DATA PROTECTION PRELIMINARY VERIFICATION TRANSLATION: ITALY

Date of decision:
12 September 2013

Requested by:
Fineco Bank S.p.A.

Italy; data protection; preliminary verification; biometric data; advance electronic signature

System for subscription of acts, documents, contracts and other documents in electronic form related to products and services offered by a bank – Preliminary verification requested by Fineco Bank S.p.A. – 12 September 2013

Record of the action

n. 396 of 12 September 2013

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

Having convened today, in the presence of Dr Antonello Soro, the President, Dr Augusta Iannini, vice president, Dr Giovanna Bianchi Clerici and Professor Licia Califano, components, and Dr Giuseppe Busia, general secretary;

HAVING REGARD TO Legislative Decree 30 June 2003, n. 196, 'Code regarding the protection of personal data' (hereinafter the 'Code');

CONSIDERING the Legislative Decree 7 March 2005, n. 82 containing the 'Digital Administration Code';

CONSIDERING the d.P.C.M. 22 February 2013, containing the 'Technical rules relating to generation, affixing and verification of advanced, digital and qualified electronic signatures, in accordance with articles 20, paragraph 3, 24, paragraph 4, 28, paragraph 3, 32, paragraph 3, letter b), 35, paragraph 2, 36, paragraph 2, and 71';

HAVING REGARD TO Legislative Decree 1 September 1993, n. 385, embodying the 'Consolidated Law on Banking and Credit';

CONSIDERING the Legislative Decree 24 February 1998 n. 58, containing the 'Consolidated text of provisions on financial intermediation, pursuant to Articles 8 and 21 of the Law of 6 February 1996, n. 52';

CONSIDERING the preliminary verification request dated 29 April 2013 and presented by Fineco Bank S.p.A. pursuant to art. 17 of the Code, as well as the company's further communication of 12 July 2013;

HAVING EXAMINED the records on file;

HAVING REGARD TO the observations made by the secretary general pursuant to art. 15 of Regulation 1/2000;

REPORTER Dr Antonello Soro;

FOREWARD

1. The request made by the company.

1.1. The company – Fineco Bank S.p.A. operates 'exclusively online and through financial promoters located throughout the national territory' – has expressed its intention with the perspective (among other things) to enhance the quality of its services, to provide a system capable of allowing a subscription in electronic form of acts, contracts and other documents related to products and services offered by the bank through '[...] the combined use of electronic signatures and [...] the collection of behavioural measured biometric data' taken from the signature applied by customers on a special 'tablet' the above promoters are endowed with. The service of a 'graphometric signature'[1] (as per the term used by the bank), which when used, detects 'dynamic' characteristics (rhythm, speed, pressure, acceleration, motion), as well as an image of the signature applied by the customer when signing the above mentioned document, would have as 'main' objective to simplify and streamline the processes of interaction between the company and its customers, ensuring at the same time a standard of higher security in the subscription operations; the service would appear as 'a particular type of electronic signature', an advanced electronic signature able to ensure, in accordance with the

[1] In Italy, the term 'graphometric' is used to describe a signature that combines the use of biometry, public key encryption and hashing algorithm.

provisions of the law, the identification of the author, as well as the integrity and immutability of the document signed (see also section 1.5).

1.2. The process that Fineco intends to adopt is based on a so called graphometric signature solution developed by Namirial S.p.A. (accredited as Certification Service Provider by the Agency for Digital Italy) and that has received ISO 27001 certification of its security management system. Such signing process requires the processing of biometric data of interested subscribers and is based, in short, on the following phases:

- the financial promoters, employees of the bank, show the customer how to use the service of 'the graphometric signature';

- the promoter releases due information pursuant to art. 13 of the Code and acquires the related consent of the customer in the case of access to the service;

- the promoter submits the (previously identified) client the document in electronic format;

- the customer affixes the 'graphometric signature' on a hardware device capable of capturing biometric data at the same time of the act of affixing the signature; such data undergoes a process of intermediate encryption based on a symmetric key (which excludes the possibility of view of the data 'in the clear' in their entirety) and an additional encryption using the public key included in a digital certificate called 'protection certificate Fineco' also contained in the digital signature device supplied to the promoters;

- the encrypted biometric data and the image of the signature are entered into the appropriate fields of a document saved in pdf format;

- a series of digest strings obtained by applying a hash algorithm are generated for the subsequent verification of the integrity of the signature, and of the documents in electronic format are also encrypted with the 'public key' associated with the certificate issued by Namirial S.p.A.;

- the signed electronic document is then sent through secure channels to the 'documentary System of Fineco' and to the 'archive of compliant conservation' of In.TE.SA. S.p.A. (the company in charge of the documents management in accordance with the requirements established by Legislative Decree no. N. 82/2005) for the related preservation;

- The customer receives a hard copy of the document signed with 'graphometric signature' or, alternatively, its electronic duplicate via e-mail.

The biometric data, electronically encrypted and 'sealed within the electronic document to which they relate', would be collected by the system 'in a completely "acritical[2]" manner', in such a way that it excludes any possibility of tracing any information regarding the health status of the signatories.

In addition, these data do not 'reside', not even temporarily, within the 'tablet' and, once embedded in the document, they would be 'erased from and overwritten in the (RAM) memory of the computer', therefore not making it viewable neither to the financial promoters, nor to In.TE.SA S.p.A. (which, however, would only barely manage the electronic documents on behalf of the bank), let alone by Fineco Bank S.p.A. and Namirial S.p.A.

The bank, in fact, might not have access 'in the clear' to the 'graphometric data' embedded in these electronic documents (the data would not even be available to Namirial S.p.A.), except through the mutual cooperation between the two companies, since the private key, required to decrypt the data, would be held only by the certifying body, while the custody of its 'unlock credentials' would be entrusted only to the bank.

In any case, the deciphering of biometric data and related access to data 'in the clear' would be permitted 'exclusively in the cases envisaged by the law, upon the request of the competent authorities' (typically due to any legal proceedings relating to the disavowal of a signature); in such cases, Namirial S.p.A. would put at the disposal of a handwriting expert appointed by the court a tool (called 'Forensic FirmaCerta') that will allow the process of decryption to be managed according to high security standards, ensuring that the operations of 'encryption and decryption [would take place] contextually with the opening and closing of the expertise.'

The data collected during the investigation would be encrypted with the 'public key' contained in the authentication certificate of the expert himself, the only one 'able to open the expertise using his own signature device'.

According to the bank, the system would be devised to acquire 'a limited number of pieces of information,

[2] This means 'without applying any verification mechanism'.

relevant to the purpose [...] pointed out, not [being] envisaged the acquisition of data, additional or related to the state of health' of the interested parties. In addition, the processing of biometric data would be 'limited in type and breadth, to the bare minimum to allow the bank to abide by the statutory requirements of CAD,' so that 'no other processing or use would be possible.'

1.3. The service, as described, would be activated on a purely voluntary basis, (including the option to provide the information to the concerned persons), after obtaining the free consent of the latter. Should the customer not wish to give consent to the processing, or later withdraw such consent, the documents could be subscribed according to 'the process of signing in the "traditional" way on paper'.

The bank also said that it will designate IN.TE.SA. S.p.A. as the data processor pursuant to art. 29 of the Code, stating in detail the tasks assigned to it and supervising the strict compliance with the instructions given; by contrast, the financial promoters, in charge of the operations of collecting biometric data of the persons concerned, would be designated as operators in charge of processing pursuant to art. 30 of the Code.

The biometric data collected, encrypted, and 'embedded' within the electronic document would be kept, within the limits of the specified objectives, for the period of time established by the provisions in force (art. 2220 cod. Civ., Art. 119 d. lgs. n. 385/1993), subject to the need for their further preservation by reason of any dispute in court.

On the merits of the additional requirements imposed on the processor of the personal data processing, the bank said it had already taken steps to update (as duly reported by the Office) the notification previously made, pursuant to art. 37 of the Code, as well as having adopted the envisaged security measures to protect the personal data of the persons concerned (including the 'immediate encryption of the biometric information' and the use of channels of 'encrypted communication'), and stating that the retention of data by IN.TE.SA. S.p.A. will also take place in accordance with the requirements set by the resolution of the (former) CNIPA n. 11/2004.

1.4. The system, in addition to ensuring greater rapidity in the transactions with the promoters and a reduction in operating costs and litigation, would ensure the bank will be able to properly fulfil the obligations imposed by the law in force, having particular regard to the fulfilment of the requirement of written form under penalty of a contract being invalid (article 117 of Legislative Decree no. n. 385/1993 and art. 23 of Legislative Decree no. n. 58/1998). As already mentioned, in fact, the service described would, in the banks view, meet the requirements of the Digital Administration Code and the recent d.P.C.M. of 22 February 2013 on the theme of an advanced electronic signature (especially with regard to the requirement of 'writing') and would diverge – as far as the characteristics of the treatment are concerned – from the digital signature solutions so far examined by the Authority (see Provv. January 31, 2013, cit.), being the collection of biometric data functional to ensure a unique connection between the signature applied in electronic form on the document and its author.

2. Authority Assessment.

2.1. The preliminary verification presented by Fineco Bank S.p.A. relates to the processing of personal data in relation to the use of a system suitable to detect the image of a handwritten signature affixed by the interested parties on suitable devices ('tablets') and to analyse several parameters of which (pressure, acceleration, inclination, etc.) in view of the subscription in electronic form of acts, contracts and documents related to products and services offered by the bank by means of its promoters.

Preliminarily, it should be noted that the Article 29 Working Party on the protection of personal data under art. 29 of Directive 95/46/EC believes that systems based on the use of devices that can detect the'dynamics' features of the signature determine a processing of biometric data ('graphometric' as used by the bank) are behavioural in nature, as such due under the scope of the rules for the protection of personal data (see Working Document on Biometrics of 1 August 2003, WP 80, and Opinion 3/2012 on developments in biometric technologies of 27 April 2012, WP 193, see also Measure by the Guarantor 31 January 2013, cit.).

That said, it is important to assess, in this perspective, if the system under the scrutiny of the Authority could be deemed as compliant, limited to profiles regarding the treatment of a graphic signature and biometric data of the users, to the discipline of the Code, with particular reference to meeting the principles of necessity, legality, purpose and proportionality (article

3:11, paragraph 1, lett. a), b) and d) of Legislative Decree n. 196/2003).

2.2. In this regard, it is worth underlining that the processing of personal data (including biometric) that the company intends to carry out, is permissible according to the documents produced and the statements made pursuant to art. 168 of the Code.

Granted, in fact, that the treatment of the image of the signature on the 'tablet' is not characterized, even if performed with electronic instruments, by specific and obvious risks for those involved (also because of the security measures declared by the owner and strict operating protocols required by the law on the certifying agent), it must also be emphasised, with specific reference to the processing of biometric data of subscribers, that the recent d.P.C.M. of 22 February 2013, adopted with the favourable opinion of the Guarantor (see Provv. 24 November 011, doc. Web n. 1.870620), expressly includes that data among the elements used for the generation of advanced electronic signatures (article 56).

To this must be added that the processing of these data, made only after obtaining the free and informed consent of the signatories (articles 13 and 23 of the Code) and the pursuit of legitimate goals made known to the parties concerned (article 11, paragraph 1, letter b) of the Code), may actually be functional, also as a guarantee to the latter, in view of possible litigation related to the disavowal of the subscription applied to acts and contractual documents, providing possible evaluation elements that can also be used in court.

This is a corollary to the fact that the use of the proposed solution could effectively contribute, through the guarantee of authenticity, integrity and non-repudiation of the documents signed electronically, to give more certainty in legal relationships with users (in this case, however, mediated by financial advisors).

Therefore, to the extent that the 'graphometric signature' – especially in light of the requirements of art. 117 of Legislative Decree no. 385/1993 and 23 of Legislative Decree no. 58/1998 –, can actually be included among the solutions that, in accordance with the law (cf. art. 21 of Legislative Decree no. 82/2005), satisfy the requirement of written form, it can reasonably be concluded that the treatment of personal data (including biometric) connected to the service in question – which undoubtedly favours the legitimate organisational needs of the company – where made in the manner specified and within the limits of its stated purpose, is not in violation of the principles of art. 11, paragraph 1, lett. a) and b) of the Code; the above, moving from the further consideration that the system is also compliant with the 'technical specifications' laid down by ISO – in this case relating to the requirements for the management of information security: ISO/IEC 27001: 2005 – already deemed relevant by the Guarantor also under the terms of the regulation on the protection of personal data (see Provv. 14 July 2011, doc. web n. 1836335; Provv. 26 May 2011, doc. web n. 1832558; Provv. 2 December 2010 doc. web n. 1779678).

With regard, then, to the observance of the principles of necessity and proportionality (article 3:11, paragraph 1, lett. d) of the Code), the system described, in the specified configuration modalities, – i.e. such that, according to the company, it is not allowed, under any circumstances, to acquire information about the health status of those concerned – , results as being designed to collect a limited amount of information (rigidly listed as: the image of the signature, the rhythm, the speed, the pressure, the acceleration, the movement), as of now not exceeding the purposes stated by the company. In addition, the biometric data will not be available 'in the clear' to the controller except in cases provided for and at the express request of the judicial authority.

In terms of security of data processed, it can be assumed that the set of measures adopted in the whole process of the management of the biometric data of the interested parties constitute, as a whole, security measures that, on the basis of current knowledge, may be deemed appropriate.

In particular, it is considered appropriate that the company given the task of the issuance of certificates for signing and encryption is a certification body accredited by AgID under art. 29 of CAD[3] and that the private key and the corresponding unlock code associated with the security certificate used by Fineco for encryption of the biometric data are kept separate, thus avoiding the possibility of proceeding to decrypt the biometric data except in cases where is necessary and ordered by the court.

[3] Codice dell'Amministrazione Digitale, i.e. Legislative Decree No 82/2005.

Notwithstanding the above, it is considered appropriate, in the absence of such indications by the holder, to indicate further steps and measures aimed at improving the safety of the process to guarantee the persons concerned.

In fact, the confidentiality of the biometric data during the collection phase is based not only on the robustness of the procedure, but also on the security of the devices, an aspect on which the bank must pay the utmost attention to ensuring their use exclusively to users (financial promoters) enabled to their use.

In this regard, if not yet provided, appropriate measures should be adopted aiming to reduce the risk of the installation of unauthorised software or modification of the configuration of the devices supplied to the promoters, also adopting every precaution useful to counteract the action of any malicious software (malware). If it has not been done so yet, a management system shall also be adopted of the devices used in graphometric treatments based on digital certificates and security policies that govern, on the basis of predetermined criteria, the conditions for their secure use; in particular, remote wiping capabilities shall be available and applicable in cases of lost or stolen devices. The bank must also provide for appropriate policies for the management of security incidents within the different phases of the biometric process.

Still, it appears as appropriate, on the other hand, the proposed designation of financial promoters such as personal data operators, to the extent that the bank – upon renewed assessment – does not consider subsisting, with reference to the role played by them in practice, the assumptions referred to in articles. 4, paragraph 1, lett. f) and g), 28 and 29 of the Code.

Finally, the company cannot keep personal data (including biometric) taken from the signature applied on tablets beyond the deadline for conservation of the act or document to which the signature relates (article 11, paragraph 1, lett. e) of the Code), subject to the possible need for their further preservation by reason of specific provisions of the law or for the protection of a legal claim.

It is understood that, under rule n. 25 of the technical regulations regarding minimum security measures, the installer of the graphometric system shall provide Fineco with the certificate of conformity, to be kept by the controller.

Likewise, it is understood that the lawfulness of the processing remains subject to the actual observance of all the obligations that the company, in the course of the proceedings, is committed to respecting (point 1.3) and to the possibly additional ones imposed on the basis of the existing rules (in this effect, however, it appears that the fact that the 'graphometric' signature service that the bank intends to use in its relationships – mediated – with its customers is applicable, as stated by the same company, as an 'advanced electronic signature' as planned and regulated by the aforementioned Legislative Decree no. 7 March 2005, n. 82 and d.P.C.M. 22 February 2013).

NOW, THEREFORE, THE GUARANTOR

pursuant to articles 17 and 154 of the Code and at the conclusion of the relevant procedural process, accepts the request for prior checking submitted by Fineco Bank S.p.A. and, consequently, allows the processing of personal data (including biometric) associated with the use of the system described, provided that:

- it is carried out in the manner indicated in fiction and for the sole stated purpose;

- the company, if it has not already done so, adopts additional technical and organisational security mechanisms to protect the biometric data of the interested parties described in paragraph 2.2 and, in particular:

- it adopts appropriate measures to reduce the risk of unauthorised installation of software or modification of the configuration of the devices supplied to the promoters, additionally taking every precaution useful to counteract the action of possibly malicious software (malware);

- a management system of the devices used in the graphometric treatments based on digital certificates and security policies that govern, on the basis of predetermined criteria, the conditions for their secure use. In particular, remote wiping capabilities applicable in cases of lost or stolen devices shall be available;

- suitable policies for the management of security incidents within the different phases of the biometric process are implemented;

- the company is released and keeps the certificate of conformity referred to in Rule 25 of Appendix 'B' to the Code;

- the company actually observes all the obligations that, in the course of the proceedings, it committed to respect (point 1.3) and the additional ones imposed on the basis of the rules in force.

Under articles 152 of the Code and 10 of the legislative decree n. 150/2011, against the present provision may be opposed to the ordinary courts, by application lodged at the ordinary court of the place of residence of the owner of the data, within the period of thirty days from the date of communication of the measure or sixty days if the applicant resides abroad.

Rome, 12 September 2013

THE PRESIDENT

Soro

THE REPORTER

Soro

THE SECRETARY-GENERAL

Busia

With thanks to **Franco Ruggieri** for his help with this translation.