PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4196 di Mercoledì 14 marzo 2018

Pubblicata la linea guida sulla notificazione in caso di violazione dei dati

La versione iniziale della linea guida è stata sottoposta all'esame di numerosi soggetti coinvolti ed oggi l'articolo 29 Working party può pubblicare la versione definitiva di questa preziosa linea guida.

Come ben sanno tutti i professionisti coinvolti nell'applicazione del nuovo regolamento generale europeo, a differenza di quanto accadeva in passato, oggi praticamente tutte le violazioni dei dati devono essere notificata all'autorità Garante, quando vi possono essere rischi oggettivi che riguardino la tutela dei sacrosanti diritti degli interessati.

Per meglio chiarire le circostanze nelle quali esiste l'obbligo di segnalare all'autorità Garante la violazione, l'articolo 29 Working party aveva pubblicato tempo addietro un documento preliminare, che era stato sottoposto all'esame di tutti i soggetti coinvolti.

Oggi viene pubblicata la versione definitiva di queste linee guida, che rappresenteranno un prezioso strumento, a disposizione dei titolari e responsabili, per adottare corretti modelli di comportamento, a fronte di possibili violazioni dei dati personali.

Rimandando i lettori ad una attenta disamina del documento allegato, riporto nella tabella che segue alcuni esempi di situazioni tipiche, con i modelli di comportamento raccomandati l'articolo 29 Working party.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[USBGDPR] ?#>

Ecco una tabella indicativa, che illustra alcuni esempi di violazione dei dati e le attività conseguenti.

Esempio	**è necessario notificare all'autorità Garante?**	**È necessario notificare all'interessato coinvolto?**	**Note e raccomandazioni**
Un titolare del trattamento ha archiviato la copia di backup di un archivio di dati personali, su una chiavetta USB, proteggendoli con un algoritmo crittografico. La chiavetta viene rubata durante una effrazione	no	no	se i dati personali sono stati cifrati con un algoritmo di elevata qualità, e sono disponibili delle copie di backup dei dati, i dati stessi non vengono compromessi e i dati possono essere ripristinati rapidamente. In questo caso non ci troviamo davanti ad una violazione che debba essere segnalata. Tuttavia occorre tenere sotto controllo la situazione per accertarsi che, magari in tempi successivi, i dati

			non siano stati compromessi
Un titolare del trattamento gestisce un servizio on-line. A seguito di un attacco informatico su questo servizio, i dati personali di interessati vengono catturati. Il titolare ha a che fare solo con interessati che si trovano in uno specifico paese dell'Unione Europea	Si, occorre riferire la violazione all'autorità Garante se vi possono essere delle conseguenze negative per gli interessati coinvolti	Sì, occorre riferire la violazione agli interessati coinvolti, in funzione della natura dei dati personali violati e della gravità delle possibili conseguenze, in caso di utilizzo improprio dei dati	
Una breve interruzione dell'alimentazione elettrica, che si è protratta per alcuni minuti nel call center del titolare, impedisce ai clienti di chiamare il call center e accedere ai propri dati	no	no	non siamo davanti ad una violazione che debba essere notificata, ma conviene comunque registrare questo incidente in conformità alle indicazioni dell'articolo 33 comma 5. È bene tenere una documentazione di quanto accaduto, a cura del titolare
Un titolare è vittima di un attacco per ransomware, che porta alla cifratura di tutti i suoi dati. Non sono disponibili backup e i dati non possono essere ripristinati. A seguito delle indagini, appare chiaro che l'unica funzionalità dell'attacco è legata alla cifratura dei dati e non vi sono altri malware presenti nel sistema	Sì, occorre riferire la violazione all'autorità Garante, se vi sono possibili conseguenze per gli interessati, in quanto ci troviamo davanti a una perdita di disponibilità dei dati	Sì, occorre notificare l'accaduto agli interessati coinvolti, in funzione della natura dei dati personali coinvolti e delle possibili conseguenze della indisponibilità dei dati, od altre conseguenze negative	Se è disponibile un backup dei dati e i dati possono essere ripristinati rapidamente, questa violazione non ha bisogno di essere notificata all'autorità Garante od agli interessati coinvolti, in quanto non vi è stata una perdita permanente di disponibilità o di riservatezza. Tuttavia, se l'autorità Garante viene a conoscenza di questo incidente, grazie ad altri canali di informazione, è possibile che essa attivi una indagine per valutare la conformità con le più incisive misure di sicurezza, illustrate all'articolo 32
Un interessato telefona al call centre di una banca, riferendo di una violazione dei suoi dati. L'interessato infatti ha ricevuto un estratto conto mensile, che è invece destinato ad altro soggetto. Il titolare del trattamento avvia una indagine, che ad esempio può essere completata entro ventiquattr'ore, e stabilisce, con ragionevole probabilità, che si è effettivamente verificata una violazione dei dati personali e questa violazione potrebbe esser conseguente a una anomalia sistemica del sistema informativo, che potrebbe portare alla violazione dei dati personali di altri interessati	Si	La notificazione va inviata soltanto agli interessati coinvolti se vi è un rischio elevato e se è evidente che altri soggetti non potrebbero essere coinvolti	Se, a seguito di una indagine più approfondita, ci si accorge che vi sono numerosi interessati coinvolti, deve essere inviato un aggiornamento all'autorità Garante. Il titolare deve prendere misure aggiuntive per notificare l'accaduto anche ad altri interessati, se vi sono rischi per questi ultimi

Un titolare gestisce un sistema di vendita on-line a clienti in numerosi Stati europei. Il sito on-line è vittima di un attacco informatico e i codici identificativi personali, le parole chiave e le schede degli acquisti precedenti vengono pubblicati on-line dall'attaccante	Sì, occorre riferire l'accaduto all'autorità Garante, se coinvolge trattamenti afferenti a più paesi europei	Sì, in quanto questa situazione può portare ad alti rischi per l'interessato	Il titolare deve attivarsi, ad esempio obbligando ad un reset delle parole chiave dei conti dei clienti coinvolti, nonché altre iniziative che possono mitigare il rischio. Il titolare deve anche verificare se vi sono altri obblighi di notifica, ad esempio nel quadro della direttiva NIS, in quanto il titolare è un fornitore di servizi digitali
Una azienda che ospita un sito Web, in qualità di responsabile del trattamento, identifica la presenza di un errore nel codice che controlla la autorizzazione dell'utente. Le conseguenze di questa anomalia sono che qualsiasi utente può accedere ai dettagli dei conti di qualsiasi altro utente	In qualità di responsabile del trattamento, la azienda che ospita il website deve notificare tutti gli enti coinvolti, in particolare i titolari, senza ritardo. Nel caso questa azienda abbia già condotto le proprie indagini, deve essere in grado di informare i titolari circa il fatto che i loro siti siano stati coinvolti, subendo una violazione. In questo caso i titolari vengono a conoscenza della violazione non appena sono stati informati dal responsabile del trattamento. Successivamente il titolare deve notificare l'accaduto alla autorità Garante	Se non si vede la presenza di un alto rischio per gli interessati coinvolti, essi non devono essere informati	Il responsabile del trattamento deve analizzare tutti gli altri possibili obblighi di notifica, con particolare riferimento agli obblighi che gli competono come fornitore di servizi digitali, nel quadro della direttiva NIS. Se non vi è evidenza che questa vulnerabilità possa essere utilizzata in danno degli interessati, è bene comunque riferire l'accaduto a tutti i titolari coinvolti, nel quadro delle disposizioni dell'articolo 32
Le cartelle cliniche di un ospedale non sono disponibili per un periodo di 30 ore, a seguito di un attacco informatico	Sì, la struttura sanitaria obbligata a notificare l'accaduto, per i rischi che possono coinvolgere la salute di un paziente e la violazione dei suoi dati personali	Sì, occorre riferire accaduto anche ai pazienti coinvolti	
I dati personali di un gran numero di studenti vengono inviati per errore su una mailing list errata, con più di 1000 destinatari	Sì, l'accaduto deve essere notificato all'autorità Garante	Sì, occorre notificare agli interessati coinvolti, in funzione delle finalità è del tipo di dati personali coinvolti e dopo aver esaminato la gravità di possibili conseguenze	
Un messaggio di posta elettronica di e- marketing è spedito ai destinatari nel campo "to", oppure nel campo "cc". È così possibile ad ogni destinatario vedere gli indirizzi di posta elettronica degli	Sì, può essere obbligatori notificare all'autorità Garante, se il numero degli interessati coinvolti è elevato, se vengono rivelati dati sensibili, ad esempio	Si, occorre notificare accaduto agli interessati coinvolti, in funzione delle finalità e del tipo di dati personali coinvolti e	La notificazione potrebbe non essere necessaria se non vengono rivelati dati sensibili e se solo un numero molto limitato di indirizzi di posta elettronica è coinvolto

altri destinatari	l'indirizzo di posta elettronica di uno psicoterapeuta, o se vi sono altri fattori che presentano rischi elevati, come ad esempio il fatto che il messaggio di posta elettronica contenga delle parole chiave di tipo one off	della gravità delle possibili conseguenze	

Allegato (pdf, 1 MB)

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.