Si fa presto a dire backup. Rispettando i principi del GDPR

Il GDPR non parla mai direttamente di backup o di copie di riserva. Eppure, uno dei primi elementi che le organizzazioni verificano (o fanno verificare) nel percorso di adeguamento alla nuova normativa europea sulla protezione dei dati personali è proprio il backup. Le domande che si pongono sono quasi sempre le stesse: si fanno i backup? Con quale frequenza? Con quale politica? Quali supporti si usano? Dove si conservano i supporti?

- La finalità delle copie di riserva, in realtà, è ben definita dalla lettera c), comma 1 dell'art. 32 del GDPR: ogni organizzazione che tratta dati personali deve avere la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

L'incidente

Ecco, appunto, l'incidente: quando accade, tutti si mobilitano per ripristinare una situazione accettabile ricorrendo alle copie di riserva.

Quali sono i problemi? Il problema principale è che tra il tempo T, dell'incidente, ed il tempo T-ξ, nel quale è stato eseguito l'ultimo backup, le organizzazioni sono andate avanti, i dati sono cambiati e, se si parla di aziende con migliaia di clienti e con sedi in molti punti della Terra, la questione è molto seria. Di solito si agisce su ξ cercando di minimizzarlo, arrivando a parlare, impropriamente da un punto di vista teorico, di sincronizzazione tra copie: la perfetta sincronizzazione non esiste ed un'azione di recupero della

storia tra T ξ e T è sempre necessaria.

Quindi, al backup, inteso come insieme di policy, strumenti e procedure per produrre copie di riserva dei propri dati, occorre affiancare policy, strumenti e procedure di ripristino. Inoltre, il GDPR prevede, alla lettera d), comma 1 dell'art. 32, che le misure di sicurezza tecniche ed organizzative, tra le quali il backup ed il ripristino, siano testate (che vuol dire provate), verificate (cioè corrispondenti all'obiettivo e ripetibili) e valutate (cioè esaminate negli eventuali margini di miglioramento) regolarmente nella loro efficacia.

Le conseguenze dell'incidente

Accade, invece, che molte organizzazioni si concentrino sul backup e perdano di vista cosa può succedere dopo un incidente. In particolare, si crede che basti avere il backup da qualche parte e, prima o poi, tutto si risolverà.

A parte gli impatti diretti sul business che il prima o poi può significare, la riflessione che si vuole condurre riguarda le conseguenze che un ripristino affrettato e mal gestito può avere nell'infrangere i principi del GDPR e, quindi, i diritti degli interessati. Non bisogna dimenticare, infatti, che, soprattutto per le piccole e medie imprese, violare i principi del GDPR o incidere sui diritti dell'interessato può essere economicamente molto più gravoso che ritardare la consegna di un ordine o sospendere le funzionalità di consultazione del sito: il rischio è una sanzione amministrativa che può arrivare fino a 20.000.000 di euro.

Quindi, calma e gesso: non conviene prendere il database salvato la settimana precedente e ripristinarlo sui sistemi in esercizio. Prima di procedere, è doveroso porsi le seguenti domande sui principi:

- i dati personali che si stanno ripristinando sono

minimizzati rispetto alla finalità che perseguo “oggi”?
- i dati personali che si stanno ripristinando sono esatti ed aggiornati?
- i dati personali che si stanno ripristinando sono in chiaro mentre, normalmente, dovrebbero essere pseudonimizzati?

E, ancora, le seguenti domande sui diritti degli interessati:

- si rischia di ripristinare un dato personale per il quale era stata chiesta una rettifica?
- si rischia di ripristinare un dato personale per il quale era stata chiesta una cancellazione?
- si rischia di ripristinare un dato personale per il quale era stata chiesta una limitazione al trattamento?
- si rischia di ripristinare un dato personale per il quale era stata manifestata un’opposizione al trattamento?
- si rischia di ripristinare un dato personale per il quale era stato revocato il consenso?

In pratica tra il tempo T ξ ed il tempo T può essere successa qualsiasi cosa: in particolare, può accadere che qualche interessato abbia effettuato una richiesta di esercizio di un diritto che rende l’operazione di ripristino molto rischiosa. Per esempio, un cliente può aver richiesto l’esercizio del diritto alla cancellazione (art. 17 del GDPR) il giorno dopo l’esecuzione del backup; a fronte di tale richiesta, vengono cancellati definitivamente i dati personali del cliente dal sistema in esercizio. Tuttavia, a seguito di un incidente, può essere necessario ripristinare il backup che, sfortunatamente, contiene ancora i dati personali del cliente. Tra i dati personali, c’è anche l’indirizzo email dello stesso interessato che, quindi, viene raggiunto dalla newsletter periodica inviata a tutta la clientela. È verosimile che il cliente si rivolga al Garante per la Protezione dei Dati Personali e che la sanzione non tardi ad arrivare.

Qualche ipotesi risolutiva

Senza voler entrare nelle sofisticate strategie di backup e di ripristino che le grandi organizzazioni possono permettersi, qualche ipotesi risolutiva può essere suggerita ai soggetti che non possono disporre di risorse (umane e strumentali) tali da evitare gli inconvenienti ipotizzati a seguito di incidenti.

1 – Eseguire le richieste “a blocchi”

Il suggerimento è di non dare immediatamente corso alle richieste di esercizio dei diritti; il GDPR prevede che queste siano eseguite senza ingiustificato ritardo ma, se il backup viene eseguito settimanalmente (o con maggiore frequenza), si possono accumulare tutte le richieste e si possono eseguire poco prima dell’esecuzione del backup. Il ritardo di esecuzione può essere ampiamente giustificato, documentandolo opportunamente, con la garanzia di effettività dell’esercizio dei diritti a favore degli interessati. Tuttavia, chi dovesse optare per questa soluzione ha il dovere di informare immediatamente l’interessato del momento, leggermente differito, nel quale diventerà effettiva la sua richiesta.

2 – Backup incrementale immediato

Si può ipotizzare di configurare il software applicativo per scatenare un backup incrementale immediato (e circoscritto alle sole strutture logiche interessate) al momento dell’esecuzione di una richiesta di esercizio di un diritto da parte dell’interessato. Non è una soluzione semplice e può richiedere una significativa manutenzione evolutiva del software.

3 – Registro per l’esercizio dei diritti

Un registro per l’esercizio dei diritti, manuale o disponibile in formato elettronico su un apparato elaborativo separato dai sistemi core, può essere una soluzione semplice ed immediata.

In caso di ripristino di un backup effettuato al tempo T ξ, occorre consultare il registro e verificare quali operazioni sono state eseguite in corrispondenza di richieste di esercizio dei diritti fino al tempo T dell’incidente: basta replicarle senza rischiare di ledere gli interessati.

Articolo a cura di **Francesco Maldera**

L’articolo Si fa presto a dire backup. Rispettando i principi del GDPR proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/si-fa-presto-a-dire-backup-rispettando-i-principi-del-gdpr/