PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4865 di Venerdì 05 febbraio 2021

Costruzione e revisione dei profili di accesso ai dati personali

Gli autorizzati al trattamento possono accedere ai dati personali del titolare, sotto la vigilanza del titolare stesso e dei responsabili coinvolti. La costruzione, manutenzione e cancellazione di questi profili deve rispettare alcune regole basilari.

Nei tempi lontani in cui non era ancora entrato in vigore il regolamento europeo sulla protezione dei dati personali, la nostra autorità Garante si era già allora preoccupata della costruzione di manutenzione dei profili di accesso ai dati personali di quei soggetti fisici, che un tempo si chiamavano incaricati del trattamento. In particolare, si richiedeva che, almeno una volta all'anno, venisse effettuata una revisione della congruità tra i profili di accesso e le mansioni svolte dall'incaricato, per tenere allineate le esigenze operative con le esigenze di protezione dei dati. Era un'ottima raccomandazione che certamente vale ancor oggi, anche se nel tempo in alcuni titolari e responsabili si è attenuata l'attenzione a questo tema.

Quanto la situazione possa essere preoccupante nasce dall'esame di quanto accade in altri contesti, come ad esempio nell'ambito dei profili di accesso attribuiti ai dipendenti di istituzioni finanziarie. Chi scrive ricorda perfettamente che un dipendente di una grande istituzione nazionale, che aveva cambiato tre volte mansione nel giro di quattro anni, si era portato appresso i tre profili di accesso, perché non veniva effettuata ad intervalli regolari una valutazione aggiornata della congruità tra i profili di accesso inizialmente attribuiti e quelli effettivamente necessari.

Ma è successo di peggio: dipendenti andati in pensione, o che avevano cambiato datore di lavoro, hanno mantenuto talvolta per mesi e mesi il profilo di accesso iniziale, con la possibilità di operare a distanza su dati, sui quali non avevano più alcuna autorità di intervento.

È in questo contesto che offriamo ai lettori una sintetica scaletta dei passi appropriati, congrui con la corretta impostazione e gestione di questo aspetto operativo, in fase di trattamento dei dati personali.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0551] ?#>

Passo numero uno: definire una politica di costruzione di questi profili

Una politica di costruzione questi profili deve come minimo includere:

- una rassegna dei dati personali trattati, che può essere trovata nel registro del trattamento,
- una lista dei soggetti che sono responsabili del trattamento delle specifiche categorie di dati,
- una descrizione di alcuni tipici profili di accesso,

- una procedura di aggiornamento della congruità del profilo con le mansioni attribuite agli autorizzati,
- le modalità di cancellazione del profilo di accesso,

Infine, ancora una volta si sottolinea la necessità di inserire nella politica un programma di istruzione ed addestramento, e l'indicazione del soggetto cui rivolgersi, in caso di dubbi.

Nella costruzione di questi profili, un principio fondamentale da rispettare è quello che gli anglosassoni hanno contrassegnato con l'espressione "need to know". Nessuno deve accedere dati, cui non ha bisogno di accedere.

Resta poi fondamentale, nella costruzione del profilo, l'attribuzione dei livelli di intervento, corrispondenti rispettivamente alla costruzione del dato ed all'aggiornamento del dato.

Una volta che il dato è stato creato e tenuto aggiornato, gli autorizzati potranno accedere ai dati con il privilegio di sola lettura, il privilegio di modifica, il privilegio di comunicazione a terzi, il privilegio di cancellazione.

Passo numero due: effettuare una revisione periodica della politica aziendale

Poiché spesso, nella attribuzione dei profili di accesso agli autorizzati, gli stessi fanno riferimento al responsabile che li ha designati, occorre chiedere al responsabile di effettuare, come già chiedeva l'autorità Garante nazionale, ad intervalli regolari una rivalutazione della congruità tra il profilo concesso all'autorizzato e le esigenze operative dello stesso. Oggi viviamo in un mondo dinamico, in cui gli scenari operativi cambiano rapidamente: si pensi soltanto allo scenario del lavoro a distanza, che può richiedere una significativa modifica dei profili di accesso, per consentire anche a distanza di poter operare con relativa fluidità.

Passo numero tre: eventuali interventi correttivi e reportistica

Sulla base della revisione periodica della politica aziendale e dei profili autorizzati, dovranno probabilmente essere effettuati degli interventi correttivi. La conoscenza di questi interventi non è tanto importante per individuare chi è responsabile di che cosa, in termini di "colpevolezza", ma per comprendere se questi interventi correttivi sono da imputare a lacune nella politica aziendale ed alla necessità di correggerla in modo appropriato.

Il rapporto deve prendere in considerazione ogni singolo autorizzato, con l'illustrazione delle mansioni precedenti ed attuali, con relativi profili di accesso; deve essere indicato chi ha concesso lo specifico profilo e se tale profilo è compatibile con le indicazioni che erano state dati dal "proprietario" del dato.

Come quando si effettua il debriefing, al termine di una simulazione di emergenza, tutto ciò che è andato bene deve passare in secondo piano, mentre le eventuali anomalie rilevate devono costituire il punto di partenza per interventi correttivi, la cui validità verrà verificata al prossimo punto di controllo.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.

www.puntosicuro.it