ALLEGATO 3

Regione Marche
Azienda Sanitaria Unica Regionale
AOO:Registro ASUR - ANCONA
0009861 | 03/04/2018
ASUR | AAGG | P

AREA DIPARTIMENTALE AFFARI GENERALI E CONTENZIOSO

Regione Marche
Azienda Sanitaria Unica Regionale
AOO:Registro ASUR - ANCONA
0009893 | 04/04/2018
ASUR | AAGG | P

Al Garante per la protezione dei dati personali
Piazza di Montecitorio, 121
00186 - Roma
via Pec: urp@gpdp.it protocollo@pec.gpdp.it

OGGETTO: Regolamento UE 2016/679 (c.d. GDPR) - Quesiti in ordine all'applicazione delle disposizioni

PREMESSO CHE

- L'Azienda Sanitaria Unica Regionale (ASUR) è stata istituita con Legge regionale 20 giugno 2003 n. 13 "Riorganizzazione del Servizio Sanitario regionale", e successivamente riformata ai sensi della Legge regionale n. 17/2010 e della Legge regionale n. 17/2011;

- Ai sensi dell'art. 3, Legge regionale 20 giugno 2003, n. 13, la Giunta regionale Marche, nel rispetto del piano socio-sanitario regionale, esercita le funzioni di indirizzo e controllo in materia di sanità e di integrazione socio-sanitaria;

- L'ASUR "esercita a livello centralizzato le funzioni d'indirizzo, coordinamento e controllo dell'attività aziendale e delle Aree Vaste, nel rispetto degli obiettivi assegnati e delle direttive impartite dalla Giunta Regionale";

- L'ASUR è attualmente articolata in n. 5 Aree Vaste, aventi il compito di assicurare alla popolazione residente le prestazioni incluse nei livelli essenziali di assistenza (LEA) e l'equo accesso ai servizi e alle funzioni di tipo sanitario, sociale e di elevata integrazione sanitaria, organizzate nel territorio;

- In data 4 gennaio 2007, la Giunta regionale Marche ha adottato il "Regolamento per il trattamento di dati sensibili e giudiziari della Giunta regionale, delle Aziende del servizio sanitario regionale, degli Enti e delle Agenzie regionali e degli altri Enti controllati e vigilati dalla Regione in attuazione del decreto legislativo 30 giugno 2003, n. 196 (articolo 20, comma 2, e articolo 21, comma 2)" (Regolamento regionale n. 1/2007);

- Il predetto Regolamento, ai sensi degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n 196 "Codice in materia di protezione dei dati personali", identifica i tipi di dati e le operazioni eseguibili da parte della Giunta regionale, nonché da parte delle Aziende del servizio sanitario della Regione, degli enti e agenzie

Azienda Sanitaria Unica Regionale
Via Oberdan, 2 - 60122 Ancona C.F. e P.IVA 02175860424 tel. 071/2911531 fax 071/2911500
sito internet www.asur.marche.it

regionali e degli altri enti per i quali la Regione esercita poteri di indirizzo e controllo, compresi gli enti che fanno riferimento a due o più Regioni, nello svolgimento delle loro funzioni istituzionali, con riferimento ai trattamenti di dati sensibili e giudiziari effettuati per il perseguimento delle rilevanti finalità di interesse pubblico individuate da espressa disposizione di legge, ove non siano legislativamente specificati i tipi di dati e le operazioni eseguibili;

- Gli allegati A e B al Regolamento regionale n. 1/2007, sopra menzionato, individuano i dati sensibili e giudiziari oggetto di trattamento, le finalità di interesse pubblico perseguite, nonché le operazioni eseguibili;

- Ai sensi dell'art. 4 del Regolamento regionale n. 1/2007, con apposito regolamento del Consiglio regionale viene aggiornata e integrata periodicamente l'identificazione dei tipi di dati e di operazioni eseguibili nello svolgimento delle funzioni istituzionali;

TUTTO CIÒ PREMESSO

la scrivente Azienda si trova in necessità di porre i seguenti quesiti all'intestata Autorità Garante, al fine di potersi conformare a quanto disposto dal Regolamento UE 2016/679 (c.d. GDPR):

I. Con specifico riferimento a quanto stabilito dall'art. 30 GDPR, ovvero all'obbligo di istituzione di appositi «Registri delle attività di trattamento» da parte di ogni Titolare del trattamento dei dati, si rappresenta che la Regione Marche, tramite il Regolamento Regionale 4 gennaio 2007, n. 1, già menzionato in premessa, ha provveduto a identificare i tipi di dati e le operazioni eseguibili da parte delle Aziende del servizio sanitario della Regione nello svolgimento delle loro funzioni istituzionali.
I dati sensibili e giudiziari oggetto di trattamento, le finalità di interesse pubblico perseguite, nonché le operazioni eseguibili, sono infatti individuati nelle schede contenute negli allegati A e B al suddetto Regolamento.

Inoltre, ai sensi dell'art. 4 del Regolamento regionale n. 1/2007, con apposito regolamento del Consiglio regionale viene aggiornata e integrata periodicamente l'identificazione dei tipi di dati e di operazioni eseguibili nello svolgimento delle funzioni istituzionali, previo parere del Garante per la protezione dei dati personali.

Ciò premesso, si chiede all'intestata Autorità Garante:

a) se l'adozione e l'attuazione di tale Regolamento regionale - che viene allegato alla presente - nei termini indicati possa essere di per sé sufficiente ad assolvere all'obbligo di istituzione dei «Registri delle attività di trattamento» di cui all'art. 30 del GDPR, tenuto conto che, in caso contrario, l'adeguamento a tale disposizione normativa comporterebbe in capo alla scrivente Amministrazione ingenti oneri di attuazione, stante la varietà e complessità di dati trattati per le proprie finalità istituzionali;
oppure

Azienda Sanitaria Unica Regionale
Via Oberdan, 2 - 60122 Ancona C.F. e P.IVA 02175860424 tel. 071/2911531 fax 071/2911500
sito Internet www.[illegible]

b) se tali registri riguardino operazioni di trattamento diverse da quelle codificate nelle schede di cui ai predetti allegati A e B al Regolamento regionale n. 1/2007, e - qualora debba trovare applicazione tale seconda ipotesi - resti l'obbligo preventivo di aggiornamento del Regolamento regionale ai sensi dell'art. 4, e quale debba essere in tal caso la *consecutio* operativa corretta per non incorrere in ipotesi di irregolarità nel trattamento dei dati.

II. Con riferimento al secondo quesito, occorre invece muovere dall'art. 37 del GDPR, «Designazione del responsabile della protezione dei dati».

A tal riguardo, la scrivente Azienda si trova nella necessità di richiedere all'Autorità Garante un'individuazione più puntuale dei requisiti professionali che la figura del *Data Protection Officer* dovrà possedere, con specifico riguardo al contesto delle aziende erogatrici di servizi sanitari, stante la delicatezza dei trattamenti dei dati da queste effettuati.

È infatti evidente come la figura del Responsabile della protezione dei dati sia una figura complessa, di alta professionalità, dotata di ampia libertà di azione.

Viene in rilievo come tale figura debba possedere qualità professionali e conoscenze specialistiche di normativa e prassi in materia di protezione dei dati, con un livello di conoscenze proporzionato alla complessità e quantità dei dati soggetti a trattamento (art. 37, par. 5, GDPR).

Nell'esecuzione dei propri compiti, il DPO è inoltre chiamato ad operare con un sufficiente livello di autonomia all'interno dell'organizzazione, riportando direttamente al vertice aziendale.

L'intestata Autorità Garante ha infatti avuto modo di precisare che "nel caso in cui si opti per un RPD interno, sarebbe in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione" (cfr. "Nuove Faq sul Responsabile della Protezione dei dati in ambito pubblico").

Al riguardo si domanda cosa debba intendersi per «alta professionalità» rispetto all'argomento privacy (e, in particolare, se si faccia riferimento ad una professionalità con formazione di tipo amministrativo o con competenze di tipo informatico) e cosa, invece, per espletamento delle funzioni «con autonomia e indipendenza».

Tali caratteristiche, unite alla mancanza a livello nazionale di precise indicazioni su quali requisiti debba possedere il DPO, rendono infatti assai difficoltosa la sua individuazione all'interno dell'organizzazione aziendale, e di fatto sembrerebbero voler orientare la preferenza su un soggetto/società esterna all'ente.

III. Si chiede, infine, di chiarire rapporti e differenze sussistenti tra *Data Protection Officer* e Amministratore di Sistema, precisando se le due figure possano coesistere, o se l'entrata in vigore del GDPR, viceversa, travolga le mansioni

Azienda Sanitaria Unica Regionale
Via Oberdan, 2 - 60122 Ancona C.F. e P.IVA 02175860424 tel. 071/2911531 fax 071/2911500
sito internet www.asur.marche.it

dell'Amministratore di Sistema, sostituendolo con la nuova figura, che dovrà dunque disporre anche di idonee competenze tecniche alla protezione "materiale" dei dati conservati digitalmente.

La scrivente Azienda dispone già, infatti, della figura dell'Amministratore di Sistema, il quale, in conformità al Regolamento Aziendale approvato con Determina n. 22/ASURDG del 15/01/2014, che si allega, è chiamato a vigilare sulla sicurezza delle banche dati e sulla corretta gestione delle reti telematiche.

Più in particolare, ai sensi dell'art. 7 del predetto Regolamento aziendale, l'Amministratore di sistema:

a) Monitora l'infrastruttura informatica di competenza attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
b) Introduce ed integra nuove tecnologie negli ambienti esistenti;
c) Installa e configura nuovo hardware/software sia lato client sia lato server;
d) Applica le patch e gli aggiornamenti necessari al software di base ed applicativo,
e) Modifica le configurazioni in base alle esigenze dell'organizzazione;
f) Gestisce e tiene aggiornati gli account utente ed i relativi profili di autorizzazione;
g) Fornisce risposte alle questioni tecniche sollevate dall'utenza;
h) Pone rimedio ai problemi/guasti tramite tecniche di *troubleshooting*;
i) Pianifica e verifica la corretta esecuzione dei backup e delle repliche;
j) Documenta le operazioni effettuate (*Logbook*), le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni ai problemi;
k) Ottiene le migliori prestazioni possibili con l'hardware a disposizione;
l) Opera secondo le prescrizioni di sicurezza e le procedure interne previste.

Tanto premesso, si rappresenta l'estrema difficoltà interpretativa e, conseguentemente, applicativa delle disposizioni di cui è prossima l'entrata in vigore, nonché la stringente urgenza di avere riscontro alla presente richiesta di chiarimenti, in quanto - ove ciò non dovesse avvenire - la scrivente Azienda non disporrà di elementi concreti atti a sopperire alle esposte problematiche e criticità.

Distinti saluti.

IL DIRETTORE DELL'AREA
Avv. Lucia Cancellieri

All. 1 Regolamento Regionale Marche 4 gennaio 2007, n. 1
All. 2 Regolamento Aziendale ASUR approvato con Determina n. 22/ASURDG del 15/01/2014

Il responsabile della fase istruttoria:
Dott. Alessandro Cola
Area Affari Generali e Segreteria ASUR

Azienda Sanitaria Unica Regionale
Via Oberdan, 2 - 60122 Ancona C.F. e P.IVA 02175860424 tel. 071/2911531 fax 071/2911500
sito internet www.asur.marche.it