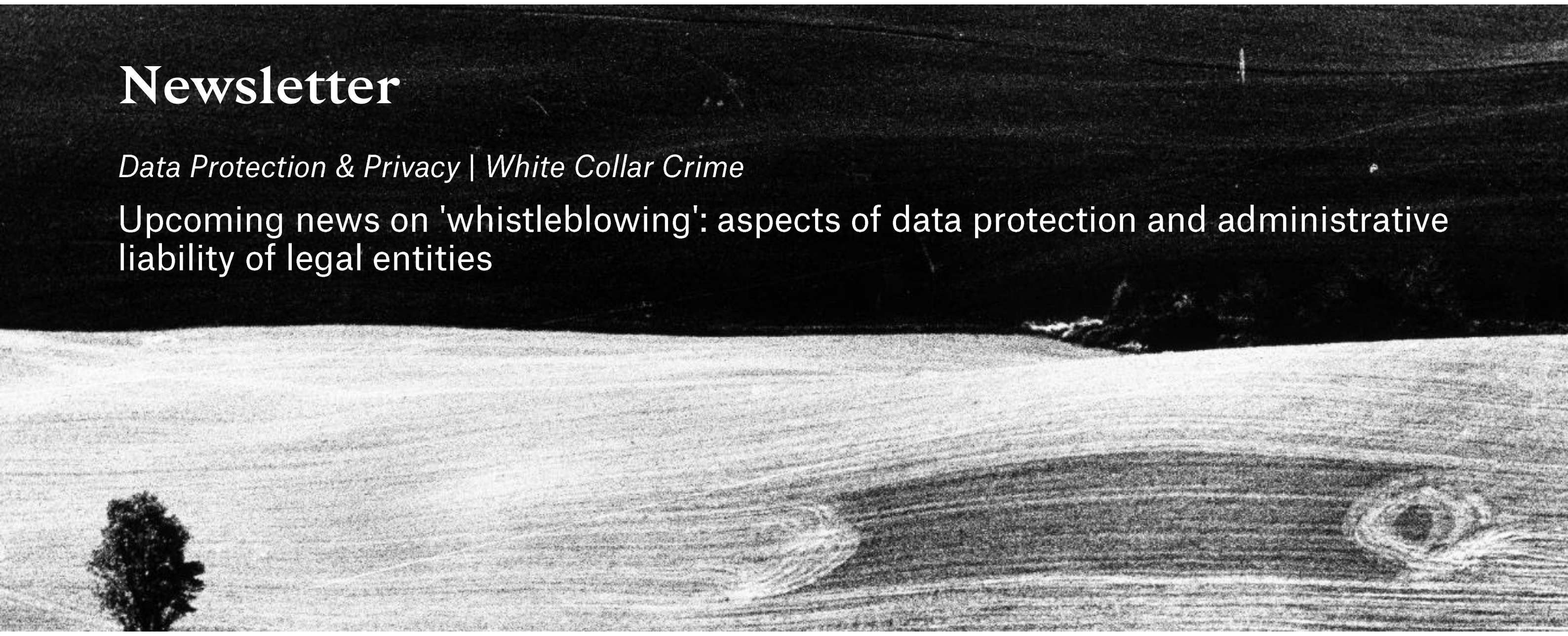
CHIOMENTI



Newsletter

Data Protection & Privacy | White Collar Crime

Upcoming news on 'whistleblowing': aspects of data protection and administrative liability of legal entities

Introduction

On 15 February 2023, Italy was referred to the Court of Justice of the European Union (CJEU) by the European Commission[1], due to its failure to transpose and notify national measures implementing *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* ("**Directive**") by the deadline (*i.e.*, 17 December 2021).

Therefore, the *Draft Legislative Decree implementing Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law and laying down provisions concerning the protection of persons who report breaches of national laws* ("**Draft Decree**") is once again extremely topical. The Draft Decree has been prepared by the Presidency of the Council of Ministers, in the exercise of the legislative delegation conferred on the Government[2], thereupon under consideration by the competent parliamentary committees since 9 December 2022.

Both in Directive and in Draft Decree, confidentiality of identity and protection of personal data are the guiding principles of the *whistleblowing* regulation, with regard to both whistleblowers and other persons involved and/or mentioned in the report.

The Presidency of the Council of Ministers has already consulted the Italian supervisory authority (*Autorità Garante per la protezione dei dati personali* – "**Garante**"). On 11 January 2023, the Garante issued its favourable opinion[3] on the Draft Decree.

---

[1] The other Member States involved are Estonia, Germany, Luxembourg, Poland, the Czech Republic, Spain and Hungary.

[2] Law No. 127 of 4 August 2022, *delegating the Government to transpose European directives and implement other acts of the European Union (European Delegation Act 2021)*, Article 13.

[3] The opinion, adopted at a meeting of the Garante on 11 January 2023, was published on 24 January 2023 and is available on the Garante's website at this link.

A. The new rules on whistleblowing: relations with Legislative Decree 231/2001

The Draft Decree is extremely innovative in that it brings together the - hitherto fragmented - national regulations on so-called *whistleblowing* into a single legal text[4] .The new rules provide for several obligations for entities in the public or private sector and in the framework of which whistleblower reports are made.

In the first place, the Draft Decree is addressed to both public sector entities (e.g., public administrations, independent administrative authorities, public economic entities, public service concessionaires, publicly controlled companies, etc.) and private sector entities that have employed, in the last year, an average of at least 50 employees under open-ended or fixed-term employment contracts, or that - independently of the number of employees employed - fall within the scope of certain European Union acts[5] .

The Draft Decree essentially covers (**i**) internal (so-called intra-company) whistleblowing, (**ii**) external whistleblowing[6] and (**iii**) public disclosures[7] . In order to be able to rely on the latter two channel, certain '*conditions for making the report*' must be met; if these conditions are not satisfied, the whistleblower will not be able to benefit from the protection provided by the present regulation for internal reports (see *below*).

Such a mechanism underlines the legislator's desire to favour intra-company reporting, which will allow the entities to self-manage the reporting on the one hand, and to contain potential negative external impacts on the other.

The scope of the Draft Decree includes all categories of workers, such as employees, self-employed persons, freelancers, as well as volunteers and trainees, including unpaid ones, shareholders, persons with administrative, management, control, supervisory or representative functions in companies, even where such roles are performed de facto (Article 3 of the Draft Decree).

The Draft Decree, moreover, confirm the obligation of how all entities that have adopted a model pursuant to Legislative Decree No. 231 of 8 June 2001 (“**Legislative Decree 231/2001**”) to establish reporting channels: more specifically, it provides that the organisation and management models must include internal reporting channels [8] .

With regard to the changes concerning the private sector, the desire to confirm the strong connection between the company management and control model *pursuant to* Legislative Decree 231/2001 and the whistleblowing regulation is therefore evident within the Draft Decree.

A new aspect is represented by the provisions concerning the communication methods of the reporting channels, where the Draft Decree provides that the information concerning the channel, procedures and prerequisites for making internal - and possibly external - reports must be clearly illustrated by the competent functions of the entities falling within the scope of application and made easily visible and consultable both in the workplace and, more generally, to all those with whom such entities have a legal relationship. In addition, if the entity has its own website - and falls within the scope of the Draft Decree - it must also publish the same information in a dedicated section of its website.

[4] See in particular Article *54-bis* of Legislative Decree No. 165 of 30 March 2001; Article 6, paragraphs *2-ter* and *2-quater* of Legislative Decree No. 231 of 8 June 2001; Article 3 of Law No. 179 of 30 November 2017.

[5] E.g. entities operating in the field of financial products and markets, the prevention of money laundering and terrorist financing, environmental protection and transport safety, etc.) and/or fall within the scope of Legislative Decree No. 231 of 8 June 2001 and adopt the organisation and management models provided for therein (Article 2(p) and (q) of the Draft Decree).

[6] Article 6 of the Draft Decree.

[7] Article 15 of the Draft Decree.

[8] Paragraph 2-bis of Legislative Decree 231/2001. as amended by Article 24 of the Draft Decree.

The Draft Decree also provides for a list of activities functional to the proper and timely management of the internal whistleblowing channel, primarily aimed at allowing the *whistleblower to* be continuously updated on the progress of the report. The person or office responsible for handling internal whistleblowing shall therefore ensure:

- **issuing an acknowledgement of receipt** of the whistleblowing to the reporting person, within 7 days of receipt;
- **maintaining interlocutions** with the reporting person, with the right to ask for additions;
- **diligence in responding** to reports received;
- **a reply to the report** within three months of receipt or, alternatively, from the date of the acknowledgement of receipt.

Lastly, it should be noted that the Italian legislator, in order to foster the *whistleblowing* protections provided for by the Directive, has introduced a further change; the recipients of the relevant obligations have been broaden, by means of a quantitative parameter, irrespective of the adoption of an Organisational and Management Model pursuant to Legislative Decree No. 231/2001.

The Draft Decree establishes a minimum threshold, related to the number of employees, above which the entity must be deemed compatible with the structure required to handle reports of offences/irregularities.

On this basis, the *whistleblowing* discipline is also extended to all other entities which, although they have not adopted a 231 Model, have employed an average of at least 50 employees in the last year.

B. Personal data protection and privacy aspects in the Draft Decree

Within the framework of the GDPR and Legislative Decree 196/2003 ("**Privacy Code**"), the Draft Decree is extremely innovative, as it specifies in detail the data protection and privacy obligations imposed on the public or private entities in the context of which the reports are made, in their capacity as data controllers ("**Data Controllers**").

In particular, the Draft Decree identifies the following fulfilments that Data Controllers will have to consider when reviewing their reporting management model, with a view to complying with the new rules:

- *Ex lege* co-ownership. Stipulation of a co-ownership agreement between the Data Controllers sharing the resources of the system for receiving and handling internal reports, regulating their respective responsibilities.
- Designations. Designation as data processors of any external suppliers processing personal data on behalf of the Data Controllers within the framework of the system at hand, as well as of persons acting under the Data Controller's authority that are expressly authorised to process personal data within the framework of the system.
- *Accountability* and **DPIA.** In accordance with the accountability principle, Data Controllers have an obligation to conduct a data protection impact assessment (DPIA), on the basis of which the model for receiving and handling internal reports shall be defined.
- *Data protection by design*. Configuration of the model for receiving and handling internal reports with specific features to guarantee, by design, the confidentiality and protection of personal data of both whistleblowers and of other persons involved/concerned in the reports, and most notably:
  - **(a)** encryption of reporting channels;
  - **(b)** *ad hoc* training of the staff of the internal office or of the external entity entrusted with the management of the reporting channel;

(c) technical specifications for documenting and storing the reports, as well as for verification, rectification or confirmation of their content by the whistleblower, which differ depending on the method of reporting (*e.g.,* recorded or unrecorded telephone lines/messaging; orally, etc.).

- RIGHTS OF DATA SUBJECTS. Handling of requests to exercise the rights of data subjects (Articles 15-22 GDPR) in accordance with the limitations set out in Article *2-undecies* of the Privacy Code - as amended by the Draft Decree - and, in particular, assessment on whether such exercise may result in actual and concrete prejudice to the confidentiality of whistleblowers.

- CONFIDENTIALITY. In order to protect the identity of the whistleblower, within the general principle that whistleblowers' reports may not be used except for the purpose of giving them appropriate follow-up, the Data Controllers shall:

(a) ensure the confidentiality of the whistleblower’s identity, the content of the report and the related documentation;

(b) ensure that the identity of the whistleblower is not disclosed to persons other than those authorised to do so, except only with the **whistleblower's explicit consent**;

(c) in the context of internal disciplinary proceedings initiated as a result of the report, *(i)* in order to be able to use the report, the prior **explicit consent of the whistleblower** to the disclosure of his/her identity shall be obtained (where the allegation of the disciplinary charge is based, in whole or in part, on the report), while *(ii)* the identity of the whistleblower **cannot be disclosed** where the allegation of the disciplinary charge is based on investigations that are separate and additional to the report;

(d) keep out whistleblowing reports from requests for access to administrative documents and civic access (which concern, in particular, Data Controllers that are public entities);

(e) ensure the above-mentioned safeguards for the identities of other persons involved/concerned in the report.

- MINIMISATION AND STORAGE. Data Controllers shall:

(a) refrain from collecting data that are manifestly not useful for processing a specific report and, if accidentally collected, proceed to their immediate deletion;

(b) keep personal data - in general, the content of reports and the relevant documentation – only for the period strictly necessary for the processing of the report and, in any case, **not exceeding five years** from the date of communication of the final outcome of the reporting procedure (a period deemed appropriate by the Garante, as it is aligned with the average duration of the statutory limitation period provided for the main offences likely to occur).

All of the above is without prejudice to the other obligations imposed on Data Controllers, as arising from the general data protection legislation. In such regard, Data Controllers must also take due account of the **indications provided over the time by the Garante in the decisions issued on whistleblowing matters and related processing of personal data**, a selection of which can be find in the following chart.

- **Injunction orders of 7 April 2022 [9768363] and of 10 June 2021 [9685922]** - The Garante found a breach of principles of integrity and confidentiality, data protection by design and obligations relating to personal data security measures in that the recording and storage in the logs of firewall systems concerned information directly identifying users of the platform.
- **Injunction order of 7 April 2022 [9768387]** - The provider of services relating to computer systems hosting the whistleblowing platform, even when it does not handle IP addresses relating to data subjects using the platform, must be designated as a data processor, since it stores the relevant personal data on its own technological infrastructure (in spite of not having access thereof).
- **Injunction order of 10 June 2021 [9685947]** - The following circumstances are to be deemed non-compliant with data protection laws: (i) the use by more than one person of non-nominal users to access the whistleblowing application and (ii) the use of an application management interface that is accessible from a public network, with a weak (single-factor) computer authentication procedure and without any automatic user-blocking mechanism in the event of repeated failed authentication attempts.
- **Corrective and sanctioning decision of 23 January 2020 [9269618]** - The data controller must not merely transpose the design choices of the whistleblowing application provider, but shall rather adopt appropriate procedures to regularly test, verify and assess the effectiveness of the technical and organisational measures so as to guarantee the security of the processing.
- **Opinion on the draft ANAC Guidelines on whistleblowing of 4 December 2019 [9215763]** - The Garante clarified *inter alia* that data controllers must: (i) provide for the traceability of the accesses and operations carried out on the whistleblowing platform by the persons authorised to process them (but not of those carried out by the whistleblower); (ii) assess, on a case-by-case basis, the adequacy of the authentication systems to access the platform in light of the processing context, including the use of strong authentication techniques; (iii) for access to the platform by users, provide for data transport protocols that are secure both in terms of confidentiality and data integrity (*e.g.*, https protocol).

C. CONCLUDING REMARKS

The Draft Decree, in line with the Directive, introduces a series of innovations and obligations that operators will be called upon to implement, should it be approved.

First of all, the Draft Decree provides that it will be effective:

A) from 17 December 2023, for private-sector entities that have employed, over the last year, an average of not less than 50 and not more than 249 employees under permanent or fixed-term employment contracts;

B) four months from the date of entry into force of the same Draft Decree (*i.e.*, unless otherwise indicated, from the 15th day of its publication in the *Official Gazette* following its future issuance by the President of the Republic), for all other persons included in its scope of application.

Until the above-mentioned effective dates, provisions of the existing whistleblowing legislation[9] will continue to apply.

Below are some preliminary considerations on the initiatives that private-sector entities should appropriately initiate and/or consider implementing the Draft Decree.

[9] See in particular Article 54-*bis* of Legislative Decree No 165 of 30 March 2001; Articles 6(*2-bis*), (*2-ter*) and (*2-quater*) of Legislative Decree 231/2001; Article 3 of Law No 179 of 30 November 2017.

Contacts

Francesco D'Alessandro
Partner – Chiomenti
White Collar Crime
T. + 39 02 72157 676
francesco.dalessandro@chiomenti.net

Marilena Hyeraci
Of Counsel – Chiomenti
Data Protection & Privacy
T. +39. 02721571
marilena.hyeraci@chiomenti.net

Pierluigi Perri
Of Counsel – Chiomenti
Data Protection & Privacy
T. +39.02.721.571
pierluigi.perri@chiomenti.net

Ennio Alagia
Senior Associate – Chiomenti
White Collar Crime
T. + 39 02 72157 828
ennio.alagia@chiomenti.net

Jacopo Baieri
Associate – Chiomenti
Data Protection & Privacy
T. +39. 02 72157 710
jacopo.baieri@chiomenti.net

Francesco Giorgi
Associate – Chiomenti
White Collar Crime
T. +39. 02 72157 544
francesco.giorgi@chiomenti.net

Matteo Leffi
Associate – Chiomenti
Data Protection & Privacy
T. +39. 02 72157 717
matteo.leffi@chiomenti.net