PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4896 di Lunedì 22 marzo 2021

Come selezionare un fornitore di servizi informatici sicuro e affidabile

Ormai è ben difficile che un titolare del trattamento possa svolgere in proprio tutta l'attività di trattamento dei dati ed è sempre più frequente l'affidamento di alcune attività a fornitori terzi: una guida per scegliere un fornitore sicuro e affidabile

Purtroppo, ancora oggi, in molte aziende il criterio con cui viene scelto un fornitore di servizi di varia natura è il criterio del prezzo; quanto possa essere pericoloso questo approccio è dimostrato quasi tutti i giorni, anche per il fatto che la evoluzione legislativa prevede che esista una responsabilità congiunta, in caso di violazione dei dati, tra il committente e l'appaltatore.

Ecco la ragione per la quale sono lieto di mettere a disposizione una lista di controllo, sviluppata dai colleghi statunitensi, che potrà aiutare un titolare ed un ufficio acquisti a selezionare un appropriato fornitore.

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

Cominciamo a restringere il capo dei soggetti da esaminare

- il potenziale fornitore ha messo a disposizione una documentazione afferente alla protezione dei dati efficiente ed efficace e pubblicamente disponibile?
- Il potenziale fornitore utilizza certificazioni afferenti alle strutture fisiche ed informatiche, dove i dati vengono trattati?
- Una rapida ricerca on-line mette in evidenza possibili violazioni dei dati, in cui sia stato coinvolto il potenziale fornitore?
- La modulistica di raccolta del consenso, disponibile sul sito web del potenziale fornitore, è sufficientemente intelligibile e priva di "trucchi"?
- Il potenziale fornitore dispone di professionisti della security e della protezione dei dati, inseriti nel proprio organigramma?

Il trattamento dei dati

- Che tipo di dati viene condiviso o viene direttamente raccolto e trattato dal potenziale fornitore?
- Sono state definite le modalità di intervento su questi dati?
- Dove vengono archiviati i dati di cui il potenziale fornitore entra in possesso?
- È stata definita la durata di conservazione dei dati ed i protocolli per una successiva cancellazione?
- Quali controlli di sicurezza vengono attivati presso il potenziale fornitore?

- Il venditore ha messo a disposizione il documento ex articolo 25 del regolamento europeo e, se appropriato, anche il documento ex articolo 35?
- Il potenziale fornitore ha sviluppato una politica di gestione di data breach e di piani di recupero, in caso di eventi perturbanti?

Il rapporto contrattuale

- è già disponibile un rapporto contrattuale standardizzato con il potenziale fornitore?
- Se il trattamento dei dati prevede il trasferimento di dati all'estero, sono state prese le appropriate precauzioni?
- Sono state concordate le modalità con cui sia possibile, ad intervalli almeno annuali, effettuare degli audit presso la struttura potenziale fornitore?

Buon lavoro a tutti coloro che utilizzeranno questa lista 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.
