DELIBERAZIONE DEL DIRETTORE GENERALE

N. 911 DEL 27.11.2019

Struttura proponente: U.O.C. Sistema Informativo, ICT e nuove tecnologie dell'informazione.

Oggetto: Procedura aziendale per la gestione dei collegamenti remoti autorizzati (VPN – Virtual Private Network) ai sensi delle normative vigenti (Regolamento UE 679/2016, D.Lgs 101/2018) in ambito del trattamento dei dati personali.

Proponente il Direttore dell'U.O.C. Sistema Informativo. ICT e nuove tecnologie dell'informazione che, con la sottoscrizione del presente atto, a seguito dell'istruttoria effettuata, attesta che l'atto è legittimo nella forma e nella sostanza ed è utile per il servizio pubblico.

F.to Il Direttore ad interim dell'U.O.C. Sistema Informativo. ICT e nuove tecnologie dell'informazione
Ing. Ciro BRUNO

Pareri ex art. 3 D.L.vo n. 502/92 e succ. mod.

favorevole
F.to Il Direttore Amministrativo
Dott. Laura COPPOLA

favorevole
F.to Il Direttore Sanitario
Dott. Emilia Anna VOZZELLA

Il Direttore ad interim dell'U.O.C. Sistema Informativo, ICT e nuove tecnologie dell'informazione

Premesso che:

- la disciplina introdotta dal Regolamento europeo per la protezione dei dati personali, Regolamento (UE) 2016/679 (c.d. GDPR), è direttamente applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018. Il GDPR stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché norme relative alla libera circolazione di tali dati. Il D.lgs. n. 101 del 10 agosto 2018 reca disposizioni per l'adeguamento della normativa nazionale al GDPR prevedendo severe sanzioni in caso di inottemperanza;
- la principale novità introdotta dal Regolamento consiste nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato sulla valutazione del rischio, in luogo del precedente approccio basato su adempimenti, e consegna la protezione dei dati nelle mani del Titolare del trattamento il quale, grazie al principio di responsabilizzazione, ("accountability") potrà, nei limiti e dentro i parametri delineati dal Regolamento, adottare le misure che ritiene più opportune a comprovare il conseguimento degli obiettivi da raggiungere, o raggiunti, nel rispetto dei principi che presiedono il trattamento dei dati personali;
- l'entrata in vigore di tale Regolamento Europeo impone alle PP.AA. di individuare azioni e misure di sicurezza organizzative adeguate a proteggere lo specifico patrimonio informativo, nel rispetto del principio della "privacy by design" e di documentare, attraverso un apposito sistema di evidenze e procedure, le scelte effettuate e il mantenimento costante nel tempo dei relativi standard di sicurezza;
- la protezione dei dati e la loro tenuta in sicurezza sono, infatti, requisiti indispensabili di qualità del sistema informativo, il cui rispetto deve tradursi in un vero e proprio sistema di misure tecniche e organizzative adeguate, capaci non solo di implementare gli adempimenti previsti dal D.Lgs. n. 196/2003 e ss.mm.ii. ma di strutturare un vero e proprio "Sistema gestionale Privacy" ai sensi del Regolamentò U.E. n. 679/2016;

Dato atto che:

- per ottemperare correttamente a quanto stabilito nel GDPR l'Azienda sta ponendo in essere tutte le misure necessarie ed urgenti per la programmazione e l'attuazione delle attività propedeutiche alla compliance al GDPR e per l'attivazione di "policy" specifiche articolate e strutturate;
- in considerazione della gravosità e molteplicità degli adempimenti dettati dalla vigente normativa in materia di tutela della privacy e dell'esigenza di costruire ed implementare uno specifico ed articolato "Modello gestionale privacy" capace di supportare l'Azienda Ospedaliera in termini di adeguata assistenza giuridica, consulenza tecnica e organizzativa, attraverso l'impostazione di un modello organizzativo e procedurale in grado di assicurare e di gestire gli adempimenti e le

misure previste dalla nuova normativa nazionale ed europea, è necessario predisporre un regolamento disciplinante la materia in oggetto;

Precisato che:

- in attuazione della normativa vigente l'A.O.U. ha nominato un Data Protection Officer (DPO) o, nella versione italiana, Responsabile della Protezione dei Dati (RPD), figura prevista dall'art.37 del GDPR;
- il DPO è un professionista con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali;

Considerato che:

- l'implementazione del "Sistema gestionale Privacy" implica la necessità di generare nell'organizzazione la piena consapevolezza del rischi inerenti ai trattamenti dei dati e le responsabilità connesse, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante dell'intero asset informativo di un'organizzazione, con particolare attenzione ai dati sanitari (ivi compresi i dati biometrici e genetici), nonché ai cosiddetti dati sensibili sotto il profilo dei diritti e delle libertà fondamentali dell'individuo;
- per il raggiungimento di tale obiettivo è necessario responsabilizzare anche tutti i soggetti esterni che trattano o elaborano i dati personali/particolari per conto dell'Azienda Ospedaliera, sulle responsabilità connesse alla sicurezza e protezione degli stessi (ad esempio fornitori di servizi esternalizzati, siano "outsourcer" tradizionali o "cloud service provider", consulenti, avvocati esterni, commercialisti ecc.);
- in attuazione della normativa vigente, l'A.O.U., nella figura del suo legale rappresentante, ha approvato, con Delibera del Direttore Generale n.180 dell'11/04/2019, una "clausola tipo" da utilizzare nei contratti/convenzioni che prevedano accesso ai dati aziendali per la nomina del terzo contraente a Responsabile del Trattamento dei dati personali;
- la procedura aziendale per la nomina dei Responsabili del Trattamento dei dati stabilisce sia attività di tipo amministrativo che di tipo informativo/ispettivo. Le prime si concretizzano nella formalizzazione del contratto che vincola il Responsabile al Titolare. Poiché il Responsabile è autorizzato a trattare i dati solo previa istruzione documentata del Titolare, l'atto definisce la durata del trattamento, la natura e le finalità del medesimo, le tipologie dei dati trattati e le categorie di interessati, gli obblighi e i diritti degli interessati. Le attività di tipo informativo/ispettivo sono volte invece a verificare "ex ante", cioè, già in fase di affidamento, che il Responsabile presenti "garanzie sufficienti per mettere in atto misure tecniche e organizzative

adeguate in modo tale che il trattamento soddisfi i requisiti del" […] "regolamento e garantisca la tutela dei diritti dell'interessato" (art. 28 GDPR) poiché solo in tal caso il Titolare potrà affidare il trattamento al Responsabile così individuato. E' pertanto necessario tener conto delle indicazioni della procedura già durante le negoziazioni relative a servizi, attività o prestazioni esternalizzati. Contestualmente è necessario verificare, aggiornare, ed integrare i contratti già in essere, che comportano esternalizzazione del trattamento di dati personali o parte di esso;

Tenuto conto:

- che l'A.O.U. vuole implementare un processo per rendere disponibili, su richiesta, collegamenti remoti autorizzati (VPN – Virtual Private Network) a favore di aziende Responsabili del Trattamento che, in base a regolare contratto di gestione e/o manutenzione, necessitano di espletare da remoto, in tutto o in parte, le attività contrattualizzate;
- che il servizio di connettività in VPN è erogato, in nome e per conto dell'A.O.U., dal C.S.I. – Centro di ateneo per i Servizi Informativi dell'Università di Napoli "Federico II" mediante atto convenzionale;
- che, al fine di regolamentare il processo secondo il "Modello gestionale Privacy", è necessario che l'A.O.U. renda disponibile apposita modulistica per la richiesta del servizio di connettività unitamente al necessario documento informativo redatto in base ai principi di trattamento corretto e trasparente (artt. 13 e 14 del Regolamento UE 679/2016) che descriva i diritti degli interessati;
- che l'U.O.C. Sistema Informativo, ICT e nuove tecnologie dell'informazione ha redatto la necessaria modulistica in base alla normativa vigente;
- che tale modulistica, correttamente compilata in ogni sua parte di interesse, dovrà essere inviata al C.S.I., Responsabile del Trattamento, per gli adempimenti privacy di sua competenza ed ai fini di una corretta ed autorizzata erogazione del servizio;

Dichiarata la regolarità giuridico – amministrativa e l'utilità per il servizio pubblico, ai sensi e per gli effetti di quanto disposto all'art. 1 della L. 20/94 e s.m.i., della presente proposta di provvedimento, a seguito dell'istruttoria effettuata, nel rispetto delle proprie competenze, funzioni e responsabilità;

Ritenuto di provvedere con urgenza in considerazione della natura bloccante di tale servizio per le attività tecniche ed assistenziali di codesta Azienda;

Propone

Per tutto quanto sopra, che si intende integralmente riportato, di adottare il presente provvedimento, sulla scorta ed in conformità della proposta:

- di adottare l'allegato modulo "Richiesta di Accesso Sicuro ed Autorizzato (VPN) al Sistema Informativo Aziendale (per soggetti esterni)", allegato n.1, parte integrante e sostanziale del presente atto deliberativo;
- di adottare l'allegata "Informativa per gli utenti esterni del servizio di Accesso Sicuro ed Autorizzato (VPN) al Sistema Informativo dell'A.O.U. "Federico II" ai fini del trattamento dei dati personali raccolti", ai sensi degli articoli 13 e 14 del Regolamento UE n.679/2016, allegato n.2, parte integrante e sostanziale del presente atto deliberativo;
- di disporre che tale modulistica, resa unica, venga messa a disposizione di tutti i Responsabili del Trattamento mediante pubblicazione, sul sito istituzionale dell'AOU "Federico II", in forma di "modulo PDF compilabile" al fine di darne ampia diffusione;
- di stabilire che, eventuali aggiornamenti di tali documenti, necessari al fine di rispettare eventuali evoluzioni della normativa vigente o di ampliare la casistica degli aventi diritto al servizio, sia effettuata a cura della P.O. Gestione reti ed infrastrutture tecniche di concerto con la Direzione dell'U.O.C. Sistema Informativo, ICT e nuove tecnologie dell'informazione;

F.to Il Direttore ad interim dell'U.O.C. Sistema
Informativo, ICT e nuove tecnologie dell'informazione
Ing. Ciro BRUNO

IL DIRETTORE GENERALE

Letta la proposta di delibera sopra riportata, presentata dal Direttore ad interim dell'U.O.C. Sistema Informativo, ICT e nuove tecnologie dell'informazione;

Preso atto che il Direttore dell'U.O.C. proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, è legittimo e utile per il servizio pubblico, ai sensi e per gli effetti di quanto disposto dall'art. 1 della L. 20/94 e succ. mod. ed int.;
Acquisito il parere favorevole del Direttore Amministrativo;

Acquisito il parere favorevole del Direttore Sanitario;

D E L I B E R A

per i motivi su esposti, che qui abbiansi per riportati e confermati:

- di adottare la proposta di deliberazione sopra riportata, nei termini indicati;
- di conferire immediata esecutività al presente atto, ricorrendone i presupposti;
- di inviare la presente deliberazione, ai sensi della normativa vigente al Collegio Sindacale.

F.to IL DIRETTORE GENERALE
Avv. Anna IERVOLINO

Data consegna . .

P.O. ALBO PRETORIO E DELIBERAZIONI

Si dichiara che la presente delibera:

E' stata pubblicata all'Albo Pretorio dell'Azienda, ai sensi dell'art. 32 della Legge 69/09

Il

F.to Il Funzionario
Dott.ssa Maria COLAMARINO

E' divenuta esecutiva il 27.11.2019

F.to Il Funzionario
Dott.ssa Maria COLAMARINO

E' stata trasmessa al Collegio Sindacale

F.to Il Funzionario
Dott.ssa Maria COLAMARINO

PER COPIA CONFORME ALL'ORIGINALE ESISTENTE AGLI ATTI D'UFFICIO

F.to Il Funzionario
Dott.ssa Maria COLAMARINO