AREU
Sistema Socio Sanitario
Regione Lombardia

DELIBERA DEL DIRETTORE GENERALE

131 / 2023 del 23/05/2023

***Oggetto*: COSTITUZIONE GRUPPO DI LAVORO SULLA "CYBERSICUREZZA" (CYBERSECURITY)**

AREU Agenzia Regionale Emergenza Urgenza
Via Alfredo Campanini, 6 - 20124 Milano | C.F. e P. IVA 11513540960
Tel 02 67129001 | Fax 02 67129002 | Mail protocollo@pec.areu.lombardia.it
www.areu.lombardia.it

OGGETTO: COSTITUZIONE GRUPPO DI LAVORO SULLA "CYBERSICUREZZA" (CYBERSECURITY)

vista la seguente proposta di deliberazione n. 248/2023, avanzata dal Direttore della Struttura Complessa Affari Generali e Legali

IL DIRETTORE GENERALE

PREMESSO che:

- la Sanità è uno dei settori più a rischio dal punto di vista della protezione dei dati, in quanto ogni struttura ospedaliera tratta dati appartenenti a categorie particolari, in primis dati sanitari che, per la loro natura, sono maggiormente esposti all'evoluzione tecnologica;
- AREU è un Ente del SSR disciplinato dall'art. 16 LR 30/12/2009 n. 33 e ss.mm.ii., attivato dalla DGR n. 2701/2019 e dalla DGR n. 4078/2020 con il compito di implementare e rendere omogeneo nel territorio regionale il soccorso sanitario di emergenza urgenza extraospedaliera, nonché di coordinare le attività trasfusionali ed il trasporto di équipe di trapianto, persone ed organi, unitamente alla gestione del servizio di "Numero Unico Emergenza 112" e del "Numero Europeo Armonizzato" (NEA) 116117, per l'accesso ai servizi di cure mediche non urgenti e altri servizi sanitari, la cui attivazione concorre alla gestione della domanda assistenziale a bassa intensità/priorità;

VISTI:

- Il Decreto Legislativo n. 196 del 2003 e ss.mm.ii, recante il "Codice in materia di protezione dei dati personali";
- il Decreto Legislativo n. 82 del 2005, recante il "Codice dell'Amministrazione Digitale" e, in particolare l'art. 17 recante i compiti e funzioni del Responsabile per la Transizione Digitale, necessari alla realizzazione di un'amministrazione digitale e all'erogazione di servizi fruibili, utili e di qualità;
- il Decreto-Legge n. 179 del 2012, convertito con modificazioni dalla L. n. 221 del 2012 e, in particolare, l'art. 33 septies che prevede il consolidamento e la realizzazione dei siti e delle infrastrutture digitali, demandando all'Agenzia per la cybersicurezza nazionale, d'intesa con la competente struttura della Presidenza del Consiglio dei Ministri, l'adozione di un regolamento per stabilire i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione, nonché le caratteristiche di qualità, sicurezza, performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione e, infine, i termini e le modalità di migrazione;
- il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (General Data Protection Regulation, o GDPR), applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018, il quale presta particolare attenzione ai dati sanitari, richiedendo ai Titolari e ai Responsabili del trattamento di fornire adeguate misure di sicurezza;
- i Regolamenti (UE) 2017/745 e 2017/746 che disciplinano rispettivamente i dispositivi medici e i dispositivi medici in vitro, entrati in vigore dal 26 maggio 2021 e dal 26

maggio 2022, prevedendo nuovi standard minimi di sicurezza per i dispositivi medici, soprattutto dal punto di vista della loro affidabilità in base allo scopo per il quale sono creati, della verifica del processo di creazione e controllo degli stessi, dell'utilizzo combinato si software e piattaforme mobili, oltre che della previsione di misure di sicurezza minime che tutelino i sistemi dall'accesso non autorizzato;

- il Decreto Legislativo n. 65 del 2018, recepimento italiano della Direttiva UE 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione (c.d. direttiva NIS-Network and Information Security) al fine di conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, si occupa in modo specifico di sanità e strutture ospedaliere, in quanto rientranti negli operatori di servizi essenziali, detta la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS;
- il Decreto-legge n. 105 del 2019 (convertito con modificazioni nella legge n.133/2019) adottato al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi;
- il Regolamento (UE) n. 2019/881 del Parlamento europeo e del Consiglio del 17/04/2019, il Cybersecurity Act, che si prefiggeva di: rafforzare il ruolo dell'ENISA (Agenzia dell'Unione europea per la sicurezza cibernetica) attraverso importanti interventi riformatori e, soprattutto, dettare una cornice normativo-regolamentare europea per la certificazione della sicurezza informatica di prodotti, servizi e processi ICT;
- il DPCM n. 131 del 2020 Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;
- il DPCM n. 81del 2021 Regolamento e relativi Allegati in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza;
- il Decreto-legge n. 82 del 2021, convertito con modificazioni nella legge 4 agosto 2021, n. 109 recante «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale»;
- il Regolamento di cui all'art. 33-septies, comma 4, del Decreto-Legge n. 221 del 2012, recante "livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione", adottato dall'AgID con Determinazione n. 628/2021 e, in particolare, gli artt. 7,8 e 11;
- visto l'Allegato 1 della Determina n. 307/2022 dell'Agenzia per la cybersicurezza nazionale (ACN) recante "l'aggiornamento degli ulteriori livelli minimi di sicurezza, capacità elaborativa, e affidabilità delle infrastrutture digitali per la pubblica

amministrazione e delle ulteriori caratteristiche di qualità, sicurezza, performance e scalabilità dei servizi cloud per la pubblica amministrazione, nonché requisiti di qualificazione dei servizi cloud per la pubblica amministrazione";

RICHIAMATO il principio di "responsabilizzazione" (c.d. accountability), introdotto dal GDPR, consistente in un approccio metodologico basato sulla preliminare valutazione dei rischi potenzialmente lesivi dei diritti e delle libertà degli interessati, sulla base del quale si attribuisce ai Titolari del trattamento il compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicabili al trattamento dei dati personali e di adottare quelle misure tecniche e organizzative che vengano valutate a ciò più idonee ed opportune;

RILEVATO che detta nuova prospettiva ha imposto di adottare un nuovo approccio nel trattamento dei dati personali, richiedendo una costante attività di adeguamento, attraverso un'analisi preventiva e un impegno applicativo che devono sostanziarsi in una serie di attività specifiche;

RITENUTO, pertanto, opportuno alla luce dell'incidenza del concetto di responsabilizzazione previsto dal GDPR e tenuto conto della complessità e molteplicità delle funzioni istituzionali dell'Agenzia, costituire un gruppo di lavoro trasversale e multidisciplinare di supporto dell'Ente, in grado di individuare, pianificare, realizzare e monitorare non solo misure tecniche di sicurezza attuate in modo specifico al perimetro dei dati personali, in ottemperanza al GDPR, ma anche misure di sicurezza organizzative, procedurali e tecniche capaci di ridurre il rischio di compromissione di tutte le informazioni e gli strumenti tecnologici critici dell'Agenzia;

VALUTATO che detto "Gruppo di Lavoro sulla cybersicurezza (Cybersecurity)" potrebbe utilmente risultare così composto:

- Dott. Gabriele Dassi, Direttore S.C. Sistemi informativi;
- Dott.ssa Eleonora Zucchinali, Direttore S.C. Gestione Approvvigionamenti;
- Dott.ssa Domenica De Giorgio, Dirigente S.C. Affari Generali e Legali;
- Dott. Aldo Locatelli, Direttore S.S. Ingegneria clinica e Direttore "ad interim" S.S.D. Tecnico Patrimoniale;
- Dott. Maurizio Migliari, Direttore S.C. SOREU;
- Dott. Fabrizio Canevari, Responsabile Coordinamento Regionale NUE 112;
- Dott. Gianluca Marconi, Direttore S.C. AAT;
- Dott.ssa Stefania Favetti, Direttore S.S. Qualità e Risk Management;
- Eventuali collaboratori delegati che ogni membro del Gruppo di Lavoro ha la facoltà di nominare.

PRESO ATTO che il coordinamento delle attività del Gruppo di Lavoro viene affidato in capo alla S.C. Sistemi Informativi, viste le specifiche competenze e professionalità possedute nella materia della sicurezza cibernetica;

DATO ATTO che alla S.C. Sistemi Informativi e, in particolare, al Direttore pro tempore - Dott. Gabriele Dassi, sono affidati i compiti e le funzioni previsti:

- dall'art. 17 del "Codice dell'Amministrazione Digitale", in qualità di Responsabile per la Transizione Digitale;
- all'Allegato A della Determina n. 307/2022 ACN" Regolamento in materia di

perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133";

- dall'Allegato B del DPCM 81/2021 - Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza;

PRESO ATTO che il responsabile di cui sopra riferisce direttamente alla Direzione Strategica riguardo agli adempimenti da predisporre, alle scelte aziendali da prendere, alle tempistiche e alle modalità di realizzazione ed assicura l'implementazione delle misure di sicurezza di cui all'allegato A della determina 307/2022 dell'ACN;

DATO ATTO che il Gruppo di lavoro, nello svolgimento delle sue funzioni, per la valutazione e la trattazione di temi specifici per cui lo stesso valuti la necessità di essere supportato in termini di competenze od in termini organizzativi, potrà avvalersi dell'ausilio di diverse e specifiche altre professionalità, anche non presenti tra il personale in servizio in AREU, che potranno essere, di volta in volta, convocate;

VISTA l'esigenza di garantire la Protezione dei Dati Personali e la Sicurezza delle Informazioni nell'ambito di tutte le attività svolte AREU, nel rispetto della normativa vigente applicabile, assicurando una gestione "integrata" e "coordinata" a livello aziendale della regolamentazione della sicurezza delle informazioni nei processi operativi;

RITENUTO pertanto opportuno creare un gruppo di lavoro che coordini le funzioni aziendali sopra indicate, che saranno chiamate a svolgere un lavoro sinergico, mettendo a sistema le singole professionalità e competenze, in raccordo con il Gruppo di Lavoro Privacy, costituito con Delibera del Direttore Generale n. 94/2023, al fine di generare valore aggiunto per AREU;

DATO ATTO che il Gruppo di Lavoro si riunirà con l'obiettivo di realizzare procedure per la Protezione dei Dati Personali e la Sicurezza delle Informazioni e risponderà direttamente alla Direzione Strategica;

PRESO ATTO che il Proponente del procedimento attesta la completezza, la regolarità tecnica e la legittimità del presente provvedimento;

ACQUISITI i pareri favorevoli del Direttore Amministrativo F.F. e del Direttore Sanitario, resi per quanto di specifica competenza ai sensi dell'art. 3 del D.Lgs. n. 502/1992 e s.m.i.;

DELIBERA

Per tutti i motivi in premessa indicati e integralmente richiamati:

1. di costituire, il Gruppo di lavoro sulla "cybersicurezza" (Cybersecurity) composto da:
   - Dott. Gabriele Dassi, Direttore S.C. Sistemi informativi;
   - Dott.ssa Eleonora Zucchinali, Direttore S.C. Gestione Approvvigionamenti;
   - Dott.ssa Domenica De Giorgio, Dirigente S.C. Affari Generali e Legali;
   - Dott. Aldo Locatelli, Direttore S.S. Ingegneria clinica e Direttore "ad interim" S.S.D. Tecnico Patrimoniale;
   - Dott. Maurizio Migliari, Direttore S.C. SOREU;

- Dott. Fabrizio Canevari, Responsabile Coordinamento Regionale NUE 112;
- Dott. Gianluca Marconi, Direttore S.C. AAT;
- Dott.ssa Stefania Favetti, Direttore S.S. Qualità e Risk Management;
- Eventuali collaboratori delegati che ogni componente del Gruppo di Lavoro ha la facoltà di nominare;

2. di dare atto che il coordinamento delle attività del Gruppo di Lavoro viene affidato in capo alla S.C. Sistemi Informativi, chiamata a riportare direttamente alla Direzione Strategica riguardo agli adempimenti da predisporre, alle scelte aziendali da prendere, alle tempistiche e alle modalità di realizzazione;
3. di dare atto che alla S.C. Sistemi Informativi e, in particolare, al Direttore pro tempore, oggi individuato nella persona del Dott. Gabriele Dassi, sono affidati i compiti e le funzioni previsti:
   - dall'art. 17 del "Codice dell'Amministrazione Digitale", in qualità di Responsabile per la Transizione Digitale;
   - all'Allegato A della Determina n. 307/2022 ACN" Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133";
   - dall'Allegato B del DPCM 81/2021 - Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza;
4. di prendere atto che il Gruppo di lavoro, nello svolgimento delle sue funzioni, per la valutazione e la trattazione di temi specifici per cui lo stesso valuti la necessità di essere supportato in termini di competenze od in termini organizzativi, potrà avvalersi dell'ausilio di diverse e specifiche altre professionalità, anche non presenti tra il personale in servizio in AREU, che potranno essere, di volta in volta, convocate;
5. di prendere atto che il predetto Gruppo di lavoro avrà il compito di supportare l'Ente al fine di individuare, pianificare, realizzare e monitorare non solo misure tecniche di sicurezza attuate in modo specifico al perimetro dei dati personali, in ottemperanza al GDPR, ma anche misure di sicurezza organizzative, procedurali e tecniche capaci di ridurre il rischio di compromissione di tutte le informazioni e gli strumenti tecnologici critici dell'Agenzia, in raccordo con il Gruppo di Lavoro Privacy, costituito con Delibera del Direttore Generale n. 94/2023;
6. di dare atto che dal presente provvedimento non derivano oneri a carico del bilancio aziendale;
7. di dare atto che, ai sensi della L. n. 241/1990, responsabile del presente procedimento è la Dott.ssa Domenica De Giorgio, Dirigente S.C. Affari Generali e Legali;
8. di disporre che vengano rispettate tutte le prescrizioni inerenti alla pubblicazione sul portale web aziendale di tutte le informazioni e i documenti richiesti e necessari ai sensi del D.Lgs. n. 33/2013 e s.m.i., c.d. Amministrazione Trasparente;
9. di disporre la pubblicazione del presente provvedimento all'Albo Pretorio on line dell'Agenzia, dando atto che lo stesso è immediatamente esecutivo (ex art. 32 comma 5 L. n. 69/2009 s.m.i. e art. 17 comma 6 L.R. n. 33/2009).

La presente delibera è sottoscritta digitalmente, ai sensi dell'art. 21 D.Lgs. n. 82/2005 e s.m.i., da:

Il Direttore Amministrativo Andrea Albonico

Il Direttore Sanitario Giuseppe Maria Sechi

Il Direttore Generale Alberto Zoli