GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento su data breach - 30 aprile 2019 [9116509]

VEDI ANCHE NEWSLETTER DEL 30 MAGGIO 2019

[doc. web n. 9116509]

Provvedimento su data breach - 30 aprile 2019

Registro dei provvedimenti
n. 106 del 30 aprile 2019

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (di seguito "Regolamento");

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

VISTA la notifica di violazione dei dati personali trasmessa, ai sensi dell'art. 33 del Regolamento, il 21 febbraio 2019 da Italiaonline S.p.a., con la quale la stessa ha rappresentato, tra le altre cose, all'Autorità che:

> "In data 20/02/2019, le analisi tecniche condotte consentivano di determinare che vi era stato un accesso fraudolento mediante un hot spot della rete Wifi";
>
> "si era potuto accertare che l'intrusione aveva permesso la violazione di circa 1.5 milioni di credenziali di account di posta Libero e Virgilio riconducibili ad utenti che avevano eseguito l'accesso mediante webmail";
>
> "erano stati eseguiti i primi interventi di contenimento e mitigazione, tra i quali: i) la predisposizione della "forzatura" del cambio password e la relativa informazione agli utenti mediante landing page"

VISTA la successiva integrazione della notifica di violazione dei dati personali, ai sensi dell'art. 33, par. 4, del Regolamento, trasmessa il 23 febbraio 2019 da Italiaonline S.p.a., con la quale la stessa, nel confermare quanto già rappresentato con la precedente notifica del 21 febbraio 2019, ha fornito una relazione tecnica dell'incidente di sicurezza e ha precisato che:

> con riferimento alle possibili conseguenze della violazione dei dati personali "non c'è stata evidenza di accesso "anomalo" (in termini di volumi e connessioni) alle caselle email degli interessati; ciò anche perché la forzatura del cambio password immediatamente predisposta ha reso inservibili le credenziali acquisite durante l'attacco." specificando che "Solo nel caso in cui le credenziali fossero state utilizzate nel lasso di tempo tra la violazione e la forzatura del cambio password potrebbe essere avvenuto l'accesso non autorizzato a caselle e-mail";
>
> con riferimento alla comunicazione agli interessati stava "provvedendo nei tempi di legge a predisporre e a inviare una mail a tutti gli interessati impattati dall'incidente, in linea con quanto previsto dall'art. 34 del GDPR"

VISTI gli atti acquisiti dall'Ufficio in occasione delle attività ispettive condotte nei giorni 21 e 22 marzo 2019 presso Italiaonline S.p.a., e in particolare il testo della comunicazione inviata agli interessati ai sensi dell'art. 34 del Regolamento;

VISTO l'art. 34, par. 1, del Regolamento che stabilisce che "quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo", fatti salvi i casi in cui tale comunicazione non è richiesta in quanto risulta essere soddisfatta una delle condizioni previste al par. 3 del medesimo articolo;

VISTI i considerando nn. 75 e 76 del Regolamento che suggeriscono che, di norma, nella valutazione dei rischi si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità dei rischi per i diritti e le libertà degli interessati e che tali rischi dovrebbe essere determinati in base a una valutazione oggettiva;

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, che hanno, fra l'altro, individuato i fattori da considerare nella valutazione del rischio – presentato da una violazione dei dati personali – per i diritti e le libertà delle persone fisiche: tipo di violazione; natura, carattere sensibile e volume dei dati personali; facilità di identificazione delle persone fisiche; gravità delle conseguenze per le persone fisiche; caratteristiche particolari dell'interessato; caratteristiche particolari del titolare del trattamento dei dati; numero di persone fisiche interessate; altri aspetti generali;

RILEVATO che la violazione si è verificata in conseguenza di un attacco informatico ai sistemi di front end per la consultazione delle caselle di posta elettronica tramite webmail che, ancorché allo stato arginato, ha permesso che fosse acquisita, da parte di soggetti terzi ignoti, una grande quantità di credenziali di autenticazione;

RILEVATO l'elevato numero di persone fisiche a cui si riferiscono i dati personali oggetto di violazione;

RILEVATA la facilità con cui è possibile identificare specifiche persone fisiche direttamente dai dati personali oggetto di violazione, senza che sia necessaria alcuna speciale ricerca per scoprire l'identità degli interessati;

CONSIDERATO che l'acquisizione da parte di terzi di credenziali di autenticazione per l'accesso ad un servizio, indipendentemente dal fatto che ne consegua un effettivo utilizzo per l'accesso a tale servizio, è da ritenere fonte di potenziale pregiudizio per gli interessati in considerazione della probabilità che le medesime credenziali possano essere utilizzate per accedere anche ad altri servizi online;

RILEVATE la gravità e la permanenza delle possibili conseguenze per le persone fisiche che potrebbero derivare dalla violazione, la quale può provocare il furto o l'usurpazione di identità;

RILEVATO che, dalla documentazione in atti, risulta che Italiaonline S.p.a. nella valutazione delle possibili conseguenze della violazione abbia tenuto conto esclusivamente di potenziali accessi abusivi alle caselle di posta elettronica le cui credenziali di autenticazione erano state oggetto di violazione;

RILEVATO il particolare contesto nel quale Italiaonline S.p.a., tra i principali fornitori di servizi di posta elettronica a livello nazionale, effettua il trattamento di dati personali in questione;

CONSIDERATO che, alla luce di un complessivo esame delle circostanze portate all'attenzione dell'Autorità, degli elementi acquisiti e delle considerazioni svolte, la violazione dei dati personali in argomento è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, condizione per cui è richiesta la comunicazione agli interessati;

VISTO l'art. 34, par. 2, del Regolamento che stabilisce che "la comunicazione all'interessato […] descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni di cui all'articolo 33, paragrafo 3, lettere b), c) e d)";

VISTE le citate "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679", che suggeriscono che il titolare del trattamento, tra le misure da adottare per far fronte alla violazione e attenuarne i possibili effetti negativi per gli interessati, "dovrebbe anche fornire consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative della violazione" in considerazione del fatto che l'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che gli stessi possono prendere per proteggersi;

PRESO ATTO che Italiaonline S.p.a. ha provveduto ad inviare, ai sensi dell'art. 34 del Regolamento, una comunicazione agli interessati coinvolti differenziandone i contenuti in relazione al fatto che l'interessato avesse provveduto o meno ad effettuare il cambio della password nell'intervallo di tempo intercorso tra il momento dell'attivazione del meccanismo di enforcement del cambio della password e il momento in cui sono state inviate le comunicazioni;

RILEVATO che, nella comunicazione inviata agli interessati che dopo la violazione avevano effettuato il cambio della password nelle 48 ore precedenti l'invio della comunicazione, l'avvenuta violazione viene descritta come "attività anomala sui sistemi" e non viene suggerita alcuna azione correttiva, evidenziando al contempo che l'operazione di cambio della password ha reso "inutilizzabili le credenziali precedenti ritenute non più sicure";

RILEVATO che, nella comunicazione inviata agli interessati che dopo la violazione non avevano ancora provveduto ad effettuare il cambio della password nelle 48 ore precedenti l'invio della comunicazione, l'avvenuta violazione viene descritta come "attività anomala sui sistemi" e viene esclusivamente suggerito, quale azione correttiva, il cambio della password al prospettato fine di "eliminare il rischio di accesso indesiderato alla […] casella mail";

CONSIDERATA la necessità di effettuare una nuova comunicazione della violazione dei dati personali agli interessati contenente una descrizione della natura della violazione e delle possibili conseguenze della stessa, nonché indicazioni specifiche sulle misure che gli interessati possono adottare per proteggersi da eventuali conseguenze negative della violazione, quale la raccomandazione di non utilizzare più le credenziali compromesse, modificando la password utilizzata per l'accesso a qualsiasi altro servizio online qualora coincidente o simile a quella oggetto di violazione;

VISTE le già citate "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679", che raccomandano al titolare del trattamento, nella definizione delle modalità di contatto, di "scegliere un mezzo di comunicazione che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate", con particolare riguardo all'eventuale utilizzo di "un canale di contatto compromesso dalla violazione";

RITENUTO che, allo stato, le comunicazioni inviate agli interessati non risultano essere conformi a quanto indicato all'art. 34, par. 2, del Regolamento;

RILEVATO altresì che le predette comunicazioni sono state inviate alle stesse caselle di posta elettronica le cui credenziali di autenticazione sono state oggetto di violazione, e che tale circostanza potrebbe inficiare l'efficacia della comunicazione stessa, posto che tali comunicazioni potrebbero non aver raggiunto i reali utilizzatori delle caselle di posta elettronica;

RAVVISATA, pertanto, la necessità di esercitare il potere dell'Autorità di ingiungere, ai sensi dell'art. 58, par. 2, lett. e), del Regolamento, al titolare del trattamento di comunicare agli interessati la violazione dei dati personali;

RITENUTO necessario disporre che la predetta comunicazione sia effettuata senza ritardo e comunque entro trenta giorni dalla data di ricezione del presente provvedimento, riservandosi ogni altra determinazione all'esito della definizione dell'istruttoria avviata sul caso;

TENUTO CONTO che, ai sensi dell'art. 83, par. 6, del Regolamento, "l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, 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";

RITENUTO, altresì, ai sensi dell'art. 58, par. 1, lett. a), del Regolamento e art. 157 del Codice, di ingiungere a Italiaonline S.p.a. di fornire all'Autorità, entro i successivi sette giorni, un riscontro adeguatamente documentato in merito alle iniziative intraprese al fine di comunicare la violazione agli interessati, nonché alle eventuali ulteriori misure adottate per attenuare i possibili effetti negativi della violazione nei confronti degli interessati;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal Segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 del 28 giugno 2000;

RELATORE la dott.ssa Giovanna Bianchi Clerici;

TUTTO CIÒ PREMESSO, IL GARANTE

1) ai sensi dell'art. 58, par. 2, lett. e), del Regolamento, ingiunge a Italiaonline S.p.a. di comunicare la violazione dei dati personali a tutti gli interessati coinvolti senza ritardo, e comunque entro trenta giorni dalla data di ricezione del presente provvedimento, fornendo almeno le informazioni di cui all'art. 34, par. 2, del Regolamento e utilizzando mezzi di comunicazione che permettano di raggiungere il maggior numero di interessati;

2) ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, ingiunge altresì a Italiaonline S.p.a. di comunicare all'Autorità, entro sette giorni dal completamento delle comunicazioni di cui al punto 1) precedente, quali iniziative siano state intraprese al fine di dare attuazione a quanto prescritto nel presente provvedimento e di fornire comunque un riscontro adeguatamente documentato. Si ricorda che il mancato riscontro alla presente richiesta è punito con la sanzione amministrativa ai sensi del combinato disposto di cui agli artt. 83, par. 5, lett. e), del Regolamento e 166 del Codice.

Ai sensi dell'art. 78 del Regolamento, nonché degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 30 aprile 2019

IL PRESIDENTE
Soro

IL RELATORE
Bianchi Clerici

IL SEGRETARIO GENERALE
Busia