UNIONE POLIZIA LOCALE ITALIANA
Articolo disponibile all'indirizzo: www.unionepolizialocaleitaliana.it/2021-16/

LA PROCEDURA OPERATIVA IN CASO DI DATA BREACH

di Massimiliano Mancini (massimiliano.mancini-privacy@hotmail.com)[a]

ABSTRACT: *Come agire in caso di violazione della sicurezza dei dati personali, ad esempio in caso di diffusione accidentale oppure di attacco di pirati informatici (hacking) o quando i sistemi sono bloccati con la richiesta di un riscatto (ransomware) o quando I sistemi o anche solo le immagini delle telecamere di videosorveglianza, delle body cam, delle fototrappole sono rubate, distrutte o acquisite da terzi, oppure sono smarriti o rubati i computer, o tablet, i cellulari, i registri cartacei che contengono dati personali? Chi deve fare cosa in questi casi? In questo articolo una breve guida schematica sulla procedura operativa da seguire.*

KEYWORDS: #databreach #violazionedatipersonali #privacy #GDPR #videosorveglianza #bodycam #fototrappole #malware #phishing #hacking #ransomware #hacking #accessoillecito #trattamentoillecitodatipersonali #accessoillecitoaisistemiinformatici #MassimilianoMancini #EspertiUPLI #UPLI #UnionePoliziaLocaleItaliana.

INDICE

PREMESSA

Il data breach è il fallimento di protocolli e dei sistemi di tutela dei dati personali, e avviene quando, per ragioni accidentali o per comportamenti illeciti, si compromette la riservatezza, l'integrità o la disponibilità [art.4 p.1 GDPR[1]] di dati personali, ossia qualsiasi informazione riguardante persone fisiche identificate o identificabili, definite dalla normativa come "interessati" [art.4 p.12 GDPR[2]].

Tipici casi di data breach sono[3]: la distruzione anche per cause accidentali come incidenti, incendi o altre calamità, la perdita dei dati contenuti negli archivi o nei dispositivi informatici che li contengono; la modifica accidentale o la deliberata alterazione di dati personali; l'accesso ai dati personali trasmessi, conservati o comunque trattati da parte di terzi non autorizzati e l'eventuale divulgazione non autorizzata; il blocco o comunque l'impossibilità ad accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ransomware.

In questi casi ci si trova all'improvviso con il dilemma: chi deve fare cosa e in quanto tempo?

---

[a] *Segretario Generale UPLI, criminologo, già comandante dirigente di Polizia Locale e Provinciale, DPO/RPD e consulente privacy in enti pubblici e aziende private esperto in DPIA.*

[1] Reg. UE/2016/679 GDPR, art.4 p.12 "*1. Ai fini del presente regolamento s'intende per: …omissis… [12] La «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;*".

[2] Reg. UE/2016/679 GDPR, art.4 p.12 "*1. Ai fini del presente regolamento s'intende per: [1] «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*".

[3] Casi esposti sul sito del Garante per la protezione dei dati personali: https://servizi.gpdp.it/databreach/s/self-assessment.

CHI DEVE AGIRE IN CASO DI DATA BREACH

In caso di data breach il primo soggetto responsabile è il titolare del trattamento, sia esso un privato, un professionista, un'azienda, un ente pubblico, un'associazione o un partito politico, ha l'obbligo di accertare i fatti e le circostanze in cui esso è avvenuto, valutarne le conseguenze, adottare tutte le misure necessarie per porvi rimedio e deve anche documentare tutto dettagliatamente, in modo che l'autorità di controllo, ossia il Garante per la protezione dei dati personali, qualora ne abbia necessità possa verificare il rispetto della normativa [art.33 c.5 GDPR[4]].

Quindi il titolare del trattamento deve annotare l'evento sul registro dei data breach e, se ritiene che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche allora, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante per la protezione dei dati personali e, qualora la comunicazione sia inviata oltre il termine, si deve giustificare il ritardo [art.33 c.1 GDPR[5]].

Anche il responsabile del trattamento ha specifiche responsabilità in caso venga a conoscenza di un data breach dovendo informare tempestivamente il titolare in modo che possa attivarsi con tutta la procedura [art.33 c.2 GDPR[6]].

COME COMPILARE LA COMUNICAZIONE

La notifica deve contenere una serie di informazioni minime espressamente previste dalla normativa [art.33 c.3 GDPR[7]] e dal Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali [doc.web n 9126951]:

- la descrizione della natura della violazione dei dati personali nella maniera più ampia e dettagliata possibile quindi, ad esempio, se essa è stata accidentale o dolosa, come è avvenuta, cosa ha comportato;
- se possibile accertarlo, l'indicazione o la stima delle categorie e il numero approssimativo dei soggetti interessati dalla violazione e le categorie e il numero approssimativo di registrazioni dei dati personali violati;
- i riferimenti del responsabile della protezione dei dati-DPO, nominativo, contatti mail, pec, telefonici e di qualsiasi altro soggetto in grado di riferire sui fatti;
- la stima e la descrizione delle probabili conseguenze della violazione dei dati personali;

---

[4] Reg. UE/2016/679 GDPR, art.33 c.5 "*Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.*".

[5] Reg. UE/2016/679 GDPR, art.33 "*1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.*".

[6] Reg. UE/2016/679 GDPR, art.33 c.2 "*Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.*".

[7] Reg. UE/2016/679 GDPR, art.33 c.3 "*La notifica di cui al paragrafo 1 deve almeno: a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) 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.*".

- l'indicazione delle 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.

È possibile anche utilizzare la procedura e la modulistica già predisposta sul sito del Garante e, qualora non sia possibile fornire tutte le informazioni all'atto della comunicazione, possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo [art.33 c.3 GDPR[8]].

COME TRASMETTERE LA NOTIFICAZIONE

La comunicazione del data breach, laddove sussista l'obbligo, deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo protocollo@pec.gpdp.it o tramite posta elettronica ordinaria all'indirizzo protocollo@gpdp.it e deve essere sottoscritta digitalmente, ossia con firma elettronica qualificata/firma digitale, oppure se non si dispone di questa possibilità con firma autografa scansionata unitamente alla copia del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e, opzionalmente, la denominazione del titolare del trattamento.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito strumento di autovalutazione (self assessment) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

[8] Reg. UE/2016/679 GDPR, art.33 c.4 "*4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.*".