Mercoledi' 24/02/2021

Privacy: quanto costa perdere un hard disk esterno

A cura di: Studio Valter Franco

Sul sito del Garante per la Protezione dei Dati Personali è stato pubblicato il Provvedimento del 14 gennaio 2021 (doc. web 9538748) che riguarda il caso dell'Agenzia Regionale Protezione Ambientale della Campania (ARPAC) che ha subito il furto di un hard disk esterno.

L'ARPAC notificava ai sensi dell'art. 33 del Regolamento UE 679/20161 il furto di un hard disk esterno nel quale erano contenuti dati personali (copie di documenti di riconoscimento, CUD, modelli F24 - 730, buste paga, pratiche di rimborso etc.).

Il Garante osserva che tale situazione ha comportato una illecita sottrazione e possibile divulgazione non autorizzata dei dati contenuti nell'hard disk esterno", e quindi che essa, "in virtù del numero degli interessati, della natura, numero e grado di sensibilità dei dati personali violati possa determinare un conseguente rischio per le libertà e i diritti degli interessati"; inoltre, avrebbe compromesso sia la riservatezza dei summenzionati dati che la loro disponibilità, in quanto "il salvataggio di backup non [era] andato a buon fine, di conseguenza i dati [erano] andati quasi tutti irreparabilmente persi". Come specificato nella denuncia al Comando dei Carabinieri effettuata in data XX, "I dati in questione erano stati oggetto di backup il XX, pertanto quelli salvati successivamente alla citata data sono andati persi"; l'hard disk oggetto di sottrazione sarebbe stato "collegato al server installato in una stanza alla quale può accedere qualsiasi dipendente", nonché i dipendenti dell'ARPAC Multiservizi, società in house dell'Agenzia.

L'ARPAC presentava scritti difensivi (art. 166 c. 6 del Codice2) evidenziando che il server era protetto da password di accesso, che aveva contattato gli interessati per informarli del furto, che non appare vi siano conseguenze negative, che i dipendenti erano stati informati circa l'utilizzo improprio dei dati e dei danni che ne potevano conseguire.

Il Garante osserva che il titolare del trattamento e il responsabile del trattamento debbono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento" e che "Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati" .

Pertanto, si rileva l'illiceità del trattamento di dati personali effettuato dall' ARPAC, per non aver adottato misure tecniche e organizzative adeguate per assicurare la protezione da trattamenti non autorizzati o illeciti o dalla perdita, e per garantire un livello di sicurezza adeguato al rischio, in violazione degli artt. 5, par. 1, lett. f)3, e 32 del Regolamento.

La violazione delle predette disposizioni rende applicabile la sanzione amministrativa prevista dall'art. 83, par. 5, del Regolamento4, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento medesimo, ed ordina all'ARPAC di pagare la somma di euro 8.000,00 (ottomila/00).

Note:

1. art. 33 - RE 679/2016 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. 2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. 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. 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. 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.

2. D.lgs. 196/2003 - art. 166 c 6. Entro trenta giorni dal ricevimento della comunicazione di cui al comma 5, il contravventore può inviare al Garante scritti difensivi o documenti e può chiedere di essere sentito dalla medesima autorità.

3. f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

4. art. 83 c. 5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9; b) i diritti degli interessati a norma degli articoli da 12 a 22; c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49; d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX; e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

Dott.ssa Valentina Serra