Provvedimento del 17 aprile 2026 [10252460]

VEDI ANCHE Newsletter del 21 maggio 2026

[doc. web n. 10252460]

Provvedimento del 17 aprile 2026

Registro dei provvedimenti
n. 280 del 17 aprile 2026

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, e il dott. Agostino Ghiglia, componente, e il dott. Luigi Montuori, 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");

VISTE la notifica preliminare di violazione dei dati personali effettuata da The European House - Ambrosetti S.p.A. all'Autorità in data 8 aprile 2024, ai sensi dell'art. 33 del Regolamento, e la successiva notifica integrativa effettuata in data 23 maggio 2024;

ESAMINATA la documentazione in atti;

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

RELATORE la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. L'istruttoria dell'Ufficio sulla violazione dei dati personali oggetto di notifica, ai sensi dell'art. 33 del Regolamento.

The European House - Ambrosetti S.p.A. (di seguito, la Società), in data 8 aprile 2024, ha trasmesso all'Autorità, ai sensi dell'art. 33 del Regolamento, una notifica preliminare di violazione dei dati personali, determinata da una "esfiltrazione di dati in seguito ad accesso non autorizzato da parte di un attaccante" che ha riguardato i dati anagrafici e di contatto (indirizzo di posta elettronica) e le credenziali di autenticazione (username e password) di un numero non determinato di interessati.

La Società ha inoltre precisato che "sono ancora in corso indagini tecniche per individuare in

dettaglio i sistemi interessati" e ha rappresentato di non aver comunicato la violazione dei dati personali agli interessati coinvolti, ritenendo che la stessa non sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Il 9 aprile 2024, l'Ufficio ha rivolto alla Società una prima richiesta di informazioni, al fine di acquisire elementi utili alla valutazione dei profili di protezione dei dati personali e la Società, con nota del 17 aprile 2024, nell'evidenziare che "intende perfezionare [la notifica] in tutti i suoi elementi e conseguenti obblighi una volta esaurite le attività d'indagine tecnologica, presumibilmente entro il 30/05/2024" – ha rappresentato, tra le altre cose, che:

> "risulterebbero […] potenzialmente coinvolti 134.303 interessati. […] il numero deriva da una stima preliminare ma che si presume più basso, posto che, tenuto conto dell'esperienza professionale di Ambrosetti, spesso singoli interessati utilizzano e-mail differenti per autenticarsi ai servizi. La Società sta svolgendo tutte le opportune verifiche sul punto" (v. nota 17/04/2024, p. 2);
>
> "con l'entrata in vigore del GDPR nel 2016, la Società ha iniziato un processo di valutazione e implementazione di misure di sicurezza a presidio dei dati personali adeguate al nuovo dettato normativo, rispetto al quale si sintetizza di seguito quanto ad oggi svolto e di impatto per la questione in esame. Nel 2018 Ambrosetti ha avviato l'implementazione di un sistema di gestione delle password negli applicativi web, decidendo di adottare un sistema di crittografia delle password. Tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, la Società aveva quindi individuato in Bcrypt, uno dei principali strumenti consolidati sul mercato, l'algoritmo da utilizzare. Nel mentre sono proseguiti i lavori di rafforzamento dei sistemi di protezione, innescando parallelamente la Società lo studio e la fattibilità di una nuova architettura sistemica e applicativa. Viene quindi avviata nel 2021 una attività di selezione e ricerca, culminata nell'introduzione di sistemi certificati in grado di offrire servizi di sicurezza avanzata per le applicazioni web tali da soddisfare le necessità di aumento delle sicurezze aziendali. Il processo che viene portato avanti dalla Società prevede a partire dal gennaio 2022 la gestione della sola abilitazione a registrarsi ai portali di Ambrosetti. […] Il sistema invia automaticamente, all'indirizzo e-mail dell'utente comunicato dal cliente al momento di definizione dei rapporti contrattuali con la Società per l'erogazione dei servizi pattuiti tra le parti, il link, dedicato e personale, alla pagina web da cui l'utente accede ai servizi pattuiti, consentendo all'utente la creazione e gestione delle proprie credenziali di accesso" (v. nota cit., p. 3);
>
> "in merito alle valutazioni in ordine ai rischi per i diritti e le libertà degli interessati, è lo stesso Comitato nelle «Linee Guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali» a chiarire che le analisi dei casi proposte «si riferiscono esplicitamente a quelli in esame», con l'obiettivo di fornire assistenza ai titolari del trattamento per la valutazione delle violazioni dei dati che li riguardino, ma che, al contempo, «qualsiasi modifica delle circostanze riferite alle fattispecie descritte […] può comportare livelli di rischio diversi o più significativi, e quindi rendere necessarie misure diverse o supplementari», e la comunicazione può essere considerata una «buona prassi» solo in alcuni casi. Non si può quindi prescindere da valutazioni che tengano conto di tutti gli elementi concretamente sussistenti nel caso specifico in esame" (v, nota cit., p. 6);
>
> "Ambrosetti, pur analizzando le linee Guida ed il Caso 06 richiamati [… dall']Autorità, nella valutazione del rischio effettuata, ha proceduto ad approfondire quelle che sono le specificità del caso in esame, ed è giunta alla conclusione, tenuto conto di quanto ad oggi noto, che i rischi per i diritti e le libertà degli interessati siano trascurabili. Infatti, dagli accertamenti ad oggi svolti dalla Società, risulta che: 1. I dati esfiltrati sono tutti credenziali di accesso ad oggi

inutilizzabili, relative a sistemi non più in uso dal 2022: a partire dal 2022 la modalità di archiviazione delle credenziali di accesso ai sistemi di Ambrosetti è infatti cambiata […]. 2. I file di cui alla violazione notificata contengono credenziali di prima registrazione dei clienti di Ambrosetti, impostate dalla Società e rilasciate ai clienti successivamente alla definizione dei rapporti negoziali disciplinanti l'erogazione dei servizi di formazione al personale con gli stessi pattuiti. È onere dell'utente procedere alla modifica della password di ricevuta, nel rispetto dei vincoli di sicurezza imposti a sistema. Alla scadenza del contratto concluso con il cliente della Società, le utenze dei discenti sono automaticamente disattivate, e ciò comporta l'impossibilità di accesso ai servizi di Ambrosetti utilizzando dette credenziali. 3. È emerso altresì che il 96% dei dati esfiltrati sono relativi ad utenze inattive dal 31/12/2023 e, pertanto, inutilizzabili. Relativamente al restante 4%, successivamente alla scoperta della violazione in esame, la Società in data ha tempestivamente impostato l'obbligo per l'utente di modifica della propria password. Fermo restando che si tratta quindi di dati obsoleti quantomeno nel 96% dei casi ed in ogni caso di credenziali inutilizzabili in quanto relative a sistemi non più in uso, trattandosi altresì di credenziali di prima registrazione non impostate dall'utente, non sussistono rischi connessi all'abitudine degli utenti di utilizzare la stessa o similare password per l'accesso ad altri servizi online. 4. Inoltre […] è altresì emerso come solo «in un caso, le password fossero conservate in chiaro». Si tratta del file denominato «sgc_login.csv», che risulta essere un'estrazione di un database relativo ad un'applicazione non più in uso dal 18/11/2020, e pertanto tali dati non sono tecnicamente utilizzabili per accedere ai servizi della Società. 5. Vi è poi da considerare, che la violazione sostanzialmente non riguarda dati trattati in rapporto business to consumer bensì business to business; pertanto, gli interessati ai sensi di legge hanno ricevuto dai datori di lavoro policy che indicano specifiche cautele per la gestione delle password utilizzate nell'esecuzione delle proprie mansioni, nonché adeguata formazione in materia. 6. La violazione in esame riguarda credenziali di prima registrazione ai siti web della Società attraverso cui questa eroga servizi di formazione professionale, e che pertanto la natura dei siti e dei dati ipoteticamente accedibili non generano connotazioni negative per gli interessati. Non sono infatti in nessun caso presenti categorie di dati particolari quali ad esempio dati giudiziari o dati di pagamento, dati che rilevano appartenenza ad un sindacato o sullo stato di salute" (v. nota cit., pp. 6, 7);

"la Società, successivamente alla scoperta dell'evento, ha tempestivamente provveduto ad annullare tutte le password di accesso ai sistemi di Ambrosetti di cui ai file esfiltrati, imponendo agli utenti attivi l'obbligo di aggiornamento delle proprie password, nel rispetto dei vincoli di sicurezza imposti dalla Società per l'accesso ai propri sistemi" (v. nota cit., p. 7);

"la Società ha sin da subito organizzato un team multidisciplinare dedicato alla questione, composto dai referenti ICT interni, dal DPO e dai consulenti in cybersecurity esterni, che ad oggi continua a gestire e monitorare gli accertamenti in corso" (v. nota cit., p. 7).

Il 18 aprile 2024, l'Ufficio ha rivolto alla Società una seconda richiesta di informazioni, al fine di acquisire ulteriori elementi in merito alla violazione dei dati personali, evidenziando come, all'esito di un accertamento tecnico effettuato sui dati oggetto di diffusione in rete, alcune delle password in questione apparissero impostate dagli utenti a cui le stesse si riferiscono.

Con nota del 24 aprile 2024, la Società ha fornito riscontro alla predetta richiesta di informazioni, rappresentando che:

le credenziali di autenticazione oggetto di diffusione erano relative ai diversi servizi online o applicazioni web della Società ("aggiornamentoconoscenza.it", "cocircle.ambrosetti.eu", "fondir.ambrosetti.eu", "healthcare.ambrosetti.eu", "innotechhub.ambrosetti.eu", "live.ambrosetti.eu", "management.ambrosetti.eu", "www.aggiornamentopermanente.it", "www.ambrosetti.eu", "www.ambrosettilive.eu" e "www.leaderdelfuturo.it") (v. nota

24/04/2024, pp. 1-3);

“le suddette applicazioni permettono un potenziale accesso esclusivamente agli utenti che avevano attivato il servizio erogato tramite l’applicazione, rendendo tecnicamente impossibile l’autenticazione ai clienti che non avevano acquistato il relativo servizio. Tutti i portali […] richiamati consentivano esclusivamente l’accesso a contenuti formativi quali ad esempio slide, ricerche e presentazioni, o l’iscrizione ad eventi organizzati dalla Società” (v. nota cit., p. 3);

“le categorie di utenti a cui si riferiscono le credenziali di autenticazione sono: dipendenti di clienti della Società e dipendenti della Società. Nel file AP_USERS-AMBROSETTI.CSV l’indirizzo e-mail presente non era reale, e quindi né direttamente né indirettamente consentiva di individuare una persona fisica; bensì semplicemente inserito in quanto campo obbligatorio poiché tecnicamente richiesto come necessario dall’applicazione” (v. nota cit., p. 3);

“si precisa rispetto ai singoli files le funzioni crittografiche che erano state adottate:”

> login_users.csv: “MD5 (Message Digest Algorithm 5), funzione di hash crittografica ampiamente diffusa e supportata da un'ampia varietà di software e hardware per calcolare l'hash di una stringa o un messaggio, nota per la sua efficienza computazionale, semplicità, ampia diffusione e compatibilità, risultando una soluzione compatibile con la varietà dei software e hardware a suo tempo in uso dalla Società”;
>
> ldf_users.csv: “il sito è sviluppato con Joomla 1.5 ed usa MD5 con un salt di 32 caratteri che viene aggiunto alla fine della stringa della password stessa”;
>
> ap_users.csv: “il sito è sviluppato con Joomla 1.5 ed usa MD5 per effettuare l'hashing delle passwords. Quando vengono create le password, vengono sottoposte ad hashing con un salt di 32 caratteri che viene aggiunto alla fine della stringa della password stessa”;
>
> chat_users.csv e uni_login.csv: “misto di md5 e md5 con salt di 32 caratteri che viene aggiunto alla fine della stringa della password stessa” (v. nota cit., p. 4);

con riferimento alle modalità con le quali le password in questione sono state impostate:

> login_users.csv: “le password sono state impostate da un amministratore di sistema all’atto della creazione dell’utenza e poi modificabili dallo stesso utente. Essendo presente la funzione crittografica MD5 non è tecnicamente possibile verificare se le password siano state preimpostate dall'amministratore o cambiate dall'utente”;
>
> sgc_login.csv: “le password sono state impostate da un amministratore di sistema all’atto della creazione dell’utenza e poi modificabili dallo stesso utente”;
>
> ldf_users.csv e ap_users.csv: “le password sono state impostate da un amministratore di sistema all’atto della creazione dell’utenza e poi modificabili dallo stesso utente. Essendo presente la funzione crittografica MD5 con salt non è tecnicamente possibile verificare se le password siano state preimpostate dall'amministratore o cambiate dall'utente”;
>
> chat_users.csv e uni_login.csv: “le password sono state impostate da un amministratore di sistema all’atto della creazione dell’utenza” (v. nota cit., pp. 4, 5);

una delle applicazioni web della Società (“aggiornamentoconoscenza.it”) è stata dismessa

nel mese di marzo 2020, mentre le altre applicazioni web sono state oggetto di interventi di aggiornamento dell'algoritmo di password hashing svolti nel periodo che va da febbraio 2020 a ottobre 2022 (v. nota cit., p. 5);

"la Società conserva i dati personali trattati nell'esecuzione delle attività pattuite con i clienti per dieci anni successivi alla cessazione dei rapporti con il cliente per l'adempimento di obblighi normativi (es. fiscali, contabili) che permangono anche successivamente alla cessazione dei rapporti, nonché per far valere in giudizio i diritti derivanti dal contratto. A tal fine, si evidenzia che la Società, stante anche la tipologia e la varietà dei servizi erogati ed i consolidati rapporti nel tempo con la propria clientela, ha adottato una prassi commerciale di gestione dei rapporti contrattuali con i clienti che tende a propendere per la definizione di accordi quadro, disciplinanti genericamente i rapporti tra le parti e dalla durata indeterminata salva la facoltà di ciascuna parte di cessare i rapporti con adeguato preavviso, affiancati alle singole offerte disciplinanti le specifiche attività di volta in volta richieste. Inoltre, i servizi erogati dalla Società sono caratterizzati, per loro stessa natura, anche dalla ripetitività nel tempo della richiesta di tipologie di servizi analoghi da parte del medesimo cliente (es. Servizi di formazione ripetuti a cadenze concordate, ma relativi ad argomenti diversi e quindi disciplinati da specifiche offerte del caso), con conseguente perdurare nel tempo dei rapporti con la propria clientela, che comportano quindi la necessità di conservazione dei relativi dati" (v. nota cit., p. 6);

"al momento della richiesta di settaggio della nuova password, all'utente è apparso il seguente messaggio: […] Si sconsiglia l'utilizzo di una password già utilizzata in altri sistemi. La password deve essere composta da almeno 8 caratteri e includere almeno un simbolo speciale, una lettera maiuscola, una lettera minuscola e un numero. […] In attesa di definire gli accertamenti in corso, ad oggi non sono state mandate ulteriori comunicazioni agli utenti" (v. nota cit., pp. 6, 7);

"soltanto un numero limitato di Clienti ha richiesto di avere degli approfondimenti sulla nota vicenda. In tali casi, si sono pertanto svolte alcune riunioni ad hoc alla presenza dei rispettivi tecnici informatici e DPO, i quali, ad oggi, hanno tutti convenuto per la trascuratezza del rischio" (v. nota cit., p. 7).

Successivamente, con la notifica integrativa del 23 maggio 2024, la Società ha fornito ulteriori informazioni sulle iniziative assunte a seguito della violazione dei dati personali e ne ha confermato la natura e la portata.

La Società, in tale occasione, ha inoltre ribadito di non aver effettuato agli interessati alcuna comunicazione ai sensi dell'art. 34 del Regolamento.

Nelle more dello svolgimento dell'istruttoria, l'Ufficio ha poi valutato la conformità delle iniziative intraprese dalla Società, a seguito della violazione, con particolare riferimento all'adempimento degli obblighi di comunicazione di cui all'art. 34 del Regolamento nei confronti degli interessati a cui sono riferite le credenziali di autenticazione oggetto di violazione.

In particolare, dall'esame di quanto dichiarato, il Garante ha ritenuto che la violazione dei dati personali in questione fosse suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, contrariamente a quanto sostenuto dalla Società, e pertanto, con il provvedimento n. 327 del 23 maggio 2024 (doc. web n. 10037682 in www.garanteprivacy.it), ha ingiunto alla stessa, ai sensi degli artt. 34, par. 4, e 58, par. 2, lett. e), del Regolamento, di comunicare la violazione dei dati personali agli utenti le cui password erano conservate in chiaro o con tecniche crittografiche non allo stato dell'arte.

Con il predetto provvedimento, l'Autorità ha altresì chiesto alla Società di fornire un riscontro

adeguatamente documentato in merito alle iniziative intraprese al fine di comunicare la violazione dei dati personali agli utenti le cui password erano conservate in chiaro o con tecniche crittografiche non allo stato dell'arte.

In adempimento di ciò, con nota del 7 giugno 2024, la Società ha rappresentato che:

> "la comunicazione è stata effettuata direttamente con riferimento agli interessati rispetto ai quali la società ha nella propria disponibilità un indirizzo di posta elettronica. In data 07/06/2024 la Società ha pertanto inviato a 54.917 interessati il testo contenuto nel documento All. 1 – 240607 Comunicazione Interessati" (v. nota 07/06/2024, p. 1);
>
> "al fine di garantire un'analoga efficacia anche nei confronti degli interessati rispetto ai quali non si dispone di un contatto diretto, la Società ha optato per differenti canali di comunicazione, provvedendo:
>
> > in data 07/06/2024 a pubblicare sul proprio portale aziendale una pagina dedicata reperibile al presente link https://www.ambrosetti.eu/news/violazione-informatica-in-the-european-house-ambrosetti/
> >
> > in data 07/06/2024 ad inviare a 25 testate giornalistiche, elencate nell'allegato All. 3 – 240607 Lista testate invio CS, databreach_070624, il testo del documento All. 2 – 240607 Sito Comunicato, ai fini della pubblicazione su canali di ampia diffusione" (v. nota cit., p. 1).

Il 12 giugno 2024, l'Ufficio ha rivolto alla Società una terza richiesta di informazioni, al fine di acquisire ulteriori elementi in merito all'adempimento del citato provvedimento del Garante da parte della Società.

Con nota del 17 giugno 2024, la Società ha fornito riscontro alla predetta richiesta di informazioni, rappresentando che:

> "gli interessati rispetto ai quali la Società non dispone di un contatto diretto sono 12.709. In ragione del necessario lavoro manuale di pulizia e del riconoscimento di taluni utenti, il numero potrà essere ulteriormente ridotto" (v. nota 17/06/2024, p. 1);
>
> in data 17 giugno 2024, l'ANSA ha pubblicato "nell'area paywall" il comunicato stampa trasmesso dalla Società; "in seguito ai comunicati inviati alle altre testate giornalistiche, già dalla scorsa settimana la Società si è attivata con dei recall per richiedere nuovamente la pubblicazione del comunicato. Ad oggi sono in corso delle interlocuzioni con il Corriere della Sera, Il Sole 24 Ore e Repubblica al fine di concordare un'ulteriore eventuale pubblicazione" (v. nota cit., pp. 1, 2);
>
> "in assenza di un legame diretto fra i residui interessati non raggiunti via email e le aziende di appartenenza, abbiamo lanciato una campagna sui social di TEHA" (LinkedIn, Facebook, X, Threads e Instagram) (v. nota cit., p. 3);
>
> "la Società ha inviato un comunicato contente un incident report alle Società interessate richiedenti, chiedendo di dare ampia diffusione dell'accaduto al proprio interno (es. pubblicandolo sulla intranet e/o sulla bacheca aziendale), al fine di massimizzarne la conoscibilità tra i propri dipendenti" (v. nota cit., p. 3).

Successivamente, con nota del 3 luglio 2024, la Società ha fornito alcuni ulteriori aggiornamenti, in merito alle ulteriori misure adottate per informare gli interessati, rappresentando, tra le altre cose, che:

"Ambrosetti ha inviato a 83 Società proprie clienti presso cui lavorano 11.264 interessati, un comunicato di dettaglio […] chiedendo altresì a tale Società di dare ampia diffusione dell'accaduto al proprio interno (es. pubblicandolo sulla intranet e/o sulla bacheca aziendale), al fine di massimizzarne la conoscibilità tra gli interessati. A seguito della comunicazione di cui sopra, 4 Società hanno richiesto ulteriori chiarimenti, che sono stati forniti durante incontri in videoconferenza" (v. nota 03/07/2024, p. 1);

"il comunicato stampa relativo alla violazione dei dati personali è stato pubblicato sul quotidiano nazionale "La Repubblica" in data 01/07/2024 a pag. 14 […], con tiratura di 125.502 e diffusione di 138.093 copie" (v. nota cit., p. 2);

"nell'homepage del sito web aziendale raggiungibile all'indirizzo www.ambrosetti.eu, posizionato in alto centralmente ed evidenziato da una cornice arancione […], continua ad essere pubblicato specifico avviso relativo alla violazione, contenente link alla pagina web in cui sono disponibili news e comunicazioni di Ambrosetti sul punto" (v. nota cit., p. 2);

"prosegue la campagna lanciata sui social di TEHA" (v. nota cit., p. 2);

"per completezza di informazioni, si rende noto […] il recente sviluppo nelle operazioni di riorganizzazione societaria del gruppo. In data 02 luglio u.s. è stata infatti costituita la TEHA Group S.p.A., società soggetta a Direzione e Coordinamento da parte di The European House - Ambrosetti S.p.A. a cui verranno demandate attività operative" (v. nota cit., p. 3).

All'esito delle valutazioni tecniche di competenza, l'Ufficio ha redatto, in data 22 luglio 2024, una specifica relazione tecnica in cui sono stati ravvisati gli estremi di una violazione degli obblighi di cui all'art. 34 del Regolamento in relazione alla tardiva comunicazione, da parte della Società, della violazione di dati personali agli utenti dei propri servizi online le cui password erano conservate in chiaro o con tecniche crittografiche non allo stato dell'arte. Sono stati ravvisati, inoltre, gli estremi di una violazione dei principi di limitazione della conservazione e di integrità e riservatezza di cui all'art. 5, par. 1, lett. e) e f), del Regolamento, nonché degli obblighi in materia di sicurezza del trattamento di cui all'art. 32 del Regolamento.

2. L'avvio del procedimento per l'adozione dei provvedimenti correttivi e le deduzioni della Società.

Sulla base delle violazioni accertate con la relazione tecnica di cui sopra, il 18 settembre 2024, l'Ufficio ha effettuato, ai sensi dell'art. 166, comma 5, del Codice, la notificazione delle presunte violazioni del Regolamento nei confronti della Società, con riferimento agli artt. 5, par. 1, lett. e) e f), 32 e 34 del Regolamento, , per avere conservato, in chiaro o con tecniche crittografiche non allo stato dell'arte, le password degli utenti, per avere conservato le credenziali di autenticazione degli stessi utenti, relative ad alcuni sistemi, non più in uso e per non avere informato gli interessati coinvolti dalla violazione dei dati personali occorsa, essendovi tenuta.

Con scritti difensivi inviati in data 16 ottobre 2024, la Società ha rappresentato che:

- "la violazione ha riguardato nome, cognome, username (corrispondente alla e-mail) e password di accesso a servizi di Ambrosetti. Il trattamento di tali categorie di dati è necessario per l'esecuzione dei servizi offerti dalla Società ai propri clienti (es. formazione, consulenza etc.)" (v. nota 16/10/2024, p. 1);

- "inizialmente la Società non ha ritenuto la violazione suscettibile di presentare un rischio elevato per gli interessati, avendo in ogni caso provveduto, nell'immediatezza della scoperta, a imporre la modifica delle credenziali di accesso ai propri servizi, avviando altresì analisi approfondite dell'evento" (v. nota cit., p. 1);

- “in base alle informazioni al tempo disponibili, risultavano potenzialmente coinvolti 134.303 interessati. Le analisi ad oggi svolte da Ambrosetti hanno permesso di circoscrivere il numero di interessati coinvolti a 61.670. Applicando un processo progressivo di de-duplicazione, considerando uguali le righe riferite allo stesso nome/cognome ed e-mail, sono stati eliminati i duplicati (es. Utenti presenti più volte, con nome e cognome uguali seguiti ogni volta da numeri diversi; Utenti inseriti più volte con "Nome/punto/Cognome", "Nome/spazio/cognome", "NomeCognome", "NomeCognomeNumero"; Indirizzi e-mail presenti più volte, preceduti o seguiti da caratteri speciali). A tale normalizzazione automatica dei campi ha fatto seguito ulteriore aggiornamento manuale volto a eliminare utenze non riconducibili, né direttamente né indirettamente, a persone fisiche, quali utenti fittizi, riducendo quindi il numero di interessati nel caso di specie. Gli approfondimenti svolti dalla Società negli ultimi mesi hanno altresì consentito di precisare che gli interessati le cui utenze risultavano archiviate con password in chiaro sono 25.705” (v. nota cit., pp. 1, 2);

- “in seguito alle suddette analisi tecniche svolte, nonché in ragione delle comunicazioni intercorse con [… l’] Autorità, la Società ha quindi provveduto a comunicare la violazione con le modalità già dettagliate. In particolare, la comunicazione della violazione è stata inviata a mezzo e-mail a 54.917 soggetti, pari all’89% del totale degli interessati nel caso di specie. Ambrosetti ha altresì provveduto a informare gli interessati contattando le società proprie clienti presso cui lavorano gli interessati, pubblicando specifico banner nella homepage del proprio sito web, mediante post dedicati sui canali social aziendali e provvedendo alla pubblicazione del comunicato stampa […] su Ansa.it e sul quotidiano nazionale “La Repubblica”” (v. nota cit., p. 2);

- “la condotta non è dolosa in quanto non c’è stata la coscienza e volontà dell’azienda nel violare specifiche norme di legge e di causare o accettare anche potenzialmente di recare rischi agli interessati” (v. nota cit., p. 2);

- “i servizi erogati dalla Società, per loro stessa natura, [sono] caratterizzati dalla ripetitività nel tempo di analoghe richieste da parte dei propri clienti di tipologie di servizi analoghi da parte del medesimo cliente (es. Servizi di formazione ripetuti a cadenze concordate). In risposta anche alle esigenze dei clienti per l’avvio dei progetti di volta in volta concordati, la Società tende quindi a propendere per la definizione di accordi disciplinanti, all’inizio, genericamente i rapporti continuativi tra le parti, di durata quindi tendenzialmente indeterminata, a cui si affiancano singoli ordini/offerte di dettaglio delle attività di volta in volta richieste. Fintanto che perdurano i rapporti con i propri clienti, il trattamento dei relativi dati personali (quali nome, cognome, email) è quindi necessario alla Società per poter erogare i propri servizi” (v. nota cit., pp. 2, 3);

- “la Società ha da tempo intrapreso un percorso di continuo efficientamento di fatto della sicurezza delle applicazioni e dei dati, ivi ricomprendendo il tema della protezione e gestione degli accessi, in ottica di perpetuo rafforzamento della resilienza sistemica ed applicativa” (v. nota cit., p. 3);

- “nell’immediatezza della scoperta dell’incidente, è stato imposto l’obbligo di modifica delle credenziali di accesso ai sistemi di Ambrosetti di cui ai file esfiltrati, imponendo l’obbligo di aggiornamento delle proprie password, nel rispetto dei vincoli di sicurezza imposti dalla Società per l’accesso ai propri sistemi. La Società ha sin da subito organizzato un team multidisciplinare dedicato alla questione, composto dai referenti ICT interni, dal DPO e dai consulenti in cybersecurity esterni, che ad oggi continua a gestire e monitorare la vicenda. La Società ha provveduto a comunicare l’incidente” (v. nota cit., p. 3);

- “dal 2016 la Società ha iniziato un processo di valutazione e implementazione di misure di sicurezza a presidio dei dati personali adeguate al nuovo dettato normativo in materia di dati

personali, avviando a tal fine lo studio e la fattibilità di una nuova architettura sistemica e applicativa aziendale. Viene quindi avviata una attività di selezione e ricerca, culminata nell'introduzione di sistemi certificati in grado di offrire servizi di sicurezza avanzata per le applicazioni web tali da soddisfare le necessità di aumento delle sicurezze aziendali. Il processo che viene portato avanti dalla Società prevede a partire dal gennaio 2022 la gestione della sola abilitazione a registrarsi ai portali di Ambrosetti, consentendo all'utente la creazione e gestione delle proprie credenziali di accesso in base alle regole e Access Control List (ACL) definite a sistema. [OMISSIS] (v. nota cit., pp. 3, 4);

- "[OMISSIS]" (v. nota cit., p. 4);

- "la violazione ha riguardato esclusivamente dati identificativi e di accesso degli interessati, e non ha interessato categorie particolari di dati personali" (v. nota cit., p. 4);

- "la Società è venuta a conoscenza della potenziale violazione da un post pubblicato sul social network "X" e, verificata la fondatezza della notizia, ha provveduto a notificare la violazione [… all']Autorità" (v. nota cit., p. 4);

- "durante la pandemia di COVID-19, la Società ha dovuto modificare in tempi brevi le modalità di erogazione dei propri servizi, aumentando drasticamente le attività svolte da remoto che, da residuali, sono diventate, stante la natura stessa dell'attività imprenditoriale di Ambrosetti, le uniche possibili. Ciò ha comportato il conseguente aumento esponenziale delle richieste di attivazione di nuovi strumenti e modalità, da rendere operativi con tempistiche ben inferiori rispetto all'ordinario processo di implementazione che la Società aveva in essere, e con risorse anche di personale ridotte, stante l'emergenza sanitaria […]. Situazione emergenziale che ha quindi contribuito al concretizzarsi ed alla mancata tempestiva rilevazione della disattenzione del 2020 che ha comportato il mancato rispetto delle procedure aziendali, adottate dal 2018, che prevedevano (e prevedono) l'adozione di adeguate misure di sicurezza e la cancellazione dei dati personali il cui trattamento non sia più necessario, come quelli relativi ad applicazioni non più in uso, nonché controlli periodici su quanto implementato" (v. nota cit., p. 5).

In data 16 dicembre 2024, si è tenuta l'audizione della Società, come chiesto dalla stessa. In tale occasione la parte ha rappresentato che:

- "per quanto riguarda la violazione dell'art. 34 del Regolamento la Società inizialmente non aveva ritenuto di inviare la comunicazione della violazione agli interessati in quanto destavano particolare preoccupazione i possibili rischi reputazionali derivanti dall'invio di detta comunicazione che avrebbe avuto un impatto mediatico in un periodo in cui la Società era impegnata, da un lato, ad organizzare la cinquantesima edizione del forum di Cernobbio, che si è tenuta all'inizio del mese di settembre 2024 […] e, dall'altro, a gestire una serie di cambiamenti relativi all'assetto societario (liquidazione di uno dei soci residui della famiglia Ambrosetti; costituzione di TEHA Group S.p.A.; trasformazione dei contratti stipulati con i propri collaboratori in assunzioni a tempo indeterminato)";

- "la Società ha interrotto il rapporto con il precedente Dpo […], in quanto ha ritenuto di non avere avuto da tale figura l'adeguato supporto formativo ed informativo sui diritti e obblighi sanciti dal Regolamento nei confronti del Titolare del trattamento, nonché nella valutazione dei rischi derivanti dalla violazione dei dati personali";

- "la violazione dei dati personali è avvenuta tramite un accesso non autorizzato a un database che serviva circa dieci applicativi. È stata sfruttata una vulnerabilità di tipo sql injection che è stata scoperta solo post incidente";

- “lo sviluppo dei predetti applicativi era stato affidato a personale esterno inizialmente impiegato per lo svolgimento di incarichi relativi alla componente sistemistica dei sistemi informativi. Con la crescente esigenza di sviluppare rapidamente un numero considerevole di applicazioni, dovuta all'importanza sempre maggiore della presenza online in seguito alle restrizioni imposte per contrastare il Covid-19, questi fornitori hanno trovato un impiego sempre più rilevante anche nella sfera applicativa. Gli applicativi gestiti dalla Società sono così cresciuti in maniera esponenziale durante la pandemia ed è stata data maggiore rilevanza alla loro gestione operativa piuttosto che al controllo sistematico della loro sicurezza applicativa, assumendo che la sicurezza fosse assolta dai citati fornitori”;

- "successivamente alla violazione la Società si è resa conto che i fornitori esterni non avevano le competenze adeguate per sviluppare tali applicativi tenendo conto anche degli aspetti relativi alla sicurezza e alla protezione dei dati personali”;

- “al momento della violazione dei dati personali erano stati effettuati degli interventi di miglioramento delle procedure di autenticazione informatica utilizzate nell’ambito dei citati applicativi attraverso l’adozione e l’integrazione con nuovi sistemi IAM (identity access management) e l’introduzione di un secondo fattore di autenticazione”;

- “la Società non era consapevole né del fatto che all’interno del citato database fossero ancora conservate le password degli utenti né delle misure tecniche adottate dai fornitori esterni per proteggerle”;

- “a seguito della violazione dei dati personali la Società ha messo in campo una serie di iniziative ed investimenti per l’adozione di ulteriori misure tecniche organizzative […] tra queste si segnalano: la scelta di avviare un percorso per l’ottenimento della certificazione ISO 27001, la cessazione dei contratti con i fornitori esterni senza competenze in materia di sicurezza per la componente di sviluppo applicativo e al netto delle remediation delle vulnerabilità riscontrate, la definizione di una procedura per l’affidamento di incarico a fornitori ICT esterni che prevedesse anche una valutazione delle competenze di cyber security, la risoluzione anticipata del contratto con il precedente Dpo […] e la sottoscrizione di un diverso rapporto contrattuale con un nuovo Dpo; la previsione di iniziative formative rivolte al personale, rafforzamento del dipartimento IT con la ricerca attiva di un nuovo responsabile. […] la Società ha avviato un percorso di responsabilizzazione e di cambiamento in materia di protezione dei dati personali, che consentirà di gestire al meglio eventuali violazioni future”.

3. L’esito dell’istruttoria e del procedimento per l’adozione dei provvedimenti correttivi e sanzionatori.

All’esito dell’esame delle dichiarazioni rese all’Autorità nel corso del procedimento nonché della documentazione acquisita, risulta che la Società, in qualità di titolare, ha effettuato alcune operazioni di trattamento che risultano non conformi alla disciplina in materia di protezione dei dati personali per i motivi di seguito indicati.

In particolare risulta accertato che la Società non ha comunicato la violazione dei dati personali ai sensi dell’art. 34 del Regolamento agli interessati coinvolti nonostante la violazione fosse suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La Società, inoltre, ha conservato, in chiaro o con tecniche crittografiche non allo stato dell’arte, le password degli utenti e ha conservato le credenziali di autenticazione degli stessi utenti oggetto di violazione relative ad alcuni sistemi non più in uso.

In proposito, si evidenzia che, salvo che il fatto non costituisca più grave reato, chiunque, in un

procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante".

3.1. Il quadro normativo di riferimento.

L'art. 34 del Regolamento dispone 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" (par. 1), che "la comunicazione all'interessato […] descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)" (par. 2) e che detta comunicazione non è richiesta, in particolare, se "il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura" (par. 3, lett. a)).

L'art. 5, par. 1, del Regolamento stabilisce che i dati personali devono essere "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati […] («limitazione della conservazione»)" (lett. e)) e devono essere "trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)" (lett. f)).

L'art. 32 del Regolamento, concernente la sicurezza del trattamento, dispone poi che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" (par. 1) e che "nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati" (par. 2).

Con particolare riferimento alle misure da porre in essere, in caso di conservazione delle password di utenti, il Garante ha adottato, in collaborazione con l'Agenzia per la cybersicurezza nazionale, specifiche linee guida in materia di conservazione delle password (provvedimento n. 594 del 7 dicembre 2023, doc. web n. 9962283 in www.garanteprivacy.it), con le quali ha fornito ai titolari e ai responsabili del trattamento indicazioni e raccomandazioni sugli algoritmi di password hashing allo stato dell'arte, ricordando, tra l'altro, che: "Risulta […] fondamentale che gli algoritmi di password hashing presentino i seguenti requisiti:

> una complessità computazionale tale per cui sia rapido calcolare un singolo digest, ma sia eccessivamente dispendioso calcolarne un numero elevato, così da scoraggiare gli attaccanti a cercare le password degli utenti procedendo per tentativi;
>
> una capacità di memoria richiesta tale da saturare la RAM quando molti digest vengono calcolati contemporaneamente.

Per tali ragioni, quando si parla di password hashing, servono algoritmi ad hoc che mirino a rallentare le capacità offensive dell'attaccante." (p. 7).

È stato inoltre rammentato che "è fortemente sconsigliato calcolare un digest per la conservazione

delle password tramite la semplice applicazione singola di una funzione di hash crittografica come quelle indicate [… nelle “Linee guida funzioni crittografiche – Funzioni di Hash” adottate dall’ACN]” (p. 9)”.

3.2. Mancata comunicazione della violazione dei dati personali agli interessati.

È stato in primo luogo accertato, sulla base delle risultanze della specifica relazione tecnica redatta in data 22 luglio 2024, che la Società non ha informato gli interessati coinvolti dalla violazione dei dati personali, pari a 61.670.

Ciò, in quanto la stessa ha ritenuto che la violazione dei dati personali, avente ad oggetto le credenziali di autenticazione (username e password) degli utenti dei propri servizi online, non fosse suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

A differenza di quanto sostenuto dalla Società, il Garante, già con il provvedimento n. 327 del 23 maggio 2024, ha ritenuto invece che la violazione dei dati personali fosse suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche e che pertanto la Società avrebbe dovuto effettuare la comunicazione agli interessati ai sensi dell’art. 34, par. 1, del Regolamento.

Ciò, in considerazione di una molteplicità di fattori, in particolare: la natura della violazione dei dati personali che si è verificata nell’ambito di un attacco informatico finalizzato ad acquisire credenziali di autenticazione (username e password, in alcuni casi sotto forma di stringa di testo, detta anche digest) e altri dati personali (tra i quali, nome, cognome e indirizzo di posta elettronica, in alcuni casi fittizio); la gravità e la persistenza delle possibili conseguenze per le persone fisiche che potrebbero derivare dall’utilizzo delle credenziali di autenticazione oggetto di diffusione per accedere illecitamente a sistemi informatici o servizi online e consultare, o acquisire, dati personali degli interessati a cui sono riferite o di altre categorie di interessati.

Al riguardo occorre tenere in considerazione anche le modalità di impostazione delle password (che in assenza di elementi idonei a comprovare il contrario – debbono essere considerate, in via prudenziale, come se fossero state scelte da ciascun utente) e l’abitudine degli utenti di utilizzare la medesima password, anche a distanza di tempo, per lo stesso o per altri sistemi informatici o servizi online o, comunque, di utilizzare password simili tra loro cambiando solo alcuni caratteri.

Sono stati inoltre considerati il numero elevato di interessati a cui sono riferite le credenziali di autenticazione in questione e la facilità con cui è possibile risalire a specifiche persone fisiche, identificate o identificabili, dai dati personali oggetto di violazione; il basso livello di sicurezza garantito dalle funzioni crittografiche utilizzate per proteggere le password degli utenti conservate nei sistemi della Società, in termini di resistenza ai più comuni attacchi informatici (es. a forza bruta o a dizionario) volti a individuare la password che ha generato un determinato digest.

In particolare, in relazione a quest’ultimo fattore - da valutarsi anche alla luce delle indicazioni e raccomandazioni fornite dal Garante con le citate linee guida in materia di conservazione delle password, predisposte in collaborazione con l’Agenzia per la cybersicurezza nazionale - è emerso che alcune password (circa 98.000) erano conservate previa applicazione di una funzione di hashing (“MD5”, non sempre con l’utilizzo di un salt) non in grado di assicurare un adeguato livello di sicurezza, mentre altre (circa 36.000) erano addirittura conservate in chiaro.

Pertanto, con il citato provvedimento del 23 maggio 2024, il Garante – anche tenuto conto del fatto che non risultava soddisfatta alcuna delle condizioni di cui all’art. 34, par. 3, del Regolamento in presenza delle quali non è richiesta la comunicazione agli interessati a seguito di una violazione di dati – ha ingiunto alla Società di comunicare la violazione dei dati personali agli utenti le cui password erano conservate in chiaro o con tecniche crittografiche non allo stato dell’arte,

descrivendone con un linguaggio semplice e chiaro la natura e le possibili conseguenze, nonché fornendo indicazioni specifiche sulle misure che gli stessi interessati possono adottare per proteggersi da eventuali conseguenze negative della violazione.

Solo a seguito del provvedimento correttivo adottato dall'Autorità, la Società ha informato gli interessati, coinvolti nella violazione dei dati personali, ai sensi dell'art. 34 del Regolamento, con l'invio di una comunicazione a 54.917 interessati per i quali disponeva di un indirizzo di posta elettronica e con l'effettuazione di comunicazioni pubbliche per informare i restanti 12.709 interessati.

Tali comunicazioni pubbliche sono state effettuate: tramite comunicati stampa pubblicati sul sito web e sui canali social della Società e su un quotidiano a tiratura nazionale, nonché inviati ad alcune società clienti (presso cui lavorano numerosi interessati) con l'invito a darne ampia diffusione al loro interno al fine di massimizzarne la conoscibilità tra gli interessati coinvolti.

In particolare, è emerso che la comunicazione della violazione dei dati personali agli interessati coinvolti è stata effettuata tardivamente, rispetto al momento in cui la Società ne è venuta a conoscenza (4 aprile 2024): circa 55.000 interessati sono stati infatti informati solo in data 7 giugno 2024, con una comunicazione diretta, mentre circa 13.000 interessati sono stati informati, solo con comunicazioni pubbliche effettuate nei mesi di giugno e luglio 2024.

In proposito la Società ha precisato che il motivo del ritardo nella comunicazione è dipeso dal fatto che "inizialmente la Società non ha ritenuto la violazione suscettibile di presentare un rischio elevato per gli interessati" (v. nota 16/10/2024, p. 1) nonché "in quanto destavano particolare preoccupazione i possibili rischi reputazionali derivanti dall'invio di detta comunicazione che avrebbe avuto un impatto mediatico in un periodo in cui la Società era impegnata, da un lato, ad organizzare la cinquantesima edizione del forum di Cernobbio, che si è tenuta all'inizio del mese di settembre 2024 […] e, dall'altro, a gestire una serie di cambiamenti relativi all'assetto societario (liquidazione di uno dei soci residui della famiglia Ambrosetti; costituzione di TEHA Group S.p.A.; trasformazione dei contratti stipulati con i propri collaboratori in assunzioni a tempo indeterminato)" (v. verbale audizione 16/12/2024).

Le motivazioni addotte dalla Società non giustificano il ritardo con il quale è stata effettuata, peraltro a seguito di un provvedimento correttivo dell'Autorità, la comunicazione ai sensi dell'art. 34 del Regolamento.

Si osserva, inoltre, che l'avere fatto prevalere motivi reputazionali sui diritti di protezione dei dati degli interessati rappresenta un elemento di evidente scarso rispetto del principio di accountability al quale il titolare ha l'obbligo di conformare i trattamenti dallo stesso effettuati.

La Società, con la tardiva comunicazione della violazione dei dati personali, ha pertanto violato quanto previsto dall'art. 34 del Regolamento.

3.3. Sicurezza del trattamento.

Nel corso dell'istruttoria, è inoltre emerso che, al momento in cui si è verificata la violazione dei dati personali, alcune password (circa 98.000) erano conservate previa applicazione di una funzione di hashing ("MD5", non sempre con l'utilizzo di un salt), mentre altre (circa 36.000) erano addirittura conservate in chiaro.

La citata funzione di hashing utilizzata risulta comunque non robusta, in termini crittografici, e il suo utilizzo non rappresenta quindi una misura efficace per proteggere le password degli utenti in quanto sono note, già da diversi anni, gravi vulnerabilità di tale funzione che consentono di risalire, a partire da un digest, alla password che lo ha generato.

Al riguardo, si rileva come la conservazione delle password mediante l'utilizzo di tecniche crittografiche allo stato dell'arte sia una delle misure che devono essere adottate per proteggere adeguatamente le password degli utenti di un sistema informatico o di un servizio online.

La conservazione delle password degli utenti in chiaro, o con tecniche crittografiche non allo stato dell'arte, si pone quindi in contrasto con l'art. 5, par. 1, lett. f), e con l'art. 32 del Regolamento che, al suo par. 1, lett. a), individua espressamente la cifratura come una delle possibili misure di sicurezza idonee a garantire un livello di sicurezza adeguato al rischio (v. anche cons. 83 del Regolamento nella parte in cui prevede che "il titolare del trattamento […] dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura"). In proposito, in tal senso, si è recentemente pronunciata l'Autorità (v. provv. n. 759 del 13 novembre 2024, doc. web n. 10109352 in www.garanteprivacy.it; provv. n. 198 dell'11 aprile 2024, doc. web n. 10013321).

Nel corso dell'istruttoria, è altresì emerso che le credenziali di autenticazione (e gli altri dati personali) oggetto di violazione sono "relative a sistemi non più in uso dal 2022". In particolare, l'applicazione web "aggiornamentoconoscenza.it" è stata dismessa nel mese di marzo 2020, mentre le altre applicazioni web, a cui le predette credenziali di autenticazione consentivano l'accesso, sono state oggetto di interventi di aggiornamento dell'algoritmo di password hashing, svolti nel periodo che va da febbraio 2020 a ottobre 2022.

Al riguardo si rileva come la conservazione di credenziali di autenticazione (username e password) – tenuto conto degli elevati rischi per i diritti e le libertà delle persone fisiche presentati da tale trattamento – debba essere effettuata solo per il tempo strettamente necessario al perseguimento delle finalità per le quali tali dati sono trattati, quali, ad esempio, quelle di consentire la verifica dell'identità degli utenti ai fini dell'accesso a sistemi informatici o servizi online o, se del caso, di 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).

Ciò, anche in considerazione del fatto che il progresso tecnologico, con il passare del tempo, può compromettere l'efficacia delle misure tecniche adottate per proteggere le password degli utenti.

Con riferimento a quanto affermato dalla Società in sede di audizione in merito al fatto che la sicurezza applicativa dei sistemi fosse compito dei fornitori esterni e che la stessa Società, successivamente alla violazione, "si è resa conto che i fornitori esterni non avevano le competenze adeguate per sviluppare tali applicativi tenendo conto anche degli aspetti relativi alla sicurezza e alla protezione dei dati personali" (v. verbale audizione del 16/12/2026) si rammenta che la Società ha rivestito, con riferimento ai trattamenti oggetto del presente procedimento, il ruolo di titolare del trattamento e che, in considerazione di ciò, proprio visto l'art. 4, punto 7, del Regolamento, avrebbe dovuto dare adempimento agli obblighi che gravano sul titolare del trattamento tra cui l'applicazione dei principi di limitazione della conservazione e di integrità e riservatezza di cui all'art. 5, par. 1, lett. e) e f), del Regolamento, nonché l'adozione delle misure di sicurezza di cui all'art. 32 del Regolamento.

Si precisa, inoltre, che, laddove il titolare del trattamento decida di effettuare il trattamento per il tramite di responsabili del trattamento deve ricorrere esclusivamente a soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Risulta evidente, dunque, come, nel caso di specie, anche considerato quanto dichiarato dalla Società in proposito, sussista una colpa in eligendo in capo alla società stessa (cfr. art. 28 del Regolamento).

La Società ha pertanto violato l'art. 5, par. 1, lett. e) e f), del Regolamento, nonché l'art. 32 del Regolamento.

4. Conclusioni: dichiarazione di illiceità del trattamento. Provvedimenti correttivi ex art. 58, par. 2, Regolamento.

Per i suesposti motivi, l'Autorità ritiene che le dichiarazioni, la documentazione e le ricostruzioni fornite dal titolare del trattamento, nel corso dell'istruttoria, non consentano di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento che risultano pertanto inidonee a consentire l'archiviazione del presente procedimento, non ricorrendo peraltro alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Le condotte poste in essere dalla Società e segnatamente l'omessa comunicazione agli interessati coinvolti dalla violazione dei dati personali ai sensi dell'art. 34 del Regolamento nonché la violazione dell'obbligo di adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, risultano illecite, nei termini su esposti, in relazione agli artt. 5, par. 1, lett. e) e f), 32 e 34 del Regolamento.

La violazione accertata nei termini di cui in motivazione non può essere considerata "minore", tenuto conto della natura delle plurime violazioni accertate, che hanno riguardato i principi generali del trattamento nonché l'obbligo di adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e l'obbligo di comunicazione, senza giustificato ritardo, di una violazione dei dati personali agli interessati quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Pertanto, visti i poteri correttivi attribuiti dall'art. 58, par. 2 del Regolamento si dispone l'irrogazione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del Regolamento, commisurata alle circostanze del caso concreto (art. 58, par. 2, lett. i) Regolamento).

5. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i), e 83 del Regolamento; art. 166, comma 7, del Codice).

All'esito del procedimento, risulta pertanto che la Società ha violato gli artt. artt. 5, par. 1, lett. e) e f), 32 e 34 del Regolamento.

Per la violazione delle predette disposizioni è prevista l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. a), e par. 4, lett. a), del Regolamento, mediante adozione di un'ordinanza ingiunzione (art. 18, l. 24.11.1981, n. 689).

Il Garante, ai sensi dell'art. 58, par. 2, lett. i), del Regolamento e dell'art. 166 del Codice, ha il potere di infliggere una sanzione amministrativa pecuniaria prevista dall'art. 83 del Regolamento, mediante l'adozione di una ordinanza ingiunzione (art. 18, L. 24 novembre 1981, n. 689), in relazione al trattamento dei dati personali posto in essere dalla Società, di cui è stata accertata l'illiceità, nei termini sopra esposti.

Ritenuto di dover applicare il paragrafo 3 dell'art. 83 del Regolamento laddove prevede che "Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento […] viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave", l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5.

L'Autorità, alla luce delle Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR adottate in data 24 maggio 2023, alle quali sono state apportate lievi modifiche in

data 29 giugno 2023, ritiene che il livello di gravità della violazione sia medio, tenuto conto di tutti i fattori rilevanti nel caso concreto.

In particolare sono state prese in considerazione la natura, la gravità e la durata della violazione, tenendo conto della natura, dell'oggetto o della finalità del trattamento in questione nonché del numero di interessati lesi dal danno e del livello del danno da essi subito (v. art. 83, par. 2, lett. a), del Regolamento). In particolare, è stata considerata la durata delle violazioni: per quanto riguarda la violazione dell'art. 34 del Regolamento, si rileva che la comunicazione agli interessati è stata effettuata a distanza di circa due mesi dal momento in cui la Società è venuta a conoscenza della violazione dei dati personali; per quanto riguarda la violazione degli artt. 5, par. 1, lett. e) e f) e 32 del Regolamento, si rileva che le credenziali di autenticazione oggetto di violazione erano trattate dalla Società, in assenza di adeguate misure di sicurezza, da oltre due anni. È stato inoltre considerato il numero considerevole di interessati coinvolti, pari a 61.670.

L'Autorità ha altresì preso in considerazione i criteri relativi al carattere doloso o colposo della violazione e le categorie di dati personali interessate dalla violazione, nonché la maniera in cui l'autorità di controllo ha preso conoscenza della violazione (v. art. 83, par. 2, lett. b) e g), e Considerando 148 del Regolamento).

Con riferimento agli altri elementi elencati dall'art. 83, par. 2, del Regolamento ai fini della applicazione della sanzione amministrativa pecuniaria e la relativa quantificazione, per quanto riguarda la Società, ritenuto che il livello di gravità della violazione sia medio, tenuto conto che la sanzione deve "in ogni caso [essere] effettiva, proporzionata e dissuasiva" (art. 83, par. 1 del Regolamento), si rappresenta che, nel caso di specie, sono state considerate le seguenti circostanze:

a) la Società, dopo essere venuta a conoscenza della violazione dei dati personali, ha adottato alcune misure comunque non idonee a mitigare i rischi per i diritti e le libertà degli interessati (art. 83, par. 2, lett. c), del Regolamento);

b) con riferimento al grado di responsabilità del titolare, è stata presa in considerazione la condotta negligente della Società e il grado di responsabilità della stessa che non si era conformata alla disciplina in materia di protezione dei dati relativamente a una pluralità di disposizioni (art. 83, par. 2, lett. d), del Regolamento);

c) non risultano precedenti violazioni pertinenti commesse dal titolare del trattamento (art. 83, par. 2, lett. e), del Regolamento);

d) si è tenuto conto della cooperazione con l'Autorità di controllo (art. 83, par. 2, lett. f), del Regolamento).

Si ritiene inoltre che assumano rilevanza, nel caso di specie, tenuto conto dei richiamati principi di effettività, proporzionalità e dissuasività ai quali l'Autorità deve attenersi nella determinazione dell'ammontare della sanzione (art. 83, par. 1, del Regolamento), in primo luogo le condizioni economiche del contravventore, determinate in base al conto economico della Società con riferimento al bilancio ordinario d'esercizio per l'anno 2024, ultimo disponibile.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti della Società la sanzione amministrativa del pagamento di una somma pari a euro 85.000 (ottantacinquemila).

In tale quadro si ritiene che ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante.

Ciò in considerazione della tipologia delle violazioni accertate che hanno riguardato i principi generali del trattamento nonché l'obbligo di adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e l'obbligo di comunicazione, senza giustificato ritardo, di una violazione dei dati personali agli interessati quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, rileva l'illiceità del trattamento effettuato da The European House - Ambrosetti S.p.A., in persona del legale rappresentante, con sede legale in Via Francesco Albani, 21, Milano, C.F. 09638920158, nei termini di cui in motivazione, per la violazione degli artt. 5, par. 1, lett. e) e f), 32 e 34 del Regolamento;

ORDINA

a The European House - Ambrosetti S.p.A. ai sensi dell'art. 58, par. 2, lett. i), del Regolamento, di pagare la somma di euro 85.000,00 (ottantacinquemila/00) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

INGIUNGE

a The European House - Ambrosetti S.p.A. di pagare la predetta somma di euro 85.000,00 (ottantacinquemila/00), secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dell'art. 27 della legge n. 689/1981. Si ricorda che resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento – sempre secondo le modalità indicate in allegato – di un importo pari alla metà della sanzione irrogata, entro il termine di cui all'art. 10, comma 3, del d. lgs. n. 150 dell'1.9.2011 previsto per la proposizione del ricorso come sotto indicato (art. 166, comma 8, del Codice);

DISPONE

- ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito Internet del Garante;

- ai sensi dell'art. 154-bis, comma 3, del Codice e dell'art. 37 del Regolamento del garante n. 1/2019, la pubblicazione del presente provvedimento sul sito Internet del Garante;

- ai sensi dell'art. 17 del Regolamento n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2, del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u), del Regolamento.

Ai sensi dell'art. 78 del Regolamento, nonché degli articoli 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo individuato nel medesimo art. 10, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 17 aprile 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL SEGRETARIO GENERALE
Montuori