GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DIPARTIMENTO TECNOLOGIE DIGITALI
E SICUREZZA INFORMATICA

Fascicolo: DB006747
Titolare del trattamento: Comune di Castellucchio
Notifica di violazione dei dati personali: 25/06/2024

DETERMINAZIONE DIRIGENZIALE

Il Dirigente del Dipartimento tecnologie digitali e sicurezza informatica
del Garante per la protezione dei dati personali

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati, di seguito "Regolamento");

VISTO il decreto legislativo 30 giugno 2003, n. 196, come novellato dal decreto legislativo 10 agosto 2018, n. 101, recante "*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE*" (di seguito "Codice");

VISTE le "*Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679*" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 (di seguito "Linee guida");

VISTO il Regolamento interno del Garante per la protezione dei dati personali n. 1/2019, concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante (pubblicato sulla G.U. n. 106 dell'8 maggio 2019);

VISTO il provvedimento del Garante del 22 febbraio 2018, n. 118, che individua le competenze per materia delle Unità organizzative a far data dal 1° marzo 2018, disponendo che il Dipartimento tecnologie digitali e sicurezza informatica curi "*l'istruttoria relativa alla notifica delle violazioni dei dati personali all'Autorità di controllo ai sensi di quanto previsto dall'art. 33 del Regolamento (UE) 2016/679, coordinandosi con i dipartimenti competenti per gli specifici profili di carattere strettamente giuridico*";

VISTA la notifica di violazione dei dati personali in epigrafe e le successive integrazioni;

CONSIDERATO che il titolare del trattamento ha notificato la violazione dei dati personali al Garante senza ingiustificato ritardo dal momento in cui ne è venuto a conoscenza;

CONSIDERATO che la violazione dei dati personali è consistita in un attacco di tipo ransomware, condotto sui sistemi del Responsabile del trattamento Territorio Energia Ambiente Mantova S.p.a. Società Benefit attraverso l'inoculazione del ransomware della famiglia Black Basta mediante l'utilizzo del tool CobaltStrike, che ha comportato la cifratura e la parziale esfiltrazione dei dati dalla Farm WMWare;

CONSIDERATO che l'evento è imputabile ad una azione intenzionale esterna, che ha coinvolto circa 4655 interessati e le seguenti categorie di dati personali: dati anagrafici e di contatto ;

CONSIDERATO che il titolare del trattamento ha dichiarato che il responsabile ha adottato una serie di misure tecniche e organizzative volte a porre rimedio alla violazione dei dati personali. (disabilitazione delle interfacce esterne su Cluster Firewall; inserimento del blocco di indirizzi IP pubblici malevoli relativi alla classe di ransomware C&C Cobalt

Strike;
modifica della scadenza delle copie snapshot dei sottosistemi dischi per i dati della farm VMWare, integri prima dell'attacco; Full Scan Antivirus SentinelOne su tutti i personal computer aziendali) nonché a prevenire simili violazioni future (revisione delle installazioni dell'EDR sui server e sui personal computer aziendali; accensione graduale delle applicazioni produttive secondo l'elenco dei processi critici compromessi; riattivazione della navigazione Internet per i personal computer; riattivazione VPN L2L e Client; modifica forzata delle password di tutti gli utenti; inibizione di indirizzi IP non italiani nelle connessioni VPN Client);

CONSIDERATO che il Responsabile del trattamento ha dichiarato di aver tempestivamente ripristinato i dati oggetto dell'attacco, cosicché "*l'indisponibilità degli stessi può dirsi temporanea e perdurata dal giorno 16 aprile ore 7:00 al giorno 19 aprile ore 19:00*";

CONSIDERATO che il titolare del trattamento ha rappresentato di ritenere che l'evento fosse suscettibile di presentare un rischio elevato per i diritti e libertà delle persone fisiche, avendo, pertanto, comunicato la violazione agli interessati;

RITENUTO che dall'esame degli atti non si ravvisano, allo stato, gli estremi di una violazione degli obblighi di cui all' art. 33 del Regolamento;

TENUTO CONTO che, in ogni caso, ai sensi dell'art. 19, comma 6, del Regolamento del Garante n. 1/2019, è fatta salva l'attività di controllo, anche con riferimento ad affari già oggetto di archiviazione, in caso di sopravvenuti elementi di fatto o di diritto ovvero di diversa e ulteriore valutazione del Garante;

DETERMINA

di procedere, ai sensi degli artt. 19, comma 5, e 11, comma 1, lett. b) del Regolamento del Garante n. 1/2019, all'archiviazione del fascicolo in epigrafe.

Roma, 5 agosto 2024

Il dirigente
Cosimo Comella
(*documento sottoscritto con firma digitale*)

ET