DATA PROTECTION PRELIMINARY VERIFICATION TRANSLATION: ITALY

Date of decision:
31 January 2013

Requested by:
Unicredit S.p.A.

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

See also Newsletter dated 19 April 2013 [doc. web n. 2304808]

Processing of biometric data. Preliminary request from Unicredit S.p.A. – 31 January 2013

Record of the action

n. 37 of 31 January 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 the legislative decree 30 June 2003, n. 196 (Code relating to the protection of personal data);

CONSIDERING the request of the preliminary verification of 21 September 2012, presented by Unicredit S.p.A. pursuant to art. 17 of the Code and regulated by communication of 29 November 2012;

HAVING EXAMINED the records on file;

HAVING REGARD TO the observations made by the Secretary-General pursuant to art. Regulation No 15 of the Guarantor. 1/2000;

REPORTER Dr Antonello Soro;

FOREWARD

1. The request made by the company.

By memorandum of 21 September 2012, Unicredit S.p.A., in view of a 'improvement in the quality of delivery of its services,' said it wanted to make available for the benefit (even) of customers a subscription service of documents with digital signature based on a biometric authentication procedure performed by the use of a signpad (called 'tablet'), intended to confer, among other things, greater security in the performance of operations at the counter. The system, as reported, would collect behavioural biometric characteristics of the client, by detecting and, at the same time, by analysing some parameters (rhythm, speed, pressure, acceleration, movement) relative to its handwritten signature – affixed by means of a hardware device 'dedicated' and connected via a USB (Universal Serial Bus) to the branch office operator's terminal in charge of them – in order to compare them with those previously stored during the subscription to the 'service' phase. Any positive comparison, which would result in user authentication, will enable the initiation of the procedure of digital signature of the document examined by the customer.

The adoption of such a system, according to the company, would allow, amongst other things, 'to develop a series of numerous advantages, also to the benefit of customers', being able to guarantee a 'greater security against fraud attempts' through the reduction of 'risks of identity theft and [of] forgery of the signature.'

2. Operation of the system and methods of the processing of biometric data associated with it.

2.1. According to a summary of the proposed action, the system would operate in the following terms.

The customer who wishes to join the service, once he/she grants his/her informed consent to treatment, would be invited, during the enrolment phase, to affix 6 signatures on the 'tablet' for the purposes of biometric 'recognition'; the information collected (called a specimen), is acquired by the system in a way that is relevant and not excessive in relation to the purpose of the service and in 'acritical[1]' form – in such a way, that is, not to allow, even accidentally, to identify that the signatory sufferes a health problem from the nature of his signature – would be sent to

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

the 'biometric server' for the purpose of their immediate conversion, through a hashing algorithm, into a sequence of characters ('string') unchangeable and non-reversible into the 'original' biometric data.

After the enrolment phase, on the occasion of the signing of documents with a digital signature, the customer would be invited to affix his signature on the tablet for authentication every time: the biometric data thus collected would be compared with those previously stored by the system, which would allow the initiation of procedures for the use of digital signatures only in the case of where the 'match' is positive. Following biometric authentication, in fact, cryptographic keys, owned by In.Te.S.A. S.p.A. (a certification authority certified by the Agenzia per l'Italia Digitale, previously DigitPA) kept inside secure devices called Hardware Security Module (HSM), would be made available for the digital signature of the documents viewed by the individual.

The system, 'thanks to a self-learning function (continuous enrolment),' would be able to constantly update the originally recorded user 'profile', so as to guarantee the ability to use the service even in the event of any changes, in the course of time, of the 'style of signature'; in addition, it would be configured 'with a minimum acceptance level of signature verification (a score) equal to 80% of compliance with respect to the template originally created,' so as to ensure, 'on the point of signature verification (a trade-off of false positives vs. false negatives) [...] a high level of credibility and reliability', however, could be expandable as a result of periodic monitoring and verification that the company has declared its intention to carry out.

The biometric data acquired, immediately encrypted and indexed with unique codes associated with each customer, would be stored on servers located variously in the country at the facilities of Unicredit S.p.A. and UniCredit Business Integrated Solutions S.c.p.a. (a company tasked, on behalf of the former, to the management and delivery of information systems and related technical infrastructure), designated as processor in charge of the treatment under articles 4, paragraph 1, lett. g) and 29 of the Code. In addition, the same data, without prejudice to the eventual withdrawal of consent by the parties concerned and the need for further conservation dictated by any dispute, would be retained for the duration of the service.

The company, in order to ensure high security standards, claimed to have adopted, together with the minimum measures listed in annex 'B' to the Code, 'any additional security measures, in line with the current technical and technological knowledge, aimed at achieving the irreversibility of the graphometric[2] data, the immutability of the same, as well as to rule out the risk of corruption and theft'. In particular, it is claimed that the biometric data of the persons concerned, encrypted using encryption keys (in turn encrypted with a digital certificate previously produced), are immutable and irreversible; moreover, even the communication flows between the various 'infrastructure components occur in authenticated and encrypted mode,' while 'accesses [are] recorded in the audit log of the system and made available' for inspection.

The authentication process, as described, would be 'independent and distinct versus the signature procedures for the banking provisions and/or subscription of contracts' with the bank. The affixing of the signature on the tablet, in fact, would constitute 'the only element that leads to the authentication process, resulting in the signing process.' To confirm this, the company stated that the 'certification authority [...] is in no way involved in the treatment process of the biodynamic data', the latter acting 'solely in the process of signing documents' and in view of 'creation and management of the qualified certificate and keys for signing.'

2.2. The information that the company intends to provide to the interested parties prior to the enrolment phase 'will be further and distinct from the general information provided to all customers when establishing a business relationship with Unicredit' and will explicitly indicate the 'optional' character of the treatment. The latter, moreover, 'will be subject to the express manifestation of consent by the parties concerned [...] and [it will be possible to] revoke it at any time.' The company, moreover, stated that it will designate operators of the treatment 'giving them appropriate instructions on the operation of instruments and methods of affixing digital signature', stating that it had already taken steps to modify the notification of processing operations on 7 June 2012 (a circumstance verified by the Authority).

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

2.3. The decision to adopt the system in question, according to the applicant company, meets the need, among other things, to rigorously identify customers during the performance of banking operations, in accordance with the obligations provided for that purpose by the anti-money laundering legislation (Legislative Decree no. n. 231/2007). In addition, the use of biometric data – considered appropriate, as mentioned, to prevent and hinder fraud associated, above all, for identity theft[3] – would guarantee the signer from further risk of loss of the other tools (smart cards, USB tokens, etc.) required for the activation of the application process of digitally signing documents.

3. Observations by the Authority.

3.1. The preliminary application submitted to the Authority relates to the processing of biometric data for the purposes of authentication in relation to the use of a system designed to analyse and compare a number of parameters derived when an interested party affixes their handwritten signature on a predefined device, as part of the procedure for digitally signing documents. This measure, which takes into account the content of the statements made by the applicant company (pursuant to art. 168 of the Code) on the difference between the digital signing procedure and the authentication, focuses only on matters relating to the processing of biometric personal data connected to the latter.

Worth a preliminary mention in this regard is that the Article 29 Working Party under art. 29 of Directive 95/46/EC believes that the use of systems based on the use of devices that can detect the signature 'dynamic' features determines, in fact, a treatment of behavioural biometrics data, that as such falls in the scope of the regulations for the protection of personal data (see Working Document on Biometrics of 1 August 2003, WP 80, cf. further Opinion 3/2012 on developments in biometric technologies of 27 April 2012, WP 193). That said, it is important to assess, in this perspective, if the system under the scrutiny of the Authority can be assessed as compliant, limited to laws regarding the processing of biometric data of customers in the authentication phase, with the discipline of the Code, with particular reference to compliance with the principles of necessity, legality, purpose and proportionality (article 3:11, paragraph 1, lett.), b) and d) of Legislative Decree n. 196/2003); this, even in the case in which the biometric data is collected, as in the present case, only for purposes of completion of the enrolment phase and is subsequently used (in the form of a numerical code) for the operations of comparison in the authentication procedure (in topic, see Provv. 23 January 2008, doc. web n. 1487903; Provv. 26 May 2011, doc. web n. 1832558; Provv. 4 October 2012, doc. web n. 2059743).

3.2. In this regard, it should be noted that the processing of biometric data that the company intends to make, based on the documentation submitted and the statements made, is lawful. It is worth to emphasise, in general terms, that the rigorous and reliable identification of customers, already required from the banks in the interests of sound and prudent risk management (see Basel Committee on Banking Supervision), is, often, even placing an obligation on the part of all the financial companies by specific sector regulations (see, for example, the Legislative Decree n. 231/2007, over which also see Guarantor Opinion of 25 July 2007, doc web n. 1431012, more generally, on the obligations regarding customer identification, cf. Provv. 27 October 2005, doc. web n. 1189435 and Provv. 25 October 2007, bearing 'Guidelines for processing data on the relationship between banks and customers', doc. web n. 1457247) the violation of which, however, can be a source of civil liability (see Cass. 16 December 2009, n. 3350), also assessable on the basis of art. 1176, 2nd paragraph, cc (with possible relevance, therefore, also of minor negligence: in this sense, Trib. Ariano Irpino 2 October 2008, Cass. 30 January 2006, n. 1865). To this, it must be added that the biometric authentication of customers in view of the digital signature of the documents would, on the one hand, help to effectively counter any attempts of fraud and, secondly, streamline and speed up (also for the benefit of the same customers) recognition operations at the counter. Given, then, that the processing of biometric data of the signatories, to the extent that it can actually be considered compatible with the current regulatory framework applicable to services of a digital signature (in this sense, however, a first opening to usability of biometric techniques, albeit within the wider context for the services of 'the electronic signature', seems apparent already in the 'Guide to the Digital Signature' prepared by the then CNIPA, version 1.3 in April 2009, p. 11, in perspective, the 'Scheme d.P.C.M. under articles 20, paragraph 3,

[3] That is, a thief using the personal information of a victim for the purposes of theft.

24, paragraph 4, 28, paragraph 3, 32, paragraph 3, letter b), 35, paragraph 2, 36, paragraph 2, and 71 of the del d. l.gvo 7 March 2005, n. 82', available at www.digitpa.gov.it), will be based on the free consent of the parties and to the pursuit of legitimate goals made known in advance to the latter ones, it must be held that, in the light of what is mentioned above, are integrated, with respect to this case, the requirements laid down in articles. 11, paragraph 1, lett. a) and b), 13 and 23 of the Code.

With regard, then, to the observance of the principles of necessity and proportionality (articles 3 and 11, paragraph 1, lett. D) of the Code), is to be stressed that the system described in the light of the statements made, is ordained to capture only the information relevant to the purpose of authentication of the parties concerned. Also, the service appears being configured, based on the information provided, to collect a limited amount of information (in this sense, cf. template information produced by the company), not resulting, however, in the proposed system configuration mode – such, according to the company, not to allow, under any circumstances, the acquisition of information about the health status of those concerned – prepared for the acquisition of data beyond the scope of those required for authentication purposes.

In terms of security of the data processed, it can be assumed that the immediate encryption of the biometric information of the interested parties (through a key in turn encrypted itself), the use of channels for transmitting encrypted data and also the use of authentication and access logging constitute appropriate measures under articles 31 and following of the Code. Also, the fact that the biometric data will not reside, not even for limited periods, on the tablet (see Project SignPad of 25 June 2012) and the template, not reversible in the original biometric data, will be stored in a database specifically 'dedicated' – measures, together with those already mentioned, suitable to suggest as remote the risk of any improper operations on the biometric data of the interested parties – leads to consider the proposed treatment, in terms of security, as conforming to the rules of the Code.

Similarly, by reason of the provisions of art. 11, paragraph 1, lett. c) of the Code, it must be assessed in a positive way the choice to adopt the mechanisms of self-learning, suitable to ensure, over time, the 'quality' of biometric data processed.

Finally, it is noted that the product information in the documents submitted by the bank does not have any problematic aspects, and it is deemed as law compliant that the company, subject to any applicable specific standards, retain the biometric data of the interested parties for a period of time strictly necessary to achieve the purposes for which the same data will be collected and further processed (article 11, paragraph 1, lett. e) of the Code), while remaining without prejudice their further retention in the case of any dispute, even when also in court. In the event of termination of the treatment, of course, the data must be deleted immediately or within the necessary technical time allowed by the system.

NOW, THEREFORE, THE GUARANTOR

pursuant to art. 17 of the Code, at the conclusion of the preliminary verification requested by Unicredit S.p.A. regarding the use, as part of the subscription service of documents with digital signatures, of a system for the recognition of biometric characteristics of the handwritten signature affixed by the interested parties on devices dedicated to it, admits the processing of biometric data, provided that it occurs only for the stated purpose, with the modalities indicated in this application and in due respect of the statements from the instant pursuant to art. 168 of the Code.

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 where 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, 31 January 2013

THE PRESIDENT

Soro

THE REPORTER

Soro

THE SECRETARY-GENERAL

Busia

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