Sophos Group Policy

Sophos Whistleblowing Data Processing and Confidentiality Policy

Approved By –Mark Kinzie- VP Compliance

Date of Approval -July 4th 2019

You should read this information before submitting a report via the Whistleblowing portal or hotline.

1. Sophos Whistleblowing Data Processing Information

What personal data we process and store: When you raise a whistleblowing report, we will record your name and contact details unless you raise your report anonymously. Details below.

What your data is used for and where it is processed: The Whistleblowing hotline and portal are provided by NAVEX Global. For the purpose of processing and investigating your report and subject to the provisions of local law, the personal data and information you provide may be accessed, processed and used by the relevant personnel of Sophos, including Human Resources, Finance, Internal Audit, Legal, Corporate Compliance, management, external advisors (e.g. legal advisors), or, in limited circumstances, by technical staff at NAVEX Global. Those individuals may be located in the United States or elsewhere.

How long your data is stored for: The personal data you provide will be kept until 12 months after the resolution of the whistleblowing report.

Your right to access and rectification: You have the right to request access, correction, or erasure of personal data or to object to the processing or receive a copy of the personal data held through this service. Any such request should be directed through the hotline to preserve the confidentiality of the service and your report.

Your right to complain: You have the right to lodge a complaint with the relevant supervisory authority.

2. Confidentiality and anonymity

All calls are treated with strict confidentiality subject to the limited condition below[1]. If your report is filed anonymously, we will not ask you for your name or refer to your gender in your report. Anonymous reporting is not permitted for a limited set of issues in some jurisdictions; details below[2]. We do not capture the telephone number of incoming calls.

2.1 Confidentiality exclusion for legal obligation:

We may transfer or disclose your personal data to any government department, agency, court or other official bodies where we believe disclosure is necessary (i) as a matter of applicable law or regulation (such as in response to a subpoena, warrant, court order, or other legal process), (ii) to exercise, establish, participate in, or defend our legal rights, or limit the damages we sustain in litigation or other legal dispute, or (iii) to protect your vital interests, privacy, or safety, or those of our customers or any other person.

2.2 Reporting Limitations

Within the following countries, Whistleblowing reporting is limited by law to Financial, Auditing and Accounting, Banking, and Anti-Bribery issues:

Austria, Belgium, France, Germany, Hungary, Italy, Luxembourg, Netherlands, Poland, Portugal, Spain, Sweden, Switzerland, United Kingdom

Other issues identified in these countries should be raised through company reporting lines.

In Portugal it is not possible to raise a whistleblowing report about financial issues on an **anonymous** basis. These issues may still be raised **confidentially** within the constraints outlined above.

The Whistleblowing service is not legally permitted in China.