



The important data protection aspects related to the new whistleblowing legislation in Italy

📅 21/11/2023

📌 EU AND COMPETITION, PRIVACY AND CYBERSECURITY, PERSPECTIVES

Camillo Campi
Jacopo Piemonte
Adriano Garofalo

By way of the Decree No. 24/2023 (“Decree”), Italy has transposed into law the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of union law into various jurisdictions.

The Decree has been enacted on 30 March 2023. The purpose of the Decree is to safeguard individuals who report breaches of certain national or European Union laws (which came to their knowledge in the work context) that may jeopardize the public interest, the integrity of public administration or of a private entity¹.

The Decree took effect on 15 July 2023 for employers with an average of at least 250 employees in the year 2022².

For companies that had an average of up to 249 employees in 2022 the main obligation provided by the Decree to set up internal reporting channels will have to be implemented by 17 December 2023³.

We have described in another article the compliance aspects related to the Decree⁴. In this contribution we will focus instead on the quite important data protection actions that the companies should put in place.

¹ See article 1(1) of the Decree.

² See article 24(1) of the Decree.

³ See article 24(2) of the Decree.

⁴ <https://www.dejalex.com/2023/11/confindustria-guidelines-2023-italy-whistleblowing-legislation/>



1. PRINCIPLES OF THE GDPR TO KEEP IN MIND WHEN READING THIS ARTICLE

Art. 5 of the GDPR sets some principles related to processing of personal data, which should be observed while carrying out (or designing) activities that imply such processing.

More specifically, these principles delimit the boundaries within a data processing activity can be considered lawful. Failure to comply with these principles, and the gravity of the related violation, will determine the imposition of possible fines and/or penalties. The data controller shall be responsible for (and be able to demonstrate) compliance with those principles. “Accountability” is the one term which better summarizes the GDPR, and this dictum, of course, also applies to data processing activities related to the management of a whistleblowing channel.

The principles that any data controller must be able to demonstrate, are:

- a) “... *lawfulness, fairness and transparency* ...”, which means that the processing must be based on one of the legal basis provided for in art. 6 of GDPR, and must also be inspired by good faith (*i.e.*, for companies obligated to adopt a whistleblowing system, the provisions of the Decree will constitute a legal basis for the processing of personal data pursuant to art. 6.1.(c) GDPR). Moreover, those principles provide the data controller with a general disclosure duty to data subjects of the main features and information about the processing;
- b) “... *purpose limitation* ...”, which means that data collected for specified, explicit and legitimate purposes, shall not further processed in a manner that is incompatible with those purposes (*i.e.*, the data related to a whistleblowing report, shall be used only to handle the report, give feedback to the whistleblower, etc.);
- c) “... *data minimisation* ...”, which means that data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (*i.e.*,

data that are not useful or irrelevant for the handling of a whistleblowing report, shall not be collected or, if collected, shall be promptly deleted);

- d) “... *accuracy* ...”, which means that data must be accurate and, where necessary, kept updated (*i.e.*, if a whistleblower wishes to amend its report because it contains erroneous data, every reasonable step must be taken to ensure that such data are rectified without delay);
- e) “... *storage limitation* ...”, which means that data must be kept in a form which permits identification of data subjects for no longer the time necessary for the purposes for which the personal data are processed (*i.e.*, once the whistleblowing report is successfully handled, or once the legal term for data retention provided for in the Decree is expired, such data must be deleted or anonymized);
- f) “... *integrity and confidentiality* ...”, which means that data must be processed in a manner that ensures appropriate security against unauthorised or unlawful processing and against accidental loss, destruction or damage (*i.e.*, the whistleblowing system shall be properly secured with encryption, or shall be used only by authorized employees, etc.).

Last (but not least), art. 25 of the GDPR provides the so-called principle of “... *data protection by design and by default* ...”, which means that the data controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures. It shall then take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the varying risks to the the rights and freedoms of natural persons, in order to meet the requirements of the GDPR and protect the rights of data subjects.

2. SPECIFIC DATA PROTECTION ISSUES INVOLVED IN THE DECREE

We will now discuss of the specific issues arising from Decree.

As mentioned, the Decree main obligation is to set up internal communication channels to allow to the whistleblower to report certain facts to the company.

The receipt and handling of whistleblowing reports result in the processing of personal data referable to the individuals involved in the reported facts.

This implies that the companies obliged to implement a whistleblowing channel have to adopt (in their quality of data controller) a series of measures to ensure the lawfulness, confidentiality and security of the processing carried out (directly, or by means of their employees and/or collaborators involved in the management of the reports).

Indeed, the principles set forth by the GDPR at the basis of all kind of data processing activities cannot be ignored. On the one hand, attention must be given to the privacy roles played by those involved in the management of reports. On the other, security and organizational measures designed to ensure the confidentiality of the information received cannot be neglected either. We will then analyse the main features that the companies must comply with (and take into consideration) when implementing a whistleblowing channel.

3. THE OBLIGATION TO DEFINE THE PRIVACY ROLES TAKING INTO CONSIDERATION THE DIFFERENT SCENARIOS

The company obliged to implement a whistleblowing channel, could alternatively entrust its management to:

- a) a person/office (with dedicated staff properly trained) within its own organization;
- b) an external entity.

The result of the choice could be two-fold as we explain below.

3.1. The scenario in which the company sets internally its own reporting channel

As mentioned above, the company that establishes the reporting channel is considered a data controller. A data controller is the subject that will delineate the means and purposes of the data processing, and, therefore, will always have to guarantee that the data processing complies with the principles and regulations placed at the basis of any data processing activities.

Art. 4.4 of the Decree also states that private sector companies that have employed, in the last year, an average number of employees (permanent or fixed term) not exceeding 249, can share the internal reporting channel and the related management. In such event, the companies that share the internal reporting channel will be considered as joint data controllers. This means that such companies have to jointly determine the purposes and means of the processing of personal data, and they are required to establish, in a transparent manner, through an internal agreement⁵, their respective responsibilities for compliance with the obligations arising from the legislation on personal data protection. The essential contents of such agreement must be made available to the data subjects and all the parties eventually concerned.

Data controllers and joint data controllers shall then identify, within their own organizational structure, the individuals (employees) expressly designated with specific tasks and functions related to the processing of personal data⁶. These individuals will operate (for data protection purposes) under the authority of the data controllers and

⁵ See art. 26 of the Reg. (EU) 2016/679

⁶ See art. 29 of the Reg. (EU) 2016/679

joint data controllers, and should receive appropriate and specific instructions from them, as well as adequate and professional training.

Such role, as clarified by ANAC Guidelines, may be entrusted, among others, to individuals within the internal audit bodies, or the Supervisory Board provided for in the regulations of Legislative Decree No. 231/2001, or to ethics committees.

In any case, it is expressly provided that the individuals/office entrusted with the management of the whistleblowing channel, must be:

- a) Impartial, in order to ensure that reports are handled fairly and free from internal or external influences;
- b) Independent, in order to ensure objective and impartial analysis of the report.

3.2. The scenario in which the company outsources externally the channel

It may occur, however, that data controllers decide to outsource the management of the whistleblowing channel (and the relevant reports) to third parties, external to their organization, instead of appointing their own employees as authorized subjects. In the event that a third party is entrusted with the management of the whistleblowing channel (or, otherwise, is involved in a part of the reports' management procedure such as the provider of the IT platform on which the reporting channel is based), the latter must be appointed, by contract or other legal act, as data processor⁷; the data processor is indeed the subject that carries out the data processing on behalf of the data controller. Therefore, the data processor must comply with the

specific instructions that the data controller has provided. Finally, it is mandatory that the data processor presents sufficient guarantees, in particular in terms of specialized knowledge, reliability and resources, to put in place technical and organizational measures that ensure respect for confidentiality, data protection and secrecy.

4. THE NECESSITY TO CARRY OUT A DATA PROTECTION IMPACT ASSESSMENT AND RELEVANT SECURITY MEASURES

After having examined and defined the roles that those involved in the management of the whistleblowing channel may have, there are other relevant consequences of adopting a whistleblowing channel.

First of all, it is fundamental that the employer (as data controller) guarantees, from the design of the reporting channel (privacy by design), and by default (privacy by default), that only the personal data strictly necessary in relation to the specific reporting purpose are processed. In order to do so, the data controllers must carry out, while designing the features of the reporting channel, and thus before the start of processing of the reports, a data protection impact assessment⁸ (“**DPIA**”), in order to identify possible risks related to the processing and apply the necessary measures to avoid or mitigate these risks.

The DPIA will need to take into consideration that since the processing of whistleblowing reports entails high risks to the rights and freedoms of data subjects, data controllers must adopt several measures to protect the confidentiality of reports and relative information. Such measures⁹ could result in the use of encryption tools within the reporting channel, as well as ensuring the segregation of duties of the subjects involved in the processing.

⁷ See art. 28 of the Reg. (EU) 2016/679

⁸ See art. 35 and 36 of the Reg. (EU) 2016/679

⁹ In addition to those already identified in Article 32 of the Reg. (EU) 2016/679

With specific reference to the case where the access to the reporting channel is made through the data network of the data controller, it must be ensured that there is no traceability of the whistleblower, both on the IT platform and in the network possibly involved. Otherwise, the recording and storage (e.g., in the logs of firewall equipment), of information about connections to the reporting channel could allow the traceability of the individuals who used the platform, including the whistleblowers, and therefore frustrate the other measures eventually adopted by data controller in order to protect the identity of the whistleblower. On the other hand, where possible, the tracking of the activities of the authorized personnel shall be ensured, in order to prevent the misuse of data related to the reporting, except for those data from which the identity or activities of the whistleblower could be disclosed¹⁰.

5. INFORMATION DUTIES TO BE GIVEN TO THE DATA SUBJECTS

Data controllers must provide possible data subjects with appropriate information about the processing of personal data¹¹.

This means, *inter alia*, that the following should be brought to the attention of the data subjects:

- i) the data controller and its contact details;
- ii) the contacts of the data processor (if the service has been outsourced externally);
- iii) the purpose of the processing;
- iv) the legal basis of the processing;
- v) the methods of processing;
- vi) the scope of processing and the subjects to whom the data are disclosed;
- vii) the storage period of personal data;

- viii) the contact details of the DPO, whether existent;
- ix) the data subjects' rights and guidance on how they can exercise them.

By way of example, such information may be provided as an annex to the whistleblowing procedure, (e.g., on the website of the data controller), or in a special section of the IT application used for the filing of the reports, as well as being made available in the workplaces.

With reference to the obligation to make the disclosure, however, it must be noted that, in the phase of acquisition of a report and/or in any subsequent investigation, no specific information or disclosure should be provided to parties other than the whistleblower. The aim is to avoid the frustration of the confidentiality protections provided by the Decree.

6. OBLIGATION TO ADJOURN THE REGISTER OF PROCESSING

Moreover, the record of processing¹² must be adjourned with the relevant details of the data processing related to the management of the reports. The record should contain the name and contact details of the data controller and, where present, the joint data controller, a description of the categories of data subjects and categories of personal data that are processed, the competent authorities to which the such data have been or will be disclosed, etc..

7. DATA RETENTION

In the Decree, it is expressly provided that personal data shall be kept in a form that allows the identification of the data subjects for a period of time not longer than the achievement of the purposes for which they are processed, and that reports and related documentation be retained for as long as necessary for the processing of the report and, in any case,

¹⁰ See ANAC Guidelines, par. 4.1.3 (https://www.anticorruzione.it/documents/91439/146849359/Delibera+n.+311+del+12+luglio+2023+LLGG+WB+versione+unitaria_.pdf/c87e8c07-86d0-baf9-685d-274e2eb6c93e?t=1690552947182).

¹¹ See art. 13, co. 4, of the Decree, as well as articles 13 and 14 of the Reg. (EU) 2016/679

¹² See Art. 30 of the Reg. (EU) 2016/679

no longer than five years from the communication of the final outcome of the procedure.¹³

8. EXERCISE OF DATA SUBJECTS' RIGHTS

The rights referred to in Articles 15 to 22 of the Reg. (EU) 2016/679 may not be exercised by request to the data controller nor by a complaint under Article 77 of the Reg. (EU) 2016/679, if they may result in prejudice of the confidentiality of the whistleblower's identity, within the limits in which this constitutes a measure necessary and proportionate, taking into account the fundamental rights and freedoms of the data subjects.

9. CONCLUSIONS

As discussed in our previous article on the subject matter, the Decree imposes significant compliance burdens on companies regarding the establishment of whistleblowing procedures, with a particular emphasis on criminal law and organizational aspects.

Understandably, stakeholders have focused on meeting these requirements in their rush to comply.

However, as emphasized in this contribution, important privacy measures also need implementation within the same deadline specified in the Decree.

It is crucial not to overlook these measures, and steps should be taken to ensure compliance with them as well.


¹³ See Art. 14, para. 1 of the Decree




Camillo Campi

ASSOCIATE

 c.camp@dejalex.com

 +39 06 809154.1


 Via Vincenzo Bellini, 24
00198 – Roma




Jacopo Piemonte

ASSOCIATE

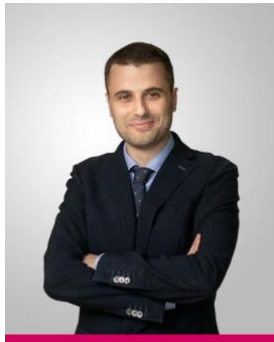
 j.piemonte@dejalex.com

 +39 02 72554.1

 Via San Paolo 7
20121 – Milano

 +32 (0)26455670

 Chaussée de La Hulpe 187
1170 – Bruxelles



Adriano Garofalo

ASSOCIATE

 a.garofalo@dejalex.com

 +39 02 72554.1

 Via San Paolo 7
20121 – Milano

MILANO

Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA

Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES

Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW

Potapovsky Lane, 5, build. 2, 4th floor, office 401/12/9 · 101000, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com