WHISTLEBLOWING POLICY

Courtesy translation. The original version of this document has been issued in Italian language.

1 About this Policy

1.1 Pursuant to and for the purposes of Legislative Decree March 10, 2023, no. 24 ("**Whistleblowing Decree**"), implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 (hereinafter, collectively referred to as the "**Whistleblowing Legislation**"), the following Policy (the "**Whistleblowing Policy**" or the "**Policy**") has been adopted by the following legal entities (hereinafter, collectively referred to as the "**Company**"):

(a) Protiviti S.r.l., a company with sole stakeholder having legal seat in Via Tiziano 32, 20145, Milano (MI) and VAT code 04156610968;

(b) Protiviti Government Services S.r.l., a company with a sole stakeholder having legal seat in Via Tiziano 32, 20145, Milano (MI) and VAT code 09692380968.

1.2 Robert Half Inc. ("**Robert Half**") and its subsidiaries have implemented a code of business conduct and ethics ("**Code of Conduct**") that reflects the commitment to ethical and integrity-related issues. The Code of Conduct sets expectations for maintaining ethical standards. Robert Half encourages every individual with sincere concerns regarding a suspected internal Breach within the organization (such as unethical behavior, forms of misconduct, illegal acts, non-compliance with regulatory requirements, accounting irregularities, or Breaches of company policies) to report such concerns through the internal reporting channels (either global or local) described below. Additionally, the Company adopted an Organizational and Control Model in compliance with Legislative Decree 231/2001 (the "**Organizational Model**").

1.3 For the purpose of this Policy, a "**Breach**" is any event, incident, situation, act, or omission that falls into the scope outlined by paragraph 2 of this Policy.

1.4 Recipients of this Policy are encouraged to report alleged Breaches, including well-founded suspicions regarding actual or potential Breaches, whether the alleged Breach occurred within the Company, was committed by an individual acting on behalf of the Company, or involved an attempt to conceal such Breaches.

1.5 A local and a global reporting channel have been established to receive reports. Global reporting channel means the submission of a report via the Global 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. (the "**Global Reporting Channel**"). Local reporting channel means the submission of a report directly to the local entity with which you either have a work-based relationship or which you have selected as the recipient of your report (the "**Local Reporting Channel**").

1.6 In compliance with these commitments, this Policy:

(a) offers guidance on how to report facts related to an actual or suspected Breach confidentially and, if applicable, anonymously;

(b) provides guidelines on the receipt and handling of reports of actual or suspected Breaches received by the Company; and

(c) clarifies the Company's intention to apply disciplinary sanctions, as provided by current regulations, to any person found responsible for retaliatory behaviour.

2 Scope

2.1 The Whistleblowing Decree applies to breaches of national or European Union legal provisions that harm the public interest or the integrity of public administration or private entities, of which whistleblowers become aware in a public or private work context.

2.2 This Policy applies to the legal entities mentioned by art. 1.1. and to the following individuals who acquire information about a reportable Breach in a work context:

(a) employees with permanent or fixed-term contracts;

(b) temporary workers, where the worker is provided by a third party to the Company;

(c) freelancers, self-employed individuals, consultants;

(d) volunteers and interns;

(e) suppliers;

(f) members of the administrative, executive, and supervisory bodies of the Company (including non-executive members);

(g) anyone operating under the supervision of consultants, suppliers, or contractors of the Company;

(h) anyone in any of the above categories whose legal relationship with the Company is yet to commence (if information about Breaches is acquired during the selection or pre-contractual phase) or has ended (if information about Breaches is acquired during the course of the relationship itself)."

2.3 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.

2.4 In connection with the scope of this Policy, the aforementioned individuals are encouraged to report conduct that they reasonably believe constitutes an unlawful Breach.

2.5 Exclusions

(a) As provided by the Whistleblowing Decree, disputes, claims, or requests related to the personal interests of the reporting person or the person who filed a complaint with the judicial or accounting authority that exclusively concern their individual employment or public service relationships or are related to their employment or public service relationships with hierarchically superior figures are excluded from the scope of the regulations.

(b) By way of example and not exhaustively, reports concerning employment disputes and pre-litigation phases, discrimination among colleagues, interpersonal conflicts between the reporting person and another worker or with hierarchical superiors, and reports related to data processing within the context of the individual employment relationship in the absence of harm to public interest or the integrity of public administration or private entities are excluded from the scope of this Policy.

3 Protection against retaliation

3.1 The Company understands that the decision to make a report can be difficult, especially because there may be fear of retaliation from the subjects of the report (for example, those who may have committed the Breach, etc.). The Company will not tolerate retaliation against anyone making a report through the reporting channels provided in this Policy when, at the time of the report, there are reasonable grounds to believe that the reported facts are true, even if it later emerges that there is no reason to conclude that a Breach has occurred or is likely to occur.

3.2 Protection from retaliation also applies, where relevant:

(a) to facilitators (those assisting a reporting person in the reporting process, operating within the same work context, and whose assistance must be kept confidential);

(b) to individuals within the same work context as the reporting person and who are connected to them by a stable emotional or familial bond within the fourth degree;

(c) to coworkers of the reporting person working in the same work context and having a regular and current relationship with that person;

(d) to entities owned by the reporting person.

3.3 The Company will take appropriate measures and disciplinary actions to protect all individuals involved, in accordance with applicable regulations, against anyone engaging in any form of retaliation or threatening to do so.

4 False accusations

4.1 Just as the Company will protect those who make reports when there are 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 that is later determined to be false. The Company will take, in accordance with applicable regulations, the necessary actions against any individual who knowingly reports false information.

5 Raising a concern

5.1 General Principles

(a) If there are reasonable grounds to believe that the facts to be reported are true, the Company encourages recipients of this Policy to make a report even when there are only mere suspicions of a Breach, rather than investigating the matter independently.

(b) The Company encourages individuals to ask questions and discuss suspicions with their supervisor, who often can be a valuable resource for clarification. However, the Company acknowledges that a person may not always feel comfortable raising sensitive issues with a superior. Therefore, employees can always report any suspicions through the reporting channels as detailed in this Policy.

(c) Reports can be made anonymously, but individuals are encouraged to provide their identity. Anonymous reports are less impactful and tend to be more challenging to manage effectively. In any case, they will be considered and handled by the Company as comprehensively as possible.

5.2 Internal Reporting Channels

(a) The Global and Local Reporting channels are managed by OneTrust LLC, formerly Convercent, through a dedicated platform ("**OneTrust**").

(b) Reports can be made orally or in writing.

(i) To make a written report, both global and local, access the OneTrust portal at the following address www.RobertHalfEthicsLine.com.

(ii) To make an oral report via phone call, contact OneTrust's Helpline at the following telephone number: 800.727.419.

(iii) To make an oral report through a direct meeting, please request a meeting a with the Whistleblowing Committee (as defined below). To do so, please, reach out to the head of the Human Resource department and to the head of the Legal & Compliance department of the Company, who will arrange a confidential meeting at the company's premises.

If the reporting person chooses to make an oral report, a transcript of the conversation will be drafted and provided to the reporting person, in compliance with the Whistleblowing Legislation.

(c) All reports of actual or suspected Breaches must be based on concrete facts and contain as much information as possible. All reported information, including the identity of the reporting person, is treated as confidential and will be handled pursuant to the applicable laws. Reports, including anonymous ones, should be as detailed as possible and based on specific and consistent factual elements. In particular, the report should clearly indicate (also by attaching documents):

(i) the circumstances of time and place in which the reported Breach occurred;

(ii) the description of the Breach and how it came to your attention;

(iii) the personal details or other elements that allow the identification of the subject to whom the reported facts are attributed.

(d) Within seven days of submitting the report, a confirmation of receipt of the report will be sent to the reporting person.

(e) The Company has established a "**Whistleblowing Committee**" within the Legal & Compliance and the Human Resources departments to handle reports made via the Local Reporting Channel. The Whistleblowing Committee will be responsible for:

(i) maintaining communication with the reporting person, requesting additional information about the report, if necessary;

(ii) ensuring that the report is followed/investigated to assess the accuracy of the allegations made in the report;

(iii) ensuring that a decision is made on the actions necessary to address the reported Breach or deciding to close the procedure;

(iv) providing feedback on the report, including information on the action taken or planned to follow up with the report and the reasons for such action; such feedback will be provided within a reasonable timeframe, not exceeding 3 (three) months from the confirmation of receipt of the report.

(v) evaluating and managing any conflicts of interest by activating appropriate escalation procedures, if necessary, in order to handle the reports in line with the spirit of the regulation, which is aimed at the protection of the reporting person.

5.3 Operating principles to conduct the investigation

(a) An internal procedure for handling reports has been established with the aim of assessing the validity of the content of the reports, upon receiving them. If the report is not evidently unfounded, an investigation will be conducted to determine the relevant facts in the most sensitive and expedient manner possible.

(b) In some cases, it may be necessary to forward the report to an external authority for further investigations, including the judicial authority.

(c) The findings reached at the end of the investigations will be communicated and/or used in accordance with applicable Whistleblowing Legislation.

5.4 Keeping and managing records

(a) When an individual makes a report, personal data collected in accordance will be treated in accordance with applicable laws and regulations and in accordance with the Data Protection Policy. Data collected from the moment an individual makes a report is securely stored, accessible only to authorized individuals, and processed solely for purposes related to the management of the report.

(b) Personal data may have to be shared with other companies within the Robert Half's group, external investigative agencies, legal consultants, and/or local authorities. Such third parties may be located outside the EU, such as the United States of America. Where data transfers outside the EU are necessary, the Company will take adequate measures to protect the data in accordance with applicable law.

(c) Personal data that is not relevant to the management of a specific report will not be collected, or if collected accidentally, will be promptly deleted.

(d) The Company recognizes the importance, and in the interest of all, of transcribing the contents of the report in the manner provided by the Whistleblowing Decree. Recordings/transcriptions/documentation will be retained for the time strictly necessary and in a proportionate manner to comply with the Company's privacy and document retention obligations.

(e) When an individual requests an in-person meeting to make a report (pursuant to art. 5.2 (a) (iii) of this Policy), with the individual's consent, the Company will keep complete and accurate records of the meeting, in the following ways:

(i) recording the conversation on digital support; or

(ii) through minutes of the meeting, prepared by the Whistleblowing Committee and reviewed, amended (if necessary), approved and signed by the reporting person, in the light of the applicable Whistleblowing Legislation.

5.5 Duty to cooperate and preserve relevant evidence

(a) During the course of investigations, the reporting person may be asked to provide additional documents related to the reported incident or to participate in an interview. Reporting persons and those involved in the investigation are encouraged to cooperate in the course of inquiries, promptly providing truthful accounts and relevant documents in response to interviews, questions, and/or requests for information. Destruction of documents or other evidence related to an investigation is prohibited. Any individual who fails to cooperate or otherwise hinders, obstructs, or improperly influences an investigation, or attempts to do so, may be subject to disciplinary action, in compliance with applicable law and in accordance with applicable company policies.

5.6 External Reporting Channel

This Policy provides individuals with the opportunity to make reports through an internal reporting channel. The Company believes that the measures set forth by this Policy enable the handling of reports of an (alleged) Breach in a way that best serves the interests of the Company and any reporting person.

However, in the event that

(a) the Company's internal reporting system is not active, available, or deemed non-compliant with the requirements of the Whistleblowing Decree,

(b) an internal report has already been submitted and has not been followed up by the Company,

(c) there are reasonable grounds to believe that the report will not be effectively addressed by the Company or that such a report could entail the risk of retaliation; and

(d) there is reasonable cause to believe that the Breach may constitute an imminent or clear risk to public interest,

it is possible to submit an external report to the competent authority, the National Anti-Corruption Authority (www.anticorruzione.it).

5.7 Public Disclosure

In specific circumstances, the Whistleblowing Decree provides the whistleblower with the option to make a public disclosure of the Breach. With public disclosure, information about the breaches is made public through the press, the web, or other means capable of reaching a large number of people.

The reporting person making a public disclosure can benefit from the protections provided by the Decree if the following conditions are met:

(a) the reporting person has previously made an internal and external report or has directly made an external report and has not received a response within a reasonable timeframe;

(b) the reporting person has reasonable cause to believe that the Breach may constitute an imminent or clear danger to public interest;

(c) the reporting person has reasonable cause to believe that the external report may entail the risk of retaliation or may not have an effective follow-up due to the specific circumstances of the case, such as those in which evidence may be concealed or destroyed, or where there is a reasonable fear that the recipient of the report may be colluding with the author of the violation or involved in the violation itself.

6 Confidentiality

The following applies to the Global and Local Reporting channel processes:

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 treated in confidentiality and will not be disclosed, without the individual's consent, to anyone beyond authorised individuals 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 individual's identity will be kept confidential and protected for so long as investigations triggered by the report are ongoing and the individual will be treated fairly including being given the presumption of innocence and a right to be heard.

7 Miscellaneous

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

INFORMATION REGARDING THIS POLICY

Name of the Document:	LC 01 – Whistleblowing Policy
Version:	V1
Previous Version:	/
Effective Date:	17.02.2024
Governance and allocation of responsibility:	This Policy has been drafted by the Legal & Compliance Team, in coordination with the Leadership Team of the Company.
Approval mechanism:	This Policy is reviewed by Leadership Team and eventually approved by the Country Market Leaders of the Company, in their quality of authorized attorneys of the Company.
Review mechanism:	This Policy will be revised in the event of substantial changes to the processes governed therein, in order to reflect such modifications. The Company also reserves the right to amend this document in relation to evolving business requirements and/or in case of new elements to be taken into consideration with regards to the subject matter covered by this Policy.