REGIONE DEL VENETO
AZIENDA OSPEDALIERA DI PADOVA

Delibera del Direttore Generale n. 537 del 24/04/2018

OGGETTO: Adempimenti da attuare per dare corretta applicazione alla normativa del nuovo Regolamento Europeo 679/2016 sulla Data Protection (GDPR -General Data Protection Regulation). Approvazione Relazione Tecnica.

NOTE TRASPARENZA: Con il presente provvedimento si approva la Relazione Tecnica ad oggetto ¿ Adempimenti da attuare per dare corretta applicazione alla normativa del nuovo Regolamento Europeo 679/2016 sulla Data Protection (GDPR -General Data Protection Regulation).

Il Direttore della **UOC Affari Generali e Legali** riferisce:

A partire dal 25 maggio 2018 è direttamente applicabile in tutti gli Stati membri il Regolamento UE 2016/679 (approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016) noto come GDPR (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali. Il GDPR nasce da precise esigenze, di certezza giuridica, armonizzazione e maggiore semplicità delle norme riguardanti il trasferimento di dati personali dall'Ue verso altre parti del mondo. Si tratta poi di una risposta, necessaria e urgente, alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini Ue.

Il Regolamento UE impone una forte responsabilizzazione, un cambio di passo, un approccio proattivo; la protezione dei dati personali diventa un asset strategico delle pubbliche amministrazioni una pietra angolare nella progettazione dei servizi, programmi, software e dei processi aziendali.

La data del 25 maggio 2018 è inderogabile, in quanto le prescrizioni stabilite dal Regolamento, di cui si tratta, troveranno diretta ed immediata applicazione, indipendentemente dalla preesistenza di differenti norme nazionali in materia che, quindi, verranno automaticamente superate dai precetti del Regolamento UE 2016/679.Ciò comporta che le disposizioni legislative di cui al vigente Codice della

privacy (D.lgs. 196/2003 e ss.mm.ii.), verranno superate, a far data dal 25/05/2018, da quelle del Regolamento UE, nella misura in cui le norme nazionali siano contrastanti o incompatibili con quelle europee.

Il legislatore italiano, al fine di facilitare il compito di chi sia chiamato ad applicare tali norme, che propongono nuovi concetti ed obblighi, ha delegato (Legge Delega 25 ottobre 2017 n. 163 art.13) il Governo ad adeguare (entro la data del 21 maggio 2018) la legge italiana sulla privacy (D.lgs. 196/2003) alle nuove disposizioni europee.

Il Consiglio dei Ministri, in attuazione di suddetta Legge delega, nella seduta del 21/03 u.s. ha approvato, in via preliminare, lo schema di decreto legislativo di adeguamento del quadro normativo nazionale alle disposizioni del regolamento UE 2016/679 GDPR, prevedendo che il vigente Codice in materia di protezione dei dai personali, di cui al decreto legislativo 30 giugno 2003, n. 196, sarà abrogato e che la nuova disciplina in materia sarà rappresentata principalmente dalle disposizioni del suddetto Regolamento immediatamente applicabili e da quelle recate dallo schema di decreto volte ad armonizzare l'ordinamento interno al nuovo quadro normativo dell'Unione Europea in tema di tutela della privacy.

Va precisato che nel schema di Decreto è stato scelto, invece, di mantenere la continuità facendo salvi per un periodo transitorio i provvedimenti del Garante (si pensi, per esempio a quello in materia di Fascicolo Sanitario Elettronico, di Dossier Sanitario Elettronico, di videosorveglianza etc.) e le autorizzazioni, che saranno oggetto di successivo riesame.

Questa situazione, unita alle sanzioni elevate che il Regolamento UE introduce per le ipotesi di violazione degli obblighi introdotti dal medesimo (il Regolamento ha aumentato l'ammontare delle sanzioni amministrative pecuniarie, che potranno arrivare fino ad un massimo di 20 milioni di Euro o fino al 4% del fatturato mondiale totale annuo), implica la necessità per le aziende di iniziare quanto prima il processo di adeguamento, senza lasciarsi spaventare dalle incertezze, ma iniziando a pianificare e implementare una strategia, fondata magari su liste di priorità, che possa consentire di non trovarsi completamente impreparati all'indomani del giorno in cui il Regolamento inizierà ad applicarsi (il 25 maggio 2018).

Questa Azienda Ospedaliera ha, quindi, ritenuto opportuno affrontare la tematica in argomento, in aderenza anche al nuovo principio di "accountability" (obbligo di rendicontazione), per cui il titolare dovrà dimostrare l'adozione di politiche privacy e di misure di sicurezza,

organizzative e tecniche, adeguate ed efficaci a protezione dei dati, in conformità al Regolamento, disciplinando, sin d'ora, compiti, regolamenti e policy interne che garantiscano l'assolvimento dei (non pochi) adempimenti imposti dalle norme europee, a tutela dei diritti e delle libertà degli interessati.

A tale scopo, il proponente Servizio Affari Generali e Legali ha predisposto una Relazione Tecnica, dal titolo: "Adempimenti da attuare per dare corretta applicazione alla normativa del nuovo Regolamento Europeo n. 679/2016 sulla Data Protection (GDPR -General Data Protection Regulation)".

Scopo di detta Relazione è rappresentare, in modo schematico e per quanto possibile sintetico, gli adempimenti cui deve far fronte questa Azienda Ospedaliera per effetto delle norme europee, individuando gli ambiti di attività aziendale dove far rientrare i numerosi adempimenti di carattere strategico, organizzativo, tecnologico informatico e comunicativo, tenendo conto sia del fatto che molti di questi adempimenti non sono ancora ben definiti per il descritto contesto normativo attuale, sia delle disposizioni organizzative contenute nel nuovo atto Aziendale di questa Azienda Ospedaliera (ad oggi ancora al vaglio della Regione Veneto per la prevista valutazione di conformità).

La succitata Relazione Tecnica è stata presentata e condivisa in un apposito incontro tenutosi presso la Direzione Generale di questa Struttura Ospedaliera in data 03/04/2018.

Alla luce di quanto sopra esposto si propone di approvare, quale strumento a carattere programmatico la Relazione Tecnica che si allega alla presente deliberazione di cui ne costituisce parte integrante, dando avvio alle prime azioni di carattere strategico, organizzativo, tecnologico informatico e comunicativo volte ad ottemperare in ambito aziendale agli obblighi del Regolamento Europeo n. 2016/679 sulla Privacy.

Come da indicazioni fornite dalla Direzione Generale, nell'incontro del 03/04 u.s., si propone, infine, di rinviare ad un successivo provvedimento l'individuazione del "Responsabile della Protezione dei Dati Personali" (c.d. "Data Protection Officer" o "D.P.O."), al fine di ponderare le possibili indicazioni statali o regionali che dovessero nel frattempo essere emanate relativamente alle modalità e ai criteri di individuazione di detta figura obbligatoria (art. 37 e 38 del Regolamento UE), elemento imprescindibile per la tutela dei dati personali**,** con particolare riferimento alla realtà delle aziende socio sanitarie.

IL DIRETTORE GENERALE

PRESO ATTO della suestesa proposta e accertato che il Direttore della **UOC Affari Generali e Legali** ha attestato l'avvenuta regolare istruttoria della pratica, anche in ordine alla conformità con la vigente legislazione statale e regionale, nonché la copertura della spesa prevista nel budget assegnato per l'anno in corso;

RITENUTO di dover adottare in merito i provvedimenti necessari;

VISTO il Decreto Legislativo n. 502/92 e successive modifiche ed integrazioni e le leggi regionali n. 55 e n. 56 del 1994 e successive modifiche ed integrazioni;

ACQUISITO il parere favorevole del Direttore Amministrativo e del Direttore Sanitario per quanto di rispettiva competenza;

IN BASE ai poteri conferitigli dal D.P.G.R.nr.92 del 01.08.2016.

DELIBERA

1. di approvare, per le motivazioni espresse in premessa, quale strumento a carattere programmatico, la Relazione Tecnica predisposta dalla UOC Affari Generali e Legali dal titolo: *"Adempimenti da attuare per dare corretta applicazione alla normativa del nuovo Regolamento Europeo n. 679/2016 sulla Data Protection (GDPR -General Data Protection Regulation)",* che si allega alla presente deliberazione di cui ne costituisce parte integrante ed essenziale;

2. di dare avvio, tenendo conto dell'attuale contesto normativo e del processo di modifica dell'assetto organizzativo aziendale, alle prime azioni di carattere organizzativo, gestionale e documentale volte ad ottemperare, nell'ambito dell'Azienda Ospedaliera di Padova, agli obblighi del Regolamento Europeo UE 2016/679 sulla privacy, secondo le linee operative descritte nella Relazione Tecnica di cui al punto n. 1, alla quale si fa espresso rinvio;

3. di incaricare le Strutture, i Servizi e gli Uffici coinvolti negli adempimenti di cui si tratta, come appositamente individuati nella Relazione Tecnica allegata alla presente deliberazione, affinché pongano in essere, ciascuno secondo le rispettive competenze, ogni azione utile ad ottemperare agli obblighi europei correlati all'applicazione diretta, a far data dal 25 maggio 2018, del Regolamento UE 2016/679 sulla privacy;

4. di rinviare ad un successivo provvedimento l'individuazione del "Responsabile della Protezione dei Dati Personali" (c.d. "Data Protection Officer" o "D.P.O."), figura obbligatoria (art. 37 e 38 del Regolamento UE), al fine di ponderare le possibili indicazioni statali o regionali che dovessero nel frattempo essere emanate relativamente alle modalità e ai criteri di individuazione di detta figura, con particolare riferimento alla realtà delle aziende sanitarie.

Il Direttore Generale
F.to Dott. Luciano Flor

Regione del Veneto
AZIENDA OSPEDALIERA - PADOVA
www.sanita.padova.it – P.E.C.: protocollo.aopd@pecveneto.it
via Giustiniani, 1 – 35128 PADOVA

Cod.Fisc./P.IVA 00349040287

UOC AFFARI GENERALI E LEGALI

RELAZIONE TECNICA

Oggetto: adempimenti da attuare per dare corretta applicazione alla normativa del nuovo Regolamento Europeo n.679/2016 sulla data Protection (GDPR -General Data Protection Regulation).

Dal **prossimo 25 maggio diventerà pienamente efficace in tutti gli Stati dell'Unione Europea il nuovo Regolamento Europeo della Privacy n. 2016/679, comunemente detto GDPR**, già in vigore dal 24 maggio 2016, il cui scopo è fornire a tutti gli Stati membri della UE regole comuni in materia di trattamento dei dati personali, in modo da eliminare le disparità di trattamento tra i soggetti dell'Unione. L'applicazione del GDPR, normativa europea **immediatamente efficace ed attiva** nei rapporti tra i soggetti di un determinato Stato, senza alcuna necessità di essere recepito da una legge nazionale, come invece accade alle Direttive Europee, pone la necessità di evidenziare le principali differenze tra tale normativa e quella attualmente in vigore in Italia, in modo da avere presente quali devono essere i punti di attenzione per risultare in linea con la disciplina europea.

Fin dalla sua pubblicazione nella Gazzetta Ufficiale della UE, nel 2016, il GDPR, infatti, ha posto questioni interpretative, alcune delle quali ancora da risolvere, in quanto le disposizioni legislative di cui al vigente Codice della Privacy *(D.lgs.196/2003),* così come le norme regolamentari emanate negli anni dall'Autorità Garante per la protezione dei dati personali, contrastanti o incompatibili con quelle europee devono essere modificate o integrate alla luce delle disposizioni del GDPR.

E', pertanto, auspicabile, per fare chiarezza sui rapporti definitivi tra Codice Privacy e GDPR, un intervento chiarificatore da parte del legislatore e dell'autorità Garante, sciogliendo in tal modo tutti gli ulteriori dubbi a riguardo.

Ed è proprio per facilitare il compito di chi sia chiamato ad applicare tali norme, che è il Legislatore italiano si è attivato pubblicando in Gazzetta Ufficiale 06.11.2017 n. 259 **la Legge Delega 25 ottobre 2017 n. 163** che, all'articolo 13, delega il Governo ad adeguare (entro la data del 21 maggio 2018) la legge italiana sulla privacy (D.lgs. 196/2003) alle nuove disposizioni europee.

In attuazione di tale Legge delega il Consiglio dei Ministri nella seduta del 21/03 u.s. ha approvato uno schema di decreto che, finalmente, chiarisce quale sarà il destino del Codice Privacy a far data dal 25 maggio quando entrerà definitivamente in forza il GDPR Regolamento Ue 2016/679. Lo strumento normativo deputato a regolamentare su base nazionale gli obblighi in materia di tutela dei dati personali che il GDPR riserva alla competenza degli Stati membri, **sarà un nuovo Decreto** il cui iter di approvazione si concluderà giusto in prossimità del 25 maggio (quando le pesanti sanzioni previste dal GDPR saranno operative).

Non sarà, quindi, il Codice Privacy ad assumere il ruolo di corpus nazionale attuativo delle disposizioni del GDPR. Il **Codice Privacy sarà abrogato** e spetterà ad un nuovo decreto il compito di armonizzare l'ordinamento interno alla nuova disciplina europea.

Ciò che è certo che il mondo della privacy, andrà incontro a una serie di profondi cambiamenti ed obblighi di *compliance* particolarmente stringenti nei confronti degli operatori che trattano dati personali, che si possono così sintetizzare, sebbene tale sintesi non può rivestire, allo stato attuale, requisiti di esaustività e di specificità che potranno essere forniti solo a seguito di un'attenta analisi del succitato Decreto Legislativo di adeguamento della normativa, italiana sulla privacy (D.lgs. 196/2003) alle nuove disposizioni europee:

Ecco cosa cambia con il **Regolamento Europeo Privacy** :

- viene introdotto **il principio di "Accountability",** ovvero della responsabilità "verificabile". Il Nuovo Regolamento ri-definisce la figura di Titolare attribuendogli obblighi ulteriori rispetto a quanto previsto dall'attuale Codice Privacy. La non concretezza e l'inefficienza delle policies ad esso attribuite costituisce per il Titolare fonte di responsabilità. Con il Nuovo Regolamento il Titolare ha un ruolo più

proattivo e obblighi più pregnanti, finalizzati non soltanto al formalistico rispetto delle regole, ma anche all'adozione di tutti gli accorgimenti tecnici e organizzativi necessari a garantire la compliance effettiva dei trattamenti, anche sotto il profilo della sicurezza, che tengano conto costantemente del rischio che un determinato trattamento può comportare (Risk based approach) per i diritti e le libertà degli interessati.
Il GDPR attribuisce direttamente al Titolare del trattamento il compito di assicurare ed essere in grado di comprovare, tutti gli altri principi. Il Titolare deve, pertanto, conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente - per ognuno di essi - una serie "nutrita" di informazioni, tali da assicurare e comprovare la conformità di ciascuna operazione alle disposizioni del Regolamento Chi non documenta, è soggetto a possibili sanzioni: a prescindere dall'utilizzo che si fa dei dati, è sufficiente non avere i documenti per essere perseguibili.

- viene istituita la **figura del Data Protection Officer (DPO)** (in italiano: Responsabile della protezione dei dati – RDP): il DPO è una figura obbligatoria, di alta professionalità, che deve essere nominato (ai sensi dell'art. 37 del GDPR) con delibera del Direttore Generale e l'atto di nomina deve essere corredato dalle relative clausole contrattuali. Il DPO dovrà essere individuato dal Titolare, con estrema attenzione, scegliendo o tra risorse interne di comprovata competenza ed esperienza in materia Privacy, adeguate alla complessità del compito da svolgere, specialmente con riferimento a settori delicati come quello della sanità., oppure nominare una figura esterna anch'essa di comprovata competenza o addirittura certificata DPO, La designazione di un DPO, tenuto conto dei compiti che questo deve svolgere e sempre a condizione che sia ad esso garantita l' indipendenza e i mezzi organizzativi e strumentali necessari, può costituire per il Titolare del trattamento una misura molto importante ai fini di dimostrare la sua compliance con quanto previsto dal GDPR.

Sia che il DPO sia interno che esterno, è necessario stipulare con il medesimo un contratto ad hoc.

Nel caso il cui il DPO sia un “esterno” (persona o società) tutte le clausole, oltre che il compenso per l’incarico, dovranno essere inserite in un apposito contratto di servizi, ove siano anche previste le risorse necessarie a far funzionare l’ufficio del DPO.

Per la scelta del DPO esterno, le pubbliche amministrazioni devono tenere conto, ovviamente, della normativa sugli appalti pubblici.

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

- **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati.

  Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;
- **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse.** In linea di principio, ciò significa che il DPO non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali.

  A tale riguardo la Dottrina esclude che possa essere nominato DPO, ad esempio, chi ricopre ruoli gestionali rispetto all’attività o ai fini istituzionali dell’Azienda ed esclude, altresì, chi sia impegnato nelle quotidiane attività operative volte a realizzare e/o a monitorare gli adempimenti in materia.

  A tale proposito, è escluso, per esempio, che possa essere designato RDP il Responsabile dell’ Information Technology, il Responsabile delle Risorse Umane o il Responsabile Sanitario, tutte situazioni che originano, per loro natura, conflitti di interesse.

  Pare evidente, peraltro, come le stesse considerazioni valgano per i Dirigenti dei Servizi amministrativi centrali dell’Azienda (Affari Generali, Ufficio Legale o Controllo di Gestione).

- **disporre di risorse umane e finanziarie, messe a disposizione dal Titolare, per adempiere ai suoi scopi.**

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

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

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

Da sottolineare che, in caso di inosservanza degli obblighi sulla protezione dei dati, il soggetto responsabile resta il titolare, mai il DPO.

- viene **istituito il Registro delle Attività di Trattamento**, Il Titolare deve tenere un registro delle attività di trattamento in forma scritta, anche in formato elettronico, contenente gli elementi di cui all'art. 30 del Nuovo Regolamento. Si tratta di un documento attraverso il quale il Titolare rendiconta (in base al principio di Accountability) tutte le attività in materia di protezione e circolazione dei dati personali che li

riguardano. La ratio è quella di dimostrare la conformità del trattamento alle disposizioni del Regolamento.

- viene introdotta la **gestione dei data breach**, le violazioni dei dati personali. E' stato sancito l'obbligo, per il Titolare, di comunicare le violazioni (data breach) all'Autorità Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, nonché al soggetto interessato, qualora la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà.

- vengono introdotti i **principi di "Privacy by Design" e "Privacy by Default".**

La "Privacy by design" richiede che Il Titolare adotti e attui misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati.

La "Privacy by default" presuppone, invece, nella modalità operativa del trattamento, misure e tecniche che, per impostazione predefinita, garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.

- **viene introdotto l'obbligo di valutazione d'impatto sulla protezione dei dati (DPIA - Data Protection Impact Assessment)**

Quando un determinato trattamento, tenuto conto dell'uso di nuove tecnologie e della sua natura, del contesto e delle finalità, può presentare un rischio elevato per i diritti e libertà delle persone fisiche, il Titolare deve effettuare una valutazione d'impatto privacy analizzando i rischi, definendo i gap rispetto alla corretta gestione dei rischi, stabilendo un piano per colmarli e controllando annualmente gli effetti degli interventi per ridurre i rischi.

Quale contenuto minimo della valutazione si individua la descrizione sistematica dei trattamenti previsti e delle finalità, compresi l'interesse legittimo perseguito dal titolare, la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità, la valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per

affrontare i rischi, nonché le misure per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento.

- viene **introdotto l' obbligo**, in capo al Titolare, **di garantire la formazione** sul nuovo Regolamento UE a favore degli "autorizzati" al trattamento dei dati (quindi di tutti i dipendenti)

– vengono **introdotte regole più chiare e stringenti in materia di informativa e consenso**, che comporteranno l'aggiornamento dell'area documentale (procedure, consensi nomine etc.)

- viene introdotto **un nuovo e più aspro apparato sanzionatorio** in caso di mancato adeguamento al predetto regolamento. Saranno inflitte, tra le altre, le seguenti sanzioni pecuniare:

- una multa fino a 10 milioni di euro, o fino al 2% del volume d'affari globale registrato nell'anno precedente nei casi previsti dall'art. 83, paragrafo 4 (*vedi schema riportato in calce alla presente relazione*)

- fino a 20 milioni di euro o fino al 4% del volume d'affari nei casi previsti dai paragrafi 5 e 6 (*vedi schema riportato in calce alla presente relazione)*

Elencate le principali novità introdotte dal GDPR, va, tuttavia, sottolineato che in questo periodo transitorio e sin tanto che non entri in vigore il nuovo decreto legislativo sulla privacy, ci si dovrà confrontare con un sistema "a doppio binario" in cui l'attuale Codice della privacy ed i regolamenti del "Garante" continueranno a applicarsi assieme al Regolamento europeo e per tutti quegli aspetti non modificati o soppressi per effetto delle preminenti norme europee.

E' necessario pertanto prepararsi, come Azienda, sin da ora, disciplinando compiti, regolamenti e policy interne che garantiscano l'assolvimento dei numerosi adempimenti imposti dalle norme europee.

Il Garante, in particolare, ha individuato, tra tutti i nuovi obblighi introdotti dal Regolamento UE,sopra elencati, **tre priorità**:

1.La designazione in tempi stretti della figura del Data Protection Officer (DPO);
2.L'istituzione del Registro delle attività di trattamento;

3. La notifica dei data breach.

Alla luce di quanto sopra argomentato si rappresenta di seguito, in modo schematico e per quanto possibile sintetico, gli obblighi/adempimenti/cautele, anche se ancora non ben definiti, di spettanza del titolare del trattamento in base alle norme del Regolamento UE, tenendo conto in base alle disposizioni organizzative contenute nel nuovo Atto Aziendale di questa Azienda, gli ambiti di attività aziendali ove far rientrare i numerosi adempimenti previsti dal Regolamento UE, collegando a ciascun adempimento (inserito nella rispettiva area di riferimento) la competenza dello specifico Servizio o Struttura di questa Azienda chiamata a farvi fronte.

Il Titolare del trattamento dei dati è il Direttore Generale dell'Azienda.

Egli risponde civilmente e penalmente del mancato adeguamento, con onere a suo carico di provare che il danno non gli è imputabile (art. 82 e seguenti del Reg. UE).

OBBLIGHI DI CARATTERE STRATEGICO ORGANIZZATIVO TECNOLOGICO INFORMATICO E COMUNICATIVO		
ADEMPIMENTO	**RIFERIMENTO NORMATIVO**	**Titolare dell'obbligo e Struttura/e di supporto competente/i per l'adempimento**
Obbligo di attuare il Regolamento UE ponendo in atto adeguate politiche in materia di protezione dei dati, con l'adozione di **misure tecniche, organizzative, tecnologiche, informatiche e comunicative**, che siano concretamente e sempre **dimostrabili** (PRINCIPIO DI ACCOUNTABILITY)	Regolamento UE (art. 24 eseg.) Guida applicativa del Garante (pag. N 24/29)	**Titolare del Trattamento (Direttore Generale)** **con il supporto del DPO** UOC Affari Generali UOS Sistemi Informativi (*Tutte le UUOOCC amministrative e sanitarie coinvolte nel trattamento dei dati*)
Obbligo di designare il **Responsabile della Protezione dei dati**", c.d.	Regolamento UE (art. 37, 38 e 39)	**Titolare del Trattamento (Direttore Generale)**

"Data Protection Officer"	Guida applicativa del Garante (pagine n. 24 / 29)	
Obbligo di predisporre il **Registro delle attività di trattamento**	Regolamento UE art. 30 Guida applicativa del Garante (pagine n. 26 e seg.)	**Titolare del Trattamento (Direttore Generale)** **con il supporto del DPO** UOS Sistemi Informativi
Obbligo di notifica al Garante delle **violazioni dei dati personali** nei casi previsti dal Regolamento UE (c.d. **"Data Breach")**	Regolamento UE (art. 33) Guida applicativa del Garante (pagine n. 24 / 29)	**Titolare del Trattamento (Direttore Generale)** **tramite il DPO** UOS Sistemi Informativi UOC Affari Generali (*in attesa di specifica modulistica da parte del Garante Privacy*)
Obbligo di adottare istruzioni operative per garantire i nuovi principi di **"privacy by design"** e **"privacy by default"** nell'intero ambito aziendale *(Cioè in tutte le operazioni di trattamento dati, sia nella progettazione, che nella impostazione predefinita)*	Regolamento UE (art. 26) Guida applicativa del Garante (pagina n. 24)	**Titolare del Trattamento Direttore Generale** **con il supporto del DPO** UOS Sistemi Informativi
Obbligo di stipulare I nuovi "Patti di contitolarità" (serve accordo contrattuale interno per c.d. "Joint Controller")	Regolamento UE (art. 25) Guida applicativa del Garante (pagine n. 24)	**Titolare del Trattamento (Direttore Generale)** **con il supporto del DPO** UOC Affari Generali (*su segnalazione delle UUOOC che ne abbiano necessità*)

Obbligo di documentare le violazioni dei dati personali (c.d. **"Registro delle violazioni privacy"**)	Regolamento UE (art. 33) Guida applicativa del Garante (pagine n. 24 / 29)	**Titolare del Trattamento (Direttore Generale)** **per il tramite del DPO** UOS Sistemi Informativi
Obbligo, in capo al Titolare di effettuare la **"Consultazione preventiva"** *(Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio)*	Regolamento UE (art.36) Guida applicativa del Garante (pagine n. 24 / 29)	**Titolare del Trattamento (Direttore Generale)** **per tramite del DPO**
Obbligo di garantire la **formazione** sul nuovo Regolamento UE a favore degli "autorizzati" al trattamento dei dati (quindi di tutti i dipendenti) ,così da ottemperare alle previsioni europee (*prevista formazione e-learning*)	Regolamento UE (art. 39 e seg.) Guida applicativa del Garante (pagine n. 20 e seguenti)	**Titolare del Trattamento (Direttore Generale)** **con il supporto del DPO** UOC Affari Generali UOS Formazione UOS Sistemi Informativi
Acquisizione **certificazione** ed adesione a **codici di condotta**		**Titolare del Trattamento (Direttore Generale)** ***con il supporto del DPO***
Predisposizione del nuovo modello aziendale di **Informativa**, che ottemperi alle previsioni europee *N.B. nella nuova Informativa vanno inseriti anche i "dati di contatto" del Data Protection Officer*	Regolamento UE (art. 13 e 14) Guida applicativa del Garante (pagina n. 8 e seguenti)	**Titolare del Trattamento (Direttore Generale)** ***con il supporto del DPO*** UOC Affari Generali

Predisposizione del nuovo modello aziendale di **consenso al trattamento dei dati**, che ottemperi alle previsioni europee	Regolamento UE (art. 7 e seg.) Guida applicativa del Garante (pagine n. 4 / 7)	**Titolare del Trattamento (Direttore Generale)** ***con il supporto del DPO*** UOC Affari Generali
Nomina, per l'intero ambito aziendale, dei Responsabili del trattamento dei dati, in ottemperanza alle nuove previsioni europee: predisposizione modulistica e trasmissione delle nomine con le istruzioni operative	Regolamento UE (art. 28 e seg.) Guida applicativa del Garante (pagine n. 20 e seguenti)	**Titolare del Trattamento (Direttore Generale)** ***con il supporto del DPO*** UOC Affari Generali
Predisposizione della modulistica e delle linee procedurali per la nomina dei **Responsabili *esterni* del trattamento dei dati** (in ottemperanza alle nuove previsioni europee) (outsourcing di attività)	Regolamento UE (art. 28 e seg.) Guida applicativa del Garante (pagine n. 20 e seg.)	**Titolare del Trattamento (Direttore Generale)** ***con il supporto del DPO*** UOC Affari Generali *(per fornitura modulistica standard)* Servizi interessati alle nomine in virtù di gare ed appalti di servizi, forniture e convenzioni con enti esterni
Adozione, con atto deliberativo pubblicato all'albo on line, di un **"Regolamento aziendale privacy"** che dia evidenza complessiva della *policy aziendale* adottata in materia al fine di ottemperare alle nuove norme europee; delibera che adotti, contestualmente, la nuova modulistica di cui ai punti precedenti. Detta Delibera, inoltre, deve stabilire con chiarezza compiti e responsabilità assegnate a ciascuna Area o Servizio dell'Azienda (*come esposti*	Principi generali dell'ordinamento giuridico nella PA Linee generali, di carattere organizzativo, riconducibili al "Titolare", che si desumono dal Regolamento UE (art. 24 / 43) Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)	**Titolare del Trattamento (Direttore Generale)** ***con il supporto del DPO*** UOC Affari Generali

nella presente Relazione)		
Raccolta e inserimento nel "Regolamento privacy" dell'attuale e vigente ***normativa aziendale "di settore" collegata alla privacy*** (ad esempio): ➢ *modulistica relativa al Dossier Sanitario Elettronico* ➢ *Regolamento aziendale sulla videosorveglianza* ➢ *Regolamento sull'utilizzo dei mezzi informatici e telematici dell'Azienda*	Principi generali dell'ordinamento giuridico nella PA Linee generali, di carattere organizzativo, riconducibili al "Titolare", che si desumono dal Regolamento UE (art. 24 / 43)	**Titolare del Trattamento (Direttore Generale)** UOC Affari Generali previa intesa con il *Data Protection Officer*
Valutazione d'impatto sulla protezione dei dati ("VIP") c.d. *"Data Protection Impact Assessment"*	Regolamento UE (art. 35 e seg.) Guida applicativa del Garante (pagina n. 25 e seg.)	**Titolare del Trattamento (Direttore Generale)** **con il supporto del DPO** UOS Sistemi Informativi
Predisposizione delle **Misure tecniche ed informatiche** per garantire che (l'eventuale) **trasferimento in Paesi Terzi fuori dell'Unione Europea dei dati personali** avvenga nel rispetto delle nuove norme europee	Regolamento UE (art. 44 e seg.) Guida applicativa del Garante (pagine n. 30 e seg.)	**Titolare del Trattamento (Direttore Generale)** **con il supporto del DPO** UOS Sistemi Informativi
Aggiornamento del sito web aziendale con l'inserimento della nuova documentazione e di tutta la nuova modulistica necessaria ad ottemperare alle norme europee	Principi generali dell'ordinamento giuridico nella PA Linee generali, di carattere organizzativo, riconducibili al "Titolare", che si desumono dal Regolamento UE (art. 24 / 43)	**Titolare del Trattamento (Direttore Generale)** **con il supporto del DPO** UOS Comunicazione e URP *consultandosi con il Data Protection Officer e sulla base della documentazione che verrà fornita dalla UOC Affari Generali e dal Responsabile Aziendale per la Trasparenza,secondo le rispettive competenze.*

Sanzioni previste dal Regolamento UE per la violazione degli obblighi indicati

ADEMPIMENTO		**ENTITA' SANZIONE**
Registro trattamenti	▸	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Documento valutazione dei rischi	▸	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Documento di valutazione di impatto privacy	▸	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Procedura Data Breach	▸	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Accordo con contitolari	▸	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Contratto di responsabile esterno	▸	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Contratto con sub-responsabili	▸	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Nomine dipendenti e collaboratori	▸	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Corsi per gli autorizzati *(dipendenti dell'azienda)*	▸	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Informativa	▸	Fino 20 mln/oppure se più elevato fino al 4% fatturato totale mondiale annuo
Raccolta consensi, salvo esonero	▸	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Nomina Data Protection Officer	▸	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Trasferimenti dati all'estero	▸	Fino 20 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
Certificazione	▸	Fino 20 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo

Padova, 03/04/2018

Il Sostituto Responsabile
UOC Affari Generali e Legali
avv. Maria Grazia Calì

ATTESTAZIONE DI PUBBLICAZIONE

La presente deliberazione e' stata pubblicata in copia all'Albo di questa Azienda Ospedaliera di Padova per 15 giorni consecutivi dal

Il Sostituto Responsabile
UOC AFFARI GENERALI E LEGALI
(Avv.Maria Grazia Cali)

CERTIFICAZIONE DI ESECUTIVITA'

La presente deliberazione e' divenuta esecutiva il 24/4/2018

Il Sostituto Responsabile
UOC AFFARI GENERALI E LEGALI
(Avv.Maria Grazia Cali)

Copia composta di n°19 fogli (incluso il presente) della delibera n. 537 del 24/4/2018 firmata digitalmente dal Direttore Generale e conservata secondo la normativa vigente presso Infocert S.p.a.

Padova, li

Il Sostituto Responsabile
UOC AFFARI GENERALI E LEGALI
(Avv.Maria Grazia Cali)
