ALLEGATO A

REGOLAMENTO AZIENDALE SULLA PROTEZIONE DEI DATI PER GLI AMMINISTRATORI DI SISTEMA

Versione 1.1	Data versione
Approvato con delibera n° ___ del _____	

INDICE

1.GENERALITA'

Il Garante per la protezione dei dati personali ha definito l'Amministratore di Sistema (in seguito anche AdS) quale *"figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali"* (Provvedimento del Garante del 27/11/2008 come modificato con provvedimento del 25/06/2009).

Tale figura professionale è stata implicitamente richiamata anche dal Regolamento UE 2016/679 sulla protezione dei dati personali (GDPR), laddove è previsto in capo al Titolare del trattamentoo, il compito di mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio (art. 32 GDPR).

L' Amministratore di sistema rappresenta, infatti, una figura essenziale per la sicurezza del sistema informatico, delle banche dati e della corretta gestione delle reti telematiche, in *quanto il suo compito primario è quello di proteggere la privacy dei dati personali, attraverso il controllo sul corretto utilizzo, sul regolare funzionamento e la protezione dei sistemi di gestione ed elaborazione elettronica dei dati,* nonché di provvedere al monitoraggio di tali sistemi per rilevare immediatamente una eventuale violazione o perdita dei dati, accidentale od intenzionale (cosiddetto "data breach").

È, quindi, compito dell'Amministratore di sistema monitorare costantemente lo stato di sicurezza di tutti i processi di elaborazione dati di cui sopra, mantenendo aggiornate le risorse hardware e software e proponendo al Titolare le misure necessarie per garantire un livello di sicurezza adeguato al rischio, in proporzione alla tipologia e alla quantità dei dati personali trattati.

Gli specifici compiti affidati alla suddetta figura professionale, però, possono comportare elevate criticità rispetto alla protezione dei dati, anche quando non vengano consultate "in chiaro" le informazioni.

Per quanto innanzi, l'Azienda Sanitaria Locale di Brindisi (d'ora in poi denominata il Titolare o ASL BR), nella sua qualità di Titolare del trattamento dei dati personali, in ossequio al principio di responsabilizzazione (art. 24 GDPR), con il presente Regolamento Aziendale ha inteso adottare specifiche misure tecniche ed organizzative in relazione alla figura dell'Amministratore di Sistema, sia per valutare con particolare attenzione la sua nomina e le relative attribuzioni, sia per prevedere una procedura finalizzata alla verifica della sua attività lavorativa, allo scopo di prevenire, ed eventualmente, rilevare possibili accessi non consentiti ai dati personali.

Tanto, il linea con il **provvedimento del 27/11/2008 del Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema",** tuttora applicabile, ai sensi della disposizione transitoria e finale del D.Lgs. 101/2018, art. 22, comma 4, per la quale *"a decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento (GDPR) e con le disposizioni del presente decreto".*

2.RIFERIMENTI NORMATIVI

- Regolamento Europeo 2016/679 del 27/04/2016, adottato il 27 aprile 2016, pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016, entrato in vigore il 25 maggio dello stesso anno e divenuto pienamente efficace a partire dal 25 maggio 2018;
- Provvedimento del Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 (*G.U. n. 300 del 24 dicembre 2008);*
- Provvedimento del Garante "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento" del 25 giugno 2009 (*G.U. n. 149 del 30 giugno 2009);*
- Provvedimento del Garante "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali " del 13 ottobre 2008 (G.U. n. 287 del 9 dicembre 2008).

3.OGGETTO

Il presente Regolamento ha per oggetto le politiche di sicurezza dettate con riferimento alla figura dell'Amministratore di Sistema, in ottemperanza al provvedimento del Garante del 27/11/2008, ed in applicazione del principio di responsabilizzazione previsto dal Regolamento Europeo 2016/679, al fine di:

- garantire la tutela dei diritti dell'interessato e la sicurezza dei dati personali ed in particolare la riservatezza, l'integrità e la disponibilità dei dati personali trattati da parte dell'Amministratore di Sistema;

- tutelare i beni aziendali;

- evitare condotte inconsapevoli, scorrette o illecite dell'Amministratore di sistema che potrebbero esporre l' Azienda a violazioni di sicurezza, danni patrimoniali e di immagine.

4.DESIGNAZIONE DELL' AMMINISTRATORE DI SISTEMA INTERNO O ESTERNO

Il Titolare del trattamento può designare Amministratore di Sistema (AdS) uno o più soggetti, sia interni che esterni all'Azienda.
L' AdS interno è un dipendente del Titolare del trattamento in possesso di specifici requisiti, designato in funzione delle sue qualità personali e professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati personali e sicurezza informatica.

L'AdS interno è autorizzato dal Titolare per iscritto allo svolgimento delle mansioni e dei compiti assegnati, i quali dovranno essere elencati in maniera analitica.

L' AdS esterno assolve i suoi compiti in base ad un contratto di servizi. In questo caso è necessaria la stipula di un atto giuridico con cui il fornitore del servizio sia nominato **responsabile del trattamento** (art. 28 GDPR), con l'assegnazione delle specifiche funzioni affidate e l'elencazione analitica di tutte le attività che dovranno essere svolte (vedi anche art. 9 del presente Regolamento Aziendale).

5.SELEZIONE DEI CANDIDATI ALLA FIGURA PROFESSIONALE DI AMMINISTRATORE DI SISTEMA SULLA BASE DELLA VALUTAZIONE DELLE CARATTERISTICHE SOGGETTIVE E DELLE COMPROVATE CAPACITA' TECNICHE

La designazione dell'Amministrazione di Sistema deve essere individuale, in quanto la persona designata deve essere identificabile.

A) AMMINISTRATORE DI SISTEMA INTERNO

Il Titolare del trattamento, prima di nominare l'Amministratore di Sistema, deve valutare attentamente le qualità (tecniche, professionali e di condotta) del dipendente cui dovranno essere attribuite le suddette funzioni, anche in considerazione delle responsabilità che possono derivare da una designazione inidonea o incauta.

Il candidato, pertanto, è tenuto a fornire idonea garanzia relativamente:

- alla conoscenza della normativa vigente in materia di protezione dei dati personali, dei provvedimenti del Garante, dei regolamenti e procedure aziendali, nonché della normativa e best practices di riferimento in ordine alla gestione "sicura" dei sistemi informativi;
- alla propria capacità, affidabilità ed esperienza in materia,

dimostrando di avere consapevolezza dei rischi di sicurezza derivanti da errori/omissioni/violazioni nell'ambito della gestione dei sistemi ed impegnandosi a procedere al trattamento dei dati personali secondo la normativa vigente.

All'esito della selezione, il Titolare procederà alla nomina dell'Amministratore di sistema con uno specifico atto di nomina contenente:

- ✓ l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- ✓ la comunicazione all'AdS nominato che il suo operato sarà oggetto di verifiche, mediante la previsione di forme per la registrazione dei suoi accessi e per la verifica del suo operato;
- ✓ la comunicazione che il suo nominativo sarà reso noto al personale, nel caso in cui l'AdS possa trattare dati personali dei lavoratori.

B) AMMINISTRATORE DI SISTEMA ESTERNO

Gli Amministratori di sistema esterni, con riferimento ai servizi in outsourcing, saranno valutati, quanto al possesso delle caratteristiche soggettive e delle comprovate capacità tecniche, dalle società fornitrici del servizio, le quali dovranno fornire al Titolare gli estremi identificativi delle persone fisiche designate.

6.ASSEGNAZIONE DI ADEGUATI LIVELLI DI RESPONSABILITA' AI SOGGETTI INDIVIDUATI QUALI AMMINISTRATORI DI SISTEMA

La designazione dell'Amministratore di Sistema deve comprendere l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Sono definiti i seguenti ambiti di responsabilità e di operatività, che possono essere implementati secondo le necessità aziendali:

- ✓ Gestione, sicurezza e manutenzione del sistema informatico;
- ✓ Gestione sistemistica e sicurezza delle postazioni di lavoro;
- ✓ Gestione sistemistica, sicurezza e monitoraggio della rete informatica;
- ✓ Gestione sistemistica e sicurezza dei Server aziendali;
- ✓ Back-up e Disaster Recovery;
- ✓ Gestione dei sistemi software e delle basi dati relative agli applicativi in uso.

L'Amministratore di Sistema, in quanto preposto alla gestione dei sistemi informatici, è responsabile della sicurezza dei sistemi informatici e delle informazioni di carattere personale, in relazione al suo ambito di responsabilità ed operatività.
Ha il compito di proteggere la privacy dei dati personali sin dalle fasi di progettazione e protezione dei dati (privacy by design e privacy by default di cui all'art. 25 del medesimo Regolamento UE 2016/679) e di proporre al Titolare l'adozione delle soluzioni più adeguate a tale fine.

Le attività tecniche riconducibili a tale figura professionale sono, a titolo esemplificativo:

a) progettazione, installazione, configurazione, gestione e manutenzione dei sistemi informatici;

b) controllo sul corretto utilizzo, funzionamento e protezione dei sistemi di gestione ed elaborazione dei dati;
c) impostazione e gestione dei sistemi di autenticazione e di autorizzazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
d) organizzazione e gestione dei flussi di rete;
e) gestione dei supporti di memorizzazione;
f) manutenzione dell'hardware;
g) classificazione analitica delle banche dati ed impostazione/organizzazione di un sistema complessivo di trattamento informatizzato dei dati personali comuni e particolari, nel rispetto della normativa vigente in materia di protezione dei dati personali;
h) predisposizione e gestione dei sistemi di salvataggio (backup), anche automatici, con adozione di adeguate procedure per la custodia delle copie di sicurezza dei dati;
i) adozione di adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS ecc.);
j) predisposizione di sistemi di ripristino dei dati e dei sistemi (recovery), anche automatici, che assicurino di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
k) adozione di un sistema idoneo alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Tali registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate ed essere conservate per un congruo periodo, non inferiore a dodici mesi;
l) adozione di tutte le misure di sicurezza adeguate al rischio, ivi compresa la pseudonimizzazione e la cifratura dei dati personali, che assicurino su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, nonché l'adozione delle misure di sicurezza ICT emanate dall'AgID, adeguate alla realtà organizzativa aziendale**;**
m) verifica e monitoraggio costante dei sistemi informatici al fine di rilevare immediatamente eventuali tentativi di accessi non autorizzati al sistema provenienti da soggetti terzi, quali accesso abusivo al sistema informatico o telematico, frode, danneggiamento di informazioni, dati e programmi informatici, danneggiamento di sistemi informatici e telematici;
n) controllo sugli interventi informatici effettuati da operatori esterni;
o) predisposizione di un piano di controlli periodici, da eseguire con cadenza almeno semestrale, atti a testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
p) provvedere alla distruzione e smaltimento dei supporti informatici di memorizzazione logica obsoleti e/o alla cancellazione dei dati ivi registrati per consentirne il loro reimpiego, secondo quanto disposto dal Garante per la protezione dei dati personali con il Provvedimento in data 13 ottobre 2008 in materia di smaltimento degli strumenti

elettronici[1].

7.DEFINIZIONE ED IMPLEMENTAZIONE DI PROCEDURE TECNICHE DI SUPERVISIONE E CONTROLLO SULL'OPERATO DELL'AMMINISTRATORE DI SISTEMA

7.1.PRINCIPI

Nell'espletamento della sua attività l'Amministratore di Sistema deve sempre applicare i principi fondamentali previsti dal Regolamento Europeo 2016/679 e precisamente i principi di:

- ✓ **liceità**, nel senso che i dati devono essere trattati in modo lecito, corretto e trasparente (ad es. le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori);
- ✓ **limitazione della finalità**: i dati devono essere raccolti per finalità legittime ed individuate fin dall'inizio, e successivamente trattati in modo che non sia incompatibile con tali finalità. In caso di interventi per esigenze di manutenzione del sistema, l'Amministratore di sistema deve svolgere solo operazioni strettamente necessarie al perseguimento delle proprie finalità d'ufficio, evitando, per quanto possibile, l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati ai dipendenti;
- ✓ **minimizzazione dei dati**: i dati trattati devono essere solamente quelli indispensabili, quindi pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. I sistemi informativi ed i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi in relazione

[1] **Allegato A) al provvedimento del Garante del 13 ottobre 2008**
Reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche
In caso di reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti, adottati nel rispetto delle normative di settore, devono consentire l´effettiva cancellazione dei dati o garantire la loro non intelligibilità. Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti e possono consistere, tra l´altro, in:
Misure tecniche preventive per la memorizzazione sicura dei dati, applicabili a dispositivi elettronici o informatici:
1. Cifratura di singoli file o gruppi di file, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura. Questa modalità richiede l´applicazione della procedura di cifratura ogni volta che sia necessario proteggere un dato o una porzione di dati (file o collezioni di file), e comporta la necessità per l´utente di tenere traccia separatamente delle parole-chiave utilizzate.
2. Memorizzazione dei dati sui dischi rigidi (hard-disk) dei personal computer o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata al momento della loro scrittura, tramite l´uso di parole-chiave riservate note al solo utente. Può effettuarsi su interi volumi di dati registrati su uno o più dispositivi di tipo disco rigido o su porzioni di essi (partizioni, drive logici, file-system) realizzando le funzionalità di un c.d. file-system crittografico (disponibili sui principali sistemi operativi per elaboratori elettronici, anche di tipo personal computer, e dispositivi elettronici) in grado di proteggere, con un´unica parola-chiave riservata, contro i rischi di acquisizione indebita delle informazioni registrate. L´unica parola-chiave di volume verrà automaticamente utilizzata per le operazioni di cifratura e decifratura, senza modificare in alcun modo il comportamento e l´uso dei programmi software con cui i dati vengono trattati.
Misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici:
3. Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali wiping program o file shredder) che provvedono, una volta che l´utente abbia eliminato dei file da un´unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati.
Il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza o all´importanza delle informazioni di cui si vuole impedire l´indebita acquisizione) varia da sette a trentacinque e incide proporzionalmente sui tempi di applicazione delle procedure, che su dischi rigidi ad alta capacità (oltre i 100 gigabyte) possono impiegare diverse ore o alcuni giorni), a secondo della velocità del computer utilizzato.
4. Formattazione "a basso livello" dei dispositivi di tipo hard disk (low-level formatting–LLF), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;
5. Demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l´accessibilità del dispositivo da parte del sistema a cui è interconnesso).

Allegato B) al provvedimento del Garante del 13 ottobre 2008
Smaltimento di rifiuti elettrici ed elettronici
In caso di smaltimento di rifiuti elettrici ed elettronici, l´effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche può anche risultare da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali.
La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali:
- ✓ sistemi di punzonatura o deformazione meccanica;
- ✓ distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);
- ✓ demagnetizzazione ad alta intensità.

alle finalità perseguite; eventuali attività di monitoraggio devono essere mirate solo sull'area di rischio, a norma di legge;

- ✓ **esattezza:** i dati devono essere corretti e, se necessario, aggiornati, con conseguente obbligo di cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- ✓ **limitazione della conservazione**: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per il tempo strettamente necessario al conseguimento delle finalità per le quali sono trattati e, successivamente, nel rispetto dei termini previsti dalle vigenti procedure di scarto degli archivi documentali;
- ✓ **integrità e riservatezza**: i dati devono essere trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

E' vietato qualsiasi trattamento di dati personali preordinato al controllo a distanza dei lavoratori.

All'atto della cessazione del rapporto con il Titolare, l'AdS designato dovrà restituire tutti i dati personali trattati, con espresso divieto di conservarli.

7.2.REGISTRAZIONE DEGLI ACCESSI LOGICI DELL' AMMINISTRATORE DI SISTEMA INTERNO AGLI ARCHIVI ELETTRONICI

Al fine di verificare il corretto espletamento dell'attività lavorativa dell'Amministratore di Sistema, devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte dello stesso AdS.
Ciascun Amministratore, quindi, deve poter essere identificato e loggato, in quanto occorre tenere traccia di tutti i suoi accessi sui server, sui client ed anche sui database.
I file log generati devono contenere almeno le seguenti informazioni:

- utenza che ha generato l'evento ("user-name" impiegato);
- sistema informatico che ha generato l'evento (sistema di elaborazione o software utilizzato);
- informazioni relative alla data e all'ora dell'evento (timestamp);
- tipologia ed esito dell'evento (qualificazione dell'evento come "log-in", "log-out" , ecc.).

Le registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste.
In particolare, per **completezza** si intende far riferimento a tutti gli eventi di accesso interattivo generati dall'Amministratore di sistema su tutti i sistemi di elaborazione.
Per soddisfare la caratteristica della **inalterabilità** dei dati raccolti dai sistemi di log occorre utilizzare una piattaforma centralizzata con canali di trasmissione sicuri o supporti di archiviazione non riscrivibili.
La **verifica dell'integrità dei log** può essere realizzata con l'applicazione di tecniche di cifratura.

Le suddette registrazioni devono essere conservate per un periodo non inferiore a dodici mesi.
E' severamente vietato durante tale periodo intervenire in alcun modo su di esse, compiendo qualsiasi attività, come ad esempio cancellandole, modificandole o alterandole.

7.3.VERIFICA DELLE ATTIVITÀ DELL'AMMINISTRATORE DI SISTEMA

AMMINISTRATORE DI SISTEMA INTERNO

L´operato dell'AdS interno sarà oggetto di un´attività di verifica ispettiva con cadenza annuale (ogni dicembre dell'anno), in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti in materia di trattamento dei dati personali.
Le attività di verifica devono comprendere, tra l'altro, i seguenti controlli:

- ✓ **riscontro, su un campione significativo, della corretta generazione dei log di accesso,** della loro conformità e della conservazione sicura per almeno dodici mesi;
- ✓ **analisi di dettaglio dei log di accesso**, al fine di riscontrare eventuali anomalie nella frequenza e nella modalità.

Le attività di verifica annuali saranno formalizzate con la redazione di un verbale di controllo.
Il Direttore dell'Area Tecnica è delegato dal Titolare per la suddetta attività ispettiva.

AMMINISTRATORE DI SISTEMA ESTERNO

La verifica sulle attività degli Amministratori di Sistema (verifica dei log di accesso), afferenti a servizi erogati da fornitori esterni, può essere demandato in sede contrattuale al fornitore di tale servizio, nominato Responsabile del trattamento.

8.ELENCO DEGLI AMMINISTRATORI DI SISTEMA

Gli estremi identificativi delle persone fisiche Amministratori di sistema, con l´elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.
Qualora gli AdS, nell'espletamento delle proprie mansioni, trattino (o, semplicemente, possano trattare, anche in caso fortuito) dati personali dei lavoratori, questi ultimi hanno diritto di conoscere l'identità dei predetti.
In tal caso, l'ASL BR renderà noto ai lavoratori dipendenti l'identità degli Amministratori di sistema secondo una delle seguenti modalità: a mezzo dell'informativa resa agli interessati ai sensi dell'art. 13 del GDPR o mediante altri strumenti di comunicazione (ad esempio, tramite rete aziendale o internet).
L'elenco contenente gli estremi identificativi degli Amministratori di sistema esterni deve essere aggiornato dal fornitore del servizio, nominato responsabile esterno del trattamento, e deve essere reso disponibile al Titolare all'avvio del contratto di fornitura, ad ogni aggiornamento derivante dalla sostituzione dell' AdS e ad ogni richiesta del Titolare.

9.SERVIZIO DI AMMINISTRAZIONE DI SISTEMA IN OUTSOURCING

Il Provvedimento del Garante del 27 novembre 2008 prevede che le Società che offrono servizi di amministrazione di sistema in outsourcing debbano anch'esse garantire l'adempimento alle prescrizioni del provvedimento del Garante.
Pertanto, qualora il servizio di amministrazione di sistema sia affidato in outsourcing, il fornitore del servizio, designato quale Responsabile esterno del trattamento dei dati, è obbligato a:

a) specificare per ciascun soggetto designato quale amministratore di sistema l'ambito di operatività consentito in base al profilo di autorizzazione assegnato;
b) conservare e aggiornare direttamente e specificatamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema su apposito elenco;
c) verificare l'operato degli amministratori;
d) adottare sistemi di registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori.

10.RESPONSABILITA' PERSONALE DELL' AMMINISTRATORE DI SISTEMA

L' Amministratore di Sistema è tenuto ad un comportamento consapevole, ispirato ai principi di diligenza, fedeltà, correttezza ed idoneo a preservare l'integrità delle risorse aziendali e la riservatezza delle informazioni, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 del codice civile e della normativa vigente in materia di protezione dei dati personali.
E' personalmente responsabile dei dati trattati.
L'accesso ai sistemi informatici è consentito all'AdS unicamente nell'ambito di operatività consentito in base al profilo di autorizzazione assegnato, potendo effettuare solo le operazioni necessarie a garantire il corretto funzionamento e la sicurezza di tali sistemi.
E' fatto espresso divieto di trattare i dati personali per finalità diverse da quelle consentite.
L'AdS è, altresì, tenuto a mantenere l'assoluto riserbo sui dati personali di cui possa venire a conoscenza, anche incidentalmente, in ragione dell'esercizio delle funzioni/mansioni assegnate.

Adozione misure di sicurezza

L'Amministratore di sistema garantisce le più avanzate soluzioni per la protezione dei dati e la sicurezza informatica.
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, l'AdS propone al Titolare l'adozione di misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio, assicurandone la corretta installazione, configurazione, gestione e risoluzione dei problemi nel rispetto dei tempi e delle specifiche fornite.
Tali misure devono comprendere:

a) le misure di sicurezza ICT emanate dall'AgID, adeguate alla realtà organizzativa dell'Azienda,
b) le misure di sicurezza previste dall'art. 32 del Regolamento UE 2016/679, ivi comprese:

- ✓ la pseudonimizzazione e la cifratura dei dati personali;
- ✓ la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- ✓ la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- ✓ una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.

È responsabilità dell' AdS comprendere le minacce di sicurezza incombenti sui propri sistemi e di adottare le contromisure di sicurezza necessarie ad assicurare confidenzialità, integrità e disponibilità dei dati e delle informazioni.

Analisi dei rischi

Ogni progetto che prevede l'installazione, l'utilizzo, la modifica, l'eliminazione di uno o più sistemi informatici deve essere adottato dall'AdS previa un'adeguata analisi dei rischi che tenga conto delle risorse da proteggere, delle potenziali minacce di sicurezza e dei meccanismi di sicurezza.

Collaborazione con il Titolare, il Designato al trattamento ed il Responsabile della Protezione dei Dati

L'AdS è tenuto a collaborare con il Titolare, il Designato al trattamento ed il Responsabile della Protezione di Dati, per l'adempimento degli obblighi previsti dal Regolamento Europeo 2016/679.

E' obbligato a collaborare con il Titolare nel condurre, laddove necessario, una valutazione di impatto sulla protezione dei dati (DPIA) ed, in generale, nella predisposizione e/o nell'aggiornamento e/o nell'integrazione di tutti i documenti necessari per il rispetto del Regolamento Europeo in materia di privacy.

Attività di verifica delle misure di sicurezza adottate

L' AdS è responsabile della verifica delle misure di sicurezza adottate e della valutazione della loro efficacia e l'efficienza.

Il Titolare può affidare tale attività anche a fornitori esterni di servizi tenuti a rilasciare all'Azienda apposita attestazione di conformità del servizio ai requisiti previsti dalla normativa vigente in materia di protezione dei dati personali.

Nel caso in cui, a seguito dell'analisi dei rischi privacy (DPIA) od in conseguenza dell'attività di verifica, le misure di sicurezza adottate risultino non adeguate al rischio, l'AdS deve proporre con urgenza la loro implementazione al Titolare ed ai Responsabili del trattamento.

Data breach

L'AdS è obbligato a reagire agli incidenti di sicurezza prontamente e con spirito di cooperazione ed a segnalare immediatamente eventuali data breach, seguendo le istruzioni dettate **PROCEDURA AZIENDALE DI GESTIONE DELLA VIOLAZIONE DI DATI (DATA BREACH),** pubblicata sul sito internet aziendale nella sezione privacy, a cui si fa rinvio.

Documentazione tecnica

L'AdS è responsabile della tenuta ordinata della documentazione e del tempestivo aggiornamento della stessa, in relazione a tutti i sistemi, banche dati, apparati di rete e

sicurezza, applicazioni software di qualunque natura e complessità, nonché alle procedure operative di installazione, configurazione ed aggiornamento delle strumentazioni informatiche e telematiche, in relazione al proprio ambito di responsabilità ed operatività.
Tale documentazione deve essere messa a disposizione per la consultazione dei soggetti autorizzati, per quanto di rispettiva competenza.

Sanzioni

La violazione delle disposizioni del presente Regolamento espone l'AdS a sanzioni disciplinari (nel caso di AdS interno) ed eventualmente anche a responsabilità di carattere penale e civile, oltre che al risarcimento dei danni, qualora causati all'Azienda ed a terzi.
Il ruolo di Amministratore di sistema può costituire una aggravante in alcuni reati penali compiuti nell'esercizio delle sue funzioni ed in relazione ai "privilegi" allo stesso concessi, quali, a mero titolo esemplificativo:

- Accesso abusivo a sistema informatico o telematico (art. 615 ter c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617 quater c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (617 quinquies c.p.);
- Frode informatica (art. 640 ter c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (artt. 635 bis e ter c.p.);
- Danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinques c.p.).

ALLEGATI:

ALL. A - NOMINA AMMINISTRATORE DI SISTEMA PERSONALE DIPENDENTE
ALL. B - ELENCO AMMINISTRATORI DI SISTEMA

ALLEGATO A

NOMINA AMMINISTRATORE DI SISTEMA
PERSONALE DIPENDENTE

IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

Azienda Sanitaria Locale di Brindisi, in persona del Direttore Generale Dr. Giuseppe Pasqualone,

- **Visto il provvedimento del Garante per la protezione dei dati personali del 27/11/2008**, pubblicato nella G.U. n°300 del 24/12/2008 e s.m.i., il quale ha richiamato l'attenzione dei Titolari del trattamento sulla rilevanza, specificità e particolare criticità del ruolo svolto dall'Amministratore di sistema, richiedendo l'adozione di adeguate cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, soprattutto quelli realizzati con abuso della qualità di Amministratore di sistema;
- **Visto il Regolamento Aziendale sulla protezione dei dati per gli Amministratori di sistema,** per il quale l'attribuzione delle relative funzioni deve avvenire previa valutazione delle specifiche caratteristiche del soggetto designato, secondo le prescrizioni dell'Autorità Garante;
- **Considerato** che per l'attribuzione delle funzioni di Amministratore di sistema occorre indicare l'elencazione analitica degli ambiti di operatività allo stesso consentiti in base al profilo di autorizzazione assegnato;
- **Dato atto che per le necessità organizzative aziendali sono stati definiti i seguenti ambiti di operatività:**
  - ☐ Gestione, sicurezza e manutenzione del sistema informatico;
  - ☐ Gestione sistemistica delle postazioni di lavoro;
  - ☐ Gestione sistemistica, sicurezza e monitoraggio della rete informatica;
  - ☐ Gestione sistemistica dei Server aziendali;
  - ☐ Back-up e Disaster Recovery;
  - ☐ Gestione dei sistemi software e delle basi dati relative agli applicativi in uso;
  - ☐ Altro_____;
- **Valutato il curriculum professionale** del candidato da cui emerge una accertata esperienza nel settore ed una adeguata formazione professionale in relazione all'attribuzione della nomina di Amministratore di Sistema;
- **Valutate la capacità e l'affidabilità tecnica sotto il profilo della sicurezza,** dichiarate e garantite dal candidato;

Con la presente,

NOMINA

il/la ***Sig.***_____
Matr._____ ***Cod. Fisc.***_____ , quale Amministratore di Sistema (in seguito AdS) della ASL BRINDISI con il seguente ambito di operatività:

- ☐ Gestione, sicurezza e manutenzione del sistema informatico;
- ☐ Gestione sistemistica e sicurezza delle postazioni di lavoro;
- ☐ Gestione sistemistica, sicurezza e monitoraggio della rete informatica;
- ☐ Gestione sistemistica e sicurezza dei Server aziendali;
- ☐ Back-up e Disaster Recovery;
- ☐ Gestione dei sistemi software e delle basi dati relative agli applicativi in uso;
- ☐ Altro _____.

COMPITI E RESPONSABILITÀ DELL'AMMINISTRATORE DI SISTEMA

L'Amministratore di sistema deve assicurare il corretto funzionamento ed utilizzo del sistema informatico oggetto dell'incarico ed espletare tutte le attività tecniche necessarie, ivi comprese le seguenti:

- ☐ progettazione, installazione, configurazione, gestione e manutenzione dei sistemi informatici;
- ☐ controllo sul corretto utilizzo, funzionamento e protezione dei sistemi di gestione ed elaborazione dei dati;
- ☐ impostazione e gestione dei sistemi di autenticazione e di autorizzazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
- ☐ organizzazione e gestione dei flussi di rete;
- ☐ gestione dei supporti di memorizzazione;
- ☐ manutenzione dell'hardware;
- ☐ classificazione analitica delle banche dati ed impostazione/organizzazione di un sistema complessivo di trattamento informatizzato dei dati personali comuni e particolari, nel rispetto della normativa vigente in materia di protezione dei dati personali;
- ☐ predisposizione e gestione dei sistemi di salvataggio (backup), anche automatici, con adozione di adeguate procedure per la custodia delle copie di sicurezza dei dati;
- ☐ adozione di adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS ecc.);
- ☐ predisposizione di sistemi di ripristino dei dati e dei sistemi (recovery), anche automatici, che assicurino di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- ☐ adozione di un sistema idoneo alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Tali registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate ed essere conservate per un congruo periodo, non inferiore a dodici mesi;
- ☐ adozione di tutte le misure di sicurezza adeguate al rischio, ivi comprese:

- ✓ la pseudonimizzazione e la cifratura dei dati personali;
- ✓ la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- ✓ la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- ✓ una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.

- ☐ adozione delle misure di sicurezza ICT emanate dall'AgID, adeguate alla realtà organizzativa aziendale**;**
- ☐ verifica e monitoraggio costante dei sistemi informatici al fine di rilevare immediatamente eventuali tentativi di accessi non autorizzati al sistema provenienti da soggetti terzi, quali accesso abusivo al sistema informatico o telematico, frode, danneggiamento di informazioni, dati e programmi informatici, danneggiamento di sistemi informatici e telematici;
- ☐ controllo sugli interventi informatici effettuati da operatori esterni;
- ☐ predisposizione di un piano di controlli periodici, da eseguire con cadenza almeno semestrale, atti a testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- ☐ provvedere alla distruzione e smaltimento dei supporti informatici di memorizzazione logica obsoleti e/o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento dei dati personali;
- ☐ altro _____.

L' Amministratore di Sistema è tenuto ad un comportamento consapevole, ispirato ai principi di diligenza, fedeltà, correttezza ed idoneo a preservare l'integrità delle risorse aziendali e la riservatezza delle informazioni, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 del codice civile e della normativa in materia di protezione dei dati personali.
E' personalmente responsabile dei dati trattati.
L'accesso ai sistemi informatici è accordato all'AdS unicamente nell'ambito di operatività consentito in base al profilo di autorizzazione assegnato e limitatamente a quanto necessario per garantire il corretto funzionamento e la sicurezza di tali sistemi.
E' fatto espresso divieto di trattare i dati personali per finalità diverse da quelle consentite.
L'AdS è, altresì, tenuto a mantenere l'assoluto riserbo sui dati personali di cui possa venire a conoscenza, anche incidentalmente o per caso fortuito, in ragione dell'esercizio delle funzioni/mansioni assegnate.

Adozione misure di sicurezza

L'amministratore di sistema garantisce le più avanzate soluzioni per la protezione dei dati e la sicurezza informatica.
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, l'AdS propone al Titolare l'adozione di misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio, assicurandone la corretta installazione, configurazione, gestione e risoluzione dei problemi nel rispetto dei tempi e delle specifiche fornite.

È responsabilità dell' AdS comprendere le minacce di sicurezza incombenti sui propri sistemi e di adottare le contromisure di sicurezza necessarie ad assicurare confidenzialità, integrità e disponibilità dei dati e delle informazioni.

Analisi dei rischi

Ogni progetto che prevede l'installazione, l'utilizzo, la modifica, l'eliminazione di uno o più sistemi informatici deve essere adottato dall'AdS previa un'adeguata analisi dei rischi che tenga conto delle risorse da proteggere, delle potenziali minacce di sicurezza e dei meccanismi di sicurezza.

Collaborazione con il Titolare, il Designato al trattamento ed il Responsabile della Protezione dei Dati

L'AdS è tenuto a collaborare con il Titolare, il Designato al trattamento ed il Responsabile della Protezione di Dati, per l'adempimento degli obblighi previsti dal Regolamento Europeo 2016/679.

E' obbligato a collaborare con il Titolare nel condurre, laddove necessario, una valutazione di impatto sulla protezione dei dati (DPIA) ed, in generale, nella predisposizione e/o nell'aggiornamento e/o nell'integrazione di tutti i documenti necessari per il rispetto del Regolamento Europeo in materia di privacy.

Attività di verifica delle misure di sicurezza adottate

L' AdS è responsabile della verifica delle misure di sicurezza adottate e della valutazione della loro efficacia e l'efficienza.

Il Titolare può affidare tale attività anche a fornitori esterni di servizi tenuti a rilasciare all'Azienda apposita attestazione di conformità del servizio ai requisiti previsti dalla normativa vigente in materia di protezione dei dati personali.

Nel caso in cui, a seguito dell'analisi dei rischi privacy (DPIA) od in conseguenza dell'attività di verifica, le misure di sicurezza adottate risultino non adeguate al rischio, l'AdS deve proporre con urgenza la loro implementazione al Titolare ed ai Responsabili del trattamento.

Data breach

L'AdS è obbligato a reagire agli incidenti di sicurezza prontamente e con spirito di cooperazione ed a segnalare immediatamente eventuali data breach, seguendo le istruzioni dettate dalla **PROCEDURA AZIENDALE DI GESTIONE DELLA VIOLAZIONE DI DATI (DATA BREACH),** pubblicata sul sito internet aziendale nella sezione privacy, cui si fa rinvio.

Documentazione tecnica

L'AdS è responsabile della tenuta ordinata della documentazione e del tempestivo aggiornamento della stessa, in relazione a tutti i sistemi, banche dati, apparati di rete e sicurezza, applicazioni software di qualunque natura e complessità, nonché alle procedure operative di installazione, configurazione ed aggiornamento delle strumentazioni informatiche e telematiche, in relazione al proprio ambito di responsabilità ed operatività.

Tale documentazione deve essere messa a disposizione per la consultazione dei soggetti autorizzati.

Sanzioni

La violazione delle disposizioni del presente Regolamento espone l'AdS a sanzioni disciplinari ed eventualmente anche a responsabilità di carattere penale e civile, oltre che al risarcimento di eventuali danni causati all'Azienda e a terzi.

****

L'Amministratore di Sistema è fin d'ora informato del fatto che il suo operato sarà oggetto di loggatura e registrazione e che, con cadenza annuale, il suo profilo sarà oggetto di attività di monitoraggio al fine di verificare la rispondenza alle misure organizzative, tecniche e di sicurezza predisposte per l'esercizio delle funzioni dell'amministratore di sistema, in ottemperanza del Provvedimento del Garante del 27 novembre 2008.

Si informa, infine, l'Amministratore di Sistema che i suoi dati identificativi saranno pubblicati sul sito aziendale, nella sezione privacy, a disposizione di tutti i dipendenti.

La presente designazione di Amministratore di sistema si dovrà considerare automaticamente revocata in caso di cessazione del rapporto di lavoro.

****

L'Amministratore di Sistema designato, con la sottoscrizione della presente, accetta la presente nomina e

DICHIARA

- di essere a conoscenza degli obblighi previsti dai Provvedimenti del Garante ed in particolare dal provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni del amministratore di sistema - 27 novembre 2008(G.U. n. 300 del 24 dicembre 2008)", dalla normativa vigente in materia di trattamento dei dati personali (Regolamento UE 2016/679 e Codice Privacy - D.Lgs. 196/03 modificato dal D.Lgs.101/18 e dai Regolamenti Aziendali, che si impegna a rispettare;
- di aver preso visione, in particolare, del Regolamento aziendale sulla protezione dei dati per gli Amministratori di sistema;
- di garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e di impegnarsi a procedere al trattamento dei dati personali nel pieno rispetto delle istruzioni del Titolare;
- di possedere le qualità tecniche, professionali e di condotta, le competenze e l'esperienza necessarie allo svolgimento del suddetto incarico.

Brindisi,

IL TITOLARE DEL TRATTAMENTO

_____

PER RICEVUTA ED ACCETTAZIONE

_____

ALLEGATO B

ELENCO AMMINISTRATORI DI SISTEMA
Provvedimento Garante privacy 27/11/2008

IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

Azienda Sanitaria Locale Br di Brindisi, in persona del Direttore Generale Dr. Giuseppe Pasqualone, dichiara che il sottoelencato personale dipendente, è stato nominato quale amministratore di sistema, in ottemperanza del provvedimento del Garante per la protezione dei dati personali del 27/11/2008, pubblicato nella G.U. n°300 del 24/12/2008 e s.m.i:

COGNOME	NOME	DATA NOMINA	AMBITO