REGIONE DEL VENETO

ULSS6 EUGANEA

N. 323 **del** 29-04-2022

DELIBERAZIONE DEL DIRETTORE GENERALE

dott. Paolo FORTUNA

Coadiuvato dai Signori:

DIRETTORE AMMINISTRATIVO	dr.ssa Michela Barbiero
DIRETTORE SANITARIO	dr. Aldo Mariotto
DIRETTORE DEI SERVIZI SOCIO SANITARI	dr.ssa Maria Chiara Corti

Note Trasparenza: Il provvedimento approva il sistema di gestione aziendale della Protezione dei dati personali - SGA PDP - e costituisce un team multiprofessionale di supporto.

OGGETTO: Approvazione del sistema di gestione aziendale della Protezione dei dati personali - SGA PDP - e costituzione di un team multiprofessionale di supporto.

Il Direttore Amministrativo

Riferisce quanto segue:

Come noto un “sistema” è inteso come l’insieme delle procedure e dei processi organizzativi funzionali al soddisfacimento di requisiti definiti ed è uno strumento di carattere organizzativo e gestionale utilizzato per rispettare, in modo visibile e dimostrabile, i criteri ed i requisiti previsti dalla norma di riferimento. Inoltre, un sistema presenta fisiologiche caratteristiche di dinamicità, flessibilità e capacità di miglioramento.

Nello specifico, il “sistema di gestione della protezione dei dati personali (SGA PDP)” è il modello di gestione, organizzazione e controllo che governa il trattamento in sicurezza dei dati personali ed il rispetto dei principi e delle regole delle normative di riferimento, sostanziale e strettamente interconnesso alle attività dell’azienda.

Le norme in materia di protezione dei dati personali impongono ormai modalità operative concrete e lontane dai formalismi del mero adempimento normativo: di conseguenza, l’utilizzo di un sistema di gestione della protezione dei dati personali costituisce un efficace strumento utile non solo per la messa in sicurezza dei dati stessi, ma anche per la loro valorizzazione e la tutela dell’intero patrimonio informativo aziendale.

Poiché è compito dell'azienda dimostrare la propria diligenza perseguendo gli obiettivi di conformità normativa, responsabile e documentata attraverso l'implementazione di un complesso di misure di sicurezza in grado di proteggere, nel tempo, i dati personali, si rende necessario, cogliendo una preziosa opportunità di miglioramento continuo, uno sforzo ulteriore rispetto al passato che richiede la revisione dell'attuale sistema di gestione, adeguandolo ai continui cambiamenti organizzativi dell'azienda.

Infatti, i principi del Regolamento UE 679/2016 (GDPR) devono tradursi in prassi operative, controlli e comportamenti efficaci, assumendosi la responsabilità delle scelte. Si tratta dell'oramai noto principio di accountability: "*Titolare e Responsabili devono saper progettare e implementare misure di sicurezza pertinenti alla propria realtà organizzativa, ai rischi connessi al trattamento, funzionali agli obiettivi di protezione dei dati e del rispetto del Regolamento*".

A tal fine, stante la complessità dell'azienda, per la quale sono ancora in corso attività di revisione dei processi organizzativi derivanti dalla fusione delle tre ex aziende sanitarie padovane (ULSS15 - ULSS16 - ULSS17) e dei trattamenti gestiti, nonché nell'ambito del percorso di miglioramento continuo, previsto e rappresentato anche nel piano delle performance 2022-2024 e nel documento di direttive per l'anno 2022, si ravvede la necessità di ridefinire il sistema di gestione della Protezione dei dati personali - e di costituire un team multidisciplinare di supporto al fine di dare maggior impulso al cammino intrapreso e garantire un sostegno operativo in grado di puntellare l'impianto di protezione dei dati dimostrando le capacità e l'attitudine dell'intera organizzazione alla valorizzazione e tutela del patrimonio informativo, assicurando il monitoraggio ed il miglioramento continuo dei processi e delle procedure.

A tal fine si propone l'approvazione del documento di sistema, come rappresentato nell'allegato, parte integrante della presente deliberazione, nonché la costituzione di un team di supporto in un'ottica multidisciplinare tecnica/giuridica perfettamente in linea con il principio di responsabilizzazione sancito dal Reg. UE679/2016 (GDPR) che, anche alla luce dei più recenti provvedimenti dell'Autorità Garante per la Protezione dei dati personali in materia, deve essere delineato in una prospettiva giuridica (artt. 5 par. 2 e 24 GDPR) come in una più moderna dimensione tecnologica (art. 25 GDPR).

Si propone che il team sia così composto:

- Dr.ssa Marzia Serafini - Infermiere - UOS Qualità e accreditamento istituzionale, in qualità di coordinatore del gruppo;
- Dr.ssa Giulia Gusella - collaboratore amm.vo prof. - ufficio privacy UOC Affari Generali;
- Sig. Marco Calore - collaboratore tecnico professionale - UOSD Servizi Informativi;
- Dr. ssa Francesca Danesin - collaboratore tecnico professionale - UOS Innovazione e sviluppo;
- Dr. Luca Benacchio - collaboratore amministrativo prof. - Dipartimento di Prevenzione;
- Dr.ssa Michela Tregnaghi - dirigente amm.vo - UOS Servizi amministrativi distrettuali afferente all'UOC Direzione Amministrativa Territoriale;
- Dr.ssa Cristina Del Vecchio - collaboratore amm.vo prof. - Direzione Amm.va;

- Dr. Enrico Pinton - infermiere - UOS Rischio clinico;
- Dr.ssa Michela Zanella - Dirigente amm.vo Resp. UOS Programmazione integrata Risorse Umane afferente all'UOC Risorse Umane;
- Dr. Antonio Madia - Dirigente medico - Direzione Medica Ospedale di Cittadella;
- Dr.ssa Paola Giuriato - Dirigente Medico - NAC;
- Dr.ssa Annalisa Timpini - Dirigente Medico Cure Primarie - Distretto 1 Bacchiglione;
- Ing. Alessio Magliani - Responsabile UOS Monitoraggio attività, qualità del dato e analisi statistiche afferente all'UOC Controllo di gestione.

Il team potrà, su indicazione del Direttore dell'UO di afferenza, essere implementato con ulteriori figure professionali a seconda delle necessità e dell'ambito di analisi.

Al team si propone di attribuire funzioni di analisi e supporto all'ufficio aziendale protezione dati personali (ex ufficio privacy), in raccordo con il DPO - con particolare riferimento al supporto per:

- ✓ la revisione e implementazione del registro dei trattamenti (art. 30 GDPR);
- ✓ le valutazioni dell'ambito di applicazione, del contesto e delle finalità del trattamento (art. 24, par. 1 GDPR), particolarmente importanti nel caso di avvio di nuove attività o tecnologie che hanno impatto sul trattamento dei dati personali (es. videosorveglianza, servizi web, nuove applicazioni, servizi evolutivi di gestione dei dati, uso di dati biometrici ecc.);
- ✓ la valutazione del rischio, da cui derivano le misure di sicurezza messe in atto (art. 24, par. 1 e art. 32 GDPR), che necessitano revisione periodica a fronte dei cambiamenti interni (del contesto) o esterni (evoluzione delle minacce ecc.);
- ✓ la protezione per impostazione predefinita (art. 25 GDPR). La privacy "by default", per definizione, implica il costante presidio dell'efficace attuazione dei principi di protezione dei dati;
- ✓ le attività di controllo in vigilando del mantenimento delle garanzie offerte dai Responsabili del trattamento (art. 28 GDPR) e della pertinenza delle istruzioni fornite rispetto al risultato atteso (art. 29 GDPR);
- ✓ le valutazioni di impatto (art. 35 par. 11 GDPR) che devono essere sottoposte a riesame qualora insorgano significative variazioni di rischio.

Al team dovrà essere garantito un adeguato percorso formativo necessario a fortificare la conoscenza delle disposizioni del GDPR e degli strumenti per la realizzazione delle valutazioni di impatto privacy (DPIA) nonché dei modelli di riskassessment.

In tal modo si ritiene che il processo di trattamento dei dati possa concretamente superare logiche più formalistiche di adeguamento al dettato normativo, implementando sistematici meccanismi di verifica sia *ex ante* che *ex post.* Il fine è garantire un supporto multidisciplinare per non perdere di vista l'obiettivo di protezione e di mantenere efficiente nel tempo il complesso di misure di sicurezza adottato, migliorandolo se e quando necessario.

IL DIRETTORE GENERALE

Coadiuvato dai Direttori Sanitario e dei Servizi Socio Sanitari, che, ai sensi dell'art. 3 del D.Lgs. n. 502/1992 e successive modifiche e integrazioni, e ai sensi dell'art.

16 della L.R. n. 56/1994 e successive modifiche e integrazioni, esprimono parere favorevole per quanto di rispettiva competenza;

In base ai poteri conferitigli dal D.P.G.R. n. 25 del 26/02/2021;

DELIBERA

1. Di considerare le premesse parti integranti del seguente provvedimento;
2. Di approvare il sistema di gestione aziendale della protezione dei dati personali (SGA PDP), come illustrato nell'allegato documento parte integrante della presente deliberazione;
3. Di costituire un team multiprofessionale tecnico/giuridico di supporto composto da:
   - Dr.ssa Marzia Serafini - Infermiere - UOS Qualità e accreditamento istituzionale, in qualità di coordinatore del gruppo;
   - Dr.ssa Giulia Gusella - collaboratore amm.vo prof. - ufficio privacy UOC Affari Generali;
   - Sig. Marco Calore - collaboratore tecnico professionale - UOSD Servizi Informativi;
   - Dr. Domenico Zanella - collaboratore tecnico professionale - UOSD Sistemi informativi;
   - Dr. ssa Francesca Danesin - collaboratore tecnico professionale - UOS Innovazione e sviluppo;
   - Dr. Luca Benacchio - collaboratore amministrativo prof. - Dipartimento di Prevenzione;
   - Dr.ssa Michela Tregnaghi - dirigente amm.vo - UOS Servizi amministrativi distrettuali afferente all'UOC Direzione Amministrativa Territoriale;
   - Dr.ssa Cristina Del Vecchio - collaboratore amm.vo prof. - Direzione Amm.va;
   - Dr. Enrico Pinton - infermiere - UOS Rischio clinico;
   - Dr.ssa Michela Zanella - Dirigente amm.vo Resp. UOS Programmazione integrata Risorse Umane afferente all'UOC Risorse Umane;
   - Dr. Antonio Madia - Dirigente medico - Direzione Medica Ospedale di Cittadella;
   - Dr.ssa Paola Giuriato - Dirigente Medico - NAC;
   - Dr.ssa Annalisa Timpini - Dirigente Medico Cure Primarie - Distretto 1 Bacchiglione;
   - Ing. Alessio Magliani - Responsabile UOS Monitoraggio attività, qualità del dato e analisi statistiche afferente all'UOC Controllo di gestione;

   precisando che il team potrà, su indicazione del Direttore dell'UO di afferenza, essere implementato con ulteriori figure professionali a seconda delle necessità e dell'ambito di analisi;
4. Di attribuire, al sopra citato team, funzioni di analisi e supporto all'ufficio aziendale protezione dati personali (ex ufficio privacy), in raccordo con il DPO - con particolare riferimento al supporto per:
   - ✓ la revisione e implementazione del registro dei trattamenti (art. 30 GDPR);

- ✓ le valutazioni dell'ambito di applicazione, del contesto e delle finalità del trattamento (art. 24, par. 1 GDPR), particolarmente importanti nel caso di avvio di nuove attività o tecnologie che hanno impatto sul trattamento dei dati personali (es videosorveglianza, servizi web, nuove applicazioni, servizi evolutivi di gestione dei dati, uso di dati biometrici ecc.);
- ✓ la valutazione del rischio, da cui derivano le misure di sicurezza messe in atto (art. 24, par. 1 e art. 32 GDPR), che necessitano revisione periodica a fronte dei cambiamenti interni (del contesto) o esterni (evoluzione delle minacce ecc.);
- ✓ la protezione per impostazione predefinita (art. 25 GDPR). La privacy "by default", per definizione, implica il costante presidio dell'efficace attuazione dei principi di protezione dei dati;
- ✓ le attività di controllo in vigilando del mantenimento delle garanzie offerte dai Responsabili del trattamento (art. 28 GDPR) e della pertinenza delle istruzioni fornite rispetto al risultato atteso (art. 29 GDPR);
- ✓ le valutazioni di impatto (art. 35 par. 11 GDPR) che devono essere sottoposte a riesame qualora insorgano significative variazioni di rischio;

5. Di incaricare l'UOSD Formazione all'organizzazione e attivazione di un adeguato percorso formativo in accordo con il proponente e il DPO aziendale;
6. Di incaricare l'UOS Qualità e accreditamento istituzionale di pubblicare la presente deliberazione nell'area riservata dei dipendenti.

Il Direttore Generale
dr. Paolo Fortuna

Direttore Amministrativo	Direttore Sanitario	Direttore dei Servizi Socio Sanitari
dr.ssa Michela Barbiero	dr. Aldo Mariotto	dr.ssa Maria Chiara Corti

SISTEMA DI GESTIONE AZIENDALE PROTEZIONE DATI PERSONALI **(SGA PDP)**

Sommario

1 PREMESSA

Come noto un "sistema" è inteso come l'insieme delle procedure e dei processi organizzativi funzionali al soddisfacimento di requisiti definiti ed è uno strumento di carattere organizzativo e gestionale utilizzato per rispettare, in modo visibile e dimostrabile, i criteri ed i requisiti previsti dalla norma di riferimento. Inoltre, un sistema presenta fisiologiche caratteristiche di dinamicità, flessibilità e capacità di miglioramento.

Nello specifico, il **"Sistema di Gestione Aziendale Protezione Dati Personali (SGA PDP)"** è il modello di gestione, organizzazione e controllo che governa il trattamento in sicurezza dei dati personali ed il rispetto dei principi e delle regole delle normative di riferimento, sostanziale e strettamente interconnesso alle attività dell'azienda.

Le norme in materia di protezione dei dati personali impongono ormai modalità operative concrete e lontane dai formalismi del mero adempimento normativo: di conseguenza, l'utilizzo di un sistema di gestione costituisce un efficace strumento utile non solo per la messa in sicurezza dei dati, ma anche per la loro valorizzazione e la tutela dell'intero patrimonio informativo aziendale.

Poiché è compito dell'azienda dimostrare la propria diligenza perseguendo gli obiettivi di conformità normativa, responsabile e documentata attraverso l'implementazione di un complesso di misure di sicurezza in grado di proteggere, nel tempo, i dati personali, si rende necessario, cogliendo una preziosa opportunità di miglioramento continuo, uno sforzo ulteriore rispetto al passato che richiede la revisione dell'attuale sistema di gestione della privacy, adeguandolo ai continui cambiamenti organizzativi dell'azienda.

Infatti, i principi del Regolamento UE 679/2016 (GDPR) devono tradursi in prassi operative, controlli e comportamenti efficaci, assumendosi la responsabilità delle scelte. Si tratta dell'oramai noto principio di *accountability*: "Titolare e Responsabili devono saper progettare e implementare misure di sicurezza pertinenti alla propria realtà organizzativa, ai rischi connessi al trattamento, funzionali agli obiettivi di protezione dei dati e del rispetto del Regolamento".

2 SCOPO

Scopo del presente documento è quello di delineare il **Sistema di Gestione Aziendale Protezione Dati Personali (SGA PDP)** all'interno dell'Azienda ULSS6 Euganea, individuando compiti e responsabilità dei vari attori aziendali e sovra-aziendali coinvolti.

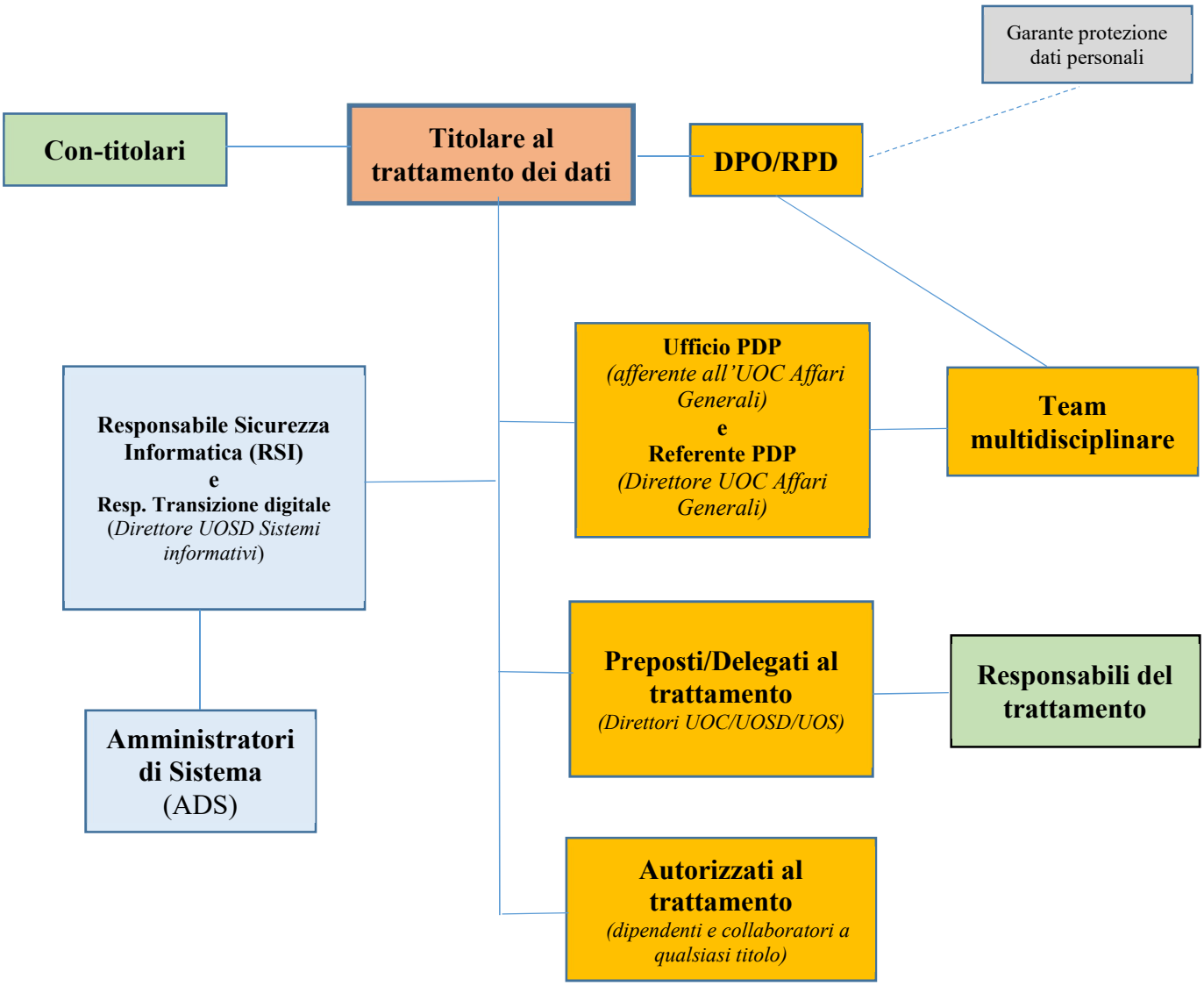
3 DEFINIZIONI ED ACRONIMI

Acronimi	
SGA PDP	Sistema Gestione Aziendale Protezione Dati Personali
GDPR	General Data Protection Regulation (Regolamento generale sulla protezione dei dati)
DPO/RPD	Data Protection Officer /Responsabile Protezione Dati

RSI	Responsabile Sicurezza Informatica
ADS	Amministratore Di Sistema
SI	Sistema Informativo
Definizione	
Dati personali	Informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

4 ORGANIGRAMMA DEL SGA PDP

Viene di seguito rappresentato **l'organigramma** del Sistema di Gestione Aziendale Protezione Dati Personali (SGA PDP)



5 DESCRIZIONE DI COMPITI E RESPONSABILITA'

Il **Titolare del trattamento (AULSS 6 Euganea)** per la messa in atto degli obblighi derivanti dalla normativa in materia di trattamento dati personali (Regolamento Europeo 2016/679 e Codice Privacy Adeguato di cui al D.Lgs 101/2018) definisce il proprio modello di sistema denominato **Sistema Gestione Aziendale Protezione Dati Personali (SGA PDP).**

Nell'ambito del SGA PDP il Titolare del trattamento affida:

- **all'Ufficio Protezione Dati Personali - PDP -** (ex Ufficio Privacy), incardinato nell'UOC Affari Generali, la competenza in merito all'adeguamento derivante dagli obblighi della normativa europea (Regolamento UE 20167679) e al monitoraggio sullo stato di mantenimento del SGA PDP;
-
- **al DPO/RPD** la competenza di monitorare l'applicazione del Regolamento Europeo (UE) 2016/679 e di quello aziendale con funzioni specifiche di: consulenza, informazione, verifica e audit, pareri sulla valutazione d'impatto per i diritti e le libertà degli interessati, cooperazione con le autorità di controllo. Il DPO/RPD riferisce direttamente al vertice gerarchico del titolare/responsabile e svolge la duplice funzione di auditor e advisor. Svolge inoltre attività di sensibilizzazione e formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

- **ai Delegati / Preposti del trattamento** (Direttori e Responsabili UOC / UOSD / UOS di Staff) le funzioni di organizzazione e gestione del trattamento dei dati personali nell'ambito dei processi direttamente governati nonché di autorizzazione del personale diretto ai diversi livelli di trattamento secondo quanto indicato nell'atto di delega. In particolare viene loro affidata, al momento della sottoscrizione di contratti/convenzioni per acquisizione di beni e/o servizi, che prevedono il trattamento di dati personali, il compito di nominare Responsabili del Trattamento i relativi fornitori, nelle modalità descritte nella specifica procedura aziendale;

- **agli Autorizzati del trattamento** (dipendenti e collaboratori a qualsiasi titolo) il trattamento dei dati personali nello svolgimento delle attività operative quotidiane secondo quanto impartito dal Delegato / Preposto del Trattamento;

- **ai Responsabile del trattamento** - qualora un trattamento debba essere effettuato per conto del titolare - la messa in atto di misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato, nonché, qualora a sua volta il responsabile del trattamento debba ricorrere a un altro responsabile, l'acquisizione della preventiva autorizzazione scritta, specifica o generale, del titolare.

- **agli Amministratori di Sistema – ADS -**(autorizzati al trattamento con funzioni particolari) i compiti di gestione e manutenzione del sistema informatico, telematico e delle banche dati aziendali compresa l'implementazione di misure di sicurezza e backup e il supporto alle attività di disaster recovery;

- **al Team multidisciplinare,** in un'ottica multidisciplinare tecnica/giuridica, vengono attribuite funzioni di analisi, evoluzione del contesto, pianificazione, supporto, valutazione, raccolta

criticità e proposte di miglioramento del Sistema SGA PDP in appoggio dell'Ufficio SGA PDP e in condivisione con il DPO/RPD, in linea con il principio di responsabilizzazione sancito dal Reg. UE 679/2016 (GDPR) che, anche alla luce dei più recenti provvedimenti dell'Autorità Garante per la Protezione dei dati personali in materia, deve essere delineato in una prospettiva giuridica (artt.5 par.2 e 24 GDPR) come in una più moderna dimensione tecnologica (art. 25 GDPR);

- **al Responsabile della Sicurezza Informatica -** RSI **-** (Direttore UOSD Sistemi Informativi) il compiti di implementare e garantire le misure di sicurezza informatica previste dalle normative e linee guide nazionali (es. AGID), necessarie a garantire la protezione dei dati personali trattati dall'azienda;

- **Al Responsabile Transizione Digitale** (Direttore UOSD Sistemi Informativi) il compito di garantire operativamente la trasformazione digitale dei processi aziendali, coordinando lo sviluppo dei servizi e di nuovi modelli di relazione con i cittadini anche in relazione al trattamento dei dati personali**.**

6 DOCUMENTI A SUPPORTO DEL SISTEMA

La base documentale a supporto del mantenimento del SGA PDP è costituita da:

- Il **Manuale del Sistema SGA PDP** (ISO:9001 – 27001 - PDR 43) con policy e procedure/istruzioni operative del SI (manuale della sicurezza delle informazioni), con policy e procedure/istruzioni operative del DPO e dell'Ufficio PDP;
- Il **Regolamento Aziendale trattamento dati personali** (per l'applicazione del Regolamento Europeo (UE) 2016/679, Codice Privacy Adeguato di cui al D.Lgs 101/2018);
- Il **Regolamento per la ripresa di immagini** nelle strutture dell'AULSS 6 EUGANEA;
- Il **Registro dei trattamenti dati personali aziendali** (ex art. 30 del Regolamento UE 2016/679);
- Il **Regolamento sull'utilizzo degli strumenti informatici**;
- Ogni altra **procedura/Istruzione operativa aziendale** in materia di gestione e protezione dei dati.

7 NORMATIVA DI RIFERIMENTO

- Regolamento (UE) 2016/679 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("Regolamento Generale sulla Protezione dei Dati personali");
- Codice Privacy adeguato di cui al D.Lgs 101/2018;
- Linee guida AgiD;
- Circolari AgID n° 1 e 2/2018;
- Piani triennali AgID.
- Delibera n° 520 del 22/07/2020 Adozione Piano Operativo per l'applicazione di alcuni adempimenti previsti dal Regolamento Europeo (UE) 2016/679 in materia di trattamento dati personali.

REGIONE DEL VENETO

ULSS6 EUGANEA

ATTESTAZIONE DI PUBBLICAZIONE

La presente deliberazione è stata pubblicata all'Albo On-line di questa ULSS 6 per 15 giorni consecutivi dal 02-05-2022

Il Direttore
U.O.C. Affari Generali
(Dott. Tullio Zampieri)

CERTIFICAZIONE DI ESECUTIVITA'

La presente deliberazione è divenuta esecutiva il 02-05-2022

Il Direttore
U.O.C. Affari Generali
(Dott. Tullio Zampieri)

Copia composta di n. 0012 fogli (incluso il presente) della delibera n. 323 del 29-04-2022 firmata digitalmente e conservata secondo la normativa vigente presso Infocert S.p.a.

Padova, li 02-05-2022

Il Direttore
U.O.C. Affari Generali
(Dott. Tullio Zampieri)
