MISURE DI SICUREZZA E ACCORGIMENTI PRESCRITTI AI TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI RELATIVAMENTE ALLE ATTRIBUZIONI DELLE FUNZIONI DI AMMINISTRATORE DI SISTEMA

Titolare del Trattamento	Diocesi di Sabina – Poggio Mirteto
Indirizzo sede legale	Via Mario Dottori, 14 – 02047 Poggio Mirteto (RI)
Codice Fiscale	91000810571
PEO	diocesi@diocesisabina.it
Presidente pro-tempore	S.E. Mons. Ernesto MANDARA
Responsabile ITC	
DPO	Giuliano PALOTTO

Edizione	Revisione	Data	Descrizione	il Resp. ITC	il Titolare	il DPO
1	0	04/03/2024	Prima emissione	*fatto*	*approvato*	*visto*

Documento di nr 5 (cinque) pagine compresa la presente realizzato su format della

PREMESSA

Con la definizione di "*amministratore di sistema*" si individuano, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente vengono però considerate tali anche 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.
Gli *amministratori di sistema* così ampiamente individuati nelle loro consuete attività sono, in molti casi, concretamente "*responsabili*" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.
Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "*in chiaro*" le informazioni medesime.
La rilevanza, la specificità e la particolare criticità del ruolo dell'*amministratore di sistema* sono state considerate anche dal Diritto dell'Unione, da quello nazionale e dai provvedimenti dell'Autorità i quali hanno individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante.
Ci si riferisce, in particolare:

- 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 ter),
- danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinques).

In definiva l'Amministratore di sistema è individuato quale "*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*".

MISURE DI SICUREZZA E ACCORGIMENTI PER I TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI

Di seguito sono indicati gli accorgimenti e le misure di sicurezza e gli accorgimenti per i trattamenti di dati personali effettuati con strumenti elettronici, esclusi quelli effettuati a fini amministrativo-contabili.
I seguenti accorgimenti e misure lasciano impregiudicata l'adozione delle cautele fin qui adottate in quanto ricomprese nel presente e quelle successivamente adottate anche senza comportare revisione al presente, sulla scorta dell'evoluzione tecnologica e dei costi di attuazione.

Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di *amministratore di sistema* avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Designazioni individuali

La designazione quale *amministratore di sistema* è in ogni caso individuale e reca l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, sono riportati 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, il Titolare del trattamento, nella sua qualità di datore di lavoro, rende nota la loro identità a tutti i lavoratori.
Nel caso di servizi di *amministrazione di sistema* affidati in outsourcing il Titolare del trattamento conserva direttamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

Verifica delle attività

L'operato degli *amministratori di sistema* è oggetto, con cadenza almeno annuale, di un'attività di verifica, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Registrazione degli accessi

Sono 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*) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
Le registrazioni comprendono 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**.

RESPONSABILITÀ DELL'AMMINISTRATORE DI SISTEMA

La funzione ha lo scopo di garantire il regolare funzionamento dell'infrastruttura tecnologica aziendale e il corretto utilizzo della stessa da parte degli utenti interni ed esterni all'organizzazione. Quindi, in virtù di queste sue funzioni, l'amministratore di sistema svolge attività che comportano un'effettiva capacità di azione sul dato, anche quando non consulti in chiaro il dato stesso.

Primo adempimento

L'amministratore di sistema garantisce:

- ✓ conoscenza dell'ambito di gestione dei sistemi (es. esperienza, possesso di certificazioni, ecc.);
- ✓ conoscenza della normativa vigente e delle best practice di riferimento in materia di gestione della sicurezza dei sistemi informatici;
- ✓ consapevolezza dei rischi di sicurezza derivanti da errori/violazioni nell'ambito della gestione dei sistemi.

Secondo adempimento

Il Titolare del trattamento, nell'ambito dell'assegnazione individuale del compito di *amministratore di sistema*, assicura:

- ✓ la formalizzazione di ruoli e funzioni (*segregation of duties*);
- ✓ la definizione dei profili di autorizzazione (es. aree applicative, aree funzionali, ambiti tecnologici, etc.) nel rispetto del *need to know* e *least privilege*;
- ✓ l'assegnazione di utenze nominative.

Terzo adempimento

Il Titolare del trattamento delega apposita funzione atta alla predisposizione di un processo volto a garantire:

- ✓ l'identificazione degli amministratori di sistemi, reti, basi di dati, software complessi e apparati di sicurezza, che hanno potenzialità di agire su dati personali;
- ✓ l'aggiornamento dell'elenco amministratori di sistema, specificando il ruolo e i sistemi amministrati;
- ✓ la presenza, in caso di servizi affidati in outsourcing, di un elenco degli amministratori esterni.

Quarto adempimento

Il Titolare del trattamento ha presidi e processi volti a garantire:

- ✓ l'identificazione del perimetro dei sistemi (es. applicazioni);
- ✓ l'impostazione log per la tracciatura degli eventi di "*login*", "*logout*" e "*login failure*" degli amministratori di sistema;
- ✓ l'attuazione di misure di raccolta, conservazione e cancellazione dei log;
- ✓ l'attuazione delle misure volte ad assicurare l'integrità dei log.

Quinto adempimento

Con cadenza non superiore ai dodici mesi, il titolare del trattamento verifica, a titolo esemplificativo:

- ✓ il log degli accessi;
- ✓ la conservazione dei log per il tempo stabilito (almeno 6 mesi);
- ✓ l'effettivo utilizzo di sole utenze nominali in coerenza con l'elenco degli amministratori designati;
- ✓ la frequenza degli accessi e loro modalità (es. orari, durata, sistemi cui si è fatto accesso);
- ✓ l'attribuzione di azioni alle persone fisiche, attraverso la creazione di account nominali per l'accesso al sistema;
- ✓ l'eventuale segregazione di account di gruppo, con criteri di custodia delle password non nominali e assegnazione a seguito di richiesta espressa e motivata;
- ✓ la limitazione dell'accesso ai log prodotti, mediante l'utilizzo di specifici meccanismi di protezione dell'integrità e della completezza dei log;
- ✓ la previsione di registrazione di dati ben precisi per il tracciamento delle attività:
  - o user-id che ha eseguito l'operazione,
  - o data e ora in cui è stata richiesta ed eseguita l'operazione,
  - o tipologia di evento che ha attivato il tracciamento,
  - o risorse informatiche interessate,
  - o risultato dell'azione eseguita,

- tentativi di corruzione delle informazioni gestite dal sistema (modifica di programmi eseguibili, crash di sistema, etc.),
- tentativi di violazione ed effettive violazioni della sicurezza, intenzionali e non, commessi da amministratori interni o esterni (login falliti, richieste di accesso a risorse non autorizzate, contagi da virus informatici, etc.).

Del processo di verifica viene redatto apposito verbale conservato a cura del Titolare del trattamento.

L'AMMINISTRATORE DI SISTEMA IN RELAZIONE AL GDPR

Il GDPR non prevede specifiche disposizioni relative alla figura dell'*amministratore di sistema*. Tuttavia, dall'analisi complessiva del Regolamento europeo emergono vari elementi riconducibili alla figura, al ruolo e alle responsabilità dell'amministratore di sistema. In particolare:

- la nomina di amministratori di sistema contribuisce al rispetto dei princìpi fondamentali in materia di protezione dei dati personali che ogni organizzazione è tenuta ad osservare (art. 5 GDPR);
- l'amministratore di sistema ha il compito di sviluppare le misure cosiddette di privacy by design e privacy by default (art. 25 GDPR), quali ambiti di operatività rispetto ai quali può svolgere un ruolo non secondario di progettazione e di innovazione dei processi organizzativi;
- la nomina di un amministratore di sistema rappresenta senza dubbio per il titolare del trattamento un elemento di accountability ai sensi dell'art. 24 GDPR;
- la presenza di amministratori di sistema costituisce senza dubbio un'attuazione concreta dell'adozione di misure di sicurezza adeguate al rischio di cui all'art. 32 GDPR.

Sommario

PREMESSA 2
MISURE DI SICUREZZA E ACCORGIMENTI PER I TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI 2
Valutazione delle caratteristiche soggettive 2
Designazioni individuali 3
Elenco degli amministratori di sistema 3
Verifica delle attività 3
Registrazione degli accessi 3
RESPONSABILITÀ DELL'AMMINISTRATORE DI SISTEMA 3
Primo adempimento 3
Secondo adempimento 4
Terzo adempimento 4
Quarto adempimento 4
Quinto adempimento 4
L'AMMINISTRATORE DI SISTEMA IN RELAZIONE AL GDPR 5