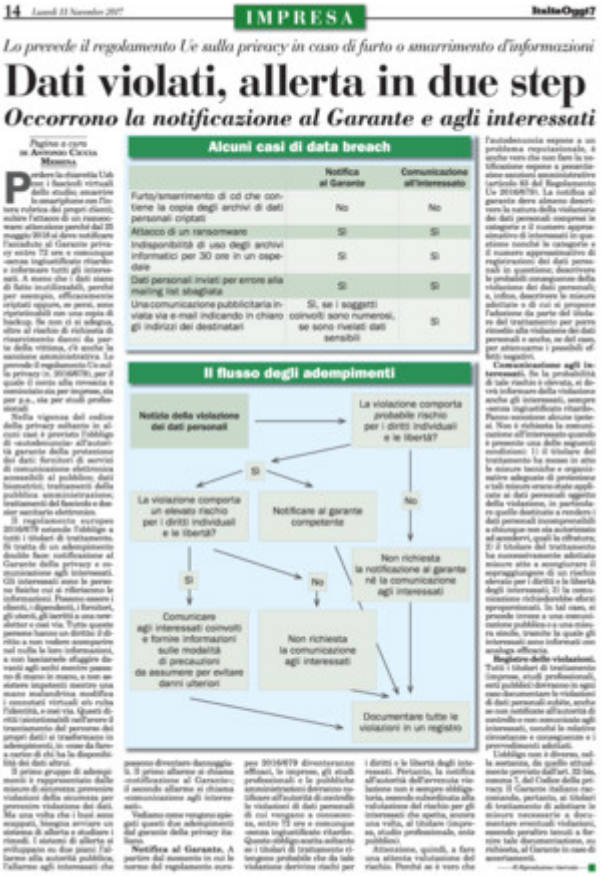
Dati violati, allerta in due step

PAGINA A CURA DI ANTONIO CICCIA MESSINA


14 Lunedì 13 Novembre 2017 IMPRESA ItaliaOggi7

Lo prevede il regolamento Ue sulla privacy in caso di furto o smarrimento d'informazioni

Dati violati, allerta in due step

Occorrono la notificazione al Garante e agli interessati

Alcuni casi di data breach

	Notifica al Garante	Comunicazione all'interessato
Furto/smarrimento di cd che contiene la copia degli archivi di dati personali criptati	No	No
Attacco di un ransomware	Sì	Sì
Indisponibilità di uso degli archivi informatici per 30 ore in un ospedale	Sì	Sì
Dati personali inviati per errore alla mailing list sbagliata	Sì	Sì
Una comunicazione pubblicitaria inviata via e-mail indicando in chiaro gli indirizzi dei destinatari	Sì, se i soggetti coinvolti sono numerosi, se sono rivelati dati sensibili	Sì

Il flusso degli adempimenti

Perdere la chiavetta Usb con i fascicoli virtuali dello studio; smarrire lo smartphone con l' intera rubrica dei propri clienti; subire l' attacco di un ramsonware: attenzione perché dal 25 maggio 2018 si deve notificare l' accaduto al Garante privacy entro 72 ore e comunque «senza ingiustificato ritardo» e informare tutti gli interessati. A meno che i dati siano di fatto inutilizzabili, perché per esempio, efficacemente criptati oppure, se persi, sono ripristinabili con una copia di backup. Se non ci si adegua, oltre al rischio di richiesta di risarcimento danni da parte della vittima, c' è anche la sanzione amministrativa. Lo prevede il regolamento Ue sulla privacy (n. 2016/679), per il quale il conto alla rovescia è cominciato sia per imprese, sia per p.a., sia per studi professionali Nella vigenza del codice della privacy soltanto in alcuni casi è previsto l' obbligo di «autodenuncia» all' autorità garante della protezione dei dati: fornitori di servizi di comunicazione elettronica accessibili al pubblico; dati biometrici; trattamenti della pubblica amministrazione; trattamenti del fascicolo e dossier sanitario elettronico. Il regolamento europeo 2016/679 estende l' obbligo a tutti i titolari di trattamento. Si tratta di un adempimento double face: notificazione al Garante della privacy e comunicazione agli interessati. Gli interessati sono le persone fisiche cui si riferiscono le informazioni. Possono essere i clienti, i dipendenti, i fornitori, gli utenti, gli iscritti a una newsletter e così via. Tutte queste persone hanno un diritto: il diritto a non vedere scomparire nel nulla le loro informazioni, a non lasciarsele sfuggire davanti agli occhi mentre passano di mano in mano, a non assistere impotenti mentre una mano malandrina modifica i connotati virtuali e/o ruba l' identità, e così via. Questi diritti (sintetizzabili nell' avere il tracciamento del percorso dei propri dati) si trasformano in adempimenti, in «cose da fare» a carico di chi ha la disponibilità dei dati altrui. Il primo gruppo di adempimenti è rappresentato dalle misure di sicurezza: prevenire violazioni della sicurezza per prevenire violazione dei dati. Ma

una volta che i buoi sono scappati, bisogna avviare un sistema di allerta e studiare i rimedi. I sistemi di allerta si sviluppano su due piani: l' allarme alla autorità pubblica; l' allarme agli interessati che possono diventare danneggiati. Il primo allarme si chiama «notificazione al Garante»; il secondo allarme si chiama «comunicazione agli interessati». Vediamo come vengono spiegati questi due adempimenti dal garante della privacy italiano. Notifica al Garante. A partire dal momento in cui le norme del regolamento europeo 2016/679 diventeranno efficaci, le imprese, gli studi professionali e le pubbliche amministrazioni dovranno notificare all' autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque «senza ingiustificato ritardo». Questo obbligo scatta soltanto se i titolari di trattamento ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Pertanto, la notifica all' autorità dell' avvenuta violazione non è sempre obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare (impresa, studio professionale, ente pubblico). Attenzione, quindi, a fare una attenta valutazione del rischio. Perché se è vero che l' autodenuncia espone a un problema reputazionale, è anche vero che non fare la notificazione espone a pesantissime sanzioni amministrative (articolo 83 del Regolamento Ue 2016/679). La notifica al garante deve almeno descrivere la natura della violazione dei dati personali compresi le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; descrivere le probabili conseguenze della violazione dei dati personali; e, infine, descrivere le misure adottate o di cui si propone l' adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. Comunicazione agli interessati. Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre «senza ingiustificato ritardo». Fanno eccezione alcune ipotesi. Non è richiesta la comunicazione all' interessato quando è presente una delle seguenti condizioni: 1) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; 2) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati; 3) la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. Registro delle violazioni. Tutti i titolari di trattamento (imprese, studi professionali, enti pubblici) dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all' autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati. L' obbligo non è diverso, nella sostanza, da quello attualmente previsto dall' art. 32-bis, comma 7, del Codice della privacy. Il Garante italiano raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro

tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti. © Riproduzione riservata.