Whistleblowing Policy

September 1, 2025

I. Introduction

At Centric Software, we are committed to fostering a culture of transparency, integrity, accountability, and compassion. To reinforce this commitment, we have implemented this Whistleblowing Policy, designed to encourage the reporting of any misconduct or unethical behavior in good faith. By providing clear channels for raising concerns, we aim to safeguard our organization and ensure compliance with our core values and legal obligations while protecting those who come forward from retaliation.

All Centric Software, Inc., or any member of the Centric Software group of companies (known as "Centric"), employees, directors, shareholders, as well as Centric's partners, contractors, subcontractors, suppliers, and third-party representatives are expected to read, clearly understand, and abide by this Policy.

This Policy is an extension of Centric's Employee Handbooks, Code of Ethics and Business Conduct, Vendor Code of Ethics and Business Conduct, and Anti-Corruption Policy. It has been drafted and updated in accordance with applicable laws including the European Directive of October 23, 2019 on the protection of whistleblowers, as well as US and other applicable laws[1]. Country specific provisions are in Appendix B.

II. Who can be a Whistleblower?

A "Whistleblower" is an individual who, in good faith and without direct financial compensation (unless mandated by local law), reports or discloses information which raises a whistleblowing concern, such as suspected misconduct, as further detailed in this Policy.

A Whistleblower may raise an alert within or outside the scope of his or her professional activities. If the information has not been obtained in the course of professional activities, the Whistleblower must have personal knowledge of the facts. In any case, the Whistleblower must belong to one of the following categories of persons:

- Centric employees or former employees,
- Centric directors and shareholders,
- Centric partners,
- Centric contractors, subcontractors, and suppliers, or
- Any other third party, if permitted by applicable law.

Additionally, Centric undertakes to process any whistleblowing reports, even those made by persons other than those above.

---

[1] These include the French law n°2016-1691 of December 9, 2016 relating to the fight against corruption ("Loi Sapin 2"); Law n° 2017-399 of March 27, 2017 relating to the duty of vigilance of parent companies and ordering companies ("Duty of Vigilance") and Law n° 2022-401 of March 21, 2022 aimed at improving the protection of whistleblowers ("Waserman Law") transposing into French law Directive 2019/1937 of October 23, 2019 on the protection of persons who report violations of Union law, more commonly known as the Whistleblowers Directive, and its implementing decree no. 2022-1284 of October 3, 2022.

III. What can be reported?

Any Whistleblower, who has reasonable grounds to believe, given the circumstances and the information available to them at the time of reporting, that the matters they report are true, may report in good faith and without direct financial compensation (unless mandated by local law), the following matters in accordance with this Whistleblowing Policy:

- A violation (or attempted concealment of a violation) of the law or regulations of a ratified international commitment, including laws related to protection of privacy and personal data, security, tax, and financial matters;
- A criminal offense;
- Conduct or situations likely to constitute a violation of any Centric policies, in particular acts of corruption, as described in the Anti-Corruption Policy;
- A threat or harm to the public interest; or
- Risks of serious violations of human rights and fundamental freedoms, human health and safety rules, or harm to the environment.

Certain matters cannot be reported if they are covered by:

- Secrets of National defense and security,
- Protected or classified information,
- Information in judicial deliberations,
- The confidentiality of an investigation or judicial inquiry,
- Attorney-client privilege, or
- Medical confidential information.

IV. How do I raise an alert?

Anyone acting as a Whistleblower can raise an alert in the following manners:

1. For the most expedited response, the alert can be made by leaving a voice message on Centric's dedicated hotline (see **Appendix C**) or email (compliance@centricsoftware.com) to the Centric Compliance Committee, made up of Centric's General Counsel, VP of People & Culture and US Senior Legal Counsel.
2. Orally or via e-mail to a member of the Centric Executive Team, Centric People & Culture Team, or the Centric Legal Team (collectively, the "Authorized Centric Personnel") who will refer the alert to the Centric Compliance Committee.
3. By requesting a live or virtual meeting with the Centric Compliance Committee.
4. By completing a form online at the following site: https://www.centricsoftware.com/legal/whistleblowing-procedure/.

The report should include comprehensive information about the incident or concern, including any and all relevant emails, supporting documents and a timeline of events.

In the event that the report involves one or more members of the Compliance Committee or Authorized Centric Personnel, the Whistleblower may contact an alternative member of the Compliance Committee or Authorized Centric Personnel by email, who will refer the matter directly to a committee of members excluding the person who the complaint is made about.

In certain countries, Whistleblowers may have the right to use alternative local channels to make an alert as set forth in **Appendix B**, however it is encouraged to raise the alert first using the internal reporting channels listed above.

The aim of this Policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases you should not find it necessary to alert anyone externally. The law recognizes that in some circumstances it may be appropriate for you to report your concerns to an external body such as a regulator. It will very rarely if ever be appropriate to alert the media. We strongly encourage you to seek advice before reporting a concern to anyone external.

V. What are good reporting practices? How to report effectively?

To facilitate the efficient processing of alerts, a Whistleblower is strongly advised to:

1. Identify themselves,
2. Indicate whether they are acting in a professional capacity, specifying whether they fall in the category of the persons listed above (see Section 2 "Who can be a Whistleblower?") and, if not, whether they have personal knowledge of the alleged facts,
3. Describe the situation accurately, providing objective facts, dates, sequence of events or timelines, and names of people involved,
4. Present factual evidence (e.g. reports, documents, correspondence) helping to verify the alleged facts, so that a thorough investigation can be carried out.

The wording used to describe the alleged facts must honestly reflect the alleged facts as well as any elements of uncertainty. Any slanderous actions are discouraged and may be considered illegal.

Subsequently, communication between the Whistleblower and the Compliance Committee will take place by email and/or telephone contact, teams messaging and/or other means available to the parties. The Compliance Committee may also propose meetings, including remote meetings by videoconferencing.

VI. Can Whistleblowing Alerts be anonymous?

Alerts may be anonymous. However, please be aware that anonymous alerts may make it difficult to carry out a thorough investigation in order to establish the facts and organize the protection of the Whistleblower.

VII. Timeline of the Communication of the Investigation and Closing of a Whistleblowing alert.

A. The following applies in the event of an alert:

The Whistleblower is informed of the receipt their alert, in writing, at the latest within seven (7) days of receipt of the initial alert.

In the case of anonymous alerts, the Whistleblower receives this confirmation only if they have provided a contact email or address to write to.

If the alert is deemed inadmissible or cannot be processed for lack of details, the Whistleblower is informed of the reasons why Centric cannot follow up.

When it is possible to follow up on the alert, the Whistleblower is informed, in writing, of the action taken upon receipt of the alert in order to assess the accuracy of the allegations and, where appropriate,

to remedy the subject of the alert, at the latest within a period not exceeding three (3) months from acknowledgement of receipt of the alert.

B. Closing the alert:

Once the alert has been investigated, the Whistleblower will be informed by e-mail that the procedure has been completed and the alert is closed.

If a disciplinary sanction or legal proceedings are instituted against the person concerned as a result of the alert, the latter may obtain access to this information in accordance with the rules of law.

VIII. How does Centric manage the alerts?

Alerts are analyzed impartially, with the utmost care, and are subject to verification, investigation, if appropriate, and any action deemed necessary, in compliance with applicable law and regulations.

The Compliance Committee shall:

- Determine if additional employees or outside advisors may need to be informed in order to assess the alert appropriately,
- Investigate whether the alert indicates any breaches of Centric's policies and applicable laws,
- Prepare and examine the action plan to be implemented,
- The investigation procedure may include a number of steps, including but not limited to, gathering of facts and evidence, interviews, etc.,
- In the case of complex management issues or local conflicts of interest, conduct, define and monitor these plans before issuing conclusions and recommendations to Centric's executive team,
- Determine when an investigation is closed, if the allegations are inaccurate or unfounded, or if the alert has become irrelevant, and
- After the internal investigation, an official investigation report is drafted to present all of the facts and evidence gathered to substantiate or discredit suspicions, and to describe the method used. The internal investigation report draws conclusions about any further action needed on the Whistleblower's alert.

IX. Is it mandatory or exclusive to use the reporting procedure in the Centric Whistleblowing Policy?

Use of this Whistleblowing Policy for reporting is neither mandatory nor exclusive.

Alerts may be made by any means. Whether received within or outside the framework of this Policy, Centric will treat all alerts it receives by applying the confidentiality and non-retaliation principles provided in this Policy.

X. How are Whistleblowers protected by Centric?

- **<u>Confidentiality</u>**

Centric undertakes to keep the identity of a Whistleblower confidential.

Except with the express consent of the Whistleblower, their identity (or elements enabling their identification) will only be communicated to persons specifically responsible for the processing of alerts within Centric (in particular investigations and their follow-up) and under the condition that this

communication is necessary for the processing of the alert. These persons are bound by strict confidentiality obligations.

Centric also undertakes to keep confidential and to maintain the integrity of the information collected in the context of an alert, as well as:

1. The identity of the persons targeted by the Whistleblowing alert,
2. The identity of any third party mentioned in the alert.

The identity of the Whistleblower (or elements that would enable them to be identified) and the identity of the person targeted (or elements that would enable them to be identified), may always be communicated by Centric to a judicial authority. The Whistleblower is then informed, unless this information could compromise the legal proceedings.

- **No Retaliation**

Centric prohibits all retaliatory measures in response to a Whistleblowing alert that is made by a Whistleblower in good faith.

A retaliatory measure may include, for example: (i) being excluded from a recruitment process or from access to an internship or a period of professional training, (ii) being punished or dismissed, (iii) being subjected to coercion, intimidation, harassment, ostracism or reputation attacks on social media, or (iv) being subjected to a discriminatory measure, direct or indirect, in particular with regard to remuneration, training, reclassification, assignment, qualification, classification, professional promotion, transfer or renewal of contract. Depending on the facts and circumstances, acts of moral harassment may also constitute retaliation.

Centric also prohibits sanctions or retaliatory measures against persons who file an alert outside of this Whistleblowing Policy.

Improper or bad faith use of the Whistleblowing Policy or of a whistleblowing alert (for the sole purpose of harming the interests of an employee or of Centric in particular) may expose its initiator to disciplinary sanctions as well as legal proceedings.

In some countries, individuals who help a Whistleblower to file a Whistleblowing alert ("facilitators") are protected under the conditions laid down by applicable law, in particular against retaliation. Country-specific provisions are listed in **Appendix B** of this Policy.

XI. Processing of personal data in the context of Whistleblowing Policy.

Personal data collected in the context of this Whistleblowing Policy are processed by Centric as the data controller.

Personal data will only be communicated (i) to the Compliance Committee, (ii) to the Authorized Personnel to the extent the alert is made directly to them or they are necessary for the investigation or the follow-up, (iii) to persons specifically responsible for the handling of alerts within Centric (in particular investigations and their follow-up) and on condition that this communication is necessary for the processing of the alert, and (iv) to the competent authorities having the right to request the communication of this data.

The person who is the subject of the alert is informed of the existence of an alert concerning them and of the processing of their personal data in this context within a reasonable period of time, in principle one (1) month from the processing of the alert.

However, this information may be deferred when it is likely to seriously compromise the achievement of the objectives of the processing of the alert, as in the case of a risk of destruction of evidence. In this case, the information will be provided as soon as the risk has been eliminated, in particular during the first interview with the person concerned or, failing that, at the latest, at the end of the processing of the alert. Except with the express consent of the Whistleblower, the information will not contain any information relating to their identity.

Persons involved in the collection or processing of the alert (in particular witnesses) will be informed of the processing of their personal data as soon as possible and at the latest at the time of the first contact.

XII. Administration of This Policy

The Centric Legal and People & Culture Departments are responsible for the administration of this Policy. If you have any questions regarding this Policy or if you have questions that are not addressed in this Policy, please contact your local People & Culture representative or the Compliance Committee at compliance@centricsoftware.com.

XIII. Policy Effective Date and Revisions

Occasionally Centric may update this Policy as required to comply with legal requirements. The most recent Policy will be published and will reflect the effective date.

The effective date of this Policy is September 1, 2025.

Appendix A

How is Personal Data protected in the context of this Whistleblowing Policy?

The personal data collected in the context of this Whistleblowing Policy are processed by Centric as the data controller.

Personal data will only be communicated (i) to the Compliance Committee, (ii) to the Authorized Personnel to the extent the alert is made directly to them or they are necessary for the investigation or the follow-up, (iii) to persons specifically responsible for the handling of alerts within Centric (in particular investigations and their follow-up) and on condition that this communication is necessary for the processing of the alert, and (iv) to the competent authorities having the right to request the communication of this data.

1. Who is concerned by the protection of personal data?

As part of this Whistleblowing Policy, Centric will collect and store the personal data of the following persons (the "**Data Subjects"**):

- The authors of the Whistleblower alert;
- The persons targeted by the alert;
- Persons involved in the collection or processing of alerts, in particular witnesses, facilitators and third parties in contact with Whistleblowers.

2. What personal data is collected?

Personal data collected as part of the Whistleblowing Policy may include:

- The identity, function and contact details of the Data Subjects,
- Reported facts and information gathered in the course of verifying reported facts,
- Reports on verification operations and action taken on alerts.

In view of the nature of the processing and depending on the nature of the alert, Centric may also collect sensitive personal data within the meaning of the applicable Personal Data Protection Regulations.

For this reason, Centric has carried out a Data Protection Impact Assessment (DPIA) to ensure that the said processing presents all the appropriate guarantees to safeguard the rights and freedoms of the Data Subjects. This impact analysis has been assessed and validated by the Centric Data Protection Officer.

In accordance with the principle of minimization, Centric ensures that only the data necessary for the purposes of processing is actually collected and processed, reminding the authors of alerts that the information communicated within the framework of the Whistleblowing Policy must remain factual and present a direct link with the subject matter of the alert.

3. How long does Centric keep personal data?

Personal data is retained by Centric for the duration of the processing of the alert, without prejudice to legal retention obligations and statute of limitation periods.

As a general rule, alerts may only be kept for as long as is strictly necessary and proportionate for their processing and for the protection of the Whistleblower, the persons they concern and the third parties they mention, taking into account the time required for any further investigations. More specifically, the personal data of Data Subjects are kept:

- in active base for a reasonable period after receiving the alert until the final decision is made on the follow-up of the alert;
- in the form of intermediate archives (*i.e.* archives accessible by authorized persons only, on a need-to-know basis related to their functions) after the final decision has been taken, for a reasonable period, strictly proportionate to their processing and to the protection of the Whistleblower, the persons they concern and the third parties they mention, taking into account the deadlines for any additional investigations.

When the alert is followed up, in particular by disciplinary proceedings or legal action against the targeted person or the perpetrator of an abusive alert, the data relating to the alert is kept until the end of the legal proceedings, the statute of limitations or the expiration of legal remedies.

Archives are kept in accordance with the general archive retention policy applied within Centric, for a period not exceeding, in all cases, the duration of legal proceedings.

4. What are the purposes of personal data processing by Centric?

The personal data collected as part of the Whistleblowing Policy is used solely for the purposes of processing the alert (receive and process the alert, manage checks, investigations and analyses, define the follow-up of the alert, as well as protect the Data Subjects as provided for by this Policy), and defending or exercising rights before any jurisdiction in order to comply with applicable legal obligations[5] and/or the legitimate interest of Centric.

5. How does Centric manage the transfer of personal data?

For the purposes of verifying or investigating alerts, personal data processed may be transferred to countries where Centric is present.

In order to guarantee a sufficient level of protection for transfers to countries that are not considered by the authorities of the Data Subject's country (e.g. the European Commission) as offering an adequate level of protection of personal data, the transfer will be based on guarantees recognized by the authorities of the Data Subject's country as offering adequate protection of personal data (e.g. standard contractual clauses issued by the European Commission, or any other relevant mechanism).

Data Subjects may request more information about the mechanism used by Centric to transfer their personal data by sending a request to privacy@centricsoftware.com.

6. What are the rights of Data Subjects?

Subject to applicable regulations on the protection of personal data, Data Subjects have the right to access, rectify and restrict the processing of their personal data.

The right of access may be limited according to the person exercising it, the stage of the investigation and the risks of identifying the Whistleblower.

The right of rectification may only concern factual data, the material accuracy of which can be verified by Centric on the basis of evidence, and without deleting or replacing the data, even if erroneous as originally collected.

However, in accordance with applicable regulations on the protection of personal data, Data Subjects may not exercise their rights to the erasure, opposition and portability of their personal data insofar as their processing in application of the present Procedure is necessary to comply with legal obligations to which Centric is subject.

All these rights may be exercised by sending a request via the following contact form:
https://www.centricsoftware.com/contact/

According to applicable data protection legislation, Data Subjects have a right to file a complaint with their local data protection authority. If they are located in the European Union, Lichtenstein, Norway or Iceland, they have a right to file a complaint with the Commission Nationale de L'Informatique et des Libertés (CNIL).

7. Who do I contact if I have questions about my personal data?

Any interested party may contact the Centric Data Protection Officer by sending a request via the following contact form: https://www.centricsoftware.com/contact/

Appendix B

This appendix B sets out the specific Whistleblowing alert rules on a country-by-country basis.

AUSTRALIA

A. Benefit of legal protection

The Corporation Act and Tax Administration Act, hereafter referred to as "the Laws," provide additional protections beyond those outlined in this Procedure for Whistleblowers who meet the qualifications under the Laws. Generally, a disclosure qualifies under the Laws if it is made with reasonable grounds by a Whistleblower, about a Reportable Concerns to an Eligible Recipient, both as defined below.

B. Eligible Recipients

In addition to the Compliance Committee, Reportable Concerns can also be disclosed to an officer, senior manager, internal or external auditors of Centric Software ("Eligible Recipients").

The disclosures to a legal practitioner for the purposes of obtaining legal advice or legal representation in relation to the operation of the Whistleblower provisions in the Laws are also protected.

C. Reportable Concerns

"Reportable Concerns" involve any information concerning misconduct, or an improper state of affairs or circumstances in relation to Centric Software

Examples of Reportable Concerns include:

- Bribery or corruption;
- Tax evasion or misconduct in tax affairs;
- Financial fraud;
- Illegal activities (engaging in insider trading, misreporting financial information, negligent acts, a breach of trust or a breach of duty);
- A danger to public safety or the stability of or the confidence in financial system.

Generally, disclosures concerning personal work-related grievances do not meet the criteria for protection under the Laws, but they may still be covered by other applicable local regulations.

Examples of personal work-related grievances include:

- Disputes between employees that do not constitute a breach of conduct or
- Disputes between the Whistleblower and Centric Software relating to the employees performance or compensation.

A Whistleblower that reports a situation related to a work-related grievance may benefit from the protection under the Laws if:

- It includes information about misconduct, or
- If Centric Software has breached employment or other laws punishable by imprisonment for a period of 12 months or more, engaged in conduct that represents a danger to the public,
- Or the disclosure relates to information that suggests misconduct beyond the Whistleblower's personal circumstances;
- The Whistleblower suffers from or is threatened with detriment for making a disclosure.

D. Facilitators

In addition to the individuals listed in the Whistleblowing Policy, a relative, dependent or spouse of current and former employees, contractors, consultants, services providers, suppliers and business partners may benefit from the protection the Laws.

E. External reporting procedure

A Whistleblower may also report to:

- The Australian Securities and Investments Commissions (ASIC)
- The Australian Prudential Regulation Authority (APRA)
- In relation to Tax Disclosers, The Commissioner of Taxation (ATO)
- Any other prescribed Commonwealth authority or regulator.

BRAZIL

A. Reportable Concerns

In accordance Federal Law No. 12,846/2013 ("Brazilian Clean Companies Act" or "BCCA"), the following breaches can also be reported:

- Offering improper benefits, either directly or indirectly, to public officials or affiliated parties;
- Providing financial support, sponsorship, or any form of subsidy for engaging in illegal activities outlined in the BCCA;
- Employing a third party to conceal true intentions or the identities of beneficiaries involved in an action;
- Obstructing or attempting to influence investigations or audits conducted by public agencies;
- Engaging in bid rigging or committing fraud in bidding processes or associated public contracts.

FRANCE

A. Benefit of legal protection

To benefit from the protection of the Waserman law and its implementing decree, in addition to good faith, a Whistleblower must act "without any direct financial compensation".

B. Facilitators

In France, facilitators, who also benefit from protection, are defined as any natural person or legal entity with a non-profit purpose (for example, a union or an association) that assists a whistleblower in making their report.

C. External reporting procedure

The whistleblower may send an external alert, either after having sent an internal alert, or directly to the competent authorities among those designated by Decree no. 2022-1284 of October 3, 2022 relating to the procedures for collecting and processing alerts issued by whistleblowers and establishing the list of external authorities instituted by Law no. 2022-401 of March 21, 2022 aimed at improving the protection of whistleblowers.

This appendix to the Decree lists the competent authorities by subject matter. It is available here.

FINLAND

A. Facilitators

Protection applies to a facilitator assisting the Whistleblower to file a Whistleblowing alert, third persons who are connected with the Whistleblower and who could suffer retaliation in a work-related context, such as colleagues or relatives of the Whistleblower, and legal entities that the Whistleblower own, work for, or are otherwise connected within a work-related context.

B. External Reporting Procedure

A Whistleblower may send an external alert to the Office of the Chancellor of Justice.

GERMANY

A. Alternative local reporting Channel

A Whistleblower may elect to file an alert locally. The contact detail is: compliance@centricsoftware.com.

B. Facilitators

The following third parties (Facilitators) are protected from retaliation:

- Natural persons who support the Whistleblower in reporting internally, externally or making a public disclosure in a work-related context, if:
    - The information is true or the supporting person has reasonable grounds to

believe that the information is true; and

- The report relates to a reportable breach pursuant to HinSchG (i.e., German implementation law) or the supporting person has reasonable grounds and reasonable suspicion to assume this;

- Protected parties also include:
  - Third parties who have a professional or personal relationship to the Whistleblower (e.g., a colleague) and who may suffer from retaliation in a work-related context, unless retaliation is not a consequence of the report by the Whistleblower;
  - Legal entities and other associations of persons that are legally connected with the Whistleblower, employ the Whistleblower or have another professional ties with the Whistleblower.

C. Reportable concerns

A Whistleblower will be protected from retaliation if the report is based on reasonable grounds and reasonable suspicion. Information about concerns need to be obtained in a work- related context.

The following concerns shall also be reportable:

- Violations regarding public procurement and concession procedures and pertaining to the legal protections in any such procedures above the relevant EU thresholds;
- Violations under the Financial Services Supervisory Act;
- Violations of tax laws applicable to companies;
- Violations in the form of agreements aimed at obtaining a tax advantage in an abusive manner which is contrary to the objective or purpose of the tax law applicable to corporations and partnerships.

D. External Reporting Procedure

The whistleblower may send an external alert, either after having sent an internal alert, or directly to the following competent authorities:

- BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) regarding reports concerning financial services, financial products or the financial markets, money laundering or the financing of terrorism;
- Federal Cartel Office (Bundeskartellamt) regarding reports concerning violations regarding competition law and for the law in force regulating digital markets;
- Federal Office of Justice (Bundesamt für Justiz) regarding reports concerning all other violations.

IRELAND

A. External Reporting Channel

A Whistleblower may send an alert to the prescribed persons listed in Protected Disclosures Act 2014 (Disclosure to Prescribed Persons) Order 2020. In general, prescribed persons have regulatory functions in the area which are the subject of the allegations. Here is a link to the full list of prescribed persons: http://www.gov.ie/prescribed-persons/

A disclosure to a Prescribed Person is a protected disclosure if both these conditions are met:

- The Whistleblower reasonably believes that the relevant wrongdoing is within the remit of the Prescribed Person;
- The information disclosed and any allegations in it are substantially true.

A Whistleblower may also send an alert to the Office of the Protected Disclosures Commissioner, who can identify a suitable Prescribed Person or other suitable person competent to take appropriate action to follow up on the alert.

ITALY

A. Facilitators

The following third parties are protected from retaliation:

- Facilitators, being a natural person who advise a Whistleblower in the reporting process in a work-related context and whose advice is confidential;
- Third parties who have a professional or personal relationship to the Whistleblower (e.g., a colleague) and who may suffer from retaliation in a work-related context;
- Legal entities and other associations of persons having legal capacity that are legally connected with the Whistleblower, employ the Whistleblower or have another professional tie with the Whistleblower.

B. External Reporting Procedure

A Whistleblower may send an external alert to the following competent authority: ANAC ("Autorità Nazionale Anticorruzione"). However, a Whistleblower will benefit from Legal protection only if:

- a report has been sent to the company and the latter has not followed up on the relevant report;
- there are reasonable grounds to believe that if the report is sent internally to the company, it would not be followed up or there is a risk of retaliation for the Whistleblower;
- there are reasonable grounds to believe that there is an imminent or manifest danger to the public interest.

Details for the ANAC can be found here.

JAPAN

A. Who can be a Whistleblower?

Whistleblowers who benefit from protection under the Japanese Whistleblower Protection Act (the "**Japanese Act**") are:

- Employees (in the same meaning as that in 1.A in this Procedure) working for Centric and located in Japan ("**Centric Japan**"),
- Contractors working for Centric Japan who are natural persons, provided that they are subject to control and oversight by Centric Japan to the same extent as employees,
- Temporary staff working for Centric Japan who are dispatched from a third-party staffing agency,
- Former employees, contractors (natural persons) or temporary staff who had been working for Centric Japan but left Centric Japan within one year before making the alert,
- Employees, contractors (natural persons) or temporary staff working for contractors (legal entities) with which Centric Japan enters into an agreement as a contractee or those who left such contractors within one year before making the alert, and
- Directors and statutory auditors of Centric Japan and those of contractors (legal entities) with which Centric Japan enters into an agreement as a contractee.

Shareholders and holders of voting rights (in the same meaning as that in 1.A in this Procedure) at Centric Japan are not included as Whistleblowers who benefit from the Japanese Act.

B. External reporting procedures

A Whistleblower may, simultaneously with or alternatively to sending an alert to Reporting Officers or a local point of contact as described in D. below, send an alert to (i) competent administrative authorities in Japan and (ii) any other person or entity if it is deemed necessary to report a certain fact (the "**Reportable Fact**") to such person or entity in order to prevent the occurrence thereof or the spread of further damages caused thereby, such as mass media (including persons or entities who have been or are likely to be damaged by the Reportable Fact, but excluding those who are likely to cause harm to the competitiveness or other legitimate interests of Centric Japan).

C. What breaches can be reported?

A Breach shall also include a criminal offence, a violation (or attempted concealment of a violation) of the Japanese laws or regulations in general.

D. Alternative local reporting Channel

Whistleblowers may elect to file an alert locally.
The Reporting Officers as defined in 4.1 of the Whistleblowing Procedure shall include a "person who receives a whistleblower alert, and is engaged in the activities for investigating the Reported Facts and taking remedial measures" (公益通報対応業務従事者) (the "**Engaged Person**") under the Japanese Act.

In addition to the Reporting Officers, a person in Human Resource department in Centric Japan who is responsible for the receipt and the investigation of alerts and/or the implementation/management of remedial measures shall be nominated as the Engaged Person who shall comply with the relevant confidentiality obligations under the Japanese Act. If a

Whistleblower wishes to send their alert to the Engaged Person in Japan above, they may send the e-mail to Japan.Ethics@Centric.com.

LITHUANIA

A. External Reporting Procedure

A Whistleblower may send an external alert to the following competent authority: The Prosecutors Office of the Republic of Lithuania.

NETHERLANDS

A. Alternative local reporting Channel

Whistleblowers may elect to file an alert locally. The contact detail is compliance@centricsoftware.com.

B. Facilitators

The following third parties are protected from retaliation:

- A natural or legal person who advises a Whistleblower in the reporting process in a work-related context and whose advice is confidential;
- Involved third-party (*betrokken derde*), being an individual or legal entity connected with a Whistleblower and who/that could suffer a damage as a consequence of the filing of an alert by the Whistleblower;
- Independent officer(s) to whom the suspected suspicion of wrongdoing can be reported and which independent officers can carefully follow-up on that report.

C. External Reporting Procedure

A Whistleblower may send an external alert to the following competent authorities:

- Netherlands Authority for consumers and Markets (*Autoriteit Consument en Markt*);
- Netherlands Authority for the Financial Markets (*Autoriteit Financiële Markten*);
- Netherlands Data Protection Authority (*Autoriteit Persoonsgegevens*);
- Dutch Central Bank (*De Nederlandsche Bank N.*V);
- Dutch Whistleblower Authority (*Huis voor Klokkenluiders*);
- Inspection Healthcare and Youth (*Inspectie gezondheidszorg en jeugd*);
- Dutch Health Authority (*Nederlandse Zorgautoriteit*);
- Authority Nuclear Safety and Radiationprotection (*Autoriteit Nucleaire Veiligheid en Stralingsbescherming*).

SPAIN

Facilitators

A. The following third parties are protected from retaliation:

- Natural persons who, within the framework of the organization in which the Whistleblower provides services, assist the Whistleblower in the process,
- Natural persons who are related to the Whistleblower and who may suffer retaliation, such as co-workers or family members, of the Whistleblower, and
- Legal persons, for whom they work or with whom they maintain any other type of relationship in a work context or in which they hold a significant participation.

B. External Reporting Procedure

The Whistleblower may send an external alert, either after having sent an internal alert, or directly to the following competent authorities:

- Independent Authority for the Protection of the Informant *(Autoridad Independiente de Protección del Informante, AAI);*
- At a regional level, other authorities may be appointed. These regional bodies will, as a general rule, be competent in the regions where the companies are domiciled.

SWEDEN

A. External Reporting Procedure

The national competent authorities for external reporting and information on their respective areas of responsibility, can be found on the following link.

UNITED STATES

The following supplemental provisions apply to reporting within or from the U.S. relating to conduct connected to Centric's business or personnel in the U.S.

Whistleblowers are entitled to escalate reports to applicable federal or state regulators directly at any time (this includes communicating to, cooperating with, responding to any inquiry from or providing testimony to any regulatory or investigatory agency or authority), including without limitation, the United States Securities and Exchange Commission (SEC), United States Department of Labor: Occupational Safety and Health Administration (OSHA) and Whistleblowers are entitled to remain anonymous in doing so. Per Centric policy and applicable laws, retaliation against Centric employees for engaging in activities protected under those laws is prohibited.

Nothing in this Policy is intended to prevent, restrict, limit, impede or otherwise interfere with rights of a Whistleblower to:

- Provide truthful disclosures to or communicate with any US federal or state law enforcement agencies, administrative, regulatory or self-regulatory agency;
- File a charge or complaint or initiate an investigation with an applicable government agency;

- Make other disclosures that are protected under U.S. laws, including for example, to the extent applicable, reporting possible violations of law in accordance with Section 21F of the U.S. Securities Exchange Act of 1934 and related rules;
- Communicate with any government agency or otherwise participate in any investigation or proceeding that may be conducted by any government agency, including providing documents or other information, without notice to or permission by Centric;
- Receive any award for information provided to any government agency; or
- Engage in legally protected communications, including without limitation protections for non-supervisory employees under Section 7 of the U.S. National Labor Relations Act to discuss the terms and conditions of their employment with co-workers or exercising protected rights under Section 7.

A Whistleblower will not be held criminally or civilly liable under any trade secret law for any disclosure of a trade secret that is made in confidence to a government official, or to an attorney and solely for the purpose of reporting or investigating a suspected violation of law or that is made in a document filed in court in a lawsuit.

CentricSoftware

Appendix C – Whistleblowing Hotline by Country

Country	Phone Number
United States	+1 408-345-6581 +1 844-835-7106 -Toll Free
Australia	+61 2 3805 9782 +61 1800 312 437 Toll Free
Brazil	**COMING SOON**
Canada	+1 604-982-7741 +1 833-215-9248 Toll Free
China	**COMING SOON**
Germany	+49 69 50951167 +49 800 6270799 Toll Free
Spain	**COMING SOON**
France	+33 1 59 14 13 79 +33 805 98 02 25 Toll Free
United Kingdom	+44 113 547 7527 +44 808 168 6820 Toll Free
India	**COMING SOON**
Italy	**COMING SOON**
Japan	**COMING SOON**
South Korea	**COMING SOON**
Portugal	**COMING SOON**

DOCUMENT CLASSIFICATION	**External**
DOCUMENT REF	**WB Policy**
VERSION	**1**
DATED	**9/1/2025**
DOCUMENT AUTHOR	**Maria McDonough**
DOCUMENT OWNER	**Legal**

Revision History

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	9/1/2025	Maria McDonough	
2			
3			

Approval

NAME	POSITION	SIGNATURE	DATE
Marina Stavrinides	General Counsel		