 2016/679 che così recitano: *"lettera h) 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, fatte salve le condizioni e le garanzie di cui al paragrafo 3;* (C53)

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.(C53)".

nonché in base all'articolo 9 paragrafo 2 lettera i) del Regolamento Ue 2016/679 che così recita:

"lettera i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; (C54)".

Articolo 3 – Trattamento dei Dati Personali

Con la definizione “trattamento”, ai sensi dell’articolo 4, paragrafo 1, numero. 2) del Regolamento UE 2016/679 si intende: *“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”*.

Il trattamento dei dati attiene alla responsabilità del Titolare del Trattamento e dell’eventuale contitolare, ove previsto e presente e viene all’uopo delegato ai soggetti autorizzati al trattamento dei dati. Vi sono ipotesi in cui il trattamento dei dati viene, altresì, svolto in nome e per conto del titolare dai Responsabili del Trattamento dei dati.

Parte II I soggetti

Articolo 4 – Titolare del Trattamento dei Dati Personali (Direttore Generale ASL BT)

Il principio cardine introdotto dal Regolamento UE 2016/679 è quello della “responsabilizzazione” (*accountability*) che pone in carico al Titolare del trattamento dei dati l’obbligo di attuare 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*);

Il titolare ha l’obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l’applicazione del Regolamento UE 2016/679.

Il Titolare può scegliere autonomamente il modello organizzativo e gestionale che ritiene più adatto alla propria realtà e dotarsi delle misure di sicurezza che ritiene più efficaci in quanto Egli risponde delle proprie azioni e deve essere in grado, in qualsiasi momento, di darne conto verso l’esterno.

Per **Titolare del Trattamento**, ai sensi dell'articolo 4 paragrafo 1 numero 7 del Regolamento Ue 2016/679 si intende: *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri"*; **(C74)**.

Nel caso di specie il titolare del trattamento è l'Azienda Sanitaria Locale BT legalmente rappresentata dal Direttore Generale pro tempore.

Il Titolare nei casi previsti dal Regolamento UE 2016/679:

- 1) mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento UE 2016/679, così come previsto dall'articolo 24 paragrafo 1 del Regolamento UE 2016/679;
- 2) le misure di cui al punto 1 sono riesaminate e aggiornate qualora necessario, così come previsto dall'articolo 24 paragrafo 1 del Regolamento UE 2016/679;
- 3) determina e provvede all'attuazione di politiche adeguate in materia di protezione dei dati, così come previsto dall'articolo 24 paragrafo 2 del Regolamento UE 2016/679;
- 4) aderisce, ove possibile, ai codici di condotta di cui all'articolo 40 del Regolamento UE 2016/679 o a un meccanismo di certificazione di cui all'articolo 42 del Regolamento UE 2016/679, così come indicato dall'articolo 24 paragrafo 2 del Regolamento UE 2016/679;
- 5) mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione e la minimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, e ad integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti di protezione dei dati fin dalla progettazione del Regolamento UE 2016/679 e tutelare i diritti degli interessati, così come previsto dall'articolo 25 paragrafo 1 del Regolamento UE 2016/679; *(c.d. privacy by design)*;
- 6) mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati e protetti, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un

numero indefinito di persone fisiche senza l'intervento della persona fisica, così come previsto dall'articolo 25 paragrafo 2 del Regolamento UE 2016/679; (*c.d. privacy by default*)

7) nel caso in cui si individui un rapporto di contitolarità del trattamento dei dati, predispone, insieme all'altro contitolare in modo trasparente, un accordo interno, mediante il quale si determinano le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, così come previsto dall'articolo 26 del Regolamento UE 2016/679;

8) qualora un trattamento dei dati debba essere effettuato per suo conto da un soggetto esterno all'azienda, il titolare ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato, così come previsto dall'articolo 28 del Regolamento UE 2016/679;

9) i rapporti di cui al punto precedente tra il titolare del trattamento ed il responsabile esterno del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che indichi la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento, così come previsto dall'articolo 28 del Regolamento UE 2016/679;

10) individua e designa i soggetti interni all'azienda che nell'effettuare il trattamento dei dati personali agiscono sotto la sua autorità, così come previsto dall'articolo 29 del Regolamento UE 2016/679;

11) i soggetti interni individuati e designati come previsto dal punto precedente e che hanno accesso a dati personali non possono trattare tali dati se non istruiti dal titolare del trattamento stesso, così come previsto dall'articolo 29 del Regolamento UE 2016/679;

12) tiene il Registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le informazioni richieste ed indicate dall'articolo 30 del Regolamento UE 2016/679;

- 13) mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio così come previsto dall'articolo 32 del Regolamento UE 2016/679;
- 14) provvede alla notifica di una eventuale violazione dei dati personali all'autorità di controllo se ne ricorrono i presupposti, così come previsto dall'articolo 33 del Regolamento UE 2016/679;
- 15) provvede alla comunicazione di una eventuale violazione dei dati personali all'interessato se ne ricorrono i presupposti, così come previsto dall'articolo 34 del Regolamento UE 2016/679;
- 16) effettua, ove ne ricorrono i presupposti e prima di procedere al trattamento dei dati personali, la valutazione d'impatto sulla protezione dei dati, così come previsto dall'articolo 35 del Regolamento UE 2016/679;
- 17) allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, così come previsto dall'articolo 35 del Regolamento UE 2016/679;
- 18) qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indica che il trattamento presenta un rischio elevato in assenza di misure adottate dal titolare del trattamento, per attenuare il rischio prima di procedere al trattamento, consulta l'autorità di controllo, così come previsto dall'articolo 36 del Regolamento UE 2016/679;
- 19) designa sistematicamente un responsabile della protezione dei dati, così come previsto dall'articolo 37 del Regolamento UE 2016/679;

Articolo 5 — Responsabile della protezione dei dati (RPD) / Data Protection Officer (DPO)

Il titolare del trattamento designa sistematicamente un Responsabile della Protezione dei Dati (RPD) / Data Protection Officer (DPO), così come previsto dall'articolo 37 lettera a) del Regolamento UE 2016/679.

I compiti del Responsabile della Protezione dei Dati (RPD) / Data Protection Officer (DPO), così come previsto dall'articolo 39 del Regolamento UE 2016/679, sono i seguenti:

a) informare e fornire consulenza al titolare del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE

2016/679 nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del Trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo; e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

L'Azienda Sanitaria Locale BT ha designato il Responsabile della Protezione dei Dati (RPD) / Data Protection Officer (DPO) ai sensi dell'art. 37 lettera a) del Regolamento Ue 2016/679, ha pubblicato i suoi dati di contatto sul sito aziendale (Sezione Privacy/DPO) ed ha comunicato la suddetta designazione all'autorità di controllo, così come previsto dall'articolo 37 paragrafo 7 del Regolamento Ue 2016/679.

Altri compiti e funzioni possono essere conferiti al RPD a condizione che il Titolare del trattamento si assicuri che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

Il Titolare assicura che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

A tal fine:

Il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Direttori che abbiano per oggetto questioni inerenti la protezione dei dati personali;

il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

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

il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente che impatti sui dati degli assistiti.

Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili il Responsabile del Trattamento e qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento;

Il RPD non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce esclusivamente e direttamente al Titolare (Direttore Generale Asl BT) nella cui Area di Staff è posizionato funzionalmente ed organicamente.

Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare.

Articolo 6 — Cooperazione con l'autorità di controllo

L'Azienda Sanitaria Locale BT in qualità di Titolare del Trattamento coopera, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti, così come previsto dall'articolo 31 del Regolamento UE 2016/679.

Articolo 7 — Responsabili (esterni all'Azienda) del Trattamento dei dati personali

L'Azienda Sanitaria Locale BT in qualità di Titolare del Trattamento dei Dati individua gli Enti, gli organismi, altri soggetti pubblici o privati esterni all'Azienda nonché quelle strutture accreditate alle quali sono affidate attività o servizi, con esclusivo riferimento alle operazioni di trattamento di dati personali. A tali soggetti viene attribuita la qualità di Responsabile esterno del trattamento dei dati personali ai sensi dell'articolo 28 del Regolamento UE 2016/679.

Agli accordi con le strutture accreditate e nei contratti di affidamento di fornitura o di servizi all'esterno dell'Azienda (outsourcing), nuovi o in essere, dovrà essere allegato un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, mediante il quale si vincola il responsabile del trattamento al titolare del trattamento e si disciplina il trattamento dei dati, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento così come previsto dall'art. 28 del Regolamento UE 2016/679.

Le copie di tali contratti devono essere inviate alla Direzione Generale ed all'Ufficio del RPD.

I responsabili esterni operano nel rispetto del presente regolamento.

Articolo 8 – Designato / Incaricato / Autorizzato al Trattamento sotto l'autorità del Titolare del Trattamento

Ai sensi dell'articolo 29 del Regolamento UE 2016/679 "Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri."

L'Azienda Sanitaria Locale BT in qualità di titolare del Trattamento dei Dati individua i soggetti aziendali che agiscono sotto la sua autorità, che hanno accesso ai dati personali e che trattano tali dati secondo le sue istruzioni.

Per tali ragioni il Titolare (ovvero il suo Designato) del Trattamento abilita i propri collaboratori/dipendenti a trattare i dati mediante l'atto di autorizzazione al trattamento dei dati.

Il trattamento effettuato dal soggetto non autorizzato non è legittimo.

Il Titolare del Trattamento dei dati delibera la designazione dei suddetti soggetti e redige un atto di autorizzazione che contiene l'ambito del trattamento autorizzato e le istruzioni per il trattamento, per l'uso dei dispositivi e le misure di sicurezza da adottare.

La figura dell'Incaricato del trattamento ex art 30 del vecchio codice (D.Lgs. 196/2003) è una figura non presente in nessuna delle altre legislazioni degli Stati membri dell'Unione e non era prevista nemmeno dalla direttiva 95/46/CE del 1995 né dal GDPR.

L'introduzione nella legge italiana della figura autonoma dell'Incaricato (già Responsabile) del trattamento è stata il risultato di una scelta del legislatore e lo stesso Garante ha evidenziato che *"Pur non prevedendo espressamente la **figura dell'Incaricato**" del trattamento (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento)." Ed ancora "Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di Titolari e Responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene che Titolari e Responsabili del trattamento possano mantenere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante".*

Per quanto riguarda la designazione dei soggetti Incaricati (Designati) ed Autorizzati del Trattamento dei Dati, l'Azienda Sanitaria Locale BT ha adottato uno schema in due livelli, un primo livello che risponderà direttamente al Titolare del Trattamento dei Dati comprendente:

- I) figure apicali quali:
 - a) il Direttore Sanitario;
 - b) I direttori di UU.OO.CC. / UU.OO.SS. / UU.OO.SS.VV.DD.;
- II) un secondo livello che risponderà ai soggetti apicali di cui al punto I;

A tutti i dipendenti (compresi co.co.co., tempo determinate, stagisti ecc.) viene inviata, mediante comunicazione, l'autorizzazione al trattamento, nella quale sarà indicato almeno l'ambito del trattamento per il quale sono autorizzati, il profilo utente rispetto alla rete aziendale, e successivamente i corsi di formazione sulla protezione dei dati (il regolamento impone l'obbligo di formazione del personale ex articolo 39 del Regolamento UE 2016/679).

I soggetti di cui al punto I del presente articolo compiono quanto necessario nel rispetto delle vigenti disposizioni in tema di riservatezza; in particolare hanno il dovere di osservare e fare osservare le precauzioni individuate nel piano di sicurezza dei dati personali elaborato dall'Azienda.

I soggetti di cui al punto I sono tenuti a:

- comunicare tempestivamente al Titolare del Trattamento dei Dati tutte le questioni rilevanti ai fini della normativa in materia di protezione dei dati personali;
- comunicare al Titolare del Trattamento dei Dati l'inizio di ogni nuovo trattamento nonché la cessazione o la modifica dei trattamenti già in essere all'interno del proprio settore di competenza, al fine della compilazione ovvero dell'aggiornamento del registro dei trattamenti dei dati personali, nonché per quanto previsto ai sensi dell'articolo 4 ai numeri 6) e 7).

Articolo 9 — Criteri per l'individuazione dei soggetti apicali

I soggetti apicali designati ovvero incaricati del Trattamento sotto l'autorità del Titolare, così come definiti ed indicati nell'articolo 8 del presente regolamento, sono individuati fra i soggetti che per competenza ed esperienza, forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Articolo 10 — Nomina dei soggetti Designati / Incaricati (già Responsabili) del Trattamento

L'elenco dei soggetti apicali Designati/Incaricati (già Responsabili) è contenuto nelle delibere n. 522 del 28.03.2019 e 695 del 24.04.2019.

La nomina degli altri soggetti sarà effettuata con atto proprio del Titolare ovvero con atto deliberativo, e successive comunicazioni scritte.

L'atto di incarico/autorizzazione al trattamento dei dati dovrà essere comunicato per iscritto ai soggetti individuati.

Articolo 11 — Nomina dei soggetti autorizzati al Trattamento sotto l'autorità del Titolare del Trattamento ovvero delle altre figure apicali

I soggetti autorizzati sono identificati dal Titolare ovvero dai soggetti apicali designati/incaricati, sotto la loro autorità, in tutti coloro che sono autorizzati ad effettuare operazioni di trattamento dei dati nell'ambito delle attività lavorative svolte in azienda.

Essi, in relazione alle funzioni loro assegnate, devono avere accesso ai soli dati la cui conoscenza sia strettamente necessaria al trattamento.

Gli autorizzati semplici devono eseguire i trattamenti nel rispetto delle procedure e secondo le disposizioni date dal soggetto che autorizza al Trattamento, sotto l'autorità del Titolare ovvero del diretto superiore delegato, con nomina per iscritto.

Articolo 12 – Criteri per l'esecuzione del trattamento dei dati personali

L'Azienda 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 come previsto dall'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea.

L'Azienda Sanitaria Locale BT 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 all'utenza. A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di protezione dati, è l'attività formativa del personale aziendale e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Azienda, per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento europeo, e di conseguenza dal presente nuovo Regolamento aziendale.

Parte III

Articolo 13 – Il registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (come previsto dall'articolo 30, paragrafo 5 del Regolamento UE 2016/679), 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'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro, in virtù delle dimensioni e della complessità che caratterizzano questa Azienda Sanitaria Locale BT, non può che avere forma elettronica.

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

Per tali spiegate ragioni ed in ottemperanza ai principi previsti dal Regolamento UE 2016/679 l'Azienda Sanitaria Locale BT si è determinata alla realizzazione di tale registro dei trattamenti in formato elettronico.

Per la compilazione del suddetto registro l'Azienda ha realizzato un censimento dei trattamenti dei dati personali e/o sensibili (anagrafe).

Il Registro è tenuto a cura del Titolare, in collaborazione con i soggetti apicali e vi sovrintende il Responsabile della Protezione dei Dati; esso viene aggiornato qualora vengano comunicati da parte del Titolare o dei Responsabili del Trattamento nonché dei soggetti apicali autorizzati al trattamento casi di attivazione, cessazione o modifica di nuovi trattamenti.

Parte IV

L'interessato

Articolo 14 — Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

Come stabilito dall'articolo 13 del Regolamento UE 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.

L'informativa rappresenta l'elemento propedeutico al trattamento dei dati in quanto garantisce l'evidenza e la trasparenza delle attività di trattamento che vengono poste in essere.

Le predette informative vengono rese agli interessati anche tramite la pubblicazione sul sito aziendale nonché anche tramite l'affissione a stampa nei locali di accesso all'utenza e del personale aziendale.

Articolo 15 – Diritti dell'interessato

Secondo quanto disposto dal paragrafo III del Regolamento UE 2016/679 all'interessato vengono riconosciuti i seguenti diritti:

- a) il diritto di accesso dell'interessato (articolo 15 Considerando 63 e Considerando 64);
- b) il diritto di rettifica (articolo 16 Considerando 65);
- c) il diritto alla cancellazione (c.d. "diritto all'oblio" articolo 17 Considerando 65 e Considerando 66);
- d) il diritto di limitazione di trattamento (articolo 18 Considerando 67);
- e) il diritto alla portabilità dei dati (articolo 20 Considerando 68);
- f) il diritto di opposizione (articolo 21 Considerando 69 e Considerando 70);

a) diritto di accesso dell'interessato

Come stabilito dall'articolo 15 del Regolamento UE 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: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) 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; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) 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; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) 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 del Regolamento UE 2016/679 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.

Si fa espresso rinvio, in particolare, alle vigenti disposizioni normative in materia di "accesso documentale", di "accesso civico" e di "accesso generalizzato".

A tale riguardo, nel rinviare a quanto pubblicato al sito web aziendale, si fa presente che:

a) per accesso documentale si intende la domanda di accesso (richiesta di presa visione o di rilascio copia) a deliberare e provvedimenti dell'Azienda, 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 rivolgersi all'U.R.P., portando con sé il proprio documento di identità valido. I costi di ricerca, visura e riproduzione fotostatica, e le spese di spedizione, sono quelle previste dal tariffario aziendale approvato con deliberazione n. 1217 del 20/11/2006, cui si rimanda integralmente. 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 all'URP in carta semplice, ovvero a mezzo pec all'indirizzo del protocollo aziendale. L'Azienda, 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'Azienda 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 aziendale) 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 all'URP senza necessità di formule sacramentali, ovvero a mezzo pec all'indirizzo aziendale. 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 controinteressati. 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 aziendale nel rispetto della normativa vigente, l'Azienda 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.

b) Diritto di rettifica

Come stabilito dall'articolo 16 del Regolamento UE 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.

c) Diritto alla cancellazione "diritto all'oblio"

Come stabilito dall'articolo 17 del Regolamento UE 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).

d) Diritto alla limitazione al trattamento

Come previsto dall'articolo 18 del Regolamento UE 2016/679 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 successivo punto f) 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.

e) Diritto alla portabilità dei dati

Come previsto dall'articolo 20 del Regolamento UE 2016/679. 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.

f) Diritto di opposizione

Come stabilito dall'articolo 21 del Regolamento UE. 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.

g) Processo decisionale automatizzato (Profilazione)

Come stabilito dall'articolo 22 del Regolamento UE 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 responsabile 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 VI

Sicurezza

Articolo 14 — Amministratori di Sistema

II Titolare e gli altri soggetti delegati al Trattamento per i quali si prevede l'utilizzo di apparecchiature informatiche si avvalgono, nella individuazione e applicazione delle misure necessarie a garantire la sicurezza del sistema, di amministratori di sistema formalmente individuati a tale scopo dal Responsabile del Servizio Sistema Informativo Aziendale ai sensi del D.P.R. 318/99 e ss mm e ii, nominato con apposito atto interno.

Articolo 15 — Sicurezza degli archivi cartacei

L'accesso agli archivi aziendali deve essere controllato, e devono essere identificati, autorizzati e registrati i soggetti.

Con riferimento agli archivi aziendali la cura della conservazione e sicurezza dei medesimi spetta al responsabile competente per i dati oggetto del trattamento.

Gli archivi delle cartelle cliniche prodotte in ambito ospedaliero sono sotto la responsabilità:

del Direttore della U.O. (o del modulo dipartimentale) dal momento della formazione della cartella e per tutto il periodo di conservazione della medesima presso il reparto;

del Direttore del Presidio Ospedaliero dal momento in cui la cartella perviene alla Direzione Sanitaria da parte del Direttore della U.O. e sino al materiale conferimento alla società che ne cura l'archiviazione;

per le cartelle cliniche e la documentazione equipollente giacente presso strutture non ospedaliere (Distretti) la responsabilità farà capo al Direttore della Struttura ove i medesimi atti sono materialmente conservati;

Dal momento in cui la documentazione viene consegnata alla società convenzionata per l'archiviazione, il legale rappresentante della medesima è responsabile della conservazione e della sicurezza;

Il contratto di affidamento del servizio è aggiornato con previsione di apposita clausola di garanzia che preveda la possibilità per l'Azienda di accedere ai locali per verificare il rispetto alle prescrizioni della legge in materia di riservatezza e del presente regolamento.

Articolo 16 — Misure di sicurezza fisiche

Gli archivi cartacei devono essere situati in locali non esposti a rischi ambientali (quali allagamenti, incendi, deterioramenti di varia natura etc.), anche in ossequio alle disposizioni in materia di sicurezza di cui D.Lgs. 81/08 e successive modificazioni ed integrazioni.

E' opportuno che venga predisposto un piano periodico aziendale per la conservazione e lo scarto dei documenti, in conformità alla vigente normativa nazionale in tema di conservazione di documenti. A tal fine, partendo dalla rilevazione dei trattamenti di dati ai sensi del D.lgs 196/2003, le singole strutture operative aziendali sono tenute a segnalare al Referente Aziendale per la Privacy la tipologia, l'ubicazione, il metodo di catalogazione e di custodia, la quantità approssimativa e l'anno di riferimento della documentazione custodita ai fini dell'aggiornamento del censimento dei trattamenti di dati personali e/o sensibili.

Per la documentazione riguardante dati personali sensibili e non, è opportuno che ciascun presidio/edificio aziendale si doti di un proprio archivio centralizzato munito di misure di sicurezza (meccanismi di chiusura dei locali e dei contenitori, sistemi di allarme a protezione dei locali, etc.) idonee a garantire l'inaccessibilità ai locali stessi da parte di soggetti non autorizzati. Per quanto concerne specificatamente la documentazione sanitaria ed in particolare le cartelle cliniche, per le modalità di tenuta, archiviazione e rilascio copia l'Azienda dovrà attenersi alla normativa vigente, prestando particolare attenzione a quanto stabilito nell'Articolo 92 del D. Lgs.196/2003.

Articolo 17 – Misure di sicurezza logiche

L'Azienda è tenuta ad impartire ai dipendenti che, in ragione delle loro mansioni si trovino ad utilizzare dati personali sensibili e non, adeguate raccomandazioni al fine di una doverosa responsabilizzazione dei soggetti stessi, in particolare per ciò che concerne la conservazione della documentazione cartacea onde evitare accessi non autorizzati perdita smarrimento o distruzione dei dati stessi.

Ricordando che la circolazione infrazionale dei dati, in particolar modo di quelli sensibili, non può eccedere quanto necessario per il puntuale svolgimento dei compiti istituzionali, l'Azienda raccomanda di adottare modalità e accorgimenti tali da garantire il massimo rispetto della normativa vigente soprattutto in relazione ai provvedimenti amministrativi, in particolare delibere e determine dirigenziali, in

special modo nella fase di pubblicazione e di rilascio di copie ai sensi della L. 241/90 e s.m.i..

La sicurezza dei dati assicurata con le modalità qui disposte deve essere garantita anche per i dati trattati da personale non dipendente dell'Azienda, nonché da personale dipendente che svolge attività libero-professionale intramuraria nei casi in cui questa si svolga presso le strutture aziendali o comunque in locali messi a disposizione dell'Azienda.

Articolo 18 — Misure di sicurezza informatiche

Si distinguono le seguenti tipologie di trattamento dei dati informatici:

a) Trattamento dei dati su personal computer:

Ciascun dipendente è responsabile del personal computer assegnato; l'Azienda anche con delega alle UU.OO. autorizzate ai trattamenti; indicherà idonee procedure di salvataggio periodico degli archivi e l'attivazione di antivirus, tenendo sempre presente le misure adeguate di sicurezza previste dal Regolamento UE 2016/679;

b) Trattamento dei dati all'interno di procedure in rete:

le apparecchiature informatiche devono essere collocate in locali non esposti a rischi ambientali (allagamenti, incendi, deterioramenti di varia natura...), anche in conformità alle disposizioni in materia di sicurezza di cui al D.Lgs. 81/2008;

I server sono posti sotto gruppo di continuità, onde evitare sbalzi o cadute di tensione che potrebbero danneggiare i dispositivi fisici delle macchine e quindi dei dati; deve essere previsto un sistema di salvataggio periodico sul data-base aziendale;

è opportuno che vengano previste modalità di autenticazione per l'accesso;

l'Azienda è tenuta a realizzare una propria rete che si interfacci verso l'esterno in maniera controllata e garantita da appositi meccanismi di difesa (proxy-server antivirus e firewall).

c) Accessi ai dati

Gli accessi vengono gestiti mediante credenziali personali:

1) Profili utenti

i profili utenti assegnati rispecchiano compiti e mansioni assegnate.

Si raccomanda ai dipendenti il buon uso del proprio Sistema di lavoro che non dovrà mai essere utilizzato per fini personali.

2) Password

La password di accesso alla postazione di lavoro nonché quelle di accesso agli applicative aziendali sono strettamente personali.

3) Logistica e software

È vietata qualsivoglia modifica logistica ed al software. Per fare ciò è necessario contattare il servizio all'uopo incaricato dall'azienda.

4) Disattivazione dell'utenza

In caso di sospensione e/o cessazione dal rapporto di lavoro il servizio incaricato tramite la struttura CED provvederà ad annullare il relativo profilo utente e la password.

Articolo 19 – Videosorveglianza

L'Azienda disciplina l'attività di videosorveglianza finalizzata alla sicurezza degli utilizzatori, utenti o dipendenti, delle strutture aziendali, nonché alla tutela del patrimonio aziendale nel pieno rispetto della normativa vigente.

Non rientra nel campo di questa attività l'utilizzo di apparecchiature strumentali per la rilevazione ed il monitoraggio dei parametri vitali dei pazienti né l'attività di controllo a distanza dei lavoratori.

L'Azienda adotterà una specifica regolamentazione atta a garantire il rispetto della normativa in tema di riservatezza dei dati personali nonché di tutela del lavoratore dipendente (Legge n. 300/70), nonché l'attivazione di trattamenti di dati con modalità particolari tali da coinvolgere anche informazioni relative al personale dipendente (quali videosorveglianza, monitoraggio della posta elettronica e degli accessi a Internet etc.).

Articolo 20 – Valutazione di Impatto

Nel caso in cui un tipo di trattamento, specie se preveda in particolare l'uso di nuove tecnologie, presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (VIP - valutazione d'impatto sulla protezione dei dati personali) ai sensi dell'art. 35 GDPR.

La VIP è effettuata in presenza di un rischio elevato per i diritti la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La VIP è una procedura che permette di realizzare e dimostrare la conformità alle norme

del trattamento di cui trattasi.

Ai fini della decisione di effettuare o meno la VIP si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3 del GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

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

o organizzative;

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

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

2. Il Titolare garantisce l'effettuazione della VIP ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della VIP ad un altro soggetto, interno o Esterno all'organizzazione. Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la VIP; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della VIP. Il RPD monitora lo svolgimento della VIP. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della VIP fornendo ogni informazione necessaria. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della VIP.

3. Il RPD può proporre lo svolgimento di una VIP in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una VIP in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

4. La VIP non è necessaria nei casi seguenti:

A - se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, del GDPR;

B - se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una VIP. In questo caso si possono utilizzare i risultati della VIP svolta per l'analogo trattamento;

C - se il trattamento è stato sottoposto a verifica da parte dell'Autorità Garante prima del maggio 2018, in condizioni specifiche che non hanno subito modifiche;

D - se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento ed sia stata condotta una VIP all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una VIP per quei trattamenti che siano già stati oggetto di verifica preliminare da parte dell'Autorità Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica.

5. La VIP è condotta prima di dar luogo al trattamento, attraverso la descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati.

Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali;

valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- a) delle finalità specifiche, esplicite e legittime;
- b) della liceità del trattamento;
- c) dei dati adeguati, pertinenti e limitati a quanto necessario;
- d) del periodo limitato di conservazione;
- e) delle informazioni fornite agli interessati;
- f) del diritto di accesso e portabilità dei dati;
- g) del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- h) dei rapporti con i soggetti delegati al trattamento;
- i) delle garanzie per i trasferimenti internazionali di dati;
- l) consultazione preventiva dell'Autorità Garante;
- m) valutazione dei rischi per i diritti e le libertà degli interessati, valutando in particolare la probabilità e la gravità dei rischi rilevati.
- n) Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati);
- o) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Titolare può raccogliere le opinioni degli interessati o dei loro delegati, se gli stessi possano essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

Il Titolare deve consultare l'Autorità Garante prima di procedere al trattamento se le risultanze della VIP condotta indicano l'esistenza di un rischio residuale elevato.

Il Titolare consulta l'Autorità Garante anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

La VIP deve essere effettuata, con eventuale riesame delle valutazioni condotte, anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

ART. 21 - VIOLAZIONE DEI DATI PERSONALI

Per violazione dei dati personali (in seguito "**data breach**") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dalla "ASL BT".

1) In caso di violazione dei dati personali, il Titolare del Trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore è corredata dei motivi del ritardo.

2) Ciascun "Delegato o Responsabile del Trattamento dei dati" informa il Titolare del Trattamento, anche per il tramite del Responsabile della protezione dei dati, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

La notifica deve almeno:

- a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- c) descrivere le probabili conseguenze della violazione dei dati personali;
- d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il Titolare, con il supporto del Responsabile della Protezione dei Dati, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

A tal fine è reso disponibile un modello per la segnalazione interna di eventuali violazioni da trasmettere al Responsabile della Protezione dei Dati allegato allo specifico Regolamento Aziendale Data Breach.

La notifica formale è effettuata dal Titolare, ove ritenuta necessaria, tramite posta elettronica certificata con l'invio del modello per la segnalazione predisposto dal Garante, all'indirizzo email **databreach.pa@pec.gpdp.it**.

e) Quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le seguenti informazioni:

- la natura della violazione dei dati

- i dati di contatto del Responsabile della protezione dei dati
- le possibili conseguenze della violazione
- le misure adottate o di cui si propone l'adozione per porvi rimedio.

Non è richiesta la comunicazione all' interessato se sia soddisfatta una delle seguenti condizioni:

- a) il Titolare del Trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- b) 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;
- c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
- f) Nel caso in cui il Titolare del Trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui sopra è soddisfatta.
- g) Nel caso di violazione dei dati personali il Titolare del Trattamento procede con una valutazione complessiva dell'impatto sui diritti e libertà degli interessati in considerazione della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento.
- h) I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle

loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

i) Il Titolare, con il supporto del Responsabile della Protezione dei Dati, verifica se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali ed informa tempestivamente il Garante e l'interessato, se del caso.

j) A seguito della valutazione preliminare della violazione, il Titolare del trattamento con il supporto del Responsabile della Protezione dei Dati, adotta una le seguenti azioni:

a) se dalla violazione risulta probabile che possano derivare rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del *data breach* al Garante, ai sensi dell'art. 33 del Regolamento UE 2016/ 679;

b) se dalla violazione risulta probabile che possano derivare elevati rischi per i diritti e le libertà degli interessati, il Titolare procede con la notifica del *data -breach* al Garante, ai sensi dell' art. 33 del Regolamento UE 2016/679 e alla comunicazione della violazione ai soggetti interessati ai sensi dell'art. 34 del Regolamento UE 2016/ 679;

c) ove non risulti probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, il Titolare del trattamento non procede con le notifiche e comunicazioni di cui ai punti a) e b).

Pertanto, il Titolare del Trattamento è esentato dalla notifica della violazione solo se è in grado di dimostrare al Garante che il data-breach

non presenti rischi per i diritti e le libertà fondamentali delle persone fisiche interessate.

k) Ogni "Delegato o Responsabile al trattamento dei dati" (ciascun Dirigente/Direttore), per ambito di competenza, ha l'obbligo di segnalare senza ingiustificato ritardo, entro 24 ore, la violazione dei dati rilevata ai soggetti di seguito elencati:

- **Direttore Generale**
- **Responsabile della Protezione dei Dati**

La segnalazione, in prima istanza, può essere effettuata in qualsiasi forma, anche per le vie brevi e successivamente formalizzata tramite invio di posta elettronica o atto interno a mezzo del Sistema di protocollo aziendale.

Ai fini dell'osservanza dei tempi imposti dal Regolamento Ue 2016/679, il Titolare del trattamento dei dati, provvederà a convocare, non oltre 24 ore dalla rilevazione della violazione, una riunione con i soggetti di seguito elencati:

- Direttore Amministrativo
- Direttore Sanitario
- Responsabile della Protezione dei Dati
- Responsabile della Area Tecnica Aziendale
- Responsabile della Struttura interessata dalla violazione

Il Responsabile della Protezione dei Dati ha facoltà di convocare altri soggetti ritenuti necessari per la valutazione della gravità della violazione dei dati.

Il Responsabile della Protezione dei Dati è tenuto a documentare l'intera attività istruttoria, acquisendo tutte le informazioni necessarie per la registrazione dell'evento e per la notificazione al Garante, ove necessario.

A conclusione della valutazione della violazione, il Responsabile della Protezione dei Dati predispone un verbale, sottoscritto da tutti i convenuti e protocollato, che sarà inoltrato al Titolare del trattamento per i conseguenti adempimenti.

l) Il Titolare del Trattamento documenta le violazioni dei dati in apposito registro elettronico da esibire in caso di accertamento ispettivo dell'Autorità. Il registro delle violazioni è custodito dal Responsabile della Protezione dei Dati con la massima diligenza e nell'osservanza del Regolamento UE 2016/ 679.

m) Qualora l'interessato ritenga che siano stati violati i diritti di cui gode a

norma del Regolamento UE 2016/ 679, ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, costituiti in conformità del diritto di uno Stato membro, con obiettivi statuari di pubblico interesse, e che siano attivi nel settore della protezione dei dati personali, per proporre reclamo per suo conto al Garante, esercitare il diritto a un ricorso giurisdizionale per conto degli interessati o esercitare il diritto di ottenere il risarcimento del danno per conto degli interessati se quest'ultimo è previsto dal diritto degli Stati membri.

Il Titolare del Trattamento o il Responsabile del Trattamento è tenuto a risarcire i danni cagionati ad una persona da un trattamento non conforme al Regolamento UE 2016/ 679 ma è esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Articolo 22 — Norma di rinvio

Per quanto non espressamente disciplinato dal presente Regolamento si rimanda al Regolamento UE 2016/679 nonché quanto previsto dal D. Lgs. 196/03 e successive modificazioni ed integrazioni.

Si propone per l'approvazione in data 18.07.2019