

## THE ITALIAN DPA APPROVES THE RESOLUTION FOR SENSITIVE DATA

### 1. Introduction

With the Decision no. 146 dated June 5, 2019 (the "**Decision**") the Italian data protection authority (the "**Italian DPA**") approved its general resolution on sensitive data as required by Article 21, paragraph 1, of the Italian Legislative Decree no. 101/2018 (i.e. the legislative decree whereby the Italian Privacy Code has been aligned to the GDPR).

The Decision identifies the requirements relating to the processing of special categories of personal data, pursuant to Article 9 of the Regulation (EU) 2016/679 ("**GDPR**") ("sensitive data"), and overrules the previous Italian DPA's General Authorizations nos. 1/2016, 3/2016, 8/2016, 9/2016.

More specifically, the Decision concerns the processing of sensitive data:

- (i) within employment relationships between employer and employee;
- (ii) by associations, foundations, churches and religious associations or communities;
- (iii) by private investigators;
- (iv) in relation to genetic data; or
- (v) for scientific research purposes.

### 2. Requirements relating to the processing of sensitive data in employment relationships (previous General Authorisation no. 1/2016)

2.1 Scope of application. The Decision applies to all those who, for various reasons, process sensitive data for the purpose of establishing, managing or terminating an employment relationship.

2.2 Data Subjects. The categories of data subjects include, in addition to employees, also candidates to job positions, consultants and freelancers, agents, representatives, self-employed workers, natural persons holding corporate offices or other positions in legal persons, entities, associations or bodies as well as third parties suffering damages from work or professional activities and the data subjects' family members or cohabitants for the issue of benefits or permits.

2.3 Legal basis for the processing. The Decision recognizes that in many cases the processing of sensitive data in the workplace may rely, as a legal basis, on the law and the employment contracts (including collective bargaining agreements), which justify the processing of sensitive data with respect to the fulfilment, by the employer, of legal or contractual obligations relating amongst others to social security, taxation or alternative dispute resolution mechanisms.

2.4 Prohibitions. Specific obligations are imposed on employers before, during and after the recruitment of data subjects.

- i. Before the recruitment, sensitive data, as well as, in general, personal data, may be only processed for specific and legitimate purposes and only to the extent that the collection is necessary to establish the employment relationship. Anything that is superfluous for the purposes of establishing an employment relationship should not be requested or, if provided,

should not be used. In this respect, for example, employers should not assume that they are allowed to process data contained in social networks for their own purposes simply because an individual's profile in social media is publicly accessible. In order to be able to carry out such processing, a legal basis, such as a legitimate interest, is necessary, for example, to verify that the profile has a commercial purpose or has been opened specifically to increase the employee's chances of employment (e.g. LinkedIn, see Article 29 Working Party's Opinion no. 2/2017).

ii. During the course of the employment relationship, without prejudice to the prohibition of processing employees' genetic data, the Decision provides for specific limitations to the processing of data concerning: (i) religious or philosophical beliefs or membership in associations or organizations of a religious or philosophical nature; and (ii) political opinions or trade union membership, or the exercise of public functions and political duties as well as trade union activities or tasks.

2.5 Communication between offices/departments. Internal communications between departments of the same business undertaking or group, including electronic communications, which contain sensitive data, must be protected; i.e., the most appropriate measures must be adopted to prevent the unjustified knowledge of such sensitive data by third parties other than the recipient.

### **3. Requirements relating to the processing of sensitive data by foundations, churches and associations or religious communities (previous General Authorisation no. 3/2016)**

3.1 Scope of application. Compared with the "old" General Authorization, the Decision broadens the list of subjects to which the requirements to process sensitive data apply, by explicitly encompassing all the non-profit entities. It also includes, in addition to those engaged in non-profit activities and social cooperatives and mutual benefit associations, also churches, religious associations or communities. It is interesting to note that the scope of the Decision may include (in addition to those who carry out strictly charitable activities), also those pursuing civic, social, general interest or economic development objectives (for example, associations or organizations of a trade-union or professional nature, political parties, banking foundations, etc.).

3.2 Data Subjects. The list of data subjects remains unchanged; it is very broad and includes associates, adherents, supporters, assistants, users, etc., who, in various ways, adhere to, participate in, or are part of the entities mentioned above.

### **4. Regulatory prescriptions relating to the processing of sensitive data by private investigators (previous General Authorisation no. 6/2016)**

4.1 Scope of application. The requirements apply to those carrying out an authorized private investigation activity under a prefectural license, and supplement the "rules of professional conduct relating to the processing of personal data carried out to perform defensive investigations or to assert or defend a right in court" (Decision no. 512 dated December 19, 2018).

4.2 Purpose. Processing of sensitive data is permitted if: (i) carried out for the performance of the professional engagement of collecting information to be used in a judicial proceeding or arbitration; genetic data or data relating to health, sex life or sexual orientation may be processed only if the judicial defence concerns a right of equal rank (a right of personality or other fundamental right or

freedom); or (ii) carried out upon instructions coming from a lawyer in a criminal proceeding for the sole purpose of proving a fact during the trial.

4.3 Engagement and performance. The Decision regulates the processing and, in particular, sets forth certain mandatory elements of the engagement of the private investigators and the manners in which such engagement must be performed (e.g. it shall be carried out personally or through specifically identified subjects, normally at the end of the assignment all processing must cease).

## **5. Regulatory prescriptions relating to the processing of genetic data (previous General Authorisation no. 8/2016)**

5.1 Contents. In implementing Article 9, paragraph 4, of the GDPR, the Decision regulates the special modalities for the processing of genetic data and biological samples.

5.2 Safeguards. For the protection and security of these data, the following is required: (i) a procedure for the identification of those duly authorized to process the data, in relation to any access to the premises where such data are processed after normal business hours (and the admissibility of the use of biometric data to make those identifications); (ii) the storage, use and transport of the data in such a way as to ensure quality, integrity, availability and traceability; (iii) in case data are communicated through electronic means, the dispatch via secure attachments and encryption of the data, with the transmission of the cryptographic key via different communication means; (iv) the use of devices to control accesses to the processing operations based on double keys of which at least one is through an ad hoc device; (v) the use of pseudonymisation and data segregation in order to limit the identification of the data subjects.

5.3 Information notices. The Decision provides for detailed information duties with respect to data subject's choices and options and their consequences (especially in the case of investigations of parentage) and/or risks, imposing the mandatory assistance of healthcare professionals and geneticists in the best interests of the data subjects.

5.4 Consent. The Decision sets forth certain cases in which the consent of the data subjects is necessarily required as only legal basis admitted for the processing. Specifically, explicit consent is necessary in the following cases: (i) protecting the health of a third party belonging to the same genetic line as the data subject; (ii) in the context of genetic tests relating to defensive investigations or for the exercise of a right in a judicial proceeding; (iii) for the purposes of research or family reunification; or (iv) in the case of scientific and statistical research not prescribed by law. In the event of withdrawal of consent, processing must cease and the data must be deleted or anonymized.

5.5 Further considerations on research purposes. In reproducing consent as a mandatory legal basis for the processing of genetic data, the Decision deviates from the normal rule in the GDPR that, for processing for research purposes, allows instead to disregard the existence of a specific consent (pursuant to Article 9, paragraph 2, let. j).

It should also be noted that the consent to the processing of genetic data is mentioned as a possible additional security measure that the Italian DPA may (but it is not bound to) require to data controllers pursuant to the "regulation on health, genetic or biometric data" (not enacted yet) (Article 2-septies, paragraph 6, of the Privacy Code). The Decision, which requires the consent as the only legal basis in the cases mentioned above, seems to anticipate that we will find a broad use of the requirement of "explicit consent" in the aforesaid regulation.

5.6 Limitations. In relation to each of the cases above, the Decision sets forth certain clarifications, different from case to case, on the methods of processing and communication, on the information to be provided to the data subjects and on the possible exceptions to the rule of consent.

## **6. Requirements relating to the processing of sensitive data for scientific research (previous General Authorisation no. 9/2016)**

6.1 Derogations to consent. The Decision seeks to implement the legal framework provided for by Article 9, paragraph 2, let. j), of the GDPR as well as Article 110 (health data) and 110-bis (which refers to personal data in general) of the Italian Privacy Code. However, our considerations in paragraph 5.6 above with respect to genetic data equally apply to this part of the Decision, which seems to perpetuate the Italian DPA's approach based on the "need of consent" as main rule and legal basis for the processing of personal data for research purposes. That approach brings the risk of frustrating the innovations provided for in Article 9, paragraph 2, let. j), of the GDPR, which instead releases from the rule of consent the processing of sensitive data for scientific and statistical research purposes, provided that certain safeguards are applied under EU or national law. There remains, therefore, a gap between the structure designed by national law and that, more liberal, of the GDPR for processing for research purposes.

6.2 Further considerations on information notices and consents. From what is written in the Decision and in Articles 110 and 110-bis of the Privacy Act, it is clear that, as a rule, information is always due: both for the case of data collected from the data subject (Article 13 of the GDPR), and, a very frequent case in the field of research, when the data are collected elsewhere (Article 14 of the GDPR). Information notices are to be provided in relation to each single research project, which makes it problematic, for example, to allow for general, framework or catch-all information notices for scientific research issued by clinics, hospitals, medical laboratories or institutions of hospitalization and scientific care ("ICCRS") during the recruitment of patients to whom health services will be provided.

The Decision introduces a very restrictive regime for data controllers who intend to request exemption from the duty of providing information notices (and therefore from getting specific data subjects' consents): any deviation from the rule, whereby notice must be given and consent must be obtained, has in fact to be carefully justified from an ethical, clinical or organizational point of view, in the latter case even requiring an obligation of active research of the data subjects through, for example, the verification of the state of life or the questioning of the record of the patients or the resident population. It follows, moreover, that the restrictive procedures outlined above must be followed even when data are collected from third parties and the data controller intends to make use of the exemption provided for in Article 14, paragraph 5, let. b) of the GDPR, according to which the information notices to the data subjects may not be given when "*the provision of such information proves impossible or would involve a disproportionate effort*".

6.3 The research project. A crucial element in carrying out the research and assessing the related compliance obligations is the research project, which must contain all the scientific and organizational information which is necessary to carry out the study and to demonstrate the grounds of the controller's decisions in processing the data subjects' personal data (accountability).

6.4 Principle of minimisation and pseudonymisation. The focus is on the safeguards for the processing of sensitive data and the methodologies for their storage. Specific measures are required to limit the processing to the data which are strictly necessary and to apply mandatory safeguards, such as the use of encryption, pseudonymisation and separate storage techniques, to prevent data violations.

# Newsletter

AUGUST 2019

6.5 Security measures. Eventually, without prejudice to the obligation under Article 32 of the GDPR to adopt technical and organizational measures that ensure a level of security appropriate to the risk, the Decision lists some security measures that must be adopted from those storing sensitive data, among which, the most important are: the use of protected transmission channels, labelling techniques through users' identification codes, differentiated access levels according to seniority, role and need-to-know, audit log systems to control accesses to the database and to detect any anomalies.

# Newsletter

AUGUST 2019

The Data Protection Department of Legance is available to provide any clarifications, also in respect of any specific situation which may be of interest to you.

For further information:

**Andrea Fedi**

---

**Partner**

T. +39 06.93.18.271  
[afedi@legance.it](mailto:afedi@legance.it)

**Lucio Scudiero**

---

**Senior Associate**

T. +39 06.93.18.271  
[lscudiero@legance.it](mailto:lscudiero@legance.it)

or your direct contact at Legance.

# Newsletter

AUGUST 2019

## THE FIRM

Legance is an independent Italian law firm with expert, active and result-oriented lawyers, with a strong team spirit that has permitted a flexible and incisive organisational model that, through departments active in all practice areas of business law, offers the right balance between the specialist and the lawyer as a global consultant. Legance comprises around 250 lawyers, working in its Milan, Rome, London and New York offices, and has a diverse and extensive practice covering the following areas: Corporate Finance; Banking; Energy, Project & Infrastructure; Debt Capital Markets; Equity Capital Markets; Financial Intermediaries Regulation; Investment Funds; Litigation and Arbitration; Restructuring and Insolvency; EU, Antitrust and Regulation; Employment and Industrial Relations; Tax Law; Administrative Law; Real Estate; Compliance; Shipping, Aviation and Transportation Law; Intellectual Property; TMT (Technology, Media, Telecommunications); Environmental Law; Insurance; Food Law; Data Protection. For more information, please visit our website: [www.legance.com](http://www.legance.com).

## DISCLAIMER

The only purpose of this Newsletter is to provide general information. It is not a legal opinion nor should it be relied upon as a substitute for legal advice.

This Newsletter is sent to persons who have provided their personal data in the course of professional relations, meetings, seminars, workshops or similar events. It's may also receive this newsletter because Legance was authorized. You may finally receive it, because you have engaged Legance. If you wish not to receive the newsletter anymore, please write an email to [newsletter@legance.it](mailto:newsletter@legance.it) and you will be removed from the list of recipients. Until you cancel yourself from the list of recipients your personal data will be processed on paper or electronically for purposes which are related to the existing professional relations, or for information and divulgation reasons, but are not communicated to third parties, unless such communication is imposed by law or strictly necessary to carry out the relation. Data controller is **Legance – Avvocati Associati**. The list of the data processors is available if you write an email to [clienti.privacy@legance.it](mailto:clienti.privacy@legance.it). In any event, you are entitled to your rights as set forth in the current data protection legislation. All the above requests must be forwarded by fax to **Legance – Avvocati Associati**, on nr. +39 06 93 18 27 403.

Legance - Avvocati Associati and its partners are not regulated by the Solicitors Regulation Authority ("SRA") and the SRA's compulsory insurance scheme does not apply to them (they are instead covered by equivalent Italian insurance). A list of the partners of Legance - Avvocati Associati is open to inspection at the office of its London branch at Aldermay House 10-15 Queen Street - EC4N1TX, and also on the following website [www.legance.com](http://www.legance.com). Legance LLP only advises on Italian law related matters.