

Privacy Notice for Whistleblowing

Drafted on: 6.6.2022

1 Controller and contact details

Nevel Group (Nevel Oy, Nevel AB, Nevel Eesti OÜ)

Ratatie 11, 01300 Vantaa, Finland

Data Protection Officer: Mikael Calonius; mikael.calonius@nevel.com

2 What is the purpose and the legal basis of processing personal data?

The Whistleblowing channel is maintained to enable reporting of suspected breaches of certain areas of EU law and of Nevel's Code of Conduct. Personal data will be processed for the purpose of investigating whistleblowing reports and carrying out follow-up measures based on the findings.

The legal basis for processing of personal data included in the reports and collected while investigating the reports is Nevel's legitimate interest to prevent reputational risk and to ensure that its business is carried out in an ethical and sustainable manner. GDPR Article 6(1)(f)

3 What data is processed and what is its source?

Whistleblowing reports can be submitted anonymously.

Whistleblowing reports contain information on possible breaches of law. The reports may contain personal data such as names, dates when breaches occurred, descriptions of behaviour, or other information related to the subject-matter of the report. It is possible that individuals are identified from the circumstances described in a report although no names are mentioned.

Although unlikely, it is a possibility that special categories data will be processed in the reports or in the course of investigating the reports. This depends on the subject-matter of the report. Whistleblowers are advised to avoid including unnecessary personal information in the reports.

Data is collected from the whistleblowing reports and, in the course of investigating the reports, from other internal sources such as Nevel's employees and IT-systems related to the subject-matter of the report.

4 Disclosures and transfers of data

By rule, data is not disclosed to external parties unless required by applicable law such as the national laws implementing the Whistleblower Protection Directive.

We use external partners who provide the IT infrastructure and services needed for maintaining the Whistleblowing channel and for carrying out the investigations of the reports. The Whistleblowing channel we use is provided by Gurufield.

Personal data is not transferred outside the EU/EEA.

5 How do we protect the data and how long do we store them?

Only a few people charged with investigating the reports have access to the reports and the information in them. Occasionally, data from the reports may need to be shared with other people in Nevel whose co-operation is required for investigating the report. Any data potentially identifying the whistleblower or other people mentioned in the report will be kept confidential as required by the Whistleblower Protection Directive and the national laws implementing the directive.

Technical security measures include data encryption both in-transit and at-rest, two-factor authentication for maintenance users, patch management and active monitoring for security anomalies.

Personal data included in the reports that is not necessary for carrying out the investigation or follow-up measures will be deleted when the report is received.

Reports and other data collected during the investigation will be stored for two years after the case has been closed and then permanently deleted.

6 What are your rights as a data subject?

Access right

You have the right to obtain confirmation as to whether your personal data is being processed, and when it is, access the personal data.

Right to rectification or erasure

In case you find that your data is inaccurate, you may request its rectification and erasure of the the inaccurate data. In case your data is being unlawfully processed, you have the right to have the data erased.

Right to object and the right to have data processing restricted

Based on grounds relating to your particular personal situation, you have the right to object to the processing of your personal data in situations where the processing is based on Nevel's legitimate interest. When making a request to object, you need to specify the personal situation you are basing your request on. Nevel can refuse the request of objection on legal grounds.

You have the right to demand restriction of the processing of your data for example for the duration of verifying whether your data is accurate based on your claim that it is not.

Right to lodge a complaint

If you think that your data is being unlawfully processed, you have the right to lodge a complaint with a supervisory authority.

Finland: [tietosuojavaltuutettu](#)

Sweden: [Integritetsskyddsmyndigheten](#)

Estonia: [Andmekaitse Inspektsioon](#)