



International Employment Lawyer

Guide to Whistleblowing

Croatia



Contributor:

**BABIĆ &
PARTNERS**

LAW FIRM

Croatia



Marija Gregoric and
Matija Skender
Babić & Partners

Legal basis for whistleblowing

1. Which body of rules govern the status of whistleblowers?

In Croatia, the status of whistleblowers and whistleblower protection (WBP) is governed by the Act on the protection of persons who report irregularities (WBP Act). The WBP Act came into force on 23 April 2022 and replaced the previous Croatian WBP legislation of 2019, introducing amendments to implement Directive (EU) 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law (the Directive).

Implementation of the whistleblowing procedure

2. Which companies must implement a whistleblowing procedure?

Under the WBP Act, a whistleblowing procedure must be implemented by:

- any company falling within the scope of EU acts referred to in Part I.B and Part II of the Annex to the Directive, regardless of the number of employees employed by the company; and
- any company employing 50 or more employees.

Under unofficial interpretations by the officials of the Croatian Ministry of Justice and Public Administration (the Ministry), where applicable, the headcount threshold should take into account only persons employed with the company (ie, persons engaged by the company based on an employment contract) and ordinarily working for the company anywhere in the world (ie, it does not include persons engaged otherwise, such as temporary agency workers or persons engaged by the company's group company).

To implement the whistleblowing procedure, the company must adopt a whistleblowing policy establishing procedural rules and appoint a person competent for receiving and following up on whistleblowing reports, communicating with the whistleblowers and conducting the protection procedure in connection with the whistleblowing report (WBP officer) and their deputy.

3. Is it possible to set up a whistleblowing procedure at a Group level, covering all subsidiaries?

Yes, it is possible to have a whistleblowing procedure applicable at a Group level, but only in addition to an internal reporting channel. This is because the WBP Act states that each company must have its own internal reporting channel (meaning a WBP

officer and their deputy appointed by the company). However, neither the Directive (as interpreted by the European Commission) nor the WBP Act prohibits the company from having a separate central reporting channel at a Group level, provided that such a channel is available in addition to (co-existing with) a reporting channel set up under Croatian law.

4. Is there a specific sanction if whistleblowing procedures are absent within the Company?

Yes, a failure by the company to adopt or implement an internal whistleblowing policy by 23 June 2022, or appoint a WBP Officer and their deputy by 23 July 2022 may each result in liability for an administrative offence and a related fine, which may be up to about 4,000 EUR for the company, and up to about 1,350 EUR for the responsible individual within the company.

5. Are the employee representative bodies involved in the implementation of this system?

Yes, the involvement of employee representative bodies (the works council or, if there is no works council, a union trustee), provided that any such body exists with the company, is two-fold:

- the company must consult with the works council or union trustee regarding adoption of the whistleblowing policy – failure to do so would result in the adopted whistleblowing policy being null and void; and
- the company must appoint the persons requested by the works council or union trustee as the WBP Officer and deputy; if no such request is made by the works council or union trustee, the company may appoint the WBP Officer and deputy at its discretion.

6. What are the publicity measures of the whistleblowing procedure within the company?

The WBP Act does not contain rules on how the whistleblowing policy should be communicated to employees and other eligible whistleblowers, other than stating that the policy should be easily accessible to all persons within the work environment (as defined in question 12), understandable, and effective in encouraging the primary use of internal reporting channels or systems for reporting breaches or irregularities. In light of this, the publication of the whistleblowing policy should be made following the provisions of Croatian labour legislation.

Under the Croatian Employment Act and implementing regulations, any employment-related policy (which would include the whistleblowing policy) must be signed by the management of the company and published on a bulletin board in the company's premises (specifically stating that the policy will come into force on the ninth day after publication, at the earliest). It is recommended that all eligible whistleblowers (ie, both employees of the company, and persons not employed by the company) are notified of the company having in place a whistleblowing policy and that they can receive a copy of such policy upon their request.

7. Should employers manage the reporting channel itself or can it be outsourced?

Under the WBP Act, the internal reporting channel is a WBP officer and their deputy, as appointed by the company. This officer and deputy are solely authorised to receive the whistleblowing reports and conduct investigations (ie, the

conduct of these actions cannot be outsourced to any third person).

However, the WBP Act does not preclude companies from appointing individuals employed or hired by an external service provider as a WBP officer or deputy (noting, however, that the company may make such appointment at its own discretion only if these appointments have not been proposed by either the works council, or, if there is no works council, the union trustee, or if there is no works council or union trustee, by at least 20% of the company's employees).

Even if the company appoints individuals employed or hired by an external service provider, the appointed persons must keep confidential the identity of any whistleblowers and any information contained in the whistleblowing report, and will not be able to directly involve external service providers in the investigation without express consent from each whistleblower. However, the company may engage an external service provider to indirectly assist these appointed persons (regardless of whether the individuals appointed are employed by the company or by the external service provider, and regardless of whether the whistleblower provides express consent for disclosure of his or her identity and the content of the report), if such assistance will not lead to disclosure to that provider of the identity of the whistleblower and any information contained in the whistleblowing report.

8. What are the obligations of the employer regarding the protection of data collected related to the whistleblowing procedure?

The WBP Act does not provide for any specific obligations concerning the protection of data collected related to the whistleblowing procedure, other than that any processing of personal data must be carried out under EU and national laws regulating the protection of personal data.

In light of this, the record-keeping of collected data must be conducted in a way that access to records is restricted to authorised persons (ie, the WBP officer and their deputy) and that appropriate measures concerning the storage of documents (for example storage cabinets with locks and password-protected databases) are taken to prevent unauthorized access. The retention period has not been specified by either the WBP Act or any guidelines or regulations issued by the competent authorities. Consequently, it is advisable that the retention period is provided in the WBP policy and that the collected data is retained for no longer than five years since receipt of the report or until completion of any legal proceedings associated with the report, whichever is longer.

9. What precautions should be taken when setting up a whistleblowing procedure?

The following precautions should be taken into account by the company when setting up a whistleblowing procedure:

- Language of the whistleblowing policy – even though the WBP Act does not explicitly provide that the whistleblowing policy must be available in Croatian, the WBP Act requires that information on the internal whistleblowing procedure must be easily accessible, understandable and effective. If the whistleblowing policy is not prepared in Croatian, the company may run the risk of: the employee claiming that he or she did not properly understand the policy; or in the case of inspection or dispute, the inspection body or court

holding that a policy made only in English, or a language other than Croatian, is null and void as not being easily understandable.

- Appointment of WBP officer and deputy – given that a company must appoint a WBP officer and their deputy at the request of either the works council, union trustee, or 20% of employees of the company (if there is neither a works council nor union trustee), it is advisable that the company provides in the whistleblower policy that any candidate should be a person of trust and competent to conduct the duties of a WBP officer.
- WBP officer's resources – the company must ensure that the WBP officer and their deputy have the resources required to effectively perform their duties, such as providing the officer with a personal computer or laptop and a separate email address for receiving whistleblowing reports, a direct telephone line for receiving whistleblowing reports, a dedicated office for conducting meetings with whistleblowers, and equipment for keeping records of reports.

Scope of the whistleblowing procedure

10. What precautions should be taken when setting up a whistleblowing procedure?

The material scope of the WBP Act encompasses the following breaches or violations (under the WBP Act they are named "irregularities"):

- related to the scope of application of the EU Acts listed in Part I of the Annex to the Directive;
- affecting the financial interests of the EU, as stated in article 325 of the Treaty on the Functioning of the European Union and further defined by relevant EU measures;
- relating to the internal market, as stated in article 26(2) of the Treaty on the Functioning of the European Union, including breaches of EU rules on competition and state aid, and breaches of corporate tax rules or arrangements to create a tax advantage contrary to the applicable corporate tax legislation; and
- relating to other rules of Croatian law, the breach of which undermines the public interest.

The WBP Act defines the term "irregularities" as actions or omissions that are unlawful and relate to or are incompatible with the goal or purpose of the above-stated legislation.

11. Are there special whistleblowing procedures applicable to specific economic sectors or professional areas?

Yes, the WBP Act specifically excludes its application in the matters of defence and national security, except where such matters are covered by Union acts listed in Part I of the Annex to the Directive. Furthermore, the governmental bodies competent for matters of defence and national security must regulate the protection of whistleblowers and the reporting procedure in the areas of key security and defence interests (specifically the protection of key security and defence interests). To our knowledge, there are still no adopted or publicly available regulations covering WBP and reporting procedures in the areas of key security and defence interests.

In addition, if the Union acts listed in Part II of the Annex to the Directive provide for separate rules on reporting irregularities, the WBP Act restricts its application only to matters that have not been regulated by such separate rules.

Identification of the whistleblower

12. What is the legal definition of a whistleblower?

Under the WBP Act, a whistleblower is defined as a natural person who reports or publicly discloses irregularities that he or she has learned of within his or her work environment, whereas the term work environment is defined as professional activities in the public or private sector, irrespective of the nature of such activities, within which the whistleblower acquires information on irregularities and within which the whistleblower could suffer retaliation if they reported such irregularities, including when such activity has ceased in the meantime, should start or should have started.

13. Who can be a whistleblower?

Any person that acquires knowledge of or information on irregularities within their work environment and reports such irregularities under the prescribed reporting procedure may be considered a whistleblower. This includes:

- persons within an employment relationship;
- persons with the status of a self-employed person;
- holders of stocks in a joint-stock company or holders of shares in a limited liability company, as well as persons who are members of the administrative, management or supervisory body of a company, including non-executive members, volunteers, and paid or unpaid interns;
- persons working under the supervision and direction of contractors, subcontractors and suppliers; and
- persons that in any way participate in the activity of the legal or natural person.

14. Are there requirements to fulfil to be considered as a whistleblower?

Yes, persons reporting or publicly disclosing irregularities will be considered to be whistleblowers if they:

- had a legitimate reason to believe that what they report or publicly disclose is true at the time of making the report or disclosure;
- had a legitimate reason to believe that the information falls within the scope of the WBP Act; and
- make the report or public disclosure as per the rules set by the WBP Act.

15. Are anonymous alerts admissible?

Yes, anonymous whistleblowing reports are admissible, but the company is not legally required to investigate an anonymous report. This is because the WBP Act states that a whistleblowing report must contain information on the identity of the whistleblower, and the company may deem that an anonymous report does not represent a qualifying whistleblowing report. In any case, the WBP Act extends its protection to persons who submitted an anonymous report if the identity of that person becomes known.

16. Does the whistleblower have to be a direct witness of the violation that they are whistleblowing on?

No, the WBP Act expressly provides that the information on the irregularities (i.e., breaches/violations) contained in the whistleblowing report may also include reasonable doubt on actual or potential irregularities that occurred or are very likely to occur, or on attempts to cover-up such irregularities.

Processing of the whistleblowing procedure

17. What are the terms and conditions of the whistleblowing procedure?

The whistleblowing procedure must be regulated by a whistleblower policy adopted by the company. In practice, the policy should include provisions regulating eligible whistleblowers; methods of reporting; the content of the whistleblowing report; the procedure for submitting, following up on and investigating the whistleblowing report with all applicable deadlines; and the appointment of a WBP officer and a deputy.

- Eligible whistleblowers - please see answers to questions 12 and 13;
- Methods of reporting - the whistleblowing report may be submitted either in writing (including e-mail communication) or verbally (meaning via a telephone call or voice message, or in a physical meeting if so requested by the whistleblower);
- Content of the whistleblowing report - the whistleblowing report should contain information on the identity of the whistleblower, information on the reported body or person (ie, the body or person who committed irregularities), and information on the irregularities.
- Procedure for submitting, following up on and investigating the whistleblowing report – after receiving the report, the WBP officer or their deputy must:

1. acknowledge receipt of the report within seven days;
2. without delay undertake actions within the officer's competence as required to protect the whistleblower;
3. undertake actions required to investigate the reported irregularities and provide feedback to the whistleblower generally within 30 days, but in no case later than 90 days from the date of acknowledgement of receipt of the report, or if no acknowledgement was sent to the whistleblower, 90 days from the end of the seven-day period after the report was made;
4. without delay, forward the report to competent authorities for further processing if the irregularities have not been resolved in cooperation with the company;
5. without delay, notify the whistleblower in writing of the outcome of the investigation;
6. notify in writing the authority competent for external reporting on received reports within 30 days of a decision on the report;
7. keep confidential the identity of the whistleblower and all information contained in the report as required by the law; and
8. provide clear and easily available information regarding the procedure for submitting a report to the competent authority for external reporting and, as appropriate, institutions, bodies, offices or agencies of the European Union competent to take further action following the content of the report;

- Appointment of a WBP officer and a deputy – the company must appoint a WBP officer and deputy at the request of a works council. If there is no works council, then a union trustee would make the request. If there is no works council or union trustee, then 20% of employees of the company would make the request. The appointed officer and deputy must provide written consent for the appointment. If any of the above does not request the appointment of an officer or deputy, the company may make the appointment at its

discretion. If the WBP officer and deputy are appointed, and at any time the works council, union trustee or the abovementioned proportion of employees make a written request to the company proposing that any other persons be appointed as WBP officer and deputy, the company must make the necessary replacements.

18. Is there a hierarchy between the different reporting channels?

No, there is no hierarchy between the internal and external reporting channels, meaning that a whistleblower is completely free to choose whether to make a report internally or externally. On the other hand, the whistleblower may only publicly disclose irregularities if:

- the whistleblower already submitted an external whistleblowing report (regardless of whether they first submitted an internal report), but no appropriate measures were undertaken in response to the report; or
- the whistleblower did not submit an external whistleblowing report but has reason to believe that:
 1. the irregularity represents an immediate and obvious danger to the public interest, for example in case of a crisis situation or risk of irreparable damage; or
 2. if submitting an external whistleblowing report, there is a risk of retaliation or the prospect of the issue being remedied is low due to the special circumstances of the case.

19. Should the employer inform external authorities about the whistleblowing? If so, in what circumstances?

Yes, under the WBP Act it is the duty of WBP officer and deputy to:

- forward the report to competent authorities for further processing if the irregularity has not been resolved in cooperation with the company; and
- notify in writing the authority competent for external reporting on the report and the outcome of the actions undertaken within 30 days after a decision on the report is made.

20. Can the whistleblower be sanctioned if the facts, once verified, are not confirmed or are not constitutive of an infringement?

No, whistleblowers cannot be sanctioned for submitting a whistleblowing report or publicly disclosing irregularities (regardless of whether or not the facts are confirmed or such facts constitute an infringement), unless it can be proven that the whistleblower did not have a legitimate reason to believe that the information on irregularities was true at the time of making the report or disclosure, or did not have a legitimate reason to believe that the information falls within the scope of the WBP Act.

21. What are the sanctions if there is obstruction of the whistleblower?

If the company undertakes actions that constitute an obstruction of the whistleblower (for example, preventing or attempting to prevent the submission of a report, undertaking malicious processes against the whistleblower or retaliation against the whistleblower), the company may be fined up to about 6,700 EUR and the individual responsible with the company may be fined up to about 4,000 EUR.

Furthermore, any decision or other document provided by the company, or any legal transaction, whereby the company retaliates against the whistleblower or person related to or connected with the whistleblower will not have any legal effect.

Whistleblower Protection

22. What procedure must the whistleblower follow to receive protection?

To receive protection as granted under the WBP Act, the whistleblower must either:

- submit an internal whistleblowing report as per the whistleblowing procedure established by company and the WBP Act;
- submit an external whistleblowing report to the competent authority for external reporting (which in Croatia is the Croatian Ombudsman) as per the regulations adopted by that authority and the WBP Act; or
- publicly disclose information on irregularities as per the WBP Act (please see question 18).

23. What is the scope of the protection?

Regarding the personal scope of protection, the company is prohibited from retaliation, attempted retaliation or threatened retaliation against the whistleblower; any person assisting the whistleblower; persons connected with the whistleblower (for example, relatives or colleagues of the whistleblower); legal entities that the whistleblower owns, works for, or is otherwise connected with within the work-related environment; and the WBP officer and their deputy.

Concerning the material scope of protection, the following is a non-exhaustive list of what is considered retaliation under the WBP Act:

- suspension, termination, revocation or equivalent action;
- demotion or denial of promotion;
- transfer of duties, change of work location, salary decrease, change of working hours;
- denial of professional training;
- negative work performance ratings or negative employment recommendations;
- imposition or adoption of a disciplinary measure, reprimand, or other sanction (including financial sanctions);
- coercion, intimidation, harassment, or isolation;
- discrimination, being put at a disadvantage or unfair treatment;
- refusal to conclude an employment contract for an indefinite duration (if the legal requirements of this were met and the employee had a reasonable expectation that such a contract would be offered to him or her);
- refusal to conclude a consecutive fixed-term employment contract or the termination thereof;
- causing damage (including damage to reputation), especially via social media, or causing financial loss (including loss of business or loss of income);
- blacklisting the person within a sector or industry;
- premature termination of any contract for procurement of goods or services, or the cancellation thereof;
- cancellation of a licence or permit; and
- referral to a psychiatric or medical assessment.

Should a person entitled to protection under the WBP Act suffer retaliation (including if the retaliation is only attempted or threatened), they may initiate court proceedings asking the

court to: establish that the person suffered retaliation; prohibit further retaliation and undo the consequences of retaliation; award damages; or order the publication of the judgment confirming that the protected person's rights have been violated. In addition, protected persons may also ask the court to impose interim measures either before, during or after court proceedings (until enforcement is carried out).

24. What are the support measures attached to the status of whistleblower?

In addition to protection of identity and confidentiality, judicial support, and the right to compensation, whistleblowers have the following support measures: free primary legal aid; the possibility of being granted secondary legal aid; an exemption from the payment of court fees; and emotional support (which will be further defined in a supporting regulation yet to be adopted by the Ministry).

25. What are the risks for the whistleblower if there is abusive reporting or non-compliance with the procedure?

Regarding abusive reporting, any whistleblower who makes a report containing information he or she knows is false, or publicly discloses such information, may be sanctioned by a fine of up to about 4,000 EUR, or may face criminal prosecution (if the disclosure of false information amounts to a criminal act).

On the other hand, non-compliance with the procedure as provided by the company in the whistleblowing policy does not constitute an offence. Rather, non-compliance in certain cases might result in the report not being recognised as a qualifying whistleblowing report, and may result in the person making the report not receiving the status of a whistleblower and its related protection.

Visit **International Employment Lawyer** to explore the Guide to Whistleblowing comparative reference tool. Research country-specific regulations or build your own report comparing jurisdictions.

[Click here to build your own report now](#)

Authors:



Marija Gregorić, Babić & Partners

Areas of practice: Employment and Labor, M&A, Data Privacy, Dispute Resolution, Real Estate.

Professional memberships: Croatian Bar Association, IBA, EELA

[Learn more](#)



Matija Skender, Babić & Partners

Areas of practice: Corporate & Commercial, Employment and Labor, M&A, Dispute Resolution, Compliance

Professional memberships: Croatian Bar Association

[Learn more](#)