Il custode della password: dalla definizione alla nomina - con fac-simile di lettera di incarico

di Luigi Risolo

Pubblicato il 30 Gennaio 2010

analisi della figura del 'Custode delle password'

Privacy e custode della password - Premessa

Nella maggior parte dei luoghi di lavoro, e di conseguenza, in moltissime attività economiche (dal settore primario a quello dei servizi e dell'esercizio di attività professionali) nonché enti pubblici e non, vi sono oltre ai personal computer, anche i software gestionali ed in molti casi, anche, database di dati connessi in rete, e le cui relative elaborazioni vengono trasferite telematicamente (si pensi ad esempio, per i professionisti del settore fiscale e del lavoro ai canali telematici Entratel, a quelli dei servizi per aziende e consulenti dell'Inps o al Punto Cliente dell'Inail) presso altri operatori economici e/o enti pubblici; lo svolgimento di tali attività lavorative richiede l'utilizzo di username e password, le quali vengono di per se consegnate ai titolari del trattamento dei dati in maniera del tutto riservata; or bene, la normativa sulla privacy, ha trasformato in misura obbligatoria la comune pratica responsabile di custodire tali credenziali in modo che non costituiscano causa di utilizzo incauto con tutte le conseguenze, che ne potrebbero scaturire, di serie lesioni del diritto alla riservatezza circa il trattamento di dati sensibili. Da ciò nasce l'oculatezza, nel rispetto della normativa sulla privacy, di procedere alla gestione delle password e delle credenziali di autenticazione informatica, alla nomina della figura del custode delle password nonché alla previsione di tali azioni, all'interno dell'adempimento aziendale in tema di normativa sulla privacy ovvero il Documento programmatico sulla sicurezza.

Definizione di custode della password

Alla luce degli articoli 33, 34, 35, e 36 del Decreto Legislativo 30 Giugno 2003, n. 196, e della regola n. 10, dell'Allegato "B", del citato Decreto, intitolato del "Disciplinare tecnico in materia di misure minime di sicurezza", il "**Custode delle password**" è colui al quale è demandata, mediante lettera di incarico, la gestione, la custodia delle credenziali di autenticazione informatica, la consegna delle medesime ai soggetti preposti al loro fattivo utilizzo nonché la rendicontazione periodica delle assegnazioni delle medesime in riferimento ai soggetti, luoghi aziendali e codici alfanumerici con annessione delle eventuali responsabilità per negligenza o fatti delittuosi.

I compiti del custode della password

I principali compiti del custode delle password sono:

- prendere in consegna da ogni incaricato del trattamento dei dati, da ogni responsabile e da ogni altra figura professionale che operi all'interno dell'azienda, dotato di credenziale di autenticazione, la copia della password o di altra credenziale informatica hardware che consenta l'accesso allo strumento informatico in uso all'incaricato;
- consegna al Titolare del trattamento dei dati, nel momento in cui abbia la necessità per motivi di assoluta importanza di accedere ad un elaboratore in caso di prolungata assenza o impedimento dell'incaricato che lo utilizza abitualmente, della busta contenente la parola chiave dell'elaboratore sul quale egli può intervenire unicamente per necessità di operatività e sicurezza del sistema informativo;
- predisposizione per ogni nuovo incaricato del trattamento e per ogni banca dati, di una busta sulla quale è indicato lo User-Id e indirizzo, al cui interno è contenuta una Password per accedere alla Banca Dati;
- revocare tutte le password non utilizzate per un periodo superiore a sei mesi;
- revocare tempestivamente tutte le password assegnate a soggetti che su comunicazione scritta del responsabile del trattamento non sono più autorizzati ad accedere ai dati;
- gestione delle buste, chiuse, datate e sigillate con firma dell'incaricato su tutti i lembi, contenenti le password degli incaricati del trattamento per procedere, poi, alla conservazione in un luogo sicuro e protetto.

Riferimenti normativi

Sotto il profilo normativo la figura del custode della password, trova fondamento nel punto 10 del "Disciplinate tecnico in materia di misure minime di sicurezza", ovvero Allegato B del "Codice in materia di protezione dei dati personali", il quale sancisce che:

> *"quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato".*

Tale regola è collocata nella prima parte dell'Allegato B, nel quale i primi 11 punti si riferiscono al "*Sistema di autenticazione informatica*". Appare evidente che trattasi di quella parte della gestione degli adempimenti connessi alla privacy per i trattamenti di dati con strumenti elettronici. Perciò il complessivo contesto normativo, riferito alla gestione della custodia delle password e delle credenziali di autenticazione informatica, nasce dagli articoli 33, 34 e 36, del Titolo V – "*Sicurezza dei dati e dei sistemi*", Capo II – "*Misure minime di Sicurezza*", del Decreto Legislativo 30 Giugno 2003, n. 196. Nello specifico l'art. 33, intitolato delle "Misure minime", sancisce che:

> *"1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali".*

L'art. 34, intitolato dei "Trattamenti con strumenti elettronici", sancisce che:

> *"1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: a) autenticazione informatica; b) adozione di procedure di gestione delle credenziali di autenticazione; c) utilizzazione di un sistema di autorizzazione; d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici; e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi; g) tenuta di un aggiornato documento*

> *programmatico sulla sicurezza; h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari. 1-bis. Per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte. In relazione a tali trattamenti, nonché a trattamenti comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante, sentito il Ministro per la semplificazione normativa, individua con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico di cui all'Allegato B) in ordine all'adozione delle misure minime di cui al comma 1.*

L'art. 36, intitolato dell'"Adeguamento", sancisce che:

> *"1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore".*

Le norme riportate hanno non solo la funzione di delineare un quadro generale volto a disciplinare la figura del custode delle password, ma attraverso il richiamo del cosiddetto "Disciplinare tecnico delle misure minime di sicurezza", ovvero Allegato B del D. Lgs. 196/2003, ne scaturisce il legame tra questa figura e il Documento Programmatico di Sicurezza, ovvero tra la necessità di assolvere ad un obbligo di legge e quello di renderlo pratico e parte integrante del citato Documento.

Documento Programmatico di Sicurezza

Il legame tra la figura del custode delle password e l'adempimento del DPS è fondamentale e strutturale; poiché tra i contenuti del citato Documento, rientrano la distribuzione dei compiti e delle responsabilità nell'ambito della struttura di volta in volta interessata e preposta al trattamento dei dati (struttura,

trattamento, descrizione dei compiti e delle responsabilità), nonché l'esplicitazione delle misure di sicurezza ai fini dell'accesso dei dati contenuti nei computer (password, username e altre credenziali di autenticazione informatica). Perciò, il Documento Programmatico di sicurezza, in riferimento alla gestione delle credenziali di autenticazione informatica, dovrà contenere:

1. la parte descrittiva relativa all'adozione delle misure di sicurezza relativi alle credenziali di autenticazione informatica e password presenti nel luogo di lavoro;
2. il riferimento ai compiti, funzioni e responsabilità della figura del custode delle password (nella parte del DPS nella quale è prevista la distribuzione dei compiti e delle responsabilità nell'ambito della struttura di volta in volta interessata e preposta al trattamento dei dati);
3. nella parte finale, tra gli allegati, una copia della lettera di incarico, debitamente datata e sottoscritta dal Titolare/Responsabile del trattamento dei dati e dal soggetto che ha accettato l'incarico di custode delle password.

30 gennaio 2010 Luigi Lurisolo

Bozza Modello di incarico

Lettera di incarico di custode delle password

Intestazione azienda……Via ……..……nr. …..CAP……. Città…… Prov…..Tel/Fax……P.Iva……..Cod. Fisc……..Sito Web…….……E@mail..... Egr. Sig. ……..……Via …… Nr…. CAP…….Città……..Prov… Oggetto: incarico di custode delle password. In riferimento al rapporto di lavoro con Ella instaurato in data ……., con matricola aziendale nr. …., con la qualifica di …… e mansione di ……., in ossequio al Contratto di Lavoro applicato e rilevati il suo ruolo e funzioni all'interno dell'azienda, premesso che, quest'ultima:

- ha proceduto agli adempimenti di cui al D. Lgs. N, 196 del 30 Giugno 2003;
- si deve uniformare secondo quanto stabilito nell'Allegato B, ovvero "Disciplinare tecnico in materia di misure minime di sicurezza".

Vista la regola 10 dell'Allegato B del D. Lgs. n. 196/2003. Tanto premesso, l'Azienda … nella persona del suo Titolare e/o Responsabile del trattamento dei dati, le affida l'incarico di cui è cenno in oggetto e meglio identificato in "Custode delle credenziali di autenticazione informatica", con l'assolvimento delle seguenti mansioni:

- farsi consegnare da ogni incaricato del trattamento dei dati, da ogni responsabile e da ogni altra figura professionale che operi all'interno dell'azienda e che sia dotato di credenziale di autenticazione, la copia della password o di altra credenziale informatica hardware che consenta l'accesso allo strumento informatico in uso all'incaricato;
- nella situazione in cui il Titolare del trattamento abbia la necessità per motivi di assoluta importanza di accedere ad un elaboratore in caso di prolungata assenza o impedimento dell'incaricato che lo utilizza abitualmente, consegnare al titolare stesso la busta contenente la parola chiave dell'elaboratore sul quale egli può intervenire unicamente per necessità di operatività e sicurezza del sistema informativo;
- predisporre per ogni nuovo incaricato del trattamento e per ogni banca dati, una busta sulla quale è indicato lo User-Id indirizzo e al cui interno è contenuta una Password per accedere alla Banca Dati;
- revocare tutte le password non utilizzate per un periodo superiore a sei mesi;
- revocare tempestivamente tutte le password assegnate a soggetti che su comunicazione scritta del responsabile del trattamento non sono più autorizzati ad accedere ai dati;
- procedere alla gestione delle buste, chiuse, datate e sigillate con firma dell'incaricato su tutti i lembi, contenenti le password degli incaricati del trattamento e conservarle in un luogo sicuro e protetto.

La S.V. dichiara espressamente di essere a conoscenza dei compiti del custode delle password e di quanto sancito dal D. Lgs. 196/2003 e dell'Allegato B – Disciplinare tecnico in materia di misure minime di sicurezza – nonché di rispettare scrupolosamente ogni norma vigente di settore e nello specifico ogni istruzione tecnica specificata nel DPS. Luogo e data Timbro e Firma _____ (Azienda) Per accettazione e conoscenza _____ (Firma dell'incaricato)

Ti può interessare anche: Privacy ed omissione delle misure minime di sicurezza dei dati e dei sistemi