



ROVIO WHISTLEBLOWING REPORTING SYSTEM PRIVACY NOTICE

Last updated: March 11, 2025

This notice explains how Rovio Entertainment Ltd (referred to as “Rovio” or “we” in this document) collects, stores, uses, or otherwise processes the personal data of those who report incidents through our whistleblowing reporting system or are involved in incidents reported through the system (referred to as “you” in this document), and what rights you have if we are processing your personal data. It is important that you read this notice so that you are aware of how and why we may use your data.

1 Data controller

By “data controller,” we mean an entity that determines how and why personal data is processed. With regard to the activities described in this notice, we are the data controller.

2 What can be reported and by who?

The reporting system can be used by individuals who have acquired information on conduct at Rovio, which (i) they have acquired in a work-related context (capturing current and former employees, job applicants, consultants, independent contractors, freelancers, volunteers and suppliers), (ii) they believe is in violation of any of the relevant EU laws (as defined below) and (iii) may lead to imprisonment, a fine, an administrative sanction, or severely endanger the public interest protected by the defined areas of law.

You can report violations regarding the following areas of EU law: public procurement, financial services, products and markets, prevention of money laundering and terrorist financing, product safety, public health, protection of the environment, consumer protection, violations affecting the financial interests of the EU or relating to the internal market (e.g., competition and state aid rules), radiation protection and nuclear safety, food safety, animal health and welfare, consumer rights and protection of privacy, data protection and data security. Depending on the local regulations applicable to you, you may also report on violations of law outside the above list.



3 What data do we process and on what basis?

We process the following personal data in connection with the reporting system:

- **information (for example, the name and position) regarding the individual who reported the incident;**
- **information (for example, the name and position) regarding the employee(s) or member(s) of management to whose conduct the report relates to;**
- **information about the report (for example, the date of submission) and of the incident being reported, which generally includes information relating to the persons involved (for example, their actions or conduct); and**
- **any other personal information that may be included in the report or discovered during a subsequent investigation.**

In practice, after a report is submitted it will be recorded in our reporting system and shared with selected Rovio personnel who have been appointed to handle and resolve the reports. Depending on the contents of the report, relevant information may be communicated to other appropriate personnel who may need to be informed for further investigation and resolution (including certain members of our human resources department and leadership). Where necessary, the information may also be shared with certain third parties, such as our external advisers and competent authorities.

Any personal data provided by you or otherwise processed for the purposes of resolving the reports will be treated with confidentiality and only shared to persons who have a need to know the information.

We do not expect to process any special categories of data relating to you. By special categories of data, we mean genetic, biometric or health information, information revealing racial or ethnic origin, sex life or sexual orientation, political opinions, religious or philosophical beliefs or trade union membership, or information about your criminal offences or convictions. However, we may come to hold this kind of information, for example if an individual includes it in their report.

We process your personal data to comply with our legal obligations and based on our legitimate interest to investigate the report that you submitted to us.



We do not use your data to make automated decisions which significantly affect you. By an “automated decision,” we mean a decision made by an information system without any human intervention.

4 Where do we collect your data from?

We collect your personal data through our reporting system when you submit a report to us.

To investigate and resolve the report we may also collect your personal data internally (e.g. from the employees or management of the Rovio group) or externally (e.g. from our contractors). Additionally, we may contact you through our reporting system and ask you to provide us with more information where needed.

Please note that providing information through the reporting system is not mandatory.

5 Who do we share your data with?

We may share your data with third parties to achieve the purposes described in this notice. This may include sharing data with the following types of recipients:

- competent courts of law or other government authorities where we believe disclosure is necessary as a matter of applicable law or regulation (for example, to investigate suspected violations of anti-bribery, anti-corruption, or securities market laws or other crimes or misconduct such as fraud),
- other companies in the Rovio group (for example, where necessary to investigate a reported incident),
- persons or companies outside of the Rovio group that provide services to us (for example, a contractor that maintains our whistleblowing reporting system), or
- any person or entity where we believe disclosure is necessary to exercise, establish or defend our legal rights or to protect your or another person’s vital interests.

Our reporting system is managed by a third party service provider who is contractually obligated to maintain the confidentiality and security of your personal data. Our



service provider's servers are located inside the European Union (“EU”) and they will not transfer your personal data outside the European Economic Area (“EEA”).

Beyond the data transfer between us and our service provider, your data may in certain cases be transferred to or processed in countries outside of the EU and EEA (for example, where we need to share information with one of our affiliated companies to investigate the report). These countries may have data protection laws that differ from the laws of your country. In these cases, we will provide appropriate safeguards to protect your personal data as required by applicable laws and regulations. These safeguards may include compliance with the European Commission’s standard contractual clauses for transfers of personal data. Upon request, we can provide you a copy of the European Commission’s standard contractual clauses and further details on the applicable safeguards.

6 How long do we keep your data?

We will keep your data for as long as necessary to achieve the purpose(s) for which it was collected (including to investigate and resolve your report) in compliance with any legal requirements regarding the retention and deletion of your personal data.

7 How do we keep your data secure?

We have adopted measures to provide your data a level of security appropriate for the degree of risk involved with the processing activities described in this notice. These measures are designed to protect your data against accidental or unlawful destruction, loss, or alteration as well as unauthorized disclosure or access. The specific measures we employ include, for example, encryption and other technical safeguards, limiting access to the reporting system to those who have a need to have such access and making sure that all persons with access to the reporting system are bound by an appropriate obligation of confidentiality.

8 Your rights

If we are processing your data, you have the right to:

- access, correct, or request the deletion of your data,



- request us to restrict our processing of your data,
- object to our processing of your data to the extent our processing is based on our legitimate interests or the legitimate interests of a third party, or
- where technically feasible, request a copy of the personal data you have provided to us in machine-readable format.

To exercise any of these rights, please contact us at privacy@rovio.com or our Data Protection Officer in writing. To fulfil your request, we need to confirm your identity to verify your right to make the request, which may involve requesting additional information from you. While we will usually not do so, we reserve the right to charge an appropriate fee from you for the exercise of your rights where permitted by applicable laws and regulations.

Finally, you always have the right to lodge a complaint with your local data protection authority regarding our processing of your data. For more information, please contact your local data protection authority (for example, the Office of the Data Protection Ombudsman in Finland).

10 Contact Information

For questions or concerns related to this notice and our processing of your data you may contact our Data Protection Officer at any time at dpo@rovio.com or at:

Data Protection Officer
Rovio Entertainment Ltd
Keilaranta 7
02150 Espoo
Finland

11 Changes

We may update this notice from time to time, for example due to changes in our operations or the legal obligations that apply to us. Any changes will be posted on this page with an updated revision date. We may also inform you of any changes by other means that are appropriate to the significance of the changes.