ASL DI RIETI

POLICY AZIENDALE IN MATERIA DI AMMINISTRATORE DI SISTEMA

Sommario

PREMESSA

La presente procedura aziendale ha per le modalità di nomina, di attribuzione delle funzioni e di monitoraggio e controllo delle attività svolte dagli Amministratori di sistema, con particolare riguardo all'adozione di specifiche cautele e garanzie per lo svolgimento delle loro mansioni, nel rispetto di quanto prescritto dal Provvedimento dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 recante "*Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di sistema*", come modificato e integrato con successivo Provvedimento del 25 giugno 2009.

In attuazione dell'art. 5 del Regolamento Europeo 679/2016, nell'ottica del principio di "*accountability*", con la presente policy aziendale l'Asl di Rieti intende definire, in modo certo, codificato e trasparente, soggetti, ruoli, tempi e flussi organizzativi necessari per assicurare il rispetto della normativa vigente in tema di nomina, funzioni ed attività di monitoraggio e controllo sull'operato degli Amministratore di Sistema, garantendo, tra l'altro, le seguenti esigenze:

- consentire più agevolmente, nei dovuti casi, la conoscibilità dell'esistenza di tali figure o di ruoli analoghi, in relazione a talune fasi del trattamento all'interno dell'organizzazione;
- promuovere l'adozione di specifiche cautele nello svolgimento delle mansioni svolte dagli amministratori di sistema;
- assicurare tempestivamente la possibile adozione di accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del Titolare (*due diligence*);

AMMINISTRATORE DI SISTEMA

Con la definizione di "*Amministratore di sistema*" (di seguito per brevità anche "**AdS**"), si individuano in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati dì sicurezza) con cui vengano effettuati trattamenti di dati personali, e nella misura in cui consentano di intervenire sui dati personali.

COMPITI E FUNZIONI

Gli Amministratori di sistema svolgono funzioni che comportano la concreta capacità di accedere, in modo privilegiato, a risorse del sistema informativo e a dati personali di cui è Titolare l'Asl di Rieti e le loro attività tecniche possono riguardare a titolo esemplificativo e non esaustivo, in relazione alla sicurezza dei dati:

- ✓ applicazione delle misure di sicurezza;
- ✓ salvataggio dei dati (backup/recovery);
- ✓ organizzazione dei flussi di rete;
- ✓ gestione dei supporti di memorizzazione;

- ✓ custodia delle credenziali di autenticazione e di autorizzazione;
- ✓ gestione dei sistemi di autenticazione e di autorizzazione;
- ✓ manutenzione hardware.
- ✓ Possono dunque qualificarsi, quale Amministratori di sistema i seguenti soggetti:
- ✓ amministratori di Sistemi di autenticazione;
- ✓ amministratori di server;
- ✓ amministratori di apparati rete;
- ✓ amministratori di base di dati;
- ✓ amministratori di apparati di sicurezza;
- ✓ amministratori di applicazioni.

Non rientrano invece, nella definizione di AdS quei soggetti che solo occasionalmente intervengono (per es. per scopi di manutenzione a seguito di guasti o malfunzionamenti) sui sistemi di elaborazione e sui sistemi software.

DESIGNAZIONE E NOMINA

In ossequio alle disposizioni di cui al citato Provvedimento dell'Autorità Garante per la protezione dei dati personali del 25 giugno 2009, l'Asl di Rieti procede come di seguito:

1. il Direttore del Sistema Informatico aziendale individua e designa formalmente, in modo puntale ed analitico, le figure da nominare quali "*Amministratore di sistema*", all'esito di specifica valutazione circa esperienza, capacità tecniche, professionali e di condotta e affidabilità dei soggetti da indicare;
2. detta designazione comprende gli "*estremi identificativi"* degli amministratori di sistema (nome, cognome, funzione o area organizzativa di appartenenza) nonché la definizione analitica degli ambiti di operatività consentiti, in base al profilo di autorizzazione assegnato
3. i designati devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
4. alla nomina formale degli Amministratori di sistema provvede il Titolare del trattamento Asl di Rieti, in persona del legale rappresentante *pro-tempore*;
5. L'incarico di AdS è attribuito esclusivamente in via individuale;
6. il Direttore del Sistema Informatico aziendale verifica l'operato degli Amministratori di sistema, con cadenza almeno annuale al fine di controllare la piena rispondenza delle attività svolte alle mansioni attribuite nonché alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

REGIME DI CONOSCIBILITA' DEGLI AMMINISTRATORI DI SISTEMA INTERNI.

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, l'Asl di Rieti garantisce il regime di conoscibilità degli Amministratori di sistema espressamente richiesto dal più volte citato Provvedimento dell'Autorità Garante e, quindi, rende conoscibile l'identità degli amministratori di sistema nell'ambito della propria.

Per quanto sopra, le nomine degli Amministratori di sistema, sulla base degli allegati moduli/schede recanti, tra l'altro, il nominativo del soggetto nominato, le relative funzioni e i sistemi di riferimento, sono registrate in specifico documento, custodito dal Direttore del Sistema Informatico aziendale e prontamente ostensibile a richiesta degli interessati.

ATTIVITA' DI VERIFICA E CONTROLLO SULL'OPERATO DEGLI AMMINISTRATORI DI SISTEMA.

Periodicamente, il Direttore del Sistema Informatico aziendale verifica l'operato degli Amministratori di sistema, con cadenza almeno annuale, in modo da controllare la sua piena rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

A seguito della suddetta attività, il Direttore del Sistema Informatico aziendale trasmette formale relazione al Titolare del trattamento e al Responsabile Protezione Dati nonché, per conoscenza, all'Ufficio privacy aziendale.

Il citato documento aziendale contiene, fra l'altro, la revisione/aggiornamento dell'elenco degli Amministratori di sistema, anche con riguardo alle funzioni agli stessi attribuite e relativi estremi identificativi raccolti e l'indicazione circa l'adozione di possibili interventi che si reputano necessari all'esito della verifica della rispondenza alla nomina dell'operato degli Amministratori di sistema anche con particolare riguardo alle misure organizzative, tecniche e di sicurezza che appare necessario adottare rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.

OUTSOURCING E AMMINISTRATORE DI SISTEMA ESTERNI

Nel caso di servizi di amministrazione di sistema operanti in regime di outsourcing, l'Azienda inserirà nella conseguente nomina a Responsabile esterno ex art. 28 del Regolamento 2016/679/UE del fornitore, l'obbligo di adempiere direttamente alla corretta esecuzione del più volte citato Provvedimento del Garante oltre al diritto/dovere della stessa Asl quale titolare del trattamento, di

effettuare in proprio, anche per il tramite del Responsabile Protezione Dati, apposite verifiche in merito.

Il fornitore conserverà direttamente in apposito documento da tenere costantemente aggiornato e sempre a disposizione, a prima richiesta, dell'Asl di Rieti e/o del Garante, gli estremi identificativi delle persone fisiche da esso fornitore nominate quali amministratori di sistema oltre alla copia dei singoli atti di nomina.

REGISTRAZIONE DEGLI ACCESSI

Devono essere adottati ***sistemi idonei alla registrazione degli accessi logici*** (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo 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.**

Al fine di garantire omogeneità con le procedure di verifica "annuale" dell'operato degli AdS da parte del Direttore del Sistema Informatico aziendale, l'Asl di Rieti ha determinato di conservare detti file per un periodo di un anno dalla loro generazione.

Relativamente all'obbligo di registrazione degli accessi logici degli AdS, sono compresi (oltre che quelli server) anche i sistemi client, intesi come "*postazioni di lavoro informatizzate*" ove vengono trattati dati personali.

Tra gli accessi logici a sistemi e archivi elettronici sono comprese le autenticazioni nei confronti dei *data base management systems* (**DBMS**), che vanno registrate.

Per ***access log*** si intende la registrazione degli 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*.

Gli ***event records*** generati dai sistemi di autenticazione in uso alla Asl di Rieti contengono almeno i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (*timestamp*), una descrizione dell'evento (sistema di elaborazione o *software* utilizzato, se si tratti di un evento di *log-in*, di *log-out*, o di una condizione di errore e possibilmente quale linea di comunicazione o dispositivo terminale sia stato utilizzato…).

CARATTERISTICA DI COMPLETEZZA DEL LOG

La caratteristica di completezza del *log* 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.

CARATTERISTICA DI INALTERABILITÀ DEI LOG

Caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di *log* sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con **apposito *software*.** Il requisito può essere ragionevolmente soddisfatto con la strumentazione *software* in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di *log* **su supporti di memorizzazione non riscrivibili**. In casi più complessi i titolari potranno ritenere di adottare sistemi più sofisticati, quali i *log server* centralizzati e "certificati".

FINALITÀ DI AUDIT DERIVANTE DALLA REGISTRAZIONE E RACCOLTA DEI LOG.

La raccolta dei *log* serve per verificare anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso…). La Asl di Rieti favorisce l'implementazione di sistemi di controllo automatizzato sugli indici di anomalia nell'operato degli Amministratori di Sistema.
L'analisi dei *log* può essere compresa tra i criteri di valutazione dell'operato degli amministratori di sistema.

ACCESSO APPLICATIVO

L'accesso a livello applicativo non è compreso tra le caratteristiche tipiche dell'amministratore di sistema e quindi non è necessario sottoporlo a registrazione.