Servizio Sanitario Nazionale - Regione Veneto

AZIENDA ULSS N. 8 BERICA

Viale F. Rodolfi n. 37 – 36100 VICENZA

REGIONE DEL VENETO

ULSS8 BERICA

DELIBERAZIONE

n. 86 del 24-1-2018

O G G E T T O

Prime azioni di carattere organizzativo, gestionale e documentale volte ad ottemperare, nell'ambito dell'U.L.SS. n. 8 Berica, agli obblighi del Regolamento Europeo n. 2016/679 sulla privacy.

Proponente: UOC Affari Generali
Anno Proposta: 2018
Numero Proposta: 129

Il Direttore f.f. della U.O.C. Affari Generali, 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.

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 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 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 (non pochi) adempimenti imposti dalle norme europee.

A tale scopo, il proponente Servizio Affari Generali ha predisposto una relazione tecnica dal titolo:
"Verifica degli adempimenti in carico all'Azienda U.L.SS. n. 8 Berica 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.

E' doveroso precisare che, al momento in cui è stata redatta l'anzidetta relazione (dicembre 2017), 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").

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. 8 Berica approvato con la Deliberazione n. 79 del 18 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 dello specifico Servizio o Struttura 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.

Alla luce di tali considerazioni, nel precisare che la Relazione di cui si parla è stata presentata e condivisa in un apposito incontro tenutosi presso la Direzione Aziendale in data 11 gennaio 2018, si fa proposta di approvare, quale strumento a carattere programmatico, la Relazione tecnica predisposta dal proponente Servizio Affari Generali dal titolo: "*Verifica degli adempimenti in carico all'Azienda U.L.SS. n. 8 Berica 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, dando avvio alle prime azioni di carattere organizzativo, gestionale e documentale volte ad ottemperare, nell'ambito dell'U.L.SS. n. 8 Berica, agli obblighi del Regolamento Europeo n. 2016/679 sulla privacy.

Come da indicazioni fornite per le vie brevi dalla Direzione Strategica, 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 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.

Il medesimo Direttore ha attestato l'avvenuta regolare istruttoria della pratica anche in relazione alla sua compatibilità con la vigente legislazione regionale e statale in materia;

I Direttori Amministrativo, Sanitario e dei Servizi Socio-Sanitari hanno espresso il parere favorevole per quanto di rispettiva competenza.

Sulla base di quanto sopra

IL DIRETTORE GENERALE

DELIBERA

1. di approvare, quale strumento a carattere programmatico, la Relazione tecnica predisposta dal Servizio Affari Generali dal titolo: *"Verifica degli adempimenti in carico all'Azienda U.L.SS. n. 8 Berica 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 dare avvio, in conseguenza di quanto disposto al punto n. 1, alle prime azioni di carattere organizzativo, gestionale e documentale volte ad ottemperare, nell'ambito dell'U.L.SS. n. 8 Berica, 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 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 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;

5. di stabilire che la presente deliberazione venga pubblicata all'Albo on line dell'Azienda.

*****

Parere favorevole, per quanto di competenza:

Il Direttore Amministrativo
(App.to Dr. Tiziano Zenere)

Il Direttore Sanitario
(App.to Dr.ssa Simona Aurelia Bellometti)

Il Direttore dei Servizi Socio-Sanitari
(App.to Dr. Salvatore Barra)

IL DIRETTORE GENERALE
(F.to digitalmente Giovanni Pavesi)

REGIONE DEL VENETO ULSS8 BERICA
Documento Firmato digitalmente da PAVESI Giovanni in data 24/01/2018 alle ore 14:23

Il presente atto è eseguibile dalla data di adozione.

Il presente atto **è proposto per la pubblicazione** in data 25-1-2018 all'Albo on-line dell'Azienda con le seguenti modalità:

Oggetto e contenuto

Copia del presente atto viene inviato in data 25-1-2018 al Collegio Sindacale (ex art. 10, comma 5, L.R. 14.9.1994, n. 56).

IL RESPONSABILE PER LA GESTIONE ATTI
DEL SERVIZIO AFFARI LEGALI E
AMMINISTRATIVI GENERALI

REGIONE DEL VENETO
ULSS8 BERICA

Servizio Sanitario Nazionale - Regione Veneto
AZIENDA ULSS N. 8 BERICA
Viale F. Rodolfi n. 37 – 36100 VICENZA
COD. REGIONE 050–COD. U.L.SS.508 COD.FISC. E P.IVA 02441500242–Cod. iPA AUV
Tel. 0444 753111 - Fax 0444 753809 Mail protocollo@aulss8.veneto.it
PEC protocollo.centrale.aulss8@pecveneto.it
www.aulss8.veneto.it

U.O.C. Affari Generali
Viale Rodolfi, n. 37 – 36100 Vicenza
Direttore f.f.: avv. Stefano Cocco

RELAZIONE TECNICA per la Direzione Strategica

Oggetto: Verifica degli adempimenti in carico all'Azienda U.L.SS. n. 8 Berica in conseguenza della diretta applicazione, a far data dal 25 maggio 2018, del nuovo Regolamento Europeo sulla privacy.

La presente relazione, a cura dell'Ufficio affari generali e organizzazione dell'ULSS n. 8 Berica, è composta di nove 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 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 (non pochi) 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").*

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. 8 Berica approvato con la Deliberazione n. 79 del 18 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 dello specifico Servizio o Struttura di questa ULSS chiamata a farvi fronte.

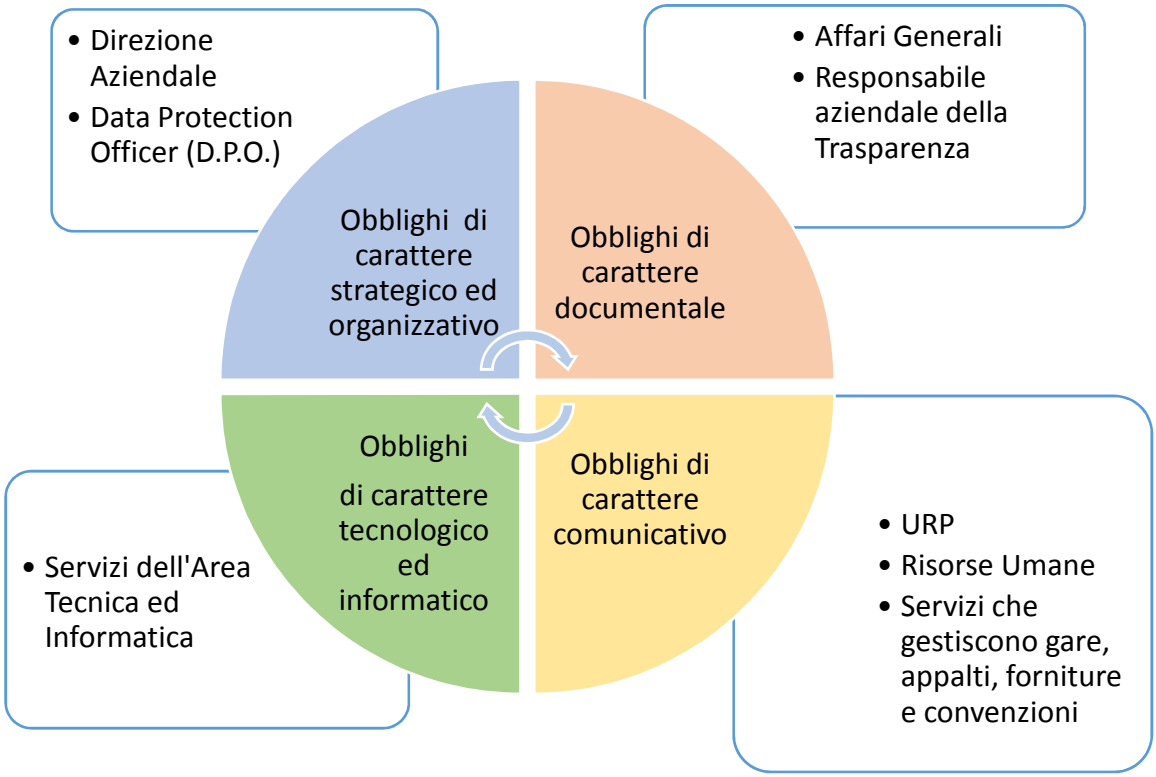
C) Ambiti di attività aziendali correlati ai nuovi obblighi europei in materia di privacy

In base allo studio effettuato da questo Ufficio, 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. 8 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 e della Dottrina sino ad oggi emanate, citate quali fonti nella presente relazione.

D) Obblighi di carattere strategico ed organizzativo

N. progr.	*Adempimento*	*Riferimento normativo*	*Area o Servizio 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 (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) Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)	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
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) Guida giuridica "Italia Oggi" (pagina n. 27 e seguenti)	**Direttore Generale** *Avvalendosi della UOC Servizi Tecnici e Patrimoniali e delle sue relative UOS dell'area informatica*

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) Guida giuridica "Italia Oggi" (pagina n. 46 e seguenti)	**Direttore Generale** avvalendosi del *Data Protection Officer*
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) Guida giuridica "Italia Oggi" (pagina n. 39 e seguenti)	**Direzione Aziendale** avvalendosi del *Data Protection Officer*
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) Guida giuridica "Italia Oggi" (pagina n. 39 e seguenti)	**Direzione Aziendale** avvalendosi del *Data Protection Officer*
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) Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)	**Direzione Aziendale** avvalendosi del *Data Protection Officer*
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) Guida giuridica "Italia Oggi" (pagina n. 20 / 22 – 63 / 67 e 116 / 135)	**Direttore Generale**

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)	Regolamento UE (art. 39 e seg.) Guida applicativa del Garante (pagine n. 20 e seguenti) Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)	**Direzione Aziendale** avvalendosi del *Data Protection Officer e del Servizio Risorse Umane*
9	Acquisizione **certificazione** ed adesione a **codici di condotta**	Regolamento UE (articoli 40 / 43) Guida applicativa del Garante (pagine n. 20 / 23) Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)	**Direzione Aziendale** avvalendosi del *Data Protection Officer*

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*, 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 i competenti Servizi e Uffici aziendali.

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

il *Data Protection Officer* (in italiano: Responsabile della protezione dei dati – RDP) è una figura dirigenziale, di alta professionalità, a metà tra il *consulente* ed il *revisore* e non dovrebbe ricoprire ruoli gestionali rispetto all'attività dell'azienda o ai fini istituzionali della P.A.

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 RDP 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 RPD, quindi, deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali.

Non deve, inoltre, essere in **conflitto di interessi** in quanto il Regolamento UE vieta di nominare RDP anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi.

A tale riguardo la Dottrina *(vedasi alcuni articoli del "Sole 24 Ore" o la Guida giuridica di "Italia Oggi")* esclude che possa essere nominato RPD, 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).*

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

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

Nel caso il cui il RDP 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 RDP.

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

**

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) Guida giuridica "Italia Oggi" (pagina n. 55 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) Guida giuridica "Italia Oggi" (pagina n. 60 e seguenti)	**UOC Affari Generali**
3	**Diritto di accesso**: armonizzazione delle procedure e della modulistica aziendale in materia di *accesso civico*, di *accesso generalizzato* e di *accesso documentale* con i principi e le nuove prescrizioni di matrice europea	Regolamento UE (art. 15) Guida applicativa del Garante (pagina n. 15) Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)	**Responsabile Aziendale della Trasparenza e della Prevenzione della Corruzione**

4	**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) Guida giuridica "Italia Oggi" (pagina n. 47 e seguenti)	**UOC Affari Generali**
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.) Guida giuridica "Italia Oggi" (pagina n. 47 e seguenti)	**UOC Affari Generali**
6	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 nella presente Relazione)*	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)	**UOC Affari Generali** previa intesa con il *Data Protection Officer*

7	Nel contesto dell'atto deliberativo di cui al punto n. 6, va effettuata la **raccolta e l'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* Così da costituire il c.d. **"Dossier privacy"** *(c.d. "compliance")*	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)	**UOC Affari Generali** previa intesa con il *Data Protection Officer*

7 (sette) sono quindi gli adempimenti riconducibili a questa area dell'Azienda.

REGIONE DEL VENETO
ULSS8 BERICA

Servizio Sanitario Nazionale - Regione Veneto
AZIENDA ULSS N. 8 BERICA
Viale F. Rodolfi n. 37 – 36100 VICENZA
COD. REGIONE 050–COD. U.L.SS.508 COD.FISC. E P.IVA 02441500242–Cod. iPA AUV
Tel. 0444 753111 - Fax 0444 753809 Mail protocollo@aulss8.veneto.it
PEC protocollo.centrale.aulss8@pecveneto.it
www.aulss8.veneto.it

F) Obblighi di carattere tecnologico ed informatico

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) Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)	**UOC Servizi Tecnici e Patrimoniali e sue relative UOS dell'area informatica**
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) Guida giuridica "Italia Oggi" (pagina n. 99 e seguenti)	**UOC Servizi Tecnici e Patrimoniali e sue relative UOS dell'area informatica**
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) Guida giuridica "Italia Oggi" (pagina n. 27 e seguenti)	**UOC Servizi Tecnici e Patrimoniali e sue relative UOS dell'area informatica**
4	Predisposizione dei **Registri delle attività di trattamento**	Regolamento UE (art. 30) Guida applicativa del Garante (pagine n. 26 e seg.) Guida giuridica "Italia Oggi" (pagina n. 28 e seguenti	**UOC Servizi Tecnici e Patrimoniali e sue relative UOS dell'area informatica** *consultandosi con il Data Protection Officer*

5	Predisposizione delle **Misure di sicurezza informatica dei dati** con la riedizione del ***Documento Programmatico della Sicurezza***	Regolamento UE (art. 32 e seg.) Guida applicativa del Garante (pagina n. 27 e seg.) Guida giuridica "Italia Oggi" (pagina n. 31 e seguenti)	**UOC Servizi Tecnici e Patrimoniali e sue relative UOS dell'area informatica**
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.) Guida giuridica "Italia Oggi" (pagina n. 36 e seguenti)	**UOC Servizi Tecnici e Patrimoniali e sue relative UOS dell'area informatica** *consultandosi con il Data Protection Officer*
7	Predisposizione del **"Registro delle violazioni nel trattamento dei dati personali"**	Regolamento UE (art.30 / 33) Guida applicativa del Garante (pagine n. 24 / 29) Guida giuridica "Italia Oggi" (pagina n. 39 e seguenti)	**UOC Servizi Tecnici e Patrimoniali e sue relative UOS dell'area informatica** *consultandosi con il Data Protection Officer*
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.) Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)	**UOC Servizi Tecnici e Patrimoniali e sue relative UOS dell'area informatica**

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

G) Obblighi di carattere comunicativo

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) Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)	**Ufficio Relazioni con il Pubblico (U.R.P.)** *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*
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) Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)	**UOC Gestione Risorse Umane**
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) Guida giuridica "Italia Oggi" (pagina n. 23 e seguenti)	Servizi interessati alle nomine in virtù di gare ed appalti di servizi, forniture e convenzioni con enti esterni In particolare, quindi: ✓ **UOC Servizi Tecnici sue relative UOS dell'area informatica** ✓ **UOC Provveditorato** ✓ **Direzione Amm.va Osped.ra** ✓ **Direzione Amm.va Territ.le**

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) Guida giuridica "Italia Oggi" (pagina n. 34 in particolare)	**UOC Servizi Tecnici e Patrimoniali e sue relative UOS dell'area informatica** *sulla base delle indicazioni dei Servizi Informatici (come da D.P.S.)*

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

REGIONE DEL VENETO
ULSS8 BERICA

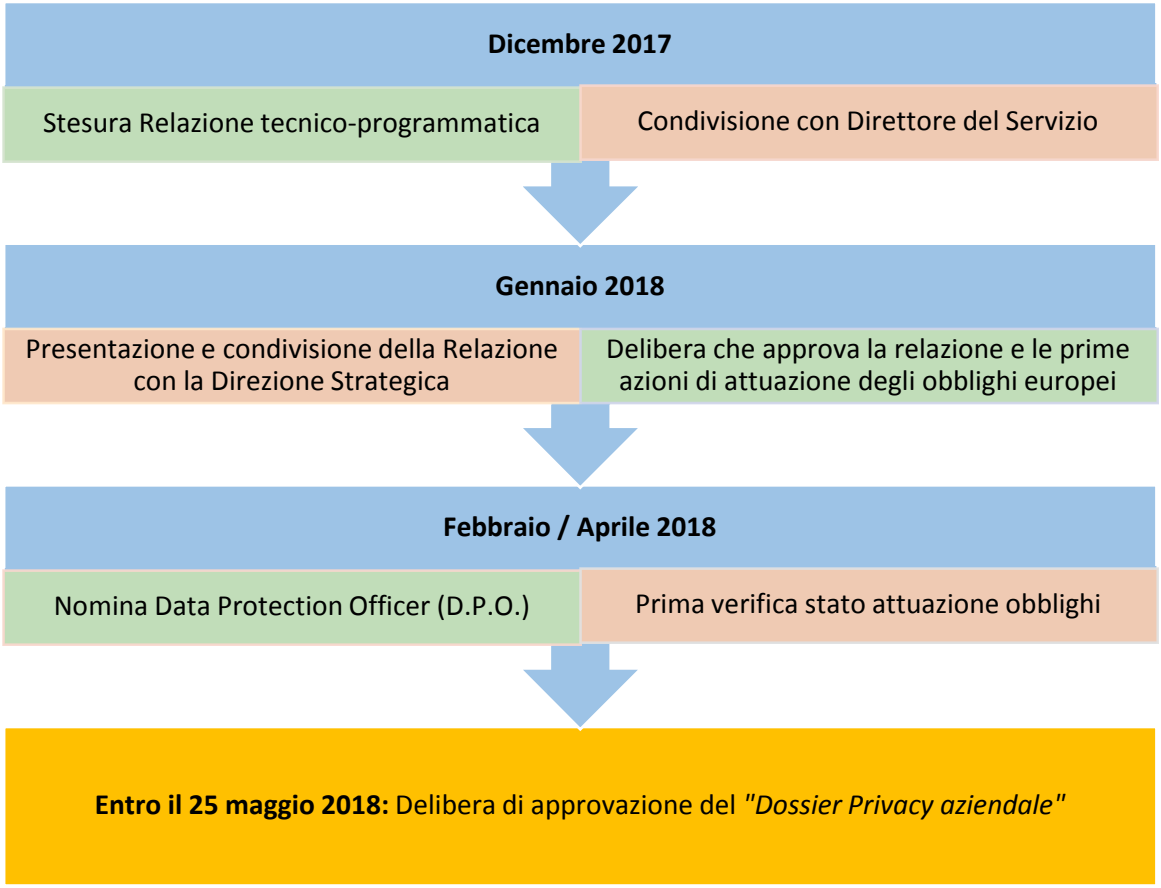
Servizio Sanitario Nazionale - Regione Veneto
AZIENDA ULSS N. 8 BERICA
Viale F. Rodolfi n. 37 – 36100 VICENZA
COD. REGIONE 050–COD. U.L.SS.508 COD.FISC. E P.IVA 02441500242–Cod. iPA AUV
Tel. 0444 753111 - Fax 0444 753809 Mail protocollo@aulss8.veneto.it
PEC protocollo.centrale.aulss8@pecveneto.it
www.aulss8.veneto.it

H) Sanzioni previste dal Regolamento UE per la violazione degli obblighi indicati

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.

I) Cronoprogramma delle azioni da effettuare per mettere a norma l'ULSS n. 8



- **Documenti citati quali fonti nella Relazione:**

  - *Regolamento Europeo 2016/679 (testo al 24.11.2017)*
  - *Guida applicativa del Garante Privacy (testo al 24.11.2017)*
  - *Guida giuridica di "Italia Oggi" (del 18.10.2017)*

Vicenza, 22 gennaio 2018

U.O.C. Affari Generali — Ufficio affari generali e organizzazione

***