

DELIBERAZIONE DEL DIRETTORE GENERALE

UNITÀ OPERATIVA: U.O.C. PROGETTAZIONE SVILUPPO E MANUTENZIONE IMMOBILI ED IMPIANTI, SISTEMI INFORMATICI E ICT

OGGETTO: INTEGRAZIONE DEL “REGOLAMENTO PER L’ACCESSO DA REMOTO ALLA RETE AZIENDALE TRAMITE VPN (VIRTUALE PRIVATE NETWORK)” DI CUI ALLA DELIBERA N.371 del 13/07/2018 E APPROVAZIONE MODULISTICA PER LA REGOLAMENTAZIONE DELL’ACCESSO IN VPN DA PARTE DI AMMINISTRATORI DEI SISTEMI LOCALI

Il Direttore della UOC propone quanto di seguito riportato

PREMESSO

- Che il Regolamento UE 2016/679 denominato **General Data Protection Regulation (GDPR)**, pubblicato sulla Gazzetta Ufficiale Europea in data 4 maggio 2016 ed entrato in vigore il 24 maggio dello stesso anno nasce con l’obiettivo di *“rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini e dei residenti dell’Unione Europea, sia all’interno che all’esterno dei confini...”* e che, a decorrere dal 25 maggio 2018, l’inadempienza al citato GDPR prevede l’applicazione di sanzioni, come previsto dall’art. 83;
- Che l’ottemperanza al Regolamento UE 2016/679 prevede, all’art. 25, comma 2, che il Titolare del trattamento sia tenuto a mettere *“in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l’accessibilità”*;
- Che l’ottemperanza al disposto regolamentare prevede, all’art. 32, comma 1, che, *“Tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio...”*;
- Che l’art. 33, comma 5, impone al titolare del trattamento di documentare *“qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all’autorità di controllo di verificare il rispetto del presente articolo”*;
- che, con provvedimento a carattere generale del 27 novembre 2008, l’Autorità Garante Italiana, vigente la precedente disciplina, ha imposto che sia predisposto un *“elenco degli amministratori di sistema e loro caratteristiche”* e che, quindi, il titolare del trattamento deve designare individualmente i singoli amministratori di sistema, a mezzo di un atto che deve elencare analiticamente gli ambiti di operatività consentiti, in base al profilo di autorizzazione assegnato;

- che il Titolare del trattamento deve adottare idonei sistemi di registrazione degli accessi logici, compiuti dagli amministratori, ai sistemi di elaborazione ed alle operazioni compiute sugli archivi e che è tenuto a indicare in un documento interno gli estremi identificativi delle persone fisiche designate quali amministratori di sistema, con l'elenco delle funzioni ad esse attribuite;

DATO ATTO

- Che con Delibera n.371 del 13/07/2018 è stato già adottato da questa AORN il *“Regolamento per l'accesso da remoto alla rete aziendale tramite VPN (Virtuale Private Network)”* contenente la definizione di precise regole da seguire, corredate da modulistica dedicata, per un corretto e sicuro accesso da remoto, attraverso connessioni VPN, sia dei dipendenti dell'AORN che delle numerose parti terze (Fornitori, Collaboratori,...) che interagiscono a qualunque titolo con la stessa, secondo quanto stabilito dal Codice di protezione dei dati personali D.Lgs 196/2003, dal Regolamento UE 2016/679 e dalla ulteriore normativa vigente in materia.

CONSIDERATO

- Che numerosi accessi da remoto, attraverso utilizzo di VPN, sia da parte di dipendenti interni che di personale esterno all'AORN, già oggetto di regolamentazione come sopra detta, possono però avvenire oltre che in qualità di semplici “utenti”, anche in qualità di “Amministratori dei sistemi locali”, ossia un profilo di accesso con caratteristiche differenti e più invasive e, pertanto, definito più sensibile, stante la possibilità per gli stessi di accedere ai server ed intervenire sui dati aziendali;
- Che l'Amministratore di sistema, nell'espletamento delle sue funzioni, gestisce il sistema informatico nel quale risiedono le banche dati di proprietà del titolare del trattamento, in osservanza alla normativa vigente in materia, attenendosi alle disposizioni del titolare del trattamento e/o dei responsabili del trattamento, in tema di sicurezza
- In virtù di quanto sopra detto, la necessità, ormai prioritaria ed urgente, di integrare le procedure in essere al fine di assicurare un accesso ai dati e la conseguente gestione degli stessi in maniera “protetta e sicura” da parte degli utenti con caratteristiche di “Amministratori dei sistemi locali”, secondo quanto stabilito dal Codice di protezione dei dati personali D.Lgs. 196/2003, dal Regolamento UE 2016/679 e dalle ulteriori normative vigenti in materia.

CONSIDERATO, altresì

- che la scrivente UOC, agendo in base all'art.17 del C.A.D. (Codice dell'Amministrazione digitale Decreto Legislativo 7 marzo 2005, n. 82), ha preliminarmente predisposto una ricognizione degli accessi, ad oggi, di tipo “Amministratore dei Sistemi Locali”, opportunamente elencate in un documento agli atti della proponente UOC, individuando in maniera chiara le specifiche caratteristiche di tali situazioni nell'ambito dell'AORN
- che è stato predisposto da questa UOC, ai fini della gestione degli accessi da parte di utenti classificati “Amministratori dei Sistemi Locali”, apposita modulistica che regola l'intero processo, a partire dalla fase di richiesta di rilascio delle credenziali per l'accesso, con l'individuazione dettagliata dei singoli server da raggiungere, sino all'approvazione ed al formale rilascio delle stesse, autorizzato dalle figure aziendali competenti;

- che risulta invece già approvato e codificato, per questa AORN, il format da utilizzare quale “Contratto di nomina di Amministratore di Sistema” che sarà inoltrato, a cura di questa UOC proponente, insieme alla modulistica sopra detta, al Richiedente e con il quale viene disciplinato, in maniera dettagliata, il trattamento dei dati personali da parte dell’Amministratore di sistema, specificando l’oggetto, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati e gli obblighi e i diritti delle Parti.

RAVVISATA, pertanto

- la necessità di dover procedere ad un’integrazione delle procedure afferenti al “Regolamento per l’accesso da remoto alla rete aziendale attraverso VPN (Virtual Private Network)” deliberato con atto n.371/2018, attraverso l’introduzione di modulistica dedicata al caso in questione, da accompagnare al “Contratto di nomina di Amministratore di sistema”, con l’obiettivo ultimo di agevolare il governo ed il contenimento dei rischi emersi dagli accessi alla rete da parte di utenti classificati “Amministratori dei Sistemi Locali” ed in particolare di:
 - preservare il patrimonio informativo aziendale;
 - garantire la fiducia e la soddisfazione degli utenti dei servizi “core” dell’AORN, proteggendo i dati degli interessati;
 - garantire la fiducia e la soddisfazione dei fornitori, tutelando e proteggendo i dati di loro interesse o di loro titolarità o relativi ai servizi da loro erogati;
 - garantire la riservatezza ed integrità delle informazioni;
 - garantire la continuità del servizio;
 - adempiere a quanto espressamente disposto dalla normativa italiana ed europea in materia di sicurezza e protezione dei dati, con particolare riferimento al Codice in materia di protezione dei dati personali (D.Lgs. 196/03) ed alle Misure Minime di Sicurezza.

VISTI

- Il Regolamento (UE) 2016/679 (Regolamento Generale sulla Protezione dei Dati – GDPR);
- Il D.Lgs. n.196 del 30/06/2003 e ss.mm.ii (D.Lgs 101 del 10/08/2018 “Disposizioni per l’adeguamento della normativa nazionale al GDPR”);
- Il Del. n.13 del 01/03/2007 - Lavoro: le linee guida del Garante per posta elettronica e internet;
- Il D.Lgs. n.231/2001- Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300;
- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), come modificato dal provvedimento del 25 giugno 2009.

PROPONE

- L’approvazione della modulistica denominata “Modulo Richiesta Rilascio Credenziali Amministratore dei Sistemi Locali”, allegata al presente provvedimento, che ne costituisce

parte integrante e sostanziale e che integra il “Regolamento per l’accesso da remoto alla rete aziendale attraverso VPN (Virtual Private Network)”, deliberato con atto n.371/2018;

- Di regolarizzare gli accessi tramite VPN, ad oggi in essere, in qualità di utenti classificati come “Amministratori dei Sistemi Locali”, in ottemperanza alla normativa vigente in materia ed al Regolamento aziendale sopra citato, attraverso l’inoltro da parte di questa UOC del Contratto di nomina di amministratore di sistema e della modulistica sopra detta e la conseguente formale autorizzazione, con relativo rilascio di credenziali, all’accesso alla rete aziendale in maniera protetta e sicura.

DATO ATTO

- Che la modulistica allegata al presente atto è stata debitamente trasmessa per l’approvazione al DPO aziendale con e-mail del 03/12/2021;
- Che il DPO ha ritrasmesso con e-mail del 13/12/2021 il modulo definitivo revisionato da utilizzare in osservanza alla normativa vigente in materia, che si allega al presente atto;
- Che anche il presente atto ha ricevuto formale approvazione del DPO con e-mail del 13/01/2022 agli atti di questa UOC.

Il Direttore

(Ing. Gennaro Sirico)

(F.to digitalmente)

Acquisito il parere favorevole del Direttore Sanitario che sottoscrive per conferma

Il Direttore Sanitario

Dott. Vincenzo Giordano

(F.to digitalmente)

IL DIRETTORE GENERALE

In virtù dei poteri conferitigli con D.P.G.R.C. N. 171 DEL 09/12/2020

Alla stregua dell’istruttoria compiuta dalla Unità Operativa proponente o che predispose l’istruttoria, nonché dell’espressa dichiarazione di regolarità resa dal responsabile di tale Unità Operativa con la firma apposta in calce.

Per tutto quanto in premessa espresso e che qui si intende integralmente richiamato:

Acquisito il parere favorevole del Direttore Sanitario

DELIBERA

- 1. Di approvare** il “Modulo Rilascio Credenziali amministratore Sistemi Locali” che, allegato al presente provvedimento, ne costituisce parte integrante e sostanziale;

2. **Di integrare**, con il presente atto, il “Regolamento per l’accesso da remoto alla rete aziendale attraverso VPN (Virtual Private Network)” già adottato da questa AORN, di cui alla delibera n.371 del 13/07/2018;
3. **Di dare mandato** alla UOC proponente di regolarizzare gli accessi di tipo “Amministratore dei Sistemi Locali” ad oggi in essere, in ottemperanza alla normativa vigente in materia ed alla regolamentazione aziendale suddetta, attraverso l’inoltro del “Contratto di nomina di Amministratore di sistema” già in uso presso l’AORN e della modulistica approvata con il presente atto ed il successivo formale rilascio delle credenziali di accesso “autorizzate”;
4. **Di trasmettere** il presente atto alla UOC ABS, alla UOC GRU, alla UOSD Sistemi e Flussi informativi aziendali, al DPO aziendale, al RCPT, alla UOSID Controllo Interno, alle Direzioni Mediche dei Presidi Ospedalieri, al Collegio Sindacale e alla UOC proponente;
5. **Di procedere** alla sua divulgazione, mediante pubblicazione sul sito web aziendale www.santobonopausilipon.it nella sezione “Amministrazione Trasparente” – Disposizioni generali – Atti amministrativi generali e nella sezione “Modulistica”;
6. **Di stabilire** che la presente modulistica è suscettibile di revisione a seguito di aggiornamenti, normativi, giurisprudenziali e pronunce del Garante della Privacy o di eventuali problematiche che potrebbero insorgere in sede di applicazione dello stesso;
7. **Di conferire** immediata esecutività alla presente deliberazione ai sensi ed agli effetti dell’art. 21 quater della L.241/90, per procedere alla regolamentazione degli accessi di utenti “Amministratori dei sistemi locali” attualmente attivi, al fine di garantire la sicurezza agli accessi alla rete aziendale.

Visto

Il Dirigente Amministrativo

Dr.ssa Antonella Giuliani

(f.to digitalmente)

Il Direttore Generale

Dr. Rodolfo Conenna

(f.to digitalmente)

