REGIONE DEL VENETO
ULSS5 POLESANA

N. 313 del Reg. Deliberazioni

del 10/04/2018

DELIBERAZIONE DEL DIRETTORE GENERALE

- Dott. Fernando Antonio Compostella -
nominato con Decreto del Presidente della Giunta Regionale del Veneto
n. 195 del 30.12.2015 e
confermato con Decreto del Presidente della Giunta Regionale del Veneto
n. 160 del 30.12.2016

OGGETTO: Azioni di carattere organizzativo, gestionale e documentale volte ad ottemperare, nell'ambito dell'U.L.SS. n. 5 Polesana, agli obblighi del Regolamento Europeo n. 2016/679 sulla privacy

Struttura UOC Affari Generali

Si attesta l'avvenuta regolare istruttoria del presente provvedimento proposto per l'adozione in ordine alla legittimità con ogni altra disposizione regolante la materia.

Il Direttore della Unità Operativa Complessa
Dr.ssa Patrizia Davì

Il Direttore della U.O.C. Affari Generali, Dr.ssa Patrizia Davì, riferisce:

A far data dal 25 maggio 2018 troverà diretta applicazione, sul territorio nazionale, il nuovo Regolamento Europeo (n. 2016/679) sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016.

Il Regolamento disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, ed abroga la precedente Direttiva 95/46/CE.

Entro la data del 25 maggio 2018, tutti gli Stati membri dell'Unione debbono uniformarsi alle nuove regole comunitarie, evitando così di incorrere nelle pesanti sanzioni (sia economiche che di natura penale) previste dalla nuova normativa.

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 n. 2016/679.

Ciò comporta che le disposizioni legislative di cui al vigente Codice della privacy (D.lgs. 196/2003 e ss.mm.ii.), così come le norme regolamentari emanate negli anni dall'Autorità Garante per la protezione dei dati personali, 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.

Si segnala che, alla data di predisposizione del presente atto deliberativo, 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.

Il Governo, nell'attuare la delega, dovrà "*abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali incompatibili con le disposizioni contenute nel Regolamento UE*" nonché "*modificare il codice limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel Regolamento UE*", al fine di "*coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal Regolamento europeo*" (così l'articolo 13 della Legge Delega n. 163/2017).

E' facile prevedere, quanto meno per un periodo transitorio e sin tanto che non entri in vigore il nuovo decreto legislativo sulla privacy, che ci si dovrà confrontare con un sistema "a doppio binario" in cui l'attuale Codice della privacy ed i regolamenti del "Garante" continueranno ad applicarsi assieme al Regolamento europeo e per tutti quegli aspetti non modificati o soppressi per effetto delle preminenti norme europee.
Nonostante le attività finora poste in essere per adeguarsi alla nuova normativa, è necessario disciplinare gli ulteriori compiti, attività e policy interne che garantiscano l'assolvimento dei (non pochi) adempimenti imposti dalle norme europee.

A tale scopo, la proponente UO Affari Generali ha predisposto una relazione tecnica dal titolo: "*Verifica degli adempimenti in carico all'Azienda U.L.SS. n. 5 Polesana in conseguenza della diretta applicazione, a far data dal 25 maggio 2018, del nuovo Regolamento Europeo sulla privacy*".

Scopo di detta relazione è rappresentare, in modo schematico e per quanto possibile sintetico, gli adempimenti cui deve far fronte questa Azienda ULSS per effetto delle norme europee ed entro il termine del 25 maggio 2018 ed ai quali si è già iniziato a dar corso.

E' doveroso precisare che, al momento in cui è stata redatta l'anzidetta relazione (marzo 2018), molti di questi adempimenti non sono esattamente definiti e si lascia alle imprese e agli enti pubblici l'onere di indicare come comportarsi, con disciplinari interni e con valutazioni caso per caso (ad esempio, non vi sono ancora direttive nazionali sui contenuti di alcuni importanti obblighi di carattere informativo e tecnologico, come il "*registro dei trattamenti*", la "*valutazione d'impatto*" e la "*consultazione preliminare*"), mentre è già chiaro il contenuto di alcuni obblighi di carattere organizzativo e documentale (ad esempio, con riguardo alla nomina del *Data Protection Officer*, alla predisposizione della nuova informativa e alla procedura di segnalazione al Garante che va sotto il nome di "*Data Breach*"). Poiché, proprio con riferimento alla nomina del *Data Protection Officer*, sembravano di imminente emanazione alcune indicazioni regionali alle quali si accennerà in prosieguo, che avrebbero consentito di disciplinare con maggior dettaglio alcuni adempimenti, si è atteso finora prima di formalizzare la presente Relazione, che, pur in carenza di alcuni contenuti di carattere operativo (software gestionale, individuazione del *Data Protection Officer* unico, modalità di gestione dei vari registri ecc.) si ritiene opportuno adottare ora, per non procrastinare ulteriormente il completamento degli ulteriori adempimenti da portare a compimento.

L'approccio metodologico della relazione in parola consta quindi nell'individuare, *ratione materiae* e tenendo conto delle disposizioni organizzative contenute nel nuovo Atto Aziendale di questa ULSS n. 5 Polesana approvato con la Deliberazione n. 31 del 11 gennaio 2018, 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 della specifica Unità Operativa o Servizio di questa ULSS chiamata a farvi fronte.

In estrema sintesi, come descritto nella Relazione, risultano configurabili quattro tipologie di adempimenti e quindi quattro "macro ambiti di attività aziendali" ad essi collegati: il Regolamento europeo, infatti, detta obblighi di carattere: a) strategico ed organizzativo, b) documentale, c) tecnologico ed informatico, d) comunicativo.

Ciò premesso, si fa proposta di approvare, quale strumento a carattere programmatico, la Relazione tecnica predisposta dalla proponente UO Affari Generali dal titolo: "*Verifica degli adempimenti in carico all'Azienda U.L.SS. n. 5 Polesana in conseguenza della diretta applicazione, a far data dal 25 maggio 2018, del nuovo Regolamento Europeo sulla privacy*", nel testo allegato alla presente deliberazione di cui costituisce parte integrante, indicando le azioni di carattere organizzativo, gestionale e documentale volte ad ottemperare, nell'ambito dell'U.L.SS. n. 5 Polesana, agli obblighi del Regolamento Europeo n. 2016/679 sulla privacy.

Si fa proposta, infine, di rinviare ad un successivo provvedimento l'individuazione del "*Responsabile aziendale della Protezione dei Dati Personali*" (c.d. "*Data Protection Officer*" o "*D.P.O.*"), al fine di ponderare le possibili indicazioni regionali che risultano essere in corso emanazione e che paiono essere orientate, attualmente, all'individuazione di un unico soggetto a livello regionale per tutte le aziende socio sanitarie del Veneto.

Per quanto sopra esposto,

IL DIRETTORE GENERALE

Visto il D.Lgs n. 502/1992 come modificato ed integrato nel tempo;

Viste le LL.RR. n. 55 e 56 del 1994 come modificate ed integrate nel tempo;

Vista la L.R. n. 19/2016;

Preso atto che il Direttore della U.O.C. proponente, Dott.ssa Patrizia Davì, competente dell'istruzione dell'argomento in questione, ha attestato l'avvenuta regolare istruttoria della pratica, anche in ordine alla compatibilità con la vigente legislazione regionale e statale;

Acquisiti i pareri favorevoli del Direttore Amministrativo, del Direttore Sanitario del Direttore dei Servizi Socio-Sanitari, ai sensi dell'art. 3 del D.Lgs n.502/92 e successive modificazioni ed integrazioni e ai sensi dell'art. 16 della L.R. n. 56/1994 e successive modificazioni ed integrazioni;

delibera

1. di approvare, quale strumento operativo e a carattere programmatico, la Relazione tecnica predisposta dalla UOC Affari Generali dal titolo: "*Verifica degli adempimenti in carico all'Azienda U.L.S.S. n. 5 Polesana in conseguenza della diretta applicazione, a far data dal 25 maggio 2018, del nuovo Regolamento Europeo sulla privacy*", nel testo allegato alla presente deliberazione di cui ne costituisce parte integrante ed essenziale;

2. di approvare, in conseguenza di quanto disposto al punto n. 1, le azioni di carattere organizzativo, gestionale e documentale volte ad ottemperare, nell'ambito dell'U.L.SS. n. 5 Polesana, agli obblighi del Regolamento Europeo n. 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 Unità Operative, 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 n. 2016/679 sulla privacy;

4. di rinviare ad un successivo provvedimento l'individuazione del "*Responsabile aziendale 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, con particolare riferimento alla realtà delle aziende socio sanitarie venete.

Responsabile Procedimento: dott.ssa Patrizia Davì
Referente istruttoria: dott.ssa Cristina Ghirardello

* * * * *

Pareri favorevoli in quanto di competenza:

IL DIRETTORE AMMINISTRATIVO

Avv. Gianluigi Barausse

IL DIRETTORE SANITARIO

Dott. Edgardo Contato

IL DIRETTORE DEI SERVIZI SOCIO-SANITARI

Dott. Urbano Brazzale

Il DIRETTORE GENERALE

Dott. F. Antonio Compostella

Il presente atto, eseguibile dalla data di adozione:
- è soggetto a controllo _ ;
- non è soggetto a controllo X

Rovigo,

Il Direttore UOC Affari Generali

Dr.ssa Patrizia Davì

Attestazione di pubblicazione

Copia del presente atto è pubblicata all'Albo on line dell'Azienda per 15 giorni consecutivi da oggi.
Rovigo,

Il Direttore UOC Affari Generali

Dr.ssa Patrizia Davi'

Copia del presente atto viene inviata in data odierna al Collegio Sindacale (ex art. 10, comma 5, L.R. 56 del 14.9.94)
Rovigo,

Il Direttore UOC Affari Generali

Dr.ssa Patrizia Davi'

Copia conforme all'originale, per uso amministrativo
Rovigo,

Il Direttore UOC Affari Generali

Dr.ssa Patrizia Davi'

Da distribuire a:

DIRETTORE GENERALE	_	UOC GESTIONE RISORSE UMANE	_	UFFICIO PROTEZIONE DATI	_
DIRETTORE AMMINISTRATIVO	_	UOC DIREZIONE AMM.VA TERRITORIALE	_	UFF. TRASPARENZA E ANTICORRUZIONE	_
DIRETTORE SANITARIO	_	UOC DIREZIONE AMM.VA OSPEDALIERA	_	UFF. RELAZIONI CON IL PUBBL.E COMUNICAZIONE	_
DIRETTORE SERVIZI SOCIO-SANITARI	_	UOC CONTROLLO DI GESTIONE	_	_____	_
COLLEGIO DI DIREZIONE	_	UOC DIREZ. PROFESSIONI SANITARIE	_	_____	_
DIREZIONE FUNZIONE OSPEDALIERA	_	UOC ASS. FARMACEUTICA TERRITORIALE	_	_____	_
DIREZIONE FUNZIONE TERRITORIALE	_	UOC FARMACIA OSPEDALIERA	_	_____	_
DIPARTIMENTO SALUTE MENTALE	_	UOC DISABILITA' NON AUTOSUFFICIENZA	_	_____	_
DIPARTIMENTO DI PREVENZIONE	_	UOC INFANZIA, ADOL.E FAM.DISTRETTO 1	_	_____	_
UOC DISTRETTO 1 ROVIGO	_	UOC INFANZIA, ADOL.E FAM.DISTRETTO 2	_	_____	_
UOC DISTRETTO 2 ADRIA	_	UNITA' OPERATIVA PER IL SOCIALE	_	_____	_
UOC DIREZIONE MEDICA OSP. RO-TRE	_	UOC PSICHIATRIA	_	_____	_
UOC DIREZIONE MEDICA OSP. ADRIA	_	UOC SERD	_	_____	_
POLO FORMATIVO	_	UOS QUALITA' E RISCHIO CLINICO	_	_____	_
UOC AFFARI GENERALI	_	UOS ASSISTENZA SPECIALISTICA AMB.	_	_____	_
UOC CONTABILITA' E BILANCIO	_	UOS MEDICO COMPETENTE	_	_____	_
UOC PROVV. ECONOM. LOGISTICA	_	UOS INTERNAL AUDITING E CERT.BIL.	_	_____	_
UOC SERVIZI TECNICI PATRIMONIALI	_				

RELAZIONE TECNICA per la Direzione Strategica

Verifica degli adempimenti in carico all'Azienda U.L.SS. n. 5 Polesana in conseguenza della diretta applicazione, a far data dal 25 maggio 2018, del nuovo Regolamento Europeo sulla privacy.

La presente relazione, a cura della UOC Affari Generali dell'ULSS n. 5 Polesana, è composta di otto parti:

Vengono di seguito descritti gli argomenti sopra elencati.

A) Premessa di carattere normativo

A far data dal 25 maggio 2018 troverà diretta applicazione, sul territorio nazionale, il nuovo Regolamento Europeo (n. 2016/679) sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016.
Il Regolamento disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati. Esso abroga la precedente Direttiva 95/46/CE.
La sua entrata in vigore è stabilita il 24 maggio 2016: entro due anni a partire da tale data, e quindi entro la data del **25 maggio 2018**, tutti gli Stati membri dell'Unione debbono uniformarsi alle nuove regole comunitarie, evitando così di incorrere nelle pesanti sanzioni (sia economiche sia di natura penale) previste dalla nuova normativa (sanzioni che potranno arrivare fino a 20 milioni di Euro o fino al 4% del fatturato globale del trasgressore, come si dirà nel corso della relazione).
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 n. 2016/679.
Ciò comporta che le disposizioni legislative di cui al vigente Codice della privacy *(D.lgs. 196/2003 e ss.mm.ii.),* così come le norme regolamentari emanate negli anni dall'Autorità Garante per la protezione dei dati personali, 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.
Si segnala che, alla data di redazione della presente relazione, 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.
Il Governo, nell'attuare la delega, dovrà *"abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali incompatibili con le disposizioni contenute nel Regolamento UE*" e *"modificare il codice limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel Regolamento UE",* al fine di *"coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal Regolamento europeo"* (così l'articolo 13 della Legge 163/2017).
E' facile prevedere, quanto meno per un periodo transitorio e sin tanto che non entri in vigore il nuovo decreto legislativo sulla privacy, che ci si dovrà confrontare con un sistema "a doppio binario" in cui l'attuale *Codice della privacy* ed i regolamenti del "Garante" continueranno ad applicarsi assieme al Regolamento europeo e per tutti quegli aspetti non modificati o soppressi per effetto delle preminenti norme europee.

E' necessario pertanto organizzarsi, come Azienda, disciplinando compiti, regolamenti e *policy* interne che garantiscano l'assolvimento degli adempimenti imposti dalle norme europee.

B) Premessa di carattere metodologico

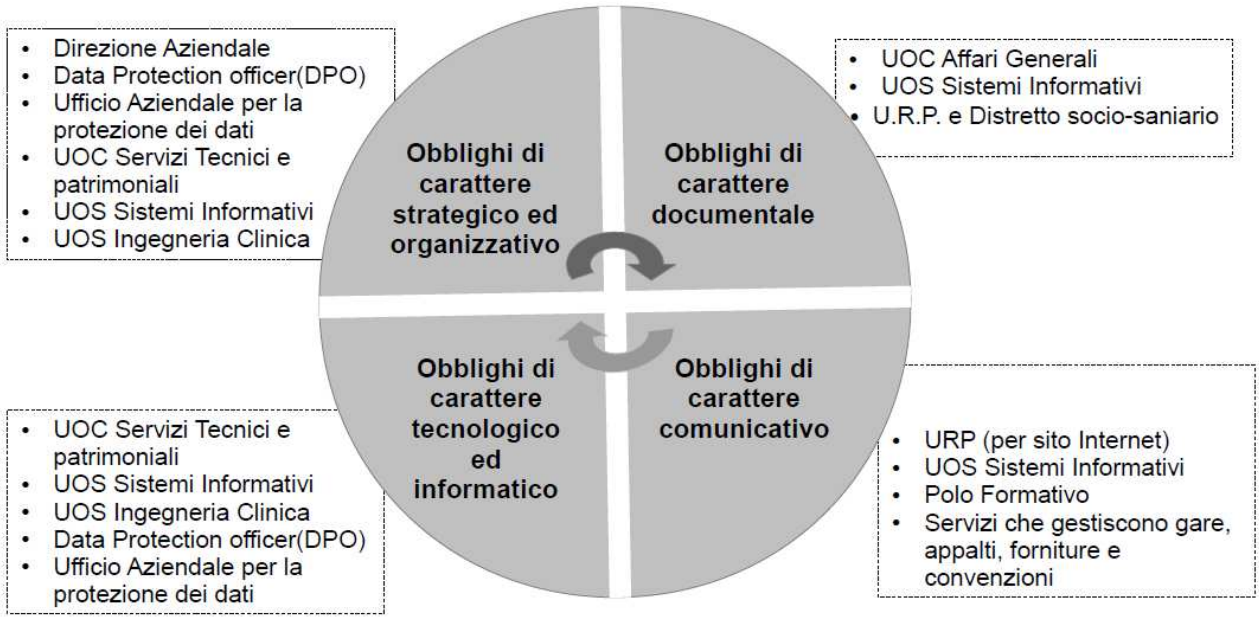
Scopo di questa relazione è rappresentare, in modo schematico e per quanto possibile sintetico, gli adempimenti cui deve far fronte questa Azienda ULSS per effetto delle norme europee ed entro il termine del 25 maggio 2018.
E' doveroso precisare che, al momento in cui viene redatta questa relazione, molti di questi adempimenti non sono esattamente definiti e si lascia alle imprese e agli enti pubblici l'onere di indicare come comportarsi, con disciplinari interni e con valutazioni caso per caso *(ad esempio, non vi sono ancora direttive nazionali sui contenuti di alcuni importanti obblighi di carattere informativo e tecnologico, come il "registro dei trattamenti", la "valutazione d'impatto" e la "consultazione preliminare"),* mentre è già chiaro il contenuto di alcuni obblighi di carattere organizzativo e documentale *(ad esempio, con riguardo alla nomina del Data Protection Officer, alla predisposizione della nuova informativa e alla procedura di segnalazione al Garante che va sotto il nome di "Data Breach*"). Circa il Data Protection Officer si ritiene opportuno soprassedere per il momento a qualsiasi decisione in attesa di indicazioni regionali che si ritiene siano di imminente emanazione e dovrebbero prevedere l'istituzione di un'unica figura a livello regionale per tutte le aziende socio-sanitarie.
L'approccio metodologico di questa relazione, quindi, consta nell'individuare, *ratione materiae* e tenendo conto delle disposizioni organizzative contenute nel nuovo Atto Aziendale di questa ULSS n. 5 Polesana adottato con la Deliberazione n. 31 in data 11 gennaio 2018, 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 della specifica Unità Operativa o Servizio di questa ULSS chiamata a farvi fronte.

C) Ambiti di attività aziendali correlati ai nuovi obblighi europei in materia di privacy

In base allo studio effettuato da questa unità operativa, risultano, al momento, **quattro tipologie di adempimenti** e quindi quattro macro-ambiti di attività aziendali ad essi collegati.
Il Regolamento europeo, infatti, detta obblighi di carattere:

- **strategico ed organizzativo**
- **documentale**
- **tecnologico ed informatico**
- **comunicativo**

Nel *grafico* che segue viene rappresentato il "ciclo di adempimenti" che, a parere di questo Ufficio, si rende necessario porre in essere per realizzare la *privacy europea*, individuando le strutture dell'U.L.SS. n. 5 coinvolte nel medesimo ciclo:



Si procede ad elencare, in dettaglio, le caratteristiche di ciascuno dei ***macro-obblighi*** sopra menzionati, rinviando, per l'esame degli specifici contenuti dei medesimi, alle norme del Regolamento europeo e/o alle indicazioni del Garante sino ad oggi emanate, citate quali fonti nella presente relazione.

D) <u>Obblighi di carattere strategico ed organizzativo</u>

N. progr.	*Adempimento*	*Riferimento normativo*	*Area o UO/Servizio/Ufficio competente per l'adempimento*
1	In capo al "Titolare del trattamento dei dati" è posto l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di **misure tecniche ed organizzative, anche certificate**, che siano concretamente e sempre **dimostrabili** (principio dell'*accountability*). Formalmente, il Regolamento UE pone direttamente a carico del "Titolare" numerosi adempimenti tecnici, che in realtà dovranno essere tradotti e gestiti a livello aziendale dai Servizi dell'area IT – Information Technology, dall'Ingegneria Clinica e dall'Ufficio Tecnico (vedasi successivo punto "F"); su tutti, si segnalano: a) L'adozione dei *Registri delle attività di trattamento* b) L'adozione delle *Misure di sicurezza dei dati* *c)* La *Valutazione di impatto sulla privacy (VIP)*	Regolamento UE (art. 24 e seg.) Guida applicativa del Garante (pagine n. 24 / 29)	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) Sono previste pesanti sanzioni: vedasi capitolo "H" della presente Relazione. Tutti questi adempimenti dovranno essere gestiti a livello aziendale dai Servizi dell'area IT – Information Technology, dall'Ingegneria Clinica e dalla UOC Servizi tecnici

			e patrimonali
2	Obbligo di adottare misure tecniche ed organizzative 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. 25) Guida applicativa del Garante (pagina n. 24)	**Direttore Generale** avvalendosi della *UOC Servizi Tecnici e Patrimoniali, delle UOS Sistemi Informativi e Ingegneria Clinica e dell'Ufficio Aziendale per la protezione dei dati*
3	Obbligo di stipulare i nuovi **"Patti di contitolarità"** (serve accordo contrattuale per c.d. "Joint Controller")	Regolamento UE (art. 26 e seg.) Guida applicativa del Garante (pagina n. 20)	**Direttore Generale** avvalendosi della *UOC Servizi Tecnici e Patrimoniali e delle UOS Sistemi Informativi e Ingegneria Clinica,* del *Data Protection Officer e dell'Ufficio Aziendale per la protezione dei dati*
4	Obbligo di notifica al Garante (tramite il *Data Protection Officer*) 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)	**Direzione Aziendale** avvalendosi della *UOC Servizi Tecnici e Patrimoniali e delle UOS Sistemi Informativi e Ingegneria Clinica,* del *Data Protection Officer e dell'Ufficio Aziendale per la protezione dei dati*
5	Obbligo di documentare (tramite il *Data Protection Officer*) le violazioni dei dati personali (c.d. **"Registro delle violazioni privacy"**)	Regolamento UE (art. 33) Guida applicativa del Garante (pagine n. 24 / 29)	**Direzione Aziendale** avvalendosi della *UOC Servizi Tecnici e Patrimoniali e delle UOS Sistemi Informativi e Ingegneria Clinica* del *Data Protection Officer e dell'Ufficio Aziendale per la protezione dei dati*
6	Obbligo, in capo al Titolare (tramite il *Data Protection Officer*) di effettuare la **"Consultazione preventiva"**	Regolamento UE (art.36) Guida applicativa del Garante (pagine n. 24 / 29)	**Direzione Aziendale** avvalendosi della *UOC Servizi Tecnici e Patrimoniali e delle UOS Sistemi Informativi e Ingegneria Clinica,* del *Data Protection Officer e dell'Ufficio Aziendale per la protezione dei dati*
7	Obbligo, in capo al Titolare, di designare il **"Responsabile della Protezione dei dati**", c.d. *"Data Protection Officer"*	Regolamento UE (art. 37, 38 e 39) Guida applicativa del Garante (pagine n. 24 / 29)	**Direttore Generale** Avvalendosi della *UOC Affari Generali*
8	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 e i collaboratori che trattano dati)	Regolamento UE (art. 39 e seg.) Guida applicativa del Garante (pagine n. 20 e seguenti)	**Direzione Aziendale** avvalendosi del *Polo Formativo* e della *UOC Affari Generali*, del *Data Protection Officer e dell'Ufficio Aziendale per la protezione dei dati*

9	Acquisizione **certificazione** ed adesione a **codici di condotta**	Regolamento UE (articoli 40 / 43) Guida applicativa del Garante (pagine n. 20 / 23)	**Direzione Aziendale** avvalendosi del *Data Protection Officer e dell'Ufficio Aziendale per la protezione dei dati*

→ **9 (nove)** sono quindi gli adempimenti riconducibili a questa prima area dell'Azienda. *****

***** Nota relativa alla nomina del **"Data Protection Officer"**

Si segnala che uno degli adempimenti più importanti, poiché collegato all'attuazione di gran parte degli altri, è la nomina del *Responsabile aziendale della protezione dei dati (DPO)*, che deve essere designato obbligatoriamente entro il 25 maggio 2018 ma che è auspicabile venga individuato prima, così che questa figura possa coordinare e supervisionare la gestione degli adempimenti descritti in questa relazione, confrontandosi con le competenti Unità Operative, Servizi e Uffici aziendali.

A livello di Regione Veneto, sembra prospettarsi una nomina a *DPO* unica per tutte le Aziende Sanitarie della Regione che, al momento, non è ancora stata definita (risulta che sia al vaglio l'ipotesi di nomina a DPO del Consorzio Arsenàl.IT).

Per quanto concerne le caratteristiche di detta nuova Figura, in estrema sintesi va detto quanto segue.

Il *Responsabile della protezione dei dati*, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà 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.
Il *Responsabile della protezione dei dati* dovrà adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il *Responsabile della protezione dei dati* non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali.
Il *Responsabile della protezione dei dati* dovrà operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (DPO esterno).

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;
  collaborare 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;
- ✓ **cooperare 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**.

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 RPD non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;

- ✓ **operare alle dipendenze del titolare oppure sulla base di un contratto di servizio** (RPD esterno);
- ✓ **disporre di risorse umane e finanziarie**, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

La nomina del *Responsabile della protezione dei dati* è obbligatoria in tutte le organizzazioni, anche pubbliche, che trattano come **attività principali i dati sensibili su larga scala**, come ospedali, assicurazioni e istituti di credito.

Chi svolge la funzione di *Responsabile della protezione dei dati*, quindi, deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali.

Il *Responsabile della protezione dei dati* deve essere nominato con delibera del direttore generale e l'atto di nomina deve essere corredato dalle relative clausole contrattuali.

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

Sia che il *Responsabile della protezione dei dati* sia interno che esterno, è necessario stipulare con il medesimo un **contratto ad hoc.**

Nel caso in cui il *Responsabile della protezione dei dati* 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 *Responsabile della protezione dei dati*.

E) Obblighi di carattere documentale

N. progr.	*Adempimento*	*Riferimento normativo*	*Area o Servizio competente per l'adempimento*
1	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)	**UOC Affari Generali**
2	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)	**UOC Affari Generali** per quanto attiene alla modulistica cartacea e **UOS Sistemi Informativi** per quanto attiene alla gestione informatica del consenso
3	**Diritto di accesso**: diritto dell'interessato ad ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano	Regolamento UE (art. 15) Guida applicativa del Garante (pagina n. 15)	**U.R.P. e Distretti Socio Sanitari** avvalendosi della *UOS Sistemi Informativi*
4	**Nomina, per l'intero ambito aziendale, dei Responsabili (interni) del trattamento dei dati**, in ottemperanza alle nuove previsioni europee: predisposizione modulistica e trasmissione delle	Regolamento UE (art. 28 e seg.) Guida applicativa del Garante (pagine n. 20 e seguenti)	**UOC Affari Generali**

	nomine con le istruzioni operative		
5	Predisposizione della modulistica e delle linee procedurali per la nomina dei **Responsabili *esterni* del trattamento dei dati** (in ottemperanza alle nuove previsioni europee)	Regolamento UE (art. 28 e seg.) Guida applicativa del Garante (pagine n. 20 e seg.)	**UOC Affari Generali**

→ **5 (cinque)** sono quindi gli adempimenti riconducibili a questa area dell'Azienda.

F) <u>Obblighi di carattere tecnologico ed informatico</u>

N.progr.	*Adempimento*	*Riferimento normativo*	*Area o Servizio competente per l'adempimento*
1	Misure tecnologiche per **adeguare i sistemi informatici ai nuovi principi europei** in materia di: ➢ *Profilazione automatizzata* ➢ *Pseudonomizzazione* ➢ *Diritto all'Oblio* ➢ *Minimizzazione dei dati* ➢ *Limitazione del trattamento*	Regolamento UE (art. 12 e seg.) Guida applicativa del Garante (pagina n. 12 e seguenti)	**UOC Servizi Tecnici e Patrimoniali e delle UOS Sistemi Informativi e UOS Ingegneria Clinica e Ufficio Aziendale per la protezione dei dati**
2	Misure tecnologiche per garantire il nuovo **diritto alla portabilità dei dati** (fra diversi *Service Provider*) **in formato interoperabile** *(queste misure si applicano esclusivamente ai trattamenti effettuati "con mezzi automatizzati")*	Regolamento UE (art. 20, 22 e 23) Guida applicativa del Garante (pagine n. 18 e 19)	**UOC Servizi Tecnici e Patrimoniali e delle UOS Sistemi Informativi e UOS Ingegneria Clinica e Ufficio Aziendale per la protezione dei dati**
3	Misure tecnologiche per garantire la protezione dei dati sia nella progettazione, che nella impostazione predefinita **(privacy by design e by default)**	Regolamento UE (art. 25 e seg.) Guida applicativa del Garante (pagina n. 24)	**UOC Servizi Tecnici e Patrimoniali e delle UOS Sistemi Informativi e UOS Ingegneria Clinica**
4	Predisposizione, gestione ed aggiornamento del **Registro delle attività di trattamento**	Regolamento UE (art. 30) Guida applicativa del Garante (pagine n. 26 e seg.)	**UOS Sistemi Informativi** *consultandosi con il Data Protection Officer e dell'Ufficio Aziendale per la protezione dei dati*
5	Predisposizione delle **Misure di sicurezza informatica dei dati**	Regolamento UE (art. 32 e seg.) Guida applicativa del Garante (pagina n. 27 e seg.)	**UOC Servizi Tecnici e Patrimoniali e delle UOS Sistemi Informativi e UOS Ingegneria Clinica**
6	**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.)	**UOC Servizi Tecnici e Patrimoniali e delle UOS Sistemi Informativi e UOS Ingegneria Clinica** *consultandosi con il Data Protection Officer e dell'Ufficio Aziendale per la protezione dei dati*
7	Predisposizione del **"Registro delle violazioni nel trattamento dei dati personali"**	Regolamento UE (art.30 / 33) Guida applicativa del	**UOC Servizi Tecnici e Patrimoniali e delle UOS Sistemi**

		Garante (pagine n. 24 / 29)	**Informativi e UOS Ingegneria Clinica** *consultandosi con il Data Protection Officer e dell'Ufficio Aziendale per la protezione dei dati*
8	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.)	**UOC Servizi Tecnici e Patrimoniali e delle UOS Sistemi Informativi e UOS Ingegneria Clinica e Ufficio Aziendale per la protezione dei dati**

→ **8 (otto)** sono quindi gli adempimenti riconducibili a questa area dell'Azienda.

G) <u>Obblighi di carattere comunicativo</u>

N. progr.	*Adempimento*	*Riferimento normativo*	*Area o Servizio competente per l'adempimento*
1	**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)	**Ufficio Relazioni con il Pubblico (U.R.P.) in collaborazione con il Responsabile della trasparenza e della prevenzione della corruzione** *consultandosi con il Data Protection Officer e con l'Ufficio Aziendale per la protezione dei dati e sulla base della documentazione che verrà fornita dalla UOC Affari Generali*
2	**Formazione a favore del personale dipendente**, così da ottemperare alle previsioni europee	Regolamento UE (art. 39) Guida applicativa del Garante (pagine n. 24 / 29)	**Polo Formativo e UOC Affari Generali**
3	Nomina dei **Responsabili "esterni"** del trattamento dei dati e dei **"Sub- Responsabili"** *(outsourcing di attività)* *(la modulistica standard sarà fornita dalla UOC Affari Generali come stabilito al punto "E" della presente Relazione)*	Regolamento UE (art. 28 e seg.) Guida applicativa del Garante (pagine n. 24 / 29)	Servizi interessati alle nomine in virtù di gare ed appalti di servizi, forniture e convenzioni con enti esterni
4	Inserimento di **clausole sulle misure di sicurezza nel trasferimento dei dati** all'interno del ***Disciplinare degli appalti pubblici****,* che prevedono un flusso di dati da Pubblica Amministrazione a impresa aggiudicataria del servizio (e viceversa)	Regolamento UE (art. 28 / 32 e seg.) Guida applicativa del Garante (pagine n. 24 / 29)	**UOC Servizi Tecnici e Patrimoniali e relative UOS dell'area informatica** *sulla base delle indicazioni dei Servizi Informatici*

→ **4 (quattro)** sono quindi gli adempimenti riconducibili a questa area dell'Azienda.

H) <u>Sanzioni previste dal Regolamento UE per la violazione degli obblighi indicati</u>

N. progr.	***Adempimento***		***Entità sanzione***
1	Registro trattamenti	⇨	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
2	Documento valutazione dei rischi	⇨	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
3	Documento di valutazione di impatto privacy	⇨	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
4	Procedura Data Breach	⇨	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
5	Accordo con contitolari	⇨	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
6	Contratto di responsabile esterno	⇨	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
7	Contratto con sub-responsabili	⇨	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
8	Nomine dipendenti e collaboratori	⇨	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
9	Corsi per gli autorizzati *(dipendenti dell'azienda)*	⇨	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
10	Informativa	⇨	Fino 20 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
11	Raccolta consensi, salvo esonero	⇨	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
12	Nomina Data Protection Officer	⇨	Fino 10 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
13	Trasferimenti dati all'estero	⇨	Fino 20 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo
14	Certificazione	⇨	Fino 20 mln/oppure se più elevato fino al 2% fatturato totale mondiale annuo

→ **14 (quattordici)** sono quindi le sanzioni previste dal Reg. UE.

Documenti citati quali fonti nella Relazione:

- *Regolamento Europeo 2016/679*
- *Guida applicativa del Garante Privacy (testo edizione aggiornata Febbraio 2018)*

Rovigo, 22 marzo 2018
U.O.C. Affari Generali