ASLGallura
Azienda socio-sanitaria locale

Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali in conformità alla disciplina di cui al Regolamento UE 2016/679

Approvato con Delibera del Direttore Generale n. del

SOMMARIO

INTRODUZIONE

Il 27 aprile 2016 è stato approvato il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, con abrogazione della direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

Il nuovo regolamento UE, obbligatorio in tutti i suoi elementi e direttamente applicabile a ciascuno degli Stati membri a decorrere dal 25 maggio 2018, si fonda sul principio in forza del quale, la protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, è un diritto fondamentale come previsto dall'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea ("Carta") e dall'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione Europea ("TFUE") che stabiliscono che "*ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*".

La principale novità introdotta dal Regolamento UE riguarda il nuovo approccio al rischio basato sul concetto di *accountability* ovvero sul c.d. "principio di responsabilizzazione"; grava sul Titolare del trattamento dei dati personali l'obbligo di valutare le misure tecniche ed organizzative da adottare sulla base della natura dei dati, dell'oggetto, delle finalità del trattamento.

Tra i criteri che i Titolari ed i Responsabili sono tenuti ad utilizzare nella gestione degli obblighi vi sono, in primo luogo, il criterio del "*data protection by default and by design*", ossia la necessità di configurare fin dalla progettazione ed in modo predefinito la tutela dei dati personali prevedendo fin dall'inizio l'adozione di misure idonee per garantire un livello di sicurezza adeguato al rischio e per tutelare i diritti degli interessati.

È posto in capo al Titolare ed al Responsabile del trattamento l'obbligo di valutare il rischio di impatti negativi sulle libertà e sui diritti degli interessati, impatti che devono essere analizzati attraverso un apposito processo di valutazione, tenendo conto del contesto complessivo nel quale il trattamento si colloca e dei rischi per i diritti e per le libertà degli interessati.

Ne consegue che l'intervento dell'Autorità di controllo, nel nuovo impianto gestionale, è destinato a svolgersi principalmente "*ex post*", ossia a collocarsi, sul piano cronologico, in un momento successivo rispetto alle scelte ed alle determinazioni assunte autonomamente dal Titolare e dal Responsabile[1].

[1] A partire dal 25 maggio 2018 sono stati aboliti alcuni istituti previsti dalla direttiva del 1995 e dal D. Lgs. 196/03, come la notifica preventiva dei trattamenti all'Autorità di controllo e la verifica preliminare, sostituiti da obblighi di

CAPO I - DISPOSIZIONI GENERALI

Art. 1 - Oggetto

1. Il presente Regolamento ha per oggetto le misure procedimentali e le regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (*General Data Protection Regulation* del 27 aprile 2016 n. 679), di seguito indicato con "RGPD", relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione dei dati trattati dalla ASL Gallura quale Titolare del Trattamento.

Art. 2 - Quadro normativo di riferimento

1. Il presente Regolamento tiene conto dei seguenti documenti:

- RGPD UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Codice in materia di dati personali (D. Lgs. n.196/2003) così come riformato dal D. Lgs. n. 101/2018;
- Linee guida, Provvedimenti e Raccomandazioni del Garante per la protezione dei dati personali;
- Linee guida sui responsabili della protezione dei dati (DPO) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico Titolare o Responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;

tenuta di un registro dei trattamenti da parte del Titolare/Responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia

- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e profilazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (*data breach notification*) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Linee Guida 07/2020 adottate in data 02 settembre 2020 dal Comitato Europeo per la protezione dei dati le sui concetti di "*Controller*" e "*Processor*" equivalenti rispettivamente al Titolare del trattamento ed al Responsabile del trattamento dei dati;
- L. 241/90 e ssmmii;
- D. Lgs. 33/2013 e ss.mm.ii.

Art. 3 - Definizioni

1. Il presente Regolamento utilizza le seguenti definizioni ai sensi dell'art. 4 RGPD:

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

«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;

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

«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;

«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;

«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;

«Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

«**Dirigente Designato allo svolgimento di specifici compiti e funzioni connessi al trattamento»:** la persona fisica espressamente designata che, sotto la responsabilità del Titolare e nell'ambito della propria struttura organizzativa, svolge specifici compiti e funzioni connessi al trattamento dei dati personali;

«**Autorizzato al trattamento**»: la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del Titolare, individuato con provvedimento del dirigente designato allo svolgimento di specifici compiti e funzioni connessi al trattamento;

«Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

«**Interessato**»: la persona fisica cui si riferiscono i dati personali oggetto di trattamento;

«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;

«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;

«**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;

«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;

«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;

«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;

«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;

«Autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del RGPD;

«Autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto

- il Titolare del trattamento o il Responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
- gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;
- oppure un reclamo è stato proposto a tale autorità di controllo.

2. Ai sensi dell'art. 2-*ter*, comma 4, D. Lgs. 196/03 e ss.mm.ii, si intende per:

«comunicazione»: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-*quaterdecies*, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

«diffusione»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Art. 4 - Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorra almeno una delle seguenti condizioni:

a) 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;

b) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

c) 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;

d) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;

e) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

2. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri, al fine di verificarne la liceità, il Titolare tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9 del RGPD, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del medesimo RGPD;

d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Art. 5 - Trattamento di categorie particolari di dati personali di cui all'art. 9 RGPD

1. In ossequio alla previsione di cui all'art. 9, paragrafo 1, RGPD, rientrano nella nozione di "categorie particolari di dati personali", i dati idonei a rivelare: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. È vietato trattare i dati di cui al precedente comma a meno che non si verifichi uno dei seguenti casi:

a) il trattamento è necessario per motivi di interesse pubblico rilevante previsti dal diritto dell'Unione o nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Ai sensi dell'art. 2-*sexies*, comma 2, D. Lgs. 196/03 e ss.mm.ii., si considera rilevante l'interesse pubblico relativo a trattamenti effettuati dalla ASL Gallura nelle seguenti materie:

- accesso a documenti amministrativi e accesso civico;
- esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;
- attività di controllo e ispettive;
- concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni (n.a.)
- rapporti tra i soggetti pubblici e gli enti del terzo settore;
- obiezione di coscienza;
- attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- attività socioassistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
- attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonchè alle trasfusioni di sangue umano;
- compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonche' compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
- programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;

- vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
- tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;
- istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
- trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché' per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);
- instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva;
- per i dati genetici, biometrici e relativi alla salute il trattamento avviene comunque nel rispetto di quanto previsto dall'articolo 2-*septies*, D. Lgs. 196/03

b) L'interessato ha prestato il proprio consenso esplicito al trattamento di tali categorie particolari di dati personali per una o più finalità specifiche.
c) Il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.
d) Il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato.
e) Il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.
f) Il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro e per la valutazione della capacità lavorativa del dipendente.
g) Il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, sulla base del diritto dell'Unione o nazionale, che è

proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Art. 6 - Trattamento di dati personali relativi a condanne penali e reati di cui all'art. 10 RGPD

1. In ossequio alla previsione di cui all'art. 10 RGPD, rientrano nella nozione di "dati personali relativi a condanne penali e reati", i dati personali relativi alle condanne penali, ai reati o alle connesse misure di sicurezza.
2. Fatto salvo quanto previsto dal decreto legislativo 18 maggio 2018, n. 51, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza che non avviene sotto il controllo dell'autorità pubblica, è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati.
3. Il trattamento dei dati di cui al precedente comma è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, nei casi di seguito elencati:

a) l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi;

b) la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;

c) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;

e) l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto.

CAPO II - SOGGETTI DEL TRATTAMENTO

Art. 7 - Titolare del Trattamento

1. Il Titolare del trattamento dei dati è la Azienda sociosanitaria locale n. della Gallura (ASL Gallura), nel suo complesso, che ha sede in via Bazzoni Sircana 2/2A - 07026 – in Olbia, in ossequio alla previsione di cui all'art. 4, Paragrafo 1, n. 7, RGPD.

2. La ASL Gallura agisce per mezzo del suo legale rappresentante individuato nel Direttore Generale.
3. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; aggiornamento e limitazione della conservazione; integrità e riservatezza.
4. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali venga effettuato in modo conforme al RGPD, con particolare riferimento all'adozione delle misure di sicurezza di cui all'art. 32 RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD.
5. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa, di bilancio, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
6. Il Titolare adotta misure appropriate per fornire all'interessato le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato e le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.
7. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare effettua una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35 RGDP, in ragione della natura, dell'oggetto, del contesto e delle finalità del medesimo trattamento, sulla base dell'elenco delle tipologie di trattamento da sottoporre a valutazione di impatto redatto dal Garante per la protezione dei dati personali.
8. Il Titolare, prima di procedere al trattamento, qualora la richiamata valutazione di impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio, consulta preventivamente il Garante per la protezione dei dati personali in ossequio alla previsione di cui all'art. 36 RGPD.
9. Il Titolare provvede:

a) a definire gli obiettivi strategici per la protezione dei dati personali oggetto di trattamento, provvedendo all'inserimento di tali obiettivi strategici nei documenti di programmazione e pianificazione della ASL Gallura affinché sia garantita l'adozione delle necessarie ed idonee misure tecniche e organizzative atte a garantire che il trattamento sia effettuato conformemente al Codice, al RGPD e al presente Regolamento;
b) in ossequio alle previsioni di cui all'art. 29 RGPD ed all'art. 2-*quaterdecies*, comma 1, D. Lgs. 196/03 a designare ciascun dirigente al quale sia assegnata la responsabilità di uno dei dipartimenti/strutture/UO nelle quali si articoli l'organizzazione della ASL Gallura, quali persone fisiche destinatarie di specifici compiti connessi al trattamento dei dati, attribuendo loro i compiti e le funzioni di cui al successivo art. 8;
c) a nominare, con proprio atto, il Responsabile della Protezione dei Dati (DPO);
d) a notificare al Garante per la protezione dei dati personali la violazione dei dati che rappresenti un rischio per i diritti e le libertà degli interessati, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza ai sensi del disposto di cui all'art. 33 RGPD;
e) a comunicare all'interessato, senza ingiustificato ritardo, la violazione dei dati personali suscettibile di presentare un rischio elevato per i diritti e le libertà dello stesso interessato in conformità alle previsioni di cui all'art. 34 RGPD;
f) ad assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.

10. Nel caso di esercizio associato di funzioni e servizi che comportino il trattamento di dati personali, nonché nel caso in cui la gestione di funzioni o servizi sia affidata alla ASL Gallura da parte di altre Amministrazioni ed organismi statali o regionali, allorché due o più Titolari determinano congiuntamente le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. In questi casi, i contitolari determinano in modo trasparente, mediante un accordo interno, le responsabilità di ciascuno in merito all'osservanza degli obblighi in materia di tutela del diritto alla riservatezza, con particolare riferimento all'esercizio dei diritti dell'interessato, e alle rispettive funzioni in relazione agli obblighi di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD. Il richiamato accordo, il cui contenuto essenziale è messo a disposizione degli interessati, disciplina adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati; esso può individuare uno degli Enti contitolari del trattamento quale punto di contatto per gli interessati.

Art. 8 – Attribuzione di specifici compiti e funzioni connessi al trattamento dei dati in capo al Dirigente

1. Ciascun dirigente al quale sia assegnata la responsabilità di uno dei dipartimenti/strutture/UO è, con provvedimento del Direttore Generale, designato allo svolgimento di specifici compiti connessi al trattamento dei dati personali in conformità alle previsioni di cui all'art. 2-*quaterdecies,* comma 1, del D. Lgs. n. 196/2003.
2. Detti dirigenti, destinatari del provvedimento di designazione, assumono tutti gli obblighi, le responsabilità ed i poteri funzionali a garantire la correttezza e la conformità dei trattamenti alle prescrizioni di cui al RGPD in relazione ad ogni singola fase del trattamento, agli obblighi di 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, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, al fornire istruzioni alle persone autorizzate al trattamento in ossequio alle previsioni di cui all'art. 29 RGPD e all'art. 2-*quaterdecies*, comma 2, D. Lgs. 196/03 e ss.mm.ii.;
3. Con il provvedimento di nomina ai medesimi sono, pertanto, specificatamente attribuiti i seguenti compiti e funzioni:
   a) individuare nominativamente ed autorizzare al trattamento dei dati le persone che nell'ambito del Settore/Area/Ufficio/Servizio di competenza siano preposte ad attività di trattamento sotto l'autorità diretta del titolare, a ciò provvedendo con propria determinazione, attivandosi affinché siano impartite loro apposite istruzioni organizzative ed operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29 RGPD e art. 2–quaterdecies, comma 2, D. Lgs. 196/03;
   b) garantire che dette persone autorizzate siano opportunamente istruite e formate al trattamento con riferimento alla tutela del diritto protezione dei dati nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati, in conformità alle previsioni di cui all'art. 32, paragrafo 4 del RGPD;
   c) nominare i Responsabili del trattamento in tutti i casi in cui si faccia ricorso a soggetti esterni, persone fisiche o giuridiche, mediante affidamento di contratti di appalto relativi a lavori, servizi, forniture o consulenze che abbiano ad oggetto o comportino attività di trattamento di dati per conto della ASL Gallura. Il medesimo provvedimento

di nomina andrà adottato nei confronti di autorità pubblica, servizio o organismo che tratti dati personali per conto del titolare del trattamento. I trattamenti da parte dei Responsabili sono disciplinati mediante contratto ovvero altro atto giuridico che vincoli il Responsabile del trattamento al Titolare del trattamento ai sensi dell'art. 28 RGPD, redatto dal dirigente affidante;

d) rendere l'informativa agli interessati ai sensi degli artt. 12 e ss. RGPD, anche mediante adeguamento puntuale e tempestivo della modulistica resa disponibile dalla ASL Gallura. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato;
e) verificare e controllare che, nell'ambito dell'Area/Settore di competenza, il trattamento dei dati sia effettuato nel rispetto dei principi di cui all'art. 5 del RGPD e, in particolare, assicurare che i dati personali siano trattati in modo lecito, corretto e trasparente;
f) garantire, in caso di raccolta, che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;
g) assicurare che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
h) adottare, tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, tutte le misure tecniche ed organizzative, ivi comprese la pseudonimizzazione e la cifratura dei dati personali, necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD;
i) assistere il Titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;
j) assistere il Titolare nel garantire il rispetto degli obblighi di sicurezza di cui all'art. 32 RGPD, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, ciascun Dirigente designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali provvede a formulare, al Direttore Generale, una proposta di adozione delle misure necessarie ed una stima dei costi preventivati per la realizzazione degli interventi proposti;

k) garantire l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, ciascun Dirigente designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali provvede a formulare, al Direttore Generale, una proposta di adozione delle misure necessarie ed una stima dei costi preventivati per la realizzazione degli interventi proposti;

l) assicurare l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;

m) informare senza ingiustificato ritardo il Titolare del trattamento, in caso di violazione dei dati personali;

n) assistere il Titolare nelle procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;

o) assistere il Titolare del Trattamento nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD, consultato il Responsabile della Protezione dei Dati (DPO), e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del RGPD;

p) affiancare il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1 e 2, del RGPD, nell'istituzione e aggiornamento del Registro delle attività di trattamento, secondo quanto meglio definito dal successivo art. 17 del presente Regolamento. In particolare, con cadenza almeno annuale, ciascun Dirigente/Direttore, provvede ad istituire le nuove eventuali schede relative a nuove categorie di trattamento e ad aggiornare le schede del Registro dei trattamenti di propria competenza.

q) garantire che il Responsabile della Protezione dei Dati (DPO) designato dal Titolare del trattamento, sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e riceva un adeguato affiancamento nell'esecuzione dei suoi compiti;

r) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto incaricato;

s) informare immediatamente il Titolare qualora, a suo parere, un'istruzione impartita da quest'ultimo violi la normativa comunitaria o nazionale relativa alla protezione dei dati;

t) custodire e controllare i dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

u) aggiornare sistematicamente la mappatura dei Procedimenti amministrativi di competenza dell'Area/Settore assegnato alla sua direzione e censire periodicamente le banche dati di pertinenza;

v) assicurare che il personale facente capo all'Area/Settore di propria pertinenza si attenga, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantire che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;

w) garantire la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale assegnato all'Area/Settore di propria pertinenza, previo consulto del Responsabile della Protezione dei dati (DPO), necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;

x) vigilare sul rispetto da parte delle persone autorizzate al trattamento circa gli obblighi di corretta e lecita raccolta dei dati, di utilizzazione, di comunicazione nonché di diffusione degli stessi a mezzo pubblicazione all'Albo Pretorio On line (ai sensi dell'art. 32, L. 69/2009) ovvero nella Sezione del sito istituzionale dell'Ente denominata "Amministrazione Trasparente" (ai sensi del D. Lgs. 33/2013 e ss.mm.ii.);

y) vigilare sul rispetto del diritto alla riservatezza nell'ambito dei procedimenti di accesso documentale ai sensi e nei limiti degli artt. 22 e ss. L. 241/90, ovvero nei procedimenti di richiesta di accesso civico, ai sensi dall'art. 5, comma 2 e dall'art. 5 bis, D. Lgs. 33/2013 di pertinenza del proprio Settore/Area. Il medesimo obbligo di vigilanza troverà applicazione anche nelle richieste formulate dai consiglieri regionali, nell'esercizio del diritto di accesso a documenti ed informazioni, se ed in quanto applicabile.

z) comunicare tempestivamente al Titolare, l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 RGPD, riguardanti l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

aa) disporre periodiche verifiche, anche per il tramite del Responsabile della Protezione dei Dati (DPO), sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati ed alla formazione ed istruzione dei dipendenti autorizzati al trattamento.

Art. 9 – Responsabili del Trattamento dei dati

1. In tutti i casi in cui la ASL Gallura, nell'ambito dell'affidamento di un incarico, un servizio, un lavoro, una fornitura, una collaborazione o una consulenza, affidi all'esterno un trattamento di dati da effettuarsi per conto della ASL Gallura stessa, il soggetto affidatario dell'incarico, del servizio, del lavoro, della fornitura, della collaborazione o della consulenza, sia esso persona fisica o persona giuridica, dovrà essere preventivamente individuato quale Responsabile del trattamento ai sensi dell'art. 28 RGPD.
2. In ossequio alla previsione di cui all'art. 8, comma 3, lett. c) del presente Regolamento, l'obbligo di provvedere all'esaustiva ed analitica disciplina dei trattamenti da parte dei Responsabili, mediante contratto o altro atto giuridico, è posto in capo ai singoli Dirigenti designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali che procedono, in ossequio alle vigenti disposizioni in materia, all'affidamento di servizi, forniture, lavori, incarichi, consulenze e collaborazioni che comportino un trattamento di dati svolto dal soggetto affidatario per conto della ASL Gallura.
3. Per effetto delle previsioni di cui al precedente comma ed in conformità alle disposizioni di cui all'art. 28, paragrafo 3 del RGPD i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o altro atto giuridico adottato da ciascun Dirigente/Direttore affidante.

Art. 10 – Persone autorizzate al trattamento dei dati

1. Le persone autorizzate al trattamento dei dati sono le persone fisiche, dipendenti del Titolare, espressamente individuate ed autorizzate con provvedimento formale adottato da ciascun Dirigente/Direttore assegnatario delle risorse umane che trattino dati sotto l'autorità diretta e nell'ambito del Settore/Area/Ufficio/Servizio di competenza.
2. In ossequio alle previsioni di cui all'art. 8, comma 3, lett. a) e b) del presente Regolamento, ciascun Dirigente/Direttore individua e nomina, con propria determinazione, le persone autorizzate al trattamento delle Aree/Settori/Uffici/Servizi nelle quali si articolano la macrostruttura e le microstrutture della ASL Gallura, impartendo loro apposite istruzioni

organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29 RGPD e all'art. 2-*quaterdecies*, D. Lgs. 196/03 e ss.mm.ii.

3. Tenuto conto dei procedimenti amministrativi e dei processi di pertinenza degli Uffici di assegnazione delle persone autorizzate al trattamento e delle risultanze del censimento delle Banche Dati cartacee e/o informatiche trattate dai singoli Uffici, ciascun Dirigente/Direttore, in quanto designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali, provvede ad istruire e formare le persone autorizzate al trattamento dei dati con riferimento alla tutela del diritto alla riservatezza, nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati.
4. Il provvedimento di individuazione degli autorizzati contiene le istruzioni e le regole tecniche e operative che le persone autorizzate al trattamento sono tenute a seguire nelle operazioni di trattamento dei dati personali assegnate nonché l'indicazione dei loro obblighi e delle loro responsabilità, con particolare riferimento a:
    a. l'accesso alle banche dati informatiche;
    b. la conservazione dei supporti informatici e/o cartacei contenenti dati personali;
    c. la riservatezza ed il riserbo sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;
    d. la custodia ed il controllo dei dati personali affidati;
    e. la conservazione dei dati in conformità alle misure di sicurezza adottate dall'Ente;
    f. l'utilizzo della postazione di lavoro assegnata;
    g. il collegamento ad Internet;
    h. l'utilizzo dei supporti di memoria magnetici e ottici;
    i. l'utilizzo della posta elettronica.
5. Le persone autorizzate sono tenute alla riservatezza con riferimento ai dati di cui siano venuti a conoscenza nell'esercizio delle funzioni istituzionali loro ascritte e provvedono al loro trattamento attenendosi scrupolosamente alle istruzioni impartite dal Dirigente/Direttore designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali al quale rispondono.
6. In ossequio alle previsioni di cui all'art. 5 RGPD, le persone autorizzate devono assicurare che, nel corso del trattamento, i dati personali siano:
    - trattati in modo lecito, corretto e trasparente;
    - raccolti e registrati per scopi determinati, espliciti e legittimi, e

successivamente trattati in modo compatibile con tali finalità;

- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di minimizzazione);
- esatti e, se necessario, aggiornati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali i dati sono trattati;
- trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

All'atto formale di individuazione quale persona autorizzata al trattamento, è equiparato l'atto di assegnazione del dipendente ad un'unità organizzativa (Ufficio/Servizio) per la quale risulti individuato, analiticamente e in forma scritta, l'ambito del trattamento consentito nonché i compiti e le funzioni connessi al trattamento assegnati al singolo dipendente.

7. Per effetto di tale disposizione, ogni dipendente incardinato in un determinato Ufficio/Servizio sulla base di un formale atto di assegnazione che stabilisca l'ambito del trattamento consentito ed i compiti e le funzioni connessi al trattamento attribuiti, è da considerarsi persona autorizzata al trattamento ai sensi dell'art. 2-quaterdecies, comma 2, D. Lgs. 196/03 e ss.mm.ii.
8. Le persone autorizzate sono beneficiarie sia di interventi formativi preventivi all'assegnazione all'ufficio/servizio sia di richiami formativi di aggiornamento periodici annuali, ai sensi delle disposizioni di cui agli artt. 29 e 32.4 del RGPD.

Art. 11 – Persone autorizzate al trattamento dei dati, non dipendenti del Titolare

1. Le persone fisiche, non legate alla ASL Gallura da un contratto di lavoro subordinato, che abbiano accesso ai dati personali trattati dall'Azienda per svolgere compiti di supporto agli stessi che comportino un trattamento di dati (a titolo meramente esemplificativo e non esaustivo: i tirocinanti, i volontari, i collaboratori e, tutti quei soggetti che operano temporaneamente all'interno della struttura organizzativa del Titolare), devono essere preventivamente individuate, con provvedimento formale quali persone autorizzate al trattamento.
2. Dette persone, autorizzate al trattamento, sono soggette agli stessi obblighi cui sono

sottoposte le persone autorizzate dipendenti del Titolare, in modo da garantire il pieno rispetto della tutela della riservatezza delle persone fisiche alle quali si riferiscono i dati oggetto di trattamento.

3. Le persone autorizzate sono beneficiarie sia di interventi formativi preventivi all'assegnazione all'ufficio/servizio sia di richiami formativi di aggiornamento periodici, ai sensi delle disposizioni di cui agli artt. 29 e 32.4 del Regolamento.

Art. 12 - Responsabile della Protezione dei dati (DPO)

1. Il Responsabile della protezione dei dati (DPO), è individuato, in ossequio alla previsione normativa di cui all'art. 37, paragrafo 5 e 6 RGPD, in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché della capacità del DPO di dare corretto adempimento ai compiti di cui all'art. 39 del Regolamento.
2. La funzione di DPO può essere esercitata in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna alla ASL Gallura. In tal caso, è indispensabile che le persone fisiche appartenenti alla persona giuridica che operano quali DPO della ASL Gallura possiedano tutti i requisiti richiesti dall'art. 37, paragrafo 5, RGPD e, in particolare, abbiano maturato approfondita esperienza, conoscenza e competenza con riferimento alla Pubblica Amministrazione in generale e, specificatamente agli Enti Locali ed alle Aziende del Servizio Sanitario Regionale nonché alla loro organizzazione, alle norme e procedure amministrative agli stessi applicabili. Circa la definizione dei criteri relativi alle qualità professionali ed al possesso dei titoli del DPO si richiamano integralmente le disposizioni di cui al *documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico, adottato dall'Autorità Garante per la Protezione dei Dati Personali in data 29/04/2021 (GU n. 132 del 4 giugno 2021)*, anche per ciò che concerne le ipotesi di conflitto di interesse.
3. I compiti attribuiti al DPO sono indicati in apposito contratto di servizi. Il DPO esterno è tenuto a procedere sistematicamente nell'aggiornamento della propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.
4. Il DPO può essere altresì individuato tra le risorse umane della ASL Gallura, nella figura di un dipendente in possesso di competenze e professionalità adeguate alla natura dell'incarico, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché

alla capacità di promuovere una cultura della protezione dei dati all'interno dell'organizzazione della ASL Gallura

In ossequio alla previsione di cui all'art. 37, paragrafo 3, RGPD, è possibile l'affidamento dell'incarico di DPO ad un unico soggetto, anche esterno, designato da più Enti/Organismi mediante esercizio associato della funzione, nelle forme previste dai singoli ordinamenti.

5. Il DPO è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:
    a) informare e fornire consulenza al Titolare del trattamento, ai Dirigenti/Direttori designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali ed alle Persone autorizzate al trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati personali;
    b) partecipare alle riunioni di coordinamento dei Dirigenti/Direttori che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
    c) provvedere alla formazione di Dirigenti/Direttori designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali e persone autorizzate al trattamento in merito agli obblighi derivanti dal RGPD in conformità alle disposizioni vigenti;
    d) sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché l'osservanza delle politiche adottate dal Titolare del trattamento o dai Dirigenti/Direttori designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
    e) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento ai sensi dell'art. 35 RGPD. In particolare, il Titolare e/o i Dirigenti/Direttori designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali, si consulta/no con il DPO in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi

delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

f) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del DPO è comunicato dal Titolare al Garante;

g) tenere, il Registro delle attività dei trattamenti di cui al successivo art. 17, sotto la responsabilità del Titolare del trattamento;

h) fornire supporto tecnico-giuridico e vigilare circa l'applicazione dei principi in materia di protezione dei dati personali in relazione alle attività rilevanti ai fini del trattamento realizzate dalle seguenti figure:

   a. Social media manager;
   b. Responsabile dell'ufficio per la transizione alla modalità digitale;
   c. Responsabile per Responsabile dei flussi documentali e degli archivi;
   d. Responsabile della conservazione;
   e. Responsabile della sicurezza informatica;
   f. Responsabile della sicurezza cibernetica;
   g. Amministratore di Sistema.

6. Il Titolare del trattamento ed i Dirigenti/Direttori designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine provvedono a:

   a) mettere a disposizione del DPO le risorse umane e materiali preordinate a consentirgli l'ottimale svolgimento dei compiti e delle funzioni assegnate, garantendogli l'accesso ai dati personali ed ai trattamenti;

   b) garantire al DPO il supporto dei competenti servizi tecnico-informatici per la risoluzione di tutte le problematiche relative alla protezione dei dati personali che abbiano una incidenza diretta o indiretta sulle attività di trattamento effettuate con l'ausilio di strumenti informatici;

   c) fornire al DPO tutte le informazioni in merito al trattamento dei dati personali ed alle correlate misure di sicurezza adottate dalla ASL Gallura al fine di consentire allo stesso DPO di fornire alla Azienda una consulenza funzionale con riferimento

alle problematiche oggetto di analisi. Il parere del DPO 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 DPO, è necessario che il Titolare del trattamento o i Dirigenti/Direttori designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali motivino specificamente detta decisione;

d) consultare tempestivamente il DPO qualora si verifichi una violazione dei dati o altro incidente in grado di avere rilevanza sui dati personali trattati dalla ASL Gallura.

7. Nello svolgimento dei compiti affidatigli il DPO deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
8. La figura di DPO è incompatibile con qualunque figura deputata a determinare le finalità o i mezzi del trattamento all'interno della ASL Gallura; in particolare, risultano con la stessa incompatibili:
   a) la funzione di Responsabile per la prevenzione della corruzione e per la trasparenza;
   b) la funzione di Responsabile dell'Ufficio per la Transizione al Digitale
   c) Responsabile per Responsabile dei flussi documentali e degli archivi;
   d) Responsabile della conservazione;
   e) Responsabile della sicurezza informatica;
   f) Responsabile della sicurezza cibernetica;
   g) Amministratore di Sistema.
   h) più in generale la funzione di Dirigente/Direttore designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali;
   i) la funzione di soggetto chiamato a determinare le finalità o i mezzi del trattamento.
9. Il DPO opera in posizione di autonomia nello svolgimento dei compiti attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare ad una specifica questione attinente alla normativa in materia di protezione dei dati.
10. Il DPO non può essere rimosso o penalizzato per l'adempimento dei propri compiti.
11. Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso DPO, quest'ultimo

è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare del trattamento ed ai Dirigenti/Direttori designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali.

CAPO III - PRINCIPI

Art. 13 - Principi e responsabilizzazione

1. Vengono integralmente recepiti, nell'organizzazione interna del Titolare, i principi del RGPD, per effetto dei quali, 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 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 in base al c.d. principio di "minimizzazione dei dati";

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 base del principio di "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, RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato in base al principio di "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 in base ai principi di "integrità e riservatezza";

g) configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità ("principio di necessità").

2. Il Titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di comprovarlo in base al principio di "responsabilizzazione".

Art. 14 - Condizioni per il consenso

1. Fermi restando i casi in cui il trattamento sia effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare, ovvero, per i dati di cui agli artt. 9 e 10 RGPD, nelle ipotesi in cui il trattamento sia necessario per motivi di interesse pubblico rilevante (in questi casi, infatti, il trattamento può essere legittimamente effettuato in assenza di consenso dell'interessato), qualora il trattamento dei dati personali, per una o più specifiche finalità, sia subordinato al consenso dell'interessato, si applica la disciplina di cui all'art. 7 RGPD, la quale prevede che:
   a) il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali;
   b) se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro;
   c) l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato deve essere informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato;
   d) nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.
   e) per le "categorie particolari di dati personali" di cui all'art. 9, RGPD, il consenso deve essere esplicito e prestato in forma scritta; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione;
   f) il consenso deve essere, in tutti i casi, libero e autonomo, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto;

g)deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".

2. Qualora il trattamento sia basato sul consenso, il consenso deve essere reso, da parte dell'interessato, attraverso la compilazione di apposita modulistica, resa disponibile dal Titolare, previa consegna e presa d'atto dell'Informativa di cui al successivo art. 15.
3. In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, emergenza sanitaria o di igiene pubblica, rischio grave e imminente per la salute dell'interessato, il consenso può intervenire senza ritardo, anche successivamente alla prestazione, da parte di chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente.
4. La manifestazione del consenso, ad opera dell'interessato, va resa al momento del primo accesso ai servizi/prestazioni, ed è valido ed efficace fino alla revoca della stessa.
5. Il consenso viene registrato nel registro delle attività di trattamento.

Art. 15 – Informativa all'interessato

1. Il Titolare del trattamento e ciascun Dirigente/Direttore designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali dei assicurano, anche avvalendosi dei dipendenti assegnati agli Uffici/Servizi ricompresi nella Struttura ascritta alla sua direzione che, al momento della raccolta dei dati personali, agli interessati sia fornita apposita informativa secondo le modalità previste dall'art. 13, RGPD, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.
2. L'informativa è fornita, in linea di principio, per iscritto, anche in formato elettronico, soprattutto nel contesto di servizi resi in modalità *online*.
3. L'informativa può essere fornita con le seguenti modalità:
   a) attraverso apposita modulistica resa disponibile agli interessati;
   b) attraverso avvisi agevolmente accessibili al pubblico, posti nei locali di accesso agli Uffici della ASL Gallura ovvero diffusi attraverso pubblicazione sul sito istituzionale della stessa;
   c) attraverso apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti e di altri soggetti chiamati a prestare la loro attività per conto della ASL Gallura;
   d) in sede di pubblicazione dei bandi, degli avvisi, delle lettere d'invito.
4. L'informativa contiene il seguente contenuto minimo:

a) l'identità ed i dati di contatto del Titolare;
b) i dati di contatto del DPO;
c) le indicazioni in merito alle finalità del trattamento;
d) la base giuridica del trattamento;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) l'eventuale intenzione del Titolare di trasferire i dati personali ad un Paese terzo o a un'organizzazione internazionale;
g) il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
h) l'esistenza del diritto dell'interessato di chiedere al Titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
i) qualora il trattamento sia basato sul consenso dell'interessato, l'esistenza del diritto di revocare il consenso in qualunque momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
j) l'indicazione in merito al fatto che la comunicazione dei dati personali sia un obbligo legale o contrattuale, ovvero un requisito necessario per la conclusione di un contratto, ovvero se l'interessato abbia l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione dei dati;
k) il diritto di proporre reclamo al Garante per la protezione dei dati personali;
l) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.

5. 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 e ogni ulteriore informazione ritenuta utile.
6. Nel caso in cui i dati personali non siano raccolti direttamente presso l'interessato, ciascun Dirigente/Direttore designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali, anche avvalendosi dei dipendenti assegnati agli Uffici/Servizi ricompresi nella Struttura ascritta alla sua direzione, fornisce all'interessato le seguenti informazioni:
    a) l'identità ed i dati di contatto del Titolare;
    b) i dati di contatto del DPO;

c) le indicazioni in merito alle finalità del trattamento;
d) la base giuridica del trattamento;
e) le categorie di dati personali trattati;
f) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
g) l'eventuale intenzione del Titolare di trasferire i dati personali ad un Paese terzo o a un'organizzazione internazionale;
h) il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
i) l'esistenza del diritto dell'interessato di chiedere al Titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
j) qualora il trattamento sia basato sul consenso dell'interessato, l'esistenza del diritto di revocare il consenso in qualunque momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
k) il diritto di proporre reclamo al Garante per la protezione dei dati personali;
l) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
m) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.

7. L'informativa, nei casi di cui al precedente comma 6, deve essere fornita contestualmente alla acquisizione dei dati personali. Nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, l'informativa deve essere fornita, al più tardi, al momento della prima comunicazione all'interessato. Nel caso sia invece prevista la comunicazione ad altro destinatario, l'informativa deve essere fornita non oltre la prima comunicazione dei dati personali.

Art. 16 – Formazione e sensibilizzazione del personale

1. Il Titolare del trattamento promuove, all'interno della ASL Gallura, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore del diritto alla riservatezza dei dati, al fine di migliorare la qualità dei servizi resi nei confronti degli interessati.

L’attività di formazione ed informazione costituisce uno degli strumenti essenziali per la responsabilizzazione e la sensibilizzazione dei diversi soggetti coinvolti nel trattamento di dati personali.

2. Al fine di assicurare la conoscenza capillare delle disposizioni contenute nel RGPD e nel presente Regolamento, al momento dell'ingresso in servizio è consegnata ad ogni dipendente una specifica comunicazione, che richiama l’apposita clausola inserita nel contratto di lavoro, contenente i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale.

   Il dipendente si impegna ad acquisire copia del Regolamento, prenderne visione ed attenersi alle sue prescrizioni.
3. Il presente Regolamento è pubblicato sul sito istituzionale della ASL Gallura, nella Sezione Amministrazione Trasparente, Sotto Sezione di I Livello “Altri Contenuti”, Sotto Sezione di II Livello “Privacy”.
4. Il Titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, con cadenza annuale, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione dei rischi di distruzione, perdita, modifica, divulgazione non autorizzata o accesso illegittimo ai dati conservati e trattati dai dipendenti della ASL Gallura.

   Gli interventi formativi ed informativi sono altresì finalizzati a rendere edotti i Dirigenti/Direttori, formalmente designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali, sulle misure di sicurezza adottate dalla ASL Gallura ai sensi dell’art. 32 RGPD al fine di assicurare l’integrità, la riservatezza, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
5. La formazione in materia di tutela del diritto alla riservatezza e prevenzione dei rischi di violazione dei dati personali viene integrata con la formazione in tema di trasparenza e di diritto di accesso, con particolare riguardo al corretto bilanciamento tra il diritto alla protezione dei dati personali e le contrapposte esigenze di trasparenza dell’azione amministrativa, nonché di diritto di accesso ai documenti amministrativi (di cui agli artt. 22 e ss. L. 241/90 e ss.mm.ii.) e di diritto di accesso civico generalizzato (di cui all’art. 5, comma 2, D. Lgs. 33/2013 e ss.mm.ii.), nei diversi ambiti in cui opera il Titolare.
6. La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento imprescindibile per il trattamento dei dati personali e criterio di misurazione e valutazione della performance organizzativa ed individuale.

Art. 17 - Registro delle attività dei trattamenti

1. Il Titolare del trattamento istituisce, in forma scritta, un Registro delle attività di trattamento e di tutte le categorie di attività relative al trattamento, svolte sotto la propria responsabilità, secondo quanto previsto dall'art. 30, paragrafo 1, del RGPD.
2. Il Registro delle attività dei trattamenti reca almeno le seguenti informazioni:

a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del Titolare del trattamento, del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) le categorie dei trattamenti effettuati da parte delle singole articolazioni della Struttura della ASL Gallura (aree/ settori/ servizi/ uffici);
d) una descrizione delle categorie di interessati e delle categorie di dati personali;
e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
f) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
g) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
h) il richiamo alle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3. Il Titolare delega la tenuta del registro delle attività di trattamento al Responsabile per la Protezione dei Dati (DPO), sotto la responsabilità del medesimo Titolare. Ciascun Dirigente/Direttore designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali ha comunque la responsabilità di fornire prontamente e correttamente al Responsabile per la Protezione dei Dati, ogni elemento, dato e informazione necessari alla regolare formazione, tenuta e all'aggiornamento del Registro delle attività dei trattamenti.
4. Su richiesta, il Titolare del trattamento o il Dirigente/ Direttore designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali, mettono il registro a disposizione del Garante.
5. Il registro è tenuto in forma scritta, anche in formato elettronico, e deve essere periodicamente aggiornato, con cadenza almeno annuale e, in ogni caso, ogniqualvolta vi

siano delle modifiche che richiedono la loro trascrizione nel registro dei trattamenti (modalità di trattamento, finalità, categorie di dati, categorie di interessati, ecc.).

6. Il registro delle attività dei trattamenti è adottato con provvedimento del Titolare del trattamento e, successivamente, con cadenza annuale, con analogo provvedimento sono adottate le revisioni del Registro delle attività dei trattamenti che, danno conto delle eventuali modifiche/integrazioni e novità intercorse con riferimento alle categorie di dati trattati, alle modalità di trattamento, alle finalità, alle categorie di interessati, nonché alle misure di sicurezza tecniche ed organizzative di cui all'art. 32 RGPD.

CAPO IV – PUBBLICITA' E DIFFUSIONE SUL WEB DI DOCUMENTI CONTENENTI DATI PERSONALI

Art. 18 - Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

1. I Dirigenti/Direttori designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali, in sede di pubblicazione sul sito istituzionale della ASL Gallura nelle Sezioni "Albo pretorio on-line" e "Amministrazione Trasparente", di dati personali contenuti in atti e provvedimenti amministrativi per i quali un'espressa previsione normativa ne preveda l'obbligo di pubblicazione, assicurano il rispetto dei principi di pertinenza e minimizzazione di cui all'art. 5, paragrafo 1, lett. c), RGPD.
2. La pubblicazione di un atto sul sito istituzionale della ASL Gallura costituisce un'operazione di **diffusione** dei dati personali in esso eventualmente contenuti; detta circostanza impone alla ASL Gallura di valutare preventivamente, di volta in volta, quali siano le informazioni personali la conoscenza delle quali sia realmente rilevante rispetto alle specifiche finalità perseguite con la pubblicazione medesima.

   A questo fine, si osserva che:

   - **la "diffusione" di dati personali** – ossia "il dare conoscenza dei dati personali a soggetti indeterminati" mediante la pubblicazione sul proprio sito istituzionale - da parte dei "soggetti pubblici" è ammessa unicamente quando la stessa sia prevista da una specifica norma di legge o di regolamento (art. 2-*ter*, comma 1, D. Lgs. 196/03 e ss.mm.ii.);
   - laddove l'Amministrazione riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell'atto o del documento sul proprio sito web

istituzionale è necessario selezionare i dati personali da inserire in tali documenti, verificando, caso per caso, se ricorrano i presupposti per l'oscuramento di determinate informazioni;

- è consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria (cd. "principio di pertinenza e minimizzazione" di cui all'art. 5, paragrafo 1, lett. c), RGPD).
- è sempre vietata la diffusione di dati idonei a rivelare lo "stato di salute" e "la vita sessuale" (art. 2-*septies*, comma 8, D. Lgs. 196/03 e ss.mm.ii. e art. 7-*bis*, comma 6, D. Lgs. 33/2013) nonché "la situazione di disagio economico sociale degli interessati" (art. 26, comma 4, D. Lgs. 33/2013).

3. Una volta trascorso l'arco temporale previsto dalle singole discipline per la pubblicazione degli atti e dei documenti sul sito web dell'Amministrazione, la ASL Gallura provvederà, senza indugio, alla loro defissione.

CAPO V - SICUREZZA DEI DATI PERSONALI

Art. 19 – Sicurezza del trattamento

1. Il Titolare e ciascun Dirigente/Direttore designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali mettono in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono:
   - la pseudonimizzazione;
   - la minimizzazione;
   - la cifratura dei dati personali;
   - la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
   - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
   - una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate da ciascun designato, previa consultazione del Responsabile della Protezione dati (DPO) e dei competenti servizi tecnico-informatici dell'Azienda:
   - sistemi di autenticazione;
   - sistemi di autorizzazione;
   - sistemi di protezione (antivirus; firewall; antintrusione; altro);
   - misure antincendio;
   - sistemi di rilevazione di intrusione;
   - sistemi di sorveglianza;
   - sistemi di protezione con videosorveglianza;
   - registrazione accessi;
   - porte, armadi e contenitori dotati di serrature e ignifughi;
   - sistemi di copiatura e conservazione di archivi elettronici;
   - ulteriori misure per ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico.
4. La conformità del trattamento dei dati al RGDP è dimostrata attraverso l'adozione delle misure di sicurezza adeguate al rischio in ossequio alle previsioni di cui all'art. 32 RGPD, ovvero attraverso l'adesione a codici di condotta approvati o ad altri meccanismi di certificazione approvati.

Art. 20 -Valutazioni d'impatto sulla protezione dei dati

1. La valutazione d'impatto sulla protezione dei dati (di seguito solo "DPIA") è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
2. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGPD, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

3. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'at. 35, paragrafi 4, 5 e 6 RGPD[2].
4. Al fine di attuare una DPIA, il Titolare si consulta con il Responsabile della Protezione dei Dati (DPO) che fornisce parere in merito e ne sorveglia lo svolgimento ai sensi dell'art. 35 RGPD.
5. L'Amministratore di Sistema e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare ed al Responsabile della Protezione dei Dati (DPO) per lo svolgimento della DPIA.
6. La DPIA non è necessaria nei casi seguenti:
    - se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, RGPD;
    - se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
    - se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
    - se un trattamento trova la propria base giuridica nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.
7. La DPIA antecede temporalmente l'inizio delle attività di trattamento e contiene almeno:

a) la descrizione sistematica del contesto, dei trattamenti previsti e delle finalità del trattamento. 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 (*hardware*, *software*, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) la valutazione dei rischi per i diritti e le libertà degli interessati, con particolare riguardo alla probabilità e alla gravità dei rischi rilevati;

d) l'individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare

[2] Si richiama integralmente l'Allegato 1 al Provvedimento del Garante Privacy n. 467 dell'11/10/2018 ed i successivi provvedimenti contenenti gli elenchi delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto

la protezione dei dati personali e dimostrare la conformità del trattamento al RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. La DPIA 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 - Consultazione preventiva

1. Il Titolare, prima di procedere al trattamento dei dati, consulta, per il tramite del DPO, il Garante Privacy qualora la valutazione d'impatto sulla protezione dei dati abbia evidenziato che il trattamento potrebbe presentare un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio.

Art. 22 - Notifica di una violazione dei dati personali

1. Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dalla Asl Gallura.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.
3. I Dirigenti/Direttori designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali e i Responsabili del trattamento sono obbligati ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuti a conoscenza della violazione dei dati personali.
4. La notifica al Garante Privacy deve:

   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.

5. Qualora e nella misura in cui non sia possibile fornire contestualmente le informazioni i cui al precedente comma 4, dette informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

6. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, sono quelli descritti al considerando 75 del RGPD, che si richiama integralmente: "*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*."

7. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate all'Autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione, da conservarsi diligentemente, dovrà essere esibita, su richiesta del Garante Privacy, al fine della verifica del rispetto delle disposizioni di cui all'art. 33 RGPD.

Art. 23 - Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione di dati personali è 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.

2. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le seguenti informazioni:

- il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

3. Non è richiesta la comunicazione all'interessato se è 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 ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante Privacy può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda ovvero può decidere che una delle condizioni di cui al precedente comma 3, lett. a), b) e c) sia soddisfatta.

Art. 24 - Disposizioni finali

1. Per quanto non espressamente previsto e disciplinato dal presente Regolamento si applicano le disposizioni di cui al Regolamento UE 2016/679, al D. Lgs. 196/03 (così come riformato e modificato dal D. Lgs. 101/18), nonché le Linee guida ed i provvedimenti del

Garante Privacy, e le Linee Guida del Comitato europeo per la protezione dei dati personali.

2. Il presente Regolamento s'intende automaticamente aggiornato, qualora dovessero intervenire ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.
3. Il presente regolamento entra in vigore il giorno della sua approvazione con Deliberazione del Direttore Generale.

Art. 25 - Rinvio

Per quanto non espressamente previsto nel presente regolamento, si reinvia alle disposizioni vigenti in materia che, comunque, ogni dipendente è tenuto a conoscere.

Eventuali difformità, rispetto alla legge, oltre che alle norme di rango superiore, del presente regolamento sono da intendersi automaticamente soccombenti.