Provvedimento del 7 dicembre 2023 [9962283]

 - Linee Guida Funzioni Crittografiche Conservazione delle Password

LEGGI IL COMUNICATO STAMPA

[doc. web n. 9962283]

Provvedimento del 7 dicembre 2023
(In corso di pubblicazione sulla Gazzetta Ufficiale)

Registro dei provvedimenti
n. 594 del 7 dicembre 2023

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il cons. Fabio Mattei, 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 "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", così come modificato dal decreto legislativo 10 agosto 2018, n. 101 (di seguito "Codice");

VISTE le numerose notifiche, trasmesse all'Autorità ai sensi dell'art. 33 del Regolamento a partire dalla sua applicazione, relative a violazioni dei dati personali che hanno comportato l'esfiltrazione di credenziali di autenticazione informatica costituite da un codice identificativo dell'utente (username) e da una parola chiave (password) – in alcuni casi disattivate o relative a sistemi informatici o servizi online cessati – oppure l'accesso abusivo a sistemi informatici o servizi online mediante credenziali di autenticazione illecitamente acquisite nell'ambito di attacchi informatici ad altri sistemi o servizi;

VISTE, altresì, le istruttorie condotte e in corso di svolgimento, anche mediante accertamenti ispettivi, nei confronti di titolari e responsabili del trattamento concernenti, tra l'altro, la verifica dell'adeguatezza delle misure tecniche e organizzative adottate nell'ambito di sistemi di autenticazione informatica;

CONSIDERATO che la password costituisce un dato personale riferibile all'utente che l'ha impostata e la utilizza per l'accesso a un sistema informatico o un servizio online;

CONSIDERATO che, allo stesso tempo, la password rappresenta una misura di sicurezza, essendo un elemento, appartenente alla categoria della conoscenza (qualcosa che solo l'utente conosce), su cui si basano le procedure di autenticazione informatica per l'accesso alla maggior parte dei sistemi informatici e dei servizi online e, quindi, ai dati personali ivi trattati, riferibili allo stesso utente o ad altri interessati;

RILEVATO, pertanto, che la conservazione delle password nell'ambito di sistemi di autenticazione informatica, o di altri sistemi, può comportare rischi significativi per i diritti e le libertà delle persone fisiche in caso di acquisizione, in modo accidentale o illecito, o divulgazione non autorizzata, spesso dando luogo a fattispecie di furto o usurpazione d'identità;

CONSIDERATO che la probabilità e la gravità di tali rischi devono essere valutate anche tenendo conto del numero e delle tipologie di utenti a cui le credenziali di autenticazione informatica si riferiscono, nonché dell'abitudine degli utenti di utilizzare la stessa password (o una simile) per l'accesso a più sistemi informatici o servizi online;

RITENUTO che l'adozione di adeguate misure tecniche di protezione delle password possa attenuare notevolmente i predetti rischi e, quindi, i possibili effetti negativi nei confronti degli interessati in caso di violazioni dei dati personali aventi ad oggetto credenziali di autenticazione informatica;

RILEVATO che, nell'ambito delle richiamate istruttorie effettuate dall'Autorità, è emersa una limitata applicazione di misure tecniche per proteggere in modo efficace le password di utenti conservate nell'ambito di sistemi di autenticazione informatica, o di altri sistemi, derivante anche da un'inadeguata individuazione e valutazione dei predetti rischi da parte di titolari e responsabili del trattamento;

CONSIDERATO che il Garante ha il compito di promuovere la consapevolezza e la comprensione del pubblico, dei titolari e dei responsabili del trattamento riguardo ai rischi, alle norme, alle garanzie, ai diritti e agli obblighi stabiliti dal Regolamento (ai sensi dell'art. 57, par. 1, lett. b) e d), del Regolamento) e, in quest'ottica, ha il potere di adottare linee guida di indirizzo riguardanti le misure tecniche e organizzative di attuazione dei principi del Regolamento, anche per singoli settori e in applicazione dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita (ai sensi dell'art. 154-bis, comma 1, lett. a), del Codice);

RILEVATA l'esigenza di individuare misure tecniche allo stato dell'arte per proteggere le password degli utenti conservate nell'ambito dei sistemi di autenticazione informatica, o di altri sistemi, e di favorirne la diffusione e l'adozione, in modo che i titolari e i responsabili del trattamento, anche in attuazione del principio di protezione dei dati fin dalla progettazione e per impostazione predefinita, assicurino la conformità al principio di integrità e riservatezza e l'adempimento degli obblighi di sicurezza e siano in grado di comprovarlo (artt. 5, parr. 1, lett. f), e 2, 25 e 32 del Regolamento);

VISTO il decreto-legge 14 giugno 2021, n. 82, convertito in legge, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" e, in particolare, il suo art. 7, comma 5, che prevede che, nel rispetto delle competenze dell'Autorità, la predetta Agenzia (di seguito "ACN"), per le finalità di cui al decreto-legge, consulti il Garante e collabori con esso, anche in relazione agli incidenti che comportano violazioni dei dati personali, stipulando appositi protocolli d'intenti che definiscano altresì le modalità di collaborazione;

VISTO il protocollo d'intenti stipulato tra il Garante e l'ACN il 26 gennaio 2022, al fine di garantire la cooperazione istituzionale tra i due enti e il miglior esercizio delle competenze rispettivamente affidate, promuovendo l'adozione di iniziative congiunte nel campo della sicurezza cibernetica nazionale e della protezione dei dati personali;

CONSIDERATO che, nell'ambito della citata cooperazione istituzionale, a fronte della predetta esigenza, l'ACN ha svolto approfondimenti in ordine alle migliori prassi per proteggere le password, predisponendo, in collaborazione con l'Ufficio del Garante, le "Linee Guida Funzioni Crittografiche – Conservazione delle Password", che contengono indicazioni e raccomandazioni sulle funzioni allo statodell'arte (cc.dd. algoritmi di password hashing) e sui relativi parametri di utilizzo;

RITENUTO di dover adottare le citate linee guida al fine di fornire indicazioni sulle misure tecniche in grado di garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, proteggendo in modo efficace le password, conservate nell'ambito di sistemi di autenticazione informatica, o di altri sistemi, affinché i titolari e i responsabili del trattamento possano orientare le proprie scelte tecnologiche, oppure progettare e realizzare i propri sistemi informatici e servizi online, in conformità al principio di integrità e riservatezza e agli obblighi in materia di sicurezza del trattamento (artt. 5, par. 1, lett. f), e 32 del Regolamento);

CONSIDERATO che, laddove vengano invece adottate misure tecniche diverse da quelle individuate nelle citate linee guida, i titolari del trattamento, in ossequio al principio di responsabilizzazione (artt. 5, par. 2, e 24 del Regolamento), devono essere in grado di comprovare che tali misure garantiscono comunque un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche;

RITENUTO, in ogni caso, che l'adozione delle misure tecniche individuate nelle linee guida in materia di funzioni crittografiche per la conservazione delle password risulti necessaria, in particolare, laddove sia soddisfatta una o più delle seguenti condizioni:

a) il trattamento riguarda le password di un numero significativo di utenti;

b) il trattamento riguarda le password di utenti che possono accedere a banche di dati di particolare rilevanza o dimensioni;

c) il trattamento riguarda le password di specifiche tipologie di utenti che, in modo sistematico, trattano, con l'ausilio di sistemi informatici, dati appartenenti a categorie particolari o relativi a condanne penali e reati di cui agli artt. 9 e 10 del Regolamento;

RILEVATO che, ferma restando l'adozione di misure tecniche per la protezione delle password, la conservazione delle stesse per un arco di tempo superiore a consentire la verifica dell'identità degli utenti ai fini dell'accesso a sistemi informatici o servizi online o, se del caso, a garantirne la sicurezza (es. memorizzazione delle ultime password impostate per impedirne il riuso da parte dell'utente, c.d. password history, o di copie di sicurezza per assicurare il ripristino del sistema di autenticazione informatica in caso di incidente) presenta rischi per i diritti e le libertà delle persone fisiche anche in considerazione del progresso tecnologico che, con il passare del tempo, può rendere obsolete le misure tecniche adottate o comprometterne l'efficacia;

RITENUTO, pertanto, di dover altresì intervenire, al fine di assicurare la protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 del Regolamento), affiancando alle misure indicate nelle predette linee guida, ulteriori indicazioni ai titolari e responsabili del trattamento in merito alle misure per attuare, oltre al principio di integrità e riservatezza, anche quello della limitazione della conservazione di cui all'art. 5, par. 1, lett. e), del Regolamento, affinché le password siano tempestivamente cancellate, anche in modo automatico, laddove non

siano più necessarie per verificare l'identità degli utenti ai fini dell'accesso a sistemi informatici o servizi online o per garantirne la sicurezza e, comunque, in caso di cessazione dei sistemi informatici o servizi online cui consentono l'accesso oppure di disattivazione delle relative credenziali di autenticazione;

TENUTO CONTO che la violazione dei principi di limitazione della conservazione, di integrità e riservatezza, di responsabilizzazione e di protezione dei dati fin dalla progettazione e per impostazione predefinita (artt. 5, parr. 1, lett. e) e f), e 2, e 25 del Regolamento), nonché degli obblighi in materia di sicurezza del trattamento (art. 32 del Regolamento), se accertata dal Garante nell'esercizio dei propri compiti, comporta l'applicazione dei poteri correttivi previsti dall'art. 58, par. 2, del Regolamento nei confronti di titolari e responsabili del trattamento, compreso il potere di infliggere una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del medesimo Regolamento;

RITENUTO, infine, necessario rivolgere un invito ai produttori di prodotti, servizi e applicazioni (di seguito "produttori"), a tenere conto delle predette misure relative sia alle modalità di conservazione delle password che ai criteri da utilizzare per determinarne il periodo di conservazione, oggetto del presente provvedimento, in quanto tali soggetti – come evidenziato dalle "Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita", adottate dal Comitato europeo per la protezione dei dati il 20 ottobre 2020 – rappresentano, insieme ai responsabili del trattamento, figure essenziali ai fini della protezione dei dati fin dalla progettazione e per impostazione predefinita e dovrebbero essere consapevoli del fatto che i titolari del trattamento sono tenuti a trattare i dati personali solo utilizzando sistemi e tecnologie che integrano i principi di protezione dei dati (cfr. considerando 78 del Regolamento);

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali (doc. web n. 1098801);

RELATORE il prof. Pasquale Stanzione;

TUTTO CIÒ PREMESSO, IL GARANTE

1) ai sensi dell'art. 154-bis, comma 1, lett. a), del Codice e dell'art. 57, par. 1, lett. d), del Regolamento, adotta le seguenti linee guida di indirizzo:

a) le "Linee Guida Funzioni Crittografiche – Conservazione delle Password", allegate al presente provvedimento, riguardanti misure di attuazione del principio di integrità e riservatezza e degli obblighi in materia di sicurezza del trattamento, di cui agli artt. 5, par. 1, lett. f), e 32 del Regolamento;

b) le indicazioni sui criteri da utilizzare per determinare il periodo di conservazione delle password, fornite in premessa nel presente provvedimento, riguardanti misure di attuazione del principio di limitazione della conservazione di cui all'art. 5, par. 1, lett. e), del Regolamento;

2) ai sensi dell'art. 57, par. 1, lett. b), del Regolamento, invita i produttori a progettare e sviluppare prodotti, servizi e applicazioni tenendo conto, in particolare, delle misure di cui al precedente punto, relative alle modalità di conservazione delle password (lett. a)) e ai criteri da utilizzare per determinarne il periodo di conservazione (lett. b));

3) ai sensi dell'art. 154-bis, comma 3, del Codice, dispone la trasmissione di copia del

presente provvedimento al Ministero della Giustizia – Servizio pubblicazione delle leggi e degli altri provvedimenti normativi e non normativi, per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 7 dicembre 2023

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Mattei