REGOLAMENTO AZIENDALE PER GLI

AMMINISTRATORI DI SISTEMA

Versione	Data	Modifiche
1.0	01/02/2023	Prima stesura

SOMMARIO

1. Premessa

Gli **Amministratori di Sistema** sono una categoria di operatori preposti all'esercizio dei sistemi informatici che, in funzione dei compiti ad essi assegnati, occupano i vertici della gerarchia di utenze, in termini di **privilegi di accesso alle risorse informatiche e ai dati ivi custoditi**. Per tali motivi, il processo di attribuzione degli incarichi di Amministratore, così come la definizione dei relativi profili e permessi di accesso, riveste un carattere di estrema importanza per la sicurezza dei sistemi informatici e conseguentemente per la sicurezza delle informazioni personali a cui potrebbero accedere nello svolgimento dei propri compiti.

Il presente Regolamento recepisce i requisiti definiti nel provvedimento dell'Autorità Garante per la Protezione dei dati del 27/11/2008 "**Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema**" (G.U. n. 300 del 24 dicembre 2008), così come modificato in base al Provvedimento del 25 giugno 2009, nell'osservanza del Regolamento UE 2016/679.

Il Provvedimento dell'Autorità Garante per la protezione dei dati prescrive specifiche accortezze che devono essere adottate nella designazione e gestione degli Amministratori di Sistema, prevedendo nello specifico, attività di verifica sull'operato di questi ultimi per garantire la conformità alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle normative vigenti. L'ASL di Foggia, nella persona del Titolare del trattamento dei dati personali, recepisce ed include il presente Regolamento nell'insieme delle **misure di carattere organizzativo e procedurale** che concorrono alla tutela dei diritti dell'interessato ed alla sicurezza dei dati personali, in ottemperanza al **principio di responsabilizzazione** (c.d. *accountability*), formulato nel Regolamento (UE) 2016/679.

2. Finalità e ambito di applicazione

Il presente Regolamento ha lo scopo di definire i requisiti che l'ASL di Foggia deve recepire e adottare, al fine di assicurare la conformità dell'operato degli Amministratori di Sistema alle prescrizioni del Provvedimento del Garante della Privacy del 27/11/2008, in relazione a tutti i **sistemi di elaborazione** e **archivi elettronici** contenenti **dati personali**. Gli indirizzamenti formulati nel presente documento, sono da considerarsi come misure minime la cui attuazione si rende necessaria per contenere, entro limiti accettabili, il **rischio di compromissioni della riservatezza, integrità e disponibilità** delle risorse informative dell'ASL di Foggia. In tal senso, queste costituiscono i requisiti di base minimi ed obbligatori che, in quanto tali, in virtù delle specifiche caratteristiche del contesto operativo a cui si applicano, possono essere incrementati qualora, in determinati contesti, siano richiesti livelli di protezione più elevati.

Gli indirizzamenti definiti nel presente documento, si applicano all'operato degli Amministratori di Sistema che, a vario titolo, operano sui sistemi informatici dell'ASL di Foggia, in relazione a tutti i sistemi che trattano dati personali, ai sensi del Regolamento (UE) 2016/679 e del D.lgs. 196/03, così come modificato dal D.lgs. 101/18.

3. Normative 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 (Regolamento generale sulla protezione dei dati);
- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – Garante Privacy Provvedimento del 27/11/2008 e succ. modificazioni;
- Legge n.547 del 23 dicembre 1993 sul tema della criminalità informatica;
- Linee guida del Garante per posta elettronica e internet – Garante Privacy - Provvedimento n. 13 del 1° marzo 2007 (G.U. n. 58 del 10 marzo 2007);
- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";
- Decreto Legislativo 10 agosto 2018, n. 101 “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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”.

4. Il ruolo dell'Amministratore di Sistema

Il Provvedimento del Garante Privacy del 27/11/2008, identifica come "Amministratori di Sistema" le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Sono identificati quindi come Amministratori di Sistema, le figure professionali che svolgono le seguenti funzioni, nella misura in cui esse consentono di intervenire sui dati i personali:

- Gestione e manutenzione di un impianto di elaborazione o di sue componenti;
- Gestione delle basi di dati;
- Gestione delle reti;
- Gestioni di apparati di sicurezza;
- Gestione di sistemi software complessi;
- Gestione di servizi/piattaforme software esternalizzati in *cloud*;
- Gestione impianti di videosorveglianza;
- Gestione di sistemi di gestione e conservazione documentale;
- Gestione di sistemi di messaggistica.

Non rientrano nella definizione, quei soggetti che solo occasionalmente intervengono per es. a scopo di manutenzione a seguito di guasti o malfunzionamenti sui sistemi software.

Si considerano Amministratore di Sistema le seguenti figure che ricoprono uno dei seguenti ruoli:

- *System Administrator*, ruolo attribuito agli operatori preposti alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti;
- *Database Administrator*, ruolo attribuito agli operatori preposti alla gestione della struttura logica, dei permessi di accesso, delle attività di ottimizzazione delle prestazioni, delle attività di back-up delle basi di dati ed in genere del *middleware* costituito dai *Data Base Management System*;

- *Application Administrator*, ruolo attribuito agli operatori preposti alla gestione di una specifica applicazione;
- *Network Administrator* ruolo attribuito agli operatori preposti alla gestione delle reti informatiche di comunicazione;
- *Security Administrator*, ruolo attribuito agli operatori preposti alla gestione delle componenti e delle piattaforme hw/sw dedicate alla sicurezza dei sistemi informatici e delle reti.

5. I requisiti dell'Amministratore di Sistema

Sono di seguito definiti i requisiti di attuazione delle prescrizioni contenute nel Provvedimento del 23/11/2008, che coinvolgono gli Amministratori di Sistema:

- **Valutazione delle caratteristiche soggettive**: l'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.
- **Designazioni individuali degli Amministratori di Sistema**: l'attribuzione dell'incarico di Amministratore di Sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
- **Gestione dell'elenco**: l'elenco degli estremi identificativi delle persone fisiche Amministratori di Sistema, con l'ambito di operatività ad essi attribuito, deve essere mantenuto aggiornato e disponibile in caso di accertamenti da parte del Garante.
- **Registrazione degli accessi**: devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di Sistema. Le registrazioni (access log) devono avere caratteristiche di

completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

- **Servizi in outsourcing**: nel caso di servizi di gestione in outsourcing il fornitore dovrà fornire, su richiesta dell'ASL di Foggia, nella persona del titolare del trattamento, gli estremi identificativi delle persone fisiche che svolgono il ruolo di Amministratori di Sistema in ottemperanza al servizio erogato.
- **Verifica delle attività**: l'operato degli Amministratori di Sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare del trattamento, o suo delegato, in modo da controllare l'osservanza delle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali.

Precedentemente al conferimento dell'incarico, devono essere valutate attentamente le caratteristiche soggettive quali esperienza, capacità e affidabilità, dei soggetti designati a svolgere il ruolo di Amministratore di sistema.

Ai soggetti designati, e inoltre richiesta la presa visione, la comprensione e l'accettazione delle disposizioni vigenti in materia di trattamento dei dati personali e delle norme di sicurezza, con particolare riferimento a:

- Conoscenza delle normative di leggi applicabili;
- Conoscenza delle politiche interne all'Azienda, nonché delle *best practices* di riferimento in materia di gestione "sicura" dei sistemi informatici;
- Consapevolezza dei rischi di sicurezza derivanti da errori, omissioni e violazioni delle regole applicabili allo svolgimento delle attività di Amministratore di sistema.

Per quanto riguarda gli Amministratori di Sistema esterni (collaboratori esterni non dipendenti), il processo di valutazione delle caratteristiche soggettive è a carico della società fornitrice del servizio.

Tali valutazioni posso in ogni momento essere verificate e validate dal Titolare del trattamento o da persone interne all'ASL di Foggia da questi incaricate. Relativamente ai servizi in outsourcing (es. Data Center esterni, hosting etc.) il Titolare del trattamento procede alla nomina del fornitore, in qualità di Responsabile del trattamento dei dati, ai sensi dell'art. 28 del Regolamento UE 2016/679. In tal caso, i requisiti definiti nel presente Regolamento devono essere inclusi nelle clausole contrattuali che normano la designazione del Responsabile esterno.

L'attribuzione dell'incarico di Amministratore di Sistema che tratta dati personali, deve essere in ogni caso individuale, ovvero la persona designata deve essere identificabile in maniera univoca. A tale scopo, l'ASL di Foggia, nella persona del Titolare del trattamento o suo Designato, predispone una specifica lettera di incarico (nomina dell'Amministratore di Sistema) contenente almeno le seguenti informazioni:

- elencazione analitica degli ambiti di operatività richiesti e consentiti, in base al profilo di autorizzazione assegnato;
- notifica che l'operato dell'Amministratore di Sistema può essere soggetto a verifiche con cadenza almeno annuale, anche attraverso la rilevazione e la successiva analisi dei log di accesso (login, logout) generati nel corso dello svolgimento delle attività di amministrazione;
- notifica che la nomina ed il relativo nominativo potrebbero essere comunicati al personale ed eventualmente a terzi nei modi previsti dalle vigenti disposizioni normative.

6. Principi applicabili al trattamento dei dati

L'Amministratore di Sistema, nell'espletamento delle sue attività tecniche, deve sempre applicare i principi fondamentali previsti dall'art. 5 del Regolamento UE 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 alle finalità perseguite; eventuali attività di monitoraggio devono essere mirate solo in aree critiche, 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.

È vietato qualsiasi trattamento di dati personali preordinato al controllo a distanza dei lavoratori. All'atto della cessazione del rapporto con il Titolare, l'Amministratore di sistema designato dovrà restituire tutti i dati personali eventualmente raccolti in copia su sistemi o dispositivi, con espresso divieto di conservarli. Altresì l'Amministratore di sistema uscente dovrà garantire il passaggio di consegne con particolare riferimento a credenziali di accesso privilegiate, documentazione tecnica relativa a configurazioni di sistemi o servizi e ogni altra informazione necessaria per la sicurezza e continuità dei servizi informatici.

7. Registro degli Amministratori di Sistema

Con il presente Regolamento, il Titolare del trattamento dispone al Responsabile della S.S. Sistemi informativi e Telecomunicazioni, la creazione di un **registro degli Amministratori di sistema** che deve contenere, come minimo, le seguenti informazioni:

- gli estremi identificativi (nome/cognome/matricola) delle persone fisiche designate, la cui attività riguarda anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di dati personali;
- data della nomina e l'elenco delle mansioni operative attribuite (ambiti di operatività consentiti).

L'elenco contenente gli estremi identificativi dei dipendenti designati Amministratori di Sistema e l'ambito di operatività ad essi attribuito, deve essere mantenuto aggiornato e disponibile in caso di accertamenti da parte del Garante. La revisione di correttezza delle informazioni indicate nell'elenco deve essere eseguita almeno una volta l'anno, fermo restando che eventuali aggiornamenti in caso di

nuove nomine o revoche degli incarichi, devono essere prontamente riportati, a cura della S.S. Sistemi informativi e Telecomunicazioni.

8. Registrazione accessi degli Amministratori di Sistema

Il Provvedimento dell'Autorità Garante per la protezione dei dati, richiede la registrazione degli accessi logici ai sistemi da parte degli Amministratori, pertanto devono essere adottati **sistemi idonei alla registrazione di tali eventi, relativamente all'accesso ai sistemi di elaborazione (sistemi operativi) e agli archivi elettronici (database) effettuati dagli Amministratori di Sistema.**

Non è obbligatorio il tracciamento degli accessi degli Amministratori ai servizi applicativi, a meno che tale disposizione non derivi da requisiti di sicurezza impartiti dal Titolare, applicabili a specifici trattamenti rilevati in sede di DPIA (*Data Protection Impact Assessment*), ai sensi dell'art. 35 del Regolamento UE 2016/679.

Per log di accesso, si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso (*logon o login*), o tentativo di accesso da parte di un Amministratore di Sistema o all'atto della sua disconnessione (*logoff o logout*), nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software. Tali registrazioni devono avere caratteristiche di **completezza, inalterabilità e possibilità di verifica della loro integrità**, adeguate al raggiungimento dello scopo per cui sono state richieste.

La caratteristica di completezza è riferita all'insieme degli eventi censiti nel sistema di log, che deve comprendere tutti gli eventi di accesso interattivo, generati dalle attività degli Amministratori di Sistema su tutti i sistemi di elaborazione (server, client, database) con cui vengono trattati, anche indirettamente, dati personali. Le registrazioni devono inoltre comprendere, i riferimenti temporali e la descrizione dell'evento che le ha generate. Le caratteristiche legate all'inalterabilità dei dati raccolti dai sistemi di log, può essere soddisfatta ad esempio, attraverso l'implementazione di una piattaforma

centralizzata per la gestione dei log con l'utilizzo di canali di trasmissione sicuri o l'utilizzo di supporti non riscrivibili per la conservazione dei log.

La caratteristica legata alla possibilità di verifica dell'integrità dei log può essere soddisfatta, ad esempio, tramite l'applicazione di tecniche di **cifratura, *time stamping* o *hashing***.

Pertanto, devono essere implementate idonee soluzioni tecnologiche atte a garantire la creazione e la raccolta dei log di accesso degli Amministratori di Sistema, secondo le caratteristiche di completezza, inalterabilità e verifica della loro integrità definite nel presente Regolamento.

I log di accesso ai sistemi di elaborazione e agli archivi elettronici effettuati dagli Amministratori di Sistema, devono essere conservati per un congruo periodo, non inferiore a 6 (sei) mesi. Trascorso tale periodo, dovrà esserne prevista la cancellazione definitiva da ogni supporto di archiviazione.

9. Gestione servizi in outsourcing

Il Provvedimento dell'Autorità Garante per la protezione dei dati, prevede che le società che offrono servizi di amministrazione di sistema in outsourcing, in qualità di Responsabili del trattamento, debbano anch'esse garantire l'adempimento alle prescrizioni del provvedimento del Garante. Pertanto, l'ASL di Foggia, all'avvio di un rapporto di fornitura, deve designare le **aziende fornitrici di servizi di outsourcing, quali Responsabili dei trattamenti di dati personali**, ai sensi dell'art. 28 del Regolamento UE 20106/679, rispetto ai quali sono chiamate a svolgere funzioni di Amministratore di Sistema.

Con l'aggiornamento apportato dal Provvedimento del Garante, sarà il Responsabile (e quindi la società che fornisce il servizio) a provvedere alla nomina dell'Amministratore di Sistema al proprio interno. Sarà quindi necessario, che l'ASL di Foggia, nella persona del Titolare del trattamento, notifichi al Responsabile questa incombenza e che a sua volta, quest'ultimo attesti l'avvenuta nomina del soggetto a cui sono attribuite funzioni di Amministratore di Sistema nella forma del contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri.

L'elenco contenente gli estremi identificativi degli operatori esterni che svolgono per conto dell'ASL di Foggia, mansioni di Amministratore di sistema, deve essere aggiornato e reso disponibile dalla società fornitrice su richiesta, in base a quanto previsto dal Provvedimento del Garante, nei seguenti casi:

- all'avvio del contratto di fornitura;
- ad ogni aggiornamento intercorso su tali elenchi;
- ad ogni richiesta da parte del Titolare del trattamento.

In base alla prescrizione del Garante, il Titolare del trattamento è comunque responsabile dell'attuazione del requisito di verifica sulle attività degli Amministratori di Sistema (es. verifica dei log di accesso), anche se afferenti a servizi erogati da fornitori esterni e in tal caso, questo adempimento può essere comunque demandato ad un Responsabile del trattamento nominato in sede contrattuale.

10. 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'Amministratore di sistema, previa un'adeguata **analisi dei rischi** che tenga conto delle **risorse da proteggere**, delle potenziali minacce di sicurezza e delle misure adeguate di sicurezza. L'Amministratore di sistema è tenuto a:

- collaborare con il Designato al trattamento (Dirigente) ed il Responsabile della Protezione di Dati, per l'adempimento degli obblighi previsti dagli artt. 24-32 del Regolamento UE 2016/679;
- collaborare con il Titolare nel condurre, laddove necessario, una valutazione di impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 35 del Regolamento UE 2016/679 e, in generale, nella predisposizione e/o nell'aggiornamento e/o nell'integrazione di tutti i documenti necessari a dimostrare la conformità dei trattamenti di dati personali e dei sistemi informatici.

11. Violazioni di dati

L'Amministratore di sistema è tenuto a segnalare eventuali incidenti di sicurezza con spirito di cooperazione seguendo le istruzioni riportate nella "Procedura interna per la gestione delle violazioni dei dati personali (*Data Breach*)" giusta deliberazione del Direttore Generale n. 899 del 22 giugno 2020, pubblicata sul sito internet aziendale nella sezione privacy, a cui si rinvia.

12. Custodia documenti

L'Amministratore di sistema, per quanto di competenza, è responsabile della **tenuta ordinata della documentazione tecnica 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 del Responsabile della protezione dei dati nell'ambito della sorveglianza periodica della conformità dei trattamenti di dati personali.

13. Verifica delle attività

Devono essere effettuate **verifiche periodiche** sull'operato degli Amministratori di Sistema con cadenza almeno annuale, per rilevarne la **rispondenza alle misure organizzative, tecniche e di sicurezza** riguardanti i trattamenti dei dati personali.

Di seguito sono descritte le attività di verifica, con una indicazione di massima sulla rispettiva cadenza periodica:

- Cadenza annuale: verifiche di riscontro, su un campione significativo di sistemi, della corretta generazione dei log di accesso, della loro conformità e della conservazione sicura degli stessi per almeno sei mesi;
- Cadenza annuale: analisi di dettaglio dei log di accesso, al fine di riscontrare eventuali anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, archivi digitali cui si è fatto accesso, postazioni di lavoro utilizzate, ecc …);
- Cadenza annuale: verifiche di riscontro dell'attuazione del processo di gestione dell'elenco degli Amministratori di Sistema e verifica dell'allineamento di tale lista, con l'assegnazione dei ruoli e dei relativi ambiti di operatività;
- Su richiesta, ogni qualvolta vi sia necessità interna o su richiesta degli organi esterni (e.g. Autorità Giudiziaria, Autorità Garante per la protezione dei dati), di effettuare attività di controllo specifiche.

Le suddette attività di verifica devono essere formalizzate mediante la redazione di un report denominato "Rapporto di verifica delle attività svolte dagli Amministratori di sistema", attestante:

- la data di esecuzione delle attività;
- l'ambito di applicazione (*scope*) delle verifiche effettuate (sistemi informatici e tipologie di log);
- i componenti del *team* di verifica ed eventuali altre figure presenti;
- le tipologie di verifiche compiute ed i relativi esiti;
- le eventuali non conformità o eventi anomali rilevati;
- gli eventuali *Action Plan* a fronte di non conformità rilevate, con la chiara indicazione di:

✓ Ruoli e Responsabilità per l'esecuzione e la verifica delle attività previste;

✓ tempistiche;

✓ modalità e frequenza di verifica dell'applicazione dei piani di rientro.

14. Sanzioni applicabili

La mancata applicazione dei requisiti di sicurezza espressi nel presente Regolamento può esporre l'ASL di Foggia a possibili sanzioni derivanti dall'inadempienza alle misure cogenti.
L'Amministratore di sistema è 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. In particolare, l'Amministratore di sistema non potrà comunicare o diffondere alcuna delle informazioni, notizie, dati e documenti (salvo che ciò non sia espressamente richiesto dal Titolare, dal Garante Privacy o da altra Autorità), cederli a terzi a titolo gratuito o oneroso, utilizzarli per qualsiasi finalità, anche di terzi. Gli obblighi di riservatezza, di non diffusione, di non comunicazione a soggetti che non siano autorizzati al trattamento permarranno anche dopo la cessazione del rapporto contrattuale.
La violazione delle disposizioni del presente Regolamento espone l'Amministratore di Sistema a **sanzioni disciplinari** ed eventualmente anche a **responsabilità di carattere penale e civile**, oltre che al risarcimento dei danni. 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 elevati**" allo stesso concessi, quali, a mero titolo esemplificativo:

- **accesso abusivo** ad un sistema informatico o telematico (art. 615 *ter* Codice penale);
- **danneggiamento** di sistemi informatici e telematici (art. 635 *bis* Codice penale);
- **danneggiamento** di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 *ter* Codice penale);
- **danneggiamento** di sistemi informatici o telematici (art. 635 *quater* Codice penale);
- **danneggiamento** di sistemi informatici o telematici di pubblica utilità (art. 635 *quinquies* Codice penale);
- **frode informatica** (art. 640 *ter* Codice penale).

15. Aggiornamento e revisione

Il presente Regolamento è soggetto a revisione come per Legge o qualora se ne ravveda la necessità.
Copia del presente documento verrà consegnata a ciascun dipendente aziendale con funzioni di Amministratore di Sistema, ovvero messo a disposizione di chiunque ne faccia richiesta, anche attraverso la pubblicazione nell'apposita sezione Privacy del sito internet istituzionale.
Con l'entrata in vigore del presente Regolamento, coincidente con la data di adozione formale tramite deliberazione del Direttore Generale, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.

IL DIRETTORE GENERALE

ASL FOGGIA