Attribuzione di funzioni e compiti a soggetti designati:

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali **siano attribuiti a persone fisiche, espressamente designate**, che operano sotto la loro autorità.

D.Lgs. 196/2003 ART. 2 - QUATERDECIES

2. Il titolare o il responsabile del trattamento individuano **le modalità più opportune per autorizzare** al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

AMMINISTRATORE DI SISTEMA

Il Provvedimento del Garante

Il Provvedimento del Garante

A seguito del provvedimento del Garante della Privacy del 27 novembre 2008, pubblicato sulla Gazzetta ufficiale n. 300 del 24 dicembre 2008, prorogato nei suoi tempi di applicazione prima con il provvedimento del 14 gennaio 2009 che poneva la scadenza al 30 giugno 2009 e quindi successivamente ulteriormente modificato e prorogato al 15 dicembre 2009 con provvedimento del 25 Giugno 2009, il **Legislatore pone rilievo sulla figura dell'Amministratore di Sistema**.

Definizione di Amministratore 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**.

Definizione di Amministratore di Sistema

Ai fini del provvedimento del Garante 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**
- **gli amministratori di sistemi software complessi**

Definizione di Amministratore di Sistema

Gli amministratori di sistema, 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.

Definizione di Amministratore di Sistema

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.

Adempimenti: Valutazione delle caratteristiche soggettive

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.

Adempimenti: Designazione individuale

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.

Adempimenti: Servizi in outsourcing

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

Adempimenti: Verifica delle attività

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.

Adempimenti: 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.

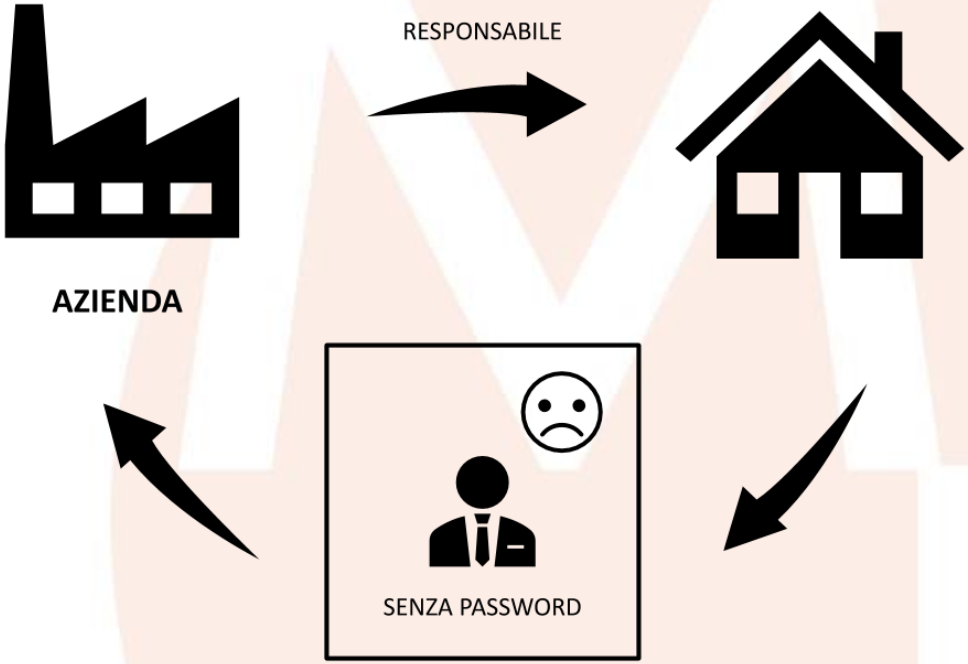
Adempimenti: Registrazione degli accessi

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 6 mesi.**

AMMINISTRATORE DI SISTEMA

Alcuni casi: sono o non sono AdS ?

Caso 1: Manutenzione hw e sw fisica senza conoscenza delle password



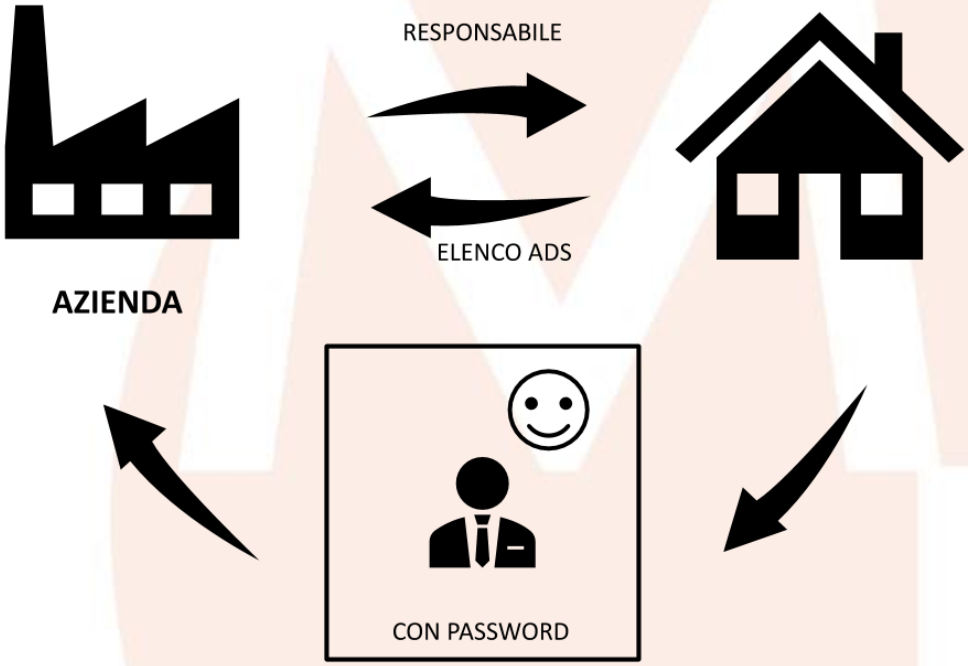
Caso 1: Manutenzione hw e sw fisica senza conoscenza delle password

In questo caso l'operatore informatico esterno accede fisicamente ai sistemi per attività di manutenzione ma, non conoscendo le password di amministratore è necessaria la presenza di un soggetto interno che gli permetta di accedere ai sistemi e lo può sorvegliare durante la sua attività:

NO ADS

SI NOMINA A RESPONSABILE

Caso 1: Manutenzione hw e sw fisica senza conoscenza delle password



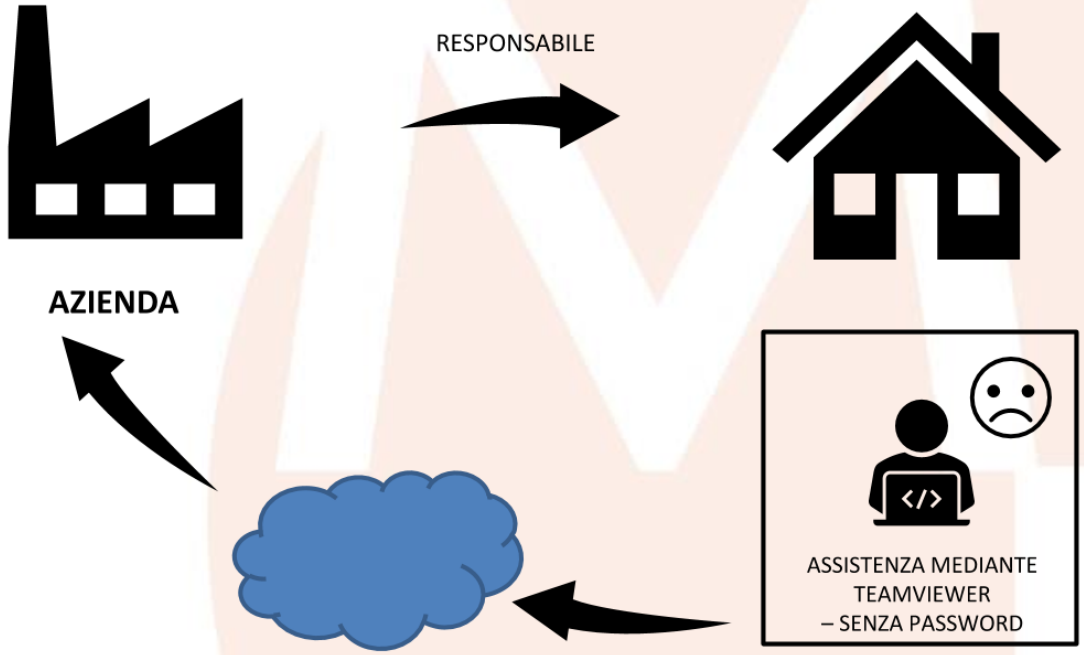
Caso 2: Manutenzione hw e sw fisica con conoscenza delle password

In questo caso l'operatore informatico esterno accede fisicamente ai sistemi per attività di manutenzione e, conoscendo le password di amministratore, può accedere ai sistemi in autonomia:

SI ADS

SI NOMINA A RESPONSABILE

Caso 1: Manutenzione hw e sw fisica senza conoscenza delle password



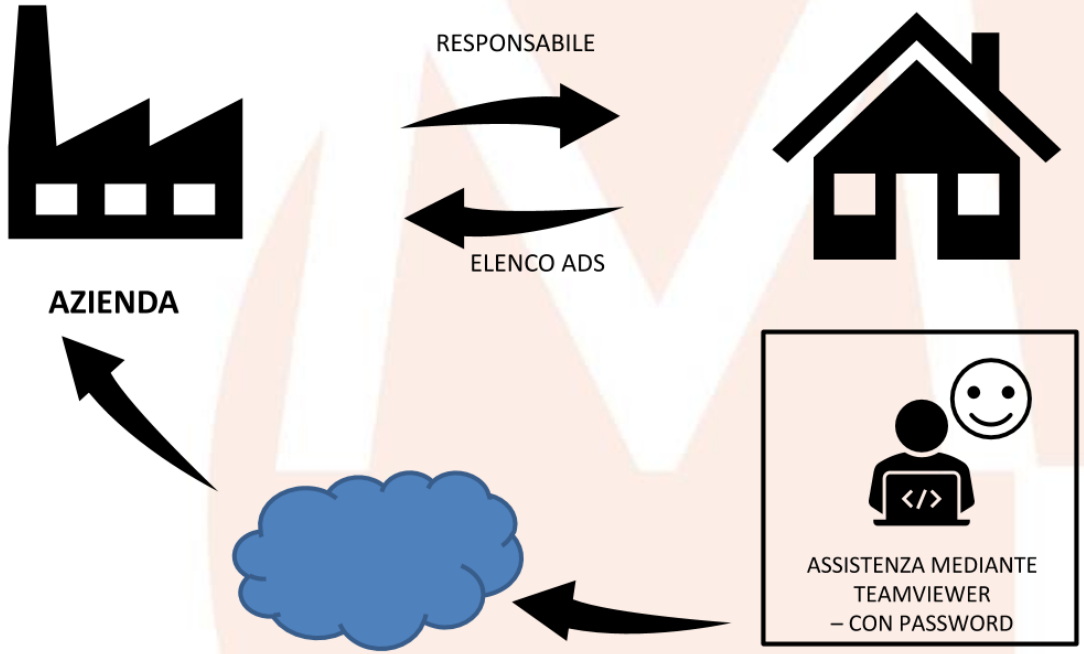
Caso 3: Manutenzione hw e sw fisica da remoto senza conoscenza delle password

In questo caso l'operatore informatico esterno accede da remoto attraverso vari sistemi (es. Teamviewer, Logmein …) ma necessita di qualcuno che, in azienda, gli fornisca una password temporanea di accesso e non può accedere ai sistemi in autonomia:

NO ADS

SI NOMINA A RESPONSABILE

Caso 1: Manutenzione hw e sw fisica senza conoscenza delle password



Caso 4: Manutenzione hw e sw fisica da remoto con conoscenza delle password

In questo caso l'operatore informatico esterno accede da remoto attraverso vari sistemi (es. VPN o Teamviewer, Logmein …) e, avendo impostato a monte password di accesso, non necessita di qualcuno in azienda che lo supporti e può accedere ai sistemi in autonomia:

SI ADS

SI NOMINA A RESPONSABILE

AMMINISTRATORE DI SISTEMA

I casi di esclusione

I casi di esclusione

"Sono **esclusi i trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili** che, ponendo minori rischi per gli interessati, sono stati oggetto delle misure di semplificazione introdotte nel corso del 2008 per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 27 novembre 2008

I casi di esclusione

Il Provvedimento di semplificazione citato recita infatti al cap. 1 del disposto:

“Soggetti che possono avvalersi della semplificazione.

Le seguenti modalità semplificate sono applicabili dai **soggetti pubblici o privati** che:

I casi di esclusione

a) utilizzano dati personali non sensibili o che trattano come unici dati sensibili riferiti ai propri dipendenti e collaboratori anche a progetto quelli costituiti dallo stato di salute o malattia senza indicazione della relativa diagnosi, ovvero dall'adesione a organizzazioni sindacali o a carattere sindacale;

I casi di esclusione

b) **trattano dati personali unicamente per correnti finalità amministrative e contabili**, in particolare presso liberi professionisti, artigiani e piccole e medie imprese (cfr. art. 2083 cod. civ. e d.m. 18 aprile 2005, recante adeguamento alla disciplina comunitaria dei criteri di individuazione di piccole e medie imprese, pubblicato nella Gazzetta Ufficiale 12 ottobre 2005, n. 238).”