

DETERMINA DEL DIRETTORE GENERALE

Oggetto: Regolamento per la protezione dei dati personali presso l’Azienda Ospedaliero – Universitaria Ospedali Riuniti di Ancona – Approvazione

VISTO il documento istruttorio, riportato in calce alla presente determina, dal quale si rileva la necessità di provvedere a quanto in oggetto specificato;

RITENUTO, per i motivi riportati nel predetto documento istruttorio e che vengono condivisi, di adottare il presente atto;

ACQUISITI i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario, ciascuno per quanto di rispettiva competenza;

DETERMINA

1. di adottare il regolamento per la protezione dei dati personali presso l’Azienda Ospedaliero – Universitaria Ospedali Riuniti di Ancona (doc. n. 1), da considerarsi parte integrante e sostanziale del presente provvedimento, la cui predisposizione e stesura è stata effettuata congiuntamente dalla SO Affari Legali e Contenzioso – Ufficio DPO e dalla SO Affari Generali, Convenzioni e Ricerca – Ufficio Referente aziendale privacy;
2. di precisare che il regolamento (doc. n. 1), di cui al presente provvedimento, verrà pubblicato sul sito istituzionale (www.ospedaliriuniti.marche.it – sezione privacy e note legali);
3. di dare mandato al responsabile del procedimento del presente atto di provvedere alla pubblicazione dello stesso, nel rispetto delle prescrizioni di cui al D. Lgs. 33/2013 e s.m.i., sul sito istituzionale aziendale;
4. di dare atto che dall’adozione del presente provvedimento non deriveranno costi aggiuntivi sul bilancio aziendale;
5. di trasmettere il presente atto al Collegio Sindacale a norma dell’art. 17 della L.R. 26/96 e s.m.i.;
6. di dare atto che la presente determina non è soggetta al controllo della Giunta Regionale ai sensi dell’art. 4 della Legge 412/91 e dell’art. 28 della L.R. 26/96 e s.m.i. e diventerà esecutiva dalla data di pubblicazione all’albo pretorio dell’Azienda (art. 28, comma 6, L.R. 26/96 e s.m.i.).

IL DIRETTORE GENERALE

(Michele Caporossi)



IL DIRETTORE AMMINISTRATIVO
(Antonello Maraldo)

IL DIRETTORE SANITARIO
(Arturo Pasqualucci)

Documento informatico firmato digitalmente, ai sensi del D.L.vo 82/2005 e s.m.i.

DOCUMENTO ISTRUTTORIO

(SO Affari Generali, Convenzioni e Ricerca)

Normativa di riferimento

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
- D. Lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) così come novellato dal D. Lgs. 10 agosto 2018 n. 101.
- Manuale RPD: *"Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e para pubblici per il rispetto del Regolamento Generale sulla protezione dei dati dell'Unione Europea"*, approvato dalla Commissione luglio 2019.

Motivazione:

Il Regolamento Europeo n. 679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, all'art. 5, attribuisce al titolare la competenza del rispetto dei principi fondamentali in materia di trattamento di dati personali ("liceità, correttezza e trasparenza", "limitazione della finalità", "minimizzazione dei dati", "esattezza"; "limitazione della conservazione" e "integrità e riservatezza").

Al fine di assicurare il rispetto dei principi sopra citati il titolare deve mettere in atto misure tecniche ed organizzative adeguate ed efficaci, valutando periodicamente l'efficacia delle stesse, ed essere in grado di dimostrare la conformità delle attività di trattamento condotte alla normativa vigente in materia di protezione dei dati personali cd. principio di responsabilizzazione.

Il considerando 74 precisa, altresì, che il titolare nell'individuazione delle misure da porre in essere dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, dello stato dell'arte, dei costi di attuazione nonché del rischio per i diritti e le libertà delle persone fisiche.

In particolare, il titolare del trattamento deve individuare, come previsto dall'art. 25 del reg. UE 2016/679, le misure tecniche e organizzative adeguate, sia al momento di determinare i mezzi del trattamento sia all'atto



del trattamento stesso, in modo tale da assicurare il trattamento dei soli dati personali necessari per ogni specifica finalità del trattamento provvedendo alla conservazione e all'accessibilità degli stessi in termini strettamente funzionali alle suddette finalità.

L'Azienda ha già adottato alcune misure organizzative volte a disciplinare specifici aspetti o aree concernenti la protezione dei dati personali, quali a titolo esemplificativo e non esaustivo:

- procedura per la gestione delle violazioni;
- procedura per la gestione dei diritti dell'interessato;
- procedura per il trattamento dei dati genetici e per ricerca scientifica;
- linee operative in materia di trattamento di dati personali negli studi clinici;
- informative per specifiche finalità;
- istruzioni per i designati e autorizzati.

L'esperienza maturata dall'Azienda durante i primi anni di applicazione del citato regolamento ha indotto la Direzione a stabilire ulteriori modalità organizzative, finalizzate a tracciare un quadro generale di riferimento, coerente con i documenti di dettaglio elaborati in precedenza, che consenta all'Azienda di agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE 2016/679.

A tal fine la SO Affari Legali e Contenzioso – Ufficio DPO e la SO Affari Generali, Convenzioni e Ricerca – Ufficio Referente aziendale privacy hanno supportato la Direzione nella predisposizione e stesura del Regolamento qui allegato.

Considerata la complessità e la molteplicità delle attività istituzionali svolte dall'Azienda si è ritenuto necessario individuare in modo specifico compiti e responsabilità, oltre a quelli attribuiti dalla norma al titolare, che coinvolgano tutti coloro che in Azienda nel proprio ruolo e nelle proprie funzioni concorrono all'attuazione della normativa di settore vigente con conseguente responsabilizzazione di ogni struttura aziendale e di figure specificamente individuate affinché al titolare del trattamento dati sia consentito l'effettivo raggiungimento delle finalità previste dalla normativa sopra citata.

Il regolamento individua innanzitutto le attività a livello macro, previste dalla normativa, che devono essere implementate nell'ambito del sistema aziendale di protezione dei dati personali.

Quindi con riferimento a ciascuna *macro* attività sono stati assegnati compiti e responsabilità alle diverse figura/strutture aziendali coinvolte, differenziando il contributo di ognuno, sulla base del *framework* della matrice di RACI (*Responsible – Accountable – Consulted, Informed*). Tale possibilità è prevista dall'art. 2 quaterdecies, comma 1, D.lgs. 196/2003 e ss.mm.ii., in base al quale il titolare può

"prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta".

In particolare le figure/strutture aziendali che concorrono al sistema di protezione dei dati personali possono ricoprire, in base alla specifica attività, il ruolo di:



- *preposto*, se risulta essere la struttura aziendale competente della specifica attività; nel caso in cui l'esecuzione dell'attività richieda il coinvolgimento di altre strutture che ricoprono il ruolo di "collaboratore", la struttura "preposta" assume anche l'onere di coordinare il contributo proveniente dalle prime;
- *collaboratore*, se la struttura è tenuta a supportare quella preposta (competente a gestire la specifica attività) fornendo, ad esempio, informazioni ben precise;
- *supervisore*, solo il DPO a cui è attribuita *ex lege* la funzione di controllo.

Esito dell'istruttoria

Per quanto sopra esposto si propone:

1. di adottare il regolamento per la protezione dei dati personali presso l'Azienda Ospedaliero – Universitaria Ospedali Riuniti di Ancona (doc. n. 1), da considerarsi parte integrante e sostanziale del presente provvedimento, la cui predisposizione e stesura è stata effettuata congiuntamente dalla SO Affari Legali e Contenzioso – Ufficio DPO e dalla SO Affari Generali, Convenzioni e Ricerca – Ufficio Referente aziendale privacy;
2. di precisare che il regolamento (doc. n. 1), di cui al presente provvedimento, verrà pubblicato sul sito istituzionale (www.ospedaliriuniti.marche.it – sezione privacy e note legali);
3. di dare mandato al responsabile del procedimento del presente atto di provvedere alla pubblicazione dello stesso, nel rispetto delle prescrizioni di cui al D. Lgs. 33/2013 e s.m.i., sul sito istituzionale aziendale;
4. di dare atto che dall'adozione del presente provvedimento non deriveranno costi aggiuntivi sul bilancio aziendale;
5. di trasmettere il presente atto al Collegio Sindacale a norma dell'art. 17 della L.R. 26/96 e s.m.i.;
6. di dare atto che la presente determina non è soggetta al controllo della Giunta Regionale ai sensi dell'art. 4 della Legge 412/91 e dell'art. 28 della L.R. 26/96 e s.m.i. e diventerà esecutiva dalla data di pubblicazione all'albo pretorio dell'Azienda (art. 28, comma 6, L.R. 26/96 e s.m.i.).

L'Addetto alla Fase Istruttoria

(Silvia Duranti)

Si attesta l'avvenuta verifica circa l'insussistenza di situazioni, anche potenziali, di conflitto di interessi ai sensi dell'art. 6-*bis* della L. 241/1990 e s.m.i.

Il Responsabile del procedimento

Il Direttore

SO Affari generali, convenzioni e Ricerca
(Dott.ssa Cinzia Cocco)



Il Direttore S.O. attesta la regolarità del presente atto e ne certifica la conformità alle disposizioni vigenti.

IL DIRETTORE

S.O. Affari Generali, Convenzioni e Ricerca
Ufficio Referente aziendale privacy
(Dott.ssa Cinzia Cocco)

IL DIRETTORE

S.O. Affari Legali e Contenzioso
Ufficio DPO
(Dott.ssa Marianna Catalini)

Documento informatico firmato digitalmente, ai sensi del D.L.vo 82/2005 e s.m.i.

ALLEGATI

Documento n. 1: regolamento per la protezione dei dati personali presso l'Azienda Ospedaliero – Universitaria Ospedali Riuniti di Ancona

