

Privacy Policy

Processing of Personal Data of Users of the Birge+ Mobile Application

1 Purpose and Owner of Records

1.1. This Policy explains how personal data is processed in the Birge+ application, including the account, the loyalty program, online orders, and additional features. The owner of the records is Umai Group LLC, TIN 01007200310037, registration number 20454-3300-OOO, OKPO 23320546; address: 16 Chokan Valikhanov St., Bishkek, Kyrgyz Republic.

1.2. This Policy is an informational document, not a request for consent. Reading it and continuing to use the application do not constitute a general authorization for processing. Necessary contractual operations are performed on their own legal basis; separate consents are used for specific voluntary purposes.

1.3. The legal framework is the Digital Code of the Kyrgyz Republic, in particular Articles 71, 73–79, 81–89, 114, and 118, as well as applicable requirements of legislation on trade, tax, and accounting. Mandatory provisions take precedence.

1.4. Requests are accepted via the “Support” section of the Birge+ application, by email at office@umai-retail.kg, by phone at 900-230, and at the Company’s address. The email address of the person responsible for processing and information on places of processing, retention periods, and contractors are disclosed in the Annex to this Policy. This information is provided before processing begins.

2 Principles and Scope

2.1. The Company processes data lawfully, fairly, and transparently, only for purposes defined in advance; it uses the necessary and sufficient amount of data, maintains its accuracy, limits the retention period, and ensures confidentiality and security. Compliance must be evidenced by records of operations and decisions taken.

2.2. Declining to provide optional data or voluntary consents does not prevent the use of core features. Without the data required for a specific service, only that particular service may be unavailable: for example, delivery without an address. Where an alternative exists, manual address entry or self-pickup is offered.

2.3. Sources include the user themselves, events of necessary operations in the application, checkout transactions with the presented card, and information on order, payment, and delivery status from the relevant participants. If information is not obtained from the data subject, the Company ensures that the subject is informed in the manner and within the time limits set by Article 73 of the Code.

3 Purposes, Data, and Legal Bases

3.1. Account: phone number, user identifier, confirmation of access, and sign-in settings. Purpose: registration, authentication, and account management. Legal basis: clause 1, part 1, Article 79. Name and email address are requested to the extent required by the selected features; a delivery address is not required at registration by default.

3.2. Loyalty program: card identifier, associated purchases, amounts, bonus accrual and redemption, coupons, and selected privileges. Purpose: performance of the participation agreement and verification of calculations; legal basis: clause 1, part 1, Article 79. If a tier mechanism is introduced, the approved calculation rules are disclosed before it is applied; this Policy does not set commercial thresholds or rates.

3.3. Online purchase: recipient’s name and phone number, order contents and value, delivery address and instructions or pickup point, payment identifier and status, requests, and returns. Legal basis: clause 1, part 1, Article 79; for mandatory accounting documents, clause 2. The user may provide another recipient’s address and name only lawfully, and the Company fulfills its own obligation to inform that person.

3.4. Payments: full card details are entered in the secure form of the payment service; to record a purchase, the application uses payment information to the extent of data actually available to the Company. The specific scheme, the recipient of card details, and any tokens or masked data available to the Company are disclosed in the Annex to this Policy. Full card details are never requested in comments or via support.

3.5. Operation and security: IP address, session and app instance identifiers, OS and app version, authorization events, errors, and necessary operation events. The contractual basis applies to data objectively necessary for the requested service. For standalone anti-fraud measures, clause 5, part 1, Article 79 is applied after a documented assessment of the balance of rights, necessity, and proportionality; a legitimate interest is not presumed automatically.

3.6. Support: the requester's contact details, the text of the request, and records relevant to the dispute; voluntarily attached documents only to the extent necessary. Legal basis: performance of the relevant contract and mandatory obligations regarding requests. Information unrelated to the issue and special categories of data should not be sent to support.

3.7. Advertising: phone number, e-mail, push token, and delivery statuses are used only for separately selected advertising channels on the basis of consent under parts 2 and 4 of Article 79. Purchase analysis and personalized offers require a separate choice; purchase history of no more than the last 12 months is used. Service messages about order fulfillment and security contain no advertising and do not depend on advertising consent.

3.8. Voluntary analytics: identifiers, device information, session data, and feature usage data listed in the relevant consent and in the Annex to this Policy. Optional SDK and cookies are not activated until consent is given. Identifiers and the IP address may constitute personal data even if the provider does not know the person's name. Cross-service advertising tracking is not authorized by this consent.

3.9. Geolocation: approximate coordinates, accuracy, and request time are processed only when the user separately chooses store search and/or address assistance and grants OS permission. No background collection or location history is maintained as part of this feature; coordinates are deleted after the request, and a confirmed address is used for delivery on a contractual basis. Marketing and precise tracking are not authorized by this consent.

4 Consents and Change of Purpose

4.1. Consent must be voluntary, specific, informed, and conscious. A separate request is distinct from contractual acceptance. Where a basis under part 1 of Article 79 exists, consent is not requested in its place: clause 3, part 3, Article 79 provides that such consent is void.

4.2. Choices are recorded by type and version of the text, purposes, channels, user identifier, and the date and time of giving, changing, and withdrawing consent. Pre-ticked boxes, silence, and continued use do not constitute consent. Giving one consent does not mean giving the others.

4.3. Withdrawal is available in the settings for the relevant choice and via support, and is no more burdensome than giving consent. After withdrawal, the relevant processing stops and, in the absence of another basis, the data is deleted immediately. Processing that was lawful before withdrawal does not become unlawful as a result of it. Independent mandatory retention and performance of an already concluded contract are disclosed separately.

4.4. New purposes, recipients for their own purposes, or a different scope of data are not automatically added to an existing consent. If new consent is required, processing does not begin until it is obtained. Amending this Policy does not replace such a choice.

5 Contractors and Other Recipients

5.1. Employee access is limited according to job duties. External IT, hosting, communications, analytics, courier, and payment organizations receive only the data necessary for a specific function and only where there is a legal basis. Illustrative service names do not replace the list of recipients actually used; information about them is disclosed in the Annex to this Policy.

5.2. A processor acts under a contract compliant with Article 86 of the Code and only on the owner's written instructions; the contract sets out the duration, purpose, categories of data and data subjects, confidentiality,

procedures for correction, deletion, and restriction, and the recording of operations. Another processor may be engaged only with the owner's prior written authorization.

5.3. A bank, seller, or other independent owner may have its own legal obligations; the Company discloses its role and the basis for the transfer. The statement "third parties have no purposes of their own" is not applied to independent owners without regard to their status.

5.4. If several legal entities jointly determine the purposes and means of processing, the Company discloses the joint owners and the published arrangement for their interaction under Article 87. The user may exercise their rights against any of the joint owners regardless of their internal arrangements.

5.5. Data is provided to government bodies only in the cases and to the extent established by law. This Policy does not permit the sale of contact databases or transfers for third parties' own advertising.

6 Cross-Border Transfer

6.1. Before any transfer abroad, including foreign hosting, backups, and remote access, the recipient, the countries, and the basis under Article 89 are determined. A provider's well-known brand or security statements do not in themselves constitute a legal basis.

6.2. For countries on the regulator's published list of countries providing adequate protection, the Company verifies their inclusion in the list in advance. The transfer is carried out under parts 2 and 3 of Article 89 in compliance with the other requirements of the Code.

6.3. For countries that do not provide adequate protection, one of the bases under part 4 of Article 89 is used: specific consent, an applicable international treaty, a case provided for by law, necessity for concluding or performing a contract with the data subject, protection of vital interests where consent cannot be obtained, or contractual safeguards in the manner provided for by the Code. The general convenience of foreign hosting does not prove that the transfer is necessary for the contract.

6.4. If the basis is consent, the specific countries, recipients, data, operations, periods, and material risks are disclosed before the choice is made; refusal and withdrawal are exercised via a separate form. Transfers on other bases are not presented as dependent on the withdrawal of this consent. The applicability of the bases and the details of each transfer are set out in the Annex to this Policy.

6.5. In the destination country, processing is governed by that country's legislation; the Company retains its own obligations under the Code. A new country or recipient is not tacitly included in a previously given consent.

7 Retention, Deletion, and Withdrawal from the Service

7.1. The retention period is determined separately for each category, based on necessity for the purpose and on mandatory provisions. The profile is used for as long as the account exists; security logs, analytics, requests, and documents have their own retention periods as specified in the Annex. A general rule of "all data plus three years" does not apply.

7.2. Records evidencing the terms of the user agreement with respect to a specific user and the performance of the agreement are retained for its entire term and for three years after its termination in accordance with part 4 of Article 114 of the Digital Code of the Kyrgyz Republic. This period does not automatically extend to all analytics events, coordinates, and other data. Data required for mandatory tax, accounting, and other records is retained for the periods prescribed by law.

7.3. When a user withdraws from the digital service, the Company provides information on the user's existing digital records, explains how to obtain a copy and transfer them to other services, and provides the option to request their deletion. Until a decision on the records is received, they are kept unchanged. If no decision is received, the records are deleted upon expiry of one calendar year following the year in which the withdrawal was received, in accordance with Article 118 of the Code. For example, if a user withdraws in 2026 without giving instructions on the records, this period expires on December 31, 2027. This does not postpone the fulfillment of a lawful deletion request already received. Records that must be retained by law are not deleted; the user is notified of their composition and the basis for their retention.

7.4. Once the purpose is achieved or the basis ceases to exist, personal records are deleted immediately under Article 83, unless a legal exception applies. Information kept for the establishment, exercise, or defense of legal claims is retained to the minimum extent, for the necessary period, and with restricted access. Withdrawal of advertising consent does not require deletion of the opt-out record needed to prevent repeat mailings and to demonstrate respect for the user's rights.

7.5. Deletion takes backups into account: data is removed from ordinary use and deleted in accordance with the disclosed backup cycle; upon restoration, previously recorded deletions are applied. The technical arrangement of backups does not cancel the obligation to delete data in a timely manner and does not grant the right to use it for new purposes.

8 Rights and Request Procedure

8.1. The user has the right to obtain confirmation of processing and information on its bases, purposes, the data involved, places of processing, recipients, and retention periods; to access and obtain copies; to correction, completion, deletion, restriction, and objection; to the transfer of records in the cases set out in Article 76; and to withdraw consents.

8.2. A request may be submitted via support, by email at office@umai-retail.kg, or to the Company's address. The Company verifies the right of access by proportionate means; excessive documents are not required. Data is provided in an accessible machine-readable format, with due regard for the rights of others. The absence of a pre-built export button does not exempt the Company from complying with the law.

8.3. Response periods and scope are determined by the relevant provision of the Code. For objections, a reasoned response is provided within 7 business days. When processing is restricted, the user is informed no later than the next business day after the restriction is imposed or lifted, under Article 85. If a request is refused, the legal basis and the appeal procedure are communicated.

8.4. Upon a complaint about the digital service, the Company takes the necessary measures to remedy violations within five business days. If more time is required, within those five business days it notifies the complainant of this, with justification of the time needed. The complainant is informed of the measures taken by the same means through which the complaint was submitted, unless another means has been chosen. An objection to the processing of personal data is reviewed with a reasoned response within seven business days; special time limits established by law take precedence.

8.5. A decision on a complaint about the digital service may be appealed through the mandatory pre-trial procedure before the sectoral regulator provided for by part 5 of Article 119 of the Digital Code of the Kyrgyz Republic, and then in court. Claims relating to personal data are governed by the special rules of Chapter 11 of the Code, and claims relating to the sale of goods by consumer protection legislation. This document does not introduce any additional mandatory pre-trial claim procedure and does not limit the consumer's choice of court as provided by law.

9 Children, Special Categories, and Automated Calculations

9.1. The Birge+ application is intended solely for persons aged 18 and over; registration terms are set out in the User Agreement, and terms of program participation in the Rules. The Company does not knowingly process personal data of persons under 18. If the Company becomes aware that an account was created by such a person, the account is blocked and the personal records are deleted, taking into account Articles 81 and 83 of the Code, unless there is a legal basis for their retention.

9.2. For ordinary use, the Company does not request genetic data, data concerning health, beliefs, or sex life, or biometric data for identification. Their processing is permitted only where an applicable exception and the safeguards of Article 80 are in place. A single separate expression of the user's will is not sufficient to circumvent the prohibition under Article 80.

9.3. Bonus accrual, coupon application, and other calculations may be performed automatically under published terms. The user is informed of the input parameters, the calculation principle, and the consequences; an error may be challenged and reviewed by an employee. This Policy does not introduce any other automated

decision-making with legal or similarly significant effects. Where the conditions of Article 82 are met, an impact assessment is carried out before processing.

10 Protection and Amendments

10.1. The Company appoints a person responsible for processing, restricts access, protects transmission channels and systems, records operations, trains employees, and monitors contractors in accordance with Article 88. Measures are selected based on risks and mandatory requirements; this Policy does not guarantee the absence of any incidents.

10.2. In the event of an incident, the Company limits its consequences, restores security, records the circumstances, and fulfills its obligations to notify and cooperate with the competent authorities and affected persons in the applicable cases and within the applicable time limits. Data about unrelated persons is not disclosed in notifications without a legal basis.

10.3. The Company gives notice of amendments at least one month before their effective date through the application and another available channel. The notice contains the new version, the effective date, and the procedure for rejecting the amendments. The user can save and reproduce the text. If the user rejects an amendment in a timely manner, the user agreement terminates with the consequences set out in Article 118 of the Digital Code of the Kyrgyz Republic; obligations already arising from purchases are fulfilled on the agreed terms. Amendments do not apply retroactively. Where consent is required for new processing, the notice and continued use of the application do not replace it.

10.4. The current version and the archive are available in the application. Records of the terms and performance of the agreement are retained under Article 114; the archive of the Policy and consents is maintained so as to make it possible to demonstrate the terms that applied and the user's choices. Mandatory language requirements are fulfilled by the Company prior to publication.

Annex Information on Data Processing

To be completed by the Company with actual data before the Policy is published and the relevant processing begins. Services and data not in use are excluded. The information is reconciled with the notices and separate consents.

1. Person responsible for processing: full name / position _____. Electronic contact office@umai-retail.kg.
2. Register of external recipients: for each, full name and address, role as processor / independent owner / joint owner, purpose, data, place of processing, and legal basis _____.
3. Countries and locations of primary storage, backup, and remote access, including subcontractors _____. Basis for each transfer under Article 89 and confirmation of the list check or safeguards _____.
4. For each SDK / cookie / identifier: name, provider, mandatory or voluntary nature, events and data, purpose, identifier lifetime, and event retention period _____.
5. Retention periods by category: security logs ____; analytics ____; requests ____; mandatory accounting documents ____ (legal provision ____); backups and deletion cycle _____. Basis for the periods and procedure for terminating processing _____.
6. Payment operator and country, composition of payment data and tokens available to the Company, technical scheme for accepting card details _____.
7. Program participants and joint owners, if any: full details, allocation of roles, published arrangement, and contact _____.
8. Automated calculations: published terms, input data, calculation principle, consequences, and challenge procedure _____.
9. Policy version and effective date _____. Paths to notices, separate consents, withdrawal settings, and data export _____.