

Identificativo: <<RC\_PG\_GA\_00\_Procedura di Gestione degli Amministratori di Sistemi>> <<Ver. 2.0>>

Data: 02/05/2024

**PROGETTO:**  
**GOVERNO DELLA CYBERSECURITY E DELLA DATA PROTECTION**

**Procedura di Gestione degli Amministratori di Sistema**



# Regione Calabria

Costituito

**Raggruppamento Temporaneo di Imprese**  
composto da:

**Deloitte Risk Advisory S.r.l.**

**EY Advisory S.p.A.**

**Teleco S.r.l.**

### Lista di Distribuzione

Rev.	Data	Destinatario	Azienda
1.0		Ing. Alfredo Pellicanò	Regione Calabria
1.0		Dott.ssa Paola Zuccaro	Regione Calabria
1.0		Ing. Giovanna Pisano	Regione Calabria
1.0		Dott. Sebastiano Massimo Rodà	Regione Calabria
1.0		Avv. Angela Stellato	Regione Calabria
1.0		Dott. Salvatore Lopresti	Regione Calabria
1.0		Avv. Daniela Labate	Regione Calabria
1.0		Dott. Giovanni Sacchi	Regione Calabria
1.0		Ilenia Pia Viceconti	Deloitte

### Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autore di rif.
1.0	14/04/2024	Prima versione	Ilenia Pia Viceconti
2.0	02/05/2024	Modifiche Misure Tecniche	Ilenia Pia Viceconti

### Calendario degli Incontri Principali

Data	Incontro	Stato
15/04/2024	Riunione con la DPO	Effettuato
18/04/2024	Riunione con la DPO, la Direttrice a capo dell'Esecuzione del contratto (DEC)	Effettuato
22/04/2024	Riunione con la DPO, la Direttrice a capo dell'Esecuzione del contratto (DEC),f) e i Referenti Ufficio Privacy Regionale	Effettuato

## SOMMARIO

SOMMARIO .....	3
1. INTRODUZIONE .....	5
1.1 SCOPO .....	5
1.2 CAMPO DI APPLICAZIONE .....	5
2. DEFINIZIONE E ACRONIMI.....	5
2.1 DEFINIZIONI .....	5
2.2 ACRONIMI.....	6
3. RIFERIMENTI .....	6
3.1 DOCUMENTI APPLICABILI.....	6
3.2 DOCUMENTI DI RIFERIMENTO .....	6
4. RIFERIMENTI NORMATIVI .....	7
5. RUOLI E RESPONSABILITÀ .....	7
5.1 MATRICE RACI.....	9
6. IL PROCESSO DI GESTIONE DEGLI AMMINISTRATORI DI SISTEMA.....	10
6.1 MISURE ORGANIZZATIVE .....	10
6.1.1 VALUTAZIONE DELLE CARATTERISTICHE SOGGETTIVE - COMMA 2, LETTERA A) .....	10
6.1.1.1 PROCESSO DI RECLUTAMENTO E SELEZIONE DEGLI AMMINISTRATORI DI SISTEMA .....	11
6.1.1.2 ATTIVITÀ DI FORMAZIONE.....	11
6.1.1.3 VALUTAZIONE .....	11
6.1.2 DESIGNAZIONI INDIVIDUALI - COMMA 2, LETTERA B) .....	12
6.1.3 ELENCO DEGLI AMMINISTRATORI DI SISTEMA - COMMA 2, LETTERA C).....	12
6.1.4 SERVIZI IN OUTSOURCING - COMMA 2, LETTERA D) .....	13
6.1.5 VERIFICA DELLE ATTIVITÀ - COMMA 2, LETTERA E).....	14
6.2 MISURE TECNICHE .....	15
6.2.1 REGISTRAZIONE DEGLI ACCESSI – COMMA 2, LETTERA F).....	15
6.2.2 VERIFICA DEI LOG DEGLI AMMINISTRATORI DI SISTEMA CHE OPERANO SU PIATTAFORME NAZIONALI .....	16
7. ALLEGATI .....	17
7.1 RC_PG_GA_01_ALLEGATO A – FORMAT PER LA DESIGNAZIONE DELL'AMMINISTRATORE DI SISTEMA .....	17
NOTE PER LA COMPILAZIONE DELLA TABELLA DELLE ATTIVITA' DI TRATTAMENTO AUTORIZZATE ....	21
7.2 RC_PG_GA_02_ALLEGATO B – FORMAT PER LA REVOCA DELLA DESIGNAZIONE DELL'AMMINISTRATORE DI SISTEMA .....	23

<b>7.3</b>	<b>RC_PG_GA_05_ALLEGATO E – FORMAT PER LA COMUNICAZIONE RELATIVA ALLA VERIFICA DEGLI ACCESSI LOGICI ALLE PIATTAFORME NAZIONALI DEGLI AMMINISTRATORI DI SISTEMA DELLA REGIONE CALABRIA .....</b>	<b>24</b>
<b>7.4</b>	<b>RC_PG_GA_06_ALLEGATO F - LINEE GUIDA ED ISTRUZIONI REGIONALI PER GLI AMMINISTRATORI DI SISTEMA ESTERNI.....</b>	<b>25</b>
<b>7.5</b>	<b>RC_PG_GA_07_ALLEGATO G – FORMAT PER LA DESIGNAZIONE DELL'AMMINISTRATORE DI SISTEMA ESTERNO .....</b>	<b>28</b>
<b>7.6</b>	<b>ULTERIORI ALLEGATI.....</b>	<b>33</b>

## 1. INTRODUZIONE

Il 27 novembre 2008 l’Autorità Garante per la Protezione dei Dati Personali (di seguito “Garante” o “Autorità”) ha pubblicato un provvedimento dal titolo *“Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema”* (di seguito Provvedimento), con l’obiettivo di identificare le misure tecniche ed organizzative necessarie a garantire che gli Amministratori di Sistema possano operare sui sistemi che trattano Dati Personali senza comprometterne la riservatezza e l’integrità.

Il Garante ha integrato e parzialmente modificato il Provvedimento di cui sopra recependo alcune indicazioni pervenute, anche da associazioni di categoria, nel corso della consultazione pubblica conclusasi il 31 maggio 2009. Con le nuove disposizioni il Garante ha inteso facilitare il corretto adempimento alle prescrizioni impartite, mantenendo comunque elevato il livello di protezione dei Dati Personali e le garanzie per i cittadini.

### 1.1 SCOPO

Regione Calabria conta un grande numero di Amministratori di Sistema sia interni all’Ente sia esterni che operano sui sistemi regionali e che necessitano di essere gestiti in maniera puntuale in coerenza con il dettame normativo vigente. La gestione degli Amministratori è deputata al singolo Dipartimento e Struttura Equiparata ma risulta necessario definire ruoli e responsabilità in maniera chiara e puntuale per tutta la Regione al fine di prevedere una struttura organica in ottemperanza al 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 ss.mm.ii. e alle relative FAQ.

### 1.2 CAMPO DI APPLICAZIONE

L’ambito di applicazione del presente documento è limitato a quanto oggetto del Provvedimento del Garante Privacy del 27 novembre 2008 e delle integrazioni e parziali modifiche comunicate dall’Autorità stessa il 26 giugno 2009. In particolare, nella definizione del perimetro di applicazione delle misure di sicurezza e degli accorgimenti prescritti dal Garante, si è tenuto conto anche delle *“Risposte alle domande più frequenti”* (FAQ) pubblicate dal Garante stesso.

## 2. DEFINIZIONE E ACRONIMI

### 2.1 DEFINIZIONI

Termine	Descrizione
Titolare del trattamento di Dati Personali	Il Titolare del trattamento è 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri. Nel caso di specie Titolare è la Regione Calabria.

Dato Personale	Un Dato Personale è una qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Misure di sicurezza	Misure tecniche ed organizzative adeguate a garantire un livello di sicurezza dei dati trattati adeguato al rischio

## 2.2 ACRONIMI

Termine	Descrizione
Provvedimento	Provvedimento dell'Autorità Garante Privacy n. 300 del 27 novembre 2008 e ss.mm.ii "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema"
GDPR	Regolamento UE 2016/679 - General Data Protection Regulation
AdS	Amministratore di Sistema
DPO	Data Protection Officer

## 3. RIFERIMENTI

### 3.1 DOCUMENTI APPLICABILI

Rif.	Codice	Titolo
DA-1.	RC05_Piano Fabbisogni_Governo Cybersecurity e Data Protection v16	Piano dei fabbisogni
DA-2.	CIG 8884642E81	Contratto Esecutivo del 05 marzo 2024

### 3.2 DOCUMENTI DI RIFERIMENTO

Rif.	Codice	Titolo
DR-1.	Doc. web n. 1577499	Provvedimento dell'Autorità Garante Privacy n. 300 del 27 novembre 2008 e ss.mm.ii "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema"
DR-2.	Doc. web n. 1577499	FAQ pubblicate dall'Autorità Garante in data 21 maggio 2009

DR-3.	Prot. N. 121662 del 11 marzo 2022	Gestione delle abilitazioni utenze Sistema SEC-SISR
DR-4.	DGR N. 29 del 1° febbraio 2021	Regolamento Regionale n. 20 del 18 dicembre 2018 modificato dalla deliberazione di Giunta Regionale n. 29 del 1° febbraio 2021
DR-5.	DGR N. 12 del 14 dicembre 2022	Regolamento Regionale n. 12/2022 e ss.mm.ii "Regolamento di organizzazione delle strutture della Giunta Regionale" (ultima modifica 28/12/2023)

#### 4. RIFERIMENTI NORMATIVI

Il presente documento è redatto in coerenza con le seguenti normative e documenti di riferimento:

- [1] L. 300 del 1970 - Statuto dei lavoratori;
- [2] D. Lgs. 196/2003 - Codice in materia di protezione di dati personali (di seguito "Codice Privacy");
- [3] Provvedimento del Garante Privacy del 27 novembre 2008 e integrazioni e parziali modifiche comunicate dall'Autorità stessa il 26 giugno 2009 (di seguito "Provvedimento");
- [4] FAQ pubblicate dall'Autorità Garante in data 21 maggio 2009 (di seguito "FAQ");
- [5] Regolamento UE 2016/679 - General Data Protection Regulation (di seguito GDPR);
- [6] D. Lgs. 101/2018 - 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 (Regolamento Generale sulla Protezione dei Dati);
- [7] Regolamento Regionale n. 20 del 18 dicembre 2018 modificato dalla Deliberazione di Giunta Regionale n. 29 del 1° febbraio 2021.

#### 5. RUOLI E RESPONSABILITÀ

Ciascun Dipartimento e Struttura Equiparata della Regione Calabria sono destinatari del presente documento e deputati al relativo controllo.

Di seguito i ruoli e le relative responsabilità così come descritte:

- **Delegato del Titolare**

Il Titolare del Trattamento delega i compiti e le funzioni di cui all'art. 1, comma 1 del Regolamento Regionale n. 20 del 18 dicembre 2018, come modificato dalla Deliberazione di Giunta Regionale n. 29 del 1 febbraio 2021, a ciascun Dirigente della Giunta Regionale, al Responsabile della prevenzione della corruzione e della trasparenza, nonché ai Responsabili di struttura o ufficio di diretta collaborazione, quali "Delegati al trattamento dei dati personali" (di seguito Delegato del Titolare), ognuno per le attività di trattamento dei Dati Personali effettuate nell'ambito dell'articolazione amministrativa di cui è responsabile. I Delegati sopracitati hanno pertanto il compito di individuare gli "Amministratori di Sistema" ai sensi del Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 e ss.mm.ii.

- **Settore referente privacy dipartimentale**

Il Settore referente privacy dipartimentale è individuato da ciascun Dirigente Generale di Dipartimento o di Struttura Equiparata compie, per le attività di trattamento dei Dati Personali effettuate dall'Ente, una serie di compiti e funzioni riportati all'art. 1, comma 2 del regolamento regionale n. 20 del 18 dicembre 2018, come modificato dalla Deliberazione di Giunta regionale n. 29 del 1 febbraio 2021, tra cui: coordina le attività dei Delegati del Titolare nell'ambito del dipartimento o struttura equiparata; costituisce il punto di contatto dipartimentale per il DPO, il settore regionale competente in materia di privacy ed il settore regionale competente in materia di Agenda Digitale.

- **Settore referente sicurezza informatica regionale**

Il Settore referente sicurezza informatica regionale, competente in materia di Agenda Digitale, supporta i Delegati del Titolare con la collaborazione del "Settore referente privacy regionale" nelle attività di valutazione della gravità delle eventuali violazioni di sicurezza e di determinazione delle misure di contenimento e contrasto per porre rimedio alle violazioni riscontrate. Inoltre, collabora con il "Settore referente privacy regionale" nelle attività di definizione e verifica delle misure di sicurezza informatica, valutazione di impatto delle attività di trattamento (DPIA), notificazione formale di violazione dati al Garante Privacy ed eventuale comunicazione agli interessati ed infine, nella verifica delle condizioni tecniche per l'eventuale trasferimento dati verso paesi terzi o organizzazioni internazionali.

- **Settore referente privacy regionale**

Il Settore referente privacy regionale competente in materia di privacy, oltre ai compiti e funzioni previsti dai vigenti atti di organizzazione, redige le lettere di designazione di Amministratore di Sistema.

- **Amministratore di Sistema**

L'Amministratore di Sistema è una figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti con cui vengono effettuati trattamenti di Dati Personali.

Ai fini di trattamento, nella definizione di "Amministratore di Sistema" rientrano anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e manutenzione hardware, laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso a Dati Personali.

Secondo la FAQ n.1, non rientrano nella definizione quei soggetti che solo occasionalmente intervengono (p.e., manutenzione a seguito di guasto o malfunzionamenti) sui sistemi di elaborazione e sui sistemi di software; inoltre, secondo la FAQ n. 22, sono da escludersi anche tutti i soggetti che operano a livello applicativo.

- **Data Protection Officer (DPO)**

Il DPO ha il compito di controllare e monitorare la corretta adozione degli adempimenti privacy all'interno della Regione Calabria, eventualmente anche con il supporto di consulenti esperti di sistemi di controllo per gli aspetti tecnici. Inoltre, supporta i Dipartimenti e le Strutture Equiparate della Regione Calabria nella valutazione dell'adozione di strumenti per assicurare la corretta gestione degli Amministratori di Sistema.

## 5.1 MATRICE RACI<sup>1</sup>

Di seguito una panoramica sui ruoli coinvolti in ciascuna fase del processo dettagliato nei successivi paragrafi:

ID	DESCRIZIONE	DELEGATO TITOLARE	SETTORE REFERENTE PRIVACY DIP.	SETTORE REFERENTE SICUREZZA INFORMATICA REG.	SETTORE REFERENTE PRIVACY REG.	AdS	DPO
1	<b>Reclutamento e Selezione degli Amministratori di Sistema</b> L'attività include il processo di reclutamento e selezione degli Amministratori di Sistema sulla base di esigenze interne espresse dai Dipartimenti e dalle Strutture Equiparate della Regione	A/R	R	-	-	C/I	-
2	<b>Formazione Amministratori di Sistema</b> L'attività concerne la pianificazione, la gestione e lo svolgimento delle attività di formazione agli Amministratori di Sistema	A/R	-	R	-	I	I
3	<b>Valutazione caratteristiche soggettive degli Amministratori di Sistema</b> L'attività prevede la valutazione delle caratteristiche soggettive degli Amministratori di Sistema in fase di recruiting e selezione del personale	A/R	R	-	-	I	-
4	<b>Designazioni qualifica individuale di Amministratori di Sistema con lettera di nomina</b> Tale attività concerne l'erogazione delle lettere di nomina alle persone che saranno designate Amministratori di Sistema	A/R	R	-	-	I	-
5	<b>Aggiornamento elenco degli Amministratori di Sistema</b> L'attività prevede l'aggiornamento dell'elenco degli Amministratori di Sistema che dovrà essere mantenuto e aggiornato nel tempo (considerando ad es. revoche, cambi mansione etc.)	I	A/R	R	C	I	-
6	<b>Garanzie per servizi in outsourcing</b> Tale attività concerne la ricezione di garanzie in ambito privacy da parte di ciascun fornitore cui sono affidate le attività di Amministratore di Sistema	C	A/R	R	-	I	-
7	<b>Verifica delle attività degli Amministratori di Sistema</b> L'attività prevede una verifica, almeno con cadenza annuale, dell'operato degli Amministratori di Sistema secondo quanto stabilito dal Provvedimento	I	R	A/R	-	I	-
8	<b>Verifica dei log degli Amministratori di Sistema</b> L'attività prevede la verifica dei log degli Amministratori di Sistema secondo quanto stabilito dal Provvedimento	I	A/R	R	-	I	I

<sup>1</sup>RACI: Responsible (chi esegue l'attività), Accountable (chi ha la responsabilità del risultato dell'attività), Consulted (chi è consultato dal Responsabile per l'esecuzione dell'attività), Informed (chi è informato sul progresso dell'attività).

## 6. IL PROCESSO DI GESTIONE DEGLI AMMINISTRATORI DI SISTEMA

Il processo di gestione degli Amministratori di Sistema è definito sulla base di specifici requisiti tratti dal Provvedimento del Garante e relative modifiche[3], pertanto la presente procedura ripercorrerà inizialmente i principali punti della normativa disciplinando, sulla base degli stessi, le fasi del processo di gestione degli Amministratori di Sistema.

Il Provvedimento, in accordo con l'art. 154, comma 1, lett. c) del "Codice in materia di protezione dei dati personali" (d. lgs. 30 giugno 2003 n. 196 così come modificato dall'art. 14, comma 1, lett. c), d.lgs. 10 agosto 2008, n. 101)[2][6] prescrive l'adozione delle misure tecniche e organizzative, ai Titolari di Dati Personali soggetti all'ambito applicativo dell'ex Codice Privacy ed effettuati con strumenti elettronici, come di seguito distinte:

- **Misure Organizzative:**
  - Valutazione delle caratteristiche soggettive;
  - Designazioni individuali;
  - Elenco degli Amministratori di Sistema;
  - Servizi in outsourcing;
  - Verifica delle attività.
  
- **Misure Tecniche:**
  - Registrazione degli accessi logici.

### 6.1 MISURE ORGANIZZATIVE

#### 6.1.1 VALUTAZIONE DELLE CARATTERISTICHE SOGGETTIVE - COMMA 2, LETTERA A)

Di seguito un estratto del Provvedimento in merito alla valutazione delle caratteristiche soggettive dell'Amministratore di Sistema:

*"L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e 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.*

*Anche quando le funzioni di Amministratore di Sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il Titolare e il Responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29."*

Le misure previste dall'Autorità Garante Privacy muovono dal presupposto secondo cui l'affidamento dell'incarico di Amministratore di Sistema e lo svolgimento delle funzioni tipiche ad esso riconducibili siano

da considerarsi rischiosi ai fini della disciplina posta a protezione dei Dati Personali e, quindi, meritevoli di maggiori garanzie e controlli. Per tali motivi nel Provvedimento si richiama, innanzitutto, l'attenzione dei Titolari su alcune valutazioni preventive che devono essere sempre effettuate in relazione alle caratteristiche qualitative del soggetto designato (esperienza, capacità e affidabilità). Il soggetto designato deve, inoltre, fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

#### **6.1.1.1 PROCESSO DI RECLUTAMENTO E SELEZIONE DEGLI AMMINISTRATORI DI SISTEMA**

Il Delegato del Titolare e il Settore Referente Privacy Dipartimentale provvedono al reclutamento<sup>2</sup> e alla selezione degli Amministratori di Sistema.

Inoltre, Il Delegato del Titolare e il Settore Referente Privacy Dipartimentale hanno anche il compito di censire gli stessi nell'elenco degli Amministratori di Sistema presente nella piattaforma Trades. Infine, dovrà avere cura di verificare il rispetto dei seguenti requisiti:

- Ruolo da ricoprire e i requisiti necessari per la posizione;
- Motivazione della richiesta di integrazione dell'organico;
- Descrizione del lavoro;
- Profilo professionale richiesto;
- Requisiti (studi, esperienza lavorativa, competenze comportamentali e qualificazioni richieste).

#### **6.1.1.2 ATTIVITÀ DI FORMAZIONE**

Il Delegato del Titolare di concerto con il Settore referente sicurezza informatica regionale, ha il compito di pianificare, organizzare ed erogare, per il tramite dei propri Referenti, l'attività di formazione agli Amministratori di Sistema periodicamente ed almeno una volta all'anno, con l'obiettivo primario di rendere il personale sensibile e consapevole dell'importanza delle tematiche di Sicurezza delle Informazioni e Protezione dei Dati Personali.

In aggiunta, i Delegati del Titolare sono tenuti a informare e tenere costantemente aggiornato il DPO della Regione Calabria dell'attività di formazione degli Amministratori di Sistema.

#### **6.1.1.3 VALUTAZIONE**

Il processo di valutazione delle caratteristiche soggettive degli Amministratori di Sistema è eseguito dal Delegato del Titolare e il Settore Referente Privacy Dipartimentale, nell'ambito delle attività di recruiting e selezione del personale. In particolare, il Delegato e il Settore Referente Privacy Dipartimentale valutano gli Amministratori di Sistema prendendo in considerazione i seguenti aspetti:

- **Competenze tecniche** in relazione agli ambiti di operatività dell'Amministratore di Sistema e ai sistemi da esso amministrati, comprovate anche da certificazioni professionali, corsi di

---

<sup>2</sup> Con il termine "reclutamento" si intendono tutti i processi di selezione interna dei funzionari con elevata qualificazione della Regione Calabria che presentano le caratteristiche necessarie per ricoprire il ruolo di Amministratori di Sistema

perfezionamento, piani di training effettuati, curriculum vitae et studiorum, esperienze pregresse su tecnologie analoghe;

- **Qualità professionali**, in termini di esperienza e capacità dell'Amministratore di Sistema, comprovate anche da precedenti incarichi professionali analoghi;
- **Competenze nell'ambito della sicurezza delle informazioni e nella protezione dei dati**, comprovate dall'esperienza, dal curriculum vitae et studiorum e verificate anche in fase di colloquio.

Inoltre, consolidano il processo di valutazione la compilazione della nomina (Allegato A) e revoca (Allegato B) ad Amministratore di Sistema e la revisione periodica dell'elenco degli Amministratori.

### 6.1.2 DESIGNAZIONI INDIVIDUALI - COMMA 2, LETTERA B)

Di seguito un estratto del Provvedimento in merito alla designazione individuale dell'Amministratore di Sistema:

*“La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.”*

Il Provvedimento prevede l'obbligo di designare individualmente l'Amministratore di Sistema, indicando in maniera analitica gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. La FAQ n. 7 precisa altresì che la descrizione puntuale dei trattamenti consentiti all'Amministratore di Sistema debba avvenire analogamente a quanto richiesto dall'art. 27, comma 1, lett. a), n. 2), d.lgs. 10 agosto 2018, n. 101[6] con riguardo agli eventuali responsabili del trattamento, al fine di evitare l'attribuzione di ambiti insufficientemente dettagliati.

In risposta a tale requisito, il Delegato del Titolare di concerto con il Settore Referente Privacy Dipartimentale designano tramite lettera gli Amministratori di Sistema (Allegato A) e contestualmente ciascun Dipartimento e Struttura Equiparata<sup>3</sup> inserisce i relativi nominativi all'interno dell'elenco riportato nella piattaforma Trades della Regione Calabria.

Qualora fosse necessario l'accesso di un dipendente a banche dati nazionali, il Delegato del Titolare e il Settore Referente Privacy Dipartimentale per i propri ambiti di attività al pari di quanto sopra, provvedono a designare la persona come Amministratore di Sistema e tramite il supporto del relativo Dipartimento e Struttura Equiparata<sup>2</sup> riportano il suo nominativo nell'elenco degli Amministratori presente sulla piattaforma Trades.

### 6.1.3 ELENCO DEGLI AMMINISTRATORI DI SISTEMA - COMMA 2, LETTERA C)

Di seguito un estratto del Provvedimento in merito all'elenco degli Amministratori di Sistema:

---

<sup>3</sup> Da intendersi, in tale specifico caso, come supporto al Delegato del Titolare nel censimento degli Amministratori di Sistema nell'apposito elenco.

*“Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.”*

Qualora l'attività degli Amministratori di Sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, il Delegato del Titolare e il Settore Referente Privacy Dipartimentale sono tenuti a rendere nota o conoscibile l'identità degli Amministratori di Sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'ente o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del GDPR nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58) o, in alternativa, mediante altri strumenti di comunicazione interna (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini) o tramite procedure formalizzate a istanza del lavoratore. Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinino uno specifico settore.

Tra le misure di carattere organizzativo prescritte dal Garante rientra anche l'obbligo di predisporre un elenco con gli estremi identificativi degli Amministratori da mantenere costantemente aggiornato. Il Settore Referente Privacy Dipartimentale, con il supporto del Settore Referente Sicurezza Informatica Regionale, si impegnano a mantenere costantemente aggiornato l'elenco mediante il censimento degli Amministratori di Sistema interni ed esterni all'interno di un documento intitolato “Registro degli Amministratori di Sistema” (Allegato I) che verrà trasposto nella piattaforma Trades della Regione Calabria.

Con particolare riferimento agli Amministratori di Sistema che accedono a banche dati nazionali, ciascun Dipartimento e Struttura Equiparata, a seguito di consultazione con il Settore Referente Privacy Regionale, informa e trasmette semestralmente al Delegato del Titolare, l'elenco delle persone che sono state nominate Amministratori di Sistema (Allegato H).

Una volta trasmesso l'elenco al Delegato del Titolare, i nominativi degli Amministratori autorizzati ad accedere a banche dati nazionali devono essere integrati nell'elenco presente nella piattaforma Trades.

Nella FAQ n.21 si precisa che i dati forniti devono essere utili ad individuare il soggetto nell'ambito dell'organizzazione di appartenenza (ad es. nome, cognome, funzione o area organizzativa di appartenenza).

#### **6.1.4 SERVIZI IN OUTSOURCING - COMMA 2, LETTERA D)**

Di seguito un estratto del Provvedimento in merito ai servizi in outsourcing:

*“Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.”*

Qualora siano presenti fornitori cui sono demandate le attività di Amministratore di Sistema cd. “esterno”, il Delegato del Titolare informa il fornitore di mantenere sempre aggiornata la lista degli Amministratori che

operano sui propri sistemi e di renderla disponibile su richiesta del Titolare come previsto dal documento “Linee guida ed istruzioni regionali per gli Amministratori di sistema esterni” (Allegato F). Inoltre, il Settore Referente Privacy Dipartimentale in accordo con il Settore Referente per la sicurezza informatica regionale verificano che il fornitore:

- assuma il ruolo di Responsabile del trattamento poiché l’esecuzione del Contratto, avente ad oggetto la gestione e amministrazione di sistemi elettronici, prevede il trattamento di Dati Personali di cui la Regione Calabria è Titolare;
- rispetti le misure di sicurezza adeguate alle attività da svolgere;
- rilasci, ove richiesto, l’attestazione di conformità;
- rispetti, con riferimento al Provvedimento, le misure previste, ed in particolare il fornitore deve provvedere in modo autonomo a identificare e designare gli Amministratori di Sistema.

#### **6.1.5 VERIFICA DELLE ATTIVITÀ - COMMA 2, LETTERA E)**

Di seguito un estratto del Provvedimento in merito alla verifica delle attività degli Amministratori di Sistema:

*“L’operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un’attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.”*

Il Provvedimento stabilisce l’obbligo di verifica, con cadenza almeno annuale, dell’operato degli Amministratori di Sistema e, in particolare, della conformità dei trattamenti di dati effettuati in linea con quanto richiesto dalle norme vigenti in materia di protezione di dati e sicurezza delle informazioni. La FAQ n. 5 precisa altresì che le verifiche hanno ad oggetto le attività svolte dall’Amministratore di Sistema alla luce delle mansioni a lui attribuite, compreso il profilo della sicurezza. La FAQ n. 16 afferma che l’analisi dei log raccolti può essere compresa tra i criteri di valutazione dell’operato dell’Amministratore di Sistema, in quanto consente di verificare eventuali anomalie nella frequenza e nelle modalità degli accessi.

In risposta a tale requisito, il Settore Referente Privacy Dipartimentale formalizza un “Piano annuale per le verifiche di conformità” (Allegato C). Durante tale fase, si identificano tutti gli attori coinvolti che dovranno essere oggetto di verifica da parte del Settore referente sicurezza informatica regionale. La pianificazione, di massima, contempla un arco temporale di un anno, ma tale piano può essere modificato a seguito di situazioni particolari. Eventuali modifiche inerenti ai cambiamenti di attività degli Amministratori di Sistema devono essere comunicate al Delegato del Titolare coinvolto per procedere all’aggiornamento dell’elenco dei ruoli.

Le attività di verifica dell’operato degli Amministratori di Sistema interni che operano su piattaforme regionali sono eseguite dal Settore Referente Privacy Dipartimentale e dal Settore referente per la sicurezza informatica regionale della Regione Calabria attraverso la verifica periodica del documento “Monitoraggio attività degli Amministratori di sistema” (Allegato D).

Le attività di verifica dell’operato degli Amministratori di Sistema esterni che operano su piattaforme regionali sono eseguite dal fornitore. Il Settore Referente Privacy Dipartimentale e il Settore referente per la sicurezza informatica regionale hanno il compito di verificare la ricezione di garanzie in ambito privacy da

parte di ciascun fornitore cui sono affidate le attività di Amministratore di Sistema, attraverso la verifica periodica del documento “Monitoraggio attività degli Amministratori di sistema” (Allegato D).

Inoltre, per le attività di verifica dell’operato degli Amministratori di Sistema che operano su banche dati nazionali, si richiede la tenuta di un apposito registro “Registro utenze abilitate su banche dati nazionali” (Allegato H) in cui dovranno essere registrate le utenze abilitate ad accedere alla relativa banca dati e di trasmettere il registro in versione aggiornata al Delegato del Titolare e al Settore referente per la sicurezza informatica regionale con cadenza semestrale.

## 6.2 MISURE TECNICHE

### 6.2.1 REGISTRAZIONE DEGLI ACCESSI – COMMA 2, LETTERA F)

Di seguito un estratto del Provvedimento in merito alla registrazione degli accessi degli Amministratori di Sistema:

*“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.”*

Il Provvedimento impone ai Titolari del trattamento destinatari delle nuove regole di adottare sistemi di registrazione degli accessi logici effettuati dagli Amministratori di Sistema su sistemi informativi, sia server che client, e su banche dati elettroniche della Regione Calabria. La tenuta delle registrazioni degli accessi informatici dovrà rispondere a specifiche caratteristiche di completezza, inalterabilità e verificabilità della loro integrità da parte del Titolare e di adeguatezza rispetto agli scopi per cui è prevista, nonché essere soggetta a conservazione per un periodo minimo di sei mesi. Nelle FAQ il Garante effettua alcune considerazioni, in particolare:

- la descrizione dell’evento che ha generato l’accesso logico da parte dell’Amministratore di Sistema riguarda esclusivamente l’accesso interattivo a sistemi di elaborazione o a sistemi software (esclusi gli accessi alle applicazioni informatiche) e non anche le attività interattive (ad es. comandi impartiti, transazioni effettuate) da questi eseguite (FAQ n. 11, 15 e 22);
- tra gli accessi logici degli Amministratori di Sistema che devono essere registrati, rientrano anche le autenticazioni nei confronti dei data base management systems (FAQ n. 19).

Il Settore Referente Privacy Dipartimentale e il Settore referente per la sicurezza informatica regionale sono tenuti a garantire la corretta registrazione degli accessi degli Amministratori che operano sui sistemi della Regione Calabria nel rispetto di quanto richiesto dal Provvedimento. A tal fine il Settore Referente Privacy Dipartimentale, di concerto con il Settore referente per la sicurezza informatica regionale, deve tenere costantemente aggiornato l’elenco degli Amministratori di Sistema che accedono ai sistemi della Regione e

monitorare gli accessi mediante l'apposito elenco (Allegato D – Monitoraggio attività degli Amministratori di Sistema).

Il monitoraggio degli accessi deve essere svolto seguendo i passaggi della procedura di sicurezza delle utenze amministrative. In particolare, il Settore Referente Privacy Dipartimentale, di concerto con il Settore referente per la sicurezza informatica regionale, hanno il compito di:

- richiedere, all'Amministratore di Sistema di competenza, l'estrazione dei log di accesso delle utenze rispetto ad un periodo di tempo definito in fase di verifica;
- verificare che le utenze per cui si è registrato un accesso hanno i privilegi necessari per accedere al sistema;
- verificare che le utenze siano nominative e non di gruppo;
- verificare che le informazioni all'interno dei log siano complete, inalterabili e verificabili nella loro integrità (es. tutti i log devono contenere il codice identificativo dell'addetto IT; data e ora di login e di logout).

I dettagli specifici e necessari per effettuare le verifiche degli accessi, in conformità ai requisiti descritti in precedenza, si consiglia di utilizzare lo sheet "*Verifiche Registrazione Accessi*" dell'Allegato D.

Le proprietà dei log che devono essere presidiate al fine di mantenere la loro integrità (completezza, inalterabilità e verificabilità) sono dettagliate in maniera specifica nella *Procedura per la classificazione, la gestione, la mitigazione e il monitoraggio degli eventi di sicurezza*.

Inoltre, il Delegato del Titolare può valutare l'introduzione di strumenti che, in ottemperanza a quanto disposto rispetto a questo punto, garantiscono una completa aderenza alla normativa.

## **6.2.2 VERIFICA DEI LOG DEGLI AMMINISTRATORI DI SISTEMA CHE OPERANO SU PIATTAFORME NAZIONALI**

La verifica dei log degli Amministratori di Sistema che accedono a piattaforme nazionali è demandata all'Ente che gestisce la piattaforma nazionale in forza del fatto che la Regione Calabria non ha accesso ai log degli Amministratori che operano sulla stessa. A tal fine il Delegato del Titolare è tenuto a fornire apposita comunicazione (Allegato E) agli Enti al fine di richiedere lo svolgimento delle suddette verifiche.

In aggiunta, ciascun Delegato del Titolare è tenuto a informare e tenere costantemente aggiornato il DPO della Regione Calabria.

## 7. ALLEGATI

### 7.1 RC\_PG\_GA\_01\_ALLEGATO A – FORMAT PER LA DESIGNAZIONE DELL'AMMINISTRATORE DI SISTEMA

**Lettera di designazione ad “Amministratore di Sistema”  
ai sensi del “Provvedimento” del Garante per la Protezione dei Dati Personali del 27 novembre  
2008 recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008 ss.mm.ii**

Oggetto: **Designazione ad “Amministratore di Sistema”**

Al/Alla Sig./Sig.ra \_\_\_\_\_ nato/a a \_\_\_\_\_ il \_\_\_\_\_, matricola  
\_\_\_\_\_ qualifica \_\_\_\_\_ del Dipartimento n. \_\_\_\_\_ Settore n.  
\_\_\_\_\_

#### PREMESSO

- che Regione Calabria, in qualità di Titolare del Trattamento, ha delegato i compiti e funzioni di cui all'art. 1, comma 1 del regolamento regionale n. 20 del 18 dicembre 2018, come modificato dalla deliberazione di Giunta regionale n. 29 del 1 febbraio 2021, a ciascun Dirigente della Giunta Regionale, al Responsabile della prevenzione della corruzione e della trasparenza, nonché ai Responsabili di struttura o ufficio di diretta collaborazione, quali “Delegati al trattamento dei dati personali” (di seguito Delegato del Titolare), ognuno per le attività di trattamento dei dati personali effettuate nell'ambito dell'articolazione amministrativa di cui è responsabile;
- il rapporto di lavoro con Lei in essere e la Sua qualifica ed assegnazione organizzativa;
- che Lei ha già ricevuto, e sottoscritto per presa visione, la lettera di designazione quale “Persona autorizzata al trattamento dei dati personali”;
- che il Provvedimento Generale del Garante per la Protezione dei Dati Personali del 27 novembre 2008 e successive modifiche, prevede che il Titolare/Responsabile del trattamento provveda a nominare, mediante atto scritto, le figure che operano in qualità di “Amministratore di Sistema”.
- Sono individuati quali Amministratori di Sistema coloro che svolgono le seguenti attività:
  - gestione e manutenzione di un impianto di elaborazione o di sue componenti (Technical Operator)
  - gestione dei sistemi di backup (Backup operator)
  - gestione dei profili di accesso degli utenti di un'applicazione (Profile Manager)
  - gestione di sistemi software complessi (programmatori, installatori e manutentori delle applicazioni, gestori del sistema di autenticazione) (Application Manager)
  - gestione di basi di dati (Database Administrator)
  - gestione di rete e di apparati di sicurezza (Network Administrator)
  - gestione della sicurezza (Security Administrator).
- Gli Amministratori così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi,

concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati;

- 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;
- la designazione quale Amministratore di Sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- gli estremi identificativi delle persone fisiche Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite, devono essere annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante;
- qualora l'attività degli Amministratori di Sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli Amministratori di Sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'ente o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Il Delegato del Titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema;
- 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;

CON LA PRESENTE

ad integrazione della suddetta lettera di designazione quale "Persona autorizzata al trattamento dei dati personali", avendo valutato che le prestazioni da Lei effettuate in via ordinaria forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza, la S.V. è designata quale "Amministratore di Sistema".

Tutte le operazioni di trattamento di dati personali saranno eseguite, con modalità e finalità decise dal Delegato del Titolare. Si riportano di seguito i sistemi ICT di cui viene chiesta la gestione e le relative funzioni attribuite.

Utenza	Sistema ICT da amministrare	Tipologia di amministrazione							Ambito di operatività e funzioni attribuite
		AdS di sistema	AdS di backup	AdS di accesso	AdS di software complesso	AdS di database	AdS di rete	AdS di sicurezza	

Per effetto di tale designazione e delle funzioni conseguentemente attribuite, Lei si impegna a:

- porre la massima cura nell'assicurare la protezione dei dati trattati, secondo le procedure definite e/o policy regionali e secondo i criteri tecnici suggeriti dalla sua esperienza e competenza professionale, allo scopo di ridurre al minimo i rischi di distruzione o perdita, intenzionale o accidentale, dei dati; accesso non autorizzato ai dati; trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento;
- assicurare l'integrità dei dati, ossia la certezza che l'informazione affidata derivi da processi di elaborazione corretti e non possa essere manipolata; la disponibilità dei dati, cioè la possibilità che l'informazione affidata sia sempre presente e utilizzabile secondo le necessità operative del Titolare/Responsabile, nei tempi concordati; la riservatezza dei dati, cioè la garanzia che l'informazione affidata ed archiviata sia accessibile solo alle persone autorizzate;
- accedere ai sistemi ICT nei limiti strettamente richiesti dall'espletamento delle Sue mansioni;
- eseguire gli accessi nel rispetto delle procedure di autenticazione a Lei già note, e di detenzione, custodia, segretezza e sicurezza delle relative credenziali di accesso;
- assicurare, per quanto di sua competenza, la disponibilità delle registrazioni (access log) di cui in Premessa. A tal proposito sarà sua cura utilizzare, per lo svolgimento delle attività riguardanti la funzione di Amministratore di Sistema, le specifiche credenziali che le sono state fornite, assicurandone la riservatezza secondo i criteri definiti dalle procedure regionali;
- eseguire gli accessi nel rispetto delle misure di sicurezza organizzative, logiche e fisiche adottate dal Titolare del Trattamento;
- attenersi alle istruzioni operative impartite dal Delegato del Titolare;
- segnalare qualunque elemento che possa pregiudicare il corretto svolgimento delle Sue funzioni di Amministratore di Sistema e/o rendere necessarie ulteriori istruzioni;
- segnalare al Delegato del Titolare e il Settore referente per la sicurezza informatica regionale del trattamento qualsiasi situazione che, anche potenzialmente, minacci la sicurezza dei dati e qualsiasi episodio che abbia concretamente costituito una perdita di integrità, disponibilità o riservatezza dei dati stessi;
- cooperare con il Delegato del Titolare e il Settore referente per la sicurezza informatica regionale per ogni verifica della rispondenza del Suo operato alle misure organizzative, tecniche e di sicurezza previste con riferimento ai dati personali trattati per conto e nell'interesse dell'ente;
- collaborare con il Delegato del Titolare e il Settore referente per la sicurezza informatica regionale per fornire periodicamente le informazioni necessarie a svolgere la prevista attività di controllo annuale, secondo quanto indicato nelle Premesse;
- gestire l'assegnazione, sospensione e cancellazione delle credenziali e dei profili di autenticazione sulle piattaforme di cui in Premessa;
- garantire che i meccanismi di generazione dei log sui sistemi siano sempre attivi e producano i record richiesti, completi ed integri, inviandoli ai sistemi centrali di collazionamento del Titolare/Responsabile del trattamento onde assicurarne la non modificabilità e la conservazione secondo gli obblighi vigenti;
- gestire gli interventi necessari a garantire il corretto funzionamento delle piattaforme di cui in Premessa (configurazione degli apparati di rete, erogazione in continuità dei Servizi ICT, assicurazione degli adeguati livelli di performance, controllo degli accessi degli utenti registrati, monitoraggio e segnalazione anomalie, corretta propagazione dei flussi di rete, cooperazione con i provider esterni di servizi anti DDoS, etc.), assicurando inoltre la segregazione degli ambienti coerentemente con i requisiti di sicurezza espressi dal Titolare/Responsabile del trattamento, sia dal punto di vista architettonico che di gestione delle regole di firewalling sui siti centrali e periferici;

- collaborare per l'attuazione delle eventuali ulteriori prescrizioni che saranno emanate dall'Autorità Garante per la Protezione dei Dati Personali in tema di Amministratori di Sistema;
- consentire il trattamento dei Suoi dati personali nei limiti e per le finalità previste dal citato provvedimento in data 27 novembre 2008 dell'Autorità Garante per la Protezione dei Dati Personali, incluso la registrazione e comunicazione di ogni dato di log, ogni comunicazione a terzi, nonché la divulgazione dei Suoi dati identificativi ai dipendenti dell'ente nell'ambito delle attività organizzative dello stesso.

Resta inteso e convenuto che:

- la presente designazione non configura alcuna variazione della Sua qualifica e delle Sue mansioni e del relativo trattamento economico e normativo del rapporto di lavoro con Lei in essere;
- la registrazione e comunicazione dei dati di log sarà eseguita al solo fine di ottemperare a quanto specificatamente prescritto al riguardo dal citato Provvedimento in data 27 novembre 2008 dell'Autorità Garante per la Protezione dei Dati Personali e non costituisce alcuna forma di controllo a distanza, neanche indiretto, della Sua attività lavorativa;
- ogni eventuale variazione dell'ambito di operatività consentito dalle Sue mansioni e dal Suo profilo di autorizzazione all'accesso ai sistemi ICT non comporterà il venir meno degli effetti della presente designazione.

Le ricordiamo, che il Provvedimento del Garante già citato, obbliga il Titolare del Trattamento alla "verifica" almeno annuale delle attività svolte dall'Amministratore di Sistema in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Distinti saluti

Catanzaro, li \_\_\_\_\_

Il Delegato del Titolare

\_\_\_\_\_

Letto firmato e sottoscritto per accettazione  
L'Amministratore di Sistema

\_\_\_\_\_

## NOTE PER LA COMPILAZIONE DELLA TABELLA DELLE ATTIVITA' DI TRATTAMENTO AUTORIZZATE

- **Tipologia di amministrazione** - Indicare con "X" la tipologia di amministrazione richiesta in base alle funzioni attribuite.
- **Sistema ICT da amministrare** - Si riporta un elenco di sistemi di esempio per ogni tipologia di amministrazione:
  - *amministrazione di rete* - sonde IPS/IDS, proxy server, firewall e apparati di sicurezza perimetrale, dispositivi d'instradamento del traffico (router, switch), ecc;
  - *amministrazione di sistema* - sistemi Operativi, sistemi software di base, middleware, sistemi o infrastrutture di Backup, ecc;
  - *amministrazione di data base* - data base management systems, data warehouse systems, big data systems, ecc;
  - *amministrazione di sistemi software complessi* - sistema amministrativo centrale, sistema sanità, sistema turismo, ecc.
- **Ambito di operatività e funzioni attribuite** - Si riporta un elenco di ambiti di operatività e funzioni di esempio per ogni tipologia di Amministratore:
  - Amministratore di sistema (*Technical Operator*): figura professionale finalizzata alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti. Si occupa, a titolo esemplificativo, della gestione delle credenziali di accesso e delle configurazioni di sicurezza dei sistemi operativi, file system, middleware, infrastrutture; gestione e configurazione dei sistemi operativi; effettua attività di manutenzione ordinaria e straordinaria sui sistemi operativi;
  - Amministratore dei sistemi di backup (*Backup Operator*): effettua attività di salvataggio e ripristino dei dati, le configurazioni; ecc;
  - Amministratore che gestisce i profili di accesso degli utenti di un'applicazione (*Profile Manager*): gestisce i profili di accesso degli utenti di una applicazione e l'assegnazione, sospensione e cancellazione delle credenziali di autenticazione per il personale incaricato al trattamento, nonché organizza tutto il sistema di autorizzazione per le cartelle che verranno realizzate all'interno del server provvedendo alla verifica, con cadenza almeno annuale, della sussistenza delle condizioni per la conservazione di tali autorizzazioni;
  - Amministratore di sistemi software complessi (*Application Manager*): tra cui vi rientrano i programmatori, installatori e manutentori delle applicazioni, gestori del sistema di autenticazione. Effettua, a titolo esemplificativo, attività di manutenzione ordinaria e straordinaria sui sistemi software complessi; applica patch o pacchetti software concernenti le applicazioni gestite; effettua attività di salvataggio e ripristino dei dati e delle configurazioni; eroga servizi di supporto di terzo livello; supporta attraverso analisi specifiche, ecc;
  - Amministratore di basi di dati (*Database Administrator*): gestisce, a titolo esemplificativo, le credenziali di accesso e le configurazioni di sicurezza dei Data Base; la gestione e configurazione dei Data Base; effettua attività di manutenzione ordinaria e straordinaria sui Data Base; effettuazione di attività di salvataggio e ripristino dei dati e delle configurazioni; erogazione servizio di supporto di terzo livello; supporto attraverso analisi specifiche; ecc;
  - Amministratore di rete (*Network Administrator*): gestisce, a titolo esemplificativo, le credenziali di accesso e le configurazioni di sicurezza dei dispositivi e di rete; gestisce e configura gli apparati dedicati alla sicurezza di rete e al traffico telematico all'interno di una rete di telecomunicazione; effettua attività

di manutenzione ordinaria e straordinaria sugli apparati di sicurezza e di rete; effettua attività di salvataggio e ripristino dei dati e delle configurazioni; ecc;

- Amministratore di sicurezza (*Security Administrator*): gestisce le credenziali di accesso e le configurazioni di sicurezza applicativa.

**7.2 RC\_PG\_GA\_02\_ALLEGATO B – FORMAT PER LA REVOCA DELLA DESIGNAZIONE DELL'AMMINISTRATORE DI SISTEMA**

**Revoca della nomina ad “Amministratore di Sistema”  
ai sensi del “Provvedimento” del Garante per la Protezione dei Dati Personali del 27 novembre  
2008 recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008 ss.mm.ii**

Oggetto: **Revoca della nomina ad “Amministratore di Sistema”**

Egregio/Gentile Signor/a \_\_\_\_\_,

con riferimento alla designazione ad Amministratore di Sistema, conferita ai sensi del Provvedimento del Garante Privacy del 27 novembre 2008 in materia di *“Misure ed accorgimenti prescritti ai titolari di trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”* e successive modifiche, si comunica che al momento non sussistono più i requisiti organizzativi e/o operativi per mantenere tale designazione e che, pertanto, la stessa viene revocata con effetto immediato.

Distinti saluti

Catanzaro, li \_\_\_\_\_

Il Delegato del Titolare

\_\_\_\_\_

Letto firmato e sottoscritto per accettazione  
L'Amministratore di Sistema

\_\_\_\_\_

### 7.3 RC\_PG\_GA\_05\_ALLEGATO E – FORMAT PER LA COMUNICAZIONE RELATIVA ALLA VERIFICA DEGLI ACCESSI LOGICI ALLE PIATTAFORME NAZIONALI DEGLI AMMINISTRATORI DI SISTEMA DELLA REGIONE CALABRIA

Regione Calabria  
DIPARTIMENTO/ STRUTTURA EQUIPARATA *[Inserire qui il nome]*

Spett.le xxx

**Oggetto: Verifica degli accessi logici degli Amministratori di Sistema della Regione Calabria che accedono a piattaforme nazionali**

Gentilissimi/e,

Con la presente, desideriamo portare alla Vostra attenzione l'importanza dell'adeguamento alle disposizioni del Provvedimento n. 300 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*" e successive modifiche, pubblicato dall'Autorità Garante per la Protezione dei Dati Personali.

In ottemperanza a tali disposizioni, è necessario procedere con la verifica degli accessi logici degli Amministratori di Sistema operanti sulle piattaforme nazionali da Voi gestite. Tuttavia, la Regione Calabria si trova nell'impossibilità di procedere con l'estrazione dei dati relativi agli accessi logici registrati nelle piattaforme nazionali. Pertanto, la stessa informa della responsabilità della verifica dei log gli Enti che gestiscono le piattaforme interessate. Tale collaborazione è fondamentale per assicurare la conformità alla normativa sulla Privacy e al Provvedimento sopracitato.

Rimanendo in attesa di Vostro cortese riscontro si porgono

Distinti Saluti.

## 7.4 RC\_PG\_GA\_06\_ALLEGATO F - LINEE GUIDA ED ISTRUZIONI REGIONALI PER GLI AMMINISTRATORI DI SISTEMA ESTERNI

### Regione Calabria DIPARTIMENTO/ STRUTTURA EQUIPARATA [*Inserire qui il nome*]

#### **Oggetto: Linee guida ed istruzioni regionali per gli Amministratori di Sistema esterni**

Il presente documento mira a fornire indicazioni utili ai fornitori della Regione Calabria che operano su sistemi regionali, al fine di svolgere correttamente l'attività di gestione degli Amministratori di Sistema in ottemperanza al provvedimento *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema"* (di seguito Provvedimento) pubblicato dall'Autorità Garante per la Protezione dei Dati Personali il 27 Novembre 2008 e successive modifiche.

Gli Amministratori di Sistema sono definiti nel Provvedimento dell'Autorità Garante Privacy come *"figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti"* e *"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"*. Pertanto, nelle loro consuete attività possono venire a contatto con diverse categorie di dati personali di interessati. Al fine di garantire la riservatezza, integrità e la tutela di tali dati, si riportano di seguito i punti del Provvedimento essenziali per la corretta gestione delle attività in qualità di Amministratore.

#### **1. Valutazione delle caratteristiche soggettive e selezione degli Amministratori di Sistema**

Nella fase di reclutamento e selezione degli Amministratori, si raccomanda di avere cura del rispetto dei seguenti requisiti: il ruolo da ricoprire e i requisiti necessari per la posizione; la motivazione della richiesta di integrazione dell'organico; la descrizione di lavoro; il profilo professionale richiesto; i requisiti (studi, esperienza lavorativa, competenze comportamentali e qualificazioni richieste).

Prima di procedere con l'attribuzione delle funzioni di Amministratore di Sistema, o altre figure equiparabili, si raccomanda di svolgere una valutazione preventiva delle caratteristiche di esperienza, capacità e 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.

Il processo di valutazione delle caratteristiche soggettive deve essere svolto in maniera attenta e precisa, prendendo in considerazione diversi aspetti: le competenze tecniche necessarie per svolgere le mansioni

nell'ambito di operatività previsto verificabili anche attraverso certificazioni professionali, corsi di perfezionamento, piani di training effettuati, curriculum vitae et studiorum, esperienze pregresse su tecnologie analoghe; le qualità professionali maturate dal soggetto designato in precedenti incarichi professionali; le competenze relative alla sicurezza delle informazioni e alla protezione dei dati personali comprovate dall'esperienza, dal curriculum vitae et studiorum e verificate anche in fase di selezione.

Tale attività risulta necessaria dal momento che le funzioni tipiche di un Amministratore di Sistema sono da considerarsi rischiose ai fini della disciplina della protezione dei dati personali e dunque meritevole di maggiori garanzie e controlli.

## **2. Designazione individuale degli Amministratori di Sistema**

Tutti gli Amministratori di Sistema che operano su sistemi regionali devono essere appositamente nominati in maniera individuale dal fornitore. Inoltre, nell'atto di nomina è necessario indicare, analiticamente, gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato evitando l'attribuzione di ambiti non sufficientemente dettagliati come previsto dall'art. 2-quaterdecies del decreto legislativo 101/2018 (Adeguamento al GDPR dell'ex Codice Privacy). La Regione Calabria, in qualità di Titolare, si riserva la possibilità di richiedere al fornitore le evidenze relative alle designazioni degli Amministratori che operano sui propri sistemi.

## **3. Attività di Formazione degli Amministratori di Sistema**

La formazione degli Amministratori di Sistema è un aspetto essenziale al fine di evitare la perdita, la distruzione o illecite diffusioni di dati personali. A tal fine, il fornitore deve necessariamente prevedere delle sessioni di formazione per gli Amministratori, e altre figure tecniche equiparabili, periodicamente ed almeno una volta all'anno, al fine di assicurarsi che il personale sia assolutamente consapevole dell'importanza delle tematiche di Sicurezza delle Informazioni e Protezione dei Dati. La Regione Calabria, in qualità di Titolare, si riserva la possibilità di richiedere al fornitore le evidenze relative allo svolgimento della formazione.

## **4. Verifiche degli Amministratori di Sistema**

Il Provvedimento stabilisce l'obbligo di verifica, con cadenza almeno annuale, dell'operato degli Amministratori di Sistema e, in particolare, della conformità dei trattamenti di dati effettuati con quanto richiesto dalle norme vigenti in materia di protezione di dati e sicurezza delle informazioni. La FAQ n. 5 precisa che le verifiche devono avere ad oggetto le attività svolte dall'Amministratore in virtù delle mansioni a lui attribuite, compreso il profilo della sicurezza. La FAQ n. 16 afferma, altresì, che tra i criteri di valutazione

dell'operato dell'Amministratore di Sistema è compresa l'analisi dei log raccolti, in quanto consente di verificare eventuali anomalie nella frequenza e nelle modalità degli accessi.

Il fornitore è tenuto a creare e tenere costantemente aggiornato un registro degli Amministratori di Sistema in cui siano puntualmente registrate le nomine/revoche ad Amministratore, le relative funzioni e l'ambito di operatività in conformità a quanto richiesto dal Provvedimento dell'Autorità Garante Privacy. Tale registro dovrà essere messo a disposizione della Regione Calabria in qualità di Titolare, ove richiesto.

In particolare, il Provvedimento impone di adottare meccanismi di registrazione degli accessi logici effettuati dagli Amministratori di Sistema che operano sui sistemi informativi e svolgere delle verifiche periodiche sull'operato degli stessi tramite l'analisi dei log. Nello specifico, ciascun fornitore è tenuto a svolgere le verifiche sull'operato dei propri Amministratori di Sistema che operano sui sistemi regionali. La Regione Calabria svolgerà le verifiche tramite analisi del log sui propri sistemi con cadenza semestrale.

Da ultimo, la Regione, nell'ottica di garantire una costante tutela dei dati personali degli interessati, richiede ai fornitori di adeguarsi alle misure di sicurezza predisposte dalla stessa in linea con gli standard nazionali e internazionali.

Distinti Saluti.

## 7.5 RC\_PG\_GA\_07\_ALLEGATO G – FORMAT PER LA DESIGNAZIONE DELL'AMMINISTRATORE DI SISTEMA ESTERNO

**Lettera di designazione ad “Amministratore di Sistema Esterno”**  
ai sensi del “Provvedimento” del Garante per la Protezione dei Dati Personali del 27 novembre  
2008 e ss.mm.ii.

Oggetto: **Designazione ad “Amministratore di Sistema Esterno”**

Al/Alla Sig./Sig.ra \_\_\_\_\_ nato/a a \_\_\_\_\_ il \_\_\_\_\_, matricola  
\_\_\_\_\_ qualifica \_\_\_\_\_

### PREMESSO

- che il Provvedimento Generale del Garante per la Protezione dei Dati Personali del 27 Novembre 2008 e ss.mm.ii. prevede che il Responsabile del trattamento provveda a nominare, mediante atto scritto, le figure che operano in qualità di “Amministratore di Sistema”;
- il rapporto di lavoro con Lei in essere e la Sua qualifica ed assegnazione organizzativa;
- che sono individuati quali Amministratori di Sistema coloro che svolgono le seguenti attività:
  - gestione e manutenzione di un impianto di elaborazione o di sue componenti (Technical Operator)
  - gestione dei sistemi di backup (Backup operator)
  - gestione dei profili di accesso degli utenti di un'applicazione (Profile Manager)
  - gestione di sistemi software complessi (programmatori, installatori e manutentori delle applicazioni, gestori del sistema di autenticazione) (Application Manager)
  - gestione di basi di dati (Database Administrator)
  - gestione di rete e di apparati di sicurezza (Network Administrator)
  - gestione della sicurezza (Security Administrator).
- Gli Amministratori così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati;
- 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;
- la designazione quale Amministratore di Sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

- gli estremi identificativi delle persone fisiche Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite, devono essere annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante;
- qualora l'attività degli Amministratori di Sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli Amministratori di Sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'ente o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Il Responsabile deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema;
- 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;

CON LA PRESENTE

avendo valutato che le prestazioni da Lei effettuate in via ordinaria forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza, la S.V. è designata quale "Amministratore di Sistema".

Tutte le operazioni di trattamento di dati personali saranno eseguite, con modalità e finalità decise dal Titolare. Si riportano di seguito i sistemi ICT di cui viene chiesta la gestione e le relative funzioni attribuiteLe.

Utenza	Sistema ICT da amministrare	Tipologia di amministrazione							Ambito di operatività e funzioni attribuite
		AdS di sistema	AdS di backup	AdS di accesso	AdS di software complesso	AdS di database	AdS di rete	AdS di sicurezza	

Per effetto di tale designazione e delle funzioni conseguentemente attribuite, Lei si impegna a:

- porre la massima cura nell'assicurare la protezione dei dati trattati, secondo i criteri tecnici suggeriti dalla sua esperienza e competenza professionale, allo scopo di ridurre al minimo i rischi di distruzione o perdita, intenzionale o accidentale, dei dati; accesso non autorizzato ai dati; trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento;
- assicurare l'integrità dei dati, ossia la certezza che l'informazione affidata derivi da processi di elaborazione corretti e non possa essere manipolata; la disponibilità dei dati, cioè la possibilità che l'informazione affidata sia sempre presente e utilizzabile secondo le necessità operative del Titolare/Responsabile, nei tempi concordati; la riservatezza dei dati, cioè la garanzia che l'informazione affidata ed archiviata sia accessibile solo alle persone autorizzate;
- accedere ai sistemi ICT nei limiti strettamente richiesti dall'espletamento delle Sue mansioni;

- eseguire gli accessi nel rispetto delle procedure di autenticazione a Lei già note, e di detenzione, custodia, segretezza e sicurezza delle relative credenziali di accesso;
- assicurare, per quanto di sua competenza, la disponibilità delle registrazioni (access log) di cui in Premessa. A tal proposito sarà sua cura utilizzare, per lo svolgimento delle attività riguardanti la funzione di Amministratore di Sistema, le specifiche credenziali che le sono state fornite, assicurandone la riservatezza;
- eseguire gli accessi nel rispetto delle misure di sicurezza organizzative, logiche e fisiche adottate dal Titolare del trattamento;
- attenersi alle istruzioni operative impartite;
- segnalare qualunque elemento che possa pregiudicare il corretto svolgimento delle Sue funzioni di Amministratore di Sistema e/o rendere necessarie ulteriori istruzioni;
- segnalare al Titolare/Responsabile del trattamento qualsiasi situazione che, anche potenzialmente, minacci la sicurezza dei dati e qualsiasi episodio che abbia concretamente costituito una perdita di integrità, disponibilità o riservatezza dei dati stessi;
- cooperare con il Responsabile per ogni verifica della rispondenza del Suo operato alle misure organizzative, tecniche e di sicurezza previste con riferimento ai dati personali trattati;
- garantire che i meccanismi di generazione dei log sui sistemi siano sempre attivi e producano i record richiesti, completi ed integri, inviandoli ai sistemi centrali di collazionamento del Responsabile del trattamento onde assicurarne la non modificabilità e la conservazione secondo gli obblighi vigenti;
- gestire gli interventi necessari a garantire il corretto funzionamento delle piattaforme (configurazione degli apparati di rete, erogazione in continuità dei Servizi ICT, assicurazione degli adeguati livelli di performance, controllo degli accessi degli utenti registrati, monitoraggio e segnalazione anomalie, corretta propagazione dei flussi di rete, cooperazione con i provider esterni di servizi anti DDoS, etc.), assicurando inoltre la segregazione degli ambienti coerentemente con i requisiti di sicurezza espressi dal Titolare del trattamento, sia dal punto di vista architettuale che di gestione delle regole di firewalling sui siti centrali e periferici;
- collaborare per l'attuazione delle eventuali ulteriori prescrizioni che saranno emanate dall'Autorità Garante per la Protezione dei Dati Personali in tema di Amministratori di Sistema;
- consentire il trattamento dei Suoi dati personali nei limiti e per le finalità previste dal citato Provvedimento in data 27.11.2008 dell'Autorità Garante per la Protezione dei Dati Personali, incluso la registrazione e comunicazione di ogni dato di log, ogni comunicazione a terzi, nonché la divulgazione dei Suoi dati identificativi nell'ambito delle attività organizzative.

Resta inteso e convenuto che:

- la presente designazione non configura alcuna variazione della Sua qualifica e delle Sue mansioni e del relativo trattamento economico e normativo del rapporto di lavoro con Lei in essere;
- la registrazione e comunicazione dei dati di log sarà eseguita al solo fine di ottemperare a quanto specificatamente prescritto al riguardo dal citato Provvedimento in data 27.11.2008 dell'Autorità Garante per la Protezione dei Dati Personali e non costituisce alcuna forma di controllo a distanza, neanche indiretto, della Sua attività lavorativa;
- ogni eventuale variazione dell'ambito di operatività consentito dalle Sue mansioni e dal Suo profilo di autorizzazione all'accesso ai sistemi ICT non comporterà il venir meno degli effetti della presente designazione.

Distinti saluti

li \_\_\_\_\_

Il Fornitore

\_\_\_\_\_

Letto firmato e sottoscritto per accettazione  
L'Amministratore di Sistema

\_\_\_\_\_

## NOTE PER LA COMPILAZIONE DELLA TABELLA DELLE ATTIVITA' DI TRATTAMENTO AUTORIZZATE

- **Tipologia di amministrazione** - Indicare con "X" la tipologia di amministrazione richiesta.
- **Sistema ICT da amministrare** - Si riporta un elenco di sistemi di esempio per ogni tipologia di amministrazione:
  - *amministrazione di rete* - sonde IPS/IDS, proxy server, firewall e apparati di sicurezza perimetrale, dispositivi d'instradamento del traffico (router, switch), etc.
  - *amministrazione di sistema* - sistemi Operativi, sistemi software di base, middleware, sistemi o infrastrutture di Backup, etc.
  - *amministrazione di data base* - data base management systems, data warehouse systems, big data systems, etc.
  - *amministrazione di sistemi software complessi* - sistema amministrativo centrale, sistema sanità, sistema turismo, etc.
- **Ambito di operatività e funzioni attribuite** - Si riporta un elenco di ambiti di operatività e funzioni di esempio per ogni tipologia di Amministratore:
  - Amministratore di Sistema (Technical Operator): figura professionale finalizzata alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti. Si occupa, a titolo esemplificativo, della gestione delle credenziali di accesso e delle configurazioni di sicurezza dei sistemi operativi, file system, middleware, infrastrutture; gestione e configurazione dei sistemi operativi; effettua attività di manutenzione ordinaria e straordinaria sui sistemi operativi;
  - Amministratore dei sistemi di backup (Backup Operator): effettua attività di salvataggio e ripristino dei dati, le configurazioni; ecc;
  - Amministratore che gestisce i profili di accesso degli utenti di un'applicazione (Profile Manager): gestisce i profili di accesso degli utenti di una applicazione e l'assegnazione, sospensione e cancellazione delle credenziali di autenticazione per il personale incaricato al trattamento, nonché organizza tutto il sistema di autorizzazione per le cartelle che verranno realizzate all'interno del server provvedendo alla verifica, con cadenza almeno annuale, della sussistenza delle condizioni per la conservazione di tali autorizzazioni;
  - Amministratore di sistemi software complessi (Application Manager): tra cui vi rientrano i programmatori, installatori e manutentori delle applicazioni, gestori del sistema di autenticazione. Effettua, a titolo esemplificativo, attività di manutenzione ordinaria e straordinaria sui sistemi software complessi; applica patch o pacchetti software concernenti le applicazioni gestite; effettua attività di salvataggio e ripristino dei dati e delle configurazioni; eroga servizi di supporto di terzo livello; supporta attraverso analisi specifiche, ecc;
  - Amministratore di basi di dati (Database Administrator): gestisce, a titolo esemplificativo, le credenziali di accesso e le configurazioni di sicurezza dei Data Base; la gestione e configurazione dei Data Base; effettua attività di manutenzione ordinaria e straordinaria sui

Data Base; effettuazione di attività di salvataggio e ripristino dei dati e delle configurazioni; erogazione servizio di supporto di terzo livello; supporto attraverso analisi specifiche; ecc;

- Amministratore di rete (Network Administrator): gestisce, a titolo esemplificativo, le credenziali di accesso e le configurazioni di sicurezza dei dispositivi e di rete; gestisce e configura gli apparati dedicati alla sicurezza di rete e al traffico telematico all'interno di una rete di telecomunicazione; effettua attività di manutenzione ordinaria e straordinaria sugli apparati di sicurezza e di rete; effettua attività di salvataggio e ripristino dei dati e delle configurazioni; ecc;
- Amministratore di sicurezza (Security Administrator): gestisce le credenziali di accesso e le configurazioni di sicurezza applicativa.

## 7.6 ULTERIORI ALLEGATI

ID	DESCRIZIONE	Titolo
C	Format Piano annuale per le verifiche di conformità	RC_PG_GA_03_ALLEGATO C_Format_Piano Annuale per le verifiche di conformità v.1.0
D	Format Monitoraggio attività degli Amministratori di Sistema	RC_PG_GA_04_ALLEGATO D_Format_Monitoraggio attività degli Amministratori di Sistema v.1.0
H	Formato Registro utenze abilitate su banche dati nazionali	RC_PG_GA_08_ALLEGATO H_Format_Registro utenze abilitate su banche dati nazionali v.1.0
I	Format Registro degli Amministratori di Sistema	RC_PG_GA_09_ALLEGATO I_Format_Registro degli Amministratori di Sistema v.1.0