SIA Rīgas nami | Reg. No. 40003109638
Rātslaukums 5, Riga, LV-1050
T: +371 66 957 267
E: rigasnami@rigasnami.lv | www.rigasnami.lv

APPROVED
SIA "Rīgas nami"
August 20, 2024
board meeting no. VP/RN-2024-34/1.3-1

SIA Rīgas nami Personal Data Processing Policy

Riga

August 20, 2024

no. RN-2024-5-pol/2.1-2

Developed in accordance with the General Data Protection Regulation[1] and the laws and regulations in force in the Republic of Latvia in the field of data protection of natural persons

I. General Issues

1. This Policy (hereinafter – Policy) sets out the procedure by which SIA Rīgas nami (hereinafter – Company):
   1.1. ensures 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. activities are performed to detect, stop, record, investigate the violations of the protection of personal data and to 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 to prevent the consequences of such violations and future violations;
   1.5. organises the processing of personal data and provides employee training on 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 automated and manual processing of personal data, regardless of whether the Company is the processing controller or the processor of the personal data.

[1] 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)

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. **Data subject** – a natural person who can be identified, directly or indirectly, by identifiers such as name, surname, personal identity number, location, etc;
   5.2. **Personal data** – any information relating to the Data subject;
   5.3. **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;
   5.4. **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;
   5.5. **Violation reporting e-mail** – rndatuspec@rigasnami.lv;
   5.6. **Notification** – notification of the Violation to the DSI and/or the Data subject in the manner provided for by the laws and regulations;
   5.7. **Register** – the Register of Infringements, which records all signs that have caused a Violation in the Company, as well as alleged and detected Violations;
   5.8. **Employee of the Company** – persons specified in the internal documents of the Company, by orders of the Board, who are entitled to perform processing of Personal data for the performance of their duties;
   5.9. **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;
   5.10. **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 performed only 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 a written assurance of non-disclosure of Personal data.

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

8. The Company complies with the following conditions when initiating and evaluating a 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. initiation of a 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. 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 departments 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 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 further processing of Personal data;
   8.7. processing of Personal data by employees of the Company must be performed only 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 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 by the Company

12. The Company, subject to Articles 13 and 14 of the Regulation, informs 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 a new processing of Personal data using new technologies, taking into account the nature, scope, context and purposes of the processing, 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 a new processing of Personal data if the shortcomings identified in the Assessment affecting the 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 is 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), which are composed of the following members of the Company:
    28.1. specialist;
    28.2. IT security 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 IT Security 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 IT Security 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 detection of a possible Violation, an employee of the Company must immediately, but no later than within eight hours, report:
    34.1. 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 provides his/her contact information (telephone number and e-mail address) for further communication;
    34.2. 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 first becomes aware that **a Violation has occurred**, the Specialist takes the following actions:
    35.1. immediately take such action as is within his/her competence to prevent or stop the Violation and to eliminate or mitigate its consequences if not taken by the employee who discovered the Violation, and make a notation to that effect in the Register;
    35.2. obtain information about the Violation and its consequences;
    35.3. inform the IT Security Manager if the information systems of the Company have been affected;
    35.4. report to the Commission and, if applicable, to the head of the division to which the Violation applies, giving any necessary instructions for further action;
    35.5. within 24 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 meeting of the Commission.

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 division and other employees of the Company to its meetings.
37. Minutes must be taken of the meetings of the Commission. Minutes of the meetings are taken by the Secretary of the Commission (hereinafter – Secretary).
38. The functions of the Secretary are performed by the head of the Legal Department.
39. The Commission immediately, but not later than within three working days of receipt of the notification of the Violation from the Specialist, takes the following actions:
    39.1. assess the Violation;
    39.2. assess whether the Violation may pose a risk (including a high risk) to the rights and freedoms of the Data subject;
    39.3. prepare and submit an opinion on the Violation to the Board of the Company.
40. If the Commission finds that the Violation has not occurred, the Violation has been remedied or terminated and the consequences of the Violation have not occurred, the Commission documents its finding and the reasons for it by entering the information in the Register.
41. If the Commission finds that the Violation has occurred but its possible adverse consequences have been remedied and there is a low risk that the rights and freedoms of Data subjects may be affected, the Commission documents its finding and the reasons for it by entering the information in the Register.
42. If the Commission finds that (<u>one of the following cases</u>):
    42.1. it is not possible to establish unequivocally from the information obtained that a Violation has occurred;
    42.2. it is not possible to establish unequivocally from the information obtained that the consequences of a Violation have occurred;
    42.3. it is not possible to establish unequivocally from the information obtained that there is no risk to the rights and freedoms of the Data subject.

    The Commission documents its opinion and the reasons for it, enter the information in the Register, adding the information obtained as a result of the assessment of the alleged Violation.
43. If the Commission finds that a Violation has occurred and is likely to result in a risk to the rights and freedoms of Data subjects, the Commission documents its finding and the reasons for it by entering the information in the Register together with the information obtained as a result of the Violation.
44. The opinions of the Commission include at least the following information:

44.1. description of the Violation;
44.2. facts indicating a possible Violation;
44.3. information on the actions taken to end the Violation;
44.4. facts indicating the possible occurrence of the consequences of the Violation;
44.5. actions taken to prevent or mitigate the consequences of the Violation;
44.6. whether the Company is the Controller or the Processor in relation to the data processing in respect of which the alleged Violation has been identified;
44.7. whether the Violation is the result of the actions (including omissions thereof) of the Processors;
44.8. whether the Violation is likely to result in adverse consequences for the Company;
44.9. whether there is a risk to the rights and freedoms of the Data subject;
44.10. whether the risk to the rights of the Data subject is considered to be high;
44.11. whether information about the Violation must be provided to the DSI and to the Data subject.

XI. Decision-making

45. The Board of the Company must, within 72 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.
46. 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.
47. The date of the discovery of the Violation is:
    47.1. the date of the decision of the Board of the Company on the discovery of the Violation;
    47.2. the date on which information of the Violation was received in cases where the Violation is obvious (e.g. lost or stolen data media on which personal data is stored).

XII. Notification of the Violation to the Supervisory Institution

48. Notification to the DSI must be made by means of a notification by the Company containing the following information:
    48.1. nature of the violation, the categories and approximate number of Data subjects affected, the types and amount of Personal data affected;
    48.2. name, surname, contact details or other point of contact of the Specialist where further information can be obtained.
49. The notice is prepared by the Specialist and signed by the Board of the Company.

XIII. Notification of the Violation to the Data Subject

50. Notification of the Violation to the Data subject is made by the Company sending a notice to the Data subject containing the following information:
    50.1. nature of the Violation;
    50.2. name, surname, contact details or other point of contact of the Specialist where further information can be obtained;
    50.3. possible consequences of the Violation;
    50.4. measures taken by the Company to prevent the Violation and mitigate its possible adverse effects.
51. The notice is prepared by the Specialist and signed by the Board of the Company.

XIV. Prevention of Repeated Violations

52. 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.

53. 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.
54. 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 Company Employees

55. 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.
56. 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. Transitional Provision

57. Provisions No. RN-2021-9-not/2.1-5 of 10 September 2021 "SIA Rīgas nami Personal Data Processing Provisions" becomes null and void upon the entry into force of this Policy.

Annexes:

1. Annex – Register of Personal Data Violations.

SIA Rīgas nami | Reg. No. 40003109638
Rātslaukums 5, Riga, LV-1050
T: +371 66 957 267
E: rigasnami@rigasnami.lv | www.rigasnami.lv

Annex 1
to SIA Rīgas nami Personal Data Processing Policy

Register of Personal Data Violations

No.	Question	Entry	Recorder (name, surname, position)	Date, time of entry
1.	Who provides information about the Violation?	*Name, surname, position, information about the external source providing information about the Violation and its status (data subject, processor, business partner of the Company, customer, DSI).*		
2.	How and when did the Specialist receive information about the Violation?	*Date, time of notification of the Violation by e-mail, telephone, verbal, internet notification.*		
3.	When and how was the Violation initially discovered?	*Type, date, time of discovery. If the person reporting the Violation is different from the person who discovered the Violation, indicated the name, surname, and position of the person who discovered the Violation.*		
4.	Information about the circumstances of the Violation – when, what happened, with what types of personal data?	*Circumstances of the Violation, date, time, what types of personal data were affected.*		
5.	What is the information on the actual or foreseeable possible consequences of the Violation?	*The consequences or foreseeable possible consequences of the Violation.*		
6.	Whether, when, by whom and how were the consequences or possible consequences of the Violation prevented, mitigated?	*Yes/no, name, surname, position, time, date, type of mitigation.*		
7.	Is the Violation ongoing, whether, when and by whom has the Violation been stopped?	*Yes/no, name, surname, position of the person who stopped the Violation, actions taken to stop the Violation.*		

8.	Has the Specialist obtained or clarified information about the circumstances or possible consequences of the Violation in addition to the initial information? What kind?	*Yes/no, circumstances of the Violation, date, time, what types of personal data were affected. Clarification of the initial information.*		
9.	What actions has the Specialist taken to prevent/mitigate the consequences of the Violation or to stop/prevent the Violation?	*Description of the activities.*		
10.	Have the information systems of the Company been affected by the Violation? Has the Specialist notified the Head of IT?	*Yes/No. Name of the systems, description of the type of impact, consequences, date, time when the information was provided to the Head of IT of the Company.*		
11.	If the Violation is not detected whether, when and to whom has it been reported?	*Name, surname, position, information about the external source providing information about the Violation and its status (data subject, processor, third parties involved, DSI), time, date, type, link to the notification.*		
12.	Has the Commission obtained or updated information on the circumstances or possible consequences of the Violation in addition to the initial information and the information provided by the Specialist? What kind?	*Yes/no, circumstances of the Violation, date, time, what types of personal data were affected. Clarification of the initial information.*		
13.	Has the Commission established the Violation?	*Yes/No. Circumstances of the Violation (loss of confidentiality, integrity, accessibility), supporting facts, evidence, if no violation has been established, link to the document containing the basis for such decision.*		
14.	If no Violation is found, when has the Commission issued an opinion?	*Time, date, type, link to the opinion.*		
15.	When did the Board of the Company receive the information about the Violation from the Commission?	*Time, date.*		
16.	Will the Violation be reported to the DSI?	*Yes/No, type of notification.*		
17.	Will the Violation be reported to data subjects?	*Yes/No, type of notification.*		
18.	Was the Violation reported to the DSI and if so, when?	*Yes/No. Time, date, link to notification.*		

19.	Was the Violation reported to the data subjects and if so, when? How were they notified?	*Yes/No. Time, date, type of notification, link to notification.*		