

PRIVACY POLICY**FOR CUSTOMERS**

1. INTRODUCTION	2
2. DATA CONTROLLER'S DATA	3
3. TERMS AND PRINCIPLES OF DATA PROCESSING, RULES ON DATA SECURITY	4
4. RECIPIENTS OF PERSONAL DATA	6
5. THE PURPOSE AND LEGAL BASIS OF DATA PROCESSING, THE SCOPE OF THE PROCESSED DATA AND THE DURATION OF DATA PROCESSING	7
a. Data processing activities related to currency exchange operations	7
b. Data processing activities related to cash transfer activities	7
c. Data processing activities related to VAT refund activities	8
d. Data processing activities related to VAT refund activities	8
e. Activities prescribed by Act No. LIII of 2017	9
f. Handling complaints	12
g. Contact	12
h. Contact with the customers	12
i. Ensuring participation in the discount and VIP card programme	13
j. Newsletter and/or notification service	13
k. Data processing related to the mandatory camera surveillance system required by law	13
6. YOUR RIGHTS	15
- Right to prior information and right of access:	15
- The right to rectification	15
- Right of erasure ("the right to be forgotten")	15
- Right to restrict data processing	16
- The right to data portability	16
- The right to objection	16
- The right to lodge a complaint	16
- The right to legal remedies	17
- Right to information for children and persons under guardianship	17
- The right to withdraw consent	17
- Obligation to notify the rectification or erasure of personal data or the restriction of processing	17
- Automated decision-making on individual cases, including profiling	17
- Informing the Data Subject about a breach of data protection	17
7. FINAL PROVISIONS	18

1. INTRODUCTION

Please read this Privacy Policy (hereinafter referred to as the **Policy**) carefully to understand how we process your personal data and to learn about your rights in relation to data processing.

Exclusive Best Change Zrt. (hereinafter referred to as the **Data Controller** or the **Company**) processes data as necessary in the course of its activities, paying particular attention to the protection of personal data, compliance with legal requirements, and safe and fair data processing.

Data Controller shall inform natural persons about the principles, process and guarantees of data processing. Data Controller recognises the right of natural persons to have control over their own personal data. At the same time, it notes that the right to the protection of personal data is not an absolute right and must be taken into account and balanced with other fundamental rights, in accordance with the principle of proportionality.

Data Controller informs its customers, enquirers and users of the service of the way in which it processes their personal data. With this Privacy Policy, the Data Controller complies with its information obligations under the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) – hereinafter referred to as the **Regulation**).

Should you require any further information about this Privacy Policy or any other information or data management practices of the Company, please contact the Data Controller using one of the contact details provided in section 2.

2. DATA CONTROLLER'S DATA

Company name: EXCLUSIVE BEST Change Zrt
Registered office: H-7621 Pécs, Citrom utca 2-6. földszint 26. ajtó
Contact: DÁVID Judit, Data Protection Officer
E-mail: adatvedelem@exclusive.hu
Telephone: +36 70 380 7397

3. TERMS AND PRINCIPLES OF DATA PROCESSING, RULES ON DATA SECURITY

The terms used in the Policy are defined primarily on the basis of the Regulation.

In processing personal data, Data Controller shall act in accordance with the following principles of data management: purpose limitation, necessity and proportionality, lawfulness and fairness, transparency, data economy, proportionality and accountability.

For more information on the principles of data processing, see Article 5 of the Regulation. The main legislation applied by the Data Controller in its data management activities and referred to in this Privacy Policy:

- Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46 (Regulation)
- The Constitution of Hungary
- Act No. V of 2013 on the Civil Code (Civil Code)
- Act No. CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Act No. CXII)
- Act No. LIII of 2017 on the Prevention and Suppression of Money Laundering and Terrorist Financing (Act No. LIII)
- Act No. CCXXXVII of 2013 on Credit Institutions and Financial Undertakings (Act No. CCXXXVII)
- Government Decree No. 297/2001 (XII. 27.) on currency exchange activities (Decree No. 297/2001)
- Act No. LII of 2017 on the Implementation of the Financial and Proprietary Restrictive Measures ordered by the European Union and the United Nations Security Council (Act. No. LII)
- Screening system pursuant to Decree No. 26/2020 (VIII.25.) of the National Bank of Hungary (MNB) regarding service providers supervised by the (MNB) on the implementation of the Act on the Prevention and Suppression of Money Laundering and Terrorist Financing, as well as the Act on the Implementation of the Financial and Proprietary Restrictive Measures ordered by the European Union and the United Nations Security Council
- Regulation No. 19/2019 (V. 13.) of the MNB on the processing and distribution of banknotes and on technical tasks related to the protection of banknotes against counterfeiting
- Regulation No. 20/2019 (V. 13.) of the MNB on the processing and distribution of coins and on technical tasks related to the protection of banknotes against counterfeiting
- Act No. LXXXV of 2009 on the provision of payment services,
- Act No. CVIII of 2001 on certain aspects of electronic commerce services and information society services (Act No. CVIII)
- Act No. XLVIII of 2008 on the basic conditions and certain restrictions of economic advertising activities
- Act No. CLV of 1997 on Consumer Protection (Act No. CLV),
- Act No. XLVII of 2008 on the prohibition of unfair commercial practices against consumers,
- Act No. CXIX of 1995 on the processing of name and address data for the purposes of research and direct marketing
- Act No. C of 2000 on Accounting (Accounting Act)
- Act No. CL of 2017 on the Rules of Taxation (Taxation Act)
- Act No. XX of 1996 on the means of identification and the use of identification codes to replace the personal identification number
- Act No. CXXVII of 2007 on Value Added Tax (VAT Act)
- Act No. XLIII of 2021 on the establishment and operation of a data reporting background related to the identification tasks of financial and other service providers (Act No. XLIII)
- Government Decree No. 45/2014 (II. 26.) on the detailed rules of contracts between consumers and businesses

Data Controller takes into account the requirement of data security in the design of its entire data protection process in accordance with the “privacy-by-design” principle of data protection by default and by design.

Data Controller aims to minimise the processing of personal data in order to reduce the risks of data processing.

Data Controller, as part of its data security responsibilities,

- takes technical and organisational measures to secure electronically stored data;
- ensures that the data security rules required by law are complied with;
- ensures that data protection and confidentiality rules are enforced;
- prevents unauthorised access to data;
- takes the necessary measures to prevent any damage to the data;
- promotes data management awareness among its employees to ensure data security;
- ensures the physical protection of data stored in a paper-based format;
- ensures the physical protection of the devices used for electronically stored data;
- ensures password protection of electronically stored data;
- ensures regular backups of data;
- ensures that access to data is restricted to authorised persons.

Data Controller performs daily backups of its electronically stored data. Backups are stored on the Data Controller's own server and on an external server provided by the data processor. The maximum storage period for backups is 5 years.

Legal basis for backup processing: the legitimate interest of the Data Controller to comply with the requirements of the Regulation and to ensure the continuous and uninterrupted availability of data generated in the course of its activities. Data Controller handles a significant amount of data, and there is a significant public interest in the safe keeping of such data and its recovery in the event of any damage.

Purpose of the data processing: increase data security, preserve documents related to the operation of the Data Controller and restore them in case of a possible data security problem, ensure the continuity of work processes.

4. RECIPIENTS OF PERSONAL DATA

Data Controller's employees and agents are entitled to access the data only to the extent necessary for the performance of their duties.

As a general rule, Data Controller does not transfer data to third countries. Where such transfers are made on an ad hoc basis, Data Controller shall pay particular attention to informing data subjects and, where necessary, documenting their consent.

Data Controller mainly carries out data processing operations with the assistance of its own staff. In case of outsourced tasks or other cooperation, Data Controller transfers data to partners (data controllers or data processors).

Data Controller ensures that the legal conditions for data processing (purpose, legal basis) are met during such data transfer and that the data transfer does not violate your rights.

For details of the data processors, see the below chart:

	Exercised activity	Data processor's name	Data processor's contact
1.	Computer system operation, Server services	BLASTER Kft.	H-5600 Békéscsaba, Lencsési út 64. II. em. 5. ajtó
2.	Computer program development	EXCLUSIVE-NET Kft.	H-1052 Budapest, Váci utca 12.

Data transfer:

Subject to the conditions set out in the applicable laws and the agreement between the parties the Company transfers personal data to

- Raiffeisen Bank Zrt. (hereinafter referred to as the Bank) in connection with its currency exchange activities, and
- Western Union Payment Services Ireland Limited (hereinafter referred to as "WU") as sub-processor of Exclusive Cash Ltd. in connection with its cash transfer activities,
- INNOVA-INVEST Pénzügyi Zrt. (hereinafter referred to as INNOVA-INVEST) in connection with its VAT refund activities
- to Kupon Portfólió Kft. (hereinafter referred to as "Kupon Portfólió") in connection with the sale of toll stickers and mobile top-ups.

5. THE PURPOSE AND LEGAL BASIS OF DATA PROCESSING, THE SCOPE OF THE PROCESSED DATA AND THE DURATION OF DATA PROCESSING

In our relations with our customers, clients and interested parties, we continuously carry out data processing in accordance with the applicable legal provisions. Specific data processing activities are described below:

5.1. Activities of the Company as a data processor

a. Data processing activities related to currency exchange operations

The Company acts as the Bank's contracted principal intermediary and therefore, from the point of view of data protection, as a data processor under its contract with the Bank in relation to the following activities:

- currency exchange activities;
- reporting suspected counterfeit cash;
- handling complaints;
- issuing accounting documents.

Data of Raiffeisen Bank as data controller:

Company name: Raiffeisen Bank Zrt.
Registered office: H-1133 Budapest, Váci út 116-118
Website: <https://www.raiffeisen.hu>
Contact: Dr. BALÁZS Gergely, Data Protection Officer
E-mail: info@raiffeisen.hu
Telephone: +36 80 488 588

For more information on the Bank's data management, please refer to the Bank's Privacy and Data Management Policy. This Information is available on the Bank's website:

<https://www.raiffeisen.hu/raiffeisen-csoport/raiffeisen-bank-zrt/jogi-nyilatkozatok/adatkezelesi-tajekoztato>

b. Data processing activities related to cash transfer activities

The Company acts as a data processor of Exclusive Cash Kft. and as a data sub-processor of WU in the processing of data related to the Western Union money transfer service, and the rights and obligations related to the use of the data are determined by the data controller.

Data of Exclusive Cash Kft. as data processor:
Company name: Exclusive Cash Kft.
Registered office: H-1051 Budapest, Szent István tér 3.
Website: <https://exclusive.hu/>
E-mail: adatvedelem@exclusive.hu
Telephone: +36 70 380 7397

For more information on data processing by Exclusive Cash Kft, please refer to the Exclusive Cash Kft Privacy Policy, which is available on its website: <https://exclusive.hu/>

Data of WU as data controller:

Company name: Western Union Payment Services Ireland Limited
Registered office: Unit 9, Richview Business Park, Clonskeagh, Dublin 14, Ireland
Website: <https://www.westernunion.com>
E-mail: hungary.customer@westernunion.com, privacy@westernunion.com
Telephone: +36 80,200,159, +32 2639 7718

For more information on WU's data management, please refer to the company's Privacy Policy, which is available on its website:
<https://www.westernunion.com/content/wucom/global/hu/privacy-statement.html>

c. Data processing activities related to VAT refund activities

The Company is a contracted partner of INNOVA-INVEST and therefore acts, from a data protection point of view, as a data processor in relation to VAT refund activities.

Data of INNOVA-INVEST as data controller:

Company name: INNOVA-INVEST Pénzügyi Zrt.
Registered office: H-1118 Budapest, Dayka Gábor u. 3.
Website: <https://www.innovainvest.hu/>
E-mail: info@innovainvest.hu
Telephone: +36 1 485 2720

For more information on INNOVA-INVEST's data management, please refer to the INNOVA-INVEST Data Management Policy. This Information is available on the INNOVA-INVEST website:
<https://www.innovainvest.hu/adatvedelem.html>

d. Data processing activities related to VAT refund activities

The Company is a contracted partner of Kupon Portfólió and therefore, in terms of data protection, acts as a data processor in relation to toll sticker sales and mobile top-up activities.

Data of Kupon Portfólió as data controller:

Company name: Kupon Portfólió Kft.
Registered office: H-2161 Csomád, Liget utca 40.
Website: <http://www.kuponportfolio.hu/>
E-mail: adatbазis@kuponportfolio.hu
Telephone: +36 1 262 6662

For more information on Kupon Kft's data management, please refer to Kupon Kft's Data Management Policy. This Information is available on Kupon Kft's website:
<https://www.innovainvest.hu/adatvedelem.html>

5.2. Activities of the Company as a data controller

e. Activities prescribed by Act No. LIII of 2017

The Company carries out its activities indicated under section 5.1 of this Policy as a data processor for the independent data controllers indicated therein. With regard to these activities, Act No. LIII of 2017, other legislation and its internal rules impose due diligence obligations which the Company fulfils as a data controller and transfers certain personal data processed by it to the independent controller on the basis of an agreement with the latter and its internal rules.

The Company shall establish a Money Laundering Policy and an Internal Risk Assessment Policy with regard to the requirements of Act No. LIII of 2017, related legislation and legal requirements, and in order to provide its services in a prudent manner, identify, assess and manage the risks that may arise, and identify and manage specific risks from a money laundering prevention perspective for each of the services it provides.

Duration of the data processing: for 8 years from the date of execution of the transaction order pursuant to Articles 56, 57 and 58 of Act No. LIII of 2017; at the request of the supervisory authority, the financial information unit, the investigative authority, the prosecution and the court for the period specified in the request, up to a maximum of 10 years from the termination of the business relationship or the execution of the transaction order.

In the case of activities where the Company has a customer due diligence obligation as a data processor of an independent data controller, the Company shall comply with this obligation under Act No. LIII of 2017 as a data controller and shall transfer the processed personal data to the independent data controller accordingly.

(i) **Customer due diligence**

Data Controller is obliged to carry out customer due diligence if the conditions set out in Act No. LIII of 2017 and its internal rules are met, by recording the data and copying the necessary documents.

Purpose of the data processing: to carry out customer due diligence in the cases provided for in Article 6 of Act No. LIII of 2017

Interested parties: natural person clients and natural person representatives and proxies of legal entities or unincorporated organisations who use the services requiring customer due diligence under Act No. LIII of 2017 and the Company's Money Laundering Regulations.

Scope of the processed personal data: name and surname, name and surname at birth, date and place of birth, citizenship, address or, in the absence thereof, a place of residence, nature and extent of ownership interest in the case of a legal person, type and number of identification document, copy of identification document, declaration of being a public figure (whether the person concerned is a public figure or a relative of a public figure or a person closely associated with a public figure)

Legal basis for data processing: Article 6(1)(c) of the Regulation, Articles 1(1)(a), 3, 28, 30, 6(1)(b), (c), (d), (i), 7(1)-(3), 8, 9, 14/A of Act No. LIII of 2017

In case of failure to provide the data, the customer due diligence cannot be performed, so the Data Controller shall refuse to provide the service.

(ii) Control of effectively connected transactions

According to Act No. LIII of 2017, the customer due diligence obligation extends to cases where the amount of several effectively connected transaction orders in the case of currency exchange reaches the amount limit specified in Article 6(1)(b), (c) and (i) of Act No. LIII of 2017 and in the Company's internal regulations. Data Controller may request the presentation of supporting documents in order to verify the data.

Purpose of the data processing: to identify effectively connected transactions in the framework of the legal verification.

Interested parties: a natural person who is a customer or a representative or agent of a legal person or an unincorporated organisation who uses a service for an amount equal to or exceeding the specified threshold.

Scope of the processed personal data: name and surname, date and place of birth, name and abbreviated name of legal person and unincorporated entity, registered office, address of its branch in Hungary, in case of a foreign company that has such a branch

Legal basis for data processing: Article 6(1)(c) of the Regulation and Articles 6(2) and 14(1) of Act No. LIII of 2017

In case of failure to provide the data, the customer due diligence cannot be performed, so the Data Controller shall refuse to provide the service.

Duration of the data processing: up to 7 days from the date of execution of the transaction in the case of currency exchange, up to 1 year in other cases.

(iii) Identification of the beneficial owner

During the customer due diligence process, the natural person customer is required to make a written declaration by personal appearance if acting on behalf or in the interest of a beneficial owner.

The representative of the client of the legal person or unincorporated entity must declare in writing, on the basis of accurate and up-to-date records kept by the client, the beneficial owner of the legal person or unincorporated entity client.

Based on the declaration, the Company will verify the data in the register of beneficial owners in accordance with Act No. XLIII.

Purpose of the data processing: to comply with the legal obligation to identify the beneficial owner

Interested parties: the natural person who is considered the beneficial owner

Scope of the processed personal data: name and surname, name and surname at birth, citizenship, place and date of birth, address, or, in the absence thereof, place of residence, where the customer is a legal person or an unincorporated entity, the nature and extent of the ownership interest

Legal basis for data processing: Article 6(1)(c) of the Regulation, Article 8(1) and Article 9(1)-(2) of Act No. LIII of 2017, Article 3(14) and Article 8(3) of Act No. XLIII

By providing the third party with personal data, the customer declares that he/she has made the third party aware of the provisions of this privacy policy. If the customer provides personal data relating to a third party without the Data Controller having made its privacy policy available, the Data Controller shall be fully and unlimitedly liable for any resulting adverse legal consequences (costs of handling the data subject's complaint, payment of any fines, etc.).

(iv) Processing data on the source of funds and assets during customer due diligence

In cases governed by law and its internal rules, the Data Controller shall process the information relating to the source of funds and assets provided by the customer in the course of customer due diligence. The data provided by the customer may contain personal data. **In such a case, by providing the third party with personal data, the customer declares that he/she has made the third party aware of the provisions of this privacy policy.** If the customer provides personal data relating to a third party without the Data Controller having made its privacy policy available, the Data Controller shall be fully and unlimitedly liable for any resulting adverse legal consequences (costs of handling the data subject's complaint, payment of any fines, etc.).

Purpose of the data processing: to obtain information on the source of funds and assets as required by law

Interested parties: the customer and any other person (other than the customer) concerned by the data supplied by the customer

Scope of the processed personal data: the scope of personal data cannot be predefined, as the data are provided by the customer

Legal basis for data processing: Article 6(1)(c) of the Regulation and Articles 16(3)(a), 16/A(1)(a), (ac) and 56 of Act No. LIII of 2017

In case of failure to provide the data, the customer due diligence cannot be performed, so the Data Controller shall refuse to provide the service.

(v) Monitoring

Data Controller shall, on the basis of the applicable legal provisions and its own internal rules, review (monitor) transactions and financial operations that are complex, unusual or without economic or legitimate purpose, shall carry out a risk assessment of customers and transactions, and establish a customer profile.

Purpose of the data processing: compulsory risk assessment of complex transactions and financial operations that are considered unusual or without economic or legitimate purpose, risk profiling for the prevention of money laundering and terrorist financing

Interested parties: customers involved in complex transactions and financial operations that are considered unusual or without economic or legal purpose, returning customers

Scope of the processed personal data: surname and given name, name and surname at birth, place and date of birth, citizenship, address or, in the absence thereof, place of residence, number and type of identification document, mother's name at birth, foreign currency status, type of transaction, currency and value

Legal basis for data processing: Article 6(1)(c) of the Regulation and Article 11(3) of Act No. LIII of 2017

f. Handling complaints

Data Controller's complaints handling is governed by its specific rules.

Purpose of the data processing: identification, ensuring the right to complain, documenting the complaint

Interested parties: person lodging the complaint, persons concerned by the complaint

Scope of the processed personal data: personal data provided in the complaint, date of the complaint, documents related to the complaint and its investigation, date of the reply to the complaint.

Legal basis for data processing: Article 6(1)(c) of the Regulation - statutory obligation, Act No. CLV of 1997, Article 17/A

Duration of the data processing: the documents related to the complaint and its investigation must be kept for 3 years in accordance with Article 17/A of the Consumer Protection Act

Method of data storage: in a paper-based format, in a locked office at the Data Controller's headquarters

g. Contact

Data Controller sends replies to the persons who contact it, and keeps contact with them.

Purpose of the data processing: keeping contact

Interested parties: persons who contact the Data Controller

Scope of the processed personal data: name and surname, telephone number, e-mail address (depending on the method of contact)

Legal basis for data processing: Article 6(1)(a) of the Regulation – consent of the data subject

In the absence of contact details, the Data Controller cannot keep contact with the data subject.

Duration of the data processing: 30 days after the completion or termination of the transaction/service or until the consent is withdrawn, whichever occurs first

h. Contact with the customers

Data Controller processes the customer's contact details in order to communicate directly with them.

Purpose of the data processing: keeping contact with customers

Interested parties: customers with whom the Data Controller maintains contact in the course of providing a service

Scope of the processed personal data: name and surname, telephone number, e-mail address

Legal basis for data processing: Article 6(1)(b) of the Regulation – performance of the contract

Data provision is not obligatory.

Duration of the data processing: 30 days after the completion or termination of the transaction / service

i. Ensuring participation in the discount and VIP card programme

The Data Controller provides its customers participating in the Discount and/or VIP Card Programs with the opportunity to benefit from discounted services.

Purpose of the data processing: Ensuring participation in the discount and/or VIP card programme

Interested parties: customers or interested parties who agree to participate in the programme

Scope of the processed personal data: name and surname, e-mail address, address in the case of a discount card, and – if the data subject provides it separately – telephone number in case of a VIP card

Legal basis for data processing: Article 6(1)(a) of the Regulation – consent of the data subject

Data provision is not obligatory.

Duration of the data processing: until consent is withdrawn or until the end of the programme (whichever occurs earlier)

j. Newsletter and/or notification service

The Data Controller sends notifications in the form of e-mail newsletters and SMS or e-mail notifications to interested parties and customers. The Data Controller sends information about news, promotions and other useful information in the promotional newsletter, and about current promotions and prices in the notification service.

Purpose of the data processing: keeping contact with interested parties, clients and conducting promotional activities

Interested parties: any person who consents to the processing of their personal data when subscribing to the newsletter and/or notification service

Scope of the processed personal data: first name and surname, (i) in case of a newsletter service, furthermore: e-mail address; (ii) in case of a notification service, e-mail address or telephone number.

Legal basis for data processing: Article 6(1)(a) of the Regulation – consent of the data subject

Data provision is not obligatory.

Duration of the data processing: until consent is withdrawn or until the end of the service (whichever occurs earlier)

k. Data processing related to the mandatory camera surveillance system required by law

Data Controller operates a camera surveillance system in its currency exchange premises. The exact location of the cameras is set out in the Annex to this Document.

Purpose of the data processing: to provide the legally required camera surveillance

Interested parties: persons entering the camera's field of view

Scope of the processed personal data: conclusion drawn from the behaviour of the person concerned, his/her image

Legal basis for data processing: Article 6(1)(c) of the Regulation and Article 11 of Decree No. 297/2001

Data recording is automatic.

Duration of the data processing: according to Article 11 (3) of Decree No. 297/2001, the Data Controller is required to keep the footage for 50 days from the date of recording and to destroy it after the expiry of the deadline.

6. YOUR RIGHTS

You may address your requests, questions, complaints, or comments on the Data Controller's conduct directly to the Data Controller's representative using the contact details provided in section 2.

You may exercise your rights in relation to data processing by submitting a request to the Data Controller. Data Controller shall respond to any request made using any of its contact details without undue delay and at the latest within 1 month of receiving the request. Data Controller shall take its decision with regard to the legal basis of data processing when assessing requests. You are entitled to exercise your above-mentioned rights as follows:

	Consent	Performance of the contract	Legal obligation	Legitimate interest
provision of information	X	X	X	X
rectification	X	X	X	X
restriction	X	X	X	X
erasure	X	X	X	X
objection				X
data portability	X	X		
withdrawal of consent	X			
lodging a complaint	X	X	X	X
legal remedies	X	X	X	X

Please contact us electronically if possible. Please be informed that the Data Controller will respond to data protection requests by electronic means wherever possible, unless you, as the data subject, explicitly request otherwise or the Data Controller does not know your electronic contact details. X

Please be informed that if the request for the release of the data involves disproportionate additional costs for the Data Controller (e.g. due to the format chosen), the Data Controller is entitled to charge you, as the data subject, for the costs related to the release of the data. The Data Controller shall inform the applicant in advance of any costs incurred.

Please note that for persons under the age of 18, only their legal representative is entitled to act on their behalf.

- Right to prior information and right of access:

You are entitled to be informed in advance of the facts and events relating to the processing of your personal data, prior to the start of the processing, which is provided by the Data Controller through the content of this Policy and other informative documents. You also have the right to receive feedback from the Data Controller as to whether or not your personal data are being processed and, if such processing is ongoing, you have the right to access the personal data and related information as set out in the Regulation. For more detailed information, see Articles 13-14 of the Regulation.

- The right to rectification

On the basis of the principle of accuracy, you have the right to have inaccurate personal data relating to you rectified by the Data Controller without undue delay upon your request. Please provide the correction relating to your data in your application. You will be informed of the rectification. For more detailed information, see Article 16 of the Regulation.

- Right of erasure ("the right to be forgotten")

You have the right to have your personal data erased by the Data Controller at your request if one of the conditions set out in Article 17 of the Regulation applies:

- o The data no longer need to be processed for the purposes for which they were originally collected.
- o The Data Subject has withdrawn his or her consent and the Data Controller has no other legal basis for the processing.

- The Data Subject objects to the processing and there are no grounds which override such exercise of the Data Subject's rights.
- The data processing was unlawful.
- The erasure of data is required by law.

For more detailed information, see Article 17 of the Regulation.

- Right to restrict data processing

You have the right to have the Data Controller restrict data processing at your request in the following cases:

- You dispute the accuracy of the data – until the verification of the accuracy of the personal data.
- In case of unlawful processing, where the Data Subject opposes to the erasure but requests the restriction of the processing.
- The purpose of the data processing has ceased, but the Data Subject requires the data in order to assert or defend a legal claim.
- Where the legal basis for processing is the legitimate interest of the Data Controller, but the Data Subject objects to the processing, the processing shall be restricted until the determination of the prevailing interest.

For more detailed information, see Article 18 of the Regulation.

- The right to data portability

If the data processing is based on your consent or on the performance of a contract and the processing is automated, you have the right to receive the personal data concerning you in a structured, commonly used, machine-readable format and you also have the right to transmit these data to another Data Controller.

For more detailed information, see Article 20 of the Regulation.

- The right to objection

You have the right to object at any time to the processing of your personal data carried out for legitimate interests (Article 6(1)(f) of the Regulation) or for direct marketing purposes. In the event of an objection, the Data Controller is entitled to further processing only if it can prove that the processing is justified by compelling legitimate grounds which override the rights of the Data Subject or if the processing is necessary for the presentation or exercise of a legal claim. If the data are processed for direct marketing purposes, then no further processing may be carried out for this purpose following the objection of the Data Subject.

For more detailed information, see Article 21 of the Regulation.

- The right to lodge a complaint

You have the right to lodge a complaint about the processing of your personal data, first of all with the Data Controller and its representative, and also with the supervisory authority in the Member State where you reside, work or where the alleged infringement occurred.

Contact details of the supervisory authority:

- Name: National Authority for Data Protection and Freedom of Information
- postal address: H-1363 Budapest, Pf. 9.
- address: H-1055 Budapest, Falk Miksa utca 9-11.
- Telephone: +36 (1) 391-1400
- Fax: +36 (1) 391-1410
- E-mail: ugyfelszolgalat@naih.hu
- URL <http://naih.hu>

- The right to legal remedies

You have the right to a judicial remedy against a binding decision of the supervisory authority that applies to you, or if the supervisory authority has not dealt with your complaint or has not been informed you of the procedure relating to your complaint within 3 months. The Data Subject may exercise his/her right of legal remedy before the competent court.

For more detailed information, see Article 78 of the Regulation.

You also have the right to an effective judicial remedy against the Data Controller or the Data Processor if you consider that your personal data have not been processed in accordance with the Regulation. You may exercise your right of legal remedy before the competent court.

For more detailed information, see Article 79 of the Regulation.

- Right to information for children and persons under guardianship

Children and persons under guardianship also have the right to information. The Data Controller shall fulfil this obligation by informing the legal representative or guardian, provided that the legal representative or guardian shall undertake to inform the child or the person under guardianship in a manner appropriate to their capacity to understand. Where the age and maturity of the child allows, the Data Controller shall also provide the child, at the explicit request of the child or the legal representative, with brief verbal information about the processing of his/her data.

- The right to withdraw consent

You may withdraw your consent to the data processing at any time, without giving any reason, but such withdrawal shall not affect the lawfulness of the processing based on your consent prior to its withdrawal.

- Obligation to notify the rectification or erasure of personal data or the restriction of processing

The Data Controller shall inform each recipient to whom or with which the personal data have been disclosed of any rectification, erasure or restriction of processing, unless this proves impossible or requires a disproportionate effort.

For more detailed information, see Article 19 of the Regulation.

- Automated decision-making on individual cases, including profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or which would affect you in a similarly significant way, except for processing based on your consent for the performance of a contract, or where such processing is permitted by law.

For more detailed information, see Article 22 of the Regulation.

- Informing the Data Subject about a breach of data protection

If a breach of personal data is likely to result in high risks to the rights and freedoms of natural persons, the Data Controller shall inform you of the personal data breach without undue delay. For more detailed information, see Article 34 of the Regulation.

7. FINAL PROVISIONS

Exclusive Best Change Kft. shall require its employees and contractual partners to apply the procedures based on the provisions of this Policy. The contents of this Policy are valid from the present date until revoked. For any further questions, the Data Controller's staff is at your disposal at the contact details indicated in section 2.

Place and date: Budapest, 1 July 2022

Exclusive Best Change Zrt.

Version number: 2.0.