PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5100 di Venerdì 11 febbraio 2022

Come impostare una corretta gestione di dati personali

Una corretta politica di conservazione dei dati personali può prevenire gravi conseguenze che possono presentarsi in caso di violazione dei dati e contribuisce a mettere al riparo il titolare da contestazioni da parte degli interessati al trattamento.

Il regolamento generale europeo sulla protezione dei dati presta molta attenzione ai due temi, che andiamo ad affrontare. Una corretta conservazione dei dati personali, ad esempio, permette di costituire una valida difesa contro un attacco per ransomware, in quanto potrebbero essere comunque disponibili per il titolare attaccato. Parimenti, una corretta e tempestiva cancellazione di dati, non più necessari, rappresenta un importante adempimento, nei confronti di tutti gli interessati coinvolti.

Vediamo come è possibile impostare i vari paragrafi di una politica di conservazione dei dati; successivamente daremo cenno alle modalità, prevalentemente tecniche, di cancellazione di dati non più necessari.

Nell'impostare una politica di conservazione e cancellazione dei dati personali occorre prendere in considerazione i seguenti fattori:

- identificare e raggruppare per categorie omogenee, le varie tipologie di dati, trattati dal titolare,
- acquisire ogni informazione di natura legislativa o regolamentare, che possa influenzare le scelte successive, sia a livello di criticità del dato, sia a livello di misure minime obbligatorie di protezione, sia a livello di tempi di conservazione,
- successivamente, individuare quali dati debbano essere costantemente disponibili on-line e quali invece possono essere archiviati, in quanto non di immediata disponibilità; ovviamente tali dati dovranno comunque essere sempre disponibili in caso di necessità. A questo proposito, si faccia attenzione al fatto che non è sufficiente classificare i dati sulla base della data di creazione del dato stesso, ma occorre invece classificarli sulla base dell'ultimo aggiornamento apportato. Parimenti, un contratto di affitto firmato 15 anni fa deve essere comunque conservato, anche se non è stato aggiornato dalla data della firma. Ecco la ragione per la quale la valutazione di disponibilità on-line di un dato richiede un impegno non trascurabile da parte del responsabile delle risorse informatiche e del responsabile del trattamento dei dati personali,
- definire, per ogni categoria, di livello di criticità e, di conseguenza, la frequenza dell'aggiornamento e la incisività delle misure di protezione e salvaguardia; ad esempio, per dati di elevata criticità si potrà prevedere sia di effettuare un aggiornamento in tempo reale o quasi reale, sia di realizzare più copie, archiviate su diversi supporti dei luoghi fisici diversi, mentre per dati meno critici una copia di backup, costantemente aggiornata, potrebbe essere sufficiente,
- individuare il luogo di conservazione delle copie di backup; ad esempio, una copia potrebbe essere disponibile presso la sede del titolare, una seconda nel cloud, una terza copia in un locale separato e protetto, come ad esempio il caveau di una agenzia bancaria. Al proposito, nell'effettuare una rassegna dei supporti di backup e della loro archiviazione, si tenga presente che il nastro, talvolta sotto utilizzato, ha un enorme capacità di archiviazione ed un ingombro fisico di custodia relativamente modesto; per contro, l'uso del cloud pubblico presenta costi attraenti, ma la rapidità di recupero potrebbe non essere soddisfacente; infine, occorre accertarsi che il gestore del cloud sia pienamente conforme alle vigenti norme informatiche, che permettono di valutare le garanzie di custodia sicura del gestore del cloud (norma ISO/IEC 27018),
- una volta definiti i tempi di conservazione, deve essere avviata la procedura di recupero di tutte le copie disponibili dei dati da cancellare; una moltitudine di supporti e di luoghi di archiviazione offre garanzie in merito alla costante

disponibilità dei dati, ma può porre dei problemi nell'essere certi di poter recuperare tutte le copie, ovunque si trovino,
- infine, occorre provvedere alla cancellazione vera e propria, secondo tecnologie appropriate al supporto, su cui i dati sono archiviati. Vi sarà quindi una procedura per la cancellazione o meglio frammentazione di supporti cartacei contenenti dati, oppure una procedura di sovrascrittura di dati su supporto informatico o, in casi estremi, di distruzione fisica del supporto informatico in causa. A questo proposito, è oltremodo prezioso il costante riferimento alla norma europea prEN 15713 [1], che illustra in dettaglio le varie modalità di distruzione o cancellazione dei dati. È bene inoltre ricordare il fatto che la prestazione di un servizio o la fornitura di un bene, in conformità ad una norma italiana, europea o internazionale, costituisce prestazione o fornitura a regola d'arte e pertanto offre adeguata tutela al titolare, che a tale norma si conforma.

Adalberto Biasiotti

---

[1] nota bene: questa norma è attualmente in corso di aggiornamento.
