Sottoscrizione documenti informatici con FEA

Relazione tecnica e organizzativa

Provvedimento generale del Garante per la protezione dei dati personali del 12 novembre 2014 (punto 4.4 lettera K)

Approvato dal Consiglio di amministrazione del 25/01/2024

Versione 4.2 Relazione Tecnica e Organizzativa FEA aggiornata al ___06-07-2022_____

Indice

1 PREMESSA

La presente Relazione descrive – in conformità a quanto previsto dal punto 4.4, lettera k del Provvedimento generale del Garante n. 513 del 12 novembre 2014 (di seguito Provvedimento) – gli aspetti tecnici ed organizzativi delle misure messe in atto e le valutazioni sulla necessità e proporzionalità del trattamento biometrico rispetto alle finalità perseguite mediante la realizzazione, erogazione ed utilizzazione della soluzione di firma elettronica avanzata.

La Relazione viene predisposta dal soggetto erogatore della soluzione di firma (art. 55 comma 1 lett. a delle *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali* di cui al DPCM 22.02.13, di seguito Regole Tecniche), e quindi segnatamente dalla Banca di Pescia e Cascina – credito cooperativo -, s.c., e da Iccrea Banca S.p.A., relativamente ai documenti sottoscritti con la soluzione di firma grafometrica realizzata da BCC Sistemi Informatici S.p.A. (in qualità di realizzatore della soluzione, a norma dell'art. 55 comma 1 lett. B delle Regole Tecniche) nell'ambito dei rapporti intercorrenti, ognuna per quanto di ragione, tra le stesse ed i propri clienti, nel rispetto della limitazione d'uso di cui all'art. 60 delle Regole Tecniche.

Di qui in appresso, tanto la Banca di Pescia e Cascina – credito cooperativo -, s.c. quanto Iccrea Banca S.p.A. vengono identificati come "la Banca".

2 MISURE TECNICHE ED ORGANIZZATIVE

2.1 Misure tecniche

Allo scopo di perseguire le finalità descritte, la Banca ha adottato un sistema di firma grafometrica realizzato dall'outsourcer BCC Sistemi Informatici.

BCC Sistemi Informatici ha predisposto e reso disponibile sulla propria extranet il documento denominato "Sicurezza Firma Grafometrica", a cui si fa rinvio, all'interno del quale il realizzatore della soluzione di firma descrive:

- le caratteristiche della soluzione di firma grafometrica;
- le misure tecniche adottate in conformità alle prescrizioni del Garante della privacy.

Il documento di BCC Sistemi Informatici descrive puntualmente, anche attraverso rinvii ad ulteriore normativa aziendale allegata o disponibile sulla extranet:

- le modalità di cancellazione dei dati biometrici grezzi e dei campioni biometrici
- le modalità di memorizzazione dei dati biometrici e grafometrici all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica con dimensione della chiave adeguata alla dimensione e al ciclo di vita dei dati e certificato digitale emesso da un certificatore accreditato ai sensi dell'art. 29 del Codice dell'amministrazione digitale
- le modalità di custodia della chiave privata da parte di un soggetto terzo fiduciario che fornisca idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave
- le modalità di generazione, consegna e conservazione delle chiavi e le condizioni e le modalità di accesso alla firma grafometrica da parte del soggetto terzo di fiducia o da parte di tecnici qualificati
- le misure adottate per la trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server
- le misure adottate e gli accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati

- le modalità di protezione dei sistemi informatici contro l'azione di malware e i sistemi di firewall adottati per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati.

I sistemi di gestione impiegati nei trattamenti grafometrici adottano certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro.

2.2 Misure organizzative

La Banca ha adottato le seguenti misure organizzative:

1. Il procedimento di firma è abilitato previa identificazione del firmatario che avviene mediante acquisizione di un documento di riconoscimento in corso di validità
2. Sono resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici. A tal fine la banca ha impartito specifiche istruzioni alle filiali
3. L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario e nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria. In caso di necessità il soggetto all'uopo delegato dalla Banca invia una richiesta scritta, anche via PEC, all'outsourcer informatico BCC Sistemi Informatici che è a sua volta tenuta ad attivare la procedura con la Certification Authority presso la quale è conservata la chiave privata, così come analiticamente descritta nel Regolamento per avviare la pratica presso Telecom Italia Trust Technologies S.r.l. (di seguito anche "TITT"). Alla richiesta deve essere allegato il provvedimento dell'Autorità giudiziaria.
4. In ipotesi di data breach (per tale intendendosi, a norma del GDPR la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizza o l'accesso ai dati personali trasmessi, conservati o comunque trattati e a norma del Provvedimento del Garante, le-violazioni dei dati o incidenti informatici - accessi abusivi, azione di malware... - che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione), la Banca garantisce la possibilità di dare seguito alla comunicazione all'Autorità dell'avvenuta violazione nel termine di 72 ore, come previsto dal Regolamento UE 2016/679 e dal Provvedimento del Garante Privacy 30 luglio 2019.

   Le misure adottate a tale fine consistono:

   - Nella individuazione all'interno della propria organizzazione di una persona fisica cui è affidata la responsabilità della gestione di eventuali data breach o incidenti informatici sulla quale incombe l'onere di procedere senza indugio, non appena ne venga a conoscenza, e comunque nel termine prescritto dal Provvedimento, alla comunicazione al Garante della violazione dei dati biometrici utilizzando l'apposita procedura online prevista dall'Autorità (e, nei casi di incidenti verificatisi al di fuori del perimetro del sistema informativo della Banca, compilato da BCC Sistemi Informatici e/o dal soggetto cui è affidato il servizio di conservazione digitale). Alla data di redazione della presente Relazione, tale compito viene assegnato al Referente Interno DPO, in collaborazione con il DPO della Società.
   - Nella previsione di uno specifico onere a carico dei soggetti designati ex art. 28 del Regolamento UE 2016/679 quali responsabili del trattamento (quanto alla Banca di Pescia e Cascina – credito cooperativo -, s.c., individuati in BCC Sistemi Informatici ed in Iccrea Banca cui è affidato il servizio di conservazione digitale; quanto ad Iccrea Banca, individuati nella Banca di Pescia e Cascina – credito cooperativo -, s.c. e in BCC Sistemi Informatici), relativamente alla immediata segnalazione mediante comunicazione via PEC all'indirizzo indicato dalla Banca della violazione eventualmente avvenuta all'interno dei rispettivi sistemi informativi, con annesso onere di supporto alla Banca, affinchè quest'ultima possa assolvere all'obbligo di comunicazione al

Garante entro il termine di 72 ore dalla conoscenza del fatto, mediante l'apposita procedura online. A tale fine BCC Sistemi Informatici ed il conservatore sono esplicitamente onerati di individuare al proprio interno le persone fisiche cui sono affidati i compiti indicati. Quanto ad Iccrea Banca, per il servizio di conservazione digitale, tale figura è individuata nel Responsabile del Servizio di Conservazione Digitale a norma che, in coerenza con il processo di gestione degli incidenti definiti nel Gruppo Bancario Iccrea, assicura la tempestiva comunicazione alla Banca per permettere la pronta attivazione delle relative procedure di gestione dell'emergenza. Quanto a BCC Sistemi Informatici tale figura è individuata nel Responsabile dell'U.O. Service & Support Management.

- Nella previsione di uno specifico onere, a carico di BCC Sistemi Informatici e del soggetto cui è affidato il servizio di conservazione digitale, relativo alla piena collaborazione con la Banca nelle attività conseguenti alla violazione (es. attività necessarie a minimizzare l'impatto della violazione e prevenire il ripetersi dell'evento).

3 VALUTAZIONI SULLA NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO RISPETTO ALLA FINALITÀ

I dati oggetto di trattamento per mezzo di sistemi biometrici sono raccolti in maniera accurata e trattati per le sole finalità che la Banca intende legittimamente perseguire e previamente indicate nell'informativa che è resa agli interessati, e non possono essere utilizzati in altre operazioni di trattamento che siano con queste incompatibili.

La finalità perseguita è quella di contrastare eventuali tentativi di frode e il fenomeno dei furti di identità. Il sistema inoltre ha lo scopo di:

- rafforzare le garanzie di autenticità e integrità dei documenti informatici sottoscritti, anche in vista di un eventuale contenzioso legato al disconoscimento della sottoscrizione apposta su atti e documenti di tipo negoziale in sede giudiziaria
- assicurare la corretta conservazione e la disponibilità dei documenti minimizzando così i rischi connessi alla perdita degli archivi in caso di eventi come incendi, allagamenti, terremoti
- ridurre il consumo di carta nelle filiali con conseguenti minori impatti ambientali.

Dai dati acquisiti non si possono desumere altre informazioni per verificare, ad esempio, l'accesso in banca del cliente.

L'installazione dei sistemi di rilevazione biometrica è stata preceduta da una valutazione d'impatto sulla protezione dei dati e da una ponderata valutazione delle esigenze di sicurezza.

La Banca, nel compiere le proprie scelte, ha considerato non solo gli aspetti economici e organizzativi, ma anche l'impatto delle soluzioni adottate sugli altrui diritti e legittimi interessi. La Banca tratta i soli dati pertinenti e non eccedenti in relazione alle finalità perseguite.

Il sistema informativo e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi. Infatti il sistema adottato assicura:

- la cancellazione dei dati biometrici immediatamente dopo il completamento della procedura di sottoscrizione);
- che nessun dato biometrico persista all'esterno del documento informatico sottoscritto;
- che i dati biometrici e grafometrici non siano conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta. In altri termini, il dato biometrico viene raccolto, cifrato per il

trasposto tra la signature pad/workstation e quindi crittografato, senza essere in alcun modo memorizzato su supporti permanenti del dispositivo di firma, del device o del P.C.

I dati biometrici, inoltre, vengono memorizzati all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica con dimensione della chiave adeguata alla dimensione e al ciclo di vita dei dati e certificato digitale emesso da Telecom Italia Trust Technologies S.r.l. (di seguito anche "TITT"), certificatore accreditato ai sensi dell'art. 29 del Codice dell'amministrazione digitale. La corrispondente chiave privata è nella esclusiva disponibilità di TITT

Il trattamento dei dati biometrici svolto dalla Banca, attesa la piena conformità a tutte le prescrizioni contenute nel Provvedimento, non presenta in nessuno dei suoi aspetti profili che concretino un superamento del principio di proporzionalità rispetto alle finalità perseguite.

Il presente documento, deliberato dal Consiglio di amministrazione del 25/01/2024, è conservato aggiornato per tutto il periodo di esercizio del sistema biometrico e mantenuto a disposizione del Garante presso la sede della Banca dal Referente DPO interno. Il documento è inoltre oggetto di verifica con cadenza almeno annuale.

Pescia, lì 26/01/2024

Banca di Pescia e Cascina – Credito Cooperativo – s.c.