Registro dei Provvedimenti
N.14 del 29 maggio 2020

AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il COLLEGIO

Nella riunione del 29 maggio 2020, alla quale hanno preso parte l'Avv. Nicola Fabiano, Presidente, il Dott. Umberto Rapetto, Vice Presidente, l'Avv. Patrizia Gigante, Componente e la Dirigente, Avv. Maria Sciarrino;

vista l'istanza presentata in data 11 maggio 2020 all'Autorità Garante da XXX, quale Responsabile per la Protezione dei Dati Personali della società XXX, con la quale ha rappresentato che: *"in data 24 aprile intorno alle ore 14:00 (GMT+2), MailUp ha avuto conoscenza di un incidente informatico che intorno alle ore 16.00 (GMT+2) è stato ricondotto ad un sofisticato attacco di elevata intensità diretto ad alcuni dei server aziendali ("Server"). Tale attacco è risultato nella cifratura del contenuto di tali Server (per mezzo di un ransomware di ultima generazione e in continua evoluzione), sui quali è ospitato anche l'account di XXX e di alcuni clienti, rendendo quindi temporaneamente indisponibili le informazioni ivi contenute, che comprendono anche dati personali quali, per es., informazioni anagrafiche (nome e cognome) e dati di contatto (indirizzo e-mail, numero di telefono) inseriti nel contesto del Servizio";*
vista la legge 21 dicembre 2018 n. 171;
vista la documentazione in atti;

CONSIDERATO

- che ai sensi dell'art. 1, comma 2, della Legge 171/2018, il trattamento dei dati personali si deve svolgere *"nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali"*;
- che, ai sensi dell'art. 1, comma 3, *"chiunque ha diritto alla protezione dei dati personali che lo riguardano"*;
- che ai sensi dell'art 2, lettera g), della Legge 21 dicembre 2018 n. 171, il *titolare del trattamento dei dati* è colui che determina le finalità e i mezzi del trattamento di dati personali e gli strumenti utilizzati*, ivi compreso il profilo di sicurezza;*
- che ai sensi dell'art. 4, comma 2, della Legge 171/2018, *il titolare del trattamento garantisce il rispetto dei principi previsti dalla legge e deve essere in grado di comprovarlo;*
- che ai sensi dell'art. 2, comma 1 lettera h), della Legge 21 dicembre 2018 n. 171*, il responsabile del trattamento dei dati è colui che tratta dati personali per conto del titolare del trattamento;*
- che ai sensi dell'art. 4, comma 1, lettera a) della Legge 21 dicembre 2018 n. 171, *i dati personali devono essere trattati in modo lecito, corretto, trasparente*;
- che ai sensi dell'art. 4, comma 1, lettera f) della Legge 21 dicembre 2018 n. 171, *i dati personali devono essere 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;*
- che ai sensi dell'art. 31, comma 1, della Legge 21 dicembre 2018 n. 171 *il titolare del trattamento ha il compito di tenere un registro delle attività di trattamento svolte sotto*

la propria responsabilità e tale registro deve contenere una serie di informazioni specifiche, come previsto dal medesimo comma 1;

- che ai sensi dell'art. 31 comma 2 *anche il responsabile del trattamento ha il compito di tenere un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento;*

RILEVATO

- che ai sensi dell'art. 2, comma 1, lett. n) della Legge n. 171/2018 per violazione dati si intende: "*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"*;
- che, ai sensi dell'art. 33, comma 1, della legge 171/2018, il titolare del trattamento e il responsabile del trattamento *devono mettere in atto misure tecniche e organizzative tali da garantire un livello di sicurezza adeguato al rischio della violazione dei dati personali;*
- che ai sensi dell'art. 34, comma 1, della legge 171/2018, il titolare del trattamento è tenuto a notificare la violazione dati all'Autorità Garante per la Protezione dei Dati Personali senza giustificato ritardo e, ove possibile, entro settantadue 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.*
- che nella fattispecie vi è stata una perdita temporanea di dati personali, quali informazioni anagrafiche (nome, cognome, sesso, data di nascita, luogo di nascita, codice ISS, ecc..) e dati di contatto (indirizzo e-mail, numero di telefono), e che può essere definita come "**violazione della disponibilità dei dati"** in quanto vi è stato il "blocco di un servizio" che ha reso i dati indisponibili per un breve lasso di tempo;
- che la perdita anche temporanea della disponibilità dei dati personali a causa di *ransomware* costituisce comunque un *data breach,* in quanto la mancanza di accesso ai dati potrebbe avere un impatto significativo sui diritti e sulle libertà della persone fisiche;
- che la valutazione sull'impatto della violazione dei dati personali, anche riguardo ai diritti e alle libertà delle persone fisiche, è di esclusiva competenza del titolare del trattamento o del responsabile del trattamento;
- che dall'istanza notificata all'Autorità Garante, si evince che la società xxxxxxx si era immediatamente attivata affinchè fosse ripristinato il servizio e tutti dati personali resi momentaneamente indisponibili.

TUTTO CIO' PREMESSO L'AUTORITA' GARANTE

1. Rileva, per i motivi sopra esposti, che la notifica alla medesima Autorità è necessaria (ex art. 34, comma 1, L. 171/2018) unicamente quando essa presenti un rischio per i diritti e le libertà delle persone fisiche, restando tale valutazione di esclusiva competenza del titolare del trattamento in ragione del principio di responsabilizzazione (*accountability*) ex art. 4, comma 2, L. 171/2018.
2. Prende atto della notificazione della violazione dei dati rappresentata dalla società XXXXXX
3. Invita il titolare del trattamento:
   a) a valutare se, nel caso specifico, la perdita di disponibilità temporanea dei dati abbia presentato "un rischio elevato per i diritti e le libertà delle persone fisiche" ai sensi dell'art. 34, comma 1, L. 171/2018;
   b) a esibire all'Autorità la documentazione di "qualsiasi violazione dei dati

personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio" ex art. 34, comma 5 della L. 171/2018;

c) a attestare all'Autorità per sé e per il responsabile del trattamento coinvolto nella violazione dei dati personali l'adozione di misure tecniche e organizzative adeguate ai sensi dell'art. 34, comma 1, L. 171/2018;
d) a documentare tutte le violazioni dei dati personali, mediante la tenuta di un apposito registro (ex art. 31 comma 2 legge 171/2018).

Tale documentazione consentirà all'Autorità di effettuare eventuali verifiche sul rispetto della normativa sopra indicata.

Delle disposizioni di cui soprà la società XXX è tenuta a darne riscontro all'Autorità Garante entro 30 giorni dal ricevimento del presente provvedimento.
Il mancato riscontro alla richiesta ai sensi dell'art. 59 è punito con la sanzione amministrativa di cui all'art. 72 com. 2 lettera d) della legge 171/2018.

Ai sensi dell'art. 69 della legge 171/2018, avverso il presente provvedimento può essere proposta opposizione all'Autorità Giudiziaria ordinaria, con ricorso giurisdizionale ai sensi dell'art. 70 della legge 171/2018.

San Marino, 29 maggio 2020

Il Dirigente **Il Collegio**

(Avv. Maria Sciarrino)

Il presente Provvedimento è inviato a: XXX e a XXX, quale Responsabile della Protezione Dati della società xxxxxxx.