

APPROVED

At SIA Rīgas nami

29 September 2026

Board Meeting No. VP/RN-2026-50/1.3-1

Personal Data Processing Policy

Rīga

29.09.2026

No. RN-2026-3-pol/2.1-2

*Drawn up in accordance with the General Data
Protection Regulation¹ and the legislation in force in
the Republic of Latvia regarding the protection of
personal data*

CONTENTS

I.	General Issues	2
II.	Organisation of the Processing of Personal Data in the Company	3
III.	Informing Data Subjects about the Processing of Personal Data in the Company	4
IV.	Procedure for Performing the Personal Data Protection Impact Assessment.....	4
V.	Personal Data Processing Register and its Maintenance	5
VI.	Personal Data Processor	5
VII.	Personal Data Violations Commission	5
VIII.	Actions to be Taken by Employees of the Company in the Event of a Violation	6
IX.	Duties and Actions to be Taken by the Specialist in the Event of a Violation.....	6
X.	Duties and Action to be Taken by the Commission in the Event of a Violation.....	7
XI.	Decision-making.....	7
XII.	Notification of the Violation to the Supervisory Institution	7
XIII.	Notification of the Violation to the Data Subject	8
XIV.	Prevention of Repeated Violations	8
XV.	Training of the Employees of the Company	8
XVI.	Final Provisions	8

I. General Issues

1. This Policy (hereinafter – Policy) sets out the procedure by which SIA Rīgas nami (hereinafter – Company):
 - 1.1. ensures the processing and protection of personal data;
 - 1.2. informs data subjects about the processing of personal data performed by the Company;
 - 1.3. performs an assessment of the impact on the protection of personal data;
 - 1.4. performs activities to detect, stop, record, investigate the violations of the protection of personal data, and report the detected violations to the supervisory institution – Data State Inspectorate (hereinafter – DSI) and to data subjects in the cases provided for in the laws and regulations, as well as prevent the consequences of such violations and future violations;
 - 1.5. organises the processing of personal data and provides employee training on the processing of personal data.
2. The processing of personal data is performed in accordance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter – Regulation) and the Personal Data Processing Law.
3. The Policy applies to both the automated and manual processing of personal data, regardless of whether the Company is the processing controller or the processor of the personal data.
4. The processing of personal data in electronic form is performed in compliance with the requirements set out in the Information Security Policy and the Provisions for the Use of Information Systems of the Company.
5. The following terms are used in the Policy:
 - 5.1. **Processor** – a person authorised by the Company/partner of the Company who, on the basis of a written contract, in accordance with the instructions of the Company as the controller, processes Personal data in accordance with the scope and for the purposes specified in the concluded contract;
 - 5.2. **Special categories of personal data** – data revealing race or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health data, or data concerning the sex life or sexual orientation of a natural person;
 - 5.3. **Data subject** – a natural person who can be identified, directly or indirectly, by identifiers such as name, surname, personal identity number, location, etc.;
 - 5.4. **Cybersecurity manager** – an employee of the Information Technology (IT) Department of the Company, whose duties include the implementation and oversight of cybersecurity measures;
 - 5.5. **Notification** – notification of the Violation to the DSI and/or the Data subject in the manner provided for by the laws and regulations;

¹REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)

- 5.6. **Violation** – a Personal data violation that results in the loss, unauthorised destruction, alteration, disclosure, access to, or affecting the integrity or availability of Personal data under the control of the Company, whether intentionally (deliberately) or by negligence;
 - 5.7. **Violation reporting e-mail** – rndatuspec@rigasnami.lv;
 - 5.8. **Personal data** – any information relating to the Data subject;
 - 5.9. **Employee of the Company** – persons specified in the internal documents and orders of the Board of the Company, who are entitled to perform the processing of Personal data for the performance of their duties;
 - 5.10. **Specialist** – a certified Personal data protection specialist engaged by the Company to monitor the compliance of the processing of Personal data by the Company with the requirements of laws and regulations, to advise the Company on issues related to the protection of Personal data, to cooperate with the DSI and organise annual training of the employees of the Company on the protection of Personal data, to provide consultations on the processing and protection of Personal data, to take measures to ensure the registration of changes in the processing of Personal data;
 - 5.11. Terms not defined in Clause 5 of the Policy are used in the Policy in accordance with their meaning in the Regulation.
- 6. The Company ensures that the processing of Personal data is only performed by an employee of the Company and/or by a Personal data processor and ensures that it is possible to identify Personal data that have been processed without the relevant authorisation, as well as the time of processing and the person who performed it.
 - 7. The employees of the Company and other persons (including external service providers and their employees) who have access to Personal data held by the Company provide written assurance of the non-disclosure of Personal data.

II. Organisation of the Processing of Personal Data in the Company

- 8. The Company complies with the following conditions when initiating and evaluating the new processing of Personal data:
 - 8.1. The Company ensures that each instance of processing of Personal data has:
 - 8.1.1. a specified purpose for the processing of Personal data;
 - 8.1.2. identified persons responsible for the processing of Personal data;
 - 8.1.3. assessed the legal basis, and in the case of legitimate interests, performed a balancing test between the interests of the controller and the interests of the Data subject;
 - 8.1.4. determined the range of persons who would need access to the information;
 - 8.1.5. set the storage period of the Personal data;
 - 8.1.6. determined the technical resources to be used for the processing of Personal data;
 - 8.1.7. defined the set of technical and organisational measures to be applied in the processing of Personal data;
 - 8.1.8. assessed whether an impact assessment on the protection of Personal data is necessary.
 - 8.2. The initiation of new processing of Personal data is to be performed with the prior agreement of the Specialist and in compliance with the principle of Personal data protection by design and Personal data protection by default as set out in Article 25 of the Regulation.
 - 8.3. The initiation of new processing of Personal data arises from laws and regulations, contractual relations, the consent given by the natural person, the needs of the Company which the divisions of the Company are charged with performing in the interests of the Company, as well as in other lawful and justified cases.
 - 8.4. Initiated if there are doubts as to the compliance of such processing of Personal data

- with the requirements of the Regulation or other applicable laws and regulations.
- 8.5. A public procurement (regardless of the type of procurement provided for by law) within the framework of which it is intended to engage a Personal data Processor or to establish a new Personal data processing process, as well as to establish or change a Personal data processing system for the processing of Personal data in the Company, must not be announced before the planned Personal data processing process has been evaluated and a decision on its implementation has been taken. The technical specifications or the draft contract must include the requirements necessary to ensure the adequate processing of Personal data.
 - 8.6. Where the new draft processing of Personal data is based on the legal basis provided for in Article 6(1)(f) of the Regulation, an assessment of the legitimate interest must be carried out accordingly when deciding whether or not to proceed with the further processing of Personal data.
 - 8.7. Processing of Personal data by employees of the Company must only be performed if the provisions of Clause 8.1 of the Policy are complied with.
 9. The heads of the divisions of the Company must inform their employees about the permitted processing of Personal data.
 10. The Specialist informs the employees of the Company about the basic principles of the processing of Personal data.
 11. Where changes are made to the processing of Personal data, the person responsible for the processing of Personal data concerned ensures that information on the changes to the processing of Personal data is provided to the Specialist, informing the latter of the purposes of the processing of Personal data, the legal basis for the processing, categories of Data subjects, types of processing, categories of recipients, types of acquisition, places of processing, types of transfer to other countries which are not members of the European Union or the European Economic Area, as well as information resource or technical resource holders and those responsible for information systems security.

III. Informing Data Subjects about the Processing of Personal Data in the Company

12. The Company, subject to Articles 13 and 14 of the Regulation, informs the Data subject of its processing of Personal data by posting the privacy disclaimers set out in Clause 13 of the Policy on the website of the Company or, upon request, by sending them to the Data subject individually.
13. The following notices and their English translation is published on the website of the Company:
 - 13.1. Privacy Notice;
 - 13.2. Personal Data Processing Notice for applicants and other data subjects involved in the recruitment process;
 - 13.3. use of website cookies.
14. The Specialist, after updating the data processing register as set out in Clause 18 of the Policy, reviews the personal data processing notices of the Company and updates them where necessary.

IV. Procedure for Performing the Personal Data Protection Impact Assessment

15. For the purpose of initiating the new processing of Personal data using new technologies, taking the nature, scope, context, and purposes of the processing into account, the Specialist, in accordance with the information provided by the division responsible for the processing of Personal data and Clause 10 of the Provisions, performs an assessment of the impact of the processing of Personal data on the protection of Personal data (hereinafter – Assessment).

16. After the Assessment, the Specialist prepares a summary of the Assessment, including the shortcomings identified, and submits it to the head of the division responsible for the processing of Personal data.
17. It is prohibited to start the new processing of Personal data if the shortcomings identified in the Assessment affecting compliance with the basic principles of processing of Personal data have not been prevented.

V. Personal Data Processing Register and its Maintenance

18. The Company maintains a Personal Data Processing Register (hereinafter – Data Processing Register) in accordance with the requirements of Article 30 of the Regulation.
19. A Data Processing Register is established and maintained for all processing activities of the Company.
20. The employees of the Company are bound by the purpose and legal basis for the processing of Personal data as set out in the Data Processing Register and are prohibited from processing Personal data in a manner contrary to that set out in the Data Processing Register.
21. The Data Processing Register is created, maintained, and updated in accordance with the performance of the tasks and delegated functions of the Company in the processing of Personal data.
22. The creation of the Data Processing Register and its subsequent updating is performed by and under the responsibility of the Specialist. In cooperation with the persons in charge of the divisions of the Company, the Specialist updates the Data Processing Register at least once in a calendar year.
23. The Data Processing Register is kept in accordance with the file nomenclature of the Company and is accessible to the employees of the Company.

VI. Personal Data Processor

24. In cases where the Company enters into service contracts, the responsible division assesses whether the other party to the contract will process Personal data as part of the performance of the contract.
25. If the processing of Personal data will be performed as part of the performance of the contract, the contract includes a set of technical and organisational measures to be implemented by the Processor to comply with the requirements set out in the Regulation.
26. Contracts in which the Processor will process Personal data are subject to the approval of the Specialist of the Company.
27. The division which has concluded the contract for the processing of Personal data ensures the control of the performance of the contract in compliance with the requirements of Article 30(2) of the Regulation.

VII. Personal Data Violations Commission

28. The Company establishes a Personal Data Violations Investigation Commission (hereinafter – Commission), comprising the following members of the Company:
 - 28.1. Specialist;
 - 28.2. Cybersecurity manager;
 - 28.3. Head of the Legal Department.
29. The Specialist has the duty to:
 - 29.1. once per working day, during working hours, check the information received on the Violation reporting e-mail to determine whether any information has been received about a possible Violation;
 - 29.2. provide an opinion as to whether a Violation has been established;

- 29.3. identify the Violation and advise the responsible employees on its prevention, suspension, avoidance, or mitigation;
- 29.4. maintain the Register and supplement/update the information therein in the cases specified in the Policy;
- 29.5. manage the work of the Commission;
- 29.6. advise the Board and the employees of the Company;
- 29.7. provide annual training to employees on the recognition, identification, and opportunities to stop or mitigate the adverse effects of potential Violations;
- 29.8. perform other duties as prescribed by applicable laws and regulations.
- 30. The Cybersecurity manager has the duty to:
 - 30.1. ensure that the information systems of the Company comply with the security requirements set out in the laws and regulations;
 - 30.2. stop, prevent, or mitigate Violations of information systems;
 - 30.3. provide an opinion to the Specialist and the Commission on whether the information systems of the Company have been affected by a Violation;
 - 30.4. cooperate with the Commission in the investigation of the Violation;
 - 30.5. advise the Board and the employees of the Company;
 - 30.6. perform other duties as prescribed by applicable laws and regulations.
- 31. The Commission has the duty to:
 - 31.1. assess the Violation;
 - 31.2. detect, stop, prevent, or mitigate the Violation;
 - 31.3. prepare opinions on Violations;
 - 31.4. prepare recommendations for the prevention of further Violations.
- 32. The heads of the divisions of the Company are responsible for the risks of Violations in the processes under the responsibility of their divisions and are obliged to take all the necessary actions within their competence to ensure the prevention and termination of Violations in the processing of Personal data in the divisions under their responsibility, as well as, in coordination with the Specialist and the Cybersecurity manager, to ensure the implementation of necessary internal procedures to prevent the occurrence of Violations in the future.
- 33. The data processed in the Information Systems (IS) is the responsibility of the Information resource holder of the specific IS, who is appointed by the order of the Board of the Company.

VIII. Actions to be Taken by Employees of the Company in the Event of a Violation

- 34. Upon the detection of a possible Violation, an employee of the Company must immediately, but no later than within eight hours, report:
 - 34.1. to the Specialist, by sending an e-mail to rndatuspec@rigasnami.lv, indicating his/her name, surname, information about the possible Violation, the consequences of the possible Violation, as well as information about the actions taken to prevent, stop, or mitigate the possible Violation, and providing his/her contact information (telephone number and e-mail address) for further communication;
 - 34.2. to his/her line manager in cases where the alleged Violation has been established in the division of the employee, providing information on the alleged Violation, the consequences of the alleged Violation, as well as information on the actions taken to prevent or stop the Violation and to prevent or mitigate the consequences of the Violation.

IX. Duties and Actions to be Taken by the Specialist in the Event of a Violation

- 35. If the Specialist determines that the information received may indicate that a Violation has

occurred, they must take the following steps:

- 35.1. immediately take the measures within their competence to prevent or stop the Violation;
- 35.2. obtain information about the Violation and its consequences;
- 35.3. inform the Cybersecurity manager if the Information Systems of the Company have been affected;
- 35.4. within 12 hours of receipt of the information, provide the Commission with information on the alleged Violation (the facts of the Violation) and its assessment, and convene a Commission meeting.

X. Duties and Action to be Taken by the Commission in the Event of a Violation

36. The Commission meetings are closed. The Commission has the right to invite the Board of the Company, heads of divisions, and other employees of the Company to its meetings.
37. Minutes must be taken of the Commission meetings. Minutes of the meetings are taken by the Secretary of the Commission (hereinafter – Secretary).
38. The functions of the Secretary of the Commission are performed by the head of the Legal Department.
39. The Commission assesses the alleged Violation immediately, but no later than within 12 hours, and decides whether or not a Violation has occurred. If the Commission finds that a Violation has occurred, it assesses:
 - 39.1. to which category of Personal data it relates;
 - 39.2. the number of Data subjects involved;
 - 39.3. the circumstances that led to the Violation;
 - 39.4. the extent of the impact of the Violation on the Data subject;
 - 39.5. other circumstances and criteria that enable the assessment of the significance of the specific Violation;
 - 39.6. the necessary corrective measures to prevent the recurrence of a similar Violation.
40. If the Commission has established that a Violation has occurred, an opinion on the Violation must be drawn up no later than 12 hours after the decision establishing the Violation has been taken, and the Specialist must inform the Board of the Violation by submitting the opinion of the Commission. If this is not possible, the Commission will set a different deadline by means of a reasoned decision.
41. The opinion of the Commission includes information on the Violation, setting out proposals for further action, including whether, in accordance with the Regulation, information regarding the Violation must be provided to the DSI and Data subjects.

XI. Decision-making

42. The Board of the Company must, within 24 hours of receipt of the opinion of the Commission, consider it and decide whether to report the Violation to the DSI and/or the Data subject.
43. If the Board of the Company has confirmed that the Violation may pose a risk to the rights and freedoms of the Data subject, a decision must be taken to perform the Notification, indicating whether it is to be performed in respect of the DSI or in respect of the Data subject.

XII. Notification of the Violation to the Supervisory Institution

44. Notification to the DSI must be made by means of a notification by the Company containing the following information:
 - 44.1. nature of the Violation, the categories and approximate number of Data subjects affected, and the types and amount of Personal data affected;
 - 44.2. name, surname, contact details or other point of contact of the Specialist from whom

further information can be obtained.

45. The Notification is prepared by the Specialist and signed by the Board of the Company.

XIII. Notification of the Violation to the Data Subject

46. Notification of the Violation to the Data subject is made by the Company sending a notification to the Data subject containing the following information:

- 46.1. nature of the Violation;
- 46.2. name, surname, contact details or other point of contact of the Specialist from whom further information can be obtained;
- 46.3. possible consequences of the Violation;
- 46.4. measures taken by the Company to prevent the Violation and mitigate its possible adverse effects.

47. The Notification is prepared by the Specialist and signed by the Board of the Company.

XIV. Prevention of Repeated Violations

48. In order to prevent the recurrence of similar Violations, within 30 days after the adoption of the decision of the Board of the Company confirming the fact of the Violation, the Commission identifies the necessary improvements to be made to the information systems of the Company, other means of processing Personal data and internal processes of the Company (including the need to reassess the relevant purpose of data processing), as well as the preliminary timeframes for making the necessary improvements and prepare a relevant report (hereinafter – Report) to be submitted to the Board of the Company.

49. If the Board determines that the Violation is the result of the actions of the Processor, the Report includes information on the necessary improvements, which the Processor is instructed to perform.

50. The Board of the Company examines the Report and decides on the improvements to be made, the timeframe for their implementation, and the performers thereof.

XV. Training of the Employees of the Company

51. The Specialist conducts, at least once a year, training of the employees of the Company on the protection of Personal data and information on data protection measures.

52. The Specialist, in cooperation with the Administrative Department of the Company, ensures the preparation of tests on Personal data protection issues and the testing of the knowledge of the employees of the Company, as necessary.

XVI. Final Provisions

53. The Board of the Company reviews the Policy and the documents drawn up and approved on the basis thereof once a year and updates them as necessary to ensure compliance with external and other internal laws and regulations of the Company.

54. The Board of Directors reports to the Council once a year on the progress and results of the implementation of the Policy.

55. The Company ensures that employees are made aware of the Policy in accordance with the procedures laid down by the Company. The Policy is available on the information system for document management of the Company and on the website of the Company.

56. Upon the Policy coming into force, the Personal Data Processing Policy No. RN-2024-5-pol/2.1-2 dated 20.08.2024 becomes invalid.