

FINAL VERSION

PRIVACY, COOKIE AND PERSONAL DATA PROCESSING POLICY

Clear information about data collection, use, retention, cookies, User Journey analytics and your rights.

DATA CONTROLLER	UAB „SANDĖLIUKŲ NUOMA“
LEGAL ENTITY CODE	305125975
WEBSITE	www.sandeliukunuoma.lt
VERSION	2.2
EFFECTIVE DATE	29 July 2026

Scope. Website, customer Account and self-service portal, enquiries, reservations, orders, agreements, access control, video surveillance, IVR, call recording, analytics and advertising attribution.

Contents

1. General Provisions	3
2. Definitions	3
3. Data Controller	4
4. Personal Data We Collect	4
5. Legal Bases for Processing	5
6. Purposes of Processing	6
7. Customer Account and Self-Service Portal	7
8. Telephone Calls, IVR and Call Recording	7
9. Cookies	8
10. Google Analytics and Marketing Technologies	9
11. User Journey and Tracking Events	9
12. Google Ads, Facebook Ads and UTM Parameters	10
13. Automated Decision-Making	11
14. Recipients of Personal Data	11
15. Transfers Outside the European Union	12
16. Retention Periods	12
17. Security Measures	13
18. Data-Subject Rights	13
19. Procedure for Handling Requests	14
20. Children's Data	14
21. Contact Information	15
22. Final Provisions	15

This document should be read together with the interactive real-time cookie list on the Website and the agreement for the relevant service.

1. General Provisions

1.1. This Privacy, Cookie and Personal Data Processing Policy (the "Policy") explains how UAB "SANDĖLIUKŲ NUOMA" processes the personal data of natural persons when they:

- visit the website www.sandeliukunuoma.lt, its subpages or related self-service pages (the "Website");
- create and use a customer account or self-service portal;
- submit an enquiry, make a reservation, place an order, rent or otherwise use our services;
- communicate with us by telephone, email, contact forms or other channels;
- enter premises or areas administered by us where electronic access control and/or video surveillance are in operation;
- represent a customer, supplier, partner or another legal entity.

1.2. The Policy applies to Website visitors, existing and prospective customers, customer representatives, payers, beneficiaries, visitors to our premises and other persons whose data we lawfully receive while providing services.

1.3. Merely visiting the Website does not constitute consent to non-essential cookies, analytics, User Journey tracking or marketing. Where consent is required for data processing, we request it separately, clearly and before such processing begins.

1.4. Refusing consent to non-essential cookies or marketing does not restrict access to the core functions of the Website or our services. Only optional functions that require a specific third-party technology may be unavailable.

1.5. This Policy has been prepared in accordance with Regulation (EU) 2016/679 (the General Data Protection Regulation, the "GDPR"), the Law of the Republic of Lithuania on Legal Protection of Personal Data, the Law of the Republic of Lithuania on Electronic Communications and other applicable legislation.

1.6. This Policy is an information document. It does not replace the terms of rental, service, self-service or other agreements.

2. Definitions

2.1. Personal data means any information relating to an identified or identifiable natural person.

2.2. Processing means any operation performed on personal data, including collection, recording, organisation, storage, use, linking, disclosure, restriction, erasure or destruction.

2.3. Controller or We means UAB "SANDĖLIUKŲ NUOMA", which determines the purposes and means of processing.

2.4. Processor means a service provider that processes data on our behalf and in accordance with our instructions.

2.5. Data subject or You means the natural person whose personal data we process.

2.6. Customer means a natural person or a representative of a legal entity who enquires about services, enters into an agreement or uses services.

2.7. Account means an electronic customer account or self-service environment used to order and manage services.

2.8. Cookie means a small text file stored on a user's terminal device. In this Policy, cookies also include similar technologies such as browser local storage ("localStorage"), pixels, software identifiers and URL tracking tags.

2.9. Tracking Event means a record of an action performed on the Website, such as a page view, use of a filter, link click, reservation, enquiry, order stage or payment confirmation.

2.10. User Journey means the linking over time of multiple visits, sessions and Tracking Events using pseudonymous identifiers and other signals in order to understand the path leading to an enquiry or order.

2.11. UTM parameters mean URL tags used to identify the source, channel, campaign and advertising content of a visit, such as `utm_source`, `utm_medium`, `utm_campaign`, `utm_content` and `utm_term`.

2.12. Advertising click identifiers mean tags generated by advertising platforms, such as gclid, gbraid, wbraid, fbclid or similar identifiers.

2.13. Profiling means the automated use of personal data to analyse or predict certain aspects of a person's behaviour, interests or actions.

3. Data Controller

3.1. The data controller is:

Detail	Information
Company name	UAB "SANDĖLIUKŲ NUOMA"
Legal entity code	305125975
Address	Eitminų g. 20-120, Vilnius, Lithuania
Telephone	+370 616 44445
Email	info@sandeliukunuoma.lt
Website	www.sandeliukunuoma.lt

3.2. Where a specific service is provided under an agreement by another legal entity, its identity and contact details as a separate controller will be stated in the agreement, order form or a separate privacy notice.

3.3. For any questions concerning this Policy, data processing or the exercise of your rights, please contact us by using the email or postal address specified in Clause 3.1.

4. Personal Data We Collect

4.1. Identity and contact data:

- first name and surname;
- telephone number, email address and residential or correspondence address;
- personal identification number, date of birth or identity document details only where necessary to verify identity, enter into an agreement, comply with legal requirements or administer a debt;
- legal entity name, registration number, position, basis of representation and representative's contact details;
- vehicle registration number where required for parking or access services.

4.2. Enquiry, reservation and contract data:

- selected location, property, premises, storage unit, parking space or other service;
- date, status and reference number of an enquiry, waiting list entry, reservation, order or agreement;
- service period, price, discounts, additional services, amendments and termination information;
- submitted documents, confirmations, consents, requests, claims and correspondence;
- information about representatives, authorised users, additional contact persons and emergency contacts where provided by you.

4.3. Payment, accounting and debt data:

- information about invoices, payments, refunds, overpayments, debts and recovery;
- payment amount, date, purpose, identifier, status and payer details lawfully received from a payment service provider or bank;
- data contained in accounting and tax documents.

4.4. Account and access-control data:

- account identifier, login name, password hash, authentication and recovery tokens;
- date and time of login, IP address, device and session information and actions performed in the Account;
- identifier of an electronic key, mobile access or other access device;

- date, time and place of entry or exit, access status, unsuccessful attempts and changes made by an administrator.

4.5. Video surveillance data:

- image of a person, direction of movement, date, time, camera and monitored location;
- incident-related information where a recording is retained for longer in order to investigate an incident, defend rights or comply with a law-enforcement request;
- we do not normally collect audio data unless separate and clear information is provided at the relevant location.

4.6. Website technical and usage data:

- IP address, approximate location, device type, browser, operating system, language and screen parameters;
- visit date, time and duration, referring page, pages viewed and URLs;
- searches, selected filters, favourite properties, comparisons, sharing actions and map or route clicks;
- clicks on and copying of telephone numbers, email addresses, addresses, review links or registration links;
- contact, reservation and waiting-list forms and order and payment stages;
- error, performance, security and system-operation logs.

4.7. Analytics, User Journey and advertising-attribution data:

- random or pseudonymous internal user identifier;
- Google Analytics client and session identifiers (client_id, session_id);
- cookie, localStorage, Google Ads, Meta or other advertising identifiers;
- UTM parameters and advertising click identifiers;
- Tracking Events, their time, sequence, parameters and relationship to a visit;
- conversion, order or payment status, amount and pseudonymous transaction identifier;
- consent status, category, date, time and technical evidence of consent.

4.8. Communication data:

- content, attachments, date and time of emails, forms, chats and other messages;
- caller and called telephone number, call date, time, duration and status;
- IVR language and menu selections and call routing, forwarding and answering data;
- telephone-call audio recording, voicemail message and related handling notes;
- your selected communication channels and marketing preferences;
- information you voluntarily provide when resolving a question or incident.

4.9. Sources of data. We receive data directly from you, your representative or employer, from your device and browser, from technologies used on the Website, from payment, access, telephony, PBX and IVR service providers, banks, public registers, debt-administration partners and public authorities where permitted by law.

4.10. We do not intentionally collect special categories of personal data, such as data concerning health, political opinions, religious beliefs or biometric data used for identification. Please do not provide such data unless necessary. If you provide such data on your own initiative, we will process it only where a lawful basis exists and only to the extent necessary to resolve the relevant matter.

4.11. We do not store full payment card details on the Website. Card data are processed during payment by the selected payment service provider under its own privacy terms. We receive only the information necessary to administer the payment.

5. Legal Bases for Processing

5.1. We process personal data only where at least one of the legal bases set out in Article 6 GDPR applies:

Legal basis	When it applies
Taking steps before entering into and performing a contract, Article 6(1)(b) GDPR	When we respond to your request, including a request made by telephone or voicemail, before entering into an agreement, accept a reservation or order, enter into and perform a service agreement and administer an Account, payments and access
Legal obligation, Article 6(1)(c) GDPR	When we are required to maintain accounting and tax records, respond to public authorities, comply with anti-money-laundering requirements or meet other applicable legal obligations
Legitimate interests, Article 6(1)(f) GDPR	When we record customer-service calls to ensure service quality, verify agreements and instructions and handle complaints or disputes, protect property and systems, operate video surveillance and access control, prevent fraud, administer debts, defend legal rights, improve services using aggregated data and maintain business relationships
Consent, Article 6(1)(a) GDPR	When we use non-essential cookies, analytics, User Journey or advertising tracking, personalised advertising or direct marketing where no statutory exception applies

5.2. The requirements of the Law of the Republic of Lithuania on Electronic Communications also apply when information is stored on or accessed from your terminal device. Non-essential technologies are activated only after prior consent has been obtained.

5.3. We send direct electronic marketing after obtaining consent or, where permitted by law, to existing customers in relation to our own similar services, provided that we obtained the contact details in connection with the provision of services, offered a clear opportunity to object and provide such an opportunity in every message.

5.4. Where we rely on legitimate interests, we assess the necessity of the processing, its impact on your rights and your reasonable expectations. You may object to such processing as described in Section 18.

5.5. Data identified as necessary for entering into and performing a contract are mandatory. If you do not provide them, we may be unable to verify your identity, enter into an agreement, provide access, issue an invoice or provide the service. Data processed on the basis of consent are optional.

6. Purposes of Processing

6.1. We process personal data for the following purposes:

- to provide information, respond to enquiries and prepare offers;
- to receive, route and answer calls and administer callback requests and voicemail messages;
- to record customer-service calls in order to ensure service quality, verify agreements, instructions and other business communications and handle complaints and disputes;
- to administer waiting lists, reservations, orders and agreements;
- to create and manage an Account and self-service portal;
- to grant, modify and revoke electronic access;
- to provide services, support customers and send contract-related communications;
- to receive and reconcile payments, issue accounting documents and administer refunds and debts;
- to protect persons, property, premises and information systems and investigate incidents;
- to prevent fraud, misuse and breaches of service rules;
- to ensure Website stability, resolve errors and perform technical diagnostics;
- subject to consent, to measure Website use, create User Journeys, analyse the sales funnel and measure advertising return;
- to attribute enquiries and purchases to campaigns, measure conversions and optimise advertising;
- to conduct direct marketing and manage marketing preferences;
- to prepare summaries, forecasts and business analyses using anonymous or aggregated data wherever possible;

- to establish, exercise or defend legal claims and comply with instructions from competent authorities.

6.2. Communications concerning contract performance, such as payment, access, reservation, security or service-change notifications, are not direct marketing and may be sent without separate marketing consent.

6.3. We do not use data for a new purpose that is incompatible with the original purpose without first assessing compatibility or obtaining a new legal basis and, where necessary, informing you.

7. Customer Account and Self-Service Portal

7.1. An Account may be created at your request, during an order or after entering into an agreement. The Account may contain identity, contact, service, document, payment, access and activity-log data.

7.2. We use Account login and activity logs for authentication, service provision, security, incident investigation and dispute resolution.

7.3. You are responsible for the accuracy of the data provided and the confidentiality of your login credentials and must inform us without delay of any suspected unauthorised access or lost device or access credential.

7.4. Login credentials must not be disclosed to third parties. To grant access to another person, use the authorised-user function provided for that purpose or contact us.

7.5. Closing an Account does not mean that all Customer-related data are immediately erased. Agreements, invoices, payments, access logs, evidence of consent and data needed for disputes are retained for the periods specified in Section 16.

7.6. If an Account is unused or services have been terminated, we may deactivate it. Where reasonably practicable, we will provide advance notice of planned deactivation.

8. Telephone Calls, IVR and Call Recording

8.1. When you call our publicly listed customer-service telephone numbers, we may process the caller's and called number, call date, time, duration and status, selected IVR language and menu option, call routing or forwarding data, call audio recording, voicemail message and notes entered by an employee while handling the matter.

8.2. Incoming calls to numbers on which IVR and recording are enabled are recorded 24 hours a day, including outside business hours, at weekends and on public holidays. Recording also applies to calls routed by IVR or forwarded to the responsible employee.

8.3. Before call recording begins, the IVR provides a clear notice about the recording in Lithuanian, English or Russian, depending on the selected language. If you do not agree, we recommend visiting our nearest office or contacting us by email. Audio recording of the call begins only after this notice has ended.

8.4. We record calls in order to:

- ensure and monitor the quality of customer service;
- accurately record enquiries, requests, instructions, agreements and other business communications;
- handle complaints, claims and disputes and establish, exercise or defend legal claims.

8.5. Where the content of a call is necessary to respond to your enquiry, take steps before entering into an agreement or perform an agreement, we process it under Article 6(1)(b) GDPR. We record calls for the purposes set out in Clause 8.4 on the basis of our legitimate interests under Article 6(1)(f) GDPR, after assessing the necessity of the processing, your reasonable expectations and the impact on your rights and in compliance with applicable electronic-communications and confidentiality requirements. We do not rely on consent as the legal basis for call recording.

8.6. If you do not wish the call to be recorded, you may end the call and contact us by email or through the Website contact form. If you object to recording during the call, you may end the call and use those alternative channels. Where technically and organisationally possible, we will offer another non-recorded method of communication. You may exercise your right to object to processing based on legitimate interests as described in Sections 18 and 19.

8.7. IVR selections and the telephone number are used to route the call to the appropriate function or responsible employee. The call may be forwarded to an employee's business telephone or another telephone

approved for work purposes. Data are displayed and disclosed only to persons who need them in order to handle the call.

8.8. If a call is not answered, you may voluntarily leave a voicemail message after the information notice and audio signal. Before recording, we inform you that the message will be recorded and sent to the responsible employee. The audio recording may be sent to a shared email mailbox assigned to the relevant function, and an authorised employee may receive an SMS notification that a message has been left. The SMS notification must contain only the minimum data necessary to perform the task.

8.9. Call recordings, voicemail messages and related technical data may, where necessary, be accessed by our authorised employees and providers of telephony, PBX, IVR, call-recording, email, SMS and IT services and, in the event of a complaint, dispute or legal claim, by legal advisers, insurers, courts, law-enforcement bodies or other competent authorities.

8.10. If a telephony or related service provider transfers data outside the EEA, the safeguards described in Section 15 apply.

8.11. We normally retain telephone-call recordings for 12 months from the date of recording. We retain a voicemail message for up to 30 calendar days after the matter has been resolved, but no longer than 90 calendar days after it was left. We retain IVR and call technical logs for up to 12 months. If a specific recording is required for a complaint, dispute, investigation or legal claim, a segregated copy may be retained until the matter has been finally resolved and the applicable limitation period has expired.

8.12. You may request access to or a copy of your call recording, object to processing based on legitimate interests and request restriction or erasure where the conditions of the GDPR are met. To locate a specific recording, we will ask you to provide the telephone number, approximate date and time of the call and any other information necessary for identification.

8.13. An employee's voice and other personal data may also be processed during the call. Employees are separately informed through internal procedures about such processing, access rights, purposes of use and retention periods.

9. Cookies

9.1. We use cookies and similar technologies to enable the Website to function, remember preferences and maintain security and, subject to consent, to perform analytics, create User Journeys, measure conversions and display more relevant advertising.

9.2. Cookie categories:

Category and examples	Purpose	Lifetime on the user's device	Legal basis
Essential: session, authentication, CSRF, security, load-balancing and consent-preference cookies; Cloudflare security cookies, if used	Website operation, login, security and retention of consent preferences	For the session or up to 12 months, depending on the function	Contract or legitimate interests; terminal-device access exemption for essential functions
Functional: language, favourites, comparison, selected location or other convenience settings	Remembering your preferences and enabling additional functions	Normally up to 12 months	Consent
Statistics and analytics: <code>_ga</code> , <code>_ga_<ID></code> , <code>_gid</code> , internal analytics identifier, if used	Traffic, action, conversion, error and usage statistics	From the end of the session up to 24 months; <code>_gid</code> normally up to 24 hours	Consent
Marketing: <code>_gcl_au</code> , <code>_fbp</code> , <code>_fbc</code> , advertising click identifiers, UTM records and similar tools, if used	Advertising attribution, conversion measurement, audience creation and personalised advertising	Normally up to 3 months; the specific duration is shown in Cookie Settings	Consent
Third-party content: map, booking, review or video tools, if embedded	Providing optional external content or functionality	As determined by the relevant provider	Consent, except for a simple external link

9.3. The table provides a summary of the principal tools. The exact name, provider, purpose, category and lifetime of the cookies and other technologies in use at any given time are shown in the interactive Cookie

Settings panel on the Website. That list forms an integral part of this Policy and must be updated whenever the Website technologies change.

9.4. On your first visit, you may:

- accept all non-essential cookies;
- reject all non-essential cookies;
- select individual cookie categories.

9.5. We do not use preselected non-essential categories. The "Accept" and "Reject" buttons must be equally easy to access, and rejection must not be made more difficult by additional unnecessary steps.

9.6. You may change or withdraw consent at any time by selecting Cookie Settings at the bottom of the Website or through the permanently available icon. Withdrawal does not affect the lawfulness of processing carried out before withdrawal but stops the future use of the relevant technologies.

9.7. You may also delete or block cookies through your browser. Browser blocking may remove the stored consent preference, in which case you may be asked to make a new selection during your next visit.

9.8. The lifetime of a cookie may be renewed during a later visit only where consent for the relevant category remains valid.

10. Google Analytics and Marketing Technologies

10.1. Subject to your consent, we may use Google Analytics 4, Google Tag Manager, Google Ads conversion measurement, Meta business tools and other analytics or marketing technologies listed in Cookie Settings.

10.2. Google Analytics 4 helps us evaluate traffic, usage trends, actions, conversions and Website performance. Events may be sent from the browser and from server to server using the Google Analytics Measurement Protocol.

10.3. We may send pseudonymous `client_id` and `session_id` identifiers, event name and time, page, device information, UTM and advertising click parameters, conversion status and amount and a pseudonymous transaction identifier to Google Analytics.

10.4. We do not intentionally send a personal identification number, first name, surname, unencrypted email address, telephone number, payment card data or special-category data to analytics or advertising platforms. Website URLs and event parameters must not be constructed so that they contain such data.

10.5. Google states that Google Analytics 4 does not log or store IP addresses in the Analytics system. However, subject to your consent, our internal Tracking Events system may store the IP address separately as described in Sections 11 and 16.

10.6. We configure Google Analytics user-level and event-level data retention for a period not exceeding 14 months, except for aggregated standard reports to which Google may apply different retention logic. The retention period for our internal analytics is specified in Section 16.

10.7. Analytics or advertising data are not collected and no User Journey is created until the relevant consent has been obtained. If consent is refused, only essential technical and security logs may be processed, and they are not used to create a cross-session marketing profile.

10.8. If we enable Google Signals, remarketing, advertising personalisation or similar advanced features, they operate only after marketing consent has been obtained and are identified in Cookie Settings.

11. User Journey and Tracking Events

11.1. We use User Journey to understand how a visitor finds the Website over one or more visits, which functions they use, when they submit an enquiry or order and which campaign contributed to the conversion.

11.2. Subject to statistics and/or marketing consent, depending on the selected category, our internal administration system may record:

- each page view and its time;
- searches, filters, favourites, comparisons and sharing actions;
- clicks on telephone numbers, email addresses, addresses, route, review and registration links;

- stages of the contact form, waiting list, reservation, ordering and payment process;
- IP address and browser and device technical data;
- internal identifier and Google Analytics `client_id` and `session_id`;
- UTM and advertising click parameters;
- order amount, status and pseudonymous transaction identifier.

11.3. These data may be linked across different sessions. If you later provide contact details, make a reservation or place an order, the previous pseudonymous journey may be linked to a specific enquiry, order or Customer.

11.4. An IP address is not used as the sole reliable method of identifying a person. It may be shared by several users and is used only as one of several technical, security or attribution signals.

11.5. User Journey and Tracking Events are used for sales-funnel analysis, campaign performance, conversion attribution, Website improvement and statistics. We do not use them to make decisions that would in themselves produce legal or similarly significant effects for you.

11.6. Each internal Tracking Event record, including the IP address, `client_id`, `session_id`, UTM and advertising parameters, is retained for no longer than 36 months from creation unless it must be preserved for a specific dispute or legal requirement.

11.7. After consent is withdrawn, no new consent-based events are recorded. Data already collected and linked to you are erased or irreversibly anonymised unless another legal basis permits their continued retention.

11.8. In order to handle a request concerning User Journey data, we may ask you to provide an available browser or Google Analytics client identifier, the time of the visit, the device used, order number or other information that helps us reliably locate your records.

12. Google Ads, Facebook Ads and UTM Parameters

12.1. Subject to your consent, we use UTM parameters, advertising click identifiers, conversion tags and, where enabled, Meta Pixel and/or a server-side conversions interface to measure Google Ads and Facebook/Instagram advertising campaigns.

12.2. We may collect and store:

- `utm_source`, `utm_medium`, `utm_campaign`, `utm_content`, `utm_term`;
- `gclid`, `fbclid` and other identifiers assigned by a platform;
- advertising campaign, ad-group, advertisement or channel labels;
- first-visit and last-visit source;
- conversion type, time, value and status and a pseudonymous order identifier.

12.3. UTM and advertising parameters may be temporarily stored in browser `localStorage` or a cookie so that they are not lost while navigating between Website pages and can be linked to a later conversion.

12.4. After successful payment confirmation, we may send an advertising or analytics platform a purchase or other conversion event, its value and pseudonymous attribution identifiers. We do not send payment card data.

12.5. Google and Meta may use received data to measure conversions, create audiences, personalise advertising and secure their systems in accordance with their privacy documents and your choices on their platforms.

12.6. If an advertising-click URL contains personal data that we did not request and that are not required for attribution, we endeavour not to record them or to remove them. Advertising campaign URLs must not be created using a name, email address, telephone number, personal identification number or other direct identifier.

12.7. UTM and advertising-attribution data are retained in our internal system for up to 36 months from creation of the relevant record. The retention periods of identifiers stored on a device are shown in Cookie Settings.

13. Automated Decision-Making

13.1. We do not currently make decisions based solely on automated processing, including profiling, that produce legal effects or similarly significantly affect you within the meaning of Article 22 GDPR.

13.2. Analytics and advertising tools may automatically:

- group visitors according to actions or interests;
- attribute a conversion to an advertising channel;
- create remarketing audiences;
- optimise advertising delivery or bids on an advertising platform;
- display certain properties, recommendations or offers based on previous selections.

13.3. These actions do not in themselves determine whether you may enter into an agreement, the essential terms of an agreement, creditworthiness, access rights or other legally significant decisions.

13.4. If we introduce automated decisions falling within Article 22 GDPR in the future, we will first provide information about the logic involved, significance, expected consequences and applicable safeguards.

14. Recipients of Personal Data

14.1. Personal data may be disclosed, only to the extent necessary for the relevant purpose, to:

- our employees, managers and authorised service administrators;
- providers of Website, self-service, database, cloud, hosting, content-delivery, cybersecurity and IT-maintenance services;
- programming, technical-analysis, marketing and advertising partners;
- Google Ireland Limited, Google LLC and entities engaged by them;
- Meta Platforms Ireland Limited, Meta Platforms, Inc. and entities engaged by them;
- payment service providers, banks and financial institutions, including Paysera LT, UAB, where their payment method is selected;
- accounting, invoicing, CRM, email, document-management, telephony, PBX, IVR, call-recording and SMS providers;
- authorised employees and service administrators who receive calls or handle voicemail messages;
- providers of electronic access control, security and video-surveillance systems;
- providers of map, booking or review tools, such as Google Maps or Calendly, where you choose to use these functions;
- auditors, insurers, lawyers, debt-recovery companies, bailiffs, notaries, courts and dispute-resolution bodies;
- police, tax authorities, supervisory authorities and other public bodies where we are required or lawfully permitted to disclose data;
- a purchaser of the business or assets, investor or its advisers where a transaction is contemplated and confidentiality is ensured.

14.2. We require processors to process data only on our instructions, ensure confidentiality and security, assist in the exercise of your rights and erase data after the service relationship ends.

14.3. Where a payment, advertising, mapping or other platform itself determines some of the purposes for which data are used, it may act as an independent controller or, to the extent provided by law, a joint controller. Its own privacy notice will then also apply.

14.4. We do not sell personal data.

15. Transfers Outside the European Union

15.1. We seek to process data within the European Union and the European Economic Area (the "EEA"). However, group companies and infrastructure of some international technology providers, including Google, Meta, cloud, security or booking platforms, may be located in the United States or other countries outside the EEA.

15.2. When transferring data outside the EEA, we rely on at least one lawful transfer mechanism:

- a European Commission adequacy decision;
- the EU-US Data Privacy Framework, where the US recipient holds a valid certification and the transfer falls within its scope;
- European Commission standard contractual clauses and, where necessary, additional technical and organisational measures;
- another mechanism provided for in Chapter V GDPR.

15.3. We assess the service provider's location, scope of the transfer, sensitivity of the data, contractual safeguards and the need for additional measures.

15.4. You may obtain information about the safeguard applicable to a specific transfer, or a copy of it with commercial and security-confidential information removed, by contacting us using the details in Section 21.

16. Retention Periods

16.1. We do not retain data longer than necessary for the purpose for which they were collected or than required by law. The principal retention periods are:

Data category or purpose	Retention period
General enquiries and correspondence where no agreement is entered into	Up to 24 months after the last meaningful contact
Waiting-list data	Until an offer is made or the person unsubscribes and for up to 12 further months where required for administration or a dispute
Incomplete reservations or orders	Up to 12 months after the last action, unless another basis applies
Active Account and service-administration data	For the duration of the agreement and Account; individual documents are retained further in accordance with the periods below
Agreements, orders, handover documents and related evidence of performance	For the duration of the agreement and normally for 10 years after its expiry, taking account of applicable limitation periods
Invoices, payment and accounting documents	For the period required by law, normally 10 years from the date of the document or transaction
Debt and debt-recovery data	Until the debt is paid, recovery is completed and the applicable limitation period has expired
Access-control event logs	Up to 12 months after the event; longer only where required for an incident, dispute or legal claim
Video-surveillance recordings	Normally up to 30 calendar days; an extract relating to an incident is retained until completion of the investigation, dispute or proceedings
Telephone-call recordings	Normally 12 months from the date of recording; a copy segregated for a specific complaint, dispute, investigation or legal claim is retained until the matter has been finally resolved and the applicable limitation period has expired
Voicemail messages	Up to 30 calendar days after the matter has been resolved, but no longer than 90 calendar days after the message was left
IVR and call technical logs	Up to 12 months after the record was created
Essential technical and security logs	Up to 12 months after the record was created, except for evidence of an incident

Data category or purpose	Retention period
User Journey, IP address, client_id, session_id, UTM parameters, advertising identifiers and Tracking Events in our internal system	No longer than 36 months after creation of each record
Google Analytics 4 user-level and event-level data	No longer than 14 months under our settings; different provider logic may apply to aggregated reports
Cookies and data on a user's device	As stated in the table in Section 9 and the current Cookie Settings list
Direct-marketing contacts	Until consent is withdrawn or an objection is received; evidence of valid consent and opt-out is retained for up to 3 years after the preference ends
Data-subject requests and responses	Up to 3 years after the request has been finally resolved, and longer only in the event of a dispute

16.2. Erased data may remain in backup copies for a limited backup cycle, normally up to 90 days. Such data are not used for normal operations and must be erased again if a backup is restored.

16.3. At the end of the retention period, we erase, irreversibly anonymise or securely destroy the data.

16.4. We may extend a retention period where data are required for an ongoing investigation, dispute, court proceeding, legal claim or instruction from a competent authority. In that case, data are used only for that specific purpose.

16.5. Withdrawal of consent or deletion of an Account does not remove our obligation to retain accounting, contract, payment, security or dispute data where another valid legal basis applies.

17. Security Measures

17.1. Taking account of the nature and scope of processing and the risks involved, we implement technical and organisational measures, including:

- restricting access rights according to job functions and periodically reviewing them;
- user authentication, password hashing and, where appropriate, multi-factor authentication;
- encrypted transmission and, where appropriate, encryption of data at rest;
- logging system actions, logins and security events;
- protecting networks, servers, end-user devices, backups and systems against malware;
- data minimisation, pseudonymisation, automated retention periods and segregation of access;
- restricted access to call recordings and voicemail messages, activity logging and automatic-deletion settings in telephony and related systems;
- procedures for deleting voicemail messages and their copies from shared email mailboxes after the retention period;
- provider due diligence and confidentiality and data-processing agreements;
- employee confidentiality obligations and training;
- procedures for detecting, managing and reporting personal-data breaches.

17.2. Complete security of data transmitted or stored over the internet cannot be guaranteed. If a personal-data breach is identified, we assess and manage it and, where required, notify the State Data Protection Inspectorate and affected persons.

17.3. Please use a unique and secure password, do not disclose login credentials, log out of shared devices and inform us immediately of any suspicious activity.

18. Data-Subject Rights

18.1. Subject to the circumstances of processing and the conditions laid down in the GDPR, you have the right to:

- obtain confirmation as to whether we process your data, access the data and receive a copy;

- request rectification of inaccurate data and completion of incomplete data;
- request erasure where the legal basis for processing no longer exists or another ground under the GDPR applies;
- request restriction of processing;
- receive data that you have provided in a structured, commonly used and machine-readable format and, where technically feasible, transmit them to another controller where processing is based on consent or contract and is carried out by automated means;
- object, on grounds relating to your particular situation, to processing based on legitimate interests;
- object at any time and free of charge to direct marketing, including related profiling;
- withdraw consent at any time as easily as it was given;
- not be subject to a decision based solely on automated processing that produces legal or similarly significant effects where the protection of Article 22 GDPR applies;
- lodge a complaint with the State Data Protection Inspectorate or bring proceedings before a court.

18.2. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

18.3. The right to erasure is not absolute. We may refuse a request to the extent that data are required to comply with a legal obligation, prove an agreement, maintain accounting records, establish or defend legal claims or apply another exception under the GDPR.

18.4. Upon receiving an objection to direct marketing, we stop such marketing to the relevant contact. We may place the minimum contact details on a suppression list solely to ensure that your preference is respected in the future.

18.5. When requesting access to or a copy of a telephone-call recording, please specify the telephone number used and the approximate date and time of the call. Before providing a recording, we may remove or mask other persons' data and ask for additional information to verify your identity.

19. Procedure for Handling Requests

19.1. You may submit a request by email to info@sandeliukunuoma.lt, by post or in person at Eitminų g. 20-120, Vilnius, Lithuania.

19.2. We recommend that your request include your first name, surname, contact details for the response, the right you wish to exercise and sufficient information to identify the relevant data, such as the Account email address, agreement or order number, visit period or available analytics identifier.

19.3. If we have reasonable doubts about the identity of the person making the request, we may ask for additional information. Please provide only the data necessary to verify identity. We request a copy of an identity document only in exceptional cases, and unnecessary information should be concealed.

19.4. We respond without undue delay and no later than one month after receiving a request. Taking account of the complexity and number of requests, we may extend this period by a further two months and will inform you of the extension and reasons within the first month.

19.5. Requests are handled free of charge. If a request is manifestly unfounded or excessive, in particular because it is repetitive, we may charge a reasonable administrative fee or refuse to act, providing reasons for our decision.

19.6. If we refuse a request in whole or in part, we provide a reasoned response and information about the right to lodge a complaint with the State Data Protection Inspectorate or bring proceedings before a court.

20. Children's Data

20.1. Our rental and related contractual services are intended for adults or persons lawfully representing a legal entity.

20.2. We do not knowingly ask persons under 14 years of age to independently provide consent-based data through the Website. If an information-society service were offered directly to a child under 14 and the processing were based on consent, parental or guardian consent would be required.

20.3. A child's image or other data may be incidentally processed through video surveillance, access control or incident administration when the child visits the premises with a Customer. The same security, necessity and retention requirements apply in such cases.

20.4. If you believe that a child has provided data without an appropriate legal basis, please contact us. After verifying the circumstances, we will erase the data or take other necessary action.

21. Contact Information

21.1. For questions concerning privacy, cookies, data processing or the exercise of your rights, please contact:

Contact	Information
Data controller	UAB "SANDĖLIUKŲ NUOMA"
Address	Eitminų g. 20-120, Vilnius, Lithuania
Email	info@sandeliukunuoma.lt
Telephone	+370 616 44445

21.2. You may lodge a complaint concerning the processing of personal data with:

Supervisory authority	Information
Name	State Data Protection Inspectorate of the Republic of Lithuania
Address	L. Sapiegos g. 17, LT-10312 Vilnius, Lithuania
Email	ada@ada.lt
Website	vdai.lrv.lt

21.3. Before lodging a complaint with the supervisory authority, we invite you to contact us first so that we can promptly investigate the matter.

22. Final Provisions

22.1. We periodically review and may update this Policy following changes to our services, technologies, purposes of processing, providers or applicable law.

22.2. The current version of the Policy is published on the Website. The version number and effective date are stated at the beginning of the document.

22.3. Where material changes may significantly affect your rights or choices, we will provide advance notice through the Website, Account, email or another appropriate channel where required.

22.4. If a change requires new consent, we will not treat previous consent as sufficient and will ask you to make a new choice.

22.5. If any provision of this Policy becomes invalid or unenforceable, the remaining provisions remain valid.

22.6. Version 2.2 of this Policy takes effect on 29 July 2026 and replaces the previous privacy policy published on the Website from that date.