GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento su data breach - 28 marzo 2019 [9104006]

[doc. web n. 9104006]

Provvedimento su data breach - 28 marzo 2019

Registro dei provvedimenti
n. 87 del 28 marzo 2019

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

VISTO il 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 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. n. 101 del 10 agosto 2018, di seguito “Codice”);

ESAMINATA la documentazione in atti;

VISTI gli atti d’ufficio e le osservazioni formulate dal segretario generale ai sensi dell’art. 15 del regolamento del Garante n. 1/2000;

RELATORE la dott.ssa Augusta Iannini;

PREMESSO

1. La violazione dei dati personali.

Il 25 luglio 2017 UniCredit S.p.A. (di seguito “UniCredit” o “la società”) ha comunicato a questa Autorità (sporgendo al tempo stesso denuncia querela presso la Procura della Repubblica di Milano che, nel maggio 2018, ha chiesto la proroga delle indagini preliminari) di aver subìto una intrusione informatica che ha determinato accessi non autorizzati ai dati personali di un rilevante numero di clienti - inizialmente stimato a 400.000 unità e successivamente accertato nella misura di circa 762.000 – che sarebbero stati effettuati con le credenziali di alcuni dipendenti di un partner commerciale esterno (Penta Finanziamenti Italia s.r.l., di seguito anche “Penta” o “Penta Finanziamenti”) attraverso un’applicazione, denominata “Speedy Arena”, che consente la gestione delle richieste di finanziamento relative, in particolare, alla cessione del quinto dello stipendio. Tali accessi abusivi sarebbero avvenuti in due momenti distinti in un arco temporale compreso tra il 28 aprile 2016 (primo log disponibile) e il 13 luglio 2017 e, come meglio precisato da Unicredit il 22 ottobre 2018, hanno riguardato: dati anagrafici e di contatto, professione, livello di studio, estremi identificativi di un documento di identità nonché informazioni relative a datore di lavoro, salario, importo del prestito, stato del pagamento, “approssimazione della classificazione creditizia del cliente” e identificativo Iban.

2. L’istruttoria del Garante

L’Autorità ha immediatamente avviato un’istruttoria e, in data 3 agosto 2017 e 29 settembre 2017, ha invitato rispettivamente UniCredit e Penta Finanziamenti a fornire alcuni chiarimenti relativamente all’incidente che ha determinato la violazione dei dati personali di un così considerevole numero di clienti.

UniCredit, con le note del 20 settembre e 6 ottobre 2017, ha quindi precisato che:

a) il contratto di agenzia in attività finanziaria stipulato con Penta Finanziamenti era stato, medio tempore, risolto ancor “prima della formalizzazione dell’atto di nomina della società medesima quale responsabile del trattamento ai sensi dell’art. 29 del Codice”; in proposito, nel corso del successivo accertamento ispettivo ha poi chiarito che Penta, quale agente monomandataria per suo conto, ha svolto la sua attività in qualità di autonomo titolare del trattamento (cfr. verbale del 22 ottobre 2018, pagg. 3 e 4);

b) l’accesso illegittimo ha interessato un numero di clienti superiore rispetto a quello inizialmente segnalato, pari a circa 762.000 (ciò è emerso a seguito di accertamenti ulteriori che hanno interessato un periodo di verifica più ampio rispetto a quello inizialmente preso in considerazione ovvero a partire dal 28 aprile 2016, primo giorno da cui i log risultavano disponibili).

La società ha inoltre rappresentato di avere immediatamente adottato - allo scopo di individuare e risolvere alcune debolezze del sistema informatico – diversi interventi di sicurezza (alerts, controlli antifrode, crash program di cui ha fornito accurata descrizione) tra cui, in particolare, il blocco (a far data dalla data di fine luglio 2017) di tutte le credenziali concesse al partner commerciale coinvolto, nonché di avere provveduto ad informare i clienti in ordine a quanto accaduto (tramite lettera cartacea, ma anche, come successivamente specificato in corso di ispezione, sms, pop up di sportello e numero verde dedicato).

Penta Finanziamenti , d’altra parte, con nota del 5 ottobre 2017, ha chiarito che nello svolgimento della propria attività, in qualità di mandataria di UniCredit per il prodotto di cessione del quinto dello stipendio, si avvaleva di dipendenti e collaboratori ai quali veniva assegnata una “matricola, identificata dalle lettere SX seguite da 5 numeri (cui corrisponde un PIN e una seconda password alfanumerica)” per l’accesso all’applicativo Speedy Arena (oggetto della intrusione segnalata); attraverso tale applicativo ciascuna matricola poteva visionare unicamente i dati personali dei clienti che avevano istruito pratiche di finanziamento con UniCredit (cessione del quinto o delegazione di pagamento) per il tramite di Penta, mentre risultava impossibile accedere ai dati dei cedenti o clienti di UniCredit che non fossero attinenti a richieste fatte per il tramite della predetta Penta. La medesima società ha peraltro dichiarato di non essere a conoscenza di utilizzi anomali di utenze o matricole SX che possano aver portato all’accesso non autorizzato ai dati di clienti di Unicredit.

Il 21 novembre 2017 l’Autorità ha inoltrato una richiesta di integrazione informativa nei confronti di Penta Finanziamenti al fine di approfondire il ruolo dei soggetti che, sulla base di quanto affermato da UniCredit, avrebbero effettuato un illecito trattamento di dati personali, nonché di accertare il numero delle pratiche di finanziamento istruite da Penta per conto di UniCredit nel periodo compreso tra il 1° aprile 2016 e il 30 giugno 2017; ciò allo scopo di valutare la coerenza delle risposte precedentemente fornite dalle due società in quanto il numero dei soggetti interessati dal data breach (oltre 700.000) risultava prima facie troppo elevato rispetto all’elemento che avrebbe determinato il loro coinvolgimento (in concreto, l’aver chiesto un finanziamento - cessione del quinto - per il tramite di Penta).

Penta Finanziamenti, con nota del 7 dicembre 2017, nel precisare di essere stata costituita in data 17 novembre 2016, di avere ottenuto l’autorizzazione ad operare l’8 marzo 2017 e di agire su mandato di Unicredit a seguito di contratto sottoscritto il 20 marzo 2017, ha dichiarato di non essere in grado di fornire il numero esatto delle pratiche istruite quale monomandataria nel periodo richiesto, anche perché “a far data dal 27 luglio 2017 UniCredit ha bloccato tutte le utenze e le matricole SX per il nostro accesso al sistema “Speedy Arena” e a decorrere dal 3 ottobre 2017 è cessato il mandato di agenzia”; purtuttavia, sulla base di “una stima realistica” ritiene che nel periodo intercorrente tra la sottoscrizione del contratto (20 marzo 2017) e il 30 giugno 2017, sono state oggetto di lavorazione “circa 300 pratiche di finanziamento”.

L’Autorità quindi, nell’evidenziare le discordanze risultanti, in data 19 gennaio 2018, ha trasmesso a UniCredit una nuova richiesta di informazioni al fine di ottenere ulteriori chiarimenti, sia con riferimento al numero dei soggetti coinvolti sia, in particolare, all’ambito interno o esterno all’istituto di credito in cui potrebbe essere avvenuta la violazione.

La società, con nota di riscontro del 9 febbraio 2018, ha inviato all’Autorità l’”Audit Report” del 30.11.2017, formulando le seguenti

precisazioni:

• il numero complessivo dei soggetti interessati dagli accessi abusivi è pari a 761.150 unità (di cui 760.738 persone fisiche) ed ha riguardato le informazioni anagrafiche e gli identificativi IBAN; non sono, invece, stati oggetto di visione illecita informazioni ulteriori quali il numero della carta di credito, le firme, i contratti, le copie dei documenti di identità o altro;

• sebbene nell'applicativo Arena fossero presenti anche pratiche riguardanti il prestito al consumo, Penta Finanziamenti aveva incarico di occuparsi esclusivamente della cessione del quinto e le credenziali (user id) in uso ai suoi dipendenti/collaboratori avrebbero dovuto consentire l'accesso esclusivamente alle pratiche relative a questa tipologia di finanziamenti. Purtuttavia, gli accessi abusivi hanno riguardato entrambe le tipologie di pratiche (cessione del quinto e prestito al consumo);

• gli accertamenti interni hanno evidenziato che gli accessi abusivi sono stati effettuati utilizzando le credenziali di utenti appartenenti a Penta Finanziamenti; gli esiti di tali accertamenti sono stati trasmessi all'autorità giudiziaria cui spetta il compito di valutare se le violazioni siano state commesse da dipendenti/collaboratori di Penta, titolari di tali credenziali, oppure da soggetti terzi, allo stato non identificati, che se ne siano manualmente o digitalmente impossessati;

• a seguito del data breach gli amministratori di Penta, nei contatti intercorsi con UniCredit, hanno rappresentato - anche tramite invio di apposita documentazione tecnica - che "la società non era dotata dei più elementari dispositivi informatici necessari a garantire la riservatezza dei dati gestiti (per esempio non vi era alcuna separazione tra la rete wi-fi utilizzata dal personale interno e quella messa a disposizione degli ospiti)"; circostanza questa che, come già evidenziato, ha comportato la risoluzione del contratto di agenzia in data 3 ottobre 2017.

In considerazione degli elementi acquisiti l'Autorità, esaminata la consistente documentazione agli atti del procedimento, ha rilevato alcune criticità sotto il profilo tecnico che hanno fatto ritenere possibile l'avvenuta violazione di disposizioni in materia di misure minime di sicurezza (vigenti all'epoca dei fatti) o di provvedimenti prescrittivi di misure necessarie da parte di UniCredit. Tuttavia, allo scopo di acquisire elementi di maggiore certezza necessari a definire le fattispecie di illiceità e quindi procedere alla contestazione di violazione amministrativa, è stata posta in essere un'attività ispettiva in loco presso gli uffici di Unicredit svoltasi il 22, 23 e 24 ottobre 2018.

2.1. Gli accertamenti ispettivi e le valutazioni dell'Autorità.

Sulla base dell'esame delle informazioni acquisite presso la sede di UniCredit e dell'analisi tecnica conseguentemente condotta dall'Autorità anche sulla documentazione integrativa pervenuta il 7 novembre 2018, il Garante, tenuto conto che la violazione dei sistemi informatici oggetto del presente provvedimento si è verificata prima dell'applicabilità del Regolamento (UE) 2016/679 e che, pertanto, la normativa di riferimento è il d.lgs. n. 196/2003, non ancora modificato dal d.lgs. n 101/2018, può formulare i rilievi di seguito indicati.

A) Inidoneità del sistema di autorizzazione dell'applicazione Speedy Arena.

La violazione in esame è stata resa possibile da alcune debolezze nella sicurezza dell'applicativo Speedy Arena, sia nella componente di front-end web (che mostrava in chiaro l'identificativo (numero) della pratica; era sufficiente modificare questo numero nel corrispondente URL per ottenere la visualizzazione della pratica dal back-end, il database sottostante l'applicazione) che in quella di back-end (che non verificava se la richiesta di accesso ai dati di una pratica fosse generata da un utente autorizzato") (v. audit report del 30 novembre 2017, p. 1).

Nel corso dall'accertamento ispettivo UniCredit ha, infatti, ulteriormente chiarito che l'applicazione Arena (la cui gestione operativa è affidata a Unicredit Business Integrated Solutions S.c.p.a., ora Unicredit Services S.c.p.a., nominata responsabile del trattamento con atto del 15.12.2015 - cfr. all. 2 al verbale del 22 ottobre u.s.) "consente la gestione di pratiche relative al "prestito al consumo" e alla "cessione del quinto dello stipendio" da parte di personale sia interno (dipendenti Unicredit) che esterno (agenti in attività finanziaria o loro dipendenti/collaboratori), in quest'ultimo caso attraverso un accesso extranet. La società Penta, quale agente in attività finanziaria, era incaricata di occuparsi unicamente delle pratiche di "cessione del quinto dello stipendio" relative ai propri clienti; pertanto le credenziali (user-id) in uso ai suoi dipendenti e collaboratori avrebbero dovuto consentire esclusivamente la creazione e la consultazione delle predette pratiche. Tuttavia, sfruttando alcune "debolezze della sicurezza" dell'applicativo, soggetti ignoti, attraverso le credenziali assegnate al personale Penta, hanno avuto accesso ai dati personali presenti in pratiche di

finanziamento (sia di “cessione del quinto dello stipendio” che di “prestito a consumo”) che non rientravano nell’ambito del mandato di Penta, determinando in questo modo il “data breach” in questione (cfr. verbale del 22 ottobre 2018, p. 3)
Ciò posto si rileva che, all’epoca della violazione dei dati personali, gli incaricati del trattamento abilitati all’accesso all’applicazione Arena, dopo aver effettuato l’autenticazione potevano accedere a una qualsiasi pratica di finanziamento (sia di cessione del quinto dello stipendio che di prestito al consumo) semplicemente modificando il numero identificativo della pratica presente all’interno dell’indirizzo web. Ciò accadeva indipendentemente dal profilo di autorizzazione assegnato agli incaricati, che avrebbe invece dovuto limitare l’accesso ai soli dati relativi alle pratiche di loro competenza.

Le sopra esposte modalità di accesso configurano, pertanto, l’omessa adozione da parte di UniCredit delle misure minime di sicurezza previste dagli artt. 33 e ss. del d.lgs. n. 196/2003, “Codice in materia di protezione dei dati personali” (di seguito “Codice”) e dal disciplinare tecnico di cui all’allegato B al Codice medesimo, con specifico riguardo all’utilizzo di un non idoneo sistema di autorizzazione (cfr. regola n. 12 del disciplinare tecnico) e all’assenza del “limite di accesso” dei profili di autorizzazione – individuati per l’accesso all’applicazione Arena – “ai soli dati necessari per effettuare le operazioni di trattamento” (cfr. regola n. 13 del disciplinare).

B) Inadeguatezza e non corretta conservazione dei log di tracciamento delle operazioni svolte sull’applicazione Arena.

Nell’audit report del 30 novembre 2017 (pag. 2) la società ha rappresentato che, conformemente al provvedimento del Garante del 12 maggio 2011, n. 192 (“Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie”), tutte “le applicazioni che contengono dati personali dei clienti alimentano un sistema di raccolta dei log adottato da Unicredit al fine di consentire l'individuazione di un eventuale abuso delle credenziali dell'utente (…). L’applicativo Arena non ha inoltrato a tale sistema il log delle azioni eseguite da agenti esterni a causa di un errore di programmazione”. Nel corso dall’accertamento ispettivo UniCredit ha confermato che, al momento in cui è venuta a conoscenza della violazione, “i log di tracciamento delle operazioni effettuate dagli utenti esterni sull’applicativo “Speedy Arena” non erano inviati al sistema “Splunk” di Unicredit (gestito da UBIS) a causa di un malfunzionamento della componente di tracciamento del medesimo applicativo” e che, comunque, erano “disponibili, per le operazioni effettuate dagli utenti esterni, i log di tracciamento generati dai sistemi firewall” (cfr. verbale del 23 ottobre 2018, p. 4).

Tuttavia, come rappresentato anche da UniCredit, “in caso di interazione da Extranet finalizzata alla lettura dei dossier Arena, il log [generato dai firewall] include il numero delle pratiche, lo user ID e l’azione eseguita” (cfr. audit report del 30 novembre 2017, p. 22), senza registrare il codice del cliente interessato dall'operazione di accesso da parte dell'incaricato.

Inoltre, UniCredit ha evidenziato che, al momento in cui è venuta a conoscenza della violazione, “a causa del limitato periodo di ‘retention’, non è stato possibile analizzare log [relativi ai firewall] antecedenti alla data del 28 Aprile 2016, in quanto non disponibili” e che, per tale motivo, “la portata esatta della violazione dei dati non può essere determinata” (cfr. audit report del 30 novembre 2017, pp. 7 e 15).

Tali circostanze configurano, pertanto, l’omessa adozione delle misure di sicurezza necessarie di cui al punto 1), lett. b) e c), del dispositivo del provvedimento del Garante del 12 maggio 2011, n. 192 sopra citato in relazione a:

- la mancata registrazione del “codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato” (cfr. punto 1), lett. b), del dispositivo del citato provvedimento) all’interno del log di tracciamento delle operazioni effettuate, attraverso l’applicazione Arena, da alcune tipologie di incaricati del trattamento (agenti in attività finanziaria o loro dipendenti/collaboratori);

- la conservazione per un periodo “inferiore a 24 mesi dalla data di registrazione dell’operazione” (cfr. punto 1), lett. c), del dispositivo del citato provvedimento) dei log di tracciamento delle operazioni effettuate, attraverso l’applicazione Arena, da alcune tipologie di incaricati del trattamento (agenti in attività finanziaria o loro dipendenti/collaboratori).

C) Mancata implementazione di alert per le operazioni svolte attraverso l’applicazione Arena.

Già in sede di audit report UniCredit ha evidenziato che la violazione dei dati personali in esame si è protratta nel tempo anche a causa della “mancanza di controllo e monitoraggio sul corretto utilizzo dell'applicazione [Arena] da parte di utenze (user-id) legittime”. In particolare, “non era presente alcun controllo per rilevare comportamenti anomali di utenti autorizzati” e, all’esito dell’analisi effettuata - nel corso delle attività di audit - sui log di tracciamento delle operazioni che hanno determinato la medesima

violazione, è emerso che le "credenziali Extranet legittime sono state utilizzate in un breve lasso di tempo da diversi indirizzi IP e da posizioni geografiche incompatibili con la localizzazione dell'utente". Dall'audit è emerso che "l'infrastruttura di sicurezza non ha rilevato questa anomalia" e che "le pratiche dei clienti sono state consultate con una frequenza sino a 10 per secondo, in ordine consecutivo da un singolo utente"; tuttavia "questo comportamento anomalo, non riconducibile ad attività manuali ma bensì realizzate mediante automatismi, non è stato rilevato" (cfr. audit report del 30 novembre 2017, pp. 2 e 10).

Nell'ambito dell'accertamento ispettivo, UniCredit ha, da ultimo, confermato che "all'epoca degli accessi illegittimi non esisteva un indicatore che rilevava le operazioni effettuate dagli utenti esterni [attraverso l'applicazione Arena], che invece è stato rilasciato in produzione a dicembre 2017" (cfr. nota del 7 novembre 2018, p. 2)

Tali circostanze configurano, pertanto, l'omessa adozione, da parte di UniCredit, della misura di sicurezza necessaria di cui al punto 1), lett. d), punto i), del dispositivo del provvedimento del 12 maggio 2011, n. 192 citato in relazione alla mancata "attivazione di specifici alert che individuino comportamenti anomali o a rischio relativi alle operazioni di inquiry" effettuate, attraverso l'applicazione Arena, da alcune tipologie di incaricati del trattamento (agenti in attività finanziaria o loro dipendenti/collaboratori).

D) Mancata esecuzione di opportune attività di audit interno di controllo

Sulla base della documentazione in atti, non risulta che UniCredit abbia effettuato le opportune attività di controllo interno che avrebbero permesso, quantomeno, di rilevare proattivamente l'inidoneità del sistema di autorizzazione dell'applicazione Arena, l'inadeguatezza e la non corretta conservazione dei log di tracciamento delle operazioni svolte sulla medesima applicazione, nonché la mancata implementazione di alert volti a rilevare comportamenti anomali o a rischio.

Al riguardo, nel corso dell'accertamento ispettivo la società ha dichiarato che, generalmente, non vengono effettuate attività di audit specifiche per verificare il corretto tracciamento delle operazioni di inquiry effettuate sugli applicativi che ricadono nell'ambito del Provvedimento del Garante del 12 maggio 2011, n. 192 (…)" e che tuttavia "periodicamente vengono effettuati audit volti a valutare il processo e il sistema di gestione dei log" [Splunk], precisando "che, nel caso in esame, sarebbe stato comunque difficile rilevare il non corretto funzionamento della componente di tracciamento dell'applicativo "Arena", in quanto lo stesso produceva comunque i log di tracciamento delle operazioni svolte dagli utenti interni" (cfr. verbale del 24 ottobre 2018, pp. 2-3).

Tali circostanze configurano, pertanto, l'omessa adozione, da parte di UniCredit, della misura di sicurezza necessaria di cui al punto 1), lett. e), punto iii), del dispositivo del provvedimento del 12 maggio 2011, n. 192 sopracitato in relazione all'omessa esecuzione di "verifiche a posteriori […] sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento" nonché di "verifiche periodiche sulla corretta conservazione dei file di log per il periodo" di almeno 24 mesi dalla data di registrazione dell'operazione.

2.2. Verifica delle misure tecniche e organizzative adottate.

Le verifiche condotte dall'Autorità (analisi della documentazione trasmessa e attività in loco) hanno consentito di accertare come la società, a seguito del data breach in questione, abbia adottato le necessarie misure tecniche e organizzative atte ad evitare il ripetersi di accadimenti similari.

In particolare:

a) ripristino del corretto funzionamento del sistema di autorizzazione dell'applicazione Arena.

Nel corso dell'accertamento ispettivo sono stati effettuati una serie di accessi all'applicazione Arena al fine di verificare le funzionalità messe a disposizione delle diverse tipologie di utenti (interni o esterni). Tali accessi hanno evidenziato che, allo stato, "un utente esterno può creare nuove pratiche di finanziamento o consultare esclusivamente le pratiche del suo portafoglio clienti" e che "un utente esterno può effettuare solo alcune tipologie di ricerca pratiche (sulla base dell'identificativo clienti, codice fiscale, numero pratica)" (cfr. verbale del 23 ottobre 2018, p. 3).

Inoltre, UniCredit, nel rappresentare che, all'epoca della violazione dei dati personali, "l'identificativo della pratica era riportato in chiaro (come parametro "GET") all'interno della URL dell'applicativo Speedy Arena", ha "confermato di aver concluso l'intervento di cifratura dell'identificativo della pratica ed ha fornito prova dell'avvenuta eliminazione di tale identificativo dalla URL dell'applicativo Speedy Arena […], che allo stato viene comunicato come parametro "POST"" (cfr.

verbale anzi citato, pag. 3).

b) ripristino del corretto tracciamento delle operazioni svolte attraverso l'applicazione Arena e della corretta conservazione dei log.

La società, già nell'audit report del 30 novembre 2017 (pag. 17) aveva rappresentato che "dall'agosto 2017 Arena sta rilasciando i log per Garante2, includendo anche gli user-id esterni (agenti)"; a conferma di ciò ha fornito all'Autorità i log di tracciamento relativi alle operazioni effettuate sull'applicazione Arena durante le attività ispettive (cfr. allegato 4 alla nota del 7 novembre 2018)

c) implementazione di alert per le operazioni svolte attraverso l'applicazione Arena.

Sono stati implementati specifici alert per individuare comportamenti anomali o a rischio nell'ambito delle operazioni che gli incaricati del trattamento pongono in essere attraverso l'applicazione Arena.

In particolare, UniCredit ha rappresentato che "sono stati definiti differenti tipologie di alert in funzione della tipologia di utenti. Sono stati, ad esempio, creati alert distinti per gli utenti interni che operano nell'ambito delle funzioni di governance e per quelli che operano presso la rete delle filiali Unicredit. Così come sono stati creati alert specifici per gli utenti esterni. Nel corso del tempo, sono state effettuate una serie di attività di fine tuning volte a migliorare l'efficacia degli alert" ed "esiste un sistema di business intelligence, denominato "Memento", su cui confluiscono i log di tracciamento raccolti dal sistema "Splunk". Il sistema "Memento" è configurato per generare specifici alert che individuino comportamenti anomali o a rischio relativi alle operazioni di inquiry eseguite dagli utenti interni e esterni" (cfr. verbale del 24 ottobre 2018, p. 2).

d) esecuzione di attività di audit interno di controllo e adozione di altre misure di sicurezza.

A seguito della violazione dei dati personali in esame, UniCredit ha avviato una specifica attività di audit interno al fine di chiarire le circostanze in cui si è determinata la violazione, di individuare le aree di responsabilità nonché di identificare e pianificare, nell'ambito di un c.d. "crash program", una serie di interventi volti a incrementare il livello di sicurezza dei propri sistemi informativi e a prevenire violazioni dei dati personali simili a quella occorsa. Nel corso dell'ispezione la società ha dato atto di aver portato a compimento la maggior parte degli interventi previsti nell'ambito del predetto "crash program".

Resta fermo che, a decorrere dal 25 maggio 2018, data di effettiva applicazione del Regolamento (UE) 2016/679, ciascun titolare del trattamento, in ossequio al principio di responsabilizzazione di cui all'art. 24, è tenuto a valutare autonomamente la conformità dei trattamenti che intende effettuare alla disciplina vigente, verificando il rispetto di tutti i principi in materia ed individuando misure a protezione dei dati sin dalla fase di progettazione dei sistemi informativi con cui si realizzano i trattamenti (art. 25 Regolamento).

TUTTO CIO' PREMESSO, IL GARANTE:

ai sensi dell'art. 58 del Regolamento (UE) 2016/679 rileva l'illiceità del trattamento posto in essere da UniCredit S.p.a. in vigenza del d.lgs. n. 196/2003 nei termini di cui al par. 2.1 lett. A), B), C) e D) e si riserva di verificare, con autonomo procedimento, la sussistenza dei presupposti per la contestazione delle sanzioni amministrative di cui all'art. 162, comma 2-bis e 2-ter del Codice.

Ai sensi dell'art. 78 del Regolamento(UE) 2016/679, nonché dell'art. 152, comma 1-bis del Codice, avverso il presente provvedimento può essere proposta opposizione all'Autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 28 marzo 2019

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia