GUIDELINES ON BIOMETRIC RECOGNITION AND GRAPHOMETRIC SIGNATURE

Annex A to the Garante's Order of 12 November 2014

VERSIONE ITALIANA

TABLE OF CONTENTS

1. FOREWORD

The use of technologies and devices to collect and process biometric data is increasingly widespread; this applies, in particular, to identification of individuals, access to digital services and/or information systems, the control on the access to buildings and areas, the operation of electro-mechanical locks and electronic devices, also for personal use, and machinery, and the undersigning of electronic documents.

This phenomenon was followed keenly by DPAs as shown by the papers and opinions drafted by the Article 29 Working Party (WP29) – which are key benchmarks for EU Member States' authorities.

At national level, this DPA has issued several decisions over the years following the applications filed by data controllers pursuant to Section 17 of the Personal Data Protection Code (legislative decree No. 196 of 30 June 2003, hereinafter the "Code"). In some cases it banned the processing subjected to the DPA's prior checking whilst in others it did allow it providing technical or organizational measures would be complied with.

Indeed, a biometric data is a personal data as it can always be considered to be "information relating to an identified or identifiable natural person" by having regard to "all the means likely reasonably to be used either by the controller or by any other person to identify the said person". Since biometric data fall under the scope of application of the Code (Section 4(1), letter b)), any operation performed on them by way of electronic tools is a personal data processing operation for all intents and purposes.

Given the current fast-pace technological evolution and the increasing availability and use of biometric devices, which are sometimes part of mainstream products, the Italian DPA is issuing these guidelines based on the experience gathered so far in order to provide a consolidated framework of measures and arrangements in technical, organizational and procedural terms. This is aimed ultimately at enhancing the security of biometric data processing and bringing it into line with the data protection legislation in force.

Processing performed by public and private entities for biometric recognition purposes or else to enable undersigning of IT documents will be addressed, whilst processing operations for public security, judicial and scientific research purposes will not be taken into consideration.

2. DEFINITIONS

There is currently no regulatory definition of "biometric data"; however, it is generally agreed that a biometric data is any data derived from "*biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability*."[1]

Nevertheless, in order to rely on harmonized wording in a highly technical context, we consider it necessary to use the definitions to be found in ISO/IEC 2832-37 ("Information Technology – Vocabulary – Part 37: Biometrics").

The main definitions are listed below:

[1] See Opinion 3/2012 on developments of biometric technologies (WP193 adopted on 27 April 2012) by the Article 29 Working Party, which is composed of representatives from EU Member States' DPAs.

- **Biometric characteristic**: biological or behavioural characteristic of an individual from which distinguishing, repeatable **biometric features** can be extracted for the purpose of **biometric recognition**;
- **Biometric recognition**: recognition of individuals based on their biological and behavioural characteristics, encompassing **biometric verification** and **biometric identification**;
- **Biometric verification**: comparison between a biometric template acquired when the subject interacts with the biometric system and a (supposedly) matching biometric template stored beforehand; this type of verification is termed **one-to-one comparison**;
- **Enrolment**: act of creating a record, here in a biometric system. The enrolment phase goes from biometric sample acquisition and storage to biometric feature extraction, up to the creation of the biometric reference to be stored for subsequent comparisons;
- **Biometric identification**: process of searching a database, by way of biometric comparison, against one or more biometric templates corresponding to the acquired data. This operation is also termed **one-to-many comparison** and does not envisage a biometric claim;
- **Biometric feature**: information extracted from a biometric sample and used for comparison;
- **Biometric sample**: analog or digital representation of a biometric characteristic, which is the output of the acquisition process (biometric capture and acquisition), for instance a record containing the image of a finger;
- **Biometric comparison**: comparison of biometric data to determine their similarities or dissimilarities, usually based on statistical methods and metrics that are typical of the selected technological environment and biometric system;
- **Biometric template**: a set of stored biometric features comparable directly to other biometric templates;
- **Biometric probe**:[2] biometric template generated whenever a data subject interacts with the biometric system;
- **Biometric reference**: biometric template used as a reference for comparison and stored in a permanent, non-modifiable manner subject to such updating as may become necessary because of changes, including physiological changes, in the biometric feature it is derived from.

For the sake of simplification, these guidelines will use the words "**biometric template**" to also refer to **biometric references** or **biometric probes**; conversely, "biometric data" will be used to refer inclusively to samples, templates, references, features and any other data that can be derived via automated processing from the data subjects' biometric characteristics.

3. MAIN BIOMETRIC CHARACTERISTICS AND CORRESPONDING PROPERTIES

Some properties of biometric characteristics, data and techniques lend themselves to introducing general categories that are described below insofar as they are instrumental to assessing personal data protection aspects.

Passive vs. Interactive Biometric Systems

Biometric systems are termed interactive or participative if they envisage the data subject's participation and require him or her to cooperate in the biometric data acquisition phase – e.g. as regards retinal scanning or placing one's handwritten signature. Conversely, passive systems collect biometric data without the data subject's perceiving or being aware of it – e.g. as regards facial image acquisition or voice recordings obtained without this being noticed by the data subject.

[2] From a technical and IT science standpoint, a biometric reference and a biometric probe may be one and the same thing; their only difference consists in the timing of their use and the fact that biometric references are acquired and stored permanently whilst biometric probes are generated whenever the data subject interacts with the biometric system. Accordingly, biometric probes may differ slightly depending on acquisition circumstances.

Biological and Behavioural Biometric Characteristics

Another applicable distinction is the one between biological characteristics, which are related to an individual's physical, bio-chemical, morphological or physiological features, and behavioural characteristics as related to actions and stances taken by an individual – e.g. signature placement dynamics, gait or even, under certain respects, a person's voice pattern.

Traceless and Non-Traceless Biometric Characteristics

Some biometric characteristics leave traces compared to others (called traceless) that do not. A non-traceless biometric characteristic is the fingerprint, as it may be left on objects; the same applies to one's facial contour, which may be collected unbeknownst to the data subject. Examples of traceless biometric characteristics include hand contour and finger vein pattern.

Other Properties

Biometric characteristics share, albeit to a different extent, uniqueness and universality features - i.e., they are distinctive of each individual and are present in each individual; generally speaking, they are stable over time. However, they are liable to degradation because of natural causes, accidental alterations and/or injuries, which may affect the operation of biometric systems.

The main characteristics used by biometric systems are described in the paragraphs below. For each of them, the mode of collection (passive or interactive), non-traceless features, liability to yield sensitive information and stability over time are highlighted.

3.1. Fingerprints

Biometric processing of fingerprints entails the collection, via optic acquisition devices, of a biometric sample reproducing the location of the Galton ridges and skin valleys that can be found on fingertips since the prenatal phase.

The *minutiae,* i.e. the biometric features, of a fingerprint include whorls, bifurcations, ridges, valleys and endings; their identification in the acquired biometric sample allows deriving a biometric template that can provide a summary digital representation of the source fingerprint such as to lend itself to developing effective comparison algorithms.

Uniqueness of the template in a biometric database cannot be ensured, because the same template may correspond to several fingerprints – especially in large databases; nevertheless, a summary representation of the biometric characteristic allows performing automated searches very effectively, in that the biometric template works as the key to search matches in a database.

This is actually the rationale underlying today's automatic fingerprint identification systems (AFIS) as used globally, in particular by law enforcement and investigation agencies.

Fingerprints are non-traceless, therefore they may, under certain circumstances, disclose information on a data subject's sensitive data; indeed, research has shown that fingerprints allow determining ethnicity of an individual. In principle, fingerprints are stable in adults and possess substantial uniqueness in a population as they differ even in homozygous twins. The latter property has actually resulted into their being often used for judicial and police purposes.

Fingerprints are usually collected in a biometric system with the data subject's active participation; however, one can collect the fingerprints left by an individual on any object and use them in a biometric system – at least theoretically.

3.2. Handwritten Signature Placement Dynamics

The dynamic features of one's handwritten signature fall under the scope of behavioral biometric features; they can be acquired via ad-hoc tablets (so-called graphometric tablets) or via standard tablets that are equipped with appropriate software and sensors. These acquisition devices can process not only stroke, but also several dynamic parameters that are associated with the placing of one's signature – writing speed, acceleration, pressure, slant, number of pen ups/downs, etc. .

Acquisition of signature dynamics may be instrumental to biometric recognition, although it is fraught with a high false-negative rate (i.e. wrong failed recognition results) which may make the procedure poorly effective and accurate outside specific contexts where human intervention can make up for inevitable recognition failures. Conversely, this procedure is used most often in the form of the so-called graphometric signature.

This behavioral characteristic is traceless and poorly stable in time.

The data subject's active participation is required for acquisition.

3.3. Voice Emission

Evolution of signal processing hardware and software allows analyzing voice emissions in a sufficiently effective manner to enable biometric recognition (speaker recognition) either via conventional phone interactions or via the Internet; this can also be done locally by interacting with a device connected to or integrated with a PC or any other IT tool.

Voice emission features are actually closely related to vocal tract anatomy and length, resonance, mouth and nasal cavity morphology.

Recognition is usually achieved not only by processing and analyzing voice signals (signal processing), but also via challenge procedures that differ depending on how an individual is prompted to repeat sentences, names or figures.

Recognition can also be achieved without challenge, e.g. if an individual is prompted to speak without any pre-defined pattern.

Usually, biometric recognition occurs in the form of a one-to-one comparison and the user is expected to provide additional information that he/she already holds (ID code, user ID, etc.) or is associated with him/her (calling line ID).

The voice signal is processed so as to create and store a biometric template and is used thereafter for comparison with the template acquired in the enrolment phase, which corresponds to the additional information provided by the user.

This biometric characteristic is non-traceless and may be collected without the individual's active participation as well as without using ad-hoc sensors – indeed, a standard microphone, even one installed on a telephone, can often be enough.

3.4. Hand or Finger Vein Pattern

The vein network of fingers and hands develops in the pre-natal phase.

This information is acquired via sensors detecting shape and pattern of the finger veins and/or the palmar or dorsal veins of the hand through a near-infrared wavelength light.

Compared to other systems, there is no need for the person's body to come into contact with the sensor and this procedure is accordingly better received by users. However, manufacturers of biometric systems do not especially favour the use of this biometric characteristic.

Biometric systems using this characteristic are highly accurate, usually more than fingerprint-based ones; they lend themselves to both biometric identification and biometric verification.

This biometric characteristic is traceless, does not disclose sensitive information, and is highly stable in time.

Acquisition requires the data subjects' active participation.

3.5. Retinal Vein Pattern

Biometric techniques based on retinal vein pattern acquisition use a low-intensity infrared light beam directed to the back of the eye. Such systems are prone to malfunctioning in the presence of eye diseases.

Retinal scans are usually relied upon when high-security requirements must be met; there is actually no known mechanism to duplicate one's retinal vein pattern, nor may one use tissue samples from deceased individuals because the sensors can detect blood circulation.

This biometric characteristic is traceless, highly distinctive, and highly stable in time.

Acquisition requires the data subject's active participation.

3.6. Iris Shape

This biometric technique consists in acquiring the shape of the eye's pupil and front via high-resolution imaging.

It is a highly accurate procedure enabling high-speed comparisons.

The false-positive rate is rather low compared to other biometric characteristics; however, a high false-negative rate has been reported such as to prevent recognition of an individual by the system.

This biometric characteristic is traceless, highly distinctive (since it differs even between one's eyes), and highly stable in time.

Acquisition may be performed without the data subject's active participation, although the most widely used sensors envisage active participation at the acquisition stage.

3.7. Hand Contour

Biometric techniques based on hand contour consist in acquiring the hand's bi- or tri-dimensional geometry via ad-hoc equipment that can detect specific features such as finger shape, width and length, knuckle location and shape, or palm shape.

The features of one's hand are not uniquely distinctive, so that they are not suitable for biometric identification in large population samples; however, they are sufficiently distinctive to enable effective biometric verification.

Sensors cost on average more than other biometric sensors and are relatively cumbersome to accommodate so that they can hardly be integrated into other devices and/or used in a mobile context.

This biometric characteristic is traceless, may provide information on a person's health (e.g. it may disclose degenerative or other diseases), and is not highly stable in time.

Acquisition requires the data subject's active participation.

3.8. Facial Features

Automatic recognition of individuals by means of facial features is a complex procedure based on visible light or "thermal" infrared light images.

Biometric comparisons are made harder by the presence of hair, glasses or the position taken by a person's head during acquisition as well as by lighting conditions.

Conversely, infrared-based techniques in this area are not affected by lighting and prove effective also in the dark.

Tri-dimensional images can also be produced by merging several images and/or via computer graphics techniques based on shadow effects.

The facial biometric sample is used to extract, via algorithms that are sometimes based on so-called neural networks, a given set of features such as the location of eyes, nose, nostrils, chin and ears in order to build up a biometric template.

If the procedure is implemented in a cooperative context, facial recognition can be highly accurate so much so that it can be used for physical or logical access controls.

Facial characteristics are non-traceless as they may be acquired automatically by – for instance – video surveillance systems; they may also disclose sensitive information. They are highly stable in time and can be acquired also without the data subject's active participation.

4. GENERAL PRINCIPLES AND LEGAL OBLIGATIONS

Biometric data must be processed in compliance with the Code and on condition no unjustified, disproportionate interference with data subjects is caused.

4.1. Lawfulness

In the first place, it should be verified that biometric data is processed by taking account of the lawfulness requirements laid down in the Code as related to the individual data controller. This is without prejudice to such additional legal requirements and orders by the Garante as may be applicable.

In the public sector, personal data may only be processed in order to fulfil institutional functions, by complying with the limitations laid down in the Code as related to the specific category of processed data, and in accordance with the applicable laws and regulations (see Section 18 et seq.). In such

cases, public bodies do not rely on the data subjects' consent unlike what is the case with private bodies and profit-seeking public bodies.

The latter must, as a rule, obtain the data subject's informed consent before starting the processing. Such consent may be withdrawn at any time and must be given freely and explicitly – i.e. without whatsoever pressure or influence. This is without prejudice to the other legal bases for the processing of personal data as set forth in Sections 23 and 24 of the Code. In particular, no consent is required if the Garante has carried out the so-called balancing of interests by way of a specific decision or order, whereby the data controller's legitimate interest has been considered to prevail. This applies to some cases where the Garante found that no prior checking application was necessary as per Section 17 of the Code – e.g. for the purpose of monitoring physical access to "sensitive" areas or checking identity prior to the use of dangerous equipment and devices; see, in this regard, the order adopted jointly with these Guidelines.

4.2. Necessity

IT systems and software must be configured so as to minimize the use of personal and identification data. Before using a biometric system, one should therefore assess whether the relevant purposes can also be achieved by way of anonymous data or else with the help of the biometric system albeit in such a manner as to only enable data subjects to be identified if necessary (see Section 3 in the Code).

Against this background, biometric systems must be designed (if this is technically feasible in the light of the purpose to be achieved) so as to immediately (and preferably automatically) erase the biometric data and the related information once the processing is terminated - except where it is provided otherwise with regard to specific cases or circumstances.

4.3. Purpose Specification and Limitation

Any data that is processed by way of biometric systems must be collected accurately and only processed for the purposes to be lawfully achieved by the data controller; those purposes must be disclosed beforehand in the information to be provided to data subjects. The data may not be used in other processing operations that are incompatible with the former (see Section 11(1), letters a) to c) and e), of the Code).

Pursuant to this principle, if the purpose to be achieved in a given case consists, for instance, in securing individuals or property, one might use biometric systems to monitor access by authorized staff to especially dangerous areas; conversely, the data might not be used for further purposes such as, for instance, in order to check employees' working hours.

Additionally, one might rely on biometric data to unambiguously identify bank customers during transactions, so as to prevent or reduce fraud; however, it must not be possible to derive additional information from such data in order to also check a customer's access to the bank.

4.4. Proportionality

Only such data as is relevant and non-excessive with regard to the purposes to be achieved may be processed (see Section 11(1), letter d), of the Code).

This means that the acquisition system must be configured in such a way as to collect a limited amount of information (minimization principle), which should not include any data that is unnecessary for the specific purposes. Thus, if the purpose is computerized authentication, biometric

data should not be processed in a manner that allows deriving sensitive information on the data subject.

One should refrain from resorting to systems that rely on multiple biometric characteristics except on account of reasoned, exceptional requirements.

4.5. Legal Obligations

Where the assessment performed on the basis of the foregoing principles yields a positive outcome, the data controller will have to fulfil the following obligations in pursuance of the Code.

4.5.1. Information Notice

The data controller must provide data subjects with suitable, specific information on the use of their biometric data before starting the processing of such data, i.e. before the enrolment phase (where envisaged). The information must include all the items mentioned in Section 13 of the Code with particular regard to the purposes sought and the processing mechanisms; reference should also be made, albeit summarily, to the precautions implemented, data storage periods, and data centralization, if any.

The notice should highlight, as appropriate, whether the data subject has discretion or is obliged to provide the data by having regard to the purposes of the processing. Where an alternative mechanism is envisaged or data subjects do not wish to or cannot rely on the biometric recognition system, perhaps on account of their physical characteristics, or if they decide at a later stage to no longer use such a system, the notice must also clarify that different arrangements may be resorted to in order to avail oneself of the service in whose connection the biometric procedure is being offered. If the biometric data is stored locally, i.e. on the device held exclusively by the data subject, the notice must provide the appropriate instructions on how to keep the device secure and explain what to do if it is lost, stolen or malfunctioning.

If the systems deployed at certain locations are potentially suitable for acquiring biometric data without the data subject's cooperation – which may be the case, for instance, with facial, voice or behavioural recognition systems – data subjects must be informed and afforded choice as to accessing any area that is subject to such biometrics-based controls. The information may be provided via ad-hoc signage placed close to the areas where biometrics acquisition is in place or data stations are located; alternatively, other mechanisms can be relied upon to ensure data subjects are informed before they interact with the biometric system – e.g. via a preplayed message in the case of phone-based voice recognition systems.

Similarly, if the biometrics-based processing is coupled with another system (e.g. a video surveillance one), the notice must highlight such a situation clearly and adequately – even if a simplified notice is used in the given circumstances.

4.5.2. Notification

The controller of biometric data processing is required to notify the Garante under Section 37(1)a) and Section 38 of the Code. Account should be taken of notification exemptions that apply to certain categories of controller because of the activities performed.[3]

[3] Reference is made here to the Decision on Notification Exemptions of 31 March 2004 (published in the Official Journal No. 81 of 6 April 2004 – web document No. 85261), the decision containing "Clarifications on Processing to Be Notified to the Garante" of 23 April 2004 (web document No. 993385), and the decision on "Notification of Processing in the Health Care Sector: Clarifications by the Garante" of 26 April 2004 (web document No. 996680).

4.5.3. Prior Checking

Under Section 17 of the Code, processing of data other than sensitive and judicial ones is allowed in accordance with such measures and precautions as are laid down to safeguard data subjects, if the processing is likely to present 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 measures and precautions in question may also be laid down with regard to "specific categories of data controller or processing".

By nature, a biometric data is directly and uniquely related to an individual and mirrors, in general, an inherently irreversible as well as universal relationship between body and identity; accordingly, special precautions must be in place when processing such data.

This means that the use of biometric systems falls under the scope of processing fraught with specific risks and requires a prior checking application to be lodged with the Garante under Section 17 of the Code before commencing the processing. The prior checking is meant to enable the Garante to order specific measures and arrangements whenever they prove necessary to appropriately use this sensitive type of information with a view to the envisaged processing.

When lodging the prior checking application, the controller will have to provide information on the risk assessment performed and the arrangements made to ensure compliance with the general requirements, legal obligations and security measures set out in paragraph 8 of these Guidelines.

More specifically, the following information will have to be included in the application:

- the type of biometric information to be processed;
- the context and the purposes aimed at via the biometric system to be deployed;
- the reasons why alternative systems posing smaller risks to data subjects' rights and fundamental freedoms are considered inappropriate vis-à-vis the purposes sought;
- the operational mechanisms of the system and the mechanisms for acquisition, use and storage of the biometric data along with the respective retention periods;
- whether the biometric data collected may disclose information on the data subjects' health;
- what benefits the use of biometric data may bring to data subjects and data controllers;
- the risks identified and the technical and organisational arrangements made to mitigate such risks;
- the mechanisms to obtain consent, if any, any alternative systems in place, and the text of the information notice.

Given the above premises, the Garante identified specific processing operations via a general application order that was adopted jointly with these Guidelines, whereby such processing operations were found not to require a prior checking application – providing the legal basis requirements set forth in the Code and these Guidelines were complied with and all the technical measures and arrangements described therein were also taken. The processing operations in question are listed below:

- IT authentication;
- Control of physical access by staff to "sensitive" areas and use of dangerous equipment or devices;

- Use of fingerprints or hand contour for purposes of facilitation;
- Undersigning IT documents.

5. USE OF BIOMETRIC TECHNIQUES

Biometric techniques are mostly used to achieve the **biometric recognition** of individuals.

Recognition may be based on **biometric verification** – i.e., the process whereby an individual claims an identity and the system compares the captured biometric template with the stored template corresponding to the claimed identity – or else on **biometric identification** – i.e., the process whereby the system compares the captured template with all the available templates in order to determine the individual's identity. The scope of application is mainly related to access control, whether logical (IT authentication) or physical.

Graphometric signature systems make up a category of their own; they are aimed at enabling IT documents to be undersigned and do not necessarily entail biometric recognition.

5.1. Biometric Recognition: Biometric Verification and Identification

In biometric processes aimed at the verification of an individual's identity, one compares a given biometric template associated with the identity claimed by the user (who may have entered a user ID or presented a badge to that end) to the biometric template that is generated at the time the recognition request is presented. This type of recognition is also termed "one-to-one comparison".

If the comparison yields a positive outcome, the identity is verified and the subsequent technical operation is enabled – e.g., a gate is opened in a physical access scenario, or access to an IT system is enabled in a logical access scenario.

If the biometric process is aimed at identification, the captured biometric template is compared to or used as an index for the database including the reference biometric templates (this is the so-called one-to-many comparison). In that case, the processing is unquestionably more complex as it depends on the size of the given database in terms of the amount of data it holds and the search and comparison algorithms relied upon.

5.2. Biometrics-Based Logical Access Controls

Biometric recognition techniques are sometimes used for security purposes on top of and/or instead of standard IT authentication systems based on information that is known to an individual (password, user ID) or held by that individual (e.g. on badges, tokens, etc.). This is also in line with Rule 2 of the Technical Specifications concerning minimum security measures (Annex B to the Code).

Standard authentication credentials based on the coupling of an identification code (username, login-name, etc.) and a password (to be kept confidential) may easily get lost, forgotten or stolen.

Token-based systems using different technologies (magnetic or optic cards, contact or contactless chips, etc.) as well as OTP (one-time-password) authentication devices used for the so-called strong (or two-factor) authentication provide unquestionably higher security compared to text-only credentials; nevertheless, they may be fraught with inconveniences as well if they get lost, are transferred unlawfully or stolen: these events may undermine the confidentiality of the

security information to be relied upon as part of their use (PIN, password, etc.) and ultimately result in a data breach.

Conversely, biometrics-based authentication is aimed at preventing the unlawful transfer or the theft of the credentials whilst enhancing the degree of certainty in identifying an individual who should be authorized to use IT systems.

5.3. Physical Access Controls

Biometric techniques can be used – more or less effectively depending on the specific process – in contexts other than the IT one, where some sort of interaction with technological equipment is envisaged. In particular, biometric systems are widely used to control physical access to restricted areas, operate gates or locks protecting specific premises, or handle specific equipment and devices.

Biometrics are mostly used for security purposes, to protect property or the integrity of individuals; however, biometrics may also lend themselves to "facilitative" applications such as regulating access to libraries, operating lockers in a gym or opening safe deposit boxes.

At all events, the biometric processes used for such applications fall under either biometric identification or biometric verification approaches.

5.4. Undersigning IT Documents

Biometric techniques based on measuring the dynamics of one's own handwritten signature (graphometric signature) can be used in undersigning IT documents also in order to enhance the soundness of legal transactions.

Unlike the scenarios described so far, the biometrics are not aimed at the recognition of an individual – although this type of implementation is possible and has actually been reported – since they are incorporated into IT documents in order to implement advanced electronic signature solutions in compliance with the applicable technical and regulatory requirements. In Italy, this type of signature was introduced by legislative decree No. 82 of 7 March 2005 ("Code of Digital Administration") and was subsequently regulated via the technical rules laid down in the order by the Prime Minister's Office dated 22 February 2013. More generally, this technique may be used to incorporate, into the IT document, information that is closely related to both the signatory party and the signed document so as to enable checking integrity and authenticity of such document regardless of the legal validity of the signature obtained in the manner described.

With graphometric signature techniques one obtains a set of biometric information that can be associated closely with a specific IT document via encryption techniques. This allows performing ex-post graphology tests by expert graphologists to establish whether the signature is genuine – similarly to what is the case with handwritten signatures on paper documents, e.g. if contractual disputes arise or the authenticity of one's signature is challenged.

Using graphometric signatures to undersign IT documents does not require, as a rule, a biometric database to be set up since the individual graphometric signatures are acquired and incorporated – after being suitably encrypted – into the undersigned IT document, which may then be stored in a file management system.

6. LIFE-CYCLE OF BIOMETRIC DATA

6.1. Biometric Capture and Acquisition

The processing of biometrics can be described as a sequence of processing operations, starting with the capture – via ad-hoc or standard sensors – of a specific biometric (biological and/or behavioural) characteristic relating to an individual so as to give rise to a biometric sample. The acquisition phase is considered to be concluded once the biometric sample is obtained. The process is summarized below:

Biometric Characteristic (e.g. face) → Biometric Acquisition Device (e.g. video camera) → Biometric Sample (e.g. facial image) → Biometric Features (e.g. specific facial points) → Biometric Template (mathematical representation)

Biometric sensors may be specialized or non-specialized. The former include fingerprint scanners, iris scanners, devices detecting hand contour or finger/hand/ocular vein patterns, and graphometric tablets to acquire the dynamics of handwritten signatures. The latter include video cameras or microphones to acquire facial images or voice recordings to be subsequently processed; tablet-like devices equipped with touch screens to implement the simplified software-based acquisition of signature dynamics without the help of specialized peripherals; webcams and microphones incorporated into mobile devices and/or laptops which can thus work as facial or vocal recognition sensors.

The biometric samples acquired by means of biometric sensors are variably sized files, depending on the biometric system and sensors. Thus, such data retain their close correlation, also analogically speaking, with the underlying biometric characteristic; they are the digital representation of that characteristic, rendered all the more truthfully in relation to accuracy and sophistication of the sensor(s) relied upon.

Any subsequent processing is carried out on the above biometric data and will depend, in turn, on the specific biometric technique and the purposes sought ultimately.

6.2. Enrolment and Creation of the Biometric Template

To enable biometric recognition one must acquire the biometric characteristic by way of a procedure ensuring that biometric enrolment is performed appropriately, that the link with the capture subject is retained, and that the quality of the resulting biometric sample is safeguarded.

Biometric data may be processed and stored not only in the form of a biometric sample, but also as a biometric template – i.e., in the form of a summary computerized description of the biometric characteristic, which is obtained by extracting only pre-defined relevant elements from the given biometric sample.

Distinctive features can actually be extracted from biometric samples – e.g. facial measurements can be extracted from an image – and then stored to be processed subsequently instead of the samples. Setting the size of the biometric template is of paramount importance: on the one hand, the size should be sufficiently large to ensure suitable accuracy in biometric recognition and prevent overlaps of biometric data and/or mistaken identities; on the other hand, it should not be excessive so as to prevent the risk of re-creating the biometric sample.

Generally speaking, the size and amount of identification features in a biometric sample should be in proportion to the scope and purposes of their use.

The biometric template extracted from the biometric sample must be kept for subsequent comparisons.

Any biometric capture procedure implemented with a view to biometric comparisons must be carried out according to the same safeguards as were in place during the initial enrolment; the templates to be compared should not be channeled on insecure networks nor should they ever be without encryption.

6.3. Biometric Recognition

Biometric identification systems require setting up centralized databases of biometric templates in order to establish a candidate's identity. The outcome of the comparison is positive (match) and thus allows identifying the candidate if the reference biometric template stored in the database corresponds to the biometric template derived from the characteristic presented.

With biometric verification it is conversely possible, in principle, to rely both on centralized and on decentralized storage. The former requires pooling all the reference biometric templates in a single database, whilst the latter envisages the storage of biometric references either directly on capture devices used for comparisons or on secure devices held by the data subject/candidate. One-to-one comparisons are by nature very quick as they do not entail any significant computational complexity even in the presence of sophisticated biometric techniques.

Certain smart cards allow biometric comparisons to be performed on the cards themselves, without any need for extracting biometric references; however, they are fraught with considerable limitations in terms of costs and performance because of their limited processing capabilities.

As a result of the different computational complexity involved, the "response time" of biometric identification systems may be considerably longer than that of biometric verification ones. This entails that the former procedure can actually be relied upon in high interaction rate scenarios if the biometric references database is not especially large. Thus, one should establish – if one can technically choose between biometric verification and identification – whether the ergonomic benefit of not requiring any identity claim is jeopardized by the longer time required for recognition, which may ultimately make the identification process ineffective and poorly suited for the specific purposes.

6.4. Biometric Data Retention

Biometric data may be held by the data controller and thus stored in a single centralized database (also in Hardware Security Module-HSM format), at the IT workstations or on biometric acquisition devices. The data are usually stored as biometric templates, although biometric samples are sometimes relied upon as well.

Alternatively, the biometric data may be stored in secure devices (tokens, smart cards) held directly and exclusively by the data subjects, so that the data controller is not required to store any biometric information (template on card). However, the data subject might be temporarily prevented from using the biometric system if the device is stolen, lost or destroyed.

The file systems of biometric smart cards and tokens should only be readable by authorized readers – at least for the biometric data partitions; the biometric data must be made unintelligible outside the respective usage context by way of cryptographic mechanisms.

7. RISK ASSESSMENT

The blanket use of biometrics may entail risks to data subjects because of the sensitive nature of the data to be processed, which may seriously affect their personal sphere in case of misuse.

The risk, whether intentional or accidental in nature, consists in the vulnerability of (a set of) technological assets such as to give rise to unlawful data processing and the danger of identity thefts affecting data subjects.

7.1. Social Control and Discriminatory Usage

Several biometric characteristics feature a high level of uniqueness in the population, which is why they lend themselves to being used as a sort of universal identifier. This entails the risk that, in future, mismanagement may allow private bodies and public entities to acquire or deduce information on individuals by matching and connecting data from several databases for purposes other than those for which such biometric data had been collected initially.

Non-cooperative, non-cognizant presentation biometric characteristics might be used to track an individual – for instance, to monitor that individual's movements by way of fully automated technologies which might be both ubiquitous and pervasive, causing the infringement of that individual's right to privacy.

Such uses would turn biometrics from a resource for security and/or facilitated access (by replacing cards, codes, passwords and signatures) into a tool for pervasive surveillance.

The suitability of certain biometric characteristics for disclosing sensitive information such as health, ethnicity or race makes discrimination an additional factual risk to be always taken into account.

7.2. Biometric Identity Theft

Biometric identity theft may be substantially detrimental to data subjects since no new biometric identity can be provided by relying on the same type of biometric data – unlike what is the case with conventional recognition systems.

Since biometric characteristics are, as a rule, non-modifiable and inextricably linked to an individual – though liable to degradation, to a variable extent, depending on age, the specific characteristic, and the data subject's life-style and activities – they make up a sort of non-revocable, non-replaceable authentication credential; if appropriated by unauthorised entities, they may enable fraudulent activities and undermine the effectiveness of biometric recognition-based security systems.

Non-traceless biometric characteristics such as fingerprints as well as non-cooperative presentation characteristics (e.g. voice recordings, facial recognition, iris scans performed via remote or hidden cameras) may entail the risk of unauthorised acquisition and theoretically enable identity thefts and fraud. However, such risks are only relevant if the procedure relied upon is based exclusively on biometric components; conversely, they play a marginal role if biometrics are used as part of a multi-factor system that envisages, for instance, the use of additional information such as passwords or similar codes or else the use of tokens.

7.3. Biometric Recognition Accuracy

Biometric recognition is usually a statistical rather than deterministic outcome; as such, it is liable to errors. Two of the main parameters to be considered in connection with a biometric system are the false rejection rate (FRR) and the false acceptance rate (FAR), respectively. This is why the performance of a biometric system should be assessed carefully in the light of the purposes sought: a high FAR enables the undue access of unauthorised users and may cause danger to individuals, property or information.

7.4. Biometric Data Forgery

Extracting biometric templates always entails a loss of information compared to what is contained in the sample.

Whenever technically possible, creation of the template should be based on a non-reversible process – that is, it should not be possible to re-create the biometric sample from the template so as to achieve the unauthorised "reconstruction" of the given biometric characteristic.

The most widely debated case concerns fingerprints. Theoretically one might generate a biometric sample from a template, via specific algorithms, and such sample might be processed by way of the same minutiae extraction procedure to generate a biometric template that is quite similar to the initial one. However, those biometric samples, when subjected to an expert's assessment, may be detected as "fakes" because of their poor anatomical closeness to real samples; furthermore, the biometric templates obtained from those samples do not correspond fully to the initial one, as they often include distortions or alien features.

Thus, the risk of obtaining a more or less faithful reconstruction of the initial biometric sample or – even less so – of the underlying biometric characteristic by way of the corresponding biometric template does not appear to be substantiated.

Recently it was shown that "artificial" high-quality fingerprint samples could be obtained to then produce biometric templates that corresponded fully to the initial biometric reference by using a minutiae extraction procedure and generating the corresponding biometric template via standard biometric system algorithms. The template produced in this manner would yield a positive match if used for a biometric comparison.

The demonstration that it is feasible to obtain a biometric sample corresponding to the source biometric template does highlight potential risks; however, such risks can be mitigated via several security measures that are widely implemented in biometric systems.

Along with the risk of sample reconstruction one should consider the danger that certain biometric characteristics may be forged via the creation of an artificial biometric characteristic (biometric spoofing) starting from fingerprints collected outside the biometric system.

A typical example consists in the use of a sort of "artificial finger" reproducing the anatomical features of a fingertip; this is currently made easier by the widespread use of low-cost 3-D printing techniques. The artificial fingertip obtained in this manner is still a gross fake than can be easily unmasked via technical procedures aimed at ensuring that the characteristic captured by the acquisition device is genuine – e.g. by way of liveness detection functions, which are to be found in some fingerprint capture sensors.

7.5. Risk Amplification in the Mobile and BYOD Contexts

A significant development in the IT sector has to do with the BYOD scenarios – that is to say, cases where an employee can connect with IT and/or documentary resources and/or services from the respective organization according to the "Bring-Your-Own-Device" paradigm, by using applications installed (with the employee's consent) on the employee's device such as to enable him or her to process corporate data as part of the respective job tasks.

These scenarios are considered by ENISA (the European Union Agency for Network and Information Security, www.enisa.europa.eu) to be among those to focus on in terms of security architectures and approaches. The Italian DPA is also well aware of the growing reliance, in the main production sectors, on job models that are heavily mobility-oriented as also related to the interaction with corporate IT systems – especially in the banking sector, where graphometric signature applications are considerably widespread.

Biometric processing operations based on mobile devices (such as tablets) may incur greater risks than those performed within a company's security perimeter – in particular if no adequate, specific security measures are in place.

The enhanced likelihood that such devices are used in different contexts, possibly for personal or household purposes or on a recreational basis, can hardly be reconciled with data security – partly because of the increased risk exposure and the use of insecure applications that can be installed by users without any restraints.

It is seldom the case that access control mechanisms are implemented in these contexts, including very basic ones such as inactivity autolocks; nor are secure connection modes offered as based on advanced protocols in order to protect the data in mobility contexts, where insecure data transmission channels are often resorted to.

8. GENERAL MEASURES APPLYING TO BIOMETRIC DATA PROCESSING

Without prejudice to adoption of the measures set forth in Sections 31 to 35 of the Code and in Annex B thereto, specific measures must be applied to the processing of biometric data as related to nature of the data, system architecture, specific purposes(s) sought, operational context of the biometric system, and data collection and storage mechanisms.

Based on the experience gathered so far and the decisions and orders issued by the DPA in this sector, the main measures and arrangements of a general nature to be implemented are described below in order to safeguard data subjects. This is without prejudice to the data controller's obligation under Section 31 of the Code to thoroughly deploy such measures as are appropriate, in the specific circumstances, to secure the processing operations being envisaged. Where the above measures depart from those listed below, the controller will have to adequately account for them and provide supporting documents.

8.1. Security Measures for Biometric Processing

The controller of electronic processing operations must take steps with the help of IT state-of-the-art technical tools in order to protect the personal data being processed according to the security measures laid down in the Code. These measures include the minimum security measures referred to in Sections 33 and 34 of the Code and in Annex B thereto along with the suitable preventative measures vis-à-vis the specific processing referred to in Section 31; the latter measures should be implemented after assessing the risk impending on the data as well as the adequacy of the technical solutions devised to counter such risk.

8.2. Selection of the Biometric System and Security Arrangements

Regarding sensor characteristics, one should prioritize, where technically feasible, the liveness detection functions as based on the capturing of several morphological and physiological parameters; for fingerprints, liveness controls take account of deformability and torsional behaviour of the fingerprint when placed on the sensor, presence of blood circulation, temperature, electric conductivity, etc. . This is aimed at preventing blatant fakes of the given biometric characteristic.

In selecting biometric processes, one should prioritize cognizant and cooperative capture processes.

Where technically feasible, low-information biometric templates should be used so as to mitigate or eliminate the risk of source sample reconstruction in all phases of the processing.

The raw biometric data generated during biometric capture will have to be erased from primary and secondary temporary storage areas as well as from the filesystem of the capture system immediately the biometric sample is generated.

Biometric data should be encrypted upon being captured by the sensor in order to reduce the risk of fraudulent acquisition via third-in-the-middle attacks on the sensor and/or its communication channels with the biometric system.

Data transmission will have to occur both in the enrolment and in the recognition phase via encrypted communication channels linking the acquisition device with the system where biometric comparisons are carried out and/or the reference biometric samples or templates are stored.

If biometric systems are deployed in mobile or BYOD contexts, regular audits should be carried out and tools for enhancing device security should be implemented such as MDM (Mobile Device Management) or MDA (Mobile Device Auditing) software systems.

Any approaches departing from the guidance contained herein will have to be described and accounted for as appropriate in the prior checking application.

8.3. IT Management and Data Storage

Where indispensable with a view to biometric comparisons, biometric samples or templates will have to be stored in encryption-protected filesystem areas or else in record-level or column-level encryption databases. If the biometric system is such as to make public-key encryption or the use of a trusted third party unfeasible, encryption will have to in any case ensure high security standards via adequate length keys as related to database size and criticality.[4]

Where technically feasible, preference will have to be given to only storing biometric templates on devices (tokens) held exclusively by users; centralized storage in databases that may be accessed also via local networks will have to be avoided.

Users' identification information will have to be stored separately from the respective biometric data.

[4] See ENISA's Recommendations in "Algorithms, Key Sizes and Parameters Report", October 2013.

If the biometric data is held by the data controller and stored in a single database, in IT workstations or on biometric capture devices, the controller will always have to take top-level precautions and implement all the safeguards required to protect the data - by minimizing the risk of unauthorized access to and/or theft, replacement or undermining of the biometric data.

Alternatively, and preferably where this is feasible, the controller should not keep any copy of the biometric data if the latter is stored in secure devices held directly and exclusively by data subjects.

Biometric smart cards and tokens should only be readable for authorized readers – at least with regard to the memory area containing the biometric data.

8.4. Biometric Data Access Log

If biometric data is stored centrally in a server, suitable systems must be implemented to log the accesses by entities that are specifically enabled to carry out server management and maintenance activities; such entities must be appointed as system administrators. The logging in question must include timestamps and meet the thoroughness, integrity, inalterability and retention standards that are applicable to the access logs mentioned in the DPA's decision of 27 November 2008 on system administrators.[5]

8.5. Storage of Biometric Data

Captured biometric data – whether relating to the raw data, the biometric sample, or the data obtained by processing either of them (i.e. biometric templates or references) – will be processed for no longer than is absolutely necessary to achieve the purposes for which the data were collected and processed, subject to the application of specific provisions under the given circumstances.

In particular, biometric samples used to generate the biometric template may only be processed in the capture and acquisition phases as required for biometric comparison; they may not be stored for longer than is absolutely necessary to generate the said template.

Where processing of a data is no longer necessary, the data must be erased securely from both volatile memory areas and memory media.

[5] See "Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator", Decision dated 27 November 2008, as published in Italy's Official Journal no. 300 of 24 December 2008 and amended by a Decision of the Italian DPA dated 25 June 2009 as published in Italy's Official Journal dated 30 June 2009.