

Whistleblowing policy for Robert Half Inc's subsidiaries (Protiviti and Robert Half) in Belgium, The Netherlands, France, Germany and Italy (the "Whistleblowing Policy")

1 About this policy

- 1.1 Robert Half Inc. ("Robert Half") and its subsidiaries (Robert Half and Protiviti) including your employer ("**Company**"), have implemented a [Code of Business Conduct and Ethics](#) ("**Code**") reflecting their commitment to ethics and integrity. The Code sets expectations for upholding ethical standards. If you have any type of question about the Code or believe a violation of the Code has occurred, you should seek clarification from, or report such suspected violation to, your local manager or Human Resources Representative. **Robert Half** encourages any individual who has genuine concerns about an alleged breach in the organisation (e.g. unethical behaviour, forms of malpractice, illegal acts, failure to comply with regulatory requirements, accounting irregularities, or violations of Company policy) to raise those concerns at an early stage through the Company's internal (global or local) reporting channel. **Global** reporting channel means the submission of a report via the reporting channel in which the report - regardless of your work-based relationship with a specific local entity - is first received by Robert Half Inc, the parent company in the U.S.. **Local** reporting channel is to be understood as the possibility of submitting a report in such a way that it is received directly by the local entity with which you either have a work-based relationship or which you have selected as the recipient of your report.
- 1.2 A Breach is any event, incident, situation, act, or omission believed to violate Company policy or procedure or an applicable law or regulation, related to the areas of concern listed in this this policy or the applicable law (**Breach** or **Breaches**).
- 1.3 You are encouraged to share any concerns or information regarding Breaches, including reasonable suspicions about actual or potential Breaches, whether occurring within the Company or being committed by an entity or an individual acting on the Company's behalf, as well as any attempts or suspected attempts to conceal a Breach.
- 1.4 The Company strives to foster a workplace conducive to open communication regarding Company business practices. We are committed to ensuring any individual who reports an actual or potential Breach through the reporting channels set out in this policy is protected from unlawful retaliation and discrimination if they make a report with reasonable grounds to believe the information in the report is true. The Company takes all reports of actual or potential Breaches seriously and is committed to ensuring that reported Breaches are addressed discretely and effectively within the Company to determine the appropriate course of action in accordance with Company policy and all applicable laws, including but not limited to the stipulations of the European Directive of 23 October 2019 on the protection of persons who report breaches of Union law (2019/1937).
- 1.5 In furtherance of these commitments, this policy:
- (a) gives guidance on the receipt, retention, and treatment of verbal or written reports of actual or suspected Breaches received by the Company;
 - (b) gives guidance on how to report information regarding an actual or suspected Breach in a confidential and, where applicable, anonymous manner; and
 - (c) makes clear the Company's intention to discipline or terminate the employment of any person determined to have engaged in retaliatory behaviour.
- 1.6 The Company will ensure that all individuals who fall within its scope are able to view a copy of this policy in a format which they can readily understand.

2 Scope

This policy applies to the Protiviti and Robert Half subsidiaries of Robert Half Inc. in Belgium, The Netherlands, France, Germany and Italy and to the following individuals who acquire information on a reportable Breach in a work-related context:

- 2.1 *employees with permanent or limited-term contracts;*
- 2.2 *contractors;*
- 2.3 *sub-contractors;*
- 2.4 *volunteers;*
- 2.5 *paid or unpaid trainees;*
- 2.6 *agency workers where the worker is supplied by a third party to the Company;*
- 2.7 *self-employed individuals;*
- 2.8 *shareholders;*
- 2.9 *members of the company's administrative, management and supervisory bodies (including non-executive members);*
- 2.10 *anyone working under the supervision and direction of contractors, subcontractors and suppliers;*
- 2.11 *anyone in any of the above categories whose work-based relationship with the company is yet to begin or has ended].*

Areas covered by the policy

- 2.12 This policy is designed to cover the reporting of an actual or suspected Breach involving the following areas:
 - (a) public procurement;
 - (b) financial services, products and markets;
 - (c) prevention of money laundering;
 - (d) prevention of terrorist financing;
 - (e) product safety and compliance;
 - (f) transport safety;
 - (g) protection of the environment;
 - (h) radiation protection and nuclear safety;
 - (i) food and feed safety;
 - (j) animal health and welfare;

- (k) public health;
- (l) consumer protection;
- (m) protection of privacy and personal data;
- (n) security of network and information systems;
- (o) Breaches affecting the financial interests of the EU;
- (p) Breaches relating to the EU internal market including Breaches of:
 - (i) competition and State aid rules;
 - (ii) rules on corporate tax including any tax arrangements;

2.13 You are encouraged to report any Breach which you reasonably believe is unlawful.

2.14 Your report can relate to any Breach anywhere in the world; it is not restricted to matters purely arising in the country where you work.

3 Protection against retaliation

3.1 The Company appreciates that the decision to raise a concern can be a difficult one to make, not least because there may be a fear of reprisal from those who may be involved in the Breach (e.g., those who may have committed the Breach, etc). The Company will not tolerate retaliation against any person who raises a concern where they have reasonable grounds to believe that the information in the report is true at the time of reporting, even if it transpires that there is no basis for concluding that any Breach has occurred, or is likely to occur.

3.2 The protections against retaliation also apply, where relevant, to:

- (a) facilitators;
- (b) third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context; such as colleagues or relatives of the reporting persons; and
- (c) legal entities that the reporting person owns, works for, or are otherwise connected with in a work-related context.

3.3 The Company will take appropriate steps to protect all impacted individuals, including taking necessary action, which may include but is not limited to disciplinary action or dismissal, against anyone who is found to be pursuing any form of retaliation, or has threatened to do so.

4 False allegations

Just as the Company will seek to protect those who raise concerns where they have reasonable grounds to believe that the information in the report is true at the time of reporting, it will also protect those who are accused of a Breach in a report which is false. The Company will take necessary action against any individual who knowingly reports false information, which may include but is not limited to disciplinary action or dismissal.

5 Raising a concern

5.1 General principles

- (a) The Company encourages individuals to raise a matter when it is just a concern, as long as they have reasonable grounds to believe that the information in the report is true, rather than waiting for proof or investigating the matter themselves. Acting sooner rather than later can avoid any further potential damage. Reports will be treated with confidentiality.
- (b) The Company encourages individuals to ask questions and discuss concerns with their supervisor, who can often be an excellent resource. However, the Company recognizes that you may not always feel comfortable raising concerns with a supervisor and, as such, you can report any concern via the internal (global or local) reporting channels, as detailed in this policy or any country specific schedule to this policy.
- (c) Reports may be made on an anonymous basis, but individuals are encouraged to submit their name with their report. Concerns expressed anonymously are less powerful and tend to be more difficult to address effectively, but will nonetheless be considered and dealt with by the Company to the fullest extent possible.

5.2 Global internal reporting

- (a) The Company's reporting channel for whistleblowing reports is operated externally by OneTrust (formerly Convercent) which has been designated to carry out this function.
- (b) You may make your report orally or in writing:
 - (i) to make an oral report you can contact the OneTrust (formerly Convercent) Helpline (phone numbers are mentioned in the country specific schedules)
 - (ii) to make a written report you can either access the OneTrust (formerly Convercent) Web Portal via www.RobertHalfEthicsLine.com or send an email to the Company's General Counsel or the Corporate Compliance Officer.

If you choose to make an oral report, a complete and accurate transcript of the conversation will be drafted. You will be given the opportunity to check, correct and ensure the accuracy of the written transcript of conversation.

- (c) All reports of actual or suspected Breaches must be factual and contain as much information as possible. All reported information, including about the identity of the reporter, is treated as confidential subject to applicable legal and regulatory requirements.
- (d) You will be sent an acknowledging receipt of his report within seven days of the report being made. It might however be impossible to send an acknowledging receipt if the individual would not agree to use the messaging facility or would not provide contact information.
- (e) The Corporate Compliance Officer has been designated to carry out and will be responsible for:
 - (i) maintaining communication with you including asking for further information on the report, where necessary;
 - (ii) ensuring your report is diligently followed up/investigated to assess the accuracy of the allegations made in the report;

- (iii) ensuring a decision is made on any action required to address the breach reported or deciding to close the procedure;
- (iv) providing feedback to you on your report including information on action envisaged or taken as follow-up to the report and the grounds for such follow-up. Feedback will be provided within a reasonable timeframe which will not exceed three months from acknowledgement of receipt of your report.
- (f) The Company would expect that raising concerns internally with a supervisor would be the most appropriate action for you to take. However, if you feel that you cannot raise your concerns in this way you may consider using the global internal reporting channel or the reporting channel of the local entity you have a work based relationship with. Details of the local internal reporting channels, the procedures and people or departments responsible for operating them, can be found in the country and legal entity specific annexes attached to this policy.

5.3 Operating principles for investigating complaints

- (a) An investigation to establish all relevant facts will be conducted as sensitively and speedily as possible.
- (b) Your report via the global internal reporting channel will be investigated by the Corporate Compliance Officer with the assistance of Robert Half's (US) personnel, consultants, or audit offices, as appropriate.
- (c) In some instances it might be necessary to refer the matter to an external authority for further investigation, such as the Police.
- (d) At the end of the investigation, the investigator will analyse all the evidence and make findings of fact, based upon the balance of probabilities, as to whether a Breach has occurred or is likely to occur.

5.4 Keeping and managing records

- (a) When an individual makes an internal (global or local) report, the Company will process any personal data collected in compliance with applicable laws and regulations and in accordance with its Data Protection Policy, which is available on Robert Half's websites. Data collected from the point at which an individual makes the report is held securely and accessed by, and disclosed to, only authorised individuals and only for the purposes of dealing with the report.
- (b) Personal data collected by the Company as a consequence of a report under this policy will be incorporated to a database controlled by Robert Half Inc., for the purposes of processing the report and conducting any investigation required. The Company may also need to share personal data with other companies/subsidiaries within the Robert Half Group, external investigative agencies, legal counsel and/or local authorities. Such third parties may be based in territories outside the EU, like the United States of America, which do not offer an equivalent level of protection on data privacy as in EU. Nevertheless, if data transfers outside the EU are needed, the Company will take appropriate measures to protect the data according to local regulations.
- (c) Personal data which are not relevant for the handling of a specific report will not be collected or, if accidentally collected, will be deleted without undue delay.
- (d) The Company recognises that it is important, and in everyone's interests, to keep written records during the concern raising process. Records will be stored for no longer than is necessary and in a way that is proportionate to comply with the Company's data privacy

obligations and record-keeping obligations. Records that will be retained and treated as confidential, include:

- (i) the nature of the concern raised;
 - (ii) a copy of any written notification setting out the nature of the concern;
 - (iii) key documents/evidence;
 - (iv) the investigation workpapers;
 - (v) the investigator's report;
 - (vi) any written response by the Company, including any action taken and the reasons for action taken; and
 - (vii) minutes of meetings.
- (e) Where an individual requests a meeting for reporting purposes, the Company will ensure, subject to the consent of the individual, that complete and accurate records are kept of the meeting which will be either:
- (i) by making a recording of the conversation; or
 - (ii) through accurate minutes of the meeting prepared by the staff member responsible for handling the report. The reporting individual will be offered the opportunity to check, rectify and agree the minutes of the meeting by signing them.

5.5 Duty to cooperate and preserve relevant evidence

From time to time, the individual who made the complaint may be asked to provide or preserve documents related to an investigation or may receive a request to participate in an investigative interview. All individuals subject to this policy are obliged to cooperate with Company investigations by timely providing truthful accounts and relevant documents in response to interviews, questions, and information requests. The destruction of documents or other evidence related to an investigation is prohibited. Any individual who fails to cooperate, or otherwise obstructs, impedes, or improperly influences an investigation, or attempts to do so, may be subject to disciplinary action, up to a possible termination of their employment, in accordance with the Company's applicable policies.

5.6 External reporting route

- (a) This policy provides individuals with the opportunity and protection necessary to raise concerns internally through a central (global or local) reporting procedure and the Company believes that the processes laid out herein are the most effective processes for dealing with reports of a Breach in a manner that serves the best interests of both the Company and any individual making a report. However, if you feel that you cannot raise your concerns in this way and reasonably believe the information you wish to report is true, you may consider reporting the matter to a competent external authority.
- (b) With regard to the Company, further details on the options for external reporting can be found in the country specific information attached to this policy.

6 Confidentiality

The Company's (global or local) internal reporting processes are secure and confidential which means that:

- 6.1 no unauthorised staff member is allowed access to information held within it;
- 6.2 the identity of an individual who makes a report, together with any other information from which their identity may be directly or indirectly deduced, will be kept confidential and protected and will not be disclosed, without the individual's consent, to anyone beyond authorised individuals within the Company or their designees who are competent to receive or follow-up on a report;
- 6.3 by way of an exception, and subject to appropriate safeguards under the applicable European Union and national rules, the identity of a reporting person and any other information from which their identity might be deduced, may be disclosed where this is necessary in the context of an investigation by any national authority or in the context of judicial proceedings;
- 6.4 where an individual is referred to in a report as a person to whom a Breach is attributed or with whom someone who committed a Breach is associated, the Company will ensure that the individual's identity is kept confidential and protected for so long as investigations triggered by the report are ongoing and will ensure that the individual is treated fairly including being given the presumption of innocence and a right to be heard.

7 Monitoring and review

The Corporate Compliance Officer will be responsible for monitoring the effectiveness of this policy and taking remedial action where it is apparent that the policy and procedures may not be achieving the Company's overall aim.

8 Contractual status

This policy does not form part of any employee's contract with the Company, however, the Company expects that its principles and procedures should be followed by all individuals within its scope. The Company reserves the right to change the content of this policy, as necessary, from time-to-time.

9 No waiver of rights

The rights of individuals to report concerns under this policy cannot be waived or limited by any agreement, policy, form or condition of employment and the Company will never require any such waiver or limitation of rights by any individual.

10 Periodic review of procedures

The Corporate Compliance Officer will review the procedures outlined above and consider changes to such procedures periodically.

11 Annexes

Country specific rules in relation to Belgium, France, Germany, Italy and the Netherlands are set out in the schedules.

Schedule Country specific rules for the Netherlands

The purpose of this schedule is to provide an overview of (i) the modalities of the local internal reporting channel in the Netherlands, (ii) the external reporting possibilities in the Netherlands, and (iii) any deviations that the Dutch Whistleblowers Protection Act has made from the stipulations of the European Directive of 23 October 2019 on the protection of persons who report breaches of Union law (2019/1937).

1 About this policy

Under Dutch legislation Breaches are acts or omissions that are unlawful and concern the areas of concern listed in (i) article 2.12 of the policy, (ii) the acts related to in article 2.1(b) of this schedule, or (iii) acts related to transport safety.

2 Scope

2.1 In addition to the scope as mentioned in article 2.12, under Dutch legislation:

An act or omission involving the public interest in:

- (a) A violation or risk of violation of a statutory provision or internal rules that constitute a concrete obligation and that have been adopted by the Company under a statutory provision, or
- (b) A danger to public health, to the safety of persons, to damage to the environment or to the proper functioning of the public service or an enterprise as a result of improper acts or omissions.

The public interest is at stake in any case if the act or omission does not merely affect personal interests and there is either a pattern or structural character or the act or omission is serious or extensive.

3 Local internal reporting channel

3.1 As indicated in this policy, the Company would expect that raising concerns internally to your supervisor would be the most appropriate action for you to take. However, if you feel that you cannot raise your concerns in this way you may consider using the global reporting channel or the internal reporting channel proper of the local entity you have a work-based relationship with.

3.2 In the Netherlands and with regards to Robert Half Nederland BV, Robert Half International BV and Protiviti BV any reports can be made through the following local legal entity internal reporting channel:

- (a) the Company's local internal reporting channel for whistleblowing reports is operated externally by OneTrust (formerly Convercent), which has been designated to carry out this function.
- (b) you may make your report orally, in writing or in person:
 - (i) to make an oral report you can contact the OneTrust (formerly Convercent) Helpline via 0-800-023-4122

- (ii) to make a written report you can either access the OneTrust (formerly Convercent) Web Portal via www.RobertHalfEthicsLine.com or send an email to the local Complaint Manager via Complaint-manager-Netherlands@roberthalf.net.

Where you choose to make an oral report you will be given the opportunity to check, correct and ensure the accuracy of the written transcript of the conversation;

- (c) all reports of actual or suspected Breaches must be factual and contain as much information as possible. All reported information, including about the identity of the reporter, is treated as confidential subject to applicable legal and regulatory requirements;
- (d) You will receive an acknowledging receipt of your report within seven days of your report being made
- (e) The local Complaint Manager has been designated to carry out and will be responsible for:
 - (i) maintaining communication with you including asking for further information on the report, where necessary;
 - (ii) providing feedback to you on your report including information on action envisaged or taken as follow-up to the report and the grounds for such follow-up. Feedback will be provided within a reasonable timeframe which will not exceed three months from acknowledgement of receipt of your report.

3.3 All articles of the Whistleblowing Policy that have not been modified by this schedule, and with the exception of article 5.2 and 5.3(b) of the policy, shall apply without prejudice to the local internal reporting channel.

4 External reporting channel

4.1 External reporting route

As indicated in this policy, if you feel that you cannot raise your concerns via the internal (global or local) reporting channel and reasonably believe the information you wish to report is true, you may consider reporting the matter to a competent external authority. With regard to the Netherlands, you can make an external report with the competent authorities as appointed by the Dutch legislator.

4.2 The authorities competent for receiving an external report

The authorities responsible for receiving reports, reporting feedback, and providing follow-up on external reports are the following:

- (i) The Netherlands Authority for Consumers & Markets (de Autoriteit Consument en Markt);
- (ii) The Dutch Authority for the Financial Markets (de Autoriteit Financiële Markten);
- (iii) The Dutch Data Protection Authority (de Autoriteit persoonsgegevens);
- (iv) De Nederlandsche Bank N.V.;
- (v) The Whistleblowers Authority (het Huis);
- (vi) The Inspectorate for Health and Youth Care (de Inspectie gezondheidszorg en jeugd);
- (vii) The Dutch Healthcare Authority (de Nederlandse Zorgautoriteit);

- (viii) The Authority for Nuclear Safety and Radiation Protection (de Autoriteit Nucleaire Veiligheid en Stralingsbescherming).