FAQ - Linee guida in materia di conservazione delle password

1. **Quali sono i soggetti destinatari del provvedimento del Garante in materia di conservazione delle password?**

   Il provvedimento del Garante intende fornire indicazioni su modalità e tempi di conservazione delle password, rivolgendosi in primo luogo a tutti i titolari e i responsabili del trattamento che conservano credenziali di autenticazione di utenti dei propri servizi all'interno di sistemi informatici. Nell'osservanza delle linee guida, titolari e responsabili possono orientare le proprie scelte tecnologiche, oppure progettare e realizzare i propri sistemi informatici e servizi online, in conformità ai principi di limitazione della conservazione e di integrità e riservatezza, nonché agli obblighi in materia di sicurezza del trattamento (artt. 5, par. 1, lett. e) e f), e 32 del Regolamento (UE) 2016/679).

   Allo stesso tempo, il provvedimento invita i produttori di prodotti, servizi e applicazioni a tener conto delle indicazioni fornite dal Garante nelle fasi di progettazione e sviluppo, al fine di consentire a titolari e responsabili del trattamento di utilizzare sistemi e tecnologie che integrino i principî di protezione dei dati.

2. **Quali sono i soggetti tenuti ad adottare adeguate misure tecniche di protezione delle password?**

   L'adozione delle misure tecniche raccomandate nelle linee guida in materia di funzioni crittografiche per la conservazione delle password, o di misure che garantiscono un analogo livello di sicurezza, risulta necessaria qualora sia soddisfatta una o più delle seguenti condizioni:

   - il trattamento riguarda le password di un numero significativo di utenti (es. un numero elevato di soggetti in termini assoluti oppure espressi in percentuale della popolazione di riferimento a livello locale, regionale e nazionale);
   - il trattamento riguarda le password di utenti che possono accedere a banche dati di particolare rilevanza o dimensioni (es. dipendenti di pubbliche amministrazioni o grandi imprese od organizzazioni);
   - 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 (UE) 2016/679 (es. professionisti sanitari, avvocati, magistrati).

   Ricorrendo una o più delle predette condizioni, sono tenuti all'adozione di adeguate misure tecniche di protezione delle password, a titolo esemplificativo e non esaustivo, i seguenti soggetti: gestori delle identità digitali SPID e CieID; gestori di posta elettronica certificata;

prestatori di servizi fiduciari a norma del regolamento (UE) n. 910/2014; soggetti, pubblici e privati, che erogano servizi di conservazione dei documenti informatici a favore di terzi; società che offrono servizi di fatturazione elettronica; Presidenza del consiglio dei ministri e Ministeri; Agenzie fiscali; Enti e istituti di ricerca pubblici di rilievo nazionale; Enti pubblici non economici di rilievo nazionale; Autorità amministrative indipendenti; Forze di Polizia; Regioni e Province autonome; Province e Città metropolitane; Comuni con popolazione maggiore o uguale a diecimila abitanti; Federazioni nazionali, Ordini, Collegi e Consigli professionali; Camere di commercio, industria, artigianato e agricoltura; Università e Istituti di istruzione universitaria; strutture sanitarie pubbliche e private; società e aziende che forniscono servizi ICT; concessionari di servizi pubblici (trasporto pubblico locale, raccolta dei rifiuti, gestione dei servizi idrici, accertamento e riscossione dei tributi locali, ecc.); 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; partiti e movimenti politici; sindacati; CAF e patronati; 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); società che offrono servizi di biglietteria per eventi teatrali, sportivi ed altri eventi ricreativi e d'intrattenimento; società che erogano servizi di streaming.

3. **In caso di utilizzo di una procedura di autenticazione informatica a più fattori, è comunque necessario adottare misure di protezione delle password?**

   Sì, le linee guida in materia di funzioni crittografiche per la conservazione delle password si applicano anche in caso di utilizzo di una procedura di autenticazione a più fattori (c.d. strong authentication) basata, ad esempio, sul contestuale utilizzo di una password e di uno o più elementi appartenenti alle categorie del possesso (qualcosa che solo l'utente possiede, come una OTP – One Time Password – consegnata via SMS o generata su un dispositivo fisico o un’app, oppure una smart card con certificato digitale) o dell’inerenza (qualcosa che caratterizza l'utente, come l'impronta digitale o il riconoscimento facciale).

   Anche in questi casi è necessario proteggere adeguatamente le password degli utenti, in considerazione del fatto che questi ultimi potrebbero utilizzare la stessa password, o una simile, per l’accesso ad altri sistemi informatici o servizi online che non necessariamente prevedono procedure di autenticazione informatica a più fattori.

4. **In caso di conservazione della cronologia delle password, è necessario applicare misure di protezione anche alle password impostate in precedenza dagli utenti?**

   Sì, le linee guida si applicano anche alla cronologia delle password (c.d. password history). Anche in questi casi è necessario proteggere adeguatamente le password degli utenti, in considerazione del fatto che questi ultimi potrebbero utilizzare 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. **In quali casi occorre cancellare le password degli utenti seppure conservate in modo sicuro?**

   La conservazione delle password per un arco di tempo superiore a quello necessario per consentire la verifica dell'identità degli utenti ai fini dell'accesso a sistemi informatici o servizi online presenta rischi per i diritti e le libertà delle persone fisiche. Infatti, il progresso tecnologico, con il passare del tempo, può rendere obsolete le misure adottate per proteggere le password o comprometterne l'efficacia.

   Nel rispetto delle politiche di sicurezza adottate dal titolare o dal responsabile del trattamento, le password possono essere conservate anche per garantire la sicurezza delle procedure di autenticazione informatica, ad esempio per impedire il riuso da parte dell'utente delle precedenti password (c.d. password history) o per assicurare il ripristino del sistema di autenticazione informatica in caso di incidente (copie di backup).

   Per tali ragioni, le password degli utenti devono essere tempestivamente cancellate, anche in modo automatico, nei seguenti casi:

   - cessazione o dismissione dei sistemi informatici o servizi online a cui le credenziali di autenticazione consentivano l'accesso;
   - 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. **Come comportarsi in caso di violazione dei dati personali aventi ad oggetto password a cui erano state applicate adeguate misure tecniche di protezione?**

   L'adozione delle misure tecniche raccomandate nelle linee guida, o di misure che garantiscono un analogo livello di sicurezza, consente di mitigare in modo significativo i rischi per gli interessati in caso di violazione dei dati personali avente ad oggetto le password medesime.

   Come indicato anche nelle "Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali" (spec. caso n. 6), adottate dal Comitato europeo per la protezione dei dati il 14 dicembre 2021, tenuto conto di quanto previsto dall'art. 34, par. 3, lett. a), del

Regolamento (UE) 2016/679, se sono state adottate tecniche crittografiche allo stato dell'arte per proteggere le password degli utenti e non sono state 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 notificarla al Garante e comunicarla agli interessati coinvolti (artt. 33 e 34 del Regolamento (UE) 2016/679), fermo restando che la violazione deve essere comunque adeguatamente documentata (art. 33, par. 5, del Regolamento (UE) 2016/679).