Ordinanza Ingiunzione – del 29 maggio 2020

Registro dei Provvedimenti

N. 11 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 la segnalazione di violazione dati personali (Data Breach) presentata dalla società XXX, nella persona di XXX, quale Titolare della Protezione Dati, in data 23 dicembre 2019, con la quale informava l'Autorità Garante per la Protezione dei Dati Personali, che l'azienda aveva subito una sottrazione di dati relativi a dati di contatto di propri clienti dalla rubrica di posta elettronica (es.: indirizzo postale o di posta elettronica, numero di telefono fisso o mobile), a seguito di un virus riscontrato sul proprio PC di lavoro e su quello di un proprio collaboratore;

Vista la documentazione agli 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, 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, 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, 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;*

RILEVATO

- Che i dati personali oggetto della violazione riguardavano dati relativi a clienti sulla rubrica di posta elettronica (es.: indirizzo postale o di posta elettronica, numero di telefono fisso o mobile);
- Che per violazione dei dati personali 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. Qualora la notifica all'Autorità Garante per la protezione dei dati personali non sia effettuata entro 72 ore deve essere corredata dai motivi del ritardo;
- Che dalla documentazione presentata dalla società XXX emerge che la violazione è avvenuta in un lasso di tempo che va dal 31/10/2019 al 31/12/2019 e che il titolare dei dati ne è venuto a conoscenza in data 4/11/2019 alle ore 11.30;
- Che la comunicazione della violazione dei dati è pervenuta presso l'Ufficio dell'Autorità Garante, il 23 dicembre 2019, oltre le settantadue ore previste per legge (art. 34, comma 1 della Legge n. 171/2018). La società XXX ha dichiarato nella documentazione in atti i motivi del ritardo e cioè che: "*il virus era stato subito individuato ed eliminato dalla rete aziendale e della sottrazione dei dati ci si è accorti solo molti giorni dopo su segnalazione di alcuni clienti che hanno ricevuto mail indesiderate*";
- Che a seguito di ulteriori atti d'ufficio, questa Autorità Garante, con nota del 3 febbraio 2020, ha invitato il Responsabile del trattamento della società XXX a fornire una relazione dettagliata su quanto indicato sulla notifica di violazione dati
- Che in data 27/02/2020, la società XXX ha trasmesso a questa Autorità Garante una relazione in cui vengono descritti i problemi riscontrati e le misure di sicurezza adottate. Dette misure sono state completate il 15/11/2019 e che dopo circa due mesi non vi sono stati conseguenze;
- Che il titolare del trattamento dati e il responsabile del trattamento dati si sono attivati per comunicare l'avvenuta violazione dei dati agli interessati in data 17 dicembre 2019, mediante posta elettronica e posta certificata, al fine di ridurre gli effetti negativi per gli interessati;
- Che il titolare dei dati ha adottato le misure tecniche e organizzative per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati;

- Che ai fini dell'ammontare della sanzione pecuniaria occorre tenere conto dell'opera svolta dall'agente per eliminare o attenuare le conseguenze della violazione, della gravità della violazione;
- Che ha ritenuto di dover determinare l'ammontare della sanzione pecuniaria nella misura **minima** per violazione dei dati di cui all'art. 34 della Legge 171/2018;
- ai sensi degli art. 72 e 73 della legge 171/2018;

TUTTO CIO' PREMESSO L'AUTORITA GARANTE
ORDINA

Alla società XXX, nella persona del suo legale rappresentate pro tempore, di pagare la somma di € 1.000,00 (mille/00) a titolo di sanzione amministrativa pecuniaria per violazione dei dati personali prevista dall'art. 34 della legge 171/2018, come indicato in motivazione.

INGIUNGE

Alla società XXX il pagamento della sanzione amministrativa pecuniaria di € 1.000,00 (mille/00) entro il termine di 30 giorni dal ricevimento della presente ingiunzione, più spese di notifica di euro 1,50 (uno/50).

Il pagamento della presente ingiunzione può essere effettuata mediante bonifico bancario:

- **IBAN SM 81 K03225 09800 000010006039**
- **Ecc.ma Camera Repubblica di San Marino**
- Codice area 225
- Causale 592
- **Indicare nel Bonifico il numero e la data del Provvedimento**

L'AUTORITA' GARANTE
AVVERTE

Che 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 stessa Legge 171/2018.
L'opposizione non sospende l'esecuzione del provvedimento.
Dell'avvenuto pagamento della sanzione amministrativa dovrà esserne data notizia all'Autorità Garante facendo pervenire l'attestazione del versamento all'Ufficio della medesima Autorità.

Il Dirigente **Il Collegio**

(Avv. Maria Sciarrino)

Il presente Provvedimento è inviato a: società XXX nella persona del legale rappresentante pro-tempore.