GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento correttivo d’urgenza nei confronti di Aruba Posta Elettronica Certificata S.p.a. - 18 dicembre 2019 [9283040]

VEDI ANCHE NEWSLETTER DEL 6 MARZO 2020

[doc. web n. 9283040]

Provvedimento correttivo d’urgenza nei confronti di Aruba Posta Elettronica Certificata S.p.a. - 18 dicembre 2019

Registro dei provvedimenti
n. 228 del 18 dicembre

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 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, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, di seguito "Codice";

Visti gli atti e la documentazione acquisita nel corso dell'istruttoria avviata dall'Ufficio nei confronti di Aruba Posta Elettronica Certificata S.p.a. (di seguito "Società" o "Aruba PEC"), con sede in Ponte San Pietro (BG), via San Clemente, 53, al fine di "verificare l'osservanza delle disposizioni in materia di protezione dei dati personali, con particolare riferimento alla gestione del servizio PEC, anche a seguito dei numerosi casi di data breach notificati al Garante da diversi titolari di caselle PEC, riguardanti la perdita o la procurata indisponibilità di dati personali a seguito della ricezione di messaggi PEC contenenti allegati infetti da virus informatici […]";

Rilevato che, nel corso dell'istruttoria, è emerso che, per la commercializzazione e attivazione del servizio PEC, la Società si avvale di una rete di Partner (circa 8.900 soggetti pubblici e privati), ai quali la stessa rende disponibile l'applicazione web denominata "Area Clienti", raggiungibile da rete Internet all'indirizzo "XX", attraverso cui i Partner possono attivare nuove caselle di posta elettronica certificata (di seguito "PEC") ed effettuare altre operazioni di gestione delle stesse (es. cambio del titolare della casella, reset della password di accesso, disattivazione della casella);

Rilevato che, allo stato, la citata applicazione web, in caso di attivazione di una casella PEC tramite Partner, provvede all'invio di un messaggio di "avvenuta certificazione" sulla casella di posta elettronica ordinaria del titolare della casella PEC, all'interno del quale è riportato un link che consente allo stesso di impostare la password di accesso alla casella PEC, mentre, come emerso dalla documentazione in atti, prima del 25 settembre 2019, la stessa applicazione web prevedeva una diversa modalità di generazione e consegna delle credenziali di autenticazione per l'accesso alla casella PEC, in base alla quale:

- il Partner impostava direttamente la password di accesso alla casella PEC che, successivamente, attraverso l'applicazione

veniva inviata, in chiaro, sulla casella di posta elettronica ordinaria del titolare della casella PEC;

la password così impostata dal Partner, doveva essere composta da almeno 8 caratteri, senza che fossero previsti ulteriori requisiti di complessità né l'aggiornamento periodico;

al momento del primo utilizzo da parte del titolare della casella, la modifica della password attribuita dal Partner in sede di attivazione, seppur consigliata, non era obbligatoria;

Ritenuto che la predetta modalità di generazione e consegna delle credenziali di autenticazione per l'accesso alla casella PEC, adottata in precedenza dalla Società, in caso di mancata modifica della password da parte dei titolari delle caselle attivate da Partner, sia suscettibile di esporre diverse categorie di interessati (titolari della casella, mittenti/destinatari dei messaggi, nonché altri soggetti i cui dati sono presenti all'interno dei messaggi o dei relativi allegati) a gravi rischi di utilizzi impropri dei propri dati personali nonché furti d'identità;

Rilevato che, come dichiarato dalla Società nella documentazione in atti, le caselle PEC attivate tramite Partner, prima del 25 settembre 2019, per le quali non è mai stata modificata la password di accesso, alla data del 20 novembre u.s., risultavano pari a 559.151;

Rilevato, altresì, che, nel corso dell'istruttoria, è emerso che, attraverso l'applicazione web denominata "PEC Log", raggiungibile da rete Internet all'indirizzo "XX", i log dei messaggi PEC sono consultabili ed esportabili, oltre che dai titolari delle caselle, anche mediante un'utenza (con credenziali di autenticazione costituite dalla username "XX" e dalla relativa password) condivisa da più soggetti coinvolti a vario titolo nella gestione del servizio PEC della Società;

Rilevato che alla predetta utenza è attribuito un profilo di autorizzazione di tipo amministrativo in grado di effettuare operazioni di consultazione e di esportazione dei log relativi a tutti i messaggi inviati o ricevuti dai circa 6,5 milioni di caselle PEC gestite dalla Società nei 30 mesi precedenti;

Considerato che i log dei messaggi PEC – che la Società, ai sensi dell'art. 11, comma 2, del d.P.R. 11 febbraio 2005, n. 68, recante il Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3, è tenuta a conservare – devono contenere almeno le seguenti informazioni: il codice identificativo univoco assegnato al messaggio originale, la data e l'ora dell'evento, il mittente del messaggio originale, i destinatari del messaggio originale, l'oggetto del messaggio originale (che può contenere anche dati di carattere riservato, come nel caso di notifiche di atti processuali, anche penali), il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.), il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.), nonché il gestore mittente;

Ritenuto che la possibilità di effettuare da rete Internet operazioni di consultazione e di esportazione dei log dei messaggi inviati o ricevuti da tutte le caselle PEC gestite da Aruba PEC presenta ingiustificati profili di rischio per i diritti e le libertà degli interessati, aggravati dall'utilizzo condiviso delle credenziali di autenticazione relative alla predetta utenza, che non consente di attribuire le azioni compiute a un determinato soggetto, impedendo così di controllarne l'operato;

Rilevato che, dall'esame della documentazione in atti, è stato constatato che i log di tracciamento degli accessi e delle operazioni compiute sull'applicazione web denominata "Area Clienti" contengono, in particolare:

i parametri con cui viene invocato il web service raggiungibile all'indirizzo "XX", comprese le credenziali di autenticazione di un'utenza tecnica (composte dalla username "XX" e da una password di 8 caratteri senza elementi di complessità, riportata in chiaro);

i parametri con cui viene invocata un'application programming interface raggiungibile all'indirizzo "XX", comprese le credenziali di autenticazione di un'utenza tecnica (composte dalla username "XX" e dalla relativa password, riportata in chiaro);

Rilevato, peraltro, che, all'interno dei predetti log di tracciamento prodotti dall'applicazione web denominata "Area Clienti", sono presenti anche informazioni riferite ai soggetti per cui viene richiesta l'attivazione, da parte di un Partner, di una casella PEC o di un altro servizio, quali il nome, il cognome, il codice fiscale, il numero di telefono, l'indirizzo di posta elettronica ordinaria, la denominazione della casella PEC, la username e la relativa password, ancorché sotto forma di hash con salt;

Ritenuto che la memorizzazione all'interno dei file di log di credenziali di autenticazione, per di più in chiaro, costituisce di per sé una grave violazione degli obblighi di sicurezza di cui all'art. 32 del Regolamento in quanto compromette la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, sia quando tali credenziali consentono di trattare direttamente dati personali, sia quando le stesse sono utilizzate per amministrare e gestire i sistemi informatici coinvolti nel trattamento (cfr. anche art. 5, § 1, lett. f), del Regolamento);

Ritenuto, più in generale, che riportare all'interno dei file di log informazioni non indispensabili per le finalità di controllo e sicurezza connesse al tracciamento degli accessi e delle operazioni compiute su un sistema informatico e sui dati in esso contenuti, determini una duplicazione di dati personali oggetto di trattamento nell'ambito del predetto sistema che risultano così esposti a maggiori rischi di trattamenti non autorizzati o illeciti, e, quindi, non sia conforme ai principi di minimizzazione e di riservatezza di cui all'art. 5, § 1, lett. c) e f), del Regolamento;

Considerate le rilevanti criticità sopra descritte, che comportano rischi di elevata probabilità e gravità per i diritti e le libertà degli interessati, relative a:

a) mancata modifica delle password impostate direttamente dai Partner al momento della loro attivazione delle predette 559.151 caselle PEC;

b) possibilità di effettuare, da rete Internet, operazioni di consultazione e di esportazione dei log dei messaggi inviati o ricevuti dai circa 6,5 milioni di caselle PEC gestite dalla Società, peraltro mediante un'utenza, condivisa da più soggetti, a cui è attribuito un elevato profilo di autorizzazione di tipo amministrativo;

c) memorizzazione, all'interno dei file di log prodotti dall'applicazione web denominata "Area Clienti", di credenziali di autenticazione di utenze tecniche (username e password riportate in chiaro), e di informazioni non necessarie al perseguimento delle finalità di controllo e sicurezza connesse al tracciamento;

Ritenuto necessario intervenire urgentemente per tutelare i diritti e le libertà degli interessati, essendo pregiudicata la capacità, da parte della Società in qualità di titolare del trattamento, di garantire, come richiesto dal Regolamento, la sicurezza dei dati trattati all'interno dei propri sistemi informatici, assicurandone, su base permanente, la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o da danni, anche accidentali; ciò in violazione degli artt. 5, § 1, lett. f), e 32 del Regolamento;

Ritenuta, in particolare, la necessità di ingiungere alla Società, ai sensi dell'art. 58, § 2, lett. d), del Regolamento, in via d'urgenza, con riserva di ogni altra determinazione, anche sanzionatoria - essendo la notifica di cui all'art. 166, comma 5, del Codice, incompatibile con la natura e finalità del presente provvedimento - di adottare le seguenti misure:

A) con riferimento alla criticità di cui al punto a):

1) l'invio, entro il termine di 10 giorni dalla ricezione del presente provvedimento, a tutti i titolari delle suindicate 559.151 caselle PEC che non abbiano già provveduto a modificare la password impostata dal Partner, di una comunicazione volta a rappresentare che, in caso di mancata modifica della stessa entro un termine congruo - da individuarsi a cura della Società - verrà adottata una procedura di modifica obbligatoria della password;

2) l'adozione, entro il termine di 30 giorni dalla ricezione del presente provvedimento, di una procedura di modifica obbligatoria dalla password di accesso alle caselle PEC in caso di inerzia dei titolari delle stesse;

B) con riferimento alla criticità di cui al punto b),

1) l'inibizione, entro il termine di 10 giorni dalla ricezione del presente provvedimento, dell'accesso, da rete Internet, all'applicazione web "PEC Log" con utenze in uso ad utenti operanti presso la Società a cui è attribuito un profilo di autorizzazione elevato, che consente di effettuare operazioni di consultazione e di esportazione dei log dei messaggi inviati o ricevuti da tutte le caselle gestite da Aruba PEC;

2) l'assegnazione, entro il termine di 10 giorni dalla ricezione del presente provvedimento, a un solo soggetto autorizzato delle credenziali di autenticazione dell'utenza "XX", previa modifica della password, assicurando, inoltre, che tutti gli utenti dell'applicazione web denominata "PEC Log" siano dotati di credenziali di autenticazione ad uso

esclusivo degli stessi;

C) con riferimento alla criticità di cui al punto c),

1) la ridefinizione, entro il termine di 30 giorni dalla ricezione del presente provvedimento, delle modalità di tracciamento degli accessi e delle operazioni compiute sull'applicazione web "Area Clienti", prevedendo che i file di log prodotti non contengano credenziali di autenticazione di utenze tecniche, né ogni altra informazione non indispensabile per le finalità di controllo e sicurezza connesse al tracciamento;

2) la ridefinizione, entro il termine di 60 giorni dalla ricezione del presente provvedimento, delle modalità di tracciamento degli accessi e delle operazioni compiute su ogni altra applicazione web che produca file di log contenenti credenziali di autenticazione di utenze tecniche o, comunque, informazioni non necessarie al perseguimento delle finalità di controllo e sicurezza connesse al tracciamento;

3) la modifica, entro i termini di adozione delle misure di cui precedenti ai punti 1) e 2), delle password utilizzate dalle utenze tecniche riportate all'interno dei file di log;

Tenuto conto che, ai sensi dell'art. 83, § 6, del Regolamento, "l'inosservanza di un ordine da parte dell'autorità di controllo ai sensi dell'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 che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante;

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Antonello Soro;

TUTTO CIÒ PREMESSO, IL GARANTE

1) ai sensi dell'art. 58, § 2, lett. d), del Regolamento, ingiunge ad Aruba Posta Elettronica Certificata S.p.a. di adottare le misure di cui alle lettere A), B), e C) indicate in premessa, entro i termini di volta in volta individuati;

2) richiede ad Aruba Posta Elettronica Certificata S.p.a. di comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto ingiunto nel presente provvedimento e di fornire comunque riscontro adeguatamente documentato ai sensi dell'art. 157 del Codice entro 10 giorni dallo spirare dei termini di cui alle lettere A), B), e C) indicate in premessa; l'eventuale mancato riscontro può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, § 5, del Regolamento.

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.

Roma, 18 dicembre 2019

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia