versione italiana

General Application Order Concerning Biometrics - 12 november 2014

THE ITALIAN DATA PROTECTION AUTHORITY,

Having convened today in the presence of Mr. Antonello Soro, President; Ms. Augusta Iannini, Vice-President; Ms. Giovanna Bianchi Clerici and Prof. Licia Califano, Members; and Mr. Giuseppe Busia, Secretary General;

Having regard to the Italian data protection Code (Legislative decree No. 196 of 30 June 2003, hereinafter the "Code");

Having regard to EU Regulation No. 910/2014 of the European Parliament and of the Council of 23 July 2014 concerning electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, published in the Official Journal of the EU 2014 L 257 (so-called eIDAS Regulation);

Taking note of the high number of notifications submitted to the Italian DPA in connection with the processing of biometric data;

Whereas evolution of biometrics-based technologies has resulted into their significantly widespread use and such use can be expected to expand further with a view to several purposes in the most diverse societal sectors;

Having regard to the prior checking applications filed under Section 17 of the Code with regard to the processing of personal data by way of biometrics-based technologies;

Considering it appropriate to make available a consolidated set of measures and arrangements in technical, organizational and procedural terms to bring the processing of biometric data into line with the data protection legislation in force as well as in order to enhance the security of such processing;

Considering that the specificities of biometric data make it necessary to provide for the mandatory notification of any breaches related to their processing;

Considering additionally that appropriate safeguards should be set out under Section 17 of the Code to protect data subjects with regard to certain types of biometric data processing, partly in the light of state-of-the-art technical knowledge, which processing may be carried out without the need for a prior checking application to the Italian DPA;

Having regard to the considerations submitted by the Office by way of the Secretary General pursuant to Article 15 of the Italian DPA's Rules of Procedure No. 1/2000;

Acting on the report submitted by Ms. Augusta Iannini;

1. PREAMBLE

The use of technologies and devices to collect and process biometric data is increasingly widespread; this applies, in particular, to identification of individuals as part of the provision of information society services and/or for the access to computerized databases; the control on the access to buildings and areas; the operation of electronic and electro-mechanical 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 in analyzing and studying the issues in question. 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". As such, biometric data fall under the scope of application of the Code (Section 4(1), letter b)) and any operation performed on them by way of electronic tools is a processing operation for all the intents and purposes of personal data protection legislation.

Consistently with the opinions rendered by the WP29, biometric samples, biometric templates, biometric references and any other data that is derived from biometric traits via computerized processing and can be traced back to an identified or identifiable individual, including via links to other databases, are considered to be biometric data in this document.

2. Guidelines on Biometric Recognition and Graphometric Signature

Following specific prior checking applications under Section 17 of the Code, this DPA has issued several decisions over the years; 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.

Faced with such a complex subject matter and by having regard to personal data protection legislation, this DPA intends to provide a consolidated reference framework by adopting the annexed "Guidelines on Biometric Recognition and Graphometric Signature" (Annex "A"), which are an integral part of this decision. Data controllers will be enabled thereby to make their own decisions as to technological approaches, bring their processing into line with the lawfulness principles set forth in the Code, and ensure compliance with top-level security standards.

The Guidelines include the fundamental terminology required to describe the relevant technological features on the basis of international standards; the main risk profiles related to the processing of biometric data are also highlighted.

3. Disclosure of Biometric Data Breaches

The peculiar features of biometric data along with the risks they carry – shown in the Guidelines – point to the need for introducing the obligation to disclose, to the DPA, any data breaches and/or any IT incidents (such as unauthorized access or malware actions) that may expose such data to the risk of a breach even though they do not impact them directly. This is actually in line with the provisions made in the European eIDAS regulation on identification, authentication, and electronic signature.

To that end, data controllers shall disclose, to the DPA, all the data breaches and/or all IT incidents that may significantly impact biometric systems or the personal data stored therein within twenty-four hours of becoming aware of the event(s). The disclosure must be made in accordance with the template shown in "Annex B" hereto and then emailed or sent via certified email ("PEC") to databreach.biometria@pec.gpdp.it.

4. Exemption from the Prior Checking Obligation Referred to in Section 17 of the Code

Biometric data is, by its very nature, related to an individual directly, uniquely and in a basically time-consistent manner. Any biometric data mirrors the in-depth relationship between an individual's body, behavior and identity and requires special precautions when processed. Accordingly, the deployment of biometric systems may entail specific risks to data subjects' rights and fundamental freedoms and to their dignity depending on the implemented technology, the context of deployment, the number and types of prospective data subjects, the arrangements and purposes of the processing.

This is why a prior checking application must be filed with the Italian DPA under Section 17 of the Code if the processing of biometric data is intended.

Nevertheless, the Italian DPA has decided – based on the experience gathered so far – to list hereby some types of processing entailing a low level of risk in the light of the specific purposes, the categories of data being processed and the security measures that can be implemented factually to protect such data. The processing in question serves biometric recognition purposes in the form of biometric identification and/or biometric verification, or else is aimed at undersigning IT documents via the so-called graphometric signature.

Accordingly, data controllers are not required to file the said application in connection with the specific processing categories mentioned above, providing they implement all the appropriate technical measures and arrangements to achieve the security objectives laid down herein; furthermore, the lawfulness requirements provided for in the Code as recalled in Chapter 4 of the Guidelines will have to be met – with particular regard to the general principles of lawfulness, necessity and proportionality of the processing and to the legal requirements such as the obligation to provide information to data subjects and notify the DPA of the processing.

Based on the experience gathered along with technological evolution, the DPA reserves the right to provide for additional exemptions.

The guidance on processing biometric data to be found in previous decisions by the DPA (such as, for instance, the guidelines on processing personal data for managing employment relationships in the private and public sectors) continues to be applicable to the extent it is compatible with the provisions contained herein.

Specific prior checking proceedings that have been already the subjects of assessment by the DPA will not require additional steps to be taken.

Any data controller for biometric processing that is exempted hereby from prior checking and has already filed the relevant application under Section 17 of the Code as of the date this decision is published in the Official Journal of the Italian Republic is required to inform the DPA, by thirty days from the latter date, that such processing complies with the instructions set out herein or that he/she will ensure compliance with them. Submission of the above information will result into a nonsuit decision by the DPA.

Conversely, any prior checking application in whose respect no information is submitted under the terms detailed above will be assessed by the DPA according to standard procedural rules.

4.1. IT Authentication

Biometric traits may be used as authentication credentials to access databases and IT systems whenever enhanced identification security is

required on account of specific risks related to the processed information and the IT resources relied upon. This is the case, for instance, with the critical IT infrastructures mentioned in the Decree of 9 January 2008 by the Minister for Home Affairs (published in the Official Journal No. 101 of 30 April 2008).

In such cases public bodies may legitimately process the data as controllers to achieve purposes related to the discharge of institutional functions; regarding private bodies, they may legitimately do so on the basis of the balancing of the interests at issue (under Section 24(1), letter g)). That is to say, private bodies may process biometric data as controllers without the data subjects' consent on the basis of the legitimate interest pursued by them, the instructions contained in this order, the purposes sought as related to specific security requirements that are commensurate with the risks impending on the data or IT systems the authentication procedure is meant to safeguard and by taking also account of the regulatory requirements concerning minimum security measures for databases.

Accordingly, data controllers are exempted from the obligation to file a prior checking application if the processing is carried out in accordance with the provisions below:

a) Biometric traits consist in fingerprint or voice data.

b) If fingerprints are relied upon, the enrolment device must include liveness detection capabilities.

c) If voice data are relied upon, the latter are only used in conjunction with other authentication factors and by making arrangements such as to rule out the risk of fraudulent use of voice recordings (e.g. by requiring the individual to repeat certain words or sentences in the course of the recognition procedure).

d) Raw biometric data are erased immediately after their transformation into biometric samples or templates.

e) Initial enrolment and operational enrolment devices are directly connected or integrated with the respective IT systems – whether they are enrolment stations, workstations or server systems protected via biometric authentication.

f) Data transmission between enrolment devices and IT systems is secured with the help of encryption using adequate length encryption keys in relation to data size and lifecycle.

g) If biometric references are stored in secure mode on portable media (smart cards or similar secure devices) equipped with adequate encryption capabilities and certified for the relevant functions in accordance with ISO/IEC 15408 or (at least level-3) FIPS 140-2:

I. The medium used is released in a single copy, it is in the data subject's exclusive possession, and it is returned and destroyed in accordance with a formalized procedure if the right to access IT systems is lifted;

II. The memory area where biometric data are stored is only made accessible to authorized readers and protected against unauthorized access;

III. Biometric samples or references are encrypted via encryption techniques using adequate length keys in relation to data size and lifecycle.

h) If biometric references or samples are stored on the IT system protected via biometric authentication:

I. Access to IT systems by sys administrators is recorded by way of suitable logging systems;

II. Suitable technical measures and arrangements are implemented to counter unauthorized software installation and changes to IT systems configuration;

III. IT systems are malware-protected;

IV. Measures and arrangements are implemented to reduce the risks that the enrolment device is tampered with or accessed fraudulently;

V. Biometric samples or references are encrypted via encryption techniques using adequate length keys in relation to data size and lifecycle;

VI. Biometric samples or references are stored for no longer than is absolutely necessary to achieve the purposes of the biometric system;

VII. Biometric samples or references are stored separately from data subjects' identifying information;

VIII. Automatic data erasure mechanisms are implemented once the purposes for which such data is collected and processed no longer obtain.

i) The creation of centralized biometric filing systems is ruled out.

j) A report is drawn up describing the technical and organizational features of the measures implemented by the data controller, including the assessment as to the necessity and proportionality of biometric data processing. This report is kept and updated, based on at least yearly controls, throughout the operation of the biometric system and must be made available to the DPA on request.

Where a data controller holds an SGSI (information security management system) certification according to ISO/IEC 27001 and includes the biometric system under the scope of application of the said certification, he/she is exempted from the obligation to draw up the aforementioned report as the documents submitted in connection with the certification process may be relied upon and supplemented by the assessment of the necessity and proportionality of biometric data processing.

4.2. Controls on Physical Access by Staff to "Sensitive" Areas and Use of Dangerous Equipment and Devices

The deployment of biometric systems based on processing fingerprints or hand contour may be allowed to restrict access to areas and premises considered to be "sensitive", where high-level security must be ensured, or else to only enable skilled, specifically authorised staff to operate dangerous equipment and devices.

This applies, in particular, to the following:

- Areas intended for the performance of activities that are especially confidential or are committed to selected staff in charge of specific tasks such as to make it necessary to process confidential information and critical applications;

- Areas where especially valuable items are kept or that are only accessible to a limited number of staff;

- Areas intended for the performance of and/or control on dangerous productive processes such as to require selected access by highly skilled, qualified staff;

- Operation of dangerous equipment and devices such as to require special dexterity to prevent accidents and harm to property or individuals.

In such cases public bodies may legitimately process the data to achieve purposes related to the discharge of institutional functions, whilst private bodies may legitimately do so on the basis of the balancing of the interests at issue (under Section 24(1), letter g)). That is to say, private bodies may process biometric data without the data subjects' consent on the basis of the legitimate interest pursued by them, the instructions contained in this order, and the purposes sought as related to specific security requirements.

By having regard to the said purposes, a controller is exempted from the obligation to file a prior checking application if the processing is carried out in compliance with the provisions below:

a) Biometric traits consist in fingerprints or hand contour.

b) If fingerprints are relied upon, the enrolment device must include liveness detection capabilities.

c) Raw biometric data are erased immediately after their transformation into biometric templates.

d) Initial enrolment and operational enrolment devices are directly connected or integrated with enrolment IT stations and access control stations, respectively.

e) Data transmission between enrolment devices and workstations or control stations is secured with the help of encryption using adequate length encryption keys in relation to data size and lifecycle.

f) If biometric references are only stored in secure mode on portable media (smart cards or similar secure devices) equipped with adequate encryption capabilities and certified for the relevant functions in accordance with ISO/IEC 15408 or (at least level-3) FIPS 140-2:

I. The medium used is released in a single copy, it is in the data subject's exclusive possession, and it is returned and destroyed in accordance with a formalized procedure if the right to access sensitive areas is lifted;

II. The memory area where biometric data are stored is only made accessible to authorized readers and protected against unauthorized access;

III. Biometric references are encrypted via encryption techniques using adequate length keys in relation to data size and lifecycle.

g) If biometric references are stored on a reader or a dedicated IT station (gate controller) equipped with the security measures mentioned under letter e) above:

I. Access to IT systems by sys administrators is recorded by way of suitable logging systems;

II. Suitable technical measures and arrangements are implemented to counter unauthorized software installation and changes

to IT systems configuration;

III. IT systems are malware-protected and firewall systems are implemented to protect network perimeter and counter unauthorized data accesses;

IV. Measures and arrangements are implemented to reduce the risks that the enrolment device is tampered with or accessed fraudulently;

V. Biometric references are encrypted via encryption techniques using adequate length keys in relation to data size and lifecycle;

VI. Biometric references are stored for no longer than is absolutely necessary to achieve the purposes of the biometric system;

VII. Biometric references are stored separately from data subjects' identifying information;

VIII. Automatic data erasure mechanisms are implemented once the purposes for which such data is collected and processed no longer obtain.

h) The creation of centralized biometric filing systems is ruled out.

i) A report is drawn up describing the technical and organizational features of the measures implemented by the data controller, including the assessment as to the necessity and proportionality of biometric data processing. This report is kept and updated, based on at least yearly controls, throughout the operation of the biometric system and must be made available to the DPA on request.

Where a data controller holds an SGSI (information security management system) certification according to ISO/IEC 27001 and includes the biometric system under the scope of application of the said certification, he/she is exempted from the obligation to draw up the aforementioned report as the documents submitted in connection with the certification process may be relied upon and supplemented by the assessment of the necessity and proportionality of biometric data processing.

4.3. Use of Fingerprints or Hand Contour for Purposes of Facilitation

Biometrics may also lend themselves to being used for enabling, regulating and simplifying physical access by users to physical areas in both the public (e.g. libraries) and the private sector (e.g. airport restricted access areas), or to specific services.

In such cases, biometric data may be legitimately used with the data subjects' truly free consent, providing alternative options are available to enable access without relying on biometric data.

A controller is exempted from the obligation to file a prior checking application if the processing is carried out in compliance with the provisions below:

a) Biometric traits consist in fingerprints or hand contour.

b) Raw biometric data and biometric samples are erased immediately after their collection and transformation into biometric templates.

c) Initial enrolment and operational enrolment devices are directly connected or integrated with enrolment IT stations and control stations or with enrolment devices, respectively.

d) Data transmission between enrolment devices and the other biometric system components is secured with the help of encryption using adequate length encryption keys in relation to data size and lifecycle.

e) If biometric references are only stored in secure mode on portable media (smart cards or similar secure devices) equipped with adequate encryption capabilities and certified for the relevant functions in accordance with ISO/IEC 15408 or (at least level-3) FIPS 140-2:

I. The medium used is released in a single copy, it is in the data subject's exclusive possession, and it is returned and destroyed in accordance with a formalized procedure if the right to access sensitive areas is lifted;

II. The memory area where biometric references are stored is only made accessible to authorized readers and protected against unauthorized access;

III. Biometric references are encrypted via encryption techniques using adequate length keys in relation to data size and lifecycle.

f) If biometric references are stored on a reader or an IT station:

I. Access to the IT station by sys administrators is recorded by way of suitable logging systems;

II. Suitable technical measures and arrangements are implemented to counter unauthorized software installation and changes to device or IT station configuration;

III. Measures and arrangements are implemented to reduce the risks that the enrolment device is tampered with or accessed fraudulently;

IV. Biometric references are encrypted via encryption techniques using adequate length keys in relation to data size and lifecycle;

V. Biometric references are stored for no longer than is absolutely necessary to achieve the purposes of the biometric system;

VI. Biometric references are stored separately from data subjects' identifying information;

g) The creation of centralized biometric filing systems is ruled out.

h) A report is drawn up describing the technical and organizational features of the measures implemented by the data controller, including the assessment as to the necessity and proportionality of biometric data processing vis-à-vis the purposes of facilitation. This report is kept and updated, based on at least yearly controls, throughout the operation of the biometric system and must be made available to the DPA on request.

Where a data controller holds an SGSI (information security management system) certification according to ISO/IEC 27001 and includes the biometric system under the scope of application of the said certification, he/she is exempted from the obligation to draw up the aforementioned report as the documents submitted in connection with the certification process may be relied upon and supplemented by the assessment of the necessity and proportionality of biometric data processing.

4.4. Undersigning IT Documents

No prior checking is necessary to process biometric data consisting in dynamic information associated with the placing of one's handwritten signature by means of specific hardware, if one relies on graphometric systems to deliver advanced digital signature solutions in accordance with Legislative Decree No. 82 of 7 March 2005 ("Code of Digital Administration") – i.e. systems that do not envisage any centralized storage of biometric data.

Reliance on such systems is justified on the one hand to counter fraud and identity theft and, on the other hand, in order to enhance authenticity and integrity of the undersigned IT documents – possibly in view of legal actions brought on account of the failure to validate one's signature on contractual instruments and documents.

In such cases, biometric data may be legitimately processed on the basis of the data subjects' truly free consent; public bodies may legitimately process such data in order to discharge their institutional tasks as controllers. Consent can be given by a data subject upon accepting the graphometric signature-based service and applies to all the documents to be undersigned until it is withdrawn.

A controller is exempted from the obligation to file a prior checking application if the processing is carried out in compliance with the provisions below:

a) The signature procedure is enabled after identification of the person undersigning the document.

b) Alternative options are available to undersign the documents, whether on paper or electronic, without relying on biometric data.

c) Raw biometric data and biometric samples are erased immediately after completion of the undersigning and no biometric data remains outside the IT document being undersigned.

d) No biometric or graphometric data is kept, not even for limited periods, on the hardware devices used for data collection, whilst it shall only be stored in the undersigned IT documents in encrypted format using public key cryptography and a suitable length key in relation to data size and lifecycle along with a digital certificate issued by an accredited certification body pursuant to Section 29 of the Digital Administration Code. The corresponding private key shall be held exclusively by a trusted third party providing appropriate independence and security safeguards as for key storage. The key may be broken up and distributed among several entities with a view to data security and integrity. In no case may the entity providing graphometric signature services retain such private key in its complete format. Key generation, delivery and storage mechanisms shall be detailed in the information notice to data subjects and in the report mentioned under letter k) hereof pursuant to Section 57(1), letters e) and f), of the Prime Minister's Decree dated 22 February 2013.

e) Biometric data transmission between enrolment hardware, IT stations and servers may only take place via encryption-secured communication channels using suitable length keys in relation to data size and lifecycle.

f) Suitable technical measures and arrangements are implemented to counter unauthorized software installation and changes to device or IT station configuration.

g) IT systems are malware-protected and firewall systems are implemented to protect network perimeter and counter unauthorized data accesses.

h) Where graphometric signature systems are used in a mobile or BYOD (Bring Your Own Device) environment, suitable mobile application/device management systems are implemented with the help of MDM (Mobile Device Management) or MAM (Mobile Application Management) tools, or equivalent ones, in order to insulate the memory area dedicated to the biometric application, reduce the risk of unauthorized software installation (also following device configuration changes), and counter any malware.

i) The management systems deployed in processing graphometric data rely on digital certifications and security policies regulating the conditions for their secure use on the basis of pre-defined criteria; in particular, remote wiping functions must be enabled in case of loss or theft of the relevant devices.

j) Access to the encrypted graphometric template only takes place by means of the private key held by the trusted third party or, in case the key was broken up, by several trusted third parties; such access may only occur if it is indispensable on account of a dispute on authenticity of the signature and at the request of a judicial authority. The conditions and arrangements for the trusted third party or eligible technicians to access the graphometric signature are detailed in the information notice to data subjects and in the report mentioned under letter k) hereof pursuant to Section 57(1), letters e) and f), of the Prime Minister's Decree dated 22 February 2013.

k) A report is drawn up describing the technical and organizational features of the measures implemented by the data controller, including the assessment as to the necessity and proportionality of biometric data processing vis-à-vis the purposes of facilitation. This report is kept and updated, based on at least yearly controls, throughout the operation of the biometric system and must be made available to the DPA on request.

Where a data controller holds an SGSI (information security management system) certification according to ISO/IEC 27001 and includes the biometric system under the scope of application of the said certification, he/she is exempted from the obligation to draw up the aforementioned report as the documents submitted in connection with the certification process may be relied upon and supplemented by the assessment of the necessity and proportionality of biometric data processing.

BASED ON THE ABOVE PREMISES, THE ITALIAN DATA PROTECTION AUTHORITY

1. Adopts the "A" Annex pursuant to Section 154(1), letter h), of the Code, containing the "Guidelines on Biometric Recognition and Graphometric Signature", which is an integral part of this decision, in order to inform data controllers, manufacturers of biometrics-based technology, service providers and data subjects on several issues related to personal data protection including security as well as on the requirements to be met in order to legitimately process biometric data;

2. Orders under Section 154(1), letter c), of the Code that the controllers of biometric data processing inform the DPA on any biometric data breaches by twenty-four hours from becoming aware of such event(s), according to the arrangements set out in paragraph 3 above;

3. Provides for exemptions from the obligation to file a prior checking application under the terms of paragraph 4 above; orders the entities intending to proceed as data controllers with the processing in question to take, under Section 17 of the Code, the technical, organizational and procedural arrangements described in the aforesaid paragraph and comply with the requirements for legitimately processing data and the relevant guidance as set forth in the annexed "Guidelines", with particular regard to Chapter 4 on "General Principles and Legal Requirements";

4. Orders any controller of biometric data processing that has not filed a prior checking application with the DPA:

a. to take, within one hundred and eighty days from publication of this order in the Official Journal of the Italian Republic, the measures and arrangements referred to in paragraph 4 above if the processing falls under the exemptions from prior checking obligations; or

b. to suspend the processing by the aforementioned deadline and subject it to prior checking by filing an application with the DPA under Section 17 of the Code;

5. Calls upon the controllers of biometric data processing exempted from prior checking obligations that have already filed an application under Section 17 of the Code, if such application is still pending, to notify the DPA by thirty days from publication of this order in the Official Journal of the Italian Republic that the processing in question complies with the instructions set forth herein, or that they will ensure compliance with those instructions. Upon submission of the said notification, the DPA will issue a nonsuit decision on the relevant application(s). Prior checking applications for which no such notification is submitted will be assessed by the DPA in accordance with standard procedures;

6. Provides, under Section 143(2) of the Code, that a copy of this order be sent to the Ministry of Justice – Ufficio pubblicazione leggi e decreti in order for it to be published in the Official Journal of the Italian Republic.

Done in Rome, this 12th day of the month of November 2014

THE PRESIDENT
Soro

THE RAPPORTEUR
Iannini

THE SECRETARY GENERAL
Busia