DATA PROTECTION PRELIMINARY VERIFICATION TRANSLATION: ITALY

Date of decision:
31 January 2013

Requested by:
IT Telecom s.r.l. and Cassa di Risparmio di Parma e Piacenza S.p.A.

Italy; data protection; preliminary verification; biometric data; advance electronic signature; need to amend contracts; consent

See also Newsletter of 19 April 2013, [doc. web n. 2311886]

Biometric recognition systems. Preliminary assessment request from IT Telecom s.r.l. and Cassa di Risparmio di Parma e Piacenza S.p.A. – 31 January 2013

Record of the action

n. 36 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 Legislative Decree of 30 June 2003, n. 196, amending the Code regarding the protection of personal data (the 'Code');

CONSIDERING the request of the preliminary verification submitted by IT Telecom s.r.l. and Cassa di Risparmio di Parma e Piacenza S.p.A. (In his capacity of leader of Cariparma Crédit Agricole) pursuant to art. 17 of the Code;

HAVING EXAMINED the records on file;

HAVING REGARD TO the observations made by the Secretary General pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000;

REPORTER Dr Antonello Soro;

FOREWARD

1. The request made by the companies.

1.1. IT Telecom s.r.l. and Cassa di Risparmio di Parma e Piacenza S.p.A., in a joint memorandum of 27 April 2012 regularized subsequently, also in the interest of Banca Popolare Friuladria S.p.A. and Cassa di Risparmio della Spezia S.p.A., in a communication of 29 November 2012 – have expressed their intention to, respectively, provide, and use a service of remote digital signature with biometric authentication 'based on the use of devices that detect the dynamic features distinctive of a handwritten signature' applied by the users when digitally signing contracts or bank forms; that, in order to ensure to them, through systems of 'strong authentication', 'the use of their private keys [necessary] to make digital signature operations' over the counter. It would, in essence, be a system based on secure devices for signature, kept by IT Telecom s.r.l. (in its grade as a certification service provider accredited at the Agenzia per l'Italia Digitale, previously DigitPA), able to recognize the 'behavioural' characteristic of the user through the analysis of a number of parameters that can be derived from the signature (speed of gesture, pressure, acceleration, inclination, etc.), affixed by the latter on a specific 'tablet' present at the counter in view of its authentication and the simultaneous initiation of procedures for the signing of documents with a digital signature. Since the service, provided in practice by IT Telecom s.r.l., by interfacing with the computer facilities available at individual banks, would lead to a processing of personal data with potentially source of a number of specific risks for the subjects at issue, which is why the companies felt they had to submit to the Authority a request for preliminary verification pursuant to art. 17 of the Code.

In support of the application, IT Telecom s.r.l. and Cariparma S.p.A. have produced two separate documents relating to the mode of operation of the system and the characteristics of the process they, within their respective jurisdiction (see below), are planning to develop.

2. Document of IT Telecom s.r.l.

2.1. According to the documentation sent out by IT Telecom s.r.l., the general pattern envisaged for the performance of the service consists of two phases.

In the first phase ('provisioning'), the user who intends to join the service, after identification at the counter and 'registration' of his personal data in the information systems of the individual bank, 'will be associated with a set of information characteristics of his handwritten signature (called a specimen) detected by requiring the [subject] to affix on the tablet his/her [subscription] for at least three times.' The specimen obtained, consisting of synthetic digital representations (templates) generated during the collection of signatures (containing information related to the image of the signature, the identifier of the tablet and the 'biometric' characteristic of the signature), will be stored in a specific database kept at IT Telecom s.r.l., for the purposes of subsequent comparison during authentication.

As part of this preliminary procedure, the specimen, together with the identification data of the person concerned, will be forwarded by the bank, in encrypted form through expressly secure channels, to IT Telecom s.r.l. for the verification and validation of the application and to issue the digital certificate associated with the applicant.

The signatory, having previously being informed by the bank regarding the processing of personal and biometrics data consequently to his/her request to activate the service – for which the agreement of the customer is also acquired – will then confirm the request by signing the form provided by IT Telecom s.r.l. (which also contains the terms and conditions of service).

2.2. In the next phase of authentication, the user is invited, every time, to affix his signature on the tablet with the purpose, amongst other things, to activate the signing process aimed at applying a digital signature to the document; the information acquired, immediately converted into a template, are transmitted in encrypted form, together with a 'footprint' of the document to be digitally signed (digest, obtained with a hash algorithm) and the numeric identification code of the signatory, to a specific server hosted by IT Telecom s.r.l. The template calculated on the spot is compared with the one generated at the time of 'registration' to verify if it matches and ascertains that the serial number of the tablet is actually among those recorded.[1] Also, for security purposes, the 'hash' of the template is calculated too, so that you can verify any correspondence with the 'hash' of one the templates already verified in previous signature operations carried out by the same signatory; this measure has the purpose of preventing the possible fraudulent use of the service.[2] The authentication operation will end positively only if all three tests are completed successfully (in particular, in order to unlock the functions of digital signature, the first two tests should succeed, while the third must fail).

2.3. The entire authentication process, according to the company, must be regarded as distinct from the one related to affixing a digital signature. The biometric data of the users, in fact, will be treated, for the purposes of authentication, exclusively through the server dedicated to it, independent and separate from those used for issuing digital certificates and for affixing the digital signature; furthermore, the identification data of the users would be stored at a server different from the one provided for storing (in encrypted form) specimens, in order to prevent their direct and immediate associability. The same server, finally, would be located in areas protected and accessible only to the persons so entitled (in charge of processing and personnel specifically authorized by IT Telecom s.r.l.), while operations on the data and the systems would be adequately tracked through a special 'access & audit logging' system.

This brings the company – as an accredited Certification Authority, under the strict supervision of the Agenzia per l'Italia Digitale, also regarding aspects related to the management of data security and systems – to affirm that the information stored for biometric signature verification would not be, in the light of organisational and management measures adopted, 'usable directly [...] in other contexts with effects on the parties concerned.'

In addition, the biometric data related to users, in the event of cessation of use, would be erased or made irreversibly anonymous 'immediately or as soon as

[1] This text is not actually in the original document, but is added to provide a better explanation.

[2] This template is calculated on the spot, at the authentication signature application. In other words, when one signer applies his signature on the tablet, this signature template is calculated. Since no two identical handwritten signatures exist, similarly there must be no identical 'on the spot' templates. If this event occurs, it means that some rogue managed to capture one template and is trying to masquerade as the authentic signatory.

technically possible and in any case no later than 30 calendar days from the recording of the event.'

2.4. The system, as a whole, will not only significantly reduce the risk of any attempts of identity theft,[3] but would, in the future, guarantee the 'dematerialisation of processes managed with paperwork' for the transactions to be carried out directly at the bank branch. In addition, the service meets the need to ensure to the parties concerned – in compliance with the constraints imposed by the legislation on digital signatures – the 'exclusive control of their private signature keys for the legal validity of signed documents and their verification'.

3. The document of Cariparma S.p.A.

Taking advantage of the system under consideration, Cariparma S.p.A., as well as Friuladria S.p.A. and Carispezia S.p.A., believe they can make significant improvements to its organisational and management processes, especially in terms of 'efficiency' (simplification and streamlining of operations at the counter; improvement of the quality of the services provided), 'security' (reliable identification of users, fraud prevention and detection) and 'economy of resources' (dematerialisation of forms, reducing the costs of storage of documents; respect for the environment); all this, without significantly altering the habits of users and at the same time relieving them of the burden of using additional tools (smart cards, tokens, etc.) for the use of the relevant 'private key', by subsidizing, this way, the subscription of digitally signed documents.

As part of this overall service, the processing of biometric data would respond primarily to the need to adequately verify the identity of users who have provided their consent for this purpose; this, not only because of the increasing number of fraud cases reported, but also in terms of compliance with the specific obligations imposed on individual banks under the legislation on money laundering.

However, should these users not be able to or not intend to adopt the biometric authentication service, an 'alternative' mode has been identified that involves the use of the cellular telephone as a device for the identification of the person concerned, in particular by sending IT Telecom s.r.l. the specific signature PIN issued to it by the same certification authority in the light of activating the procedure of signing the document with a digital signature. Nevertheless, this last mode should be considered, according to the bank, as 'exceptional', because it is aimed at a 'management of activities at the counter different from that linked to the use of the [remote digital signature]', which would fail to meet fully the purposes outlined above.

The activation of the service, in any case, would take place only after the release to interested parties of the relevant information and the acquisition of their consent to the processing of their biometric data by the respective controllers. Finally, in order to ensure high security standards with regard to users' data, the banks have said that operators for the identification and supervision of the operations of biometric authentication – identified as an 'appointee' pursuant to art. 30 of the Code – will treat the concerned personal data only after passing a specific authentication procedure.

4. Subsequent communications from the company.

With the subsequent communications of 20 and 27 November and 21 December 2012, the applicant companies have provided some information in order to process biometric data in the application for preliminary verification, providing, also, to better illustrate the architecture chosen for the contractual provision and the use of the service in view of a more precise detection, with respect to the processing of biometric data of the interested parties, the actual decision-making powers in the hands of each of the parties involved.

As refers the first profile, while reaffirming the distinction between the process of strong authentication and the signing of documents with a digital signature (a circumstance, which was confirmed by all parties), IT Telecom s.r.l. then stated, for its part, that the service takes into account the 'modifiability in the time of the handwritten signature' (through the functions of 'self-learning' that would allow a constant 'update of the specimen [on the] basis [of] rules [operating on] temporal elements, numerical and statistical data'), while the banks have confirmed, as pertaining to them, they want to make use of the same service, amongst other things, for the purpose of a 'customer due diligence required by law anti-money laundering.' Moreover, with specific reference to the degree of reliability of the system – already pre-set in order to guarantee a reduced number of possible 'false positives' and 'false negatives': called the 'degree of tolerance of the

[3] That is, misappropriation of identity.

system' – it was made clear that this risk should be considered further reduced in view of the organisational mode chosen for the same service, which provide for the recognition of the customer by the bank officer in charge of visual identification at the individual bank.

In the context, furthermore, of the complex scheme envisaged by the parties for the provision and use of the service – which provides for the conclusion of a contract between banks and Telecom Italia S.p.A. (in its capacity as provider of 'certification authority services' subcontracted to IT Telecom s.r.l.) and a separate contract between the same certification authority and signatory ('users' of the service), and the same banks ('end users') –, the companies believe, within their respective competences, to be autonomous controllers of the treatment of the data. In particular, IT Telecom s.r.l. understands that it is the controller of the treatment of personal and biometric data of the signatories for the purpose of activation, delivery, management, administration and maintenance of the service through their information systems, while Cariparma S.p.A. and other banks would be independent controllers of their respective treatments 'for the purposes of only operations of identification, activation and subsequent use of the service', limited to the portion of interfacing with their own information platforms. This is due in particular to the fact that the companies would operate 'independently in their respective areas of competence' (to be considered 'clearly distinct from the operational and organizational viewpoint') and that the banks, however, have a limited decision-making power in relation to how to perform the entire service to be rendered, through IT Telecom s.r.l., in strict accordance with local regulations concerning digital signatures.

By contrast, no processing of biometric data would be carried out by Telecom Italia S.p.A. with reference to the data of the signatories, the latter acting as a mere distributor of services provided by IT Telecom s.r.l.

In order to support the systems and procedures referred to, the companies have produced documentation related, among other things, to the draft agreement between Telecom Italia S.p.A. and purchasing banks, as well as a copy of the General Terms and Conditions relating to the service itself.

5. Authority Assessments.

5.1. The preliminary application submitted to the Authority relates to the processing of biometric data for authentication purposes related to the use of a system suitable to analyse and compare a number of parameters derived from affixing on a specific device, by interested parties, their handwritten signature on the occasion of the procedures of digitally signing documents. This measure, which takes into account the content of the instance formulated and the statements made by the parties (pursuant to art. 168 of the Code) in order to assess the difference between the digital signature procedure and the authentication one, focuses only on profiles related to the processing of biometric personal data connected to the latter.

It should first be noted in this regard that the Working Party on the protection of personal data under art. 29 of Directive 95/46/EC considers that systems based on the use of devices that can detect the 'dynamic' features of a signature come within the meaning of the treatment of behavioural biometrics data, and as such fall within 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, in this perspective, if the system under the scrutiny of the Authority can be deemed as compliant, limited to profiles regarding the processing of biometric data of users in the authentication phase, with the discipline of the Code, with particular reference to both the correct identification of the role played by each of the companies involved in the procedure of authentication, and the observance of 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 by the banks, as in the present case, only for purposes of completion of the enrolment phase and is subsequently used (in the form of numerical code), by the certification authority, for the operations in comparison authentication procedures (in argument, 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).

5.2. Compared to the first profile, it is, first of all, to emphasize that the complex architecture of the contract chosen by the parties for the provision and regulation of the entire service (including, as mentioned, the biometric data processing for authentication purposes) does not help, by itself, to

the framing of the case in terms of the identification of responsibility with regard to the processing of biometric data of users. Nevertheless, it seems to this Authority, that the statements made and documents submitted, as a matter of fact not always uniquely matching, have highlighted elements such as to make believe in any case that the present case, contrary to the claims of the applicant companies, is more properly due under of a co-ownership of the same (and only) treatment (article 4, paragraph 1, lett. f) of the Code); this, both because of what follows with reference to each of the parties involved, and in the light of the views expressed by the aforementioned group for the protection of personal data, according to which 'it is in the presence of a situation of shared responsibility when various parties determine, for specific treatments, or the purpose or the fundamental aspects of the tools [...]. In the context of shared responsibility, however, the participation of the parties to the joint determination can take many forms and does not necessarily have to be split equally', could the various holders' 'care – and answer – for the processing of personal data at different stages and different degrees' (as Opinion 1/2010 on the concepts of the controller and processor, WP 169, adopted 16 February 2010, p. 19, and some pronunciations in this context, see Provv. Garante 3 December 2009, doc. web n. 1692917; Provv. 30 May 2007, doc. web n. 1412610; Provv. 13 September 2012, doc. web n. 1927456).

Granted, in fact, that the biometric authentication service, made through the use of 'integrated' information platforms of individual banks and IT Telecom s.r.l., also and especially responds to the need – typical both to credit and financial services operators, and to the same certification authority – to 'identify' in a rigorous and unambiguous way the signatories (the first in respect of the obligations imposed by law on money laundering, the second of those provided by the regulations on digital signature) – it must be pointed out, with regard to the actors involved in various capacities in the procedure, that the statements made by the parties and the documents submitted (whose authenticity can be held accountable in criminal proceedings under the aforementioned article. 168 of the Code), it appears that:

- Telecom Italy S.p.A.: assumes no actual role in the activation and execution of the authentication procedure, nor does it deal, in practice, with biometric data relating to the parties concerned. This, regardless of its reported role of 'principal contractor' (see footnote IT Telecom 21 December 2012, p. 2), and also deduced from the accompanying draft 'agreement for the provision of services related to underwriting and retention of documents computer';

- Banks:

• determine the purpose of treatment (made known to the supplier and formalized through the aforesaid draft agreement), requiring specifically, through the signing of a special agreement, the use of the overall service of the digital signature with biometric authentication specifically provided by IT Telecom s.r.l.;

• determine the mode of execution of the treatment, limited to the operations of collecting biometric data of the interested parties (see note IT Telecom s.r.l. dated 21 December 2012, p. 3);

• claim powers of inspection and verification, exercisable at their sole discretion, with regard to the 'services' provided by the certification authority (see articles. 5, letter M) n) o) p), and 11 of the draft agreement);

• establish alternative ways of recognizing users in the event of failure to adhere to the procedure of biometric authentication (see 'Notes to the presentation,' attached to the note Cariparma S.p.A. dated 27 November 2012, p. 6);

• identify and take any further action with respect to its information infrastructure (see footnote IT Telecom s.r.l. dated 21 December 2012, p. 4);

- IT Telecom s.r.l.:

• determines the purpose of treatment, measuring it against the management of the overall digital signature service offered to the applicant banks (see note IT Telecom dated 21 December 2012, p. 2);

• determines the mode of execution of the treatment, defining the technical and organizational standards of the authentication procedure, also abiding by the related provisions of the specific sector (including Legislative Decree no. 82/2005, regarding the 'Digital Administration Code');

• identify the individuals to which possibly give the task in relation to the operations of identification and registration of data of the signatories, giving them the relevant instructions (see also art. 16 of the draft contract of 7 November 2012);

• applies, on how to deliver the service, any changes requested by the technological and regulatory evolution (see article. 3, letter. e) of the draft contract of 7 November 2012);

• adopt, as part of the overall service of digital signature (to which the processing of biometric data is appointed in advance) all necessary measures of its organization (also preparing the forms containing the terms and conditions of service usage), including security measures in accordance with the provisions of the Code (see Art. 14 of the draft contract of 7 November 2012).

In light of these overall elements, it therefore seems difficult, in this case, to recognize two distinct treatments of biometric data by the individual banks and IT Telecom s.r.l. (which, however, if considered individually, would be self-contained), having rather to be considered, also with a view to facilitating the exercise of the rights under art. 7 of the Code by those concerned, that the actors involved, although operating 'in sequence', are performing different operations of a single treatment aiming to provide for the authentication of the person concerned, using, for this purpose, tools established jointly (and operating in an 'integrated' manner) and answering, on the same treatment, only for their portion of range (in this context, see the opinion already mentioned of the Article 29 Group, p. 21).

5.3. With regard to compliance with the principles established by the Code, it is pointed out that the processing of biometric data that the companies intend to carry out, based on the documentation provided and the statements made, is lawful. It must in fact be noted, in general terms, that the secure and rigorous identification of users, already required from banks with a view to a sound and prudent risk management (see Basel Committee on Banking Supervision), is, often, also an obligation on the part of all the lenders to specific sector regulations (see, for example, Legislative Decree n. 231/2007, also Guarantor's Opinion of 25 July 2007, web n. 1189435), more in general, on the obligations regarding customer identification, cf. Provv. 27 October 2005, doc. web n. 1189435 and Provv. 25 October 2007, bearing the title 'Guidelines for processing data related to the bank-customer relationship' 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 the same way as art. 1176, 2nd paragraph, cc (with possible relevance, therefore, also of negligence: in this sense, Trib. Ariano Irpino 2 October 2008, Cass. 30 January 2006, no. 1865). To this, it is to be added that the biometric authentication of users with a view to signing digital documents could, on the one hand, help to deal effectively with the growing number of fraud cases declared by the banks and, on the other hand, streamline and speed up (and also benefit the user) the identification operations at the counter. It should then be noted, again, that the treatment in question, in so far as actually to be regarded as compatible with the current regulatory framework applicable to digital signature services provided by IT Telecom s.r.l. (in this sense, however, a first opening to the usability of biometric techniques, albeit within the wider context for the services of 'electronic signature', it seems apparent already in the 'Guide to the Digital Signature' prepared by the then CNIPA , version 1.3, April 2009, p. 11; in perspective, see the 'Scheme d.P.C.M. under articles 20, paragraph 3, 24, paragraph 4, 28, paragraph 3, 32, paragraph 3, letter b), 35, paragraph 2, 36, paragraph 2, and 71 of d. l.gvo 7 March 2005, n. 82', available at www.digitpa.gov.it) may be functional, albeit indirectly, to ensure compliance in practice with the stringent requirements for the recognition of the interested parties that the specific sector legislation (Legislative Decree n. 82/2005, cit.; d.P.C.M. 30 March 2009) imposes on the same certification authorities for the purposes of providing the service. Considering, finally, that the processing of biometric data of the signatories, except as specified in following paragraph 6, will be based on the informed consent of the persons concerned and for the pursuit of legitimate goals made known 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 of art. 11, paragraph 1, lett. a) and b) of the Code. With regard, then, to the observance of the principles of necessity and proportionality (articles 3 and11, paragraph 1, lett. D) of the Code), it is to be stressed that the system described, in the indicated configuration mode, allows the treatment of biometric data of the interested parties in the form 'separated' from the relevant registry data (stored in a special database, however, distinct from the one that contains the specimen), so as to enable them to be identified only indirectly. In addition, the biometric information acquired by the system appear to be only those necessary for the creation of the template and

to the subsequent comparison during authentication of the signing parties.

Even in terms of the processed data security, it can be assumed that the immediate encryption information at individual banks and their transmission to IT Telecom s.r.l. through the 'https' channels is considered reliable, as well as the appropriate configuration of the firewall access rules provided at the data centre of the certification authority (see document IT Telecom s.r.l. attached to the notice dated 27 April 2012, p. 17) constitute measures appropriate under articles 31 and subsequent ones of the Code. Given, then, that the companies have also declared their intention to adopt organizational solutions (physical separation of servers, location of the same in premises adequately protected and accessible only by authorized personnel; tracking of transactions and data access systems, etc.), such that, as of today's knowledge, to lead it to believe the risk of any improper operations on the biometric data of the interested parties as remote, it can conclusively be said that the treatment, as proposed, complies, also with regard to the aspects concerning the safety measures, to the discipline of the Code.

So, on the further assumption that the same certification authority – already required to operate according to the strict standards set by current legislation (Legislative Decree no. 82/2005, cit.; d.P.C.M. dated 30 March 2009) – is also subject to stringent supervision of the Agenzia per l'Italia Digitale.

Finally, by virtue of the provisions of art. 11, paragraph 1, lett. c) of the Code, it appears as being in line with the provisions of law in force for the adoption of mechanisms of self-learning suitable to ensure, over time, the 'quality' of biometric data processed.

6. Additional requirements.

As anticipated (see section 2.1), these companies shall make the required disclosure available to interested parties throughout the process of joining the service. However, in the models acquired the characteristics of the treatment relative to the biometric data of the persons concerned appear as not duly highlighted. The companies shall therefore amend and/or supplement the information made available to the signatories related to this specific treatment, making available to them all the elements of art. 13 of the Code and focusing in particular on the type of data collected and the information that can be derived from them, on the profile of co-ownership (article 13, paragraph 1, lett. F) of the Code) and the objectives pursued separately by each co-owner within the biometric authentication procedure (article 13, paragraph 1, lett. a) of the Code).

In addition, subject to any applicable specific regulations and the need for further conservation resulting from any disputes, also in legal proceedings, the biometric data of the interested parties shall be retained by the parties for the period of time strictly necessary to achieve the purposes for which they have been collected and further processed (article 11, paragraph 1, lett. e) of the Code) and deleted immediately after, or as soon as technically possible for this purpose and in any event no later than the indicated period of 30 days.

Finally, the company must take care, before the start of treatment, of modifying the existing notification made in accordance with articles 37 and following of the Code.

It is understood, of course, that the processing of biometric data of the persons concerned can be considered legitimate, in this case, only if their consent is actually freely acquired in a correct form (article 23 of the Code), and cannot be considered as such if it is collected as a result of any pressures or influences also on the occasion of adhesion to the service (in this regard, cf., most recently, Provv. 4 October 2012, doc. web n. 2059743). In this sense, it is crucial that the individual concerned is actually provided with the actual freedom of choice as to the possibility of using or not using the procedure of biometric authentication, as well as the related possibility, by each bank, however, to ensure the use of the subscription service of digitally signed documents through alternative modes of authentication.

NOW, THEREFORE, the guarantor,

pursuant to art. 17 of the Code, at the conclusion of the preliminary verification request by Cassa di Risparmio di Parma e Piacenza S.p.A., Banca Popolare Friuladria S.p.A., Cassa di Risparmio della Spezia S.p.A. and IT Telecom s.r.l., for use within the service preordained to subscribe documents with digital signature, 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 in the terms

set out in the narrative and in due respect of what stated by the companies that apply pursuant to art. 168 of the Code, and subject to the companies following actions:

1. Duly amend and/or supplement the information to be provided to the parties concerned, indicating in detail all the elements of art. 13 of the Code and focusing in particular on the profiles related to the type of data collected and the information that can be derived from them, including joint ownership and the purpose of the treatment;

2. Acquire a truly free consent by the parties concerned, in compliance with art. 23 of the Code;

3. Preserve the biometric data of the interested parties, subject to any applicable specific regulations and requirements for extended preservation deriving from any disputes arising from judicial office, also for the time strictly necessary to fulfil the purposes for which they were collected and further processed (article 11, paragraph 1, lett. e) of the Code), also ensuring their immediate deletion, or in the time technically required for this purpose and in any event no later than the indicated period of 30 days;

4. Modify, prior to the beginning of the treatment itself, the notifications already carried out in accordance with articles 37 and following of the Code.

Under articles 152 of the Code and 10 of the legislative decree n. 150/2011, the present provision may be opposed against at the ordinary courts, by application lodged at the ordinary court of the place of residence of the owner of the data treatment, 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.