D-5

# Privacy and Personal Data Processing Policy

Dalaway digital platform

| Version | Publication date | Effective date |
|---|---|---|
| **1.0** | **01.10.2026** | **01.10.2026** |
| Operator | Original language | Publication URL |
| **SteppeGate LLP, BIN 260140019690, Republic of Kazakhstan** | **Russian** | **https://dalaway.kz/legal/privacy** |

This Policy explains what personal data the Operator processes, for what purposes, on what basis, to whom they are transferred, how long they are retained and what rights the subject has. The Policy provides information about processing and does not replace separate consent: consents are executed as standalone documents.

## 1. Who processes the data

1.1. The owner and operator of the database containing personal data is SteppeGate LLP, BIN 260140019690, the owner and operator of the Dalaway digital platform. Correspondence address: 010000, Astana, Saryarka District, Berdibek Sokpakbayev Street, building 5, non-residential premises 44, Arlan Business Centre, 3rd floor.

1.2. The Operator appoints, by internal order, a person responsible for organising personal data processing. Data subjects' enquiries and questions about personal data processing are accepted at privacy@dalaway.kz.

## 2. To whom the Policy applies

2.1. This Policy applies to visitors to the Platform website, persons requesting a demonstration, registered Users, Participants' representatives and employees, and persons whose information is contained in documents submitted by Participants.

2.2. Capitalised terms have the meanings defined in section 2 of the Accession Agreement for the Dalaway digital platform.

## 3. Processing principles

3.1. The Operator observes the following principles:

1. lawfulness and transparency of processing;

2. collection only of data necessary and sufficient for the stated purposes;
3. prohibition of processing for purposes incompatible with the stated purposes;
4. ensuring data accuracy and the ability to update them;
5. limiting retention to achievement of the processing purpose or another lawful basis;
6. confidentiality, access controls and the application of legal, organisational and technical protection measures.

## 4. What data are processed

4.1. Categories of data processed:

| Category | Contents |
|---|---|
| Personal account data | First name, last name, patronymic (if provided), email address, telephone number, account identifier, language and other settings, email and telephone verification markers, profile image (if uploaded) |
| Authentication data | Password in a protected transformed form, session information, one-time verification codes |
| Corporate role data | Participant's name, position, Platform role, scope of authority granted, invitation information, history of granting and revoking access |
| Verification data | Information and documents necessary to verify the Participant and its representative's authority: electronic digital signature data, powers of attorney, letter of authority, corporate documents, to the extent necessary |
| Platform use data | Lots, Requests, Offers, Transactions, correspondence, details of Parties' Contracts, uploaded documents, statuses of Appendices, Trading Operations and Services Centre orders |
| Settlement data | Fee Calculations, Certificates of Work Performed (Services Rendered), invoices, payment information, Participant's bank details |
| Technical data | Device network address, date and time of actions, browser and device information, session identifiers, online presence and last login information, security and activity logs, checksums of accepted documents |
| Data collected using cookies | Information collected using cookies and similar technologies, including browser local storage. Their contents, purposes and retention periods are disclosed in the Policy on the Use of Cookies and Similar Technologies (D-10) |
| Demonstration request data | Last name and first name, email address, company name, role or position, telephone number if provided, request content and technical information about submission of the form |
| Completed Transaction rating data | Rating given by a party to a completed Transaction, text of the rating and response, role of the rating party, Transaction number, date and time. Displayed without the User's last name, first name or position |
| Enquiries | Support correspondence, claims, complaints, appeals, personal data requests, consideration materials |

4.2. The Operator does not seek to collect special-category data. If such information is contained in a document uploaded by a User, the User should remove excessive information before uploading where possible.

4.3. An image of the User's face, if uploaded as a profile image, is not used for biometric identification or converted into a biometric vector.

4.4. The password is stored in a protected transformed form. It is not transferred to the transactional email provider or other recipients.

## 5. Corporate data and personal data

5.1. A legal entity's name, registration number, general corporate telephone number, general email address, website, logo, address and other information about the legal entity do not constitute an individual's personal data merely because they are used on the Platform.

5.2. Information relating to an identified or identifiable individual constitutes personal data: an employee's name, personal or work email address and telephone number, signature, power of attorney information and identifiers of actions performed by that individual.

5.3. Exception for individual entrepreneurs and peasant (farm) enterprises. For business entities operating without forming a legal entity, registration, contact and other information is processed as the relevant individual's personal data, since their identification number and name relate directly to them.

## 5-1. Third-party personal data in Participants' documents

5-1.1. Participants post documents on the Platform necessary to document and perform the Parties' Contract: contracts, specifications, powers of attorney, documents accompanying the goods and shipping documents. Such documents may contain personal data of persons who are not Platform Users: signatories, representatives, drivers, freight forwarders and employees of warehouse and laboratory organisations.

5-1.2. The Participant posting a document confirms that it has a lawful basis for transferring third-party personal data contained in the document and is responsible for having that basis. This confirmation does not replace consents that those persons give to their employer or counterparty.

5-1.3. For third-party personal data contained in documents posted by a Participant, the Operator does not determine the contents of such data or request separate consent from those persons: the Participant prepares and posts the document and is responsible for having a basis for transfer. The Operator processes such data to ensure the Platform's operation — storing the document, displaying it to the parties to the relevant Transaction and granting access in the cases provided for in section 14 — and for its own lawful purposes: verifying Participant information, calculating the Fee, keeping records and reporting, considering enquiries and protecting its rights and legitimate interests. Such data are not used for other purposes.

5-1.4. A person discovering their personal data in a document posted on the Platform shall send an enquiry to privacy@dalaway.kz. The Operator considers the enquiry as regards processing it performs itself and takes measures prescribed by law within its responsibility, including blocking and ceasing unlawful processing. Within three business days, the Operator notifies the Participant that posted the document and, if necessary, requests information from it; this interaction does not extend mandatory consideration deadlines. The Participant that posted the document amends or deletes the contents of the document itself; the Operator implements the decision insofar as it relates to the Platform and provides assistance.

5-1.5. This section does not apply to personal data of Users and Participants' representatives: those data are processed on the bases specified in section 7.

## 6. Purposes of processing

6.1. Data are processed for the following purposes:

1. creating, authenticating and protecting a personal account;
2. creating the Participant's corporate profile and managing team membership;
3. verifying the Participant and its representative's authority;
4. ensuring the Platform's trading functionality, Transactions, Parties' Contracts, Appendices, Trading Operations and Services Centre;
5. providing the parties to a Transaction with necessary information and documents;
6. automated analysis of messages and published information for indications of sharing contact details before Agreement on Commercial Terms and other breaches of the Marketplace Rules;
7. access by the Operator's authorised employees to the content of Transaction correspondence and documents when considering enquiries, complaints, disputes and reviews in cases provided for in the Agreement and Marketplace Rules;
8. calculating the Fee, preparing Fee Calculations, Certificates of Work Performed (Services Rendered), invoices and closing documents;
9. compiling an export of Transaction materials in accordance with section 19 of the Agreement;
10. sending service and legally significant notices, technical support;
11. ensuring information security and preventing unauthorised access;
12. detecting and preventing circumvention of the Platform;
13. complying with the laws of the Republic of Kazakhstan and lawful requests of authorised bodies;
14. establishing, exercising and defending the Operator's claims;

15. creating De-identified Data and calculating Aggregated Indicators based on them, to develop the Platform, improve service quality, ensure security and for statistical, research and analytical purposes in accordance with section 20 of the Accession Agreement;
16. considering a request for a Platform demonstration, responding to the applicant, arranging and agreeing on the demonstration;
17. displaying a User's online presence and last login information to other Users interacting with them within a Transaction, correspondence or Services Centre order, to assess the other person's availability.;
18. traffic analytics for Dalaway website information pages, excluding registration, login and access recovery pages, to assess demand for sections, measure performance and identify display errors. This purpose applies where the visitor has given consent under the Cookie Policy. Third-party analytics tools are not used after login to an account;
19. collecting ratings given by parties to completed Transactions, calculating Participant performance indicators based on them and displaying such indicators in the Participant's card, to inform counterparties about prior performance on the Platform and detect bad-faith conduct.

6.2. Processing for purposes not specified in this section is not carried out.

6.3. De-identification. For the purpose in subclause 15 of clause 6.1, identifiers of the subject, Participant and its counterparties are removed from the data, after which restoring attribution of the information to a particular person by reasonable means becomes impossible. Publication and provision to third parties are permitted exclusively in the form of Aggregated Indicators and only if they cannot directly or indirectly identify a person or the terms of an individual Transaction. An indicator that in fact discloses the terms of an individual Transaction or information about an individual Participant is not published.

6.4. A demonstration request does not include consent to receive advertising messages. Separate consent is required to send advertising messages.

## 7. Bases for processing

7.1. Processing is carried out on the basis of the subject's consent, a contract to which the subject or the Participant they represent is a party, and other bases expressly provided for by the laws of the Republic of Kazakhstan.

7.2. Correspondence between purposes and bases:

| Purposes | Basis |
|---|---|
| 1–5, 8, 10 | Subject’s consent and performance of the Agreement |
| 6, 7 | Subject’s consent and Company Consent to the processing of business information and communications |
| 9 | Subject’s consent and Company Consent; when provided at the request of a court or authorised body, a legal requirement |
| 11, 12, 14 | Subject’s consent and legal security requirements |
| 13 | Requirement of the laws of the Republic of Kazakhstan |
| 15 | Subject’s consent and Company Consent; the processing result is de-identified and does not constitute personal data |
| 16 | Applicant’s consent when requesting a demonstration |
| 17 | Subject’s consent |
| 18 | Visitor’s consent provided under the Policy on the Use of Cookies and Similar Technologies |
| 19 | Subject’s consent and Company Consent to the processing of business information and communications |

7.3. Provision of data marked mandatory is necessary for the relevant feature. If they are not provided, the Operator may be unable to create an account, conduct verification or provide functionality.

7.4. Processing continuing after withdrawal of consent. Upon withdrawal of consent, the Operator ceases processing based exclusively on consent. Processing continues to the extent necessary to comply with mandatory legal requirements, including accounting and tax records; perform an outstanding obligation of the subject or the Participant they represent; establish, exercise and defend the Operator’s claims; complete consideration already commenced of an enquiry, complaint or dispute, or an investigation of a security incident. This list is exhaustive.

## 8. Automated processing

8.1. The Operator uses automated tools to analyse technical events, deadlines, calculations, messages and published information. Under this version, such processing aims to generate a notice, preliminary calculation or indication for subsequent review by an employee.

8.2. In particular, the following may be performed automatically:

1. detecting indications of sharing contact details before Agreement on Commercial Terms;
2. calculating deadlines and generating reminders;
3. calculating the Fee using a specified formula;
4. detecting overdue debt for referral to an employee of the Operator for review;
5. calculating the Participant's performance indicators on the Platform based on ratings of completed Transactions and performance information;
6. technical information security measures.

8.2-1. A Participant performance indicator is a calculated value and does not in itself entail legal consequences: it does not restrict trading functionality, change the Fee or constitute a breach decision. Restrictions are applied only in accordance with the Marketplace Rules.

8.3. An automatically detected indication is not a breach decision, does not establish the existence of a Related Transaction and does not in itself lead to a contractual restriction of trading functionality. Decisions capable of changing the rights or legitimate interests of a User or Participant are made by an authorised employee of the Operator, except for short-term technical measures directly necessary for account and Platform security.

8.4. The User may challenge the accuracy of input data and the decision of an employee of the Operator through the personal account or at the email address specified in this Policy. An objection to automated processing is considered within the time limit established by clause 17.4.

## 9. Public availability of data

9.1. The Operator does not publish individual Users' personal contact details and images as publicly available on the basis of their registration.

9.2. The Participant's card displays corporate information entered in fields marked as public in the interface, "Verified" status and the Participant's Platform performance indicators generated by the Operator: number of completed Transactions, information about the Service Provider's fulfilment of Services Centre orders and indicators calculated from ratings given by parties to completed Transactions. Public fields are intended for company information and corporate contacts; the Participant is responsible for information entered in them.

9.2-1. The indicators relate to the Participant as a business entity and describe its performance on the Platform. If the Participant is an individual entrepreneur or a peasant or farm enterprise, the indicators are displayed to the same extent and relate to its business activities; personal data unrelated to those activities are not included or published. An

individual User's last name, first name, position and other information are not published within indicators or when displaying ratings.

9.2-2. Disclosure occurs at two levels. Before Agreement on Commercial Terms, the Participant's card is de-identified: the business entity type, region, verification status, performance indicators and active cooperation formats are displayed. The name, identification number, contacts and description are disclosed to the other party after Agreement on Commercial Terms. The scope of displayed information and the persons to whom it is displayed are determined by the interface. Information entered in fields marked as public in the interface may also be displayed in an open Participant directory. Information in fields not marked as public is not displayed in that directory.

9.3. An individual User's data become available to a limited group of persons within a Transaction, correspondence, Trading Operation or Services Centre order, to the extent necessary for the relevant functionality.

9.3-1. A User's online presence and last login information may be displayed to other Users interacting with them within a Transaction, correspondence or Services Centre order. It is not publicly available.

9.4. Counterparty information is disclosed to the parties from Agreement on Commercial Terms and is confidential for them under clause 10.4 of the Agreement.

## 10. To whom data are transferred

10.1. Data may be transferred or access granted to:

1. other Users and Participants, to the extent necessary for a particular Transaction, Parties' Contract, Trading Operation or Services Centre order;
2. infrastructure and technical service providers engaged by the Operator to ensure Platform operation, under a data processing agreement specifying purposes, data categories, duration and protection requirements;
3. banks, payment and accounting organisations, to the extent necessary for settlements and accounting;
4. a court, arbitral tribunal, notary and authorised state bodies, in the cases and manner prescribed by law;
5. traffic analytics tool providers, to the extent of technical information collected by those tools, with the visitor's consent. The tools used are listed in the Cookie Policy.

10.2. Transfer to a third party and entrusting processing are distinct. When processing is entrusted, the processor acts on the Operator's instructions and for its specified purposes; the Operator is responsible to the subject. In a transfer to a third party, the recipient determines purposes independently.

10.3. The Operator maintains an up-to-date list of recipient and processor categories. Connecting a new service capable of accessing personal data undergoes legal and technical assessment; where necessary, the Policy and consent forms are updated and the subject's consent is requested anew.

10.4. Services of the National Certification Authority of the Republic of Kazakhstan may be used to verify electronic digital signatures. Access to personal data contained in state information systems is carried out in accordance with the procedure prescribed by law.

## 11. Cross-border transfer

11.1. The Platform is international. Cross-border data transfer may occur when a User or Participant from a foreign state obtains access through the Platform to information lawfully disclosed to them within a Transaction, Trading Operation or Services Centre order, and when the Operator engages foreign technical service providers.

11.2. Transfer to a Transaction counterparty. After Agreement on Commercial Terms, the parties are provided with information about the counterparty and its representative to the extent necessary to agree, document and perform the relevant Transaction: the representative's last name, first name and patronymic, position, work email address and work telephone number, and information contained in Transaction documents and correspondence posted by the parties to document and perform it. Copies of identity documents and Participant verification materials are not transferred to the counterparty. If the counterparty is located outside the Republic of Kazakhstan, such disclosure constitutes a cross-border transfer. The counterparty's country of location is displayed to the subject before disclosure. A User's personal data are transferred within the scope of their Consent to the Collection and Processing of Personal Data. Bases for transferring other persons' data contained in Transaction documents and correspondence are ensured in accordance with section 5-1 of this Policy.

11.2-1. Transfer of information beyond the scope specified in clause 11.2, or transfer for purposes unrelated to the relevant Transaction, requires a separate basis and is not carried out under this clause.

11.3. Transactional email provider. The Operator engages the Brevo service to deliver service messages and notices. The provider is Sendinblue, a simplified joint-stock company, French Republic. The provider acts as a processor on the Operator's instructions.

11.3-1. Information transferred. Recipient's email address; one-time verification code or link; name, if used in the message; message language; technical sending parameters. For a demonstration request, information included in the email text is additionally transferred. When inviting a Participant's employee, their work email address specified by the Owner and the invitation text are transferred on the instructions of the Participant that has

confirmed a lawful basis for such transfer under the Company Consent. The password is not transferred to the provider.

11.3-2. Purposes of transfer. Sending verification codes and other service messages. Advertising mailings are not covered and are sent only with separate consent.

11.3-3. Countries of processing. Processing takes place on the provider's infrastructure located in European Union member states: the French Republic, the Federal Republic of Germany and the Kingdom of Belgium. The Operator assesses these states as ensuring personal data protection.

11.3-3-1. Delivery logs. Information about messages and delivery events is retained in the provider's logs for twelve months and then deleted. The content of sent messages is not retained in the provider's logs.

11.3-4. Information on actual recipients and retention periods is provided to the subject on request to privacy@dalaway.kz.

11.3-5. Traffic analytics tools. Analytics tools listed in the Cookie Policy are used on Dalaway website information pages with the visitor's consent. The technical information they collect may be processed on the respective providers' servers located outside the Republic of Kazakhstan. The Operator does not control the location of these providers' infrastructure; processing terms are determined by the services' own policies, linked in the Cookie Policy. If collected information constitutes personal data, this Policy applies to it.

11.3-6. Third-party analytics tools are not used on registration, login and access recovery pages or within the Platform, and information is not transferred on the basis of clause 11.3-5.

11.4. The Operator does not engage other foreign recipients with access to personal data. Initial collection and primary storage of personal data take place in the Republic of Kazakhstan.

11.5. The Operator assesses the lawfulness of each cross-border transfer before it begins. Expanding the range of recipients beyond those specified in this Policy requires updating the Policy and obtaining the subject's consent to the necessary extent.

11.6. Programmatic data access is granted within the relevant Participant's authority and does not expand it beyond access available in the user interface.

## 12. Data storage in the Republic of Kazakhstan

12.1. The database containing personal data and primary permanent personal data storage are located in the Republic of Kazakhstan.

12.2. Backups containing personal data are also located in the Republic of Kazakhstan.

12.3. Granting access to a foreign counterparty or separate processing by a foreign provider is permitted only under the cross-border transfer procedure in section 11 and does not replace mandatory storage of the database in the Republic of Kazakhstan.

## 13. Retention periods

13.1. A single retention period does not apply to all data. The period is determined by the purpose of processing, legal requirements and the need to protect rights.

13.2. Periods by category:

| Category | Period | Starting point |
|---|---|---|
| Personal account and corporate profile data | Duration of the relationship and then up to 3 years while a lawful retention purpose remains | Date of termination of the relationship |
| Verification documents | Up to 3 years while a lawful retention purpose remains | Date of termination of the relationship |
| Transaction data: terms, details of Parties' Contracts, Appendices, Trading Operations, documents | Up to 3 years | Date of last performance under the Transaction |
| Correspondence between Transaction parties: message text | Up to 3 years | Date of Completion or cancellation of the Transaction |
| Files attached to Transaction correspondence messages | 12 months, then destroyed | Date of Completion or cancellation of the Transaction |
| Settlement documents: Fee Calculations, Certificates of Work Performed (Services Rendered), invoices, payment information | 5 years: the period prescribed by the tax and accounting laws of the Republic of Kazakhstan | End of the year in which they were issued |
| Acceptance log: document versions and checksums, device network address, date and time | Term of the Agreement and then 3 years | Date of termination of the Agreement |
| Technical security logs | 3 years | Date of the event |

| Category | Period | Starting point |
|---|---|---|
| Ratings of completed Transactions and responses thereto | Duration of the relationship with the Participant and then 3 years | Date of termination of the relationship |
| Materials concerning consideration of enquiries, complaints and appeals | 3 years | Date of completion of consideration |
| Demonstration request | Until consideration and the demonstration are completed; information confirming handling of the enquiry and consent obtained, under the rule for enquiries | Date of receipt of the request |
| Incomplete registration data | Until the purpose of address verification and protection against abuse ceases | Date of last action |
| Backups | Daily: 7 days; weekly: 1 month; monthly: 12 months; access only for recovery | Date the backup was created |
| Data processed exclusively on the basis of consent for a separate optional purpose | Until withdrawal of consent or achievement of the purpose | — |

13.3. If a dispute, claim, complaint consideration, security incident investigation or outstanding obligation remains unresolved, destruction of related data is postponed until completion of the relevant process and expiry of the subsequent mandatory period.

13.4. At the end of the period, data are destroyed or anonymised. Anonymisation means irreversible transformation that excludes the possibility of linking the data to the subject.

## 14. Correspondence, documents and event logs

14.1. Correspondence between the parties and Transaction events are retained and used to support the Transaction, consider enquiries, complaints and disputes, detect circumvention of the Platform and protect participants' rights.

14.1-1. Correspondence files and Transaction documents are distinct. A document attached to a Transaction, Appendix or Trading Operation forms part of Transaction materials and is retained for the period established for Transaction data. A file attached to a correspondence message serves operational exchange and is destroyed twelve months after Completion or cancellation of the Transaction; the message text is retained. Until the Transaction is

completed or cancelled, correspondence attachments are retained regardless of how much time has passed since the message was sent. A document with evidentiary value is posted in the documents section of the relevant Transaction.

14.2. The legal basis for processing correspondence content is the Company Consent to the processing of business information and communications and, as regards a User's personal data, their consent.

14.3. The Operator's authorised employees are granted access to correspondence content only to the extent necessary to consider enquiries, complaints, disputes and reviews provided for in the Agreement and the Marketplace Rules.

14.4. Deleting a message or object in the user interface does not mean immediate destruction of related log entries, backups and evidentiary records where there is a lawful basis to retain them. Deleted data remain in previously created backups until the retention period of the relevant backup expires (clause 13.2) and are not selectively removed from backups; after expiry, the backup is destroyed together with the data it contains.

14.5. When data are restored from a backup to the live system, previously fulfilled requirements to destroy, block and restrict processing are applied again.

## 15. Protection measures

15.1. The Operator applies legal, organisational and technical personal data protection measures prescribed by the laws of the Republic of Kazakhstan, including access controls, authentication, secure data transfer, logging of significant actions, backups and incident response measures.

## 16. Personal data security breach

16.1. Upon discovering a personal data security breach, the Operator notifies the authorised body within one business day of discovery, providing contact details of the person responsible for organising personal data processing.

16.2. Personal data subjects are notified of a personal data security breach in accordance with the procedure prescribed by the laws of the Republic of Kazakhstan. The Operator may additionally inform affected Users of the nature of the breach and measures they can take to limit its consequences.

16.3. The Operator conducts an internal investigation, takes measures to remedy consequences and prevent recurrence, and records the results.

## 17. Subject’s rights and enquiry procedure

17.1. The subject has the right to:

1. know whether the Operator holds their personal data and obtain information about the fact, purposes, sources and methods of processing, the list of data and retention periods;
2. request amendment and supplementation of their data where supporting documents exist;
3. request blocking of data where there is information indicating a breach of collection and processing conditions;
4. request destruction of data collected or processed in breach of the law;
5. withdraw previously given consent;
6. consent to or refuse dissemination of data in publicly available sources;
7. protect their rights and legitimate interests, including claiming compensation for harm.

17.2. Enquiries are sent to the email address specified in clause 1.2 or through the personal account. An enquiry sent from the verified email address specified in the account is deemed to have been submitted by the subject.

17.3. The Operator may request reasonable confirmation of identity or control of the account before fulfilling an enquiry. The scope of requested confirmation is proportionate to the enquiry’s subject matter.

17.4. The consideration period depends on the enquiry’s subject matter:

1. information about the existence of personal data, purposes, sources and methods of processing, the list of data and processing and retention periods is provided, or a reasoned refusal sent, within three business days of receipt of the enquiry;
2. an objection to automated personal data processing is considered within three business days of receipt, with the subject notified of the outcome;
3. other enquiries are considered within ten business days unless the laws of the Republic of Kazakhstan prescribe a shorter period.

17.5. Within one business day of receiving the relevant basis, the Operator amends or supplements data, blocks them where there is information indicating a breach of processing conditions, destroys data where unlawful processing is confirmed, and lifts blocking if the breach is not confirmed.

17.6. If the request cannot be fulfilled, a reasoned response is sent to the subject.

17.7. Withdrawal of consent entails the consequences specified in clause 7.4. Withdrawal of data necessary for communication may make a dependent feature unavailable.

## 18. Changes to the Policy

18.1. The Policy is updated when legislation, Platform functionality, the scope of processed data, processing purposes or the range of recipients changes.

18.2. Changes to processing purposes, the scope of processed data or the range of recipients require new consent from the subject. Processing in the changed scope is not continued on the basis of previously given consent.

18.3. Subjects are notified of changes that do not require new consent through the Platform and by email no later than the effective date of the relevant version.

18.4. Each version is retained in the archive at a permanent address, specifying its publication and effective dates.

---

**Version history.** Current version — 1.0 of 01.10.2026, effective from 01.10.2026. No previous versions.