PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4461 di Mercoledì 08 maggio 2019

I fornitori di servizi informatici possono garantire la protezione dati?

I titolari del trattamento devono spesso affidare a soggetti terzi l'elaborazione, l'archiviazione e la cancellazione di dati personali. L'esito di un recente studio dimostra che molti fornitori non offrono un servizio di sufficiente affidabilità.

Oggi l'affidamento a fornitori terzi di servizi di elaborazione dei dati rappresenta una situazione fisiologica, in quanto le aziende tendono a specializzarsi nei vari settori, offrendo appunto servizi qualificati, o almeno si spera, a prezzi competitivi.

L'esperienza dimostra come l'affidamento di dati personali a soggetti terzi, che in inglese vengono chiamati "vendors", cioè venditori di servizi informatici, lascia molto a desiderare.

Un recente studio condotto in California e nell'Europa unita ha messo in evidenza come sia bene che il titolare prenda ogni possibile precauzione in fase di selezione e controllo dell'attività di un fornitore di servizi. Un recente studio ha messo in evidenza una situazione assai preoccupante, elencando le violazioni di dati, affidati in elaborazione a soggetti terzi, nel 2018.

Ecco la situazione:

- dati perduti o rubati 15%
- incidenti ed attacchi da parte di soggetti terzi malavitosi ed hackers 21%
- incidente di origine interna 24%
- attacchi provenienti dall'esterno 40%.

Questo studio della società Forrester va abbinato ad uno studio condotto dall'ormai famoso centro di ricerche PONEMON, che valuta il danno complessivo, arrecato da queste violazioni, intorno ai 3, 86 milioni di dollari per violazione, con una tendenza alla crescita rapida, anno per anno. Naturalmente nel calcolare i costi di queste violazioni non basta calcolare i costi diretti, dovuti ad esempio alla ricostruzione dei dati, ma anche alle applicazioni di sanzioni, da parte delle autorità competenti. Non parliamo poi della perdita di immagine, che rappresenta un aspetto sempre più significativo del quadro delle perdite attribuibili a violazione di dati.

Questa è la ragione per cui al tema, in un mio recente volume, ho dedicato un intero capitolo, proprio perché la vera protezione dei dati si ottiene se non si creano soluzioni di continuità fra gli apprestamenti messi a punto dal titolare e gli apprestamenti del suo fornitore, che per solito opera come responsabile esterno del trattamento dei dati.

Le preoccupazioni relative alla qualità ed affidabilità degli applicativi forniti da soggetti terzi, anche assai prestigiosi, come ad esempio Microsoft, sono state messe in evidenza da una recente valutazione di impatto, che le autorità Garanti olandesi hanno commissionato ad un soggetto terzo, in relazione allo specifico applicativo Microsoft Office. Questo applicativo è utilizzato da più di 300.000 dipendenti della pubblica amministrazione olandese e quindi rappresenta uno strumento operativo, le cui caratteristiche di protezione dei dati sono fondamentali. Allego a questo documento la valutazione di impatto e le considerazioni relative, che costituiscono motivo di viva preoccupazione per tutti coloro che utilizzano questo applicativo.

A parte le consuete raccomandazioni, come ad esempio cercare fornitori che godano di certificazioni specifiche, come ad esempio EN 27000, oppure dimostrino di aderire a codici di condotta convalidati dai Garanti, può esser opportuno offrire ai lettori un elenco delle principali prescrizioni contrattuali, che potrebbero essere inserite nella fase di stipula di un contratto di resa di servizi informatici, da parte di un soggetto terzo.

Voce contrattuale	**breve descrizione**
Definizioni	nel contratto occorre includere una voce, come già avviene nelle tracce normative, che illustra con chiarezza il significato dei vari termini inseriti nel contratto. Un costante riferimento al regolamento europeo 679/2016 è indispensabile
Illustrazione analitica delle attività svolte dal soggetto terzo, in termini di finalità, durata del trattamento, nonché elencazione di eventuali altri soggetti terzi coinvolti	non si è mai abbastanza chiari nel definire l'oggetto del contratto, in modo che il fornitore effettui solo attività che sono inserite nel contratto stesso
Descrizione delle misure tecniche e organizzative del responsabile del trattamento esterno	occorre dapprima effettuare una ricognizione delle misure tecniche e organizzative già in vigore presso il fornitore terzo, con particolare attenzione alla gestione di trattamenti afferenti a dati personali; successivamente si possono impartire istruzioni migliorative, indicando anche il tempo entro il quale tali istruzioni migliorative devono essere attuate
Riservatezza ed accessibilità	il fornitore deve impegnarsi a rispettare specifiche indicazioni afferenti all'accessibilità a dati personali da parte di soggetti dai lui stesso autorizzati
Comunicazione di dati personali	i dati personali, forniti dal titolare, devono essere comunicati a soggetti terzi solo per attività specificamente illustrate nell'ambito delle pattuizioni contrattuali
Diritto ad effettuare degli audit anche senza preavviso	il titolare deve evidenziare con chiarezza il suo diritto di effettuare degli audit, senza preavviso, su sistemi, protocolli, profili professionali coinvolti, autorizzazioni e simili
Collaborazione tra titolare e responsabile esterno	il responsabile esterno deve offrire ogni possibile assistenza in caso di violazione di dati, di esercizio del diritto di accesso da parte di interessati e simili
Modalità di conservazione e cancellazione dei dati	al termine del contratto, il responsabile esterno deve restituire i dati forniti dal titolare oppure deve garantire la cancellazione, secondo modalità affidabili e concordate in fase contrattuale

Allegato (pdf)

Adalberto Biasiotti

---

www.puntosicuro.it