Delibera firmata digitalmente

Azienda USL Toscana sud est
Servizio Sanitario della Toscana

DELIBERAZIONE DEL DIRETTORE GENERALE

N° 332 DEL 28/02/2019

Il Direttore Generale, Dott. Enrico Desideri
su proposta della struttura aziendale
U.O.C Privacy e Internal Audit

adotta la seguente deliberazione:

OGGETTO: Adeguamento Sistema Aziendale Data Protection-determinazioni

Responsabile della struttura proponente: Salvi Paola

Responsabile del procedimento: Salvi Paola

Il Dirigente e/o il Responsabile del Procedimento sottoscrive la proposta di delibera di pari oggetto con num. Provv. 963

Hash .pdf (SHA256):
6e50f0c8a62a89062dbac63aa6a8e37b400db203a14ab568d8b2110ca842adc4
Hash .p7m (SHA256):
d6c92879222ea450a140f2a9b088f81134f7c06e5ad6ee16486e6ba3503fc036

Azienda USL Toscana sud est
Servizio Sanitario della Toscana

Adeguamento Sistema Aziendale Data Protection: determinazioni

IL DIRETTORE DELLA U.O.C. PRIVACY E INTERNAL AUDIT- Responsabile della Protezione dei Dati Personali

VISTO il D.Lgs. 30 dicembre 1992, n. 502 "Riordino della disciplina in materia sanitaria, a norma dell'articolo 1 della Legge 23 ottobre 1992, n. 421 ";

VISTA la L.R. Toscana 24 febbraio 2005, n. 40 "Disciplina del servizio sanitario regionale "e s.m.i.;

VISTE le deliberazioni del Direttore Generale:

- n. 872 del 22 luglio 2016 avente ad oggetto "Approvazione schema dello Statuto dell'Azienda USL Toscana Sud Est";
- n. 873 del 22 luglio 2016 avente ad oggetto "Approvazione schema del Regolamento di Organizzazione dell'Azienda USL Toscana Sud Est ";
- n. 876 del 22 luglio 2016 avente ad oggetto "Seconda applicazione Regolamento Aziendale di organizzazione. Nomina incarichi di staff, amministrativi e tecnici";
- n. 1102 del 29 settembre 2016 avente ad oggetto "Approvazione del documento denominato Funzioni operative delle Strutture di Staff, dei Dipartimenti Amministrativi e Tecnici";
- n. 106 del 7 febbraio 2017, avente ad oggetto: "Revisione del documento denominato "Funzioni operative delle Strutture di Staff, dei Dipartimenti Amministrativi e Tecnici" e modifiche alla Deliberazione D.G. N. 876 del 22.07.2016"
- n. 215 del 15 marzo 2017 avente ad oggetto "Staff Direzione Aziendale – Nuovo assetto organizzativo interno".
- n. 240 del 16 marzo 2017 avente ad oggetto "Integrazione del documento denominato Funzioni operative delle Strutture di Staff, dei Dipartimenti Amministrativi e Tecnici con riferimento alle funzioni dei Servizi Sociali";
- n. 858 del 18 ottobre 2017 avente ad oggetto "Revisione del documento denominato "Funzioni operative delle Strutture di Staff, dei Dipartimenti Amministrativi e Tecnici e dei servizi Sociali;
- n. 123 del 9 febbraio 2018 avente a oggetto "Revisione organizzativa interna agli Staff ed alla Direzione Amministrativa",

PRESO ATTO che:

- il Parlamento europeo ed il Consiglio in data 27.4.2016 hanno approvato il Regolamento UE 2016/679 (Regolamento Generale sulla Protezione dei Dati- RGPD) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;

- il Regolamento, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, è in vigore dal 24 maggio 2016 ed è divenuto definitivamente applicabile in via diretta in

tutti i Paesi UE a partire dal 25 maggio 2018;

PRESO ATTO, altresì, che in data 19 settembre 2018 è entrato in vigore il decreto legislativo 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE/2016/679" e che, pertanto, il quadro normativo di riferimento in materia di protezione dei dati risulta costituito, a oggi:

- dalle disposizioni del Regolamento (UE) 2016/679 Regolamento Generale sulla Protezione dei Dati "RGPD"
- dalle disposizioni del Decreto Legislativo n. 196 del 30 giugno 2003, meglio noto come «Codice Privacy», novellato dal Decreto Legislativo n. 101/2018 e ridenominato "*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE)n. 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*".

EVIDENZIATO che tale quadro normativo risulta a tutt'oggi *in fieri* in riferimento alle seguenti nuove tipologie di atti normativi, rientranti in quella che è stata definita *soft law.*

- i "Codici di condotta"di cui al l'art. 40 del RGPD;
- le Regole deontologiche ex art. 2 *quater* d.lgs n. 196/2003 la cui adozione è prevista, tra l'altro, per il trattamento di dati biometrici, genetici o relativi allo stato di salute (art. 9 par. 4 RGPD) ed è promossa dal Garante sulla base del principio di rappresentatività;
- le Misure di garanzia per il trattamento di dati biometrici, genetici e relativi alla salute ex art. 2 *septies* d.lgs n. 196/2003, che demanda al Garante il compito di disporre appositi provvedimenti, con cadenza biennale, che hanno la funzione di indicare misure ed accorgimenti da adottare nei trattamenti, sulla base delle linee guida, raccomandazioni e prassi pubblicate dal Comitato europeo e delle altre migliori prassi in materia di trattamento dei dati personali, nonché tenendo in considerazione l'evoluzione tecnologica e scientifica.Tali misure di garanzia sono espressamente previste per i trattamenti in ambito sanitario (art. 75 d.lgs n. 196/2003),
- i Provvedimenti di carattere generale ex art. 2 *quinquiesdecies* d.lgs n. 196/2003, adottati dal Garante in riferimento ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico e che possono presentare rischi elevati ai sensi dell'art. 35 del RGPD.

DATO ATTO che nell'attuale fase transitoria, oggettivamente caratterizzata da ambiti di incertezza interpretativa e in attesa dell'efficacia delle varie tipologie di provvedimenti sopra citati, è' stato comunque avviato un percorso applicativo che, con il coinvolgimento di tutte le articolazioni aziendali e con il supporto delle necessarie professionalità anche esterne all'Azienda (ESTAR), si prefigge di strutturare le soluzioni organizzative, funzionali, procedurali a presidio stabile di un Sistema Aziendale Data Protection RGPD compliant;

RILEVATO che :

- le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono, fin da subito, considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di trattamento dati personali ;

- appare necessario ed opportuno stabilire modalità organizzative, misure procedimentali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano all'Azienda

di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE;

EVIDENZIATO che la principale novità introdotta dal Regolamento è il principio di "responsabilizzazione" (cd. accountability), che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali (art. 5) e che in quest'ottica, la nuova disciplina impone alle amministrazioni un diverso approccio nel trattamento dei dati personali, prevedendo nuovi adempimenti e richiedendo un'intensa attività di adeguamento;

DATO ATTO che la responsabilizzazione del titolare si realizza anche mediante:

- la concreta adozione, sia al momento della determinazione dei mezzi del trattamento che all'atto del trattamento stesso, di misure tecniche e organizzative adeguate ed efficaci, che tengano conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché del rischio per i diritti e le libertà delle persone fisiche (c.d. privacy by design);
- l'adozione di misure tecniche ed organizzative adeguate che garantiscano che siano trattati soltanto i dati personali necessari per ogni finalità di trattamento (c.d. privacy by default);
- l'individuazione di un Responsabile della Protezione dei dati (RPD) che, tra le altre funzioni, dà indicazioni e vigila sulla corretta osservanza del RGPD all'interno dell'organizzazione del titolare;

RICHIAMATO l'art.37, paragrafo1, lett a) del RGPD che prevede l'obbligo per il titolare del trattamento di nominare il Responsabile della Protezione dei Dati, nel seguito indicato con la sigla RPD, "*quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, ...*"

RICHIAMATA la nota della Regione Toscana, Direzione Diritti di Cittadinanza e Coesione sociale, prot.n.AOOGRT_0168453 del 26/3/2018, conservata agli atti, avente ad oggetto "*Regolamento 2016/679/UE in materia di protezione dei dati personali. Indicazioni alle aziende e agli enti del Servizio Sanitario regionale*", con la quale:

- vengono fornite indicazioni per la nomina, precisati i compiti e le garanzie essenziali per consentire al Responsabile della protezione dei dati personali di operare con un grado di sufficiente autonomia all'interno delle organizzazioni del titolare;
- viene richiesto ad Estar, titolare delle competenze in materia di ICT, che "garantisca la funzione, opportunamente dimensionata, di referenza tecnico informatica per la protezione dei dati personali a supporto delle Aziende sanitarie, in diretta collaborazione con il Responsabile della protezione dati dell'Azienda" affinché sia assicurata la conformità al RGPD dell'intero sistema Information and Communication Tecnology (ICT) aziendale, in particolare nell'adozione delle misure tecniche necessarie

RICHIAMATE le seguenti note inviate dal Direttore dello Staff Direzione Aziendale a Estar, conservate agli atti:

- nota prot. n. 0038277 del 26/0272018 "*Richiesta elenco Società fornitrici in ambito ICT e tecnologie sanitarie*";
- nota prot. n.0083490 del 7/0572018 "*Adempimenti GDPR: ricognizione di applicativi, misure di sicurezza attuali e necessità di adeguamento*"

VISTA la nota conservata agli atti (prot. AUTSE n. 0096147 del 24/05/2018) con la quale il Direttore Generale di ESTAR comunica alle Aziende Sanitarie le attività in corso di svolgimento, tra le quali, in particolare *"un percorso di confronto con i fornitori di software per verificare l'adeguamento dei loro gestionali al GDPR"*; l'istituzione dei *"gruppi di lavoro che stanno predisponendo i documenti con l'analisi del rischio per le varie AASS"*; l'individuazione dei dirigenti ESTAR a supporto dei RPD delle Aziende Sanitarie, suddivisi per Area Vasta;

RICHIAMATA la Deliberazione del Direttore Generale n. 491 del 21 maggio 2018 con la quale l'Azienda ha provveduto a nominare il Responsabile della Protezione dei Dati personali (di seguito RPD),affidandogli, tra gli altri, i seguenti compiti:

- definizione di un piano di azioni per la piena applicazione del Regolamento (UE) 2016/679 e della normativa di riferimento per l'Azienda Usl Toscana sud est avvalendosi delle strutture aziendali sia in relazione ai trattamenti di cui sono responsabili che in riferimento a specifici ambiti di professionalità di volta in volta necessari;
- tenuta e implementazione, in nome e per conto del titolare, del registro delle attività di trattamento di cui all'art. 30 del Regolamento, con il supporto e la costante collaborazione dei responsabili aziendali del trattamento in relazione ai processi di trattamento di rispettiva afferenza/conoscenza nonché con l'apporto delle competenti strutture aziendali in riferimento a specifici ambiti di professionalità di volta in volta necessari;

DATO ATTO che in assolvimento a quanto previsto dall'art. 37, paragrafo 7, del RGPD, i dati di contatto del RPD sono stati pubblicati nel sito web istituzionale dell'Azienda e sono stati comunicati al Garante per la protezione dei dati personali mediante la piattaforma on line resa disponibile dal Garante stesso e dallo stesso Garante confermati, con pec del 28/5/2018 conservata agli atti;

DATO ATTO della nota prot GEN/0212700/U del 30 novembre 2018, con la quale il RPD ha trasmesso alla Direzione aziendale un primo modello di Registro delle attività di trattamento del Titolare idoneo a soddisfare il debito informativo ex art. 30 Reg. UE 2016/679;

DATO ATTO che il Registro di cui sopra è per sua natura dinamico e soggetto ad aggiornamento, in relazione sia all'attivazione di nuovi trattamenti sia all' ulteriore specificazione delle attività di trattamento già individuate e che, in particolare, il registro sarà integrato con l'indicazione delle banche dati/applicativi riferibili alle attività di trattamento e con la descrizione delle misure di sicurezza tecniche in essere, non appena ricevuto l'esito della ricognizione richiesta a ESTAR con nota prot. n. 0083490 del 7 maggio 2018, conservata agli atti;

RICORDATO che nella più sopra citata nota della Regione Toscana, è previsto che l'Ente di Supporto Tecnico-Amministrativo Regionale (ESTAR), cui la Regione Toscana ha allocato le competenze ICT, assicuri al Titolare del trattamento e al RPD la referenza tecnico-informatica per la funzione ICT, opportunamente dimensionata, a supporto e in diretta collaborazione con il RPD, affinché sia assicurata la conformità al RGPD dell'intero sistema Information and Communication Tecnology (ICT) aziendale, in particolare nell'adozione delle misure tecniche necessarie;

VISTA la nota conservata agli atti (prot. AUTSE n. 0096147 del 24/05/2018) con la quale il Direttore Generale di ESTAR comunica alle Aziende Sanitarie le attività in corso di svolgimento,

tra le quali, in particolare *"un percorso di confronto con i fornitori di software per verificare l'adeguamento dei loro gestionali al GDPR"*; l'istituzione dei *"gruppi di lavoro che stanno predisponendo i documenti con l'analisi del rischio per le varie AASS"* l'individuazione dei dirigenti ESTAR a supporto dei RPD delle Aziende Sanitarie, suddivisi per Area Vasta;

RICHIAMATA la Deliberazione del Direttore Generale DG n. 1194 del 13 novembre 2018 con la quale l'Azienda ha proceduto alla nomina di Estar quale Responsabile del trattamento dei dati personali mediante stipula con lo stesso di convenzione secondo lo schema di cui alla DGRT n. 742/2018 adeguato nei riferimenti normativi alla luce dello *ius superveniens*, in riferimento ai trattamenti di dati riportati nel registro delle attività di trattamento di ESTAR quale responsabile del trattamento allegato allo stesso atto convenzionale;

RITENUTO necessario, assumere, con il presente atto, determinazioni inerenti l'assetto organizzativo e la funzionalità del Sistema Aziendale Data Protection, quali azioni di adeguamento al RGPD al fine di rispettarne gli obblighi organizzativi, documentali e tecnici, con l'obiettivo di attuare la piena e consapevole applicazione del nuovo quadro normativo in materia di trattamento dei dati personali;

PRESO ATTO che

- l'art. 28 del RGPD prevede e disciplina la figura del Responsabile del trattamento unicamente quale figura esterna, distinta e separata dall'organizzazione del Titolare

- i previgenti artt. 29 "Responsabile del trattamento" e 30 "Incaricati del trattamento" del D. lgs n. 196/2003 sono stati abrogati per effetto delle modifiche apportate al decreto dal D.lgs 10 agosto 2018, n. 101;

PRESO ATTO che il vigente quadro normativo a fondamento dei ruoli privacy e delle connesse responsabilità all'interno dell'organizzazione del titolare risulta costituito:

- dalle previsioni del RGPD, per le quali chiunque agisca sotto l'autorità del titolare e "…. *abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento*2 (art. 29) e il "*il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro responsabilità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento*…." (art. 32 , paragrafo 4);
- dall'art. 2 *quaterdecies* del d.Lgs. 196/2003, introdotto dal d.lgs 101/2018 e rubricato "Attribuzione di funzioni e compiti a soggetti designati" il quale dispone che :
  - il titolare o il responsabile del trattamento del trattamento possano prevedere,sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità;
  - il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta;

RITENUTO necessario, alla luce del mutato quadro normativo di riferimento, adeguare il sistema aziendale dei ruoli e delle correlate responsabilità in ordine al trattamento dei dati definito con la deliberazione DG n. 546 del 14 giugno 2017 "Sistema aziendale delle responsabilità in ordine al trattamento di dati personali-determinazioni";

RITENUTO che i soggetti autorizzati al trattamento per espressa designazione del titolare ex art. 2 *quaterdecies,*comma 1, d.lgs. 196/2003,siano da identificarsi in livelli organizzativi caratterizzati da margini di autonomia gestionale e operativa anche rispetto alla specificità dei compiti e delle funzioni connessi al trattamento

di dati;

ATTESO,pertanto, di individuare i soggetti designati al trattamento in correlazione ai seguenti livelli direzionali e tipologie di incarico di direzione di struttura:
Direttore Sanitario
Direttore Amministrativo
Direttore dei Servizi sociali
Direttore di Dipartimento
Direttore di Area Funzionale Dipartimentale
Direttore di Staff
Direttore di Area di Staff
Direttore di Presidio Ospedaliero
Responsabile di Stabilimento Ospedaliero
Direttore di Zona distretto
Direttore di Unità Operativa complessa
Direttore di Unità Operativa Semplice Dipartimentale
Direttore di Unità Funzionale

RITENUTO opportuno:

- denominare i soggetti di cui sopra quali "Preposti al trattamento" in riferimento ai trattamenti di dati personali in atto o successivamente attivati nell'ambito dell'incarico o dell'unità organizzativa di competenza , in sostituzione della denominazione "Responsabili aziendali del trattamento" di cui alla citata deliberazione n. 546/2017:
- specificare compiti e funzioni dei Preposti in relazione al trattamento di dati nel documento allegato sub A) al presente atto;
- stabilire che i Preposti procedano a nominare "Incaricati del trattamento dei dati"i dipendenti/collaboratori ad altro titolo operanti all'interno delle rispettive strutture e sotto le proprie direttive, quali soggetti autorizzati al trattamento di dati personali nell'ambito delle loro specifiche competenze, secondo le istruzioni specificate nell'Allegato B);
- stabilire che l'elenco nominativo dei Preposti al trattamento dati personali sia pubblicato del sito web aziendale nell'apposita sezione "Privacy in Azienda" e periodicamente aggiornato

ATTESO che i Preposti e Incaricati al trattamento dei dati personali sono tenuti a collaborare con il Titolare e con il Responsabile per la protezione dei dati personali per tutte le attività obbligatorie di adeguamento alla nuova normativa europea, nonché alle disposizioni normative nazionali ed alle linee guida dell'Autorità Garante per la protezione dei dati personali ;

DATO ATTO che l'Azienda si riserva di designare al proprio interno ulteriori Preposti al trattamento tra coloro che rivestono altra tipologia di incarico rispetto a quelle sopra individuate, in ragione della particolare natura dell'attività di competenza o tenuto conto di specifici e peculiari ambiti o modalità di trattamento correlati all'incarico ricoperto;

DATO ATTO, in particolare, che:

- in riferimento alla conduzione di studi osservazionali o sperimentazioni cliniche è designato quale Preposto al trattamento lo sperimentatore principale che coordina il gruppo di professionisti impegnati nello studio/sperimentazione

- in riferimento allo svolgimento dell'attività libero-professionale *intramoenia* è designato quale Preposto al trattamento il dirigente sanitario autorizzato allo svolgimento dell'attività;

DATO ATTO, altresì, che nelle more dell'adozione del regolamento dei sistemi di videosorveglianza/videocontrollo dell'Azienda Usl Toscana sud est, per quanto concerne la responsabilità del trattamento dei dati correlata agli impianti attualmente installati si intendono integralmente confermate le disposizioni regolamentari e le determinazioni organizzative in vigore nei rispettivi ambiti territoriali delle ex Aziende UU.SS.LL. 7 Siena, 8 Arezzo, 9 Grosseto, peraltro intendendosi sostituita ogni attuale denominazione con quella di Preposto al trattamento

ATTESO di stabilire, riguardo le tipologie di incarico di struttura cui è correlata il ruolo di Preposto al trattamento, che nel caso di struttura organizzativa temporaneamente vacante tale ruolo è da intendersi in capo al livello organizzativo immediatamente sovraordinato;

RITENUTO di disporre che, a decorrere dall'esecutività del presente atto, la designazione a Preposto al trattamento di dati personali sia effettuata nello stesso provvedimento di conferimento dell'incarico di direzione (quale "titolare", "ad interim","sostituto")delle tipologie di struttura individuate dal presente atto, a cura delle strutture aziendali competenti alla predisposizione dei provvedimenti di attribuzione di detti incarichi, contestualmente allegando al provvedimento il documento "Compiti e funzioni dei Preposti al trattamento di dati" allegato sub A) al presente atto;

ATTESA la necessità, anche in ragione della scala territoriale e della complessità organizzativa dell'Azienda , di individuare soluzioni atte a supportare il Titolare nell'assolvimento degli obblighi normativamente previsti di vigilanza, verifica e controllo sulla puntuale osservanza da parte dei Preposti al trattamento delle vigenti disposizioni in materia di trattamento, compreso il livello di sicurezza adeguato al rischio, e delle istruzioni impartite dal Titolare stesso;

RITENUTO, pertanto, di delegare ai Direttori delle strutture funzionali di massima dimensione (Staff, Dipartimento, Presidio Ospedaliero, Zona Distretto), denominati Preposti Referenti, lo svolgimento delle seguenti funzioni per conto del Titolare:

- coordinamento dei Preposti al trattamento afferenti la macrostruttura, al fine garantire omogeneità di comportamenti e procedure/soluzioni organizzative condivise in applicazione della normativa in materia di protezione dei dati personali
- trasmissione ai Preposti al trattamento afferenti la macrostruttura di ogni comunicazione/circolare/nota pervenuta dal Titolare o dal Responsabile della Protezione dei Dati,
- vigilanza, monitoraggio e controllo sulla corretta applicazione da parte dei Preposti al trattamento afferenti la macrostruttura delle disposizioni del RGPD e del d.lgs 196/2003, delle prescrizioni dell'Autorità Garante, delle istruzioni/ direttive impartite dal Titolare e/o dal Responsabile della Protezione dei Dati;

RITENUTO di prevedere, quale misura organizzativa a supporto del Preposti Referenti la figura del Referente Data Protection di macrostruttura, focal point della macrostruttura di riferimento nella gestione operativa delle attività connesse al trattamento dei dati con, in particolare, i seguenti compiti:

- supporto all'implementazione e aggiornamento del Registro delle attività di trattamento,anche mediate

apposito applicativo
supporto nei processi di analisi del rischio e di valutazione dell'impatto sullla protezione dei dati - VIP(Data Protection Impact Assessment - DPIA) previsti dal RGPD

- supporto alla stesura/adeguamento modulistica,policy, procedure, istruzioni operative per la compliance al RGPD
- supporto ricognizione/analisi/ contratti in essere ed eventuale adeguamento
- supporto alle verifiche periodiche di compliance al RGPD
- supporto nella individuazione delle soluzioni più opportune al fine di garantire i processi di informazione e di acquisizione del consenso
- collegamento con il RPD nelle fasi di formulazione della richieste dei pareri e nelle richieste di consulenza nei casi previsti dal GDPR
- collaborazione /supporto in tutte le fasi relative alla rilevazione e gestione delle violazioni di dati (cd data breach)
- collaborazione con i Referenti Data Protection delle altre macrostrutture al fine di condividere problemi e soluzioni

EVIDENZIATO che l'art. 28 del RGPD prevede e disciplina la figura del Responsabile del trattamento unicamente quale figura esterna, distinta e separata dall'organizzazione del Titolare e, in particolare, :

- fissa dettagliatamente e caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel Regolamento;
- consente la nomina di sub-responsabili del trattamento da parte di un responsabile (art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario;
- prevede in capo ai responsabili del trattamento obblighi specifici, distinti da quelli pertinenti i rispettivi titolari. Ciò riguarda, in particolare, la tenuta del registro dei trattamenti svolti (ex art. 30, paragrafo 2) e l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32).

RITENUTO necessario, alla luce di quanto sopra, adeguare al mutato scenario normativo le modalità di individuazione del "Responsabile del trattamento" nei casi di affidamento a terzi, persone fisiche o persone giuridiche, di attività/funzioni/servizi che comportano il trattamento di dati personali nella Titolarità dell'Azienda;

PRESO ATTO che nelle more della messa a disposizione da parte dell'Autorità Garante per la protezione dei dati personali di uno schema-tipo di atto di nomina del Responsabile del trattamento, il RPD ha predisposto e messo a disposizione delle strutture aziendali che stipulano contratti /convenzioni con soggetti esterni all'azienda (nota prot. n. 0167633/U del 20.9.2018) uno schema di atto giuridico per la nomina del Responsabile in sostituzione dell'atto di nomina in uso in Azienda ai sensi della previgente normativa;

ATTESA l'opportunità di integrare nello schema di atto di nomina attualmente in uso contenuti ulteriori ai fini della gestione operativa del cd. data breach;

PRESO ATTO dello schema di atto giuridico per la nomina del Responsabile predisposto dal Responsabile della Protezione dei Dati, allegato sub C) al presente atto;

DATO ATTO di riservarsi di modificare lo schema di cui al punto precedente in conformità a sopraggiunte disposizioni normative europee, nazionali, o linee guida emanate dell'Autorità Garante per la protezione dei dati personali;

ATTESO di stabilire che :

- ove la sottoscrizione dell'atto sia contestuale a quella del contratto/ convenzione cui accede quale parte integrante e sostanziale, vi provveda lo stesso soggetto che ha facoltà di sottoscrivere il contratto/convenzione come da specifica delega del Direttore Generale;
- ove la sottoscrizione dell'atto sia disgiunta da quella del contratto/ convenzione cui accede, è delegato alla firma ogni dirigente designato Preposto al trattamento per i contratti/convenzioni di cui è RES, per quelli le cui funzioni di RES afferiscono alla propria struttura e per quelli riferiti agli ambiti di attività istituzionale di propria competenza;
- in ogni altro caso diverso da quelli di cui ai punti precedenti la nomina di soggetti terzi a Responsabil è delegata al Direttore dello Staff della Direzione Aziendale

VALUTATO necessario, alla luce delle innovazioni normative nonché della dimensione e complessità organizzativo funzionale dell'Azienda, inserire nel Sistema Aziendale Data Protection
un organismo di data governance connotato da pluralità di esperienze, conoscenze e competenze cui affidare il compito di sistematizzare le azioni per l'adeguamento del Sistema alle disposizioni normative, la manutenzione, la documentabilità e il controllo del Sistema stesso in riferimento ai seguenti asset:

- area sanitaria, con particolare riferimento ai requisiti dei processi sanitari, alle esigenze mediche e assistenziali e al rischio clinico
- area amministrativa
- area di implementazione e gestione del sistema informativo, dell'infrastruttura tecnologica e dei dispositivi medici;

RITENUTO pertanto di istituire il "Comitato Data Protection", organismo tecnico permanente di natura interdisciplinare con compiti di indirizzo, coordinamento , analisi e controllo coerenti con il principio di "accountability" previsto dal RGPD in capo al Titolare, e con funzioni operative di supporto e proposta al Titolare di soluzioni ai problemi applicativi del Regolamento (UE) 2016/679, nella seguente composizione:

- Direttore Staff Direzione Aziendale o suo delegato, con funzione di coordinatore
- dirigente medico dello Staff del Direttore Sanitario (designazione del Direttore dello Staff)
- personale (dirigente e/o non dirigente), con esperienza professionale e conoscenza dei processi sanitari, tecnici e dei principali sistemi applicativi in uso in ambito ospedaliero (designazione del direttore della Rete Ospedaliera)
- personale (dirigente e/o non dirigente), con esperienza professionale e conoscenza dei processi sanitari, tecnici e dei principali sistemi applicativi in uso in ambito territoriale (designazione del Direttore del Dipartimento Territoriale);
- personale (dirigente e/o non dirigente) delle professioni infermieristiche e ostetriche, delle professioni tecnico-sanitarie e della riabilitazione e della prevenzione (designazione del rispettivo Direttore di Dipartimento);
- personale (dirigente e/o non dirigente), con esperienza professionale e conoscenza dei processi amministrativi a supporto dei percorsi sanitari(designazione del Direttore Amministrativo);
- personale (dirigente e/o non dirigente), con competenze in ambito gestionale e di project management (designazione del Direttore Staff Direzione Aziendale);
- Responsabile della protezione dei dati personali (RPD), per lo svolgimento delle funzioni di cui all'art. 39 del RGDP e Deliberazione aziendale n.491/2018 citata;

RITENUTO di prevedere che il "Comitato Data Protection" si avvalga nell'esercizio delle sue funzioni dell'ausilio di ogni ulteriore specifica professionalità presente in Azienda nonché della collaborazione dei dirigenti tecnico-informatici individuati da ESTAR a supporto del Responsabile della protezione dei dati personali per l'Area Vasta Sud Est;

ATTESO che il Comitato è responsabile di

- promuovere l'osservanza del RGPD e delle disposizioni nazionali in materia di protezione dei dati fornendo consulenza alle varie aree dell'organizzazione e assicurando una visione complessiva e integrata di tutte le esigenze
- promuovere, predisporree/o validare la documentazione di riferimento del Sistema Aziendale Data Protection
- validare le procedure organizzative rilevanti in termini di protezione dei dati personali, definite dal titolare in merito all'esecuzione dei vari trattamenti, sia per le attività informatizzate che manuali;
- disciplinare e pianificare verifiche periodiche sul Sistema Data Protection, analizzare gli esiti delle verifiche, definire/validare gli eventuali interventi correttivi
- monitorare, valutare periodicamente il Sistema e proporre alla Direzione i piani evolutivi necessari per assicurarne conformità, adeguatezza ed efficacia rispetto al quadro normativo tenuto conto dei rischi dei vari settori e delle priorità dell'organizzazione;

RITENUTO di individuare quali prioritari nell'azione del Comitato i seguenti ambiti:

- definizione procedura per la gestione del processo di Valutazione di Impatto sulla Protezione dei dati (VIP) o Data Protection Impact Assessment (DPIA) di cui all'art. 35 RGPD;
- implementazione e aggiornamento del registro delle attività di trattamento;
- definizione fabbisogni e modalità interventi formativi
- linee guida per l'analisi del rischio (art. 32 RGPD), attività funzionale al mantenimento della sicurezza e alla prevenzione di trattamenti in violazione delle prescrizioni del RGPD;
- definizione procedura aziendale in caso di violazione dei dati personali (c.d. data breach)
- modalità di implementazione e aggiornamento del Registro delle attività di trattamento;
- predisposizione/revisione regolamenti e policy (sistema di videosorveglianza, modalità di utilizzo strumenti informatici, etc.);
- revisione/adeguamento informative riferite ad ambiti specifici di attività;
- definizione modalità attivazione, gestione e utilizzo Dossier Sanitario Aziendale (D.S.A)

RITENUTO di approvare il documento "Schema della procedura aziendale in caso di violazione dei dati personali (c.d. data breach)" predisposto dal RPD e allegato sub D) al presente atto, rimettendolo alla valutazione e validazione da parte del Comitato;

DATO ATTO che l'Azienda è componente del "Tavolo regionale privacy Regione Toscana/Enti e aziende del Servizio sanitario regionale",composto dagli RPD di tutti gli attori del SSR, di Estar e della Regione, istituito con decreto dirigenziale regionale n. 7375/2017 con il mandato di definire linee di indirizzo regionali per governare in maniera condivisa e sinergica l'applicazione del nuovo impianto regolatorio in materia di protezione dei dati, e la cui agenda di lavoro prevede due incontri mensili e un'intensa attività istruttoria e di analisi preliminare alla trattazione delle questioni all'ordine del giorno;

DATO ATTO che il Tavolo regionale è stato anche lo strumento utilizzato dal gruppo degli RPD delle Aziende e di ESTAR, di concerto con ESTAR –ICT, per affrontare congiuntamente la valutazione delle funzionalità e dei requisiti di un applicativo a supporto dei rispettivi titolari per la gestione degli adempimenti previsti dal RGPD, in previsione dell'opportunità di convergere, in una logica di sistema, sullo stesso prodotto;

DATO ATTO che della esiti della valutazione condotta dal gruppo di cui sopra sono stati formalmente trasmessi a ESTAR-ICT perché si attivi ai fini dell'acquisizione dell'applicativo, onde poterne avviare in tempi rapidi l'implementazione e formare il personale coinvolto nell'utilizzo della piattaforma (RPD, Preposti al Trattamento, Referenti Data Protection di macrostruttura etc.) ;

ATTESTATA la legittimità e la regolarità formale e sostanziale della presente proposta;

PROPONE AL DIRETTORE GENERALE

Per quanto espresso in premessa, che qui si intende integralmente riportato:

A. **DI DARE ATTO** della nomina del Responsabile della protezione dei dati personali con Deliberazione n.491/2018, della pubblicazione dei dati di contatto del RPD nel sito istituzionale dell'Azienda e dell'avvenuta comunicazione al Garante per la protezione dei dati personali

B. **DI DARE ATTO** che con nota prot GEN/0212700/U del 30 novembre 2018, il Responsabile della protezione dei dati personali ha trasmesso alla Direzione aziendale un primo modello di registro delle attività di trattamento del Titolare idoneo a soddisfare il debito informativo ex art. 30 Reg. UE 2016/679- RGPD;

C. **DI ADEGUARE** il sistema aziendale dei ruoli e delle correlate responsabilità in ordine al trattamento dei dati alla luce del combinato disposto degli artt. 29 e 32, paragrafo 4, Reg. UE 2016/679- RGPD e dell'art. 2 *quaterdecies* del d.Lgs. 196/2003, introdotto dal d.lgs 101/2018;

D. **DI DESIGNARE** "Preposti al trattamento dei dati personali" il Direttore Amministrativo, il Direttore sanitario, il Direttore dei Servizi Sociali e Direttori delle seguenti tipologie di struttura:
   - Dipartimento
   - Area Funzionale Dipartimentale
   - Staff
   - Area di Staff
   - Presidio Ospedaliero
   - Stabilimento Ospedaliero
   - Zona distretto
   - Unità Operativa complessa
   - Unità Operativa Semplice Dipartimentale
   - Unità Funzionale

   quali risultano dall'elenco pubblicato del sito web aziendale nell'apposita sezione "Privacy in Azienda" e periodicamente aggiornato, in riferimento ai trattamenti di dati personali in atto o successivamente attivati nell'ambito dell'incarico o dell'unità organizzativa di competenza, specificandone i compiti e le funzioni nel documento allegato sub A) al presente atto;

E. **DI STABILIRE** che i Preposti provvedano a nominare "Incaricati del trattamento dei dati"i dipendenti/collaboratori ad altro titolo operanti all'interno delle rispettive strutture e sotto le proprie direttive, quali soggetti autorizzati al trattamento di dati personali nell'ambito delle loro specifiche competenze, secondo le istruzioni specificate nell'Allegato B) al presente atto;

F. **DI STABILIRE** che i Preposti e gli Incaricati al trattamento dei dati personali sono tenuti a collaborare con il Titolare e con il Responsabile per la protezione dei dati personali per tutte le attività obbligatorie di adeguamento alla nuova normativa europea, nonché alle disposizioni normative nazionali ed alle linee guida dell'Autorità Garante per la protezione dei dati personali;

G. **DI DISPORRE** che, a decorrere dall'esecutività del presente atto, la designazione a Preposto al trattamento di dati personali sia effettuata nello stesso provvedimento di conferimento dell'incarico di direzione (quale "titolare" "ad interim","sostituto") delle tipologie di struttura individuate dal presente atto, a cura delle strutture aziendali competenti alla predisposizione dei provvedimenti di attribuzione di detti incarichi, contestualmente allegando al provvedimento il documento "Compiti e funzioni dei Preposti al trattamento di dati" allegato sub A) al presente atto;

H. **DI DELEGARE** ai Direttori delle strutture funzionali di massima dimensione (Staff, Dipartimento, Presidio Ospedaliero, Zona Distretto), denominati Preposti Referenti, lo svolgimento delle seguenti funzioni per conto del Titolare:
   - coordinamento dei Preposti al trattamento afferenti la macrostruttura, al fine garantire omogeneità di comportamenti e procedure/soluzioni organizzative condivise in applicazione della normativa in materia di protezione dei dati personali
   - trasmissione ai Preposti al trattamento afferenti la macrostruttura di ogni comunicazione/circolare/nota pervenuta dal Titolare o dal Responsabile della Protezione dei Dati,
   - vigilanza, monitoraggio e controllo sulla corretta applicazione da parte dei Preposti al trattamento afferenti la macrostruttura delle disposizioni del RGPD e del d.lgs 196/2003, delle prescrizioni dell'Autorità Garante, delle istruzioni/ direttive impartite dal Titolare e/o dal Responsabile della Protezione dei Dati;

I. **DI PREVEDERE**, quale misura organizzativa a supporto del Preposti Referenti l'istituzione della a figura del Referente Data Protection di macrostruttura, focal point della macrostruttura di riferimento nella gestione operativa delle attività connesse al trattamento dei dati;

J. **DI APPROVARE** lo schema di atto giuridico, predisposto dal Responsabile della Protezione dei Dati e allegato sub C) al presente atto, che le strutture aziendali che stipulano convenzioni o contratti devono utilizzare per la nomina del soggetto esterno a Responsabile del trattamento;

K. **DI STABILIRE** che ove la sottoscrizione dell'atto di nomina a Responsabile sia contestuale a quella del contratto/ convenzione di cui è parte integrante e sostanziale, provveda alla sottoscrizione lo stesso soggetto che ha facoltà di sottoscrivere il contratto/convenzione come da specifica delega del Direttore Generale;

L. **DI DELEGARE** alla sottoscrizione dell'atto di nomina a Responsabile, ove disgiunta da quella del contratto/ convenzione cui accede, ogni dirigente designato Preposto al trattamento per i contratti/convenzioni di cui è RES, per quelli le cui funzioni di RES afferiscono alla propria struttura e per quelli riferiti agli ambiti di attività istituzionale di propria competenza

M. **DI DELEGARE** al Direttore dello Staff della Direzione Aziendale la nomina di soggetti terzi a Responsabili del trattamento in ogni altro caso diverso da quelli di cui al precedente punto L.;

N. **DI ISTITUIRE** il "Comitato Data Protection", organismo tecnico permanente di natura interdisciplinare con compiti di indirizzo, coordinamento, analisi e controllo coerenti con il principio di "accountability" previsto dal RGPD in capo al Titolare, e con funzioni operative di supporto e proposta al Titolare di soluzioni ai problemi applicativi del Regolamento (UE) 2016/679, nella seguente composizione:

- Direttore Staff Direzione Aziendale o suo delegato, con funzione di coordinatore
- dirigente medico dello Staff del Direttore Sanitario (designazione del Direttore dello Staff)
- personale (dirigente e/o non dirigente), con esperienza professionale e conoscenza dei processi sanitari, tecnici e dei principali sistemi applicativi in uso in ambito ospedaliero (designazione del direttore della Rete Ospedaliera)
- personale (dirigente e/o non dirigente), con esperienza professionale e conoscenza dei processi sanitari, tecnici e dei principali sistemi applicativi in uso in ambito territoriale (designazione del Direttore del Dipartimento Territoriale);
- personale (dirigente e/o non dirigente) delle professioni infermieristiche e ostetriche, delle professioni tecnico-sanitarie e della riabilitazione e della prevenzione (designazione del rispettivo Direttore di Dipartimento);
- personale (dirigente e/o non dirigente), con esperienza professionale e conoscenza dei processi amministrativi a supporto dei percorsi sanitari(designazione del Direttore Amministrativo);
- personale (dirigente e/o non dirigente), con competenze in ambito gestionale e di project management (designazione del Direttore Staff Direzione Aziendale);
- Responsabile della protezione dei dati personali (RPD), per lo svolgimento delle funzioni di cui all'art. 39 del RGDP e Deliberazione aziendale n.491/2018 citata;

O. **DI PREVEDERE** che il "Comitato Data Protection" si avvalga nell'esercizio delle sue funzioni dell'ausilio di ogni ulteriore specifica professionalità presente in Azienda nonché della collaborazione dei dirigenti tecnico-informatici individuati da ESTAR a supporto del Responsabile della protezione dei dati personali per l'Area Vasta Sud Est;

P. **DI ATTRIBUIRE** al Comitato le seguenti funzioni:

- promuovere l'osservanza del RGPD e delle disposizioni nazionali in materia di protezione dei dati fornendo consulenza alle varie aree dell'organizzazione e assicurando una visione complessiva e integrata di tutte le esigenze
- promuovere, predisporre e/o validare la documentazione di riferimento del Sistema Aziendale Data Protection
- validare le procedure organizzative rilevanti in termini di protezione dei dati personali, definite dal titolare in merito all'esecuzione dei vari trattamenti, sia per le attività informatizzate che manuali;
- disciplinare e pianificare verifiche periodiche sul Sistema Data Protection, analizzare gli esiti delle verifiche, definire/validare gli eventuali interventi correttivi
- monitorare, valutare periodicamente il Sistema e proporre alla Direzione i piani evolutivi necessari per assicurarne conformità, adeguatezza ed efficacia rispetto al quadro normativo tenuto conto dei rischi dei vari settori e delle priorità dell'organizzazione;

Q. **DI INDIVIDUARE,** in particolare, i seguenti ambiti prioritari di intervento per il Comitato:

- definizione procedura per la gestione del processo di Valutazione di Impatto sulla Protezione dei dati (VIP) o Data Protection Impact Assessment (DPIA) di cui all'art. 35

- implementazione e aggiornamento del registro delle attività di trattamento;
- definizione fabbisogni e modalità interventi formativi;
- linee guida per l'analisi del rischio (art. 32 RGPD), attività funzionale al mantenimento della sicurezza e alla prevenzione di trattamenti in violazione delle prescrizioni del RGPD;
- definizione procedura aziendale in caso di violazione dei dati personali (c.d. data breach);
- implementazione e aggiornamento registro delle attività;
- predisposizione/revisione regolamenti e policy (sistema di videosorveglianza, modalità di utilizzo strumenti informatici, etc.);
- revisione/adeguamento informative riferite ad ambiti specifici di attività;
- definizione modalità attivazione, gestione e utilizzo Dossier Sanitario Aziendale (D.S.A)

R. **DI APPROVARE** il documento "Schema della procedura aziendale in caso di violazione dei dati personali (c.d. data breach)" predisposto dal RPD e allegato sub D) al presente atto, rimettendolo alla valutazione e validazione da parte del Comitato;

S. **DI DICHIARARE** superata e inapplicabile ogni disposizione aziendale incompatibile con la presente deliberazione;

T. **DI PARTECIPARE** il presente atto ai soggetti designati Preposti al trattamento dei dati personali e di dare allo stesso la più ampia diffusione anche mediante utilizzo delle reti web aziendali;

U. **DI DARE ATTO** che Responsabile del procedimento ai sensi dell'art. 6 L.241/90 e s.m.i. è la dott.ssa Paola Salvi, Direttore della U.O.C. Privacy e Internal Audit e Responsabile della protezione dei dati personali;

V. **DI DICHIARARE** il presente atto immediatamente esecutivo, stante la necessità di garantire coerenza del Sistema Aziendale Data Protection al quadro normativo vigente in materia;

IL DIRETTORE DELLA U.O.C. PRIVACY E INTERNAL AUDIT- Responsabile della Protezione dei Dati Personali
(Dott.ssa Paola Salvi)

IL DIRETTORE GENERALE

VISTO il D.Lgs 30 dicembre 1992, n. 502 "Riordino della disciplina in materia sanitaria a norma dell'articolo 1 della legge 23 febbraio 1982 n. 421" ed in particolare gli articoli 3 e 3-bis che disciplinano la nomina dei Direttori Generali delle Aziende USL, della Aziende Ospedaliere e degli Enti del S.S.R.;

VISTA la L.R. Toscana 24 febbraio 2005, n. 40 "Disciplina del servizio sanitario regionale " ed in particolare l'articolo 37 che disciplina la nomina ed il rapporto di lavoro del Direttore Generale delle Aziende Unità Sanitarie Locali e delle Aziende Ospedaliero-Universitarie;

VISTA la L.R. Toscana 28 dicembre 2015, n. 84 "Riordino dell'assetto istituzionale e organizzativo del sistema sanitario regionale. Modifiche alla L.R. 40/2005 ", che introduce modifiche e integrazioni alla Legge Regionale Toscana n. 40/2005, ed in particolare:

· l'art. 83, commi 2 e 3, secondo cui le "Le Aziende USL 1 di Massa e Carrara, USL 2 di Lucca, USL 3 di Pistoia, USL 4 di Prato, USL 5 di Pisa, USL 6 di Livorno, USL 7 di Siena, USL 8 di Arezzo, USL 9 di Grosseto, USL 10 di Firenze, USL 11 di Empoli, USL 12, di Viareggio sono soppresse alla data del 31 dicembre 2015. Le Aziende Unità Sanitarie Locali di nuova istituzione, a decorrere dal 1° gennaio 2016, subentrano con successione a titolo universale in tutti i rapporti giuridici attivi e passivi delle Aziende Unità Sanitarie Locali soppresse, comprese nell'ambito territoriale di competenza";

VISTO il Decreto del Presidente della Giunta Regionale n. 34 del 29 febbraio 2016, con il quale il Dr. Enrico Desideri è stato nominato Direttore Generale dell'Azienda USL Toscana Sud Est, con decorrenza dal giorno 1° marzo 2016;

LETTA E VALUTATA la sopra esposta proposta di deliberazione presentata dal Direttore della U.O.C. Privacy e Internal Audit - Responsabile della Protezione dei Dati, avente ad oggetto "Adeguamento Sistema Aziendale Data Protection - determinazioni";

PRESO ATTO dell'attestazione della legittimità, nonché della regolarità formale e sostanziale, espressa dal Dirigente che propone il presente atto;

VISTO il parere favorevole del Direttore Amministrativo e del Direttore Sanitario;

DELIBERA

per quanto sopra premesso, da intendersi qui integralmente trascritto e riportato:

DI FAR PROPRIA la proposta sopra esposta e di approvarla integralmente nei termini indicati e pertanto:

A. **DI DARE ATTO** della nomina del Responsabile della protezione dei dati personali con Deliberazione n.491/2018, della pubblicazione dei dati di contatto del RPD nel sito istituzionale dell'Azienda e dell'avvenuta comunicazione al Garante per la protezione dei dati personali

B. **DI DARE ATTO** che con nota prot GEN/0212700/U del 30 novembre 2018, il Responsabile della protezione dei dati personali ha trasmesso alla Direzione aziendale un primo modello di registro delle attività di trattamento del Titolare idoneo a soddisfare il debito informativo ex art. 30 Reg. UE 2016/679- RGPD;

C. **DI ADEGUARE** il sistema aziendale dei ruoli e delle correlate responsabilità in ordine al trattamento dei dati alla luce del combinato disposto degli artt. 29 e 32, paragrafo 4, Reg. UE 2016/679- RGPD e dell'art. 2 *quaterdecies* del d.Lgs. 196/2003, introdotto dal d.lgs 101/2018;

D. **DI DESIGNARE** "Preposti al trattamento dei dati personali" il Direttore Amministrativo, il Direttore sanitario, il Direttore dei Servizi Sociali e Direttori delle seguenti tipologie di struttura:
   - Dipartimento
   - Area Funzionale Dipartimentale
   - Staff
   - Area di Staff

- Presidio Ospedaliero
- Stabilimento Ospedaliero
- Zona distretto
- Unità Operativa complessa
- Unità Operativa Semplice Dipartimentale
- Unità Funzionale

quali risultano dall'elenco pubblicato del sito web aziendale nell'apposita sezione "Privacy in Azienda" e periodicamente aggiornato, in riferimento ai trattamenti di dati personali in atto o successivamente attivati nell'ambito dell'incarico o dell'unità organizzativa di competenza, specificandone i compiti e le funzioni nel documento allegato sub A) al presente atto;

E. **DI STABILIRE** che i Preposti provvedano a nominare "Incaricati del trattamento dei dati"i dipendenti/collaboratori ad altro titolo operanti all'interno delle rispettive strutture e sotto le proprie direttive, quali soggetti autorizzati al trattamento di dati personali nell'ambito delle loro specifiche competenze, secondo le istruzioni specificate nell'Allegato B) al presente atto;

F. **DI STABILIRE** che i Preposti e gli Incaricati al trattamento dei dati personali sono tenuti a collaborare con il Titolare e con il Responsabile per la protezione dei dati personali per tutte le attività obbligatorie di adeguamento alla nuova normativa europea, nonché alle disposizioni normative nazionali ed alle linee guida dell'Autorità Garante per la protezione dei dati personali;

G. **DI DISPORRE** che, a decorrere dall'esecutività del presente atto, la designazione a Preposto al trattamento di dati personali sia effettuata nello stesso provvedimento di conferimento dell'incarico di direzione (quale "titolare" "ad interim","sostituto") delle tipologie di struttura individuate dal presente atto, a cura delle strutture aziendali competenti alla predisposizione dei provvedimenti di attribuzione di detti incarichi, contestualmente allegando al provvedimento il documento "Compiti e funzioni dei Preposti al trattamento di dati" allegato sub A) al presente atto;

H. **DI DELEGARE** ai Direttori delle strutture funzionali di massima dimensione (Staff, Dipartimento, Presidio Ospedaliero, Zona Distretto), denominati Preposti Referenti, lo svolgimento delle seguenti funzioni per conto del Titolare:
   - coordinamento dei Preposti al trattamento afferenti la macrostruttura, al fine garantire omogeneità di comportamenti e procedure/soluzioni organizzative condivise in applicazione della normativa in materia di protezione dei dati personali
   - trasmissione ai Preposti al trattamento afferenti la macrostruttura di ogni comunicazione/circolare/nota pervenuta dal Titolare o dal Responsabile della Protezione dei Dati,
   - vigilanza, monitoraggio e controllo sulla corretta applicazione da parte dei Preposti al trattamento afferenti la macrostruttura delle disposizioni del RGPD e del d.lgs 196/2003, delle prescrizioni dell'Autorità Garante, delle istruzioni/ direttive impartite dal Titolare e/o dal Responsabile della Protezione dei Dati;

I. **DI PREVEDERE**, quale misura organizzativa a supporto del Preposti Referenti l'istituzione della a figura del Referente Data Protection di macrostruttura, focal point della macrostruttura di riferimento nella gestione operativa delle attività connesse al trattamento dei dati;

J. **DI APPROVARE** lo schema di atto giuridico, predisposto dal Responsabile della Protezione dei Dati e allegato sub C) al presente atto, che le strutture aziendali che stipulano convenzioni o contratti devono utilizzare per la nomina del soggetto esterno a Responsabile del trattamento;

K. **DI STABILIRE** che ove la sottoscrizione dell'atto di nomina a Responsabile sia contestuale a quella del contratto/ convenzione di cui è parte integrante e sostanziale, provveda alla sottoscrizione lo stesso soggetto che ha facoltà di sottoscrivere il contratto/convenzione come da specifica delega del Direttore Generale;

L. **DI DELEGARE** alla sottoscrizione dell'atto di nomina a Responsabile, ove disgiunta da quella del contratto/ convenzione cui accede, ogni dirigente designato Preposto al trattamento per i contratti/convenzioni di cui è RES, per quelli le cui funzioni di RES afferiscono alla propria struttura e per quelli riferiti agli ambiti di attività istituzionale di propria competenza

M. **DI DELEGARE** al Direttore dello Staff della Direzione Aziendale la nomina di soggetti terzi a Responsabili del trattamento in ogni altro caso diverso da quelli di cui al precedente punto L.;

N. **DI ISTITUIRE** il "Comitato Data Protection", organismo tecnico permanente di natura interdisciplinare con compiti di indirizzo, coordinamento, analisi e controllo coerenti con il principio di "accountability" previsto dal RGPD in capo al Titolare, e con funzioni operative di supporto e proposta al Titolare di soluzioni ai problemi applicativi del Regolamento (UE) 2016/679, nella seguente composizione:
   - Direttore Staff Direzione aziendale, con funzione di coordinatore
   - dirigente medico dello Staff del Direttore Sanitario (nomina del Direttore dello Staff)
   - personale (dirigente e/o non dirigente), con esperienza professionale e conoscenza dei processi sanitari, tecnici e dei principali sistemi applicativi in uso in ambito ospedaliero (designazione del direttore della Rete Ospedaliera)
   - personale (dirigente e/o non dirigente), con esperienza professionale e conoscenza dei processi sanitari, tecnici e dei principali sistemi applicativi in uso in ambito territoriale (designazione del Direttore del Dipartimento Territoriale);
   - personale (dirigente e/o non dirigente) delle professioni infermieristiche e ostetriche, delle professioni tecnico-sanitarie e della riabilitazione e della prevenzione (designazione del rispettivo Direttore di Dipartimento);
   - personale (dirigente e/o non dirigente), con esperienza professionale e conoscenza dei processi amministrativi a supporto dei percorsi sanitari(designazione del Direttore Amministrativo);
   - personale (dirigente e/o non dirigente), con competenze in ambito gestionale e di project management (designazione del Direttore Staff Direzione Aziendale);
   - Responsabile della protezione dei dati personali (RPD), per lo svolgimento delle funzioni di cui all'art. 39 del RGDP e Deliberazione aziendale n.491/2018 citata;

O. **DI PREVEDERE** che il "Comitato Data Protection" si avvalga nell'esercizio delle sue funzioni dell'ausilio di ogni ulteriore specifica professionalità presente in Azienda nonché della collaborazione dei dirigenti tecnico-informatici individuati da ESTAR a supporto del Responsabile della protezione dei dati personali per l'Area Vasta Sud Est;

P. **DI ATTRIBUIRE** al Comitato le seguenti funzioni:
- promuovere l'osservanza del RGPD e delle disposizioni nazionali in materia di protezione dei dati fornendo consulenza alle varie aree dell'organizzazione e assicurando una visione complessiva e integrata di tutte le esigenze
- promuovere, predisporre e/o validare la documentazione di riferimento del Sistema Aziendale Data Protection
- validare le procedure organizzative rilevanti in termini di protezione dei dati personali, definite dal titolare in merito all'esecuzione dei vari trattamenti, sia per le attività informatizzate che manuali;
- disciplinare e pianificare verifiche periodiche sul Sistema Data Protection, analizzare gli esiti delle verifiche, definire/validare gli eventuali interventi correttivi
- monitorare, valutare periodicamente il Sistema e proporre alla Direzione i piani evolutivi necessari per assicurarne conformità, adeguatezza ed efficacia rispetto al quadro normativo tenuto conto dei rischi dei vari settori e delle priorità dell'organizzazione;

Q. **DI INDIVIDUARE,** in particolare, i seguenti ambiti prioritari di intervento per il Comitato:
- definizione procedura per la gestione del processo di Valutazione di Impatto sulla Protezione dei dati (VIP) o Data Protection Impact Assessment (DPIA) di cui all'art. 35
- implementazione e aggiornamento del registro delle attività di trattamento;
- definizione fabbisogni e modalità interventi formativi;
- linee guida per l'analisi del rischio (art. 32 RGPD), attività funzionale al mantenimento della sicurezza e alla prevenzione di trattamenti in violazione delle prescrizioni del RGPD;
- definizione procedura aziendale in caso di violazione dei dati personali (c.d. data breach);
- modalità di implementazione e aggiornamento del egistro delle attività di trattamento;
- predisposizione/revisione regolamenti e policy (sistema di videosorveglianza, modalità di utilizzo strumenti informatici, etc.);
- revisione/adeguamento informative riferite ad ambiti specifici di attività;
- definizione modalità attivazione, gestione e utilizzo Dossier Sanitario Aziendale (D.S.A)

R. **DI APPROVARE** il documento "Schema della procedura aziendale in caso di violazione dei dati personali (c.d. data breach)" predisposto dal RPD e allegato sub D) al presente atto, rimettendolo alla valutazione e validazione da parte del Comitato;

S. **DI DICHIARARE** superata e inapplicabile ogni disposizione aziendale incompatibile con la presente deliberazione;

T. **DI PARTECIPARE** il presente atto ai soggetti designati Preposti al trattamento dei dati personali e di dare allo stesso la più ampia diffusione anche mediante utilizzo delle reti web aziendali;

U. **DI DARE ATTO** che Responsabile del procedimento ai sensi dell'art. 6 L.241/90 e s.m.i. è la dott.ssa Paola Salvi, Direttore della U.O.C. Privacy e Internal Audit e Responsabile della Protezione dei Dati Personali;

V. **DI DICHIARARE** il presente atto immediatamente esecutivo, stante la necessità di garantire coerenza del Sistema Aziendale Data Protection al quadro normativo vigente in materia;

Z. **DI INCARICARE** la U.O.C. Affari Generali:
- di provvedere alla pubblicazione all'Albo on line, ai sensi dell'art. 32, comma 1°, della Leggen. 69/2009, consultabile sul sito WEB istituzionale;
- di trasmettere il presente atto, contestualmente alla sua pubblicazione al Collegio Sindacale, ai sensi dell'art. 42, comma 2, della L.R. 24 febbraio 2005, n. 40 e s.m.i.;

Azienda USL Toscana sud est
Servizio Sanitario della Toscana

IL DIRETTORE GENERALE
(Dr. Enrico Desideri)