diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 25/07/2012

All'indirizzo http://www.diritto.it/docs/33797-biometric-signatures-and-the-eu-data-protection-commissioners-opinion-on-biometric-data

Autori: Marcoccio Gloria , Manca Giovanni

Biometric signatures and the EU Data Protection Commissioners Opinion on biometric data

Biometric signatures and the EU Data Protection Commissioners Opinion on biometric data

July 2012

Giovanni Manca, Gloria Marcoccio

The Working Party 29 (WP 29), assembly of the EU Data Protection Commissioners (DPA) under article 29 of privacy directive 95/46/EC, issued in April 2012 the Opinion 3/2012 concerning new developments of biometric techniques and related aspects for the compliance with the UE data protection and privacy law.[1] In 2003 the WP 29 already issued a first "working paper" concerning biometrics and the critical privacy and data protection issues arising from the processing of such data and the possible areas of intervention in terms of countermeasures. The present Opinion updates the framework previously examined in 2003 by identification of specific biometric data processing sectors, guidelines and recommendations to the industry in question, to users of these technologies, and to European and national authorities responsible for relevant legislation. It is well evident in the Opinion the attention of the WP 29 at European level toward the new EU privacy regulations currently under discussion (officially launched January 25, 2012, in which biometric data are explicitly referenced) and, at national level, something more than an invitation to single EU DPAs in preparing provisions concerning measures and precautions in line with those reported in the Opinion itself.

Among the various contexts of use and technologies reported in the Opinion, there is also an explicit reference to the so-called biometric signature (see paragraph 4.4.6), i.e. the solutions and the procedures that allow the signature of an electronic document, based on detection of certain biometric characteristics of the person who signs. Technological solutions and commercial proposals concerning biometric signature are becoming available on the Italian marketplace and it is understandable that there is room for their success: in fact the experience of signing an electronic document "by hand", is clearly appreciated by anyone, provided that the technical/organizational solution as a whole offers acceptable guarantees of reliability and security. In this regard, the interest in biometric signature is certainly going to increase especially considering its use as an "advanced electronic signature" to which the regulatory updates brought by Legislative Decree 235/2010[2] on electronic signature recognize, with respect to the past, an higher legal value. Indeed, the "advanced electronic signature" as defined in paragraph q-bis of paragraph 1 of article. 1 of Legislative Decree 82/2005 (Digital Administration Code):

"data in electronic form which are attached to or logically associated with other electronic data and which is capable of identifying the signatory and ensure it is uniquely linked to the signatory, it is created using means that the signatory can maintain under his sole control and it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable"

has the legal value identified in para.2 of article 21 of the Legislative Decree 82/2005:

"The electronic data [electronic document] signed with electronic signature, advanced, qualified or digital, prepared in accordance with the technical rules set out in article 20 paragraph 3 ensuring the identifiability of the author, the integrity and the immutability of the electronic document, has the effectiveness provided by article 2702 of the Civil Code. The use of the signature device is assumed due to the signatory, unless he/she proves otherwise. "

Considering security and reliability of advanced electronic signature (AES), the technical rules laid down in paragraph 3 of article 20 of Legislative Decree 235/2010 define terms and limits to be respected, from the organizational, technical and procedural point of view. These rules will be published in the Official Journal (it

1 "Opinion 3/2012 on developments in biometric technologies
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

2 Legislative Decree no. 235 December 30, 2010: Changes and integrations to Legislative Decree 7 March 2005, n. 82 "the Digital Administration Code", under Article 33 of Law no. 69 18 June 2009 - OJ No. 6 of 10.01.2011 – Ordinary Supplement. No 8

should be soon), in the meantime the corresponding scheme, notified in Brussels following the usual European procedures, is available at:

http://ec.europa.eu/enterprise/tris/pisa/app/search/index.cfm?fuseaction=recent&lang=IT

Moreover, it was returned by the competent EU offices without any changes, then the notified text can be considered as the definitive one.

This text has been the subject of many comments, available in internet and in specialized magazines[3] , and from them is worth to report that the provisions concerning AES are substantial, clearly with the aim to lay down appropriate precautions, with technical and organizational measures commensurate to its new and higher legal value.

In terms of Italian law on personal data protection, the technology solutions and processes for using the biometric signature regardless of their implementation as AES, find their reference regulation in the Privacy Code - Legislative Decree no.196/03 (and applicable authorizations and decisions issued by the Italian DPA). In summary ...

> In terms of compliance should be noted the prior notification to the DPA (letter "a" paragraph 1 Article 37 of Privacy Code) and, taking into account the "*specific risks to data subjects' fundamental rights and freedoms and dignity on account of the nature of the data, the arrangements applying to the processing or the effects the latter may produce* ", the DPA Prior Checking under Article 17 of Privacy Code.
>
> Towards the data subjects (individuals to which biometric data relate) is always necessary: Information (Article 13 Privacy Code) and Consent (Article 23 Privacy Code) unless the specific case falls within the exemptions provided in the Privacy Code, Article 24.
>
> Then it is always necessary to fulfill the provisions concerning the roles of "persons in charge of processing" and "data processors" (respectively Article 30 and 29 of the Privacy Code) and transfer of data abroad (Article 42-45 of the Privacy Code), as applicable.
>
> In terms of security measures, in all cases it must be provided for the minimum security measures (Articles 33-36 of the Privacy Code and its Annex B), the measures and precautions provided by the DPA Order concerning the role of System Administrator (treatments are carried out by "electronic means") and measures arising from risk analysis (Article 31 et seq of the Privacy Code).
>
> As for the general requirements regarding biometric data, already issued by the Italian DPA, it is worth mentioning the requirement laid down in "Guidelines for the treatment of private employee data - 23 November 2006" (OJ no 285, 7 December 2006), concerning 'biometrics data and access to "restricted areas" '(paragraph 4 of Annex 1 to the Guidelines).

Organizations that want implement and / or use biometric signature as advanced electronic signature must however observe the requirements:

- arising from privacy legislation (for aspects of processing biometric data)
- reported with the technical rules laid down in paragraph 3 of art. 20 of Legislative Decree 235/2010.

In this context, guidelines and recommendations of the WP 29 Opinion 3/2012, read from the biometric signature perspective and taken as a basis to support the requirements of technical rules contained in Legislative Decree no. 235/2010 for the AES, provide a framework of relevant value, to be kept in mind although the WP 29 opinions have no law efficacy.

PIA – Privacy Impact Assessment

The WP 29 emphasizes the need to follow a structured and systematic approach to identify risks and determine the measures necessary for the specific context of use: therefore not only purely technical measures, also those arising from the organizational/practical environment in which the signature solution

3 See "Commenti allo schema normativo relativo alla firma elettronica avanzata (FEA)" by G. Manca, published in Information Security no. 11, May 2012

will be used and relevant legal obligations. As just one example, a biometric signature solution adopted by a bank with its customers, has characteristics and regulatory issues and risk profiles different from the context of signature adopted within a company, for which users are employees, consultants and perhaps even suppliers of the company.

The approach reported is the so-called PIA - Privacy Impact Assessment. The WP 29 has already expressed in the past the need to adopt PIA methods in the field of RFID technology with specific working documents and opinions. Also the new privacy regulations under discussion at EU level specifically provide such an approach (named data protection assessment).

PIA input should consider several factors, including:

- the nature of the data to be collected
- the purpose of the collected information
- the accuracy of the systems intended to use, considering the value the biometric signatures shall have in their context of use (and legal value when used as AES)
- the legal basis and legal compliance, with regard to the legal provisions (Notification,…) and consent requirements
- access to the device where the biometric data are retained and the needs to share related information within the target organization, and consequently the necessary security measures to rule the access on a need to know basis
- the decisions regarding the retention time and procedures to achieve effective erasure when the data are no longer necessary for the purpose of the biometric signature

Moreover PIA should represent a natural and essential base to allow the fulfillment of the Accountability principle, therefore the ability to demonstrate the choices made and the countermeasures implemented for the purpose of compliance with the law in subject..

The main categories of risks highlighted by WP 29 deal with:

1. identity fraud (in the case of interest data fraud regarding biometric signature)
2. purpose divertion, i.e. use of biometric data for a purpose other than the purpose of their collection
3. data breach (which according to the severity of the violation could result in the obligation to provide notice to the parties concerned and / or to the relevant authority)

MEASURES AND PRECAUTIONS

In terms of measures and precautions the WP 29 Opinion emphasizes the importance of providing:

technical measures (considering the biometric signature context):

use of "biometric template", i.e. key information extracted and saved from the biometric data collected, processed in lieu of the input raw data. This precaution should be implemented as applicable, for example in case of biometric signature, the data collected (writing pressure sensing, speed and acceleration in writing,…) could be part of the specific biometric template

storage of biometric data on personal devices, if not really necessary make use of centralized data base, **providing for:**

- performing the required operations of encrypted data comparison/reading directly on the personal device in exclusive use to the data subject
- storing, on these devices, the minimum number of identification data of the person (to limit the risks of digital identity theft)
- always keep the data encrypted if it is actually necessary the storage of biometric data in centralized databases

renewability and revocability

- technical/organizational measures for securely renewing the data after a data breach or following technological evolutions
- measures to allow the data subjects the exercise of rights to revoke the connection

between their identities and the processed biometric data

encryption

- always keep the biometric data encrypted
- apply a strict "need to know" criterion in assigning decryption keys

antispoofing

- manufacturers should implement systems aiming to determine if the biometric data is both genuine and still connected to a natural person, for the purpose of reliability of the specific biometric system

Furthermore the WP 29 considers worthy of interest the use of biometric encryption technologies, i.e. the use of biometric data as a mean in the processes of data encryption/decryption.

automated mechanisms for data erasure

- erasing the data, at the expiration of the period within which it is necessary its retention, is considered one of the most important measures in processing biometric data, to reduce the risk of identity theft and data misuse

organizational measures:

procedures

- implement clear procedure on who can access the information on the system and provide for mechanisms able to track all the activities performed on the data concerned (therefore: to implement more than the access log as it is in Italy for the case of system administrators)

policy for providers control

- establish a detailed policy on how to control the providers, if and when involved in the service operation concerning biometric data processing, providing for appropriate inspections and control, and requiring guarantees on compliance measures for their employees and on the procedures to be triggered when a data subject exercises rights under the law, regarding the processing of his/her data

Many of the guidelines reported in the WP 29 Opinion are reflected in and support the forthcoming Italian technical requirements regarding the advanced electronic signature.
However, it is worth mentioning that a possible DPA general decision concerning the processing of biometric data, including biometric signature, should establish measures and arrangements able to facilitate the compliance with the AES, by the manufactures concerned and by whoever intends to provide AES services to its users.