Camera di commercio, industria , artigianato e agricoltura del Gran Sasso d'Italia

Disciplinare tecnico per le funzioni di amministratore di sistema

ai sensi del Regolamento UE 679/2016 e del Provvedimento 27/11/2008 del Garante per la protezione dei dati personali

INTRODUZIONE

La figura dell'"Amministratore di sistema" trova la sua iniziale disciplina nell'art. 1, comma 1, lett. c), del DPR n. 318/1999, laddove si parla del "*soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione*" . Si tratta di una figura con **specifiche caratterizzazioni professionali** dedicata non solo al controllo ed alla verifica della corretta funzionalità dei sistemi operativi e delle connesse apparecchiature e strumenti facenti parte di un sistema di elaborazione dati (il più delle volte organizzato a rete), ma anche mirata alla protezione dei dati trattati su tali sistemi/reti ed alla sicurezza degli stessi.

Nel Codice della privacy (D.Lgs. n. 196/2003), detta figura non è stata prevista, restando menzionata, solo indirettamente, nell'ambito del suo Allegato B), in relazione alla gestione del *back-up*, del [disaster] *recovery*, delle credenziali di autenticazione e dei profili di autorizzazione.

Il Garante per la protezione dei dati personali ha colmato la lacuna con un provvedimento generale 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"), emanato ai sensi dell'art. 154, lett. c), del testo precedentemente in vigore del citato Codice.

Il provvedimento, poi aggiornato, delinea ancora la materia, precisando che "in assenza di definizioni normative e tecniche condivise (…), l'amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (*Enterprise resource planning*) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali".

In altri termini, la figura dell'amministratore di sistema è necessaria qualora vi sia una condivisione, nell'ambito del sistema informatico/telematico gestito, di archivi contenenti dati personali. Data la rilevanza delle funzioni svolte, il Garante ha imposto ai Titolari misure di sicurezza e di carattere tecnico e organizzativo che prevedono la selezione dei candidati sulla base di comprovate capacità tecniche, l'assegnazione ai soggetti individuati di adeguati livelli di responsabilità aziendale e la definizione e implementazione di procedure tecniche di supervisione e controllo sull'operato svolto.

Devono infatti essere valutate con attenzione l'esperienza, le capacità, e l'affidabilità della persona chiamata a ricoprire il ruolo di amministratore di sistema, che deve essere in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali, compreso il profilo della sicurezza.

Il GDPR non fa parola della figura dell'amministratore di sistema dandola, in un certo senso, per presupposta dato che la maggior parte dei trattamenti sono oggi effettuati attraverso la gestione di reti, database ed altri sistemi complessi ed interconnessi. Pertanto le prescrizioni contenute nel provvedimento del Garante restano applicabili in un contesto normativo "riconfigurato" sulla base dei principi e delle prescrizioni contenute in detto GDPR.

In questo contesto appare utile che l'Ente disponga di un documento generale con il quale:

- comprovare, tra l'altro, la consapevolezza e la chiara conoscenza da parte degli Organi dell'Ente (cui compete la titolarità dei trattamenti), delle proprie responsabilità;
- comprovare l'adozione delle misure tecniche e organizzative ritenute adeguate;
- documentare, ed essere in grado di dimostrare, in caso di verifiche delle competenti autorità, la conformità dei trattamenti alle prescrizioni del GDPR.

Detto Regolamento prevede, infatti, la dimostrazione del livello di responsabilizzazione dell'Ente (c.d. *accountability*), ovvero non solo la conoscenza dei principi da osservare nei trattamenti di dati personali ma anche la cognizione dei rischi connessi e correlati a tali trattamenti, compresi quelli derivanti dalle attività degli Amministratori di sistema.

Più precisamente, l'art. 5 del GDPR individua nel Titolare il soggetto competente a garantire il rispetto dei principi posti dalla nuova disciplina in tema di trattamento dei dati personali e, all'art. 24, stabilisce che detto Titolare debba mettere in atto (nonché riesaminare ed aggiornare) adeguate misure tecniche ed organizzative, per garantire ed essere in grado di dimostrare che le operazioni di trattamento vengano effettuate in conformità ai principi fondamentali della disciplina in materia.

Continuano a sussistere, pertanto, per i Titolari dei trattamenti, i seguenti obblighi indicati dal Garante:

a) **designare individualmente i singoli amministratori di sistema**, a mezzo di un atto che deve elencare analiticamente gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

b) **riportare in un documento interno (disponibile in caso di accertamenti da parte del Garante) gli estremi identificativi delle persone fisiche designate amministratori di sistema, con l'elenco delle funzioni ad esse attribuite.** Nel caso in cui i servizi di amministrazione di sistema siano esternalizzati, l'elenco può essere conservato, indifferentemente, sia dal Titolare che dal Responsabile esterno del trattamento[1];

c) **adottare idonei sistemi di controllo che consentano la registrazione degli accessi logici da parte degli amministratori ai sistemi di elaborazione e agli archivi elettronici.** L'accesso di ciascun amministratore (*access log*), quindi, deve essere registrato e conservato per almeno 6 mesi, con caratteristiche di completezza, integrità ed inalterabilità e deve comprendere anche i riferimenti temporali, la descrizione dell'evento e del sistema coinvolto;

d) **rendere noto ai lavoratori dipendenti il loro diritto di conoscere l'identità degli amministratori di sistema** che, nell'espletamento delle proprie mansioni, trattino dati personali dei lavoratori e, ovviamente, fornire le relative informazioni[2];

e) **verificare, con cadenza almeno annuale, la effettiva conformità dell'operato degli amministratori di sistema** rispetto alle mansioni loro attribuite, con riferimento anche alle prescrizioni del GDPR.

OBIETTIVI DEL DOCUMENTO

Di seguito, a seguito delle prescrizioni generali contenute nel GDPR, si formalizza lo schema per le misure e gli accorgimenti tenuti dalla Camera di commercio del Gran Sasso d'Italia, in relazione al citato Provvedimento a carattere generale del 27 novembre 2008, con il quale il Garante ha disposto "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", come successivamente modificato con il provvedimento del 25 giugno 2009.

Il presente documento risponde all'esigenza – sottolineata dal citato provvedimento del Garante - di definire compiutamente le **funzioni** ed i limiti di intervento dei soggetti preposti ad attività riconducibili alle mansioni tipiche dei c.d. "amministratori di sistema", nonché di coloro che svolgono mansioni analoghe in rapporto a sistemi di elaborazione e banche di dati e/o di gestione e custodia di banche dati.

In particolare, il documento intende:

a. **evidenziare la rilevanza e delicatezza di tali peculiari mansioni** rispetto ai trattamenti di dati personali svolti da altri soggetti autorizzati/designati/delegati, diversi dagli "Amministratori di sistema", per le funzioni istituzionali proprie dell'Ente;
b. **consentire più agevolmente, nei dovuti casi, la conoscibilità per gli interessati** dell'esistenza di tali figure o di ruoli analoghi svolti in relazione a talune fasi del trattamento;
c. **definire specifiche cautele nello svolgimento delle mansioni** assegnate agli amministratori di sistema, unitamente ad accorgimenti e misure, tecniche e organizzative, volte ad agevolare

[1] Nel caso di "esternalizzazione" o, comunque, di affidamento all'esterno delle funzioni di amministratore di sistema ad un imprenditore non individuale, le persone fisiche che svolgeranno materialmente le attività di amministratore di sistema debbono possedere esperienza, capacità ed affidabilità tecnica adeguatamente comprovata.

[2] Il citato provv. del Garante, sulla questione ha stabilito che, laddove l'attività degli amministratori di sistema, "(…)*, anche solo indirettamente, possa riguardare servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori; nel qual caso i titolari pubblici e privati, nella qualità di datori di lavoro, vengono chiamati a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati 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".*

l'esercizio dei doveri di controllo da parte del Titolare o del Responsabile del trattamento (c.d. *due diligence*).

Il presente documento è strettamente integrato con quanto riportato, in particolare, nei seguenti documenti con i quali la Camera di commercio ha effettuato l'adeguamento al GDPR:

- Il *Modello organizzativo con indicati i ruoli ed il sistema di responsabilità nel trattamento dei dati*;
- **le *Linee guida per l'affidamento delle responsabilità a soggetti esterni*;**
- il *Disciplinare tecnico per l'utilizzo degli strumenti informatici, telematici e principali misure di sicurezza;*
- la *Procedura per la predisposizione di una valutazione di impatto sulla protezione dei dati personali (DPIA)*.

RIFERIMENTI NORMATIVI ESSENZIALI

Il presente documento risponde ai seguenti requisiti normativi:

1. Regolamento UE 679/2016;
2. Soggetti che trattano dati "per conto" e sotto l'autorità del Titolare del trattamento (artt. 28-29 del GDPR);
3. Garante per la protezione dei dati personali, Provvedimento generale 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" (in G.U. n. 300 del 24 dicembre 2008), come successivamente modificato con il provvedimento del 25 giugno 2009.

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE n. 679/2016 (General Data Protection Regulation)
Codice	D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" (come modificato dal D.Lgs. n. 101/2018)
Garante	Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati)
RPD/DPO	Responsabile della Protezione dei Dati/ *Data Protection Officer*
Delegato del Titolare	Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR
SG	Segretario Generale della Camera di commercio del Gran Sasso d'Italia
VSG	Vice Segretario Generale della Camera di commercio del Gran Sasso d'Italia

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione
26/02/2021	Approvato	Prima emissione	Determina del Vice Segretario Generale Vicario f.f. del 26/02/2021

INQUADRAMENTO DEGLI AMMINISTRATORI DI SISTEMA

Con la definizione di "**Amministratore di sistema**" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Il presente documento prende in considerazione come tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati *(database administrator)*, gli amministratori di reti e di apparati di sicurezza *(network & security administrator)* e gli amministratori di sistemi software complessi *(system administrator)*.

Il presente documento riguarda, quindi, le seguenti figure:

database administrator	specializzato nella progettazione ed amministrazione di basi di dati e in tutti gli aspetti di sicurezza, disponibilità, integrità e delle relative *performance*.
network & security administrator	specializzato in reti di calcolatori e relativi apparati di *networking* come *router*, *bridge* e *switch*, il suo compito principale è gestire la rete, progettando politiche di sicurezza di base e sistemi di accesso remoto sicuri.
system administrator	gestisce i sistemi ed i servizi di rete; è in grado di risolvere qualsiasi problematica di rete aziendale sia locale che remota, sia lato *client* che lato *server*.

Gli amministratori di sistema così ampiamente individuati, pur non essendovi preposti istituzionalmente, possono anche "solo incidentalmente" trovarsi nella necessità di trattare dati personali[3] ai soli fini dell'espletamento delle loro consuete attività, ovvero sono concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

IDENTIFICAZIONE, NOMINA E FUNZIONI DEGLI AMMINISTRATORI DI SISTEMA

Anche al fine di assicurare un sistema di **conoscibilità dell'identità degli Amministratori di sistema,** quale forma di trasparenza interna all'organizzazione a tutela dei lavoratori, nel caso in cui tali figure trattino anche dati personali riferiti a questi ultimi, di seguito si riportano le modalità di individuazione, nomina e gli elementi identificativi sia delle risorse interne che esterne che svolgono tali funzioni.

AMMINISTRATORI DI SISTEMA INTERNI

INDIVIDUAZIONE E NOMINA

Il Vice Segretario Generale Vicario f.f. , "delegato del Titolare/Responsabile del trattamento" secondo le deleghe-procure ricevute, ha provveduto ad individuare i soggetti interni che attualmente svolgono funzioni e detengono credenziali da Amministratori di sistema, provvedendo a verificarne esperienza, capacità ed affidabilità in relazione alle specifiche funzioni e sistemi affidati. La verifica è stata condotta in relazione alle **qualità tecniche, professionali e di affidabilità** dei soggetti da nominare[4].

Tali criteri di selezione, **equipollenti a quelli richiesti per la nomina dei responsabili del trattamento** dall'art. 28, par. 1 del GDPR, sono finalizzati ad assicurare che i soggetti individuati diano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Nell'eventualità di attivazione di **nuove credenziali da amministratore**:

a) nel caso in cui siano affidate a soggetti già compresi nel registro di cui al paragrafo successivo, la valutazione deve ritenersi come già effettuata;
b) nel caso siano affidate a soggetti diversi, il Responsabile/Referente di Area/Ufficio/Servizio cui fa capo la responsabilità del sistema da amministrare deve condividere la scelta dell'incaricato con il

---

[3] Intendendosi con tale locuzione non solo la "conoscibilità" dei dati ma anche l'abilitazione per la modifica/estrazione dei dati.

[4] Lo stesso provvedimento del Garante specifica che la verifica non deve riguardare "requisiti morali" ma esclusivamente professionali.

"delegato del Titolare", che provvederà alle valutazioni di cui al presente paragrafo, e di cui darà menzione nella lettera di nomina individuale.

La nomina di ciascun Amministratore di sistema è effettuata con una **lettera di incarico individuale**, controfirmata dall'interessato per presa visione, in cui sono specificati i trattamenti cui sono autorizzati ed i compiti che gli sono stati affidati.

Al perfezionamento della nomina, ovvero almeno una volta all'anno, **il delegato del Titolare provvede** ad aggiornare il Registro di cui al paragrafo che segue.

REGISTRO DEGLI AMMINISTRATORI DI SISTEMA INTERNI E DELLE RELATIVE FUNZIONI

			FUNZIONI				
SERVIZIO/APPLICATIVO/DB GESTITO	**DESCRIZIONE**	**NOMINATIVI AMMINISTRATORI DI SISTEMA**	GESTIONE CREDENZIALI	GESTIONE BACKUP	GESTIONE ANTINTRUSIONE	LOG MANAGEMENT	MANUTENZIONE ED ASS.ZA
Rete lan e voip	Infrastruttura rete telematica e telefonica interna (apparati hardware e software)	Amministratore interno	✓	✓	✓		✓
Applicativi Infocamere	Assistenza di primo livello ai colleghi e gestione rapporti con assistenza di secondo livello Infocamere (Apertura ticket e gestione risposte)	Amministratore interno	✓				✓
PC e stampanti postazioni di lavoro individuali	Personal Computer e stampanti assegnati ai dipendenti e assimilati della CCIAA del Gran Sasso	Amministratore interno	✓	✓	✓	✓	✓
Time Work Solari	Sistema rilevazione informatica delle presenze (apparati hardware e software)	Amministratore interno	✓	✓	✓	✓	✓
Sistema di video - conferenza	Sistemi telematici di collegamento remoto audio e video, individuali e di gruppo	Amministratore interno	✓		✓	✓	✓
Sale multimediali	Postazioni multimediali - Apparati audio e video	Amministratore interno	✓		✓	✓	✓
Stampanti di rete	Fotocopiatrici multifunzione (copie-stampe di rete-scansioni remote)	Amministratore interno	✓	✓	✓	✓	✓
Firma digitale	Emissione e rinnovo CNS (Token Usb – Smartcard) – Master RAO	Amministratore interno	✓				✓
Spid	Assistenza ottenimento Identità Digitale	Amministratore interno	✓				✓
Start up	Assistenza Qualificata alle Imprese di nuova costituzione – Gestione Applicativi	Amministratore interno	✓				✓

COMPITI E RESPONSABILITÀ DEGLI AMMINISTRATORI DI SISTEMA

In generale, gli Amministratori di sistema **non effettuano trattamenti di dati personali se non in via incidentale**, nell'ambito delle mansioni affidate e di seguito riassunte in termini meramente esemplificativi.

Qualora a tali soggetti siano affidati trattamenti di dati personali non inerenti tali mansioni specifiche, queste operazioni ricadono nelle autorizzazioni formalizzate nell'ambito della nomina ad incaricato del trattamento.
Nell'esercizio delle funzioni affidate, gli Amministratori di sistema devono:

- rispettare le disposizioni impartite dal "delegato del Titolare/Responsabile" attraverso i documenti che costituiscono il sistema di gestione della privacy della Camera di commercio del Gran Sasso d'Italia;
- rispettare le eventuali indicazioni ed istruzioni ricevute dal Titolare/Responsabile del trattamento in relazione alle modalità di svolgimento delle mansioni di Amministratore di sistema, in conformità al provvedimento del Garante citato in premessa;
- garantire che i trattamenti vengano effettuati rispettando la riservatezza, ovvero il segreto di ufficio, su tutte le informazioni acquisite nell'espletamento delle attività affidate;
- trattare i dati personali secondo i principi applicabili al trattamento indicati all'art. 5 del GDPR;
- trattare tutti i dati **esclusivamente** per i compiti assegnati dal Titolare/Responsabile del trattamento ed in coerenza con le finalità istituzionali inerenti l'attività svolta.

A ciascun Amministratore, a seconda del sistema gestito, può essere affidata **una o più delle funzioni di seguito identificate**:

- ✓ 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* amministrativo;
- ✓ attivare le credenziali 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 dall'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 (ovvero segnalare prontamente al Titolare/Responsabile del trattamento la necessità di farlo) tutti i provvedimenti necessari ad evitare o ridurre il rischio della perdita o della distruzione dei dati;
- ✓ sovraintendere alle operazioni di *back-up* periodico degli stessi con copie di sicurezza, ovvero, se del caso, alle operazioni di *disaster recovery*;
- ✓ assicurarsi della qualità delle copie di sicurezza dei dati ed applicare i criteri per la conservazione, il riutilizzo e/o la distruzione delle copie di sicurezza delle banche dati[5];
- ✓ segnalare tempestivamente al delegato del Titolare eventuali rischi o anomalie nella gestione delle misure di sicurezza relative ai dati personali;
- ✓ prestare la collaborazione tecnica richiesta dal Titolare in caso di effettuazione della DPIA;
- ✓ prestare ogni supporto utile allo svolgimento delle attività del RPD.

Nella realizzazione delle suesposte attività tecniche, gli amministratori di sistema devono garantire – ove tecnicamente possibile – il rispetto delle misure di sicurezza di natura tecnologica, organizzativa e procedurale definite come obbligatore per le Pubbliche amministrazioni e per le società a controllo pubblico dalla Circolare AgID n. 2 del 18 aprile 2017 "**Misure minime di sicurezza ICT per le pubbliche amministrazioni**" (livello minimo), cui la Camera di commercio del Gran Sasso si è adeguata, *fermo restando che tali misure possono non essere sufficienti, per il rispetto delle prescrizioni del GDPR, che non prevede più misure "minime" bensì misure "adeguate"*. La decisione di adeguatezza delle misure è competenza del Titolare.

[5] Anche in applicazione del Provvedimento del Garante Privacy del 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali", in G.U. n. 287 del 9 dicembre 2008.

La qualifica di amministratore di sistema può costituire, a particolari condizioni, una **specifica aggravante** (c.d. **abuso della qualità di operatore di sistema**[6]) nei casi previsti dalle seguenti fattispecie di reato, contenute nel codice penale:

- accesso abusivo a sistema informatico o telematico (art. 615 *ter*);
- frode informatica (art. 640 *ter*);
- danneggiamento di informazioni, dati e programmi informatici (artt. 635 *bis* e 635 *ter*);
- danneggiamento di sistemi informatici e telematici (artt. 635 *quater* e 635 *quinquies*).

SERVIZI DI AMMINISTRAZIONE DI SISTEMI AFFIDATI A TERZI

Alcuni applicativi e relativi database nonché servizi informatici e telematici sono acquisiti dalla Camera di commercio da fornitori esterni; a questi fornitori, in alcuni casi, l'Ente ha affidato anche la manutenzione, l'aggiornamento e l'amministrazione nel tempo di tali sistemi[7].

Il provvedimento del Garante prevede che nel caso di servizi di amministrazione di sistema affidati in outsourcing, ciò avvenga **nell'ambito della designazione a Responsabile esterno del trattamento** (che in questi casi è quindi necessariamente effettuata). Gli estremi identificativi delle persone fisiche preposte all'amministrazione dei sistemi possono essere, in questo caso, conservati direttamente e specificamente dal Responsabile esterno, per ogni eventuale evenienza[8].

NOMINA

In tutti i casi in cui la Camera di commercio debba acquisire servizi di amministrazione di sistema, il **responsabile unico del procedimento** - in conformità con i compiti assegnati nell'ambito del modello organizzativo per la gestione degli adempimenti privacy e tenuto conto delle procedure previste dalla legge – provvede a:

- coinvolgere formalmente il Dirigente/Responsabile dell'U.O. che abbia espresso il relativo fabbisogno di acquisto per la definizione di specifici requisiti soggettivi e di affidabilità che il fornitore deve garantire e/o per la individuazione degli adempimenti gestionali e tecnici che dovranno essere garantiti, in ragione della tipologia di dati e dei trattamenti da eseguire sugli stessi ovvero in quanto imposti contrattualmente dal Titolare del trattamento (per i sistemi e servizi acquisiti per lo svolgimento di una commessa)
- effettuare, in fase di selezione, una verifica sull'esperienza, capacità ed affidabilità dello stesso, al fine di verificare che il soggetto cui sono assegnate attività critiche per la Camera di commercio fornisca idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza (art. 28 del GDPR); tali verifiche e le conseguenti valutazioni devono essere riportate nei "considerata" che costituiscono il presupposto di legittimità degli atti di affidamento[9]);
- regolamentare le responsabilità in materia di trattamento dei dati personali con apposita lettera di nomina a Responsabile esterno di trattamento con funzioni di amministrazione di sistema (controfirmata per accettazione dal contraente) e prevedendo nel contratto/convenzione sottoscritti dalle parti istruzioni specifiche e penalità contrattuali in caso di inadempienza, fino al recesso per giusta causa per violazione di legge[10].

ELENCO DEGLI AMMINISTRATORI DI SISTEMA IN OUTSOURCING E DELLE RELATIVE FUNZIONI

Di seguito si riporta la tabella riepilogativa dei soggetti esterni cui la Camera di commercio ha attualmente affidato in outsourcing funzioni di amministratore di sistema, con il dettaglio delle funzioni svolte.

---

[6] Gli Amministratori di sistema sono dei particolari "operatori di sistema", dotati di specifici privilegi.

[7] E' il caso, ad esempio, del rapporto con InfoCamere (che non rientra, ovviamente, tra i fornitori "esterni" essendo una società *in house* del sistema camerale).

[8] Cfr. il par. 2, lett. d), del Provvedimento del Garante.

[9] Sia nel caso in cui il provvedimento costituisca l'ultimo atto di una procedura di gara ad evidenza pubblica, sia che l'affidamento venga effettuato mediante trattativa privata.

[10] Si rinvia a quanto indicato nel documento, *Linee guida per l'affidamento delle responsabilità a soggetti esterni.*

			FUNZIONI				
SERVIZIO/APPLICATIVO/ DB GESTITO	**DESCRIZIONE**	**NOMINATIVI AMMINISTRATORI DI SISTEMA**	GESTIONE CREDENZIALI	GESTIONE BACKUP	GESTIONE ANTINTRUSIONE	LOG MANAGEMENT	MANUTENZIONE ED ASS.ZA
Rete lan e voip	Infrastruttura rete telematica e telefonica interna (apparati hardware e software)	Infocamere	✓	✓		✓	✓

LOG MANAGEMENT

Il provvedimento del Garante prevede che i Titolari di trattamento adottino **sistemi idonei alla registrazione degli accessi logici** (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.

Come prescritto dal Garante le registrazioni, da conservare per un congruo periodo comunque non inferiore a sei mesi, devono riguardare esclusivamente gli ***access log***, ovvero gli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software.

La registrazione deve contenere i seguenti ***event records***: i riferimenti alla "*username*" utilizzato, alla data e all'ora dell'evento (*timestamp*), una descrizione dell'evento di accesso (sistema di elaborazione o software utilizzato, se si tratti di un evento di *log-in*, di *log-out*, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato, etc.).

Non devono invece essere sottoposti a registrazione i dati sull'attività interattiva (comandi impartiti, transazioni effettuate) degli amministratori di sistema. Qualora il sistema di *log* adottato generi una raccolta dati più ampia, la registrazione ai fini del presente documento deve essere limitata agli elementi sopra identificati, opportunamente estratti e/o filtrati.

Le registrazioni devono avere caratteristiche di **completezza, inalterabilità e possibilità di verifica della loro integrità** adeguate al raggiungimento dello scopo di verifica per cui sono richieste. In particolare si intende per:

- **completezza**: tale caratteristica è riferita all'insieme degli eventi censiti nel sistema di *log*, che deve comprendere tutti gli eventi di accesso interattivo che interessino gli amministratori di sistema su tutti i sistemi di elaborazione con cui vengono trattati, anche indirettamente, dati personali;
- **inalterabilità**: tale requisito è finalizzato a garantire che i *log* registrati non siano stati alterati da soggetti con competenze idonee (ad es., dagli stessi amministratori di sistema);
- **verificabilità:** tale requisito riguarda la possibilità che i dati così raccolti, completi ed integri, possano essere utilizzati per effettuare le verifiche di cui alla successiva sezione; ad es., possono costituire oggetto di verifica eventuali anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso, etc.).

VERIFICHE SUI LOG

Per le verifiche sui *log* si rinvia, inoltre, a quanto contenuto nel documento *Disciplinare tecnico per l'utilizzo degli strumenti informatici, telematici e principali misure di sicurezza* ed a quanto è eventualmente stabilito dal Titolare nell'ambito della nomina degli Amministratori di sistema.

FORMAZIONE

Nell'ambito del programma di formazione sulla sicurezza, nonché di quello permanente sulla tutela dei dati personali, L'Ente svolge attività di informazione e formazione con riferimento ai contenuti del presente Disciplinare.

VERIFICA DELLE ATTIVITÀ

L'operato degli Amministratori di sistema deve essere soggetto, con cadenza almeno annuale, ad un'attività di **verifica da parte del Titolare/Responsabile del trattamento**, in modo da controllare la rispondenza dell'attività svolta nell'esercizio di tali funzioni rispetto alle mansioni attribuite nonché alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

Le modalità e le tempistiche delle verifiche sono indicate nell'atto di nomina dell'Amministratore di sistema, ovvero in successive o ulteriori istruzioni comunicate dal Titolare/Responsabile del trattamento.

L'attuazione di un sistema di **monitoraggio, verifica e controllo** del sistema privacy implementato rispetto alla normativa ed alle direttive ed istruzioni impartite, anche attraverso la previsione e

realizzazione di *audit*, è una specifica competenza del RPD della Camera di commercio, secondo quanto indicato nei documenti con i quali l'Ente si adegua al GDPR.

Nell'ambito di tale funzioni, sono stati pianificati vari livelli di monitoraggio:

- ✓ analisi delle segnalazioni e degli *incident report* (situazioni anomale o incidenti di sicurezza) effettuate dagli Amministratori di sistema interni ovvero dai fornitori di applicativi e servizi di supporto in outsourcing, con definizione delle azioni preventive/correttive da apportare e verifica della applicazione delle stesse (cfr. procedura di gestione dei *data breach*)[11];
- ✓ analisi delle relazioni circa la valutazione dell'operato degli Amministratori di sistema effettuate da soggetti terzi nominati responsabili di trattamento per tali specifiche attività;
- ✓ analisi delle risultanze del sistema di *log management* interno, la cui durata di conservazione è quindi stabilita in 1 (uno) anno. Alla scadenza dell'anno ed a seguito delle attività di verifica, nel caso non siano riscontrate anomalie, i supporti rimovibili contenenti i *log* devono essere distrutti, fatti salvi eventuali obblighi di conservazione stabiliti da specifiche disposizioni di legge.

Gli esiti dell'attività di verifica devono essere formalizzati in forma di **rapporto di audit**, evidenziando almeno:

1. eventuali eventi anomali o incidenti di sicurezza;
2. le attività effettuate in proposito dalle figure identificate come amministratori di sistema, specificando se esse sono risultate congrue e idonee alla risoluzione delle problematiche;
3. una indicazione delle eventuali vulnerabilità che hanno consentito l'attualizzarsi dell'evento;
4. l'eventuale quantificazione del danno occorso ai sistemi, reti o database (in termini qualitativi e/o quantitativi).

Per facilitare l'attività di riesame del Titolare/Responsabile del trattamento, il rapporto di *audit* deve indicare:

- ✓ le eventuali azioni di miglioramento (preventive/correttive);
- ✓ la pianificazione in termini economici degli interventi;
- ✓ la schedulazione delle attività;
- ✓ i risultati attesi dall'eventuale adozione delle contromisure proposte.

Le risultanze delle verifiche effettuate dal Titolare/Responsabile del trattamento sono comunicate al RPD che – anche attraverso il ricorso ad apposite professionalità – può effettuare ulteriori verifiche ai sensi di quanto previsto dall'art. 39, par. 1, lett. a), del GDPR.

[11] Di cui al documento, *Procedura di gestione dei data breach.*