PROCEDURE FOR THE EXECUTION AND MANAGING OF THE BREACHES' REPORTING

INDEX

I – COMMON PROVISIONS

II - EXECUTION OF THE REPORTING

III - MANAGEMENT OF THE REPORTING

I – COMMON PROVISIONS

1. Introduction

Develog has an interest in knowing any breaches that may occur within the organization, in order to effectively remedy it. For this purpose, it invites all the employees to engage freely on any critical issues they should find in their work, sure that Develog will not retaliate against them.

However, where there is the intention to keep its own identity confidential and/or a fear of retaliation by other members of the organization, Develog permits to make protected reports according to the procedures laid down by this document.

2. Purpose

This document has the purpose to regulate the procedures for making and managing of reports of breaches of national or European rules that damages the public interests or Develog's integrity, as well as protection measures of whistleblowers.

3. Recipients

This document applies to Develog's employees and, due to a specific contractual clause, to all those who maintain dealings with the Company of self-employment, collaboration and professional counselling, as well as to all persons who offer their activities in Develog.

Moreover, this document applies to the Develog' stakeholders and to all the persons who carry out functions of administration, management, control, supervision or representation of the Company, even de facto,

4. Adoption

The adoption and updating of this document belong to the Governing Body, after consultation of the company union representatives or trade union organizations referred to in art. 51 d.lgs. 81/2015, when available, in relation to the internal reporting channel identified[1].

5. Communication and disclosure

This document is brought to attention of the employees when adopted, in case of update and in any case during the recruitment and selection process.

This document is exposed and made easily accessible to employees via posting in a network folder.

On the Company's website are published clear information on channel, procedures and requirements in order to make internal and external reports.

The aforementioned requirements fulfil the information burden of the internal reporting channel manager[2].

6. Normative references

- Legislative decree 8 June 2001, n. 231, concerning « Rules governing the administrative liability of legal persons, companies and associations, whether or not having legal personality, in accordance with article11 of law 29 September 2000, n. 300»;
- Directive (UE) of the European Parliament and the Council of the European Union of 23 October 2019, n. 1937, on the protection of persons who report breaches of Union law;
- Legislative decree 10 March 2023, n. 24, concerning «Implementation of 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 and on the provisions about the protection of persons who report breaches of national legislation»;

[1] Art. 4 comma 1 d.lgs. 24/2023.
[2] Art. 5 comma 1 lett. *e* d.lgs. 24/2023.

- Regulation (UE) of the European Parliament and the Council of 27 April 2016, n. 679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;
- Legislative decree 30 June 2003, n. 196, Italian data and information protection law;
- ISO 37002:2021 - *Whistleblowing management systems - Guidelines*.

In the footnotes of this document are indicated the regulatory references from which the respective forecast are taken.

7. Definitions

In order to this document, are intended for:

a) «public disclosure»: to put information into the public domain about breaches through the press or electronic means or in any case through means of distribution able to reach a large number of people;
b) «manager»: entity responsible for receiving and managing reports made through Develog's internal reporting channel;
c) «private information»: information covered by the duty of confidentiality, copyright and personal data protection;
d) «compliance program»: compliance program adopted by Develog according to the d.lgs. 231/2001;
e) «connected people»:
   1) persons working in the same work-related context who assist the whistleblower in the reporting process (e.g.: facilitators);
   2) persons of the same workplace connected to the whistleblower with a stable affective bond or up to the fourth degree of kinship;
   3) colleagues who work in the same whistleblower's workplace and who have an habitual and current relationship with him;
   4) entities owned by the whistleblower, for which the whistleblower works or which operate in the same whistleblower' work-related context (e.g.: company belonging to the same corporate group);
f) «feedback»: communication to the whistleblower of information related to the follow-up on the reports given or intended to be given;
g) «retaliation»: any behaviour, act or omission, even just tempted or threatened, committed on the basis of the report, the complaint to the Authority or the public disclosure and which causes or is likely to cause an unjust damage, directly or indirectly, to the whistleblower or to the person who made the complaint;
h) «whistleblower»: natural or legal person carried out the report or the public disclosure about breaches acquired within the workplace;
i) «reported person»: natural or legal person mentioned in the internal or external reporting or in the public disclosure as the person to whom the reporting is attributed or as person however involved on the breaches reported or publicly disclosed;
j) «reporting made in bad faith» or «reporting in bad faith»: reporting made by the whistleblower that hasn't compelling reason for considering that the information on the breaches reported, complained of or disclosed, at that moment, was true
k) «follow-up»: the action taken by the entity that manages the reporting channel for assessing the existence of reported facts, the outcome of investigations, and any measures taken.

8. Penalties

The violations of this procedure assume disciplinary significance and will be penalised as required by the internal disciplinary system. For example, constitutes a punishable violation:

a) the execution of reporting in bad faith;
b) the execution of reporting of which the Judicial Authority has ascertained the defamatory or slanderous character[3];
c) the revelation of the whistleblower, the collected person and any other information from which their identity may be found;
d) any behaviour to obstruct reporting;
e) the attempt to identify the whistleblower[4];

[3] Art. 16 comma 3 d.lgs. 24/2023.
[4] UNI ISO 37002, § 8.4.2.

f) the failed management of reporting for fraud or gross negligence, including the failure remedy to breaches or retaliation reported, by those who have the powers;
g) adoption of retaliation behaviour.

The violations of this procedure by third parties, not employed by the company, may be sanctioned due to a specific contractual clause.

II – EXECUTION OF THE REPORTING

9. Object of the reporting

According to the methods indicated in this document, the breaches or the risk of a breach[5] of national or European laws that infringe the public interest or Develog's integrity can be reported[6]. In particular:

a) illegal conduct relevant in accordance with d.lgs. 231/2001;
b) breaches of the Compliance program, including any retaliation suffered for making a report.

In the framework of this documents the disputes, claims or requests related to a personal interest of the whistleblower, that pertain exclusively to their work relationships or their relationships with the hierarchically higher figures[7], are excluded. Such representations may be communicated in standard form to the relevant company representatives.

However, unfounded reports effectuated intentionally or by gross negligence are forbidden[8]. In these cases, the protection measures, provided in this document, will be not recognized to the whistleblower and it will be applied a penalty, in according to the provisions of the disciplinary system.

10. People entitled to reporting

Reports can be made by those who maintain or have maintained work relationships with Develog[9]. In particular:

a) employees;
b) self-employed persons;
c) collaborators;
d) freelancers or consultants;
e) volunteers and trainees;
f) stakeholders;
g) persons with administration, direction, control, supervision or representation function.

Reports may be made also before and regardless of the establishment of employment relationship, where they concern information acquired during trial and/or selection period[10].

11. Protection measures of the whistleblower

Whistleblower and connected people receive protection by this document, as long as the reporting has been made in good faith and, in case of external reporting or public disclosure, if proper conditions exists[11].

The reasons inducing the person to report are irrelevant for the purpose of its protection[12].

Protection measures are applied also in cases of anonymous reporting, even if the whistleblower was later identified and has suffered retaliation[13].

11.1. Privacy of the whistleblower's identity

The whistleblower's identity is never revealed, without his express consent, to any person other than those competent to receive or follow-up the report[14]. This does not apply if, after the outcome of the assessment held by the manager, it is ascertained that the whistleblower has made the report in bad faith or has its own liability for the reported breach, also together with other people.

[5] UNI ISO 37002, Introduction.
[6] Artt. 1-3 d.lgs. 24/2023.
[7] Art. 1 comma 2 d.lgs. 24/2023.
[8] Art. 16 comma 1 lett. *a* e comma 3 d.lgs. 24/2023.
[9] Art. 3 commi 3-4 d.lgs. 24/2023.
[10] Art. 3 comma 4 lett. *a* e *b*.
[11] Art. 16 comma 1 d.lgs. 24/2023.
[12] Art. 16 comma 2 d.lgs. 24/2023.
[13] Art. 16 comma 4 d.lgs. 24/2023.
[14] Art. 12 comma 2 d.lgs. 24/2023.

The same privacy is guaranteed for any other information from which it is possible to deduce the whistle-blower's identity.

11.2. Prohibition of retaliation

The whistleblower cannot suffer any retaliation for reporting[15].

By way of example, constitute retaliation[16]:

a) suspension, lay-off, dismissal or equivalent measures;
b) demotion or withholding of promotion;
c) transfer of duties, change of location of place of work, reduction in wages, change in working hours;
d) withholding of training or any access restriction to the same;
e) negative performance assessment or negative employment reference;
f) adoption of any disciplinary measure or other penalty, including a financial penalty;
g) coercion, intimidation, harassment or ostracism;
h) discrimination, disadvantageous or unfair treatment;
i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
l) failure to renew or early termination of a temporary employment contract;
m) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
n) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
o) early termination or cancellation of a contract for goods or services;
p) cancellation of a licence or permit;
q) psychiatric or medical referrals.

The prohibition of retaliation applies also to the connected people[17].

11.3. Protection against retaliation

The possible retaliation suffered by whistleblower may be communicated to ANAC, that informs the National Labour Inspectorate for the provisions in its scope[18].

The acts of retaliation are void and the whistleblower and connected people have the right to terminate the retaliatory conduct, to receive indemnification of damages and, in case of dismissal, to be reinstated[19].

In the context of the related dispute made by the whistleblower, who claims to have suffered a retaliation for reporting, the employer must prove that the act believed retaliatory is motivated by other legitimate reasons, unrelated to the report[20].

Waivers and settlements, total or partial, which have as their object the rights and protections provided for in this document, are valid only if made in one of the seats laid down in art. 2113 co. 4 c.c. (e.g.: Territorial Labour Inspectorate; Certification Commission; Registered Office; etc.)[21].

11.4. Limitations of liability

If in the case of reporting it becomes necessary to reveal information that are confidential or offensive to the company's reputation, any whistleblower's or connected person's penal, civil and administrative liability[22] is excluded, as long as the information are related to the report and strictly necessary to disclose the breach[23].

[15] Art. 17 comma 1 d.lgs. 24/2023.
[16] Art. 17 comma 4 d.lgs. 24/2023.
[17] Art. 17 comma 1 d.lgs. 24/2023.
[18] Art. 19 comma 1 d.lgs. 24/2023.
[19] Art. 19 commi 3 e 4 d.lgs. 24/2023.
[20] Art. 17 commi 2 e 3 d.lgs. 24/2023.
[21] Art. 22 d.lgs. 24/2023.
[22] Art. 20 commi 1 e 2 d.lgs. 24/2023.
[23] Art. 20 comma 4 d.lgs. 24/2023.

In any case, reports must concern information that are legally acquired[24].

However, reporting does not exempt the whistleblower from any liability in connection with the breaches reported[25].

11.5. Measures of support

A list of Third sector entities is instituted at ANAC, providing with measures of support (consisting in information, assistance and consulting for free on reporting, on protection against retaliation, on rights of the person concerned and on the procedures and requirements for access to legal aid[26]) to whistleblowers.

12. Internal reporting

Reports may be made in the following ways[27]:

a) in written form, through the online platform "https//Develog.Segnalazioni.net";
b) in oral form, at the request of the whistleblower, through a direct contact with the manager of the reporting channel[28] in a place that guarantees privacy[29].

Regardless of the way chosen, the confidentiality of the whistleblower' identity, the content of the report and its documentation are guaranteed in any case.

[24] Art. 20 comma 3 d.lgs. 24/2023.
[25] Cass. civ., sez. lav., ord. 31 marzo 2023, n. 9148.
[26] Art. 18 d.lgs. 24/2023.
[27] Art. 4 comma 1 e 3 d.lgs. 24/2023.
[28] Art. 4 comma 3 2° periodo d.lgs. 24/2023.
[29] UNI ISO 37002, § 8.2.

III – MANAGEMENT OF THE REPORTING

13. Entity in charge of the management of the reporting

Receiving and managing of reports regulated in this document are handled by the Supervisory Body[30].

Report presented to a non-competent entity to receive it is transmitted by the latter within 7 days of its receipt to the manager of the reporting channel, with contextual notice about the transmission to whistleblower[31].

14. Receipt and taking charge of the reporting

In-person meeting[32]

With the consent of the whistleblower, the manager documents the report through registration on a device suitable for storage and listening or through minute, the content of which must be subjected to whistleblower for any changes and subscription.

Anyway, having received the reporting, the manager releases to whistleblower an acknowledgment of receipt within 7 days of its receipt[33]. The acknowledgement of receipt will include, among other things[34]:

a) reassurance and request on the preferred ways for the continuation of discussions (e.g.: reporting is made online, but the whistleblower prefers to continue in person);
b) information on successive stages of the management process, related timing and possible outcomes (e.g.: what further feedback to expect and when);
c) information, also through referral to this procedure, on measures adopted to protect the whistleblower, including measures to protect his identity, as well as on responsibilities for loyal cooperation of the whistleblower and for effective consideration and protection by the entity.

The manager gives diligent following to the report[35] and feedback to the whistleblower within 3 months of its acknowledgment of receipt and in any case within 3 months and 7 days of the report receipt[36].

If the investigations cannot be completed immediately, for example because they are particularly complex, within the same timeframe the manager updates the whistleblower on the status of the report and advises him on the further necessary timeframe to complete it[37].

15. Preliminary evaluation of the reporting

The manager carries out a preliminary investigation of the reporting in order to verify if it concerns any violation or retaliation belonging to the objective and subjective area of application of this procedure[38].

If the manager decides that the reporting does not fit within the area of application of this procedure, he gives notice to whistleblower, specifying the reasons and indicating the internal office that may eventually be competent to manage the problem reported. In order to close the report, the manager prepares a specific "report" for the Governing Body and keeps track anonymised in the Register of the reporting.

If, otherwise, the manager considers that the reporting falls within the scope of this procedure, he continues to the establishment of the breaches reporting as provided below.

16. Request of additional investigation

Where not already present in the reporting, the manager asks to the whistleblower the following information[39]:

[30] Art. 4 comma 2 d.lgs. 24/2023.
[31] Art. 4 comma 6 d.lgs. 24/2023.
[32] Art. 14 comma 4 d.lgs. 24/2023.
[33] Art. 5 comma 1 lett. *a* d.lgs. 24/2023.
[34] UNI ISO 37002, § 8.1.
[35] Art. 5 comma 1 lett. *c* d.lgs. 24/2023.
[36] Art. 5 comma 1 lett. *d* d.lgs. 24/2023.
[37] UNI ISO 37002, § 8.2.
[38] UNI ISO 37002, § 8.3.1, primo punto dell'elenco Nota.
[39] UNI ISO 37002, § 8.2.

- Where did the breach take place?
- When does the breach verify (past, present, future, ongoing)?
- Who is involved in the breaches?
- Did you have already reported previously? If yes, what, when and to whom? What actions were taken?
- What is the effect for the company, from your point of view?
- Is the company's management involved or aware of the breach?
- Do you fear a risk for you or others?
- Do you have any documents or other proof to support your reporting?
- Is there anyone else who is directly aware of the breach that we can contact?
- Has anyone tried to hide the breach or discourage you from sharing your concern? In this case, who and how?

17. Prioritization of the reporting managing (so-called triage)

In the presence of several reporting to be managed simultaneously, the manager assesses the emergency based on the probability of the breach and its possible impact over the company, taking into account the following factors[40]:

- Can the violation be considered criminal?
- Has the breach already happened, is it ongoing or is it about to happen?
- Is there an immediate need to stop or suspend business?
- Is there an immediate health and safety risk?
- Is there an immediate risk to human rights or the environment?
- Is there a need to insure and protect evidence before it is erased or destroyed?
- Is there a risk to the functions, services and/or reputation of the entity?
- Can reporting have an impact on business continuity?
- What media impact can the reporting have?
- Is there any additional information to support the reporting?
- What is the nature of the offence (e.g.: type and frequency of the infringement; role and seniority of the parties involved in the report; etc.)?
- What is the probability that the breach will also be reported outside the institution?
- Has the breach been reported before?
- How did the whistleblower obtain the information: is the information "first-hand" or "hearsay"?

18. Assessment of the breach reporting

The manager proceeds to the assessment of the breach reporting through the fulfilment of one or more of the following activities[41]:

a) involvement of competent business functions to support the assessment, unless this would compromise the confidence of the whistleblower, the impartiality of the manager or the successful outcome of the investigation;
b) collection of documentary evidence to support the alert;
c) interview with people who are able to report information relevant to the detection of the violation;
d) interview of the reported person, previously informing him about the object of the meeting and the possibility of being represented by a person of confidence, to which the manager must necessarily provide in case of a request from the latter, including by the acquisition of written observations and documents[42].

The manager documents in writing the interviews made by means of a specific minute, the content of which must undergo to the interviewee for any changes and subscription.

During the assessment, the manager maintains the interlocutions with the whistleblower and, if necessary, may request supplements[43] to the latter.

[40] UNI ISO 37002, § 8.3.1.
[41] UNI ISO 37002, § 8.3.1.
[42] Art. 12 comma 9 d.lgs. 24/2023.
[43] Art. 5 comma 1 lett. *b* d.lgs. 24/2023.

In any case, the manager shall protect the identity of the persons involved and mentioned in the reporting, until the conclusion of the investigation[44].

19. Risk of retaliation assessment and prevention

The manager shall assess the risk of retaliation for the whistleblower on the basis of the following factors [45]:

- What is the likelihood of confidentiality being maintained? For example: is anyone else aware of the breach? Has the breach been reported to anyone else? Can the nature of the information reveal their identity? Are they the only ones who have access to the information? Does the infringement constitute an offence whose evidence requires the identity of the person who has given it to be revealed?
- Is the whistleblower concerned about retaliation? Has there been any retaliatory action or is there an imminent risk of retaliation?
- Is the whistleblower involved in the breach or did he suffer it?
- Is the reporting about different types of violations?
- How did the whistleblower obtain information about the breach?
- What is the relationship between the whistleblower and the breach to which the reporting relates?
- What is the relationship between the whistleblower and the institution?

The level of protection and the actions taken depend on the type and timing of reporting and the potential consequences of the breach.

If the manager does not have the power to develop and implement strategies to prevent any damage to the whistleblower (e.g.: internal reorganisation of personnel), it shall inform the person concerned in order to allow the whistleblower to give his consent to disclosure of his identity to those within the institution who have that power, without prejudice to the other safeguards provided for in this procedure in the event that retaliation is subsequently effectively implemented.

20. Outcome of the checks out by the manager

The manager concludes the reporting management process by issuing a Report addressed to the Governing Body, in which he reports the management process of the reporting and the outcome of the investigations carried out with reference to:

a) the absence of the reported breach or retaliation, specifying whether the reporting is deemed to have been issued in bad faith for the purpose of the possible application of the disciplinary sanction against the whistleblower;
b) the existence or risk of the occurrence of the reported breach or retaliation, specifying the person held responsible and the elements collected.

The Report must not mention the identity of the whistleblower and other information to identify him, except in cases of reporting in bad faith or deemed to be the responsibility of the whistleblower for the established breach.

21. Action resulting from the investigation of the violation or retaliation

The Governing Body evaluates the content of the Report and takes appropriate action on the outcome of the checks carried out by the Manager. In particular:

a) in case of incomplete investigation carried out by the manager, it carries out further investigations, including through the competent corporate functions, a legal counsel or an external consultant;
b) in case of a breach or risk of breach, it takes appropriate measures to prevent, stop or remedy the breach, as well as appropriate disciplinary measures against any person deemed liable for the breach;
c) in case of a deemed existence of material risk of retaliation, it takes appropriate measures to protect the signaller (e.g.: internal reorganisation of staff);
d) in case of established retaliation, carried out or even threatened against the whistleblower, it takes appropriate measures to remedy the retaliation suffered[46] (e.g.: reinstatement of the signalman in the previous

[44] Art. 12 comma 7 d.lgs. 24/2023.
[45] UNI ISO 37002, § 8.3.2.
[46] UNI ISO 37002, § 8.4.3.

position), as well as appropriate disciplinary measures against any person held responsible for the retaliation;

e) in case of deemed bad faith of the whistleblower when reporting, it takes appropriate disciplined measures against the signaller.

The Governing Body shall communicate the actions taken to the Manager in order to give timely feedback to the report and regularly monitor the effectiveness of the measures taken.

The management process of the report ends with the communication to the whistleblower about the outcome of the investigations carried out and any actions taken accordingly by the Governing Body.

22. Disciplinary procedure consequent the reporting

In the framework of the disciplinary procedure intended to sanction the reported breach, the identity of the whistleblower will not be revealed without his express consent, even if knowledge of his identity is indispensable for the defence of the reported person[47].

In order to enable him to give his consent, if any, the manager informs the whistleblower in writing of the reasons for the disclosure of the confidential data [48].

23. Processing of personal data

The activities of receipt and management of reporting involve the processing of personal data, which is implemented and organized by Develog, in its capacity as Data Controller, in compliance with the applicable law and guaranteeing data subjects, on the basis of what is applicable to such processing, the exercise of its rights under artt. 15-22 reg. (UE) 2016/679.

The Supervisory Body is authorised to process personal data, on the basis of a special letter of recognition containing an indication of the confidentiality obligations that must be respected in the performance of the channel management function.

Responsible for the processing of personal data pursuant to art. 28 reg. (EU) 2016/679 is DigitalPA, on the basis of a formal designation in writing.

The information on the processing of personal data resulting from the receipt and management of reports is available to all interested parties on the company website and, for internal staff, also in network folders.

24. Storage of documentation inherent to reporting

Reporting is not used beyond what is necessary to give adequate follow-up. In particular, unnecessary personal data for the processing of a specific report, where possible, are not collected and, if collected accidentally, are deleted immediately.

The manager keeps the reporting and related documentation for the time necessary to process them and, however, not to exceed 5 years from date of notification of the final outcome of the reporting procedure[49].

In order to give evidence of the effective implementation of the system, the manager keeps an anonymous record of the reporting received and managed in a dedicated Record of reporting, in which it indicates for each of them, the subject of the report, the timing of management, the outcome of the investigation and any subsequent actions, without any reference to the persons involved.

[47] Art. 12 comma 5 d.lgs. 24/2023.
[48] Art. 12 comma 6 d.lgs. 24/2023.
[49] Art. 14 comma 1 d.lgs. 24/2023.