Proposta	n. PDEL-2024-43 del 09/04/2024
Deliberazione del Direttore Generale	n. DEL-2024-39 del 09/04/2024
Oggetto	Servizio Sistemi Informativi e Innovazione Digitale. Approvazione del "Disciplinare tecnico per Amministratori di Sistema" di Arpae Emilia-Romagna e disposizioni in merito alla nomina degli stessi.
Dirigente proponente	Servizio Sistemi Informativi E Innovazione Digitale - Cicognani Matteo
Responsabile del procedimento	Affaticati Alessandro

Questo giorno *09/04/2024* il Direttore Generale, Dott. Bortone Giuseppe, delibera quanto segue.

VISTI:

- il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, “Regolamento generale sulla protezione dei dati”, conosciuto anche come GDPR;
- il D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali” (nel seguito anche Codice) come modificato ed integrato dal D.Lgs. 10 marzo 2023, n. 24;
- il "Provvedimento sulle Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del Garante per la protezione dei dati personali in data 27 novembre 2008;
- il "Provvedimento 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 Garante per la protezione dei dati personali in data 25 giugno 2009;

RICHIAMATA:

- la D.D.G. n. 41 del 26/04/2023 che individua nella figura del Direttore Generale dell’Agenzia il Titolare del trattamento dei dati personali (ovvero del soggetto a cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso quello della sicurezza), e nella figura dei Responsabili delle strutture i soggetti attuatori degli adempimenti previsti dalla normativa in materia di protezione dei dati personali;

PREMESSO:

- che la tutela del patrimonio delle informazioni riveste importanza strategica per Arpae, oltre che essere soggetta a precisi vincoli di legge imposti dal Codice;
- che il sistema informativo regionale di Arpae è costituito da un’infrastruttura tecnologica molto articolata e complessa, formata da sistemi di elaborazione dati di varia natura, basi dati, apparati di rete e di sicurezza, sistemi software anche complessi per cui si rende necessario assicurare maggiore organicità e coordinamento all’attività del personale incaricato di gestire e amministrare i sistemi informatici e telematici;
- che la gestione tecnica e la manutenzione degli impianti di elaborazione o di sue componenti comportano in molti casi attività che vanno considerate a tutti gli effetti alla stregua di trattamenti di dati personali;

RILEVATA:

- la necessità di promuovere l’adozione di specifiche cautele nello svolgimento delle mansioni

svolte dagli amministratori di sistema, unitamente ad accorgimenti e misure tecniche, procedurali ed organizzative volte ad agevolare le attività di verifica da parte del titolare o dei responsabili da esso designati;

- la necessità di informare dell'esistenza di tali figure o di ruoli analoghi all'interno dell'Ente, svolti in relazione anche a talune fasi dei trattamenti di dati personali;
- la necessità di rendere nota l'identità degli Amministratori di Sistema qualora la loro attività riguardi anche indirettamente servizi o sistemi che permettono il trattamento di informazioni di carattere personale di lavoratori;

CONSIDERATO:

- che in base al Regolamento UE n. 679/2016 occorre specificare meglio responsabilità e competenze, in ragione del principio di accountability;

DATO ATTO:

- che ai sensi dell'art. 4, n. 7) del suddetto Regolamento UE n. 679/2016 e della sopra richiamata D.D.G. n. 41/2023 il Direttore Generale di Arpae è Titolare dei trattamenti sui dati personali che effettua per lo svolgimento delle proprie funzioni istituzionali, in quanto gli competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e ad ai mezzi, compresi gli strumenti utilizzati;
- che alcuni dei trattamenti di cui Arpae è Titolare sono affidati a soggetti, società e/o figure professionali che, in taluni casi, oltre a svolgere funzioni di Responsabile esterno dei trattamenti per il Titolare, svolgono anche funzioni di gestione e manutenzione di impianti di elaborazione o di sue componenti, intesi quali: sistemi e servizi di rete, apparati di sicurezza, basi di dati, supporto ai sistemi informativi di varia tipologia;

SPECIFICATO:

- che l'art. 2-quaterdecies del D.Lgs. 196/2003 stabilisce che il Titolare possa prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la propria autorità;
- che il Provvedimento del Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" del 27/11/2008 e successive modifiche - che tuttora regola la materia - richiede che si proceda alla designazione individuale degli Amministratori di Sistema, con indicazione analitica degli ambiti di operatività consentiti;

CONSIDERATO:

- che, quando il ruolo di Amministratore di Sistema viene affidato in outsourcing ad un soggetto

esterno, questo dovrà considerarsi altresì un responsabile del trattamento. In considerazione di ciò, il titolare dovrà vincolare l'amministratore di sistema con un contratto scritto;

- che la nomina avrà decorrenza limitata alla durata del contratto sottoscritto;

DATO ATTO:

- che nel caso di servizi di amministrazione di sistema affidati in outsourcing il Titolare o il Responsabile esterno del trattamento devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema;

RITENUTO:

- opportuno approvare uno schema di Disciplinare tecnico di riferimento per gli Amministratori di Sistema, allegato sub A) al presente atto quale parte integrante e sostanziale, al fine di definire le procedure e le regole tecniche ed organizzative cui gli Amministratori di Sistema di Arpae devono attenersi nell'esercizio delle funzioni assegnate;
- di delegare il Responsabile del Servizio Sistemi Informativi e Innovazione Digitale ad individuare gli Amministratori di Sistema e a mantenere aggiornato il relativo registro digitale, con gli ambiti di operatività degli stessi in funzione dei profili autorizzativi assegnati;

DATO ATTO:

- che l'operato degli Amministratori di Sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare o dei Responsabili esterni del trattamento al fine di controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;

SU PROPOSTA:

- del Responsabile del Servizio Sistemi Informativi e Innovazione Digitale, Dott. Matteo Cicognani, il quale ha espresso parere favorevole in merito alla regolarità amministrativa del presente atto;

DATO ATTO:

- del parere favorevole dal Direttore Amministrativo, Dott.ssa Lia Manaresi, e dal Direttore Tecnico, Dott. Eriberto de' Munari, espresso ai sensi della L.R. n. 44/95;
- che il Responsabile del procedimento, ai sensi della L. n. 241/90, è il Dott. Alessandro Affaticati del Servizio Sistemi Informativi e Innovazione Digitale;

DELIBERA

1. di approvare il “Disciplinare tecnico per Amministratori di Sistema” di Arpae Emilia-Romagna, allegato sub A) al presente atto quale parte integrante e sostanziale;
2. di delegare il Responsabile del Servizio Sistemi Informativi e Innovazione digitale di Arpae ad individuare gli Amministratori di Sistema e a mantenere aggiornato il relativo registro digitale, con gli ambiti di operatività degli stessi in funzione dei profili autorizzativi assegnati.

PARERE: FAVOREVOLE

IL DIRETTORE AMMINISTRATIVO

Dott.ssa Manaresi Lia

PARERE: FAVOREVOLE

IL DIRETTORE TECNICO

Dott. de’ Munari Eriberto

IL DIRETTORE GENERALE

Dott. Bortone Giuseppe

Si dichiara che sono parte integrante del presente provvedimento gli allegati riportati a seguire [1], come file separati dal testo del provvedimento sopra riportato:

1 L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento

Allegato A

Disciplinare tecnico
per Amministratori di Sistema

ARPAE
Agenzia per la Prevenzione, l'Ambiente e l'Energia dell'Emilia-Romagna

Sommario

1 Premessa e definizione
2 Ambito d’applicazione
3 Designazione degli Amministratori di Sistema
3.1 Amministratore di Sistema “interno”
3.2 Amministratore di Sistema "esterno"
3.2.1 Amministratori di Sistema designati dall'ente
3.2.2 Amministratori di Sistema designati dal fornitore
3.3 Amministratori di Sistema della "dotazione informatica"
4 Registro digitale degli Amministratori di Sistema
5 Verifica delle attività degli Amministratori di Sistema
6 Uso appropriato dei privilegi di Amministratori di Sistema e compiti assegnati
6.1 Sospensione dei privilegi

1 Premessa e definizione

Il presente disciplinare tecnico descrive le procedure per la corretta gestione degli amministratori di sistema e le regole tecniche ed organizzative cui gli stessi si attengono nell'esercizio delle funzioni assegnate.

Ai fini del presente Disciplinare, per **«Amministratori di Sistema»** sono intese le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (quali ad esempio, gli amministratori di dominio e di server), nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi[1].

2 Ambito d'applicazione

Il presente disciplinare si applica a tutti gli Amministratori di Sistema che operano sui servizi sistemistici, infrastrutturali e applicativi che afferiscono al sistema informatico regionale di Arpae.

3 Procedura di designazione degli amministratori di sistema

Ai fini della designazione sono previste due tipologie di Amministratori di Sistema, ovvero "interni" ed "esterni", come meglio specificato di seguito.

Il Servizio Sistemi Informativi e Innovazione Digitale (SSID) di Arpae nomina gli amministratori interni di sistema e designa gli amministratori di sistema esterni i cui nominativi sono comunicati formalmente dalle Aziende che hanno sottoscritto un contratto con l'ente che prevede la presenza di figure di comprovata capacità che debbano accedere, per l'assolvimento degli obblighi derivati dal contratto stesso, ai sistemi informativi di Arpae.

3.1 Amministratore di Sistema "interno"

Per Amministratore di Sistema "interno" si intende il personale alle dirette dipendenze dell'Ente a cui sono attribuite funzioni di amministratore di sistema.

L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto che si intende designare, il quale deve, quindi, fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza (cfr. par. 2 lett. a) del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008).

---

[1] Definizione da provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" pubblicato sulla G.U. n. 300 del 24-12-2008.

La valutazione è effettuata dal Responsabile del SSID, struttura cui il soggetto è di norma assegnato.

A ciascuna singola persona fisica cui siano attribuite funzioni di amministratore di sistema sono assegnati specifici ambiti di operatività in funzione dei privilegi assegnati.

3.2 Amministratori di Sistema "esterni"

3.2.1 Amministratori di Sistema designati dall'Ente

L'Ente può designare direttamente Amministratori di Sistemi esterni (ovverosia, soggetti alle dipendenze di società esterne e/o liberi professionisti) nei casi in cui svolgono funzioni di amministrazione su sistemi gestiti direttamente dall'Ente.

La valutazione delle caratteristiche, esperienza, capacità e affidabilità del soggetto che si intende designare deve essere effettuata, tuttavia, dalla società di appartenenza, a mezzo di formale attestazione, o a mezzo di autodichiarazione in caso di libero professionista.

In tutti i casi deve essere effettuata la nomina a Responsabile del Trattamento della società o del libero professionista.

A ciascuna singola persona fisica cui siano attribuite funzioni di amministratore di sistema sono assegnati specifici ambiti di operatività in funzione dei privilegi assegnati.

3.2.2 Amministratori di Sistema designati dal Fornitore

Nei casi non disciplinati dal paragrafo precedente la designazione degli Amministratori di Sistema è effettuata direttamente dai soggetti che erogano i servizi, i quali, designati quali Responsabili del trattamento per i servizi affidati, hanno l'obbligo di conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

Tale onere deve essere espressamente indicato nella designazione del Fornitore quale Responsabile del trattamento dei dati personali, ai sensi e per gli effetti di cui all'art. 28 del Regolamento UE 2016/679.

3.3 Amministratori di Sistema della "Dotazione Informatica"

A complemento di quanto disposto dal citato Provvedimento del Garante per la protezione dei dati personali, tutti gli utenti che sono amministratori delle dotazioni informatiche (di seguito anche solo DI) devono essere designati Amministratori di Sistema.

Preventivamente alla formale designazione, il Responsabile della struttura a cui il soggetto da designare è assegnato, deve motivare l'esigenza di assegnazione dei privilegi sulle DI, al responsabile SIID. Questo, esperita valutazione, fornisce il nulla osta alla designazione ad amministratore di sistema oppure propone soluzioni alternative alla concessione dei privilegi richiesti.

4 Registro digitale degli Amministratori di Sistema

La norma dispone che sia mantenuto costantemente e tempestivamente aggiornato l'elenco nominativo degli Amministratori di Sistema e che per ciascuno degli amministratori designati sia specificato l'ambito di operatività in funzione dei profili autorizzativi assegnati.

Il Registro degli Amministratori di Sistema contiene le seguenti macro categorie di sistemi amministrati.

Amministratori di dominio; si tratta degli amministratori dei domini Active Directory; rientrano in questa categoria i componenti dei gruppi “Domain Admins”e tutti coloro che attraverso un meccanismo di delega hanno la possibilità di agire su un sottoinsieme degli oggetti dei domini.

Amministratori di server; si tratta degli utenti che hanno diritti amministrativi su uno o più server; a titolo esemplificativo rientrano in questa categoria gli utenti appartenenti al gruppo "Administrators" di uno o più server Windows o gli utenti di uno o più server Linux che attraverso il comando “sudo” possono impersonare l’utente “root”.

Amministratori di basi di dati; rientrano in questa categoria gli utenti che hanno la possibilità di manipolare la struttura di uno o più database attraverso comandi di “Data Definition Language”.

Amministratori di apparati di rete; rientrano in questa categoria gli utenti che hanno la possibilità di accedere ad apparati di rete layer 2 o layer 3 e modificarne le configurazioni.

Amministratori di apparati di sicurezza; rientrano in questa categoria gli utenti che possono modificare le configurazioni di sistemi hardware o software dedicati alla sicurezza, quali ad esempio firewall, sistemi di intrusion prevention, web proxy e sistemi antivirus e il Security Operation Center (SOC).

Amministratori di dotazione informatica; rientrano in questa categoria gli utenti appartenenti al gruppo “Administrators” di una o più dotazione informatica, di uno o più computer, così come gli utenti con privilegi speciali sugli strumenti di mobile device management per le dotazioni mobili quali smartphone, tablet e simili.

Amministratori di sistemi software complessi; rientrano in questa categoria gli amministratori di sistemi software applicativi o infrastrutturali (anche in Cloud) che contengono diverse componenti hardware e software che interagiscono tra loro; esempi di sistemi software complessi sono i sistemi data warehouse, i sistemi di posta elettronica, i sistemi middleware i sistemi che gestiscono gli asset ovvero strumenti di lavoro fissi e mobili come ad esempio Google, Citrix, FTP, CMS, VmWare, Zabbix.

Amministratori di sistemi che trattano o permettono il trattamento di informazioni personali riguardanti i lavoratori; rientrano in questa categoria gli amministratori di sistema appartenenti ad una delle categorie sopra elencate che permettono il trattamento di informazioni personali riguardanti i lavoratori.

All’interno del registro degli Amministratori di Sistema le macro categorie elencate sono ulteriormente dettagliate in ulteriori sottolivelli. In ogni categoria così specificata vengono descritte le funzioni svolte dagli amministratori e gli identificativi degli amministratori che svolgono tali funzioni.

5 Verifica annuale delle attività degli Amministratori di Sistema

La normativa dispone che sia effettuata una verifica annuale dell'attività degli Amministratori dal Responsabile del SIID unitamente al DPO.

6 Uso appropriato dei privilegi di Amministratore di Sistema e compiti assegnati

Nell'esecuzione dei compiti di Amministratore di Sistema il soggetto designato deve:

- impostare ed aggiornare le proprie credenziali di utilizzo del sistema rispettando quanto previsto dal paragrafo "ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE" della direttiva della Presidenza del Consiglio dei Ministri del 2016 "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni", per quanto in proprio potere;

- seguire le indicazioni riportate nel Disciplinare tecnico per l'utilizzo degli strumenti informatici e nel piano di sicurezza informatica del Titolare per l'attivazione/aggiornamento degli account utenti sul sistema;

- monitorare regolarmente e adeguatamente la funzionalità del sistema, servizio, apparato, database, relazionandosi adeguatamente con il fornitore del sistema e dei servizi di assistenza e manutenzione;

- comunicare tempestivamente al Titolare o al delegato dello stesso eventuali rischi potenziali, problematiche, anomalie o criticità relative alla sicurezza dei dati occorse nelle attività di trattamento e di amministrazione di sistemi;

- relazionare sulle eventuali azioni correttive poste in atto (da lui o dal fornitore dei servizi di assistenza/manutenzione) e sugli esiti delle stesse;

- fornire ogni assistenza al Titolare e al RPD del Titolare, soprattutto qualora sia necessario attivare le procedure per i Data Breach, ovvero garantire i diritti degli interessati;

- monitorare la funzionalità del sistema, servizio, apparato, database di cui abbia la responsabilità;

- effettuare, in caso di necessità, gli interventi di assistenza e manutenzione consentiti dal profilo autorizzativo del proprio account;

- attivare le credenziali ed i profili di autenticazione univocamente correlate ai soggetti autorizzati del trattamento, con caratteristiche di robustezza adeguate a garantire una ragionevole sicurezza dei trattamenti e configurare il profilo di autorizzazione coerentemente alle specifiche mansioni affidate (basi dati accessibili e trattamenti consentiti);

- verificare la funzionalità degli strumenti per la protezione dei dati contro il rischio di intrusione (firewall) e dell'azione di programmi informatici malevoli (virus informatici etc.);

- aggiornare periodicamente i programmi per elaboratore allo scopo di prevenire la vulnerabilità degli strumenti elettronici e correggerne i difetti;

- adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e sovraintendere alle operazioni di back-up periodico degli stessi con copie di sicurezza;

- assicurarsi della qualità delle copie di sicurezza dei dati ove necessario ed applicare i criteri per la conservazione;

- segnalare tempestivamente al Titolare o al delegato dello stesso eventuali rischi o anomalie nella gestione delle misure di sicurezza relative ai dati personali.

6.1 Sospensione dei privilegi

Nel caso in cui sia accertato che il comportamento di un Amministratore di Sistema sia doloso o gravemente negligente ed in palese contrasto con le politiche di sicurezza dell'Ente i privilegi informatici ad esso assegnati sono sospesi fintantoché le cause e le responsabilità effettive dell'incidente non siano state appurate a conclusione dell'eventuale procedimento per l'accertamento di responsabilità disciplinare.