Bird & Bird

Le Linee Guida e le FAQ del Garante in materia di conservazione delle *password*

13 marzo 2024

Le Linee Guida e le FAQ del Garante in materia di conservazione delle *password*

Introduzione

Il 1° marzo 2024, l'Autorità Garante per la protezione dei dati personali ("**Garante**" o "**Autorità**") ha approvato le nuove *Frequently Asked Questions* volte a fornire chiarimenti utili alle domande più frequenti riguardanti la conservazione delle *password* ("**FAQ**").

Tali chiarimenti giungono sulla scia del provvedimento adottato lo scorso 7 dicembre ("**Provvedimento**"), di concerto con l'Agenzia per la cybersicurezza nazionale ("**ACN**"), recante le "*Linee guida in materia di funzioni crittografiche per la conservazione delle password*" ("**Linee Guida**") che, come già si evince dallo stesso titolo, forniscono raccomandazioni rilevanti sulle funzioni crittografiche ritenute attualmente più sicure per la conservazione delle *password*.

Difatti, l'obiettivo primario di tali Linee Guida è quello di evitare che le credenziali di autenticazione possano essere oggetto di violazione e finire nel possesso di cybercriminali, per essere poi messe sul (*dark*)*web* ed essere utilizzate per furti di identità, richieste di riscatto o altre tipologie di attacchi.

Viene anzitutto da chiedersi: perché è necessario porre tanta attenzione alla sicura conservazione delle *password*?

Bisogna necessariamente partire dal presupposto per cui la *password* ha una duplice valenza: come precisato dal Garante nel Provvedimento, essa rappresenta infatti sia un dato personale che una misura di sicurezza.

La *password* è anzitutto un **dato personale** «*riferibile all'utente che l'ha impostata e la utilizza per l'accesso a un sistema informatico o un servizio online*».

La *password* rappresenta, al tempo stesso, 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*».

Le *password* giocano quindi un ruolo determinante nel proteggere la vita delle persone nel mondo digitale. Ecco perché, con l'obiettivo di innalzare il livello di sicurezza, sia dei fornitori di servizi digitali sia degli sviluppatori di *software*, il Garante ha ritenuto di dover adottare le Linee Guida, fornendo importanti indicazioni sulle misure tecniche da adottare.

Il Provvedimento del Garante

Il Provvedimento origina dalle numerose notifiche ricevute dall'Autorità ai sensi dell'art. 33 del Regolamento (UE) 2016/679 ("**Regolamento**" o "**RGPD**") a partire dalla sua applicazione, relative a (i) 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 (ii) all'accesso abusivo a sistemi informatici o servizi *online* mediante credenziali di autenticazione illecitamente acquisite nell'ambito di attacchi informatici ad altri sistemi o servizi.

In tale contesto, il Garante ha condotto numerose istruttorie (alcune delle quali ancora in corso di svolgimento), anche mediante accertamenti ispettivi, nei confronti di titolari e responsabili del trattamento concernenti, tra le altre cose, la verifica dell'adeguatezza delle misure tecniche e organizzative a presidio dei sistemi di autenticazione informatica. Nell'ambito di tali istruttorie è emersa una limitata applicazione di misure tecniche

per proteggere in modo efficace le *password* degli utenti conservate nell'ambito di sistemi di autenticazione informatica, anche a causa di un'inadeguata individuazione e valutazione dei rischi da parte di titolari e responsabili del trattamento.

Non a caso, infatti, la conservazione delle *password* nei sistemi di autenticazione informatica (o in 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, che possono dare luogo a fattispecie di furto o usurpazione d'identità.

L'adozione di adeguati presidi tecnici di protezione delle *password* deve pertanto ritenersi una misura necessaria per attenuare tali rischi e, conseguentemente, i possibili effetti negativi nei confronti degli interessati in caso di violazioni dei dati personali aventi ad oggetto credenziali di autenticazione informatica.

Come rappresentato dal Garante stesso, studi di settore dimostrano che il furto di *username* e *password* consente ai cybercriminali di commettere numerose frodi a danno delle vittime. Ed è interessante vedere, a tal riguardo, alcune interessanti statistiche che la stessa Autorità mette a disposizione: i dati rubati vengono infatti utilizzati «*per entrare illecitamente nei siti di intrattenimento (35,6%), nei social media (21,9%) e nei portali di e-commerce (21,2%). In altri casi, permettono di accedere a forum e siti web di servizi a pagamento (18,8%) e finanziari (1,3%).*».

Per tutti questi motivi, il Garante ha ritenuto di dover adottare le Linee Guida, proprio «*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)*».

L'Autorità prevede anche la possibilità che i titolari e i responsabili del trattamento adottino invece misure tecniche diverse da quelle individuate nelle Linee Guida, a condizione che, in ossequio al principio di responsabilizzazione (artt. 5(2) e 24 del Regolamento), gli stessi siano in grado di comprovare che tali misure garantiscano comunque un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche.

I chiarimenti del Garante

Le FAQ adottate dal Garante lo scorso 1° marzo si occupano di fornire adeguati chiarimenti in merito all'interpretazione e applicazione delle Linee Guida, con specifico riferimento agli argomenti di seguito riportati.

1 *Individuazione dei destinatari del Provvedimento*.

I destinatari del Provvedimento sono i titolari e i responsabili del trattamento che conservano credenziali di autenticazione di utenti dei propri servizi all'interno dei propri sistemi informatici.

Tuttavia, si precisa che anche i produttori di prodotti, servizi e applicazioni devono tener conto delle indicazioni presenti nelle Linee Guida in relazione alle fasi di progettazione e sviluppo, al fine di consentire a titolari e responsabili del trattamento di utilizzare sistemi e tecnologie che integrino i principi di protezione dei dati.

2 *Individuazione dei soggetti tenuti ad adottare adeguate misure tecniche di protezione delle password*.

Le misure tecniche di protezione delle *password* indicate nelle Linee Guida (o altre misure che siano comunque in grado di garantire un analogo livello di sicurezza) devono essere adottate qualora ricorrano una o più delle seguenti condizioni: (i) il trattamento riguarda le *password* di un numero significativo di utenti, (ii) il trattamento riguarda le *password* di utenti che possono accedere a banche dati di particolare rilevanza o dimensioni, (iii) il trattamento riguarda le *password* di specifiche tipologie di utenti che sistematicamente trattano, con l'ausilio di strumenti informatici, dati appartenenti a categorie particolari o relativi a condanne penali e reati di cui agli artt. 9 e 10 del Regolamento.

Tra i soggetti destinatari di tale obbligo si rinvengono, a titolo esemplificativo e non esaustivo, i gestori delle identità digitali SPID e CieID, i gestori di posta elettronica certificata, le Agenzie Fiscali e le Forze di Polizia, soggetti, pubblici e privati, che erogano servizi di conservazione dei documenti informatici a favore di terzi, società che offrono servizi di fatturazione elettronica, società e aziende che forniscono servizi ICT, fornitori

di servizi di comunicazione elettronica accessibili al pubblico, gestori di servizi di posta elettronica, società operanti nel settore della distribuzione di energia elettrica o del gas, istituti di credito, società finanziarie, imprese assicurative, società di informazioni creditizie, società di informazioni commerciali, società che svolgono attività di commercio elettronico, società che erogano servizi di streaming, imprese di somministrazione di lavoro e ricerca del personale, società che offrono servizi di prenotazione di strutture ricettive, società che offrono servizi di biglietteria per trasporti (es. aerei, ferroviari e marittimi), etc..

3 *Procedura di autenticazione informatica a più fattori*.

Il Garante chiarisce che le Linee Guida trovano applicazione anche nell'ipotesi in cui si utilizzi una procedura di autenticazione informatica a più fattori. Si consideri, infatti, che in tal caso la necessità di proteggere le *password* degli utenti in modo adeguato non viene meno, in quanto potrebbero utilizzare la stessa *password*, o una simile, per accedere ad altri sistemi informatici o servizi online che non prevedono procedure di autenticazione a più fattori.

4 *Password impostate in precedenza dagli utenti nell'ipotesi di conservazione della cronologia delle password*.

Le Linee Guida trovano applicazione anche rispetto alla cronologia delle *password*, in quanto è possibile che l'utente utilizzi la stessa *password*, o una simile, anche a distanza di tempo, per l'accesso al medesimo o ad altri sistemi informatici o servizi online.

5 *Individuazione delle ipotesi in cui è necessario cancellare le password degli utenti seppur conservate in modo sicuro*.

Con il passare del tempo il progresso può rendere obsolete le misure adottate per proteggere le *password* o comprometterne l'efficacia.

Sulla scorta di tale considerazione, le *password* degli utenti devono essere tempestivamente cancellate, anche in modo automatico, nei seguenti casi: (i) cessazione o dismissione dei sistemi informatici o servizi online a cui le credenziali di autenticazione consentivano l'accesso, (ii) disattivazione o revoca delle credenziali di autenticazione di un utente che non ha più necessità di accedere a un sistema informatico o un servizio online o che non ha più i requisiti che ne hanno determinato l'abilitazione.

6 *Ipotesi di violazione dei dati personali avente a oggetto password a cui erano state applicate adeguate misure tecniche di protezione*.

Qualora siano state adottate tecniche crittografiche allo stato dell'arte per proteggere le *password* degli utenti e non risultino coinvolte anche altre tipologie di dati personali, la violazione può non presentare rischi per i diritti e le libertà degli interessati e quindi può non essere obbligatorio effettuare la notifica al Garante e la comunicazione agli interessati coinvolti (artt. 33 e 34 del Regolamento (UE) 2016/679).

Resta fermo, tuttavia, l'obbligo di documentare in modo adeguato la violazione avvenuta (art. 33, par. 5, del Regolamento (UE) 2016/679).

Conclusioni

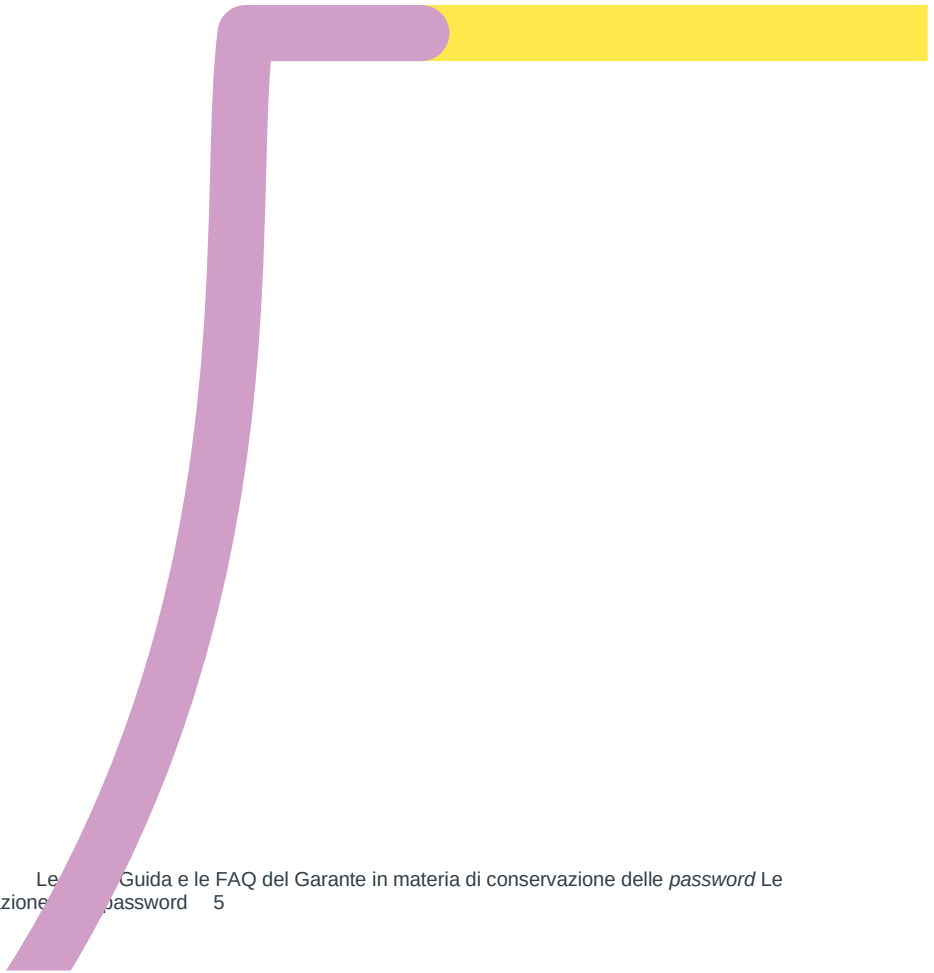
Il Provvedimento, le Linee Guida e i chiarimenti espressi dal Garante nelle FAQ fanno emergere la necessità di dover riconsiderare i presidi di sicurezza implementati ai fini della corretta gestione e conservazione delle *password*.

Ma non si tratta di un principio nuovo ovvero di un "recente" orientamento dell'Autorità.

In molti, infatti, ricorderanno bene l'art. 34 del D. Lgs. 196/2003 ("**Codice Privacy**") e l'Allegato B al Codice Privacy (abrogati da anni), con cui il legislatore italiano aveva già disposto l'adozione di misure minime di sicurezza, anche e soprattutto con riferimento alla corretta e sicura gestione delle procedure di autenticazione informatica.

Con l'introduzione del Regolamento è tuttavia venuta meno la previsione di una serie di "misure minime" la cui implementazione rappresentava un onere per i titolari del trattamento al fine di garantire quel livello "minimo" di sicurezza per anni richiesto dalla legge. Al suo posto, l'obbligo di dover adottare, preventivamente, misure tecniche ed organizzative adeguate a garantire la protezione dei dati personali in conformità al RGPD e l'obbligo di dover valutare quali misure di sicurezza adottare alla luce del grado di rischiosità dei trattamenti.

Ecco allora che le Linee Guida del Garante si pongono dunque come un valido ausilio alle valutazioni che titolari e responsabili del trattamento sono chiamati ad effettuare nel contesto dell'adeguata protezione e conservazione delle *password*.



Contatti

Adriano D'Ottavio

Counsel

+390669667000
adriano.dottavio@twobirds.com

Debora Stella

Counsel

+390230356000
debora.stella@twobirds.com

Sveva Placidi

Trainee

+390669667000
sveva.placidi@twobirds.com

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Shenzhen • Singapore • Stockholm • Sydney • Warsaw