



“MANUALE TECNICO ED OPERATIVO” PER GLI ADEMPIMENTI VERSO LA CLIENTELA IN TERMINI DI FIRMA GRAFOMETRICA

SOMMARIO

1.	Contesto di riferimento	3
2.	Obiettivo del presente documento	3
3.	Inquadramento normativo	3
4.	Conformità rispetto al Provvedimento	4
5.	BNL ed il servizio	6
6.	Processo di identificazione e sottoscrizione	6
7.	Processo di utilizzo	7
8.	Descrizione delle procedure di sicurezza	7
9.	Applicazione delle misure di sicurezza	8
10.	Conservazione	8
11.	Proporzionalità rispetto ai fini	8
12.	Liceità	8
13.	Necessità	9
14.	Finalità	9

1. CONTESTO DI RIFERIMENTO

L'utilizzo di dispositivi e tecnologie per la raccolta e il trattamento di dati biometrici è soggetto a una crescente diffusione, in particolare per l'accertamento dell'identità personale nell'ambito dell'erogazione di servizi della società dell'informazione e dell'accesso a banche dati informatizzate, per il controllo degli accessi a locali e aree, per l'attivazione di dispositivi elettromeccanici ed elettronici, anche di uso personale, o di macchinari, nonché per la sottoscrizione di documenti informatici.

Tale diffusione ha suscitato la massima attenzione delle autorità di protezione dati, testimoniata anche dall'elaborazione di pareri da parte del Working Party Article 29 (WP29) che costituiscono un significativo punto di riferimento per ogni analisi e studio del fenomeno. I dati biometrici sono infatti dati personali, poiché possono sempre essere considerati come "informazione concernente una persona fisica identificata o identificabile (...)" prendendo in considerazione "l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona". Essi rientrano quindi nell'ambito di applicazione del Codice (art. 4, comma 1, lettera b), e le operazioni su essi compiute con strumenti elettronici sono a tutti gli effetti trattamenti nel senso delineato dalla disciplina sulla protezione dei dati personali.

Sono considerati dati biometrici nel presente contesto, coerentemente con i pareri del WP29, i campioni biometrici, i modelli biometrici, i riferimenti biometrici e ogni altro dato ricavato con procedimento informatico da caratteristiche biometriche e che possa essere ricondotto, anche tramite interconnessione ad altre banche dati, a un interessato individuato o individuabile.

2. OBIETTIVO DEL PRESENTE DOCUMENTO

Obiettivo del presente documento è descrivere la soluzione tecnica che supporta gli aspetti tecnici e organizzativi delle misure messe in atto da BNL, facendo anche riferimento alla valutazione sulla necessità e sulla proporzionalità del trattamento biometrico rispetto alle finalità.

Questa attività rispetta anche un preciso vincolo normativo imposto dal Garante della Privacy con suo Provvedimento Generale del 12/11/2014: infatti, all'art. 4.4 lettera k) prescrive che sia "predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante".

3. INQUADRAMENTO NORMATIVO

La firma grafometrica è un particolare tipo di firma elettronica avanzata (di seguito "FEA") ai sensi del d.lgs. 7 marzo 2005, n. 82 (di seguito "Codice dell'amministrazione digitale" o "CAD") e delle successive modifiche nonché delle norme tecniche di attuazione emanate con il D.P.C.M. 22 febbraio 2013, n. 68380 (di seguito "Norme Tecniche") e del regolamento EIDAS 910/2014 e consiste in un insieme di dati in forma elettronica, allegati ad un documento informatico, che garantiscono:

- a) la connessione univoca della firma al soggetto che la ha apposta;
- b) il controllo esclusivo del sistema di generazione della firma da parte del firmatario;
- c) la possibilità di rilevare se i dati siano stati modificati dopo l'apposizione della firma.

La sottoscrizione con firma grafometrica garantisce, pertanto, sia l'identificabilità dell'autore che l'integrità e l'immodificabilità del documento informatico sottoscritto con la medesima.

Secondo l'art. 20, c. 1 bis, così come novellato dall'ultima modifica al CAD del 11/12/17, il documento informatico sottoscritto con firma elettronica avanzata, possiede l'efficacia prevista dall'articolo 2702 del c.c.; il successivo art 21 c. 2-bis stabilisce, inoltre, che gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale. Il requisito della forma scritta è previsto a pena di nullità per i contratti relativi ai servizi bancari di cui all'art. 117 del d.lgs. 1° settembre 1993, n. 385 (di seguito "TUB") e per i contratti relativi ai servizi d'investimento ai sensi dell'art. 23 del d.lgs. 24 febbraio 1998, n. 58 (di seguito "TUF").

Per quanto attiene ai dati biometrici, c'è da ricordare che per loro natura, direttamente, univocamente e in modo tendenzialmente stabile nel tempo, sono collegati all'individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona, e perciò richiedono particolari cautele in caso di loro trattamento.

L'adozione di sistemi biometrici, in ragione della tecnica prescelta, del contesto di utilizzazione, del numero e della tipologia di potenziali interessati, delle modalità e delle finalità del trattamento, può comportare quindi rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato. In ragione di ciò, qualora si intenda provvedere al trattamento di dati biometrici, è necessario presentare al Garante una richiesta di verifica preliminare, ai sensi dell'art. 17 del Codice.

Tuttavia il trattamento di dati biometrici costituiti da informazioni dinamiche associate all'apposizione a mano libera di una firma autografa avvalendosi di specifici dispositivi hardware è ammesso in assenza di verifica preliminare laddove si utilizzino sistemi di firma grafometrica posti a base di una soluzione di firma elettronica avanzata, così come definita dal CAD che non prevedono la conservazione centralizzata di dati biometrici. Così come prescrive il provvedimento del Garante della Privacy del 12 novembre 2014, il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni e limitazioni:



- a) Il procedimento di firma è abilitato previa identificazione del firmatario.
- b) Sono resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici.
- c) La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo il completamento della procedura di sottoscrizione, e nessun dato biometrico persiste all'esterno del documento informatico sottoscritto.
- d) I dati biometrici e grafometrici non sono conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta, venendo 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 un certificatore accreditato ai sensi dell'art. 29 del Codice dell'amministrazione digitale. La corrispondente chiave privata è nella esclusiva disponibilità di un soggetto terzo fiduciario che fornisca idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave. La chiave può essere frazionata tra più soggetti ai fini di sicurezza e integrità del dato. In nessun caso il soggetto che eroga il servizio di firma grafometrica può conservare in modo completo tale chiave privata. Le modalità di generazione, consegna e conservazione delle chiavi sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1 lettere e) ed f) del D.P.C.M. 22 febbraio 2013.
- e) La trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server avviene esclusivamente tramite canali di comunicazione resi sicuri con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.
- f) Sono adottate idonee misure e 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.
- g) I sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati.
- h) Nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device), sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri equivalenti al fine di isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nel caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware).
- i) 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 (in particolare, rendendo disponibili funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi).
- j) L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, 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 di polizia e/o autorità giudiziaria. Le condizioni e le modalità di accesso alla firma grafometrica da parte del soggetto terzo di fiducia o da parte di tecnici qualificati sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1, lettere e) ed f) del D.P.C.M. 22 febbraio 2013.
- k) È predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

4. CONFORMITÀ RISPETTO AL PROVVEDIMENTO

LETTERA A)

Il processo, così come meglio descritto nel prosieguo, e specificamente nel capitolo 8, prevede l'identificazione certa del Cliente.

Il cliente firmatario viene identificato in modo certo dall'operatore/consulente finanziario mediante la richiesta di un documento d'identità in corso di validità in conformità alla normativa di riferimento (cfr. art. 35 del D.P.R. 445/2000), che menziona: carta d'identità, passaporto, patente di guida, patente nautica, libretto di pensione, patentino per la conduzione di impianti termici, porto d'armi o altre tessere di riconoscimento purché munite di fotografia e timbro o signature equivalenti e purché rilasciate da un'Amministrazione dello Stato (cfr. art. 56, comma 1, lett. a)).

LETTERA B)

Al momento dell'avvio della procedura, l'operatore/consulente finanziario illustra al Cliente la possibilità di sottoscrivere la contrattualistica di BNL mediante Firma Elettronica Avanzata.

Questa modalità non è vincolante per la prosecuzione del processo: in ogni momento è data facoltà al Cliente di continuare la procedura mediante il sistema tradizionale su carta o con altre soluzioni alternative offerte dalla banca.

LETTERA C)

Questa previsione normativa è stata inserita per mitigare la minaccia di un terzo o di un utente malintenzionato che possa usare i dati biometrici (relativi alla firma elettronica di un Cliente) per scopi fraudolenti.

Per la massima sicurezza nel processo di acquisizione della firma grafometrica da parte del cliente, tutto il processo di cattura dei dati, cifratura degli stessi, inserimento nel documento PDF e successiva cancellazione, avviene completamente in memoria senza l'ausilio di file temporanei all'interno del file system del dispositivo. Nello specifico, i dati acquisiti in real-time durante la firma, vanno a comporre il vettore biometrico della firma, che unito all'HASH del documento PDF originale e ad eventuali altri dati di contesto (versione del SW, seriale del dispositivo, ecc ...) vanno a formare il blocco biometrico. Quest'ultimo viene cifrato con chiave asimmetrica e viene inserito nel documento PDF tramite la forma tecnica della firma digitale, impedendo quindi un qualsiasi tentativo successivo di modifica del PDF stesso.

LETTERA D)

Il tablet di firma registra i parametri biometrici (il movimento, la velocità, l'accelerazione, la pressione), e crea un vettore grafometrico che viene collegato all'hash del documento.

Dopodiché, il blocco biometrico così creato (hash del documento, vettore grafometrico) è cifrato con la chiave pubblica fornita dalla Certification Authority Aruba S.p.A. e la chiave privata (indispensabile per la fase eventuale di disconoscimento della firma a seguito di autorizzazione giudiziale) è conservata in modo sicuro da un terzo fiduciario.

LETTERA E)

Il documento PDF viene visualizzato sul device ed il cliente può navigarlo in autonomia. Una volta firmato il documento, vengono adottate le più adeguate misure di sicurezza per garantire l'immodificabilità dei dati grafometrici e del contenuto del documento stesso.

LETTERA F)

Le garanzie in capo al cliente sono che:

- vengono utilizzati più livelli di cifratura sia a livello software che hardware (a seconda della soluzione tecnologica che verrà utilizzata) così da aumentare il livello di sicurezza di tutte le componenti che trattano i dati grafometrici;
- I dati temporanei di ogni sessione di firma sono distrutti al termine dell'operazione;
- Le postazioni di lavoro BNL sono protette da sistemi antivirus costantemente aggiornati che le proteggono dai rischi dovuti all'installazione di software malevolo.

LETTERA G)

Cit. Provvedimento: *"I sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati".*

LETTERA H)

Cit. Provvedimento: *"Nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device), sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri equivalenti al fine di isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nel caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware)".*

La soluzione di firma non prevede l'utilizzo di dispositivi mobili quali tablet o smartphone con sistemi operativi iOS o Android.

LETTERA I)

La soluzione di firma utilizzata è risultata conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) per il livello di garanzia EAL 1+.

LETTERA J)

Cit. Provvedimento: *"L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, 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 di polizia e/o autorità giudiziaria."*

Ulteriori dettagli tecnici vengono definiti nel manuale tecnico del terzo fiduciario.

LETTERA K)

La presente relazione descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, e fornisce la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità.

I soggetti di cui alle lettere a) e b) dell'art. 55 del DPCM 22 febbraio 2013 si impegnano ad aggiornare la presente relazione ad ogni cambiamento che vada a modificare le condizioni di erogazione del servizio di firma elettronica avanzata attraverso firma grafometrica e comunque si impegnano a controllare che sia ancora aggiornata a cadenza almeno annuale.

5. BNL ED IL SERVIZIO

Con l'obiettivo di migliorare la qualità e la sicurezza dei propri servizi, riducendo al contempo i costi economici ed ambientali per l'erogazione degli stessi, la Banca attraverso l'operatore/consulente finanziario intende fornire alla clientela un servizio di sottoscrizione della documentazione contrattuale e di quella necessaria per l'esecuzione dei servizi prestati, mediante modalità elettroniche.

Tale Servizio prevede l'utilizzo di dati biometrici comportamentali rilevati all'atto della sottoscrizione (meglio specificati nei paragrafi seguenti) che costituiranno gli elementi della sottoscrizione del cliente (c.d. firma grafometrica).

Il servizio viene realizzato mediante l'adozione di una soluzione tecnologica che comporta la cooperazione dei seguenti soggetti:

- Euronovate SA che fornisce: i) le periferiche hardware proprietarie indispensabili per l'erogazione del Servizio, ii) il software proprietario per l'interfacciamento con l'hardware di firma;
- Postel che svolge l'attività di conservazione dei documenti informatici sottoscritti con firma grafometrica;
- Aruba S.p.A. che in qualità di Certification Authority fornisce il certificato di cifratura dei dati biometrici.

Il servizio è reso disponibile dal personale incaricato della Banca (operatori/consulenti finanziari) in configurazione mobile (vendita fuori sede) o residenziale (vendita in filiale) e consente alla clientela di sottoscrivere contratti, disposizioni e altri documenti relativi ai prodotti e servizi forniti da BNL.

6. PROCESSO DI IDENTIFICAZIONE E SOTTOSCRIZIONE

Ai sensi dell'articolo 57 comma 1 lettera a) del DPCM, i soggetti erogatori della soluzione di FEA devono identificare in modo certo l'utente tramite un valido documento di riconoscimento al fine di configurare una firma elettronica avanzata correttamente formata.

In questo capitolo si descrivono le modalità e il processo di identificazione facente parte della soluzione di FEA Grafometrica erogata da BNL.

IDENTIFICAZIONE DEL FIRMATARIO ED ACQUISIZIONE DOCUMENTO

L'identificazione certa del firmatario del documento è eseguita da BNL avvalendosi di una rete di operatori/consulenti finanziari sparsi su tutto il territorio nazionale. L'identificazione è svolta sempre in presenza del firmatario e ad ogni apposizione di firma grafometrica viene accertata l'identità dello stesso da parte del operatore/consulenti finanziario che verifica l'identità del firmatario tramite il riscontro con uno dei seguenti documenti, valido e non scaduto, secondo quanto previsto dall'art. 35, Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445 ed in coerenza con la normativa interna Banca:

- Carta d'identità
- Passaporto
- Patente di guida
- Patente nautica
- Libretto di pensione
- Patentino di abilitazione alla conduzione di impianti termici
- Porto d'armi

Sono ammesse ulteriori tessere di riconoscimento oltre a quelle indicate, purché munite di fotografia e di timbro, rilasciate da un'amministrazione dello Stato e previste all'interno della normativa della Banca.

VERIFICA DEL POSSESSO DELLA FIRMA GRAFOMETRICA

L'operatore/consulente finanziario mentre è davanti al cliente verifica se il cliente ha già aderito al servizio di Firma Grafometrica e, in caso negativo, l'operatore/consulente finanziario domanda al cliente se è intenzionato ad aderire al servizio di firma grafometrica attraverso la FES (Firma Elettronica Semplice). In caso di rifiuto del cliente il processo di raccolta dell'adesione al servizio di firma grafometrica si interrompe e si procede con il sistema cartaceo al di fuori dal campo di applicazione del presente documento.

FIRMA MODULO D'ADESIONE

Una volta identificato il firmatario e raccolto il documento di identità, al cliente viene sottoposto il contratto su supporto digitale, comprendente sia la dichiarazione di adesione ai servizi di firma elettronica avanzata con la relativa informativa, sia il consenso al trattamento dei dati personali, affinché il cliente possa leggerlo e sottoscriverlo.

Il modulo di adesione così firmato è conservato a norma per almeno 20 anni. L'adesione vale fino a successiva eventuale revoca del cliente e pertanto non sarà necessaria ulteriore adesione in fase di firma dei successivi singoli documenti contrattuali.

RILASCIO COPIA MODULO DI ADESIONE AL CLIENTE

Dopo l'apposizione delle firme sul modulo di adesione, copia dello stesso viene consegnata secondo le modalità descritte nel contratto stesso.

7. PROCESSO DI UTILIZZO

FIRMA DELLA DOCUMENTAZIONE BANCA

Una volta raccolta l'adesione, il cliente potrà firmare in modalità grafometrica tutti i documenti contrattuali e precontrattuali stipulati con BNL e per i quali la Banca avrà reso, nel corso del tempo, disponibile tale servizio. Inoltre, con la firma grafometrica è possibile sottoscrivere sia i contratti/operazioni che intende stipulare con la Banca, sia i contratti/operazioni che intende stipulare con le società di cui la Banca colloca o distribuisce i prodotti e servizi e che hanno aderito allo stesso sistema di firma grafometrica nei rapporti con la clientela. L'utilizzo della firma grafometrica sarà possibile in modo graduale, aumentando progressivamente nel tempo le tipologie di documenti sottoscrivibili dal cliente con questa nuova modalità di firma. Il cliente potrà comunque sempre chiedere che si proceda alla sottoscrizione con il sistema cartaceo al di fuori dal campo di applicazione del presente documento. Gli applicativi generano il documento in formato PDF e lo inviano alla piattaforma di firma grafometrica. I documenti possono pertanto essere visualizzati sul tablet affinché il cliente possa leggerli e firmarli.

Firmati i documenti sul tablet, gli stessi vengono trasmessi in via telematica al Cliente, nella apposita sezione del sito. Qualora il cliente non è titolare di un'utenza dei servizi online, l'operatore/consulente finanziario provvederà a svolgere l'intera procedura di vendita in formato cartaceo.

VERIFICHE CONCLUSIVE

Viene effettuata una verifica da parte del sistema di firma sulla presenza di tutte le firme all'interno dei documenti da firmare e solo dopo tale verifica il fascicolo documentale può essere chiuso. La documentazione correttamente formata, verrà inviata ai sistemi di conservazione sostitutiva in quanto incaricato del servizio di conservazione.

8. DESCRIZIONE DELLE PROCEDURE DI SICUREZZA

Tutti i documenti informatici, una volta generati in esecuzione delle procedure interne, saranno sottoposti dal sistema informativo di BNL al cliente in formato .pdf sul tablet e non saranno modificabili mediante software di scrittura, né prima né dopo la sottoscrizione da parte del cliente. I dati grafometrici acquisiti sono cifrati e sigillati elettronicamente all'interno del documento informatico cui si riferiscono ed all'interno del Tablet durante il processo di firma ed esportati in modalità criptata. Durante il processo di firma i dati grafometrici non saranno oggetto di verifica alcuna, né potranno mai fornire informazioni sui dati personali del cliente firmatario.

In definitiva, il Servizio di FEA che verrà fornito alla clientela di BNL, in conformità a quanto previsto dalle norme tecniche, è in grado di garantire:

- la connessione univoca della firma al soggetto che la ha apposta¹;
- il controllo esclusivo del sistema di generazione della firma da parte del firmatario, in quanto i dati grafometrici sono generati direttamente dallo stesso firmatario²;
- la possibilità di rilevare se i documenti informatici sottoscritti siano stati modificati dopo l'apposizione della firma da parte del cliente, in quanto, è possibile verificare in qualunque momento l'integrità e l'autenticità del documento informatico sottoscritto³.

Si precisa che BNL ha provveduto a stipulare apposita polizza assicurativa per la responsabilità civile derivante da inadeguate soluzioni tecniche nell'erogazione del servizio nei confronti dei soggetti utilizzatori della FEA⁴.

¹ Cfr. art. 56, c. 1, lett. b) delle Norme Tecniche

² Cfr. art. 56, c. 1, lett. c) delle Norme Tecniche.

³ Cfr. art. 56, c. 1, lett. d) delle Norme Tecniche; cfr. altresì Deliberazione CNIPA del 21 maggio 2009 n. 45.

⁴ Cfr. art. 57, c. 2 delle Norme Tecniche.

9. APPLICAZIONE DELLE MISURE DI SICUREZZA

In ciascuna fase del trattamento, BNL garantisce non solo l'adozione delle misure minime di sicurezza previste dall'Allegato B del Codice Privacy, ma anche l'adozione delle ulteriori misure di sicurezza messe a disposizione dall'attuale conoscenza tecnica, volte ad ottenere l'irreversibilità e l'immodificabilità dei dati grafometrici raccolti nonché ad escluderne il rischio di corruzione o sottrazione.

Le misure di sicurezza adottate da BNL nell'erogazione del servizio risultano infatti corrispondenti ai più elevati standard di sicurezza offerti dal mercato in base alle attuali conoscenze tecniche e scientifiche.

I Signature Pad non possiedono un sistema operativo atto all'installazione di software ma interagiscono esclusivamente con il client di firma grafometrica.

Il dato grafometrico acquisito dal tablet viene criptato a pacchetti direttamente durante il processo di firma ed unito al documento pdf. Nessuna traccia del dato grafometrico resta nella memoria dei dispositivi né tantomeno può essere visualizzato né dai consulenti finanziari/operatori né da parte di altri operatori coinvolti nella gestione documentale.

10. CONSERVAZIONE

I documenti prima di essere sottoscritti risiedono sul sistema di BNL, che ne cura la predisposizione.

I dati grafometrici delle singole sottoscrizioni raccolte, una volta acquisiti in modo criptato vengono incorporati nel documento informatico al quale si riferiscono al fine di garantire la connessione univoca della firma al documento sottoscritto⁵, e sono poi conservati in un tutt'uno con esso presso l'archivio di conservazione a norma.

Il cliente, la Banca ed il Consulente Finanziario hanno sempre a disposizione⁶ una copia immagine del documento informatico sottoscritto⁷.

11. PROPORZIONALITÀ RISPETTO AI FINI

Questo sistema è stato predisposto per andare in contro ad una concreta esigenza di mitigazione del rischio in aree delicate e sottoposte a concreti pericolo di contenzioso da parte del cliente.

Infatti questo sistema è stato adottato tenendo in considerazione non solo la scelta meno costosa, o meno complicata, o di più rapida attuazione, ma è stata scelta tenendo in considerazione l'impatto sui diritti degli utenti.

Nel caso di specie il titolare del trattamento, prima di installare il sistema descritto in questo documento, ha valutato, obiettivamente e con un approccio selettivo, che l'utilizzazione ipotizzata fosse in concreto realmente proporzionata agli scopi prefissati e legittimamente perseguibili.

In questo modo si è evitata un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli altri interessati.

La proporzionalità è stata tenuta in considerazione in ogni fase o modalità del trattamento, sia quando si deve stabilire:

- se sia sufficiente ai fini della sicurezza;
- se sia realmente essenziale ai fini prefissati;
- quali dati rilevare, se registrarli o meno, e secondo quali modalità.

Pertanto i dati raccolti vengono trattati in modalità pertinente e non eccedente la finalità relativa la digitalizzazione della documentazione cartacea, per poter consentire a posteriori l'analisi grafologica dei dati biometrici inseriti nel documento.

12. LICEITÀ

La firma grafometrica è utilizzata esclusivamente per la digitalizzazione della documentazione (o parte di essa) intercorrente tra la Banca (il Titolare del trattamento) ed il Cliente (l'Interessato al trattamento) e per la sostituzione della modulistica cartacea.

Inoltre il trattamento dei relativi dati biometrici è effettuato nel rispetto delle previsioni normative previste dagli artt. 7, 11, 13, 37 del d. lgs 196/03 e del Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014, previo consenso dell'interessato.

Qualora i documenti per i quali viene operata la digitalizzazione siano previsti a seguito di norme di legge o regolamenti, essi sottostanno alle previsioni e ai vincoli previsti da queste normative.

⁵ Cfr. art. 56, c. 1, lett. h) delle Norme Tecniche.

⁶ Cfr. art. 56, c. 1, lett. e) delle Norme Tecniche.

⁷ I file forniti alla clientela contengono i Dati Grafometrici. I Dati Grafometrici non possono essere estratti né da BNL né dal cliente senza la chiave privata di cifratura custodita dalla CA Aruba S.p.A.



13. NECESSITÀ

Vengono raccolti solo i dati biometrici che consentono a posteriori l'analisi grafometrica del campione biometrico a seguito di controversie sorte tra le parti.

14. FINALITÀ

Le finalità della raccolta del dato biometrico sono quelle di digitalizzazione dei documenti e di sostituzione della modulistica cartacea. Tali finalità sono comunicate agli interessati all'interno dell'informativa prevista dal Codice privacy ai sensi del relativo art.13.