Autorizzazione per il trattamento di dati personali in qualità di "Amministratore di sistema"

Ai sensi del Regolamento UE 679/2016 e del Provvedimento "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 e successive modifiche" dell'Autorità di Controllo italiana

PREMESSO CHE

- Il Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito "Regolamento"), che abroga la Direttiva 95/46/CE e le implementazioni della stessa, fissa le modalità da adottare ed individua i soggetti che, in relazione all'attività svolta, sono tenuti agli adempimenti previsti dal Regolamento;
- il considerando 171 del Regolamento prevede che le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate;
- l'Autorità di Controllo italiana (Garante per la protezione dei dati personali) ha introdotto con provvedimento del 27 novembre 2008, come successivamente modificato con provvedimento del 25 giugno 2009 ("Provvedimento Amministratori di Sistema"), una serie di obblighi per il Titolare del Trattamento concernenti l'individuazione e la designazione di Persone Autorizzate che svolgono all'interno della FSGT il ruolo di amministratore di sistema, così come definito nel provvedimento richiamato;
- l'osservanza di tali obblighi costituisce una misura di sicurezza che l'organizzazione è tenuta ad osservare e la cui inosservanza può determinare conseguenze sanzionatorie di tipo amministrativo come anche responsabilità civilistica;
- per "Titolare del trattamento" si intende "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali". Nella nostra realtà il "Titolare" è la Fondazione IRCCS San Gerardo dei Tintori (di seguito FSGT) nel suo complesso, che determina finalità e mezzi del trattamento tramite la propria articolazione organizzativa. Titolare del trattamento dei dati è il Direttore Generale, ai sensi dell'art. 16 dello Statuto vigente;
- per "Responsabile del trattamento" si intende "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare";
- La FSGT, oltre i trattamenti in essere in qualità di Titolare, svolge numerose attività di gestione sistemi, reti ed applicazioni complesse a favore di altri Titolari, operando quindi come Responsabile ai sensi dell'art. 28 del Regolamento. In tale veste la FSGT è tenuta ad adottare idonee misure di sicurezza. Tra queste misure non si può comunque prescindere dal rispetto delle misure minime di cui all'Allegato B del D. Lgs. n. 196/2003, anche a seguito della sua formale abrogazione, in quanto si ritiene che qualunque analisi del rischio, almeno nello scenario di FSGT porterebbe comunque alla loro adozione, insieme ad altre;
- La FSGT ha individuato i Designati Privacy, relativamente ai procedimenti afferenti le aree organizzative e le attività di competenza. Essi hanno il compito di individuare e autorizzare per conto della FSGT i dipendenti da autorizzare ai diversi trattamenti;
- la FSGT ha l'obbligo di seguire le prescrizioni della Circolare Agid 2/2017 "*Misure minime di sicurezza ICT per le pubbliche amministrazioni*". In ogni caso queste indicazioni possono essere assunte come "stato dell'arte" per la protezione dei dati personali di cui all'articolo 32 del Regolamento;
- deve essere considerato Amministratore di Sistema chiunque, in maniera non occasionale, si occupa della gestione e della 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, anche accidentalmente, sui Dati Personali;

- la persona in epigrafe, qualora effettui operazioni di trattamento relative alla propria funzione organizzativa e avuto riguardo ai trattamenti effettuati dall'ufficio/area di appartenenza, è stata individuata quale "Persona Autorizzata";
- la Persona Autorizzata ha esaminato e compreso la documentazione aziendale Privacy Policy presente sulla intranet aziendale;
- l'autorizzazione ad operare in qualità di Amministratore di Sistema è individuale e deve indicare in maniera analitica gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato all'Amministratore di Sistema;
- la presente autorizzazione sarà inserita in un elenco aggiornato e reso disponibile nel caso di controlli dell'Autorità di Controllo, e in ogni caso conoscibile ai lavoratori i cui dati personali possono essere trattati dai sistemi informatici della FSGT;
- tutte le operazioni di login, logout e tentativi di login ai sistemi informativi della FSGT effettuati dall'Amministratore di Sistema saranno tracciati in osservanza del Provvedimento del Garante per la protezione dei dati personali sopra richiamato e i relativi log saranno resi inalterabili;
- la FSGT ha l'obbligo di verificare che le misure di sicurezza siano state correttamente messe in opera, con particolare riferimento a quelle sopra citate;
- in taluni casi i tracciamenti potranno essere svolti direttamente dai Titolari per cui la FSGT opera in qualità di Responsabile;
- in taluni casi i tracciamenti potranno essere svolti da altri Titolari presso cui la Persona autorizzata accede;
- i dati personali inerenti all'attività svolta dall'Amministratore di Sistema saranno comunicati/trasmessi a soggetti sopra menzionati e a quelli ulteriori ai quali la normativa in materia di protezione dei dati pro tempore in vigore richieda o renda lecita la comunicazione o la trasmissione;
- l'Amministratore di Sistema potrà esercitare in qualsiasi momento i diritti riconosciuti dagli Artt. 15-22 del Regolamento e dunque, a mero titolo esemplificativo, il diritto di chiedere l'origine dei suoi dati personali, finalità e soggetti a cui i dati sono comunicati. Potrà altresì modificare, cancellare o integrare i dati personali, se ne ha interesse, così come opporsi al trattamento, ma ciò solo in quanto non vi sia contrasto con gli obblighi di legge, inclusi quelli definiti dall'Autorità di Controllo nei provvedimenti sopra richiamati;
- si intende, pertanto, procedere all'individuazione e autorizzazione al trattamento dei dati personali della persona in epigrafe in qualità di amministratore di sistema.

TUTTO CIÒ PREMESSO

Pertanto, la FSGT su delega del Direttore Generale, tramite il Direttore f.f. della S.C. Sistemi Informativi Aziendali autorizza la persona in epigrafe al trattamento dei dati personali in qualità di "Amministratore di Sistema" ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27.11.2008, modificato con provvedimento del 25.6.2009 (di seguito Provvedimento), impartendole i seguenti obblighi, in funzione del ruolo ricoperto, del profilo attribuito in Allegato 1, parte integrante della presente autorizzazione, e nell'ambito delle attività assegnatele per lo svolgimento dei compiti istituzionali:

a) osservare scrupolosamente le regole di utilizzo dei sistemi di tracciamento delle operazioni degli Amministratori di Sistema posti in essere dalla FSGT e in adempimento al citato Provvedimento;
b) segnalare qualsiasi anomalia di funzionamento in merito alla sicurezza, disponibilità e riservatezza dei dati personali al Direttore f.f. della S.C. Sistemi Informativi Aziendali ed al DPO;
c) collaborare alla verifica periodica dell'attività di Amministrazione di Sistema fatta dalla FSGT;
d) osservare le ulteriori istruzioni impartite dalla FSGT per un corretto svolgimento dell'attività di Amministratore di Sistema.

È compito dell'Amministratore di sistema (intendendo con tale termine l'amministratore del sistema operativo, l'amministratore del sistema database, l'amministratore di rete, l'amministratore di sottosistema applicativo complesso o una combinazione delle precedenti funzioni tecniche), in funzione del

Commentato [GDPR CC1]:
Commentato [MMG2R1]:

ruolo ricoperto, del profilo attribuito in Allegato 1, parte integrante della presente autorizzazione, e nell'ambito delle attività assegnatele per lo svolgimento dei compiti istituzionali:

a. attivarsi per tutelare, nei limiti delle proprie competenze e capacità professionali, la protezione dei dati, il buon funzionamento dei sistemi e la continuità operativa dei medesimi;
b. conformarsi alle indicazioni della FSGT su quanto contenuto nel provvedimento del Garante in merito a "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali - 13 ottobre 2008";
c. applicare le regole di gestione dei sistemi medesimi e le misure di sicurezza minime ed idonee individuate o comunque comunicate dalla FSGT;
d. monitorare~~,~~ ove possibile, le risorse di sistema operativo e le basi dati in modo tale da garantire l'efficienza del sistema tecnologico e l'aderenza delle configurazioni ai profili di autorizzazione stabiliti;
e. assegnare e gestire, ove possibile gli identificativi di utente, in modo che siano univoci sul sistema e quindi adeguati ad identificare l'utente che accede ed opera sul sistema;
f. predisporre, ove possibile i meccanismi di corretta gestione delle parole chiave;
g. predisporre, ove non già presenti ed attivati, meccanismi di protezione da accessi indesiderati e meccanismi di protezione nei confronti di attacchi da virus;
h. facilitare il processo di registrazione degli accessi degli amministratori, ove possibile, verificando la predisposizione dei sistemi gestiti a tale attività, evitando ogni operazione che possa inficiare detta raccolta;
i. segnalare i sistemi per i quali non è possibile procedere agli aggiornamenti di sicurezza al DPO, avvisando il Direttore f.f. della S.C. Sistemi Informativi Aziendali;
j. verificare l'applicazione dei criteri di sicurezza previsti dall'Allegato B del Codice Privacy, anche se formalmente abrogato dal D. Lgs. n. 101/2018;
k. individuare, nei limiti del possibile, accessi indebiti ai sistemi; in tale caso attivare immediatamente la procedura di Gestione delle violazioni di dati personali (*Data Breach*);
l. attuare, nell'ambito delle proprie mansioni e degli incarichi ricevuti, tutte le iniziative che contribuiscano a fare in modo che i dati personali oggetto di trattamento vengano trattati in modo lecito e secondo correttezza;
m. assistere eventualmente il Responsabile dell'applicazione nell'individuazione dei dati da salvare, come da punto 18 dell'allegato B, anche se formalmente abrogato dal D.lgs. n. 101/2018, e nella predisposizione dei profili di autorizzazione;
n. evitare, ove non strettamente indispensabile per lo svolgimento delle operazioni tecniche connesse al proprio ruolo, di entrare in contatto, visualizzare, maneggiare o mettere a rischio dati personali;
o. segnalare eventuali usi scorretti o impropri dei sistemi da parte dei tecnici che operano, a vario titolo, sul sistema e sulle sue componenti periferiche e da parte di altre persone autorizzate; attivare nell'evenienza la procedura di gestione delle violazioni di dati personali;
p. richiedere ed utilizzare soltanto i dati necessari alla normale attività lavorativa adottando le necessarie cautele nel caso si tratti di categorie particolari di dati personali e dati personali relativi a condanne penali e reati;
q. custodire i dati oggetto del trattamento in luoghi non accessibili a soggetti non autorizzati;
r. non lasciare incustodito il proprio posto di lavoro prima di aver provveduto alla messa in sicurezza dei dati;
s. non lasciare incustoditi e accessibili a terzi gli strumenti elettronici mentre è in corso una sessione di lavoro;
t. conservare e custodire le chiavi di accesso agli archivi cartacei con la massima cura e non lasciarle incustodite al fine di garantire che l'accesso all'archivio sia consentito solo ai soggetti autorizzati;
u. procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti informatici da lei eventualmente utilizzati una volta terminate le ragioni di consultazione (in particolare gli

archivi cartacei contenenti categorie particolari di dati personali o dati personali relativi a condanne penali o reati dovranno essere chiusi a chiave);

v. custodire e non divulgare la propria password di amministratore per l'accesso agli strumenti elettronici;
w. accertarsi che i terzi abbiano l'autorizzazione per l'uso dei dati richiesti;
x. accertarsi dell'identità di terzi e della loro autorizzazione al ritiro di documentazione in uscita;
y. non fornire telefonicamente per via telematica dati senza specifica autorizzazione e/o identificazione del richiedente;
z. comunicare e/o diffondere solo i dati personali preventivamente autorizzati dal Titolare e/o dal Responsabile;
aa. limitare l'accesso ai dati all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro (comprendendo nell'orario i periodi di reperibilità o altre attività specificatamente autorizzate dal proprio responsabile gerarchico);
bb. nel caso si verifichi un incidente di sicurezza e si sospetti una violazione di dati personali (Data Breach) attivare immediatamente la vigente procedura della FSGT per la gestione delle violazioni;
cc. accertarsi che le informazioni riportate nel Registro dei Trattamenti e relativi ai sistemi/applicazioni di propria competenza siano aggiornate, con particolare riguardo a:

a. Supporti;
b. Misure di sicurezza da applicare;
c. Impatti prevedibili sugli interessati.

L'autorizzato deve eseguire tutte le operazioni di trattamento di dati personali, attenendosi alle istruzioni impartite dal Titolare o dal Responsabile del trattamento. L'autorizzazione è effettuata in relazione a tutte le operazioni di trattamento dei dati, censite nel Registro dei Trattamenti, che siano strettamente necessarie per adempiere ai compiti assegnati in relazione alle attività svolte nell'ambito della Struttura di appartenenza e per le finalità strettamente pertinenti all'esecuzione della prestazione lavorativa.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico ricevuto. Nel caso di cessazione dall'attività lavorativa, Lei non sarà più autorizzato ad effettuare alcun tipo di trattamento sui dati. E' parte integrante delle istruzioni impartite mediante questa autorizzazione al trattamento dei dati personali in qualità di Amministratore di Sistema: la procedura di "DATA BREACH", pubblicata sulla intranet aziendale. Ogni dipendente ha il dovere di prenderne visione e conoscerne il contenuto. Tale documentazione è oggetto di aggiornamenti periodici, pertanto si raccomanda di controllare costantemente la documentazione in materia di privacy e sicurezza sulla intranet aziendale.
Il Direttore f.f. della S.C. Sistemi Informativi Aziendali potrà impartire ulteriori e specifiche istruzioni che saranno allegate alla presente nomina.
Per qualsiasi altra informazione o dubbio è possibile rivolgersi al Direttore f.f. della S.C. Sistemi Informativi Aziendali, nonché al DPO aziendale.

Le ricordiamo infine che il provvedimento del Garante sopracitato, obbliga la FSGT alla "verifica" almeno annuale delle attività svolte dall'Amministratore di Sistema in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalla normativa vigente.

Il rispetto e l'osservanza di quanto contenuto nella presente autorizzazione sono strettamente connessi al ruolo ricoperto all'interno dell'organizzazione della FSGT.

Il non adempimento di quanto previsto nella presente autorizzazione può comportare sanzioni disciplinari.

La presente autorizzazione annulla e sostituisce le precedenti nomine Privacy.

Il Direttore f.f. della S.C. Sistemi Informativi Aziendali
Dr. Davide Pietro Tomè

Persona Autorizzata in qualità di Amministratore di Sistema:
Per presa visione

NOME E COGNOME
Matricola

Monza,

* * *

INFORMATIVA RILASCIATA AI SENSI DELL'ART. 13 DEL REGOLAMENTO UE 2016/679

Fatto salvo quanto già indicato nell'informativa rilasciata in sede di assunzione, La informiamo che, ai sensi dell'art. 4.5 del Provvedimento Amministratori di Sistema, le sue attività, compiute in qualità di Amministratore di Sistema, devono essere registrate dalla FSGT, come indicato nell'incarico, in ottemperanza alla normativa vigente, anche con particolare riferimento alle tutele di cui all'art. 4 della L. n. 300/70 (Statuto dei Lavoratori).

Riportiamo di seguito il testo del citato articolo 4.5 del Provvedimento Amministratori di Sistema:
"*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 di verifica 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.*"

I dati identificativi e i dati sugli accessi sopra citati saranno dunque trattati dalla FSGT per finalità di controllo sulla legittimità degli accessi per le esclusive finalità indicate nel succitato Provvedimento, in particolare al fine di verificare anomalie nella frequenza degli accessi e nelle loro modalità. L'analisi dei log può essere compresa tra i criteri di valutazione dell'operato degli Amministratori di Sistema. Tali Trattamenti sono obbligatori e non facoltativi, non potendo essere rifiutati da lei se non cambiando funzione e consistendo in adempimento di obblighi normativi, e avverranno solo con strumenti elettronici. Il tempo del Trattamento sarà di sei mesi, pertanto allo scadere di tale periodo i dati in questione saranno via via cancellati. Lei ha diritto di chiedere alla FSGT, in qualunque momento, l'accesso ai suoi dati personali, la rettifica o la cancellazione degli stessi o di opporsi al loro Trattamento, ha diritto di richiedere la limitazione del Trattamento nei casi previsti dall'art. 18 del Regolamento UE 2016/679, nonché di ottenere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati che la riguardano, nei casi previsti dall'art. 20 del Regolamento.

Le richieste vanno rivolte per iscritto alla FSGT al seguente indirizzo: Via Pergolesi n. 33, Monza (MB) email: protocollo@irccs-sangerardo.it ovvero al DPO (Data Protection Officer) al seguente indirizzo: dpo@irccs-sangerardo.it.

In ogni caso, ha sempre diritto di proporre reclamo all'Autorità di Controllo competente (Garante per la Protezione dei Dati Personali), ai sensi dell'art. 77 del Regolamento, qualora ritenga che il Trattamento dei loro Dati Personali sia contrario alla normativa vigente.

Allegato 1: Amministratore di Sistema - Ambiti di operatività.

La sua autorizzazione comprende i seguenti profili e piattaforme:

Profilo	**Tecnologia**	**Autorizzato**
Sistemista	Gestione sistemi, application server e storage	SI/NO
Apparati di rete e sicurezza perimetrali	Networking (Gestione infrastruttura di Rete)	SI/NO
Gestione Database	Database (Gestione base dati)	SI/NO
Cybersecurity	Cybersecurity (Gestione e monitoraggio strumenti di sicurezza informatica)	SI/NO
Gestione Back up	Back up e Restore	SI/NO
Gestione Client e stampanti	Gestione Client, stampanti, fonia e VDC	SI/NO
Infrastruttura tecnologica	Gestione e monitoraggio Infrastruttura Data Center	SI/NO
Assistenza	Assistenza tecnica applicazioni	SI/NO
Sviluppatore	Progettista e Sviluppatore di applicazioni	SI/NO
Tester	Progettista ed esecutore di test per applicazioni	SI/NO

Tutte le risorse in possesso o meno di un profilo specifico

Tali istruzioni valgono per tutte le figure che non rientrano pienamente nei profili specifici di seguito individuati e nella misura in cui risultano concretamente applicabili al profilo indicato.

Ella dovrà attenersi pertanto alle seguenti istruzioni, in funzione del ruolo ricoperto e nell'ambito delle attività assegnate per lo svolgimento del suo lavoro:

1. Installare unicamente software autorizzati, ovvero:
    A. Utili allo svolgimento della propria attività lavorativa;
    B. Distribuiti ufficialmente dalla FSGT che ne detengono i diritti e che producano aggiornamenti di sicurezza almeno una volta l'anno;
    C. Che non siano comprese nell'elenco delle tipologie di SW non autorizzato (Cfr. Blacklist);
    D. Su esplicita indicazione del Titolare, del Responsabile, del proprio responsabile gerarchico;
    E. Nei limiti delle licenze in possesso della FSGT:
        I. Di cui si è certi che la FSGT abbia la relativa licenza nella configurazione e nelle quantità idonee oppure
        II. Software che non necessiti di licenza a pagamento per uso aziendale.
2. Chi installa e gestisce (amministra) un SW (applicativo o di ambiente) si prende la responsabilità di seguire costantemente gli aggiornamenti (vulnerabilità, fine del supporto) del SW installato;
3. Per i Software amministrati, monitorare l'emissione di aggiornamenti (vulnerabilità, fine del supporto e fine vita) e gli annunci di fine vita dei prodotti gestiti, tramite la sottoscrizione dei servizi di notifica applicabili, e comunque almeno trimestralmente verificare la disponibilità di aggiornamenti e la fine vita dei prodotti.
4. Segnalare la disponibilità degli aggiornamenti (vulnerabilità, fine del supporto e fine vita) al DPO per concordare un piano di aggiornamento nei limiti temporali previsti mettendo a conoscenza, a proprio giudizio, il Direttore f.f. della S.C. Sistemi Informativi Aziendali;
5. Rimuovere i software amministrati non più utili e che non rispettano più le condizioni per l'installazione;
6. Monitorare, ove possibile, il corretto funzionamento dei servizi erogati tramite la verifica dei log e dei messaggi prodotti dal sistema/applicazioni e dei sistemi di diagnostica applicabili;

7. Segnalare eventuali problematiche dei sistemi o situazioni anomale al Direttore f.f. della S.C. Sistemi Informativi Aziendali;
8. Intervenire prontamente in situazioni di emergenza o in caso di manutenzione ordinaria o straordinaria, seguendo, per quanto necessario, gli interventi relativi;
9. Cooperare all'installazione dei sistemi e al monitoraggio della loro continuità operativa e della fruibilità continuativa dei servizi da parte degli utenti, alla verifica delle funzionalità delle interfacce e attivare/disattivare i singoli processi software per garantire detta continuità di servizio in relazione agli specifici contesti operativi;
10. Effettuare operazioni di tuning dei parametri di configurazione del sistema/applicazione gestito applicando il principio del privilegio minimo e della minimizzazione dei servizi erogati, per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità di gestione ed il mantenimento nel tempo delle funzioni;
11. Provvedere, su richiesta del Titolare o del Responsabile, alla gestione delle credenziali di autenticazione e alla modifica o disattivazione delle utenze (ad es. User ID e PW) su cui dovesse risultare qualche problema;
12. Inviare ai soggetti deputati all'autorizzazione delle persone autorizzate, secondo quanto definito nelle procedure aziendali, l'elenco degli utenti del sistema/applicazione e delle relative autorizzazioni per consentire la verifica dell'autorizzazione;
13. Definire e configurare gli utenti, gli account che devono operare sul sistema ed i parametri relativi, attribuendo loro il profilo di autorizzazione indicato dai soggetti deputati all'autorizzazione delle persone autorizzate;
14. Custodire tutti i supporti di memorizzazione contenenti dati personali sottochiave;
15. Non lasciare mai la propria postazione di lavoro incustodita e, in caso di allontanamento, provvedere a bloccare la postazione prima di allontanarsi dal proprio posto di lavoro;
16. Segnalare eventuali interventi ritenuti necessari per migliorare gli aspetti legati alla sicurezza dei dati, al trattamento e alla loro conservazione al Direttore f.f. della S.C. Sistemi Informativi Aziendali e al DPO. Tali migliorie verranno vagliate dalle strutture tecniche e comunicate al Titolare/Responsabile;
17. Segnalare al DPO mettendo a conoscenza il Direttore f.f. della S.C. Sistemi Informativi Aziendali, tutti i casi conosciuti di non rispetto delle misure minime di sicurezza di cui Allegato B del Codice Privacy, anche se formalmente abrogato dal D.lgs. n.101/2018 e delle misure necessarie (Provvedimenti del Garante), delle normative aziendali attinenti, nonché della presente disposizione.

Inoltre, Lei è altresì autorizzato all'amministrazione della postazione di lavoro personale, attenendosi alle seguenti istruzioni:

1. Installare unicamente software autorizzati, ovvero:
    A. Utili allo svolgimento della propria attività lavorativa;
    B. Distribuiti ufficialmente dalla FSGT che ne detengono i diritti e che producano aggiornamenti di sicurezza almeno una volta l'anno;
    C. Che non siano comprese nell'elenco delle tipologie di SW non autorizzato (Cfr. Blacklist);
    D. Su esplicita indicazione del Titolare, del Responsabile, del proprio responsabile gerarchico;
    E. Nei limiti delle licenze in possesso della FSGT:
        I. Di cui si è certi che la FSGT abbia la relativa licenza nella configurazione e nelle quantità idonee oppure
        II. Software che non necessiti di licenza a pagamento per uso aziendale.
2. Chi installa e gestisce (amministra) un SW (applicativo o di ambiente) si prende la responsabilità di seguire costantemente gli aggiornamenti (vulnerabilità, fine del supporto) del SW installato;
3. Rimuovere i software non più utili e che non rispettano più le condizioni per l'installazione;
4. Applicare in ogni caso le misure di sicurezza minime e necessarie definite dalla normativa di settore;
5. Applicare in ogni caso le disposizioni aziendali in materia;
6. L'attività lavorativa con la propria postazione di lavoro deve essere svolta con la stessa attestata al dominio Windows di riferimento.

Profilo Gestione Database

1. Intervenire ogni qualvolta venga evidenziato un malfunzionamento, un guasto o una anomalia funzionale sui sistemi e sulle basi dati installati sui medesimi, sui servizi erogati per diagnosticare il problema e ripristinare il corretto funzionamento dei sistemi, coinvolgendo per quanto necessario e possibile gli altri amministratori, cercando di rispettare i livelli di servizio;

Profilo Analista/Progettista

1. Seguire i principi di “Privacy fin dalla progettazione” e “Privacy per impostazione predefinita”;
2. Se richiesto, partecipare alla Valutazione d'impatto sulla protezione dei dati ed in ogni caso applicare i requisiti prescritti dalla documentazione del processo di valutazione;
3. Tener conto dei requisiti collegati all’esercizio dei diritti dell’interessato (Accesso, Rettifica, Cancellazione, Limitazione) nel corso della progettazione;
4. Rispettare il principio di minimizzazione del trattamento nella progettazione del sistema, con particolare, riferimento alla progettazione della base dati;
5. Determinare le funzionalità di supporto per la gestione del periodo di conservazione dei dati in ossequio al principio di minimizzazione del trattamento;
6. Individuare, in cooperazione con le strutture tecniche aziendali (Sviluppatori, Sistemisti, Tester, etc.) e il DPO, i requisiti di Sicurezza nell’ambito dell’attività di definizione dei requisiti;
7. Definire le tipologie di dati e di configurazioni da salvare, le modalità di salvataggio (back-up) e le eventuali modifiche e darne comunicazione alla specifica struttura di gestione back-up;
8. Partecipare alla progettazione del sistema e delle sue evoluzioni assicurando il rispetto delle istruzioni del Titolare, delle misure minime e necessarie per garantire il livello richiesto di disponibilità, integrità e riservatezza dei dati ed applicando i seguenti principi di sicurezza (Rif. Security by Design Principles - OWASP™ Foundation https://www.owasp.org/index.php/Security_by_Design_Principles):
    I. Responsabilizzazione
    II. Privilegio Minimo
    III. Minimizzazione della superficie di attacco
    IV. Separazione dei doveri per le operazioni critiche
9. Analizzare i requisiti di sicurezza, verificandone la chiarezza e la fattibilità;
10. Individuare le componenti atte ad effettuare le operazioni di verifica sui dati in input ai moduli di competenza (“sanitization”) e utilizzarle in modo sistematico durante lo sviluppo;
11. Utilizzare le indicazioni delle migliori pratiche (es. NIST), algoritmi adeguati (vedi, ad esempio, indicazioni di ECRYPT e FIPS-140) nella progettazione di procedure crittografiche;

12. Chiedere un parere al Direttore f.f. della S.C. Sistemi Informativi Aziendali durante la progettazione di operazioni crittografiche;
13. Segnalare la disponibilità degli aggiornamenti (vulnerabilità, fine del supporto e fine vita) al DPO per concordare un piano di aggiornamento nei limiti temporali previsti mettendo a conoscenza, a proprio giudizio, il Direttore f.f. della S.C. Sistemi Informativi Aziendali;
14. Se gestisce attività di delivery e deploy di nuove release di Software applicativo, deve richiedere l'esecuzione dei test di non regressione delle applicazioni;
15. Se gestisce attività di delivery e deploy deve richiedere un adeguato test funzionale, di carico e di sicurezza, a seconda delle proprie competenze, utilizzando dati personali palesemente fittizi;
16. Sottoporre all'approvazione del DPO la necessità di effettuare test con dati di esercizio. In tali casi adottare le stesse cautele utilizzate in esercizio per le configurazioni di sistema ed applicativi;
17. Controllare il corretto funzionamento dell'applicazione, verificando lo stato delle risorse HW e SW.

Profilo Tester

1. Progettare i test, facendo uso qualora ritenuto opportuno, di dati verosimili ma non relativi a persone identificabili. Nel caso di utilizzo di dati reali chiedere autorizzazione preventiva al DPO e
2. Effettuare test:
   a. funzionali e di carico in base ai requisiti di prodotto, includendo anche le verifiche sulle funzionalità per la gestione dei diritti degli interessati di cui agli Artt. 12-22 del GDPR;
   b. di sicurezza in base ai requisiti del prodotto e alle indicazioni del Direttore f.f. della S.C. Sistemi Informativi Aziendali;
   c. di usabilità;
   d. di non regressione a seguito di installazione di nuove versioni del SW applicativo e di base.
3. Eseguire i test come pianificato e predisporre il relativo rapporto di test;
4. Sottoporre all'approvazione del DPO la necessità di effettuare test con dati di esercizio. In tali casi adottare le stesse cautele utilizzate in esercizio per le configurazioni di sistema ed applicative.

Profilo Progettista/Sviluppatore

1. Seguire i principi di "Privacy fin dalla progettazione" e "Privacy per impostazione predefinita";
2. Progettare le componenti del SW tenendo conto delle migliori pratiche:
   a. Isolamento delle componenti;
   b. Verifica degli input;
   c. Utilizzo di moduli specializzati per i controlli di sicurezza.
3. Tener conto dei requisiti collegati all'esercizio dei diritti dell'interessato (Accesso, Rettifica, Cancellazione, Limitazione) nel corso della progettazione;
4. Sviluppare le funzionalità di supporto per la gestione del periodo di conservazione dei dati in ossequio al principio di minimizzazione del trattamento. Cooperare con gli analisti e le altre strutture tecniche aziendali (Sistemisti, Tester, ecc) e DPO, nella definizione dei requisiti sulla Sicurezza. Partecipare alla progettazione del sistema e delle sue evoluzioni assicurando il rispetto delle istruzioni del Titolare, delle misure minime e necessarie per garantire il livello richiesto di disponibilità, integrità e riservatezza dei dati ed applicando i seguenti principi di sicurezza (rif. Security by Design Principles - OWASP™ Foundation):
5. Nelle fasi di progettazione e sviluppo, individuare le componenti atte ad effettuare le operazioni di verifica sui dati in input ai moduli di competenza ("sanitization") e utilizzarle in modo sistematico durante lo sviluppo;
6. Definire le tipologie di dati e di configurazioni da salvare, le modalità di salvataggio (back-up) e le eventuali modifiche e darne comunicazione alla specifica struttura di gestione back-up;
7. Utilizzare le indicazioni delle migliori pratiche (es. NIST), algoritmi adeguati (vedi ad esempio indicazioni di ECRYPT e FIPS-140) nella progettazione di procedure crittografiche;
8. Chiedere un parere al Direttore f.f. della S.C. Sistemi Informativi Aziendali, durante la progettazione di operazioni crittografiche;
9. Utilizzare solo strumenti di sviluppo e ambienti che abbiano un orizzonte di vita utile (prima di essere in stato end of life) congruo alle specifiche di progetto. Qualora la durata del supporto sia inferiore ai 18 mesi occorre chiedere autorizzazione al DPO;

10. Comunicare al Direttore f.f. della S.C. Sistemi Informativi Aziendali l'approssimarsi della scadenza del supporto o il fine vita dei SW utilizzati negli sviluppi con almeno 18 mesi di preavviso;
11. Tracciare lo sviluppo dei requisiti con particolare attenzione alle funzioni di sicurezza;
12. Utilizzare le funzioni crittografiche già specificate e nel caso di scelta di algoritmi privilegiare l'utilizzo di algoritmi standard, salvo deroghe approvate dal Direttore f.f. della S.C. Sistemi Informativi Aziendali,

Profilo Sistemista (Gestione sistemi, application server e storage)

1. Seguire i principi di "Privacy fin dalla progettazione" e "Privacy per impostazione predefinita";
2. Se richiesto, partecipare alla Valutazione d'impatto sulla protezione dei dati ed in ogni caso applicare i requisiti prescritti dalla documentazione del processo di valutazione;
3. Tener conto dei requisiti collegati all'esercizio dei diritti dell'interessato (Accesso, Rettifica, Cancellazione, Limitazione) nel corso della progettazione;
4. Rispettare il principio di minimizzazione del trattamento nella progettazione del sistema, con particolare, riferimento alla progettazione della base dati;
5. Determinare le funzionalità di supporto per la gestione del periodo di conservazione dei dati in ossequio al principio di minimizzazione del trattamento;
6. Definire le tipologie di dati e di configurazioni da salvare, le modalità di salvataggio (back-up) e le eventuali modifiche e darne comunicazione alla specifica struttura di gestione back-up;
7. Partecipare alla progettazione del sistema e delle sue evoluzioni assicurando il rispetto delle istruzioni del Titolare, delle misure minime e necessarie per garantire il livello richiesto di disponibilità, integrità e riservatezza dei dati ed applicando i seguenti principi di sicurezza:
    I. Responsabilizzazione
    II. Privilegio Minimo
    III. Minimizzazione della superficie di attacco
    IV. Separazione dei doveri per le operazioni critiche
8. Effettuare operazioni di tuning dei parametri di configurazione del sistema gestito (HW e sistema operativo e relativo middleware per i profili "Unix", "Linux", "Windows", "Gestione Client" e "Apparati di rete e sicurezza perimetrale", il database server e i relativi strumenti di supporto per i profili "Mysql", "Postgress", "Oracle", "Sqlserver", il

software di gestione dello storage e degli apparati di rete FC per il profilo "Tecnologie di virtualizzazione dello Storage" , l'ipervisore e i relativi strumenti di contorno per quanto riguarda il profilo "VmWare ed altre tecnologie di virtualizzazione", il sistema di controllo dell'antivirus per il profilo "Gestione antivirus", la piattaforma di gestione dei backup per il profilo "Gestione del backup", il sistema di monitoraggio per il profilo "Monitoraggio sistemi e reti", i sistemi di gestione e controllo degli apparati di alimentazione e condizionamento per il relativo profilo, il sistema di gestione dei log per l'omologo profilo) applicando il principio del privilegio minimo e della minimizzazione dei servizi erogati, per garantire il migliore equilibrio fra le prestazioni erogate, la sicurezza operativa, la complessità di gestione ed il mantenimento nel tempo delle funzioni;

9. Controllare il corretto funzionamento dei sistemi, verificando lo stato delle risorse HW (cpu, ram, sottosistema di storage, etc) e delle risorse SW;
10. Configurare i sistemi in modo che la parte riservata delle credenziali e i dati sanitari siano sempre gestiti tramite tecniche crittografiche rispondenti allo standard FIPS 140;
11. Verificare almeno una volta l'anno l'efficacia e l'efficienza delle procedure di backup;
12. Predisporre e controllare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi, sulla base delle altre istruzioni aziendali; tali registrazioni (access log) devono avere caratteristiche di completezza e possibilità di verifica adeguate allo scopo per cui sono richieste;
13. Attuare operazioni sui file dei file system e sui file system stessi (delle strutture interne del DB per i relativi profili) (installazione, add, move, change, copy, ecc.) per soli scopi di manutenzione del sistema, indagine diagnostica, installazione di applicazioni o di tool diagnostici o gestionali, tuning, salvataggio, anche temporaneo, di dati e configurazioni, ripristino di condizioni normali di funzionamento;
14. Controllare il corretto funzionamento dell'applicazione, verificando lo stato delle risorse HW e SW;
15. Assicurare che prima della dismissione del dispositivo tutte le informazioni riservate e tutti i dati personali siano state cancellate in modo permanente;
16. Concorrere per la parte di propria competenza all'amministrazione e gestione del servizio Cloud.

Inoltre, gli Amministratori di Sistema con profilo di autorizzazione di "Gestione caselle postali" sono autorizzati ad operare sulle caselle postali con particolare riferimento allo svolgimento delle seguenti attività:

1. Creazione, attribuzione diritti agli utenti delle caselle postali personali e logiche di funzione;
2. Gestione delle quote di spazio per le caselle postali;
3. Configurazione dei parametri delle caselle postali.

Profilo CyberSecurity

1. Individuare i requisiti di Sicurezza nel rispetto della normativa vigente nell'ambito dell'attività di definizione dei requisiti di progetto;
2. Partecipare alla progettazione del sistema e delle sue evoluzioni assicurando il rispetto delle istruzioni del Titolare, delle misure minime e necessarie per garantire il livello richiesto di disponibilità, integrità e riservatezza dei dati ed applicando i seguenti principi di sicurezza:
    i. Responsabilizzazione;
    ii. Privilegio Minimo;
    iii. Minimizzazione della superficie di attacco;
    iv. Separazione dei doveri per le operazioni critiche.
3. Predisporre e controllare sistemi idonei alla registrazione centralizzata dei log dei sistemi, degli apparati e degli accessi logici, sulla base della normativa vigente e dei requisiti di sicurezza; tali registrazioni devono avere caratteristiche di completezza e possibilità di verifica adeguate allo scopo per cui sono richieste;
4. Verificare periodicamente la sicurezza di tutta l'infrastruttura informatica in gestione e verificare l'uso di configurazioni standard sicure per la protezione dei sistemi;
5. Eseguire regolari scansioni per la ricerca di vulnerabilità sia dei sistemi che delle applicazioni, anche in modalità privilegiata, localmente o da remoto;
6. Predisporre strumenti atti a rilevare la presenza e bloccare l'esecuzione di software malevolo o non ammesso sui sistemi aziendali;
7. Assicurare che gli strumenti utilizzati siano aggiornati ed in grado di rilevare tutte le più significative vulnerabilità di sicurezza;
8. Monitorare e Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali;
9. Registrarsi a uno o più servizi che siano in grado di fornire informazioni sulle nuove minacce e vulnerabilità di sicurezza;
10. Verificare che vengano implementante opportune misure di sicurezza e le vulnerabilità segnalate vengano risolte, mitigate o documentate accettando un ragionevole rischio;
11. Implementare ed assicurare la corretta funzionalità di una procedura di gestione degli incidenti di sicurezza;
12. Concorrere per la parte di propria competenza all'amministrazione e gestione del servizio Cloud.

Gli Amministratori di Sistema con profilo di autorizzazione di Gestione back-up sono autorizzati ad operare sui sistemi utilizzati per la produzione di tutti i back-up, con particolare riferimento allo svolgimento delle seguenti attività (Back up e Restore):

1. Sorvegliare il corretto funzionamento dei sistemi che sono utilizzati per la produzione dei back-up;
2. Predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;
3. Verificare giornalmente l'esito positivo delle procedure di back-up;
4. Verificare l'esito positivo degli eventuali restore richiesti;
5. Provvedere all'archiviazione delle copie su nastro, come da procedura;
6. Monitorare, tramite gli appositi strumenti aziendali, lo stato dei servizi, della rete e dei server;
7. Verificare il corretto funzionamento delle applicazioni e dei siti, anche accedendo alle medesime;
8. Raccogliere le segnalazioni degli utenti, effettuare una prima diagnosi;
9. Attivare gli specialisti a fronte dell'insorgenza di problemi;
10. Ricevere i visitatori secondo le indicazioni contenute nel documento aziendale in proposito;
11. Concorrere per la parte di propria competenza all'amministrazione e gestione del servizio Cloud.

Gli Amministratori di Sistema con profilo di autorizzazione di "Apparati di rete e sicurezza perimetrale" (Networking – Gestione Infrastruttura di Rete)

1. Provvedere alla segmentazione delle reti in funzione delle utenze dei servizi;
2. Mantenere l'isolamento dei segmenti, collocando tra essi solo apparati di sicurezza;
3. Fornire periodicamente al Titolare o Responsabile e al DPO i seguenti elenchi:
    I. Elenco delle LAN con indicazione della tipologia di utenza
    II. Elenco degli apparati di rete
    III. Elenco degli utenti abilitati sui singoli apparati;
4. Concorrere per la parte di propria competenza all'amministrazione e gestione del servizio Cloud.

Gli Amministratori di Sistema con profilo di autorizzazione di "Infrastruttura tecnologica (alimentazione elettrica, condizionamento)" sono autorizzati a richiedere e coordinare gli interventi sugli apparati di alimentazione, sui cablaggi, sul sistema di condizionamento, dei manutentori esterni. (Gestione e monitoraggio Infrastruttura e Data Center) In particolare:

1. Verificare che le manutenzioni programmate e i controlli periodici vengano effettuati alle scadenze prestabilite;
2. Monitorare il funzionamento tramite gli strumenti di supervisione;
3. Verificare che il carico elettrico di nuovi apparati siano compatibili con i parametri di impianto;
4. Attivare prontamente le ditte esterne in caso di malfunzionamenti;
5. Verificare che gli interventi siano stati effettuati come richiesto;
6. Concorrere per la parte di propria competenza all'amministrazione e gestione del servizio Cloud.

Gli Amministratori di sistema con profilo di autorizzazione "Windows" sono inoltre responsabili dell'aggiornamento automatico dei software installati sulle postazioni utente per quei software la cui gestione è stata centralizzata.

Gli Amministratori di Sistema con profilo di autorizzazione di "Gestione Client e stampanti" sono autorizzati ad operare sui client Windows con particolare riferimento allo svolgimento delle seguenti attività:

1. Assistenza tecnica ogni qualvolta venga evidenziato un malfunzionamento, un guasto o una anomalia sulle postazioni di lavoro (hardware, sistema operativo, middleware e prodotti installati) per diagnosticare il problema e ripristinare il corretto funzionamento, coinvolgendo per quanto necessario e possibile gli altri amministratori e i fornitori terzi;
2. Supporto all'intervento svolto dagli altri amministratori nel caso venga evidenziato un malfunzionamento, un guasto, una anomalia sulla infrastruttura tecnologica (server e reti) o sulle applicazioni;
3. Installazione di nuove postazioni di lavoro, reinstallazione di postazioni già attive a seguito di malfunzionamenti;
4. Installazione/reinstallazione dei pacchetti software standard e delle procedure applicative;
5. Modifiche ad una postazione di lavoro a seguito della configurazione di periferiche aggiuntive e del relativo software (ad esempio: stampanti, scanner, lettori …);
6. Segnalazione di eventuali problematiche o di situazioni anomale dei client al proprio responsabile.