Privacy Notice for Whistleblowing Channel

Last updated: 3 July 2023

Background and summary

People who work for a public or private organisation or are otherwise in contact with such an organisation in the context of their work-related activities are often the first to know about threats or harm to the public interest arising in that context. By reporting breaches of law harming the public interest, such persons act as "whistleblowers" and in that way play an important role in detecting and preventing harmful breaches of law and safeguarding the well-being of society. However, potential whistleblowers are often discouraged from reporting their concerns for fear of retaliation.

Largely for these reasons, the European Union has passed legislation, namely the so-called Whistleblowing Directive[1], to set EU-wide minimum standards for the effective protection of whistleblowers reporting breaches of particularly important EU-level legislation. In turn, the EU member states have implemented these minimum standards in their national laws and, in their consideration, have often decided to go beyond the strictly required minimum by, for example, extending the same standards to breaches of similar national-level laws as well. In Finland, this kind of implementation has been carried out by passing the so-called Whistleblowing Act[2].

In short:

This Privacy Notice covers the collection, use, disclosure and other processing of any personal data that acquired or made available in a whistleblowing process initiated through our channel or otherwise. In addition to possible information on the whistleblowers who report breaches of law to us, this also means any other details that can be associated to personal identities revealed by the whistleblower reports, related information or possible follow-up actions such as investigations and enquiries, including those of any persons involved or mentioned in any capacity or for any reason.

We will not collect personal data which are manifestly not relevant for the handling of a specific whistleblowing report or, if we accidentally do so, we will delete such data without undue delay. Other than that, as a general rule, we will delete any personal data received through our or authority provided whistleblowing channel or through public disclosure within five (5) years of receiving the report.

The personal data of the whistleblower and *any* persons targeted or merely mentioned by such a report, may only be accessed and processed by persons we have specifically designated as responsible for handling the reports. They must and will carry out their duties impartially and independently.

We have the general obligation to fulfil your data subject rights under the EU General Data Protection Regulation (GDPR). Please note, however, that the right of access to the reported data, in particular, may be limited where this is

[1] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.
[2] Act on the protection of persons reporting breaches of European Union and national law (1171/2022).

necessary and proportionate to ensure the accuracy of the report or to protect the identity of the whistleblower.

1 About this Privacy Notice

This Privacy Notice is meant to inform you about the practices of WithSecure Corporation ("**we**", "**our**", "**ours**", "**us**" and similar expressions) regarding the collection, use, disclosure and other such processing of any personal data we have received or obtained about you either as part of or in the context of:

(i) any whistleblowing reports or related information submitted to us through our Whistleblowing Channel (as defined below) by persons who have acquired information on certain serious breach(es) of law in a work-related context as further defined and detailed in Section 1.1 below or report submitted to an authority provided whistleblowing channel or public disclosure by such person; or
(ii) any related investigation or other follow-up actions we have carried out.

Our obligation to provide this information to you is based on the EU General Data Protection Regulation (2016/679, usually called the "**GDPR**"), along with the related Finnish **Data Protection Act** (1050/2018), and applies to you to the extent you are considered a "**data subject**", i.e., a natural person identified or identifiable, directly or indirectly, based on the aforementioned data covered by this Privacy Notice.

In this Privacy Notice, "**Whistleblowing Channel**" refers to the channel and related procedures we have set up in accordance with the Whistleblowing Act, as implemented based on the Whistleblowing Directive, for the internal reporting and follow-up of breaches of certain EU and national laws as specified under said Act and Directive and other possible breaches covered by our Whistleblowing Channel (from this point on, simply jointly referred to as "**breach(es)**").

1.1 Whose personal data does this Privacy Notice cover?

The personal data covered by this Privacy Notice includes information relating to those categories of data subjects listed and defined as follows:

Note

The definitions of data subjects below also contain other definitions that are explained only later in Section 1.2. For reference, however, they are highlighted below in italics*, like these words*, when they appear for the first time.

1) ***reporting person*** (more commonly known as a whistleblower), i.e., a person who has acquired, in a *work-related context*, *information on breaches* while being our employee, director, shareholder, volunteer worker or trainee, a self-employed person working with us, our managing director or a member of our board of directors or administrative board and who *reports* or *publicly discloses* information on breaches;
2) ***facilitator***, i.e., a person who assists a reporting person in the *reporting* process in a *work-related context*, and whose assistance should be confidential;

3) ***person concerned***, i.e., a person who is referred to in the *report* or *public disclosure* as a person to whom the breach is attributed or with whom that person is associated;
4) ***third person connected with reporting person***, i.e., a person who is connected with a reporting person and who could suffer *retaliation* in a *work-related context*, such as a colleague of the reporting person;
5) ***third person mentioned in report***, i.e., any third-party natural person whose identity can be inferred directly or indirectly based on information in the *report*, such as, for example, a witness or colleague;
6) ***person responsible for handling reports***, as designated by us, and/or if the operation of the Whistleblowing Channel has been entrusted to a third party in whole or in part, by that third-party service provider; and
7) ***specialist***, i.e., an expert considered necessary for assessing the accuracy of the allegations made in a *report*, as appointed by us, and/or if the operation of the Whistleblowing Channel has been entrusted to a third party in whole or in part, by that third-party service provider.

1.2 Other definitions

For the purposes of this Privacy Notice, in line with the most important definitions under the applicable laws:

i) "**information on breaches**" refers to information, including reasonable suspicions, about actual or potential breaches, which have occurred or are very likely to occur in the organisation in which the reporting person works or has worked or in another organisation with which the reporting person is or was in contact through his or her work, and about attempts to conceal any breaches;
ii) "**report**" or "**to report**" refer to the oral or written communication of information on breaches, including through our Whistleblowing Channel ("**internal reporting**") or to the competent authorities ("**external reporting**");
iii) "**public disclosure**" or "**to publicly disclose**" refers to making information on breaches available in the public domain;
iv) "**work-related context**" refers to current or past work activities through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information;
v) "**retaliation**" refers to any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person;
vi) "**follow-up**" refers to any action taken by the recipient of a report to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions such as an internal enquiry, an investigation, or the closure of the procedure; and
vii) "**feedback**" refers to the provision to the reporting person of information on the action envisaged or taken as follow-up and on the grounds for such follow-up.

2 Data controller

WithSecure Corporation

Tammasaarenkatu 7, 00180 Helsinki, Finland

0705579-2

Data Protection Officer: Mikko Järvinen

If you have any questions about this Privacy Notice, including any requests concerning your rights as a data subject, please contact us at privacy@withsecure.com.

3 Changes to this Privacy Notice

We may update this Privacy Notice from time to time. When we update this Privacy Notice, we will strive to inform you in a manner consistent with the significance of the changes we make.

4 How do we collect your personal data?

The collection of your personal data may occur in the following ways:

- We may receive information from yourself, for example, if you submit a report or answer possible questions presented to you through our Whistleblowing Channel, or when you are involved, in whatever capacity (including those listed in Section 1.1 of this Privacy Notice), in the submission, receipt, and handling of a report, including carrying out any relevant follow-up actions.
- We may receive information about you from other people, for example by way of a reference to your identity made in a report or in the context of any follow-up action or other handling of the report.
- We may accumulate or obtain information from our internal sources such as from our IT systems and databases during an investigation or other similar follow-up actions.
- We may accumulate or obtain information from external sources such as from authorities having whistleblowing channels or from public due to public disclosure(s);
- We may also obtain additional information during the investigation or other handling of a report or breach by deriving information from or based on data we already have at our disposal. We may, for example, combine, supplement and /or analyse such data to create or derive new information, data sets or data points.
- We may accumulate information pertaining also to the persons responsible for handling reports and related information on breaches, including the name, title, email address, other communication data and timestamp information related to important handling, follow-up and feedback duties and steps, such as the receipt, investigation and assessment of a report, communications with the reporting person as well as any other relevant follow-up and feedback actions in the matter, each as carried out by said persons responsible for handling reports.

5 What data do we process about you?

The categories of personal data we process can vary significantly depending particularly on:

- Your individual and specific position(s) with respect to the report and the breaches reported, in particular, whether you are considered a *reporting person*, a *facilitator*, a *person concerned*, a *third person connected with reporting person* and/or a *third*

person mentioned in report, a *person responsible for handling reports* or a *specialist*, as each defined in Section 1.1;
- the kinds of information each reporting person chooses to provide in connection with submitting a report through the Whistleblowing Channel or information otherwise received by us in relation to the suspected breaches; and
- the kinds of information we obtain and receive when we handle a report and carry out appropriate follow-up actions and give feedback in accordance with the Whistleblowing Act.

In general, we usually process only the following categories of personal data with regard to the reports and their follow-up:

- **Contact details**, such as the name, email address and other contact details of the data subjects listed in Section 1.1 above, where necessary and relevant (e.g., the contact details of reporting persons can be processed only if they have opted to provide them in the first place);
- **Report data**, including personal data included in the contents of a submitted report, the date or timestamp and other metadata of the submission;
- **Communications data**, including any exchange of information and messages between the reporting person and a person responsible for handling reports for us, along with relevant communications metadata. We may be interested in, e.g., obtaining more details from the reporting person. We also have obligations under the Whistleblowing Act to inform the reporting person about the receipt of the report and subsequently, but primarily not later than within three (3) months of informing the person about our receipt of the report, regarding any follow-up actions to be taken in response to the report.
- **System data**, including the technical logs and system event data connected to the use and functioning of the Whistleblowing Channel and the underlying information processing systems; and
- **Additional personal data**, but only to the extent it is necessary for the handling of a report and related information on suspected breaches, including necessary follow-up and required feedback.

We process information concerning so-called special categories of personal data (see Section 6 below for details) and criminal convictions and offences only if and to the extent such processing is necessary for the protection of persons reporting breaches covered by the Whistleblowing Act.

Note

In any case, we will not collect personal data which are manifestly not relevant for the handling of a specific report or, should we accidentally do so, we will delete such data without undue delay.

6 What are the purposes and legal bases for processing your personal data?

Our main purpose for processing personal data in the context of the Whistleblowing Channel is ensuring our compliance with the Whistleblowing Act and any related legislation as well as our related internal policies. More specifically, we process personal data reported or

otherwise received by us in the context of suspected breaches for the purpose of carrying out any prevention, investigation, processing, handling, informing, reporting and other comparable measures that relate to the breaches, including any follow-up actions and their results, such as those of an investigation. Also, where necessary, we may process such data for the purpose of exercising our rights and obligations under the law or establishing, exercising or defending legal claims relevant to our interests in the Whistleblowing Channel and more generally to any other of our legitimate business interests.

The legal bases we rely on for processing your personal data as set out in this Privacy Notice are the following:

- **Legal obligation**: We process your personal data based on legal obligation when the processing is necessary for compliance with legal obligations concerning us, in particular with regard to the obligations of the Whistleblowing Act.
- **Legitimate interests**: To the extent not covered by the above-mentioned legal obligation, we may process your personal data based on legitimate interests where the processing is necessary for the purposes of our legitimate interests and where we have deemed that those interests are not overridden by the privacy interests or fundamental rights and freedoms of the data subjects. In the context of the activities covered by this Privacy Notice, our legitimate interests include ensuring (i) the fulfilment of the general purposes of whistleblowing channels, particularly the detection and prevention of societally harmful breaches of law and the effective protection of the whistleblowers involved, and (ii) compliance with our related internal policies.
- **Bases for processing sensitive data**: In individual circumstances, where the personal data included in a report (or otherwise processed by us in the context of the activities covered in this Privacy Notice) reveals your racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or includes information concerning your health, sex life or sexual orientation (collectively called *special categories of personal data* in the GDPR), or information regarding your criminal offences or convictions, our processing will rely on reasons of substantial public interest in accordance with Article 9(2)(g) of the GDPR and Section 30 of the Whistleblowing Act, provided that the processing is necessary for the protection of persons reporting breaches covered by the Whistleblowing Act. In exceptional cases, said processing may also be based on the establishment, exercise or defence of legal claims as provided for by Article 9(2)(f) of the GDPR.

7 How do we disclose your personal data?

Only where necessary for the purposes detailed above and permitted by the Whistleblowing Act, your personal data may be disclosed to the following recipients and categories of recipients:

- **Persons responsible for handling the reports:** In accordance with our obligations under the Whistleblowing Act, the personal data of *reporting persons*, *persons concerned* and any *third persons mentioned or otherwise identifiable in report* may only be processed by the designated *persons responsible for handling reports* in accordance with said Act.
- **Companies belonging to the same company group:** We may disclose personal data to other companies in the same company group.
- **Public authorities and certain other bodies**: We may disclose personal data to the public authorities detailed in the Whistleblowing Act. In addition, we may disclose

personal data to other parties where it is necessary to establish, exercise or defend legal claims.

- **Third party service providers**: We have concluded a service agreement with Lantero AB ("**Lantero**") which provides the required technical whistleblowing platform for the filing, receipt and various kinds of processing of the reports. We have also entered into a separate service agreement with HH Partners, Attorneys-at-law Ltd ("**HH Partners**"). HH Partners has access to the reports received through the platform and therefore it is the first party to receive any report. HH Partners makes an initial assessment of the report, evaluates the need for further follow-up and liaises with us and the reporting person regarding the report and the issues it raises. In addition, HH Partners assists and advises us in implementing the whistleblowing procedures and policies in general. We have made contractual arrangements with these service providers to ensure they process your personal data only on our behalf and according to our documented instructions.
- **Possible other third-party service providers**: Where necessary, we may also disclose personal data to other third-party service providers, for example, for the purposes of acquiring expert assistance necessary for assessing the accuracy of the allegations made in a report, or for outsourcing other parts of the internal reporting or follow-up (e.g., independent enquiries and investigations), provided that adequate safeguards and guarantees, such as those of respect for independence, confidentiality, data protection and secrecy, are in place in such an arrangement as required by the Whistleblowing Act.

8 Do we transfer your personal data outside the EU/EEA?

As a main rule, your personal data is not transferred to countries outside the European Union or the European Economic Area.

In any case, your personal data may be transferred to countries outside the European Union or the European Economic Area only where the European Commission has held that the country in question ensures an adequate level of protection for personal data, or where we have taken appropriate safeguards to require that your personal data remains protected in accordance with this policy, such as by implementing the Standard Contractual Clauses adopted by the European Commission for international transfers of personal data. Supplementary measures are also implemented, where necessary. You may contact us for more information on the safeguards in place. In exceptional cases, international transfers of personal data may also take place based on (i) your separate and explicit consent, (ii) the establishment, exercise or defence of legal claims, (iii) important reasons of public interest, or (iv) other permissible grounds for transfer under the GDPR or other applicable data protection laws.

For the avoidance of doubt, should the reporting person reside outside the European Union and/or the European Economic Area, any possible personal data included in a report and submitted to us from that place of residence of the reporting person in the context of reporting will be transferred to the EU and/or the EEA to be processed as set out in this Privacy Notice.

9 How long do we retain your personal data?

As a general principle, we will retain your personal data only as long as we have a legitimate reason to retain it for a purpose detailed above in this Privacy Notice. To determine the appropriate retention period, we consider and evaluate the scope, nature and sensitivity of the personal data we process, the potential risk of harm or damage from unauthorised use or disclosure, the purposes for which we process the data and the relevant legal requirements.

Notwithstanding the above, we will delete any personal data received through the Whistleblowing Channel within five years of receiving the report unless their retention is necessary for the exercise of rights or obligations provided for in the Whistleblowing Act or any other law or for the establishment, exercise or defence of legal claims. We will also regularly assess the data we keep, and where we deem the retention unnecessary, we will delete the data without undue delay. A note shall be made of any such assessment.

10 How do we secure your personal data?

We process your personal data in a strictly confidential manner. *Persons responsible for handling reports*, as well as any persons who assist a *reporting person* in the reporting process or provide him or her with legal advice, are under a legal obligation to keep secret any information they have gained on the identity of any *reporting person*, *person concerned* or *third person mentioned in report*. Such confidential information may not be disclosed without the express consent of the person for whose protection the confidentiality has been granted.

To protect your personal data, we also use appropriate technical and organizational measures designed to provide a level of security appropriate to the risk of processing. Such measures include measures to (i) prevent access to personal data by persons who are not designated to handle the reports or said data, (ii) improve the competencies of staff processing personal data, and (iii) ensure and verify a posteriori by whom personal data has been stored, modified or transferred. In addition, the measures include, inter alia, as appropriate, the encryption of personal data, procedures which ensure the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident and procedures by which the effectiveness of technical and organizational measures are regularly tested, assessed and evaluated to ensure the security of the processing. In assessing the appropriate level of security, we take account in particular of risks that are presented by processing, in particular from accidental or unlawful destruction, loss alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

11 Your rights as a data subject

Unless otherwise stipulated below, you may invoke your rights mentioned below by contacting us at the address detailed further above. Please note that as a data subject you do not have the right to restriction of processing with respect to personal data reported under the Whistleblowing Act. Please also note that some of the rights listed below are subject to limitations and are therefore not absolute.

Right of access: You have the right to obtain from us confirmation as to whether personal data concerning you is being processed by us, and where that is the case, access to that personal data.

Please note that the right of access may be limited in relation to personal data reported under the Whistleblowing Act if this is necessary and proportionate to ensure the assessment of the accuracy of the report or to protect the identity of the *reporting person*. However, if only a part of the personal data is covered by such limitation, you still have the right of access with respect to the parts not covered by the limitation. You also have the right to be informed of the reasons for the limitation and to request that the information be provided to the Office of the Data Protection Ombudsman (Finland) in accordance with Section 34 of the Data Protection Act.

Right to rectification: You have the right to obtain from us the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you also have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure ("Right to be forgotten"): You have the right to request the erasure of personal data concerning you. We will act according to your request unless we have a legal obligation or a legitimate reason to retain the data.

Data portability: You may obtain the personal data concerning you which you have provided to us and which are being processed automatically on the legal basis of consent or contract, in a structured, commonly used, and machine-readable format. Please note, however, that the processing covered by this Privacy Notice will rarely, if ever, be based on consent or contract.

Right to object: You may object, on grounds relating to your particular situation, to the processing of your personal data which is based on legitimate interest. Please note, however, that the processing covered by this Privacy Notice is for the most part not based on legitimate interest.

Right to lodge a complaint: If you consider our processing of your personal data to be inconsistent with applicable data protection laws, you may lodge a complaint with the Office of the Data Protection Ombudsman (Finland) (http://www.tietosuoja.fi).