PRIVACY NOTICE

for the use of registered office services, service of process agent services and office use

This is an English translation of the Hungarian privacy notice. In the event of any discrepancy between the Hungarian and the English text, the Hungarian text shall prevail.

Controller: E-Marketplace Szolgáltató Kft. **Effective from:** 1 January 2026 | **Version:** 2.0

---

1. DETAILS OF THE CONTROLLER

Name	E-Marketplace Szolgáltató Korlátolt Felelősségű Társaság
Registered office	1064 Budapest, Izabella utca 68/B.
Company registration number	01-09-296567
Tax number	25924916-2-42
Representative	Zoltán Kádár, managing director
E-mail	emarketplacekft@gmail.com
Telephone	06 50 104 61 16
Website	https://e-marketplace.hu

Data protection officer: under Article 37 GDPR the Controller is not required to designate a data protection officer, and has therefore not designated one. On data protection matters the Controller can be contacted at the e-mail address given above.

This notice constitutes the information to be provided under Articles 13 and 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council (**GDPR**). Act CXII of 2011 on Informational Self-Determination and Freedom of Information (**Info Act**) also applies.

2. WHO THIS NOTICE COVERS (DATA SUBJECTS)

- the executive officers, members, beneficial owners, representatives and contact persons of the Controller's client (principal);
- foreign persons concerned by the delivery agent service;
- persons requesting a quotation or initiating contact;
- persons taking receipt of documents and authorised representatives;
- persons using the office or the meeting room;
- third parties appearing in the mail items received by the Controller (see section 6).

3. PURPOSES, LEGAL BASES AND RETENTION PERIODS OF THE PROCESSING

In accordance with Article 13(1)(c) GDPR, the Controller specifies the legal basis **separately for each purpose**.

3.1. Quotations and contact

- **Data processed:** name, company name, e-mail address, telephone number, the content of the enquiry.
- **Purpose:** answering the enquiry, providing a quotation.
- **Legal basis:** Article 6(1)(b) GDPR – steps preceding the conclusion of a contract at the data subject's request; where the enquiry is made by a representative of the prospective client, the legal basis is legitimate interest under Article 6(1)(f) GDPR (responding to the request for a quotation).
- **Retention:** 1 (one) year following the expiry of the validity of the quotation; where a contract is concluded, as set out in section 3.2.

3.2. Conclusion and performance of the contract (registered office, delivery agent, office use)

- **Data processed:** the principal's company data; the representative's name, position, personal identification data and signature; the contact person's name, e-mail address and telephone number; the notification data relating to mail items; in the case of the delivery agent service, the foreign person's name, place and date of birth, mother's name, residential address, identity document number and tax identification number.
- **Purpose:** the conclusion and performance of the contract, issuing the declaration of consent to the use of the registered office, receiving, registering as incoming, scanning and forwarding mail items, keeping documents and maintaining the register of documents, performing the delivery agent tasks, and keeping in contact.
- **Legal basis:** Article 6(1)(b) GDPR (performance of the contract); for the data of representatives and contact persons, Article 6(1)(f) GDPR (the Controller's legitimate interest in being able to perform the contract and in keeping in contact). For the obligations prescribed by law – document handling, the register of documents and notification under Sections 2 and 3 of Decree 7/2017 (VI. 1.) IM on registered office services – the legal basis is Article 6(1)(c) GDPR.
- **Retention:** 5 (five) years from the termination of the contract (the general limitation period under the Civil Code (Ptk.)), for accounting documents the period set out in section 3.4, and for customer due diligence documents the period set out in section 3.3. The retention period for scanned mail items and the incoming mail register is 5 (five) years from the termination of the contract; the Controller keeps the original mail items for 30 (thirty) days following the termination of the contract and then hands them over or – if they are not collected – destroys them.

3.3. Customer due diligence, prevention of money laundering

- **Data processed:** the data prescribed by the AML Act: the natural person's name, name at birth, nationality, place and date of birth, mother's name, residential address, the type and number of the identity document and a copy of the document; the data of the beneficial ownership declaration; the politically exposed person (PEP) declaration; data on the source of funds, where it is necessary to request them.
- **Purpose:** customer due diligence under Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (**AML Act / Pmt.**), ongoing monitoring of the business relationship, compliance with reporting obligations and maintaining internal records.

- **Legal basis:** Article 6(1)(c) GDPR – compliance with a legal obligation to which the Controller is subject. Under Section 1(1) of the AML Act the Controller, as a registered office service provider, qualifies as a service provider.
- **Retention:** 8 (eight) years from the termination of the business relationship; in the event of a request from an authority, a longer period under the AML Act, up to a maximum of 10 (ten) years.
- **Note:** the provision of these data is an obligation based on law. If the data subject does not provide the data, the Controller is required under the AML Act to refuse to establish the business relationship or to carry out the instruction, or to terminate the existing business relationship.

3.4. Invoicing, retention of accounting documents

- **Data processed:** the invoicing name, address and tax number, the invoice data, and the data on performance and payment.
- **Purpose:** compliance with the statutory obligations on invoicing and the retention of accounting documents.
- **Legal basis:** Article 6(1)(c) GDPR – the obligations under Act CXXVII of 2007 on Value Added Tax and Act C of 2000 on Accounting.
- **Retention:** under the Accounting Act, 8 (eight) years from the creation of the document.

3.5. Enforcement of legal claims, debt management

- **Data processed:** the data of the contract and its performance, the payment history, the correspondence and the payment notices.
- **Purpose:** enforcing the Controller's overdue claims, bringing and defending legal claims, handling complaints and preventing abuse.
- **Legal basis:** Article 6(1)(f) GDPR – the Controller's legitimate interest in enforcing its claims and defending its rights. The legitimate interest assessment (balancing test) is available for inspection at the Controller.
- **Retention:** until the claim becomes time-barred, or, in the case of pending proceedings, until 1 (one) year after the final conclusion of the proceedings.

3.6. Compliance with requests from authorities

- **Legal basis:** Article 6(1)(c) GDPR – legal obligation (request from a court, public prosecutor's office, investigating authority, tax authority, court of registration or enforcement officer).
- **Retention:** 5 (five) years from compliance with the request.

3.7. Operation of the website, logging, cookies

- **Data processed:** IP address, the time of the request, the page viewed, browser and device data; where a form is completed, the data set out in section 3.1.
- **Purpose:** operating the website, security, preventing abuse, statistics.

- **Legal basis:** for the processing necessary for operation and for security logging, Article 6(1)(f) GDPR (legitimate interest); for cookies that are not strictly necessary (statistical and marketing cookies), Article 6(1)(a) GDPR – the data subject's **consent**, which may be withdrawn at any time via the cookie management interface.
- **Retention:** for log files, a maximum of 12 (twelve) months; for cookies, the period specified in the cookie notice.

3.8. Newsletter, marketing contact (if any)

- **Legal basis:** Article 6(1)(a) GDPR – **consent**, in line with Section 6 of Act XLVIII of 2008 on Business Advertising. Consent may be withdrawn at any time free of charge; the withdrawal does not affect the lawfulness of the processing carried out until the withdrawal.
- **Retention:** until the withdrawal of consent.

3.9. Office use, entry to the property

- **Data processed:** the name of the person entering, the time of entry and the room used by them.
- **Purpose:** the security of the property and of the documents kept there, and monitoring the use.
- **Legal basis:** Article 6(1)(f) GDPR – legitimate interest (protection of property, security of the documents).
- **Retention:** 6 (six) months from the recording of the data.

3.10. CCTV surveillance

- **Data processed:** the image of persons entering the monitored area and the time of entry.
- **Monitored areas:** the common areas of the property (entrance, corridor) and the room used for storing documents (document store).
- **Purpose:** protecting the property, the equipment and in particular the principals' documents kept here, and preventing and detecting unauthorised access.
- **Legal basis:** Article 6(1)(f) GDPR – the legitimate interest of the Controller and of its principals (protection of property, document security). The legitimate interest assessment (balancing test) is available for inspection at the Controller.
- **Retention: 7 (seven) days** from the making of the recording, after which the recording is deleted automatically. Where the recording serves to prove an infringement or a security incident, the Controller retains the recording until the matter is closed or until the final conclusion of the administrative or court proceedings.
- **Access:** only the managing director and the staff member authorised by them in writing and bound by confidentiality have access to the recordings. A copy of a recording may be released only at the request of an authority, or at the request of the data subject in respect of the part containing their own image.
- **Information on site:** a clearly visible warning sign and a short information board are displayed at the entrances to the monitored areas.

- **Rights of the data subject:** the data subject may request access to the recording made of them and its blocking within the retention period, and may object to the surveillance in accordance with section 9.

4. WHETHER THE PROVISION OF PERSONAL DATA IS MANDATORY

The provision of the data set out in section 3.2 is a precondition for concluding the contract; the provision of the data set out in sections 3.3 and 3.4 is an obligation based on law. In the absence of these data the Controller will not conclude or will not perform the contract. The processing based on consent set out in sections 3.7 and 3.8 is voluntary; refusing it does not affect the use of the service.

5. RECEIPT, OPENING AND SCANNING OF MAIL ITEMS – CONFIDENTIALITY OF CORRESPONDENCE

5.1. The Controller takes receipt of postal items addressed to the principal's company name as the principal's authorised agent, on the basis of the **postal power of attorney** given by the principal. Under Section 3 of Decree 7/2017 (VI. 1.) IM, the Controller ensures that mail items are received at the registered office and notifies the company of the receipt within one working day.

5.2. The Controller is entitled to open a sealed mail item, to acquaint itself with its contents and to scan it **solely on the basis of the principal's express written authorisation**, for the purpose of performing the contract (scanning, forwarding, registering as incoming, keeping documents). In the absence of such authorisation the Controller does not open the mail item but gives notice of its arrival.

5.3. The Controller and the persons acting on its behalf preserve the contents of the mail item and the confidentiality of correspondence, private secrets and business secrets contained in it; this obligation of confidentiality applies without any time limit and continues after the termination of the legal relationship. Its employees and contributors make written confidentiality declarations.

5.4. The Controller stores the scanned files in a password-protected business account with two-factor authentication and in its own closed administrative system (app.smartszekhely.hu); only the staff members involved in the performance of the service and bound by confidentiality have access to them.

5.5. The registration as incoming and the recording of mail items take place in the app.smartszekhely.hu system, and documents are sent electronically via the Brevo mailing system. These systems log the time of receipt, processing, dispatch and delivery of the mail item; the purpose of the log data is to evidence performance and to provide proof in the event of any legal dispute. The legal basis for processing the log data is Article 6(1)(b) GDPR (performance of the contract) and Article 6(1)(f) GDPR (the Controller's legitimate interest in evidencing performance). The retention period for the log data is 5 (five) years from the termination of the contract.

6. THIRD PARTIES' DATA IN MAIL ITEMS – ROLE AS PROCESSOR

Mail items received for the principal may also contain the personal data of third parties (the principal's clients, employees and partners). In respect of these data **the controller is the principal**, and the Controller acts – in the context of receiving, opening, scanning, forwarding and keeping the mail items – as a **processor under Article 28 GDPR**. The Controller processes these data solely in accordance with the principal's instructions, for the purpose of performing the contract, does not use them for any further purpose, and releases or erases them in accordance with the principal's instructions. Informing the data subjects is the obligation of the principal as controller. The parties conclude – where necessary – a separate processor agreement in this respect.

7. PROCESSORS AND TRANSFERS

The Controller uses the following processors. The processors process the data solely in accordance with the Controller's instructions.

Processor	Activity	Scope of data processed
Google Cloud EMEA Limited, Velasco, Clanwilliam Place, Dublin 2, Ireland	hosting for the website and the app.smartszekhely.hu system, server services	data provided on the website, data processed in the system, scanned mail items, log data
Google Ireland Limited (Google Workspace), Gordon House, Barrow Street, Dublin 4, Ireland	e-mail service and document storage	correspondence, scanned mail items
KBOSS.hu Kft. (Számlázz.hu invoicing system)	invoicing	invoicing and invoice data
Brandstädter Ügyvédi Iroda, 1149 Budapest, Nagy Lajos király útja 158. II/4.	legal representation, enforcement of claims, contractual matters	the contractual and contact data necessary for the legal matter
Brevo (Sendinblue SAS, France)	sending electronic mail, delivery logging	name, e-mail address, log data on dispatch, delivery and opening

The Controller develops and operates the app.smartszekhely.hu administrative system itself, and therefore does not use an external operator in respect of the data processed in it; the system runs on Google Cloud servers, which acts as a processor in this respect.

The bodies acting on the basis of law may access the data **as independent controllers**: the court of registration, the state tax and customs authority (including the authority acting as the financial intelligence unit), the courts, the public prosecutor's office, the investigating authority, the enforcement officer, and the postal service provider in the context of delivering mail items.

At the principal's express request or instruction, the Controller transfers the data to the partner designated by the principal (for example to the lawyer or accountant handling the company procedure).

Transfers to a third country: where Google Workspace and Google Cloud are used, the data may also be transferred to the United States of America. This transfer takes place on the basis of an adequacy decision under Article 45 GDPR (EU–US Data Privacy Framework) or standard contractual clauses under Article 46 GDPR. The Controller provides information on the current status of the adequacy decision and the safeguards at the e-mail address given above.

8. DATA SECURITY MEASURES

In accordance with Article 32 GDPR, the Controller applies the following measures to ensure the security of the data:

- paper documents are stored in a locked room that is not accessible to unauthorised persons, kept separately for each principal;
- electronic data are accessible in password-protected accounts with two-factor authentication (2FA), over an encrypted connection (HTTPS);
- access is restricted to the staff members needed to perform the task (need-to-know principle), with regular reviews of access rights;
- regular backups, virus protection and logging;
- written confidentiality declarations and data protection training for employees and contributors;
- in the event of a personal data breach the Controller records the breach, notifies it within 72 hours to the Hungarian National Authority for Data Protection and Freedom of Information, and – where the breach involves a high risk to the rights of the data subjects – informs the data subjects (Articles 33–34 GDPR).

9. RIGHTS OF THE DATA SUBJECT

Under the GDPR the data subject may exercise the following rights:

- **access** (Article 15): information as to whether the Controller processes personal data concerning them, and a copy of those data;
- **rectification** (Article 16): correction of inaccurate data and completion of incomplete data;
- **erasure** (Article 17): erasure of the data where their processing is no longer necessary or is unlawful; erasure cannot be requested for as long as the processing of the data is prescribed by law (such as the AML Act or the Accounting Act);
- **restriction** of processing (Article 18);
- **data portability** (Article 20): receiving and transmitting, in a machine-readable format, the data processed by automated means on the basis of consent or a contract;
- **objection** (Article 21): to processing based on legitimate interest;
- **withdrawal of consent** (Article 7(3)): at any time and free of charge, in the case of processing based on consent.

The Controller complies with the request **within 1 (one) month** of its receipt; under Article 12(3) GDPR this period may be extended by two months in justified cases, of which the Controller informs the data subject. The request may be submitted at the e-mail address given above or by post, sent to the Controller's registered office. Where necessary, the Controller identifies the applicant.

Automated decision-making, profiling: the Controller does not carry out automated decision-making or profiling.

10. REMEDIES

Complaint to the Authority: Hungarian National Authority for Data Protection and Freedom of Information (NAIH) 1055 Budapest, Falk Miksa utca 9–11. | Postal address: 1363 Budapest, Pf. 9. Telephone: +36 (1) 391-1400 | E-mail: ugyfelszolgalat@naih.hu | Website: https://naih.hu

Judicial remedy: the data subject may bring an action before the regional court with jurisdiction over their place of residence or place of stay. The action may – at the data subject's choice – also be brought before the regional court with jurisdiction over the Controller's registered office.

Before seeking a remedy, the data subject may also contact the Controller; the Controller investigates the complaint and informs the data subject of its outcome.

11. AMENDMENT OF THIS NOTICE

The Controller is entitled to amend this notice unilaterally if the circumstances of the processing, the legal environment or the content of the service change. The Controller publishes the amended notice on its website and informs its existing contractual clients of the amendment by electronic means.

This notice enters into force on 1 January 2026 and replaces the previous privacy notice.

Budapest, 1 January 2026

E-Marketplace Szolgáltató Kft.