EOS KSI Ltd. informs the data subjects by means of this privacy notice about the facts and circumstances related to the processing of personal data, in particular the fact, duration, legal basis and purposes of each processing, the scope and source of the personal data processed, the recipients of the data transfers, including third country recipients and international organisations. The information contained in this privacy notice also covers the rights and remedies of data subjects in relation to each processing operation.

Name of the controller: **EOS KSI Kft.** (hereinafter referred to as the "Company")
Headquarters: 1132 Budapest, Váci út 30.
Company registration number: 01-09-568714
Registered by: the Company Court of the Metropolitan Court of Budapest
Tax number: 12242078-2-41
Phone number: +36 1 885-0150
E-mail address: info@eos-ksi.hu
Web address: https://hu.eos-solutions.com/

Contact details of the Data Protection Officer:
Address: 1132 Budapest, Váci út 30.
E-mail address: adatvedelmifelelos@eos-hungary.hu

I. Definitions

1. data subject: a natural person identified or identifiable on the basis of any information
2. 'identifiable natural person' means a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person
3. personal data: any information relating to the data subject
4. special categories of personal data: any data which fall within special categories of personal data, namely personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data revealing the identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons
5. health data: personal data relating to the physical or mental health of a natural person, including data relating to health services provided to a natural person which contain information about the health of the natural person
6. data processing: any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
7. controller: a natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of the processing are determined by Union or Member State law, the controller or specific criteria for the designation of the controller may also be determined by Union or Member State law
8. 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of, in the interest of and under the instructions of the controller, for the purposes and by the means specified by the controller
9. consent: a freely given, explicit and properly informed indication of the data subject's wishes by which he or she signifies, by a statement or by other means which unambiguously express his or her wishes, his or her agreement to the processing of personal data relating to him or her
10. recipient: the natural or legal person or unincorporated body to whom or to which personal data are disclosed by the controller or processor
11. third party: a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or the persons who, under the direct authority

of the controller or processor, are authorised to process personal data
12. restriction of processing: blocking of stored data by marking it for the purpose of restricting its further processing
13. data blocking: the marking of data with an identification mark for the purpose of limiting its further processing permanently or for a limited period of time
14. data marking: the marking of data with an identification mark to distinguish it from other data
15. Profiling: any processing of personal data by automated means intended to evaluate, analyse or predict personal aspects relating to the data subject, in particular his or her performance at work, economic situation, state of health, personal preferences or interests, reliability, behaviour, location or movements.
16. data breach: a breach of data security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, transmission or access to, or unauthorised disclosure of, personal data transmitted, stored or otherwise processed
17. objection: a statement by the data subject objecting to the processing of his or her personal data and requesting the cessation of the processing or the erasure of the processed data
18. erasure: making data unrecognisable so that it is no longer possible to recover it
19. data destruction: the complete physical destruction of the data medium containing the data
20. transfer: making data available to a specified third party
21. indirect transfer: the transfer of personal data to a controller or processor in a third country or to a controller or processor in another third country or to a processor in an international organisation by transferring the personal data to the controller or processor in a third country or to a processor in an international organisation
22. third country: any state that is not an EEA member state
23. 'international organisation' means an organisation governed by public international law and its subsidiary organs, and any other organ which is established by or under an agreement between two or more States
24. EEA State: a Member State of the European Union and another State party to the Agreement on the European Economic Area, and a State whose nationals enjoy the same status as nationals of a State party to the Agreement on the European Economic Area under an international treaty between the European Union and its Member States and a State not party to the Agreement on the European Economic Area
25. data medium: any material containing personal data, in whatever form, by whatever means and by whatever process
26. Principal: other company entrusting the Company with the management of receivables
27. Customer: obligor in consumer contracts with a principal

II. Data management activities

1. Claims

1.1 Purpose of processing:

Receivables management includes the following activities, depending on the content of the order:

- the receipt of the Customer's and the claim data from the Principal;
- checking, clarifying, modifying and forwarding the Client's data to the Client with the Client's prior consent;
- Contacting and maintaining contact with the Client;
- Recording of an environmental study, assessment of the Client's ability and willingness to pay; forwarding to the Client;
- enforce the Claim outside the legal procedure, conclude a payment agreement with the Client;
- assisting in the legal enforcement of the Claim;
- find new contact details and forward them to the Client with the Client's consent;
- keeping records to enable the above to be carried out.

1.2 Scope of data processed:

Name, name at birth, place of birth, date of birth, mother's name, permanent address, postal address, place of residence, landline phone number, mobile phone number, fax, e-mail address, debt by title (principal, interest, charges), invoice number

1.3 Legal basis for processing: performance of contract, consent

1.4 Duration of processing: the Company will store the data until the earliest of the following events:

- for the period specified in the contract with the Client, failing which until the termination of the Assignment; or
- the details of the individual acting as a proxy or legal representative until the individual ceases to be so entitled; or
- for the period specified in the Act: no later than 8 years from the termination of the debt collection activity, given that these data are contained in accounting documents, in particular contracts, settlement and instalment agreements, cash flow statements, bank statements, cash receipts, court decisions on property and costs, judgments with the force of res judicata [the retention period is governed by Section 169 (2) of Act C of 2000 on Accounting]
- or until the withdrawal of the data subject's consent.

1.5 Data source: the Client, data subject, address registrar, data processor

1.6 Recipients: representative, data processor, partner office

1.7 Data processors: Express Profit Balance Kft., Reisswolf Budapest Kft., DIGICOM MÉDIA Kft., Magyar Telekom Nyrt., TC&C Kft., PCS-SYSTEM Kft., EOS Holding GmbH Cross-border Center

1.8 The fact of transfer of personal data to third countries or international organisations: transfer to a foreign controller - for recovery purposes

1.9 The fact of automated decision-making, including profiling: -

2. Voice Recording - Administration

2.1 Purpose of data processing: the purpose of recording and storage is to fulfil a legal obligation to which the Company is subject.

2.2 Data processed: voice, unique identification number of the voice recording, date and time of the call, data necessary for identification during the case management (file number, name, mother's name, place and date of birth), data spoken during the case management (e.g. data on the claim, data on the contract, etc.

2.3 Legal basis for processing: legitimate interest (The interest test is set out in Annex 1 to the Prospectus)

2.4 Identification of legitimate interest: the Company has a legitimate interest, first and foremost, to have the audio recording in its possession and to use it as evidence in pursuing its claim in court (admission of debt that interrupts the limitation period). In a complaint procedure, the Company may have to prove that the conversation giving rise to the complaint was conducted in a polite and appropriate tone; in a public authority procedure, it may have to prove that its conduct or actions were in conformity with the request made in the conversation

2.5 Duration of data processing: the Company shall retain the audio recording for 5 years, but shall erase the audio recording without undue delay if the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or limit the processing to the duration of the data subject's legitimate interest not to erase the audio recording if the audio recording is no longer necessary for the purposes of the processing but the data subject requires the

audio recording for the establishment, exercise or defence of legal claims before the expiry of the retention period

2.6 Data source: client (for identification data), data subject

2.7 Recipients: Client, representative, data processor, court, authority

2.8 Data processor: TC&C Kft.

2.9 The fact of transfer of personal data to third countries or international organisations: -

2.10 The fact of automated decision-making, including profiling: -

3. Voice recording - complaint handling

3.1 Purpose of processing: to comply with a legal obligation applicable to the Company [the purpose is governed by Section 288 (2) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings and Section 17/B (3) of Act CLV of 1997 on Consumer Protection]

3.2 Data processed: unique identification number of the voice, voice recording, date and time of the call, data necessary to identify the complainant (file number, name, mother's name, place and date of birth), data spoken during the complaint handling

3.3 Legal basis for processing: fulfilment of a legal obligation [the legal basis is governed by Section 288 (2) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings and Section 17/B (3) of Act CLV of 1997 on Consumer Protection]

3.4 Duration of data management: the Company is obliged to keep the audio recording of the complaint received by the call centre for 5 years.

3.5 Data source: client (for identification data), data subject

3.6 Recipients: Client, representative, data processor, court, authority

3.7 Data processor: TC&C Kft.

3.8 The fact of transfer of personal data to third countries or international organisations: -

3.9 The fact of automated decision-making, including profiling: -

4. Operation of an electronic monitoring and recording system

4.1 Purpose of data processing: protection of persons, protection of property, protection of confidentiality, protection of the Company's premises open to customer traffic, proof of infringements, prevention of infringements

4.2 Scope of data processed: image, action

4.3 Legal basis for processing: legitimate interest based on Article 6(1)(f) of the GDPR

4.4 Identification of legitimate interests: protection of persons, property, business, tax and banking secrecy, protection of the Company's premises open to customer traffic, proof and prevention of infringements

4.5 Duration of processing: in premises open for customer reception (e.g. (e.g. cashier, customer service, customer bargaining and entrance), the storage period of the video recordings shall not exceed 5 days, but shall delete the video recording without undue delay if the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or shall limit the processing to the duration of the legitimate interest of the data subject not to delete the recording, if he or she no longer needs the video recording for the purposes of the processing, but the data subject requires the continuous recording before the expiry of the retention period for the establishment, exercise or defence of legal claims [the retention period is governed by the provisions of the Act on the Protection of Persons and Property and on the Private Investigation Activity (2005. CXXXIII of 2005, Section 31 (4) a) and Section 31 (6) of the same section shall apply]

4.6 Data source: concerned

4.7 Addressees: court, authority

4.8 The fact of transfer of personal data to third countries or international organisations: -

4.9 The fact of automated decision-making, including profiling: -

5. Complaints handling

5.1 Purpose of processing: to comply with a legal obligation applicable to the Company [the purpose is governed by Section 288 (1) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings and Section 17/B of Act CLV of 1997 on Consumer Protection]

5.2 Scope of data processed: description of the complaint, indication of the event or fact which is the subject of the complaint, the date of lodging the complaint, a list of the documents, records and other evidence presented by the customer, a description of the action taken to settle or resolve the complaint, the reason for refusal, the date of the reply to the complaint, név, születési név, anyja neve, születési hely, idő, lakcím, kézbesítési cím, ügyiratszám, ügyfélszám, a szerződés típusa és azonosítója (száma), a szerződés létrejöttének és megszűnésének időpontja, ügyféli minőség (adós, adóstárs, kezes, dologi kötelezett, tartozásátvállaló stb.), capacity of representative (agent, trustee, guardian, legal representative), amount and currency of the loan, credit or lease, amount, title and due date of the invoice, date of issue, serial number of the invoice, date of default, amount and currency of the instalment, due date, method and frequency, place of consumption, billing address, property to be covered (name of the municipality, location, parcel number, ownership), vehicle/leased object (type, engine number, chassis number, registration number), date of application for payment order, order number, court file number, date of application for enforcement, enforcement file number, bailiff file number, final decision number, date of entry into force, date of assignment, title, amount, composition of debt (principal, interest, costs)

5.3 Legal basis for processing: fulfilment of a legal obligation [the legal basis is defined in Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings No.288. § (3) of the Government Decree No. 435/2016 (XII. 16.) on the detailed rules for the complaint handling procedure and complaint handling rules of investment firms, payment institutions, electronic money institutions, voucher issuers, financial institutions and independent financial service intermediaries, paragraphs (2)-(3) of Article 3 of the Government Decree No. 435/2016 (XII. 16.), Annex 1, No. II.1 of the MNB Decree No. 28/2014 (VII. 23.) on the rules for the complaint handling of financial institutions..7., III.1., V.1. and Section 17/B of Act CLV of 1997 on Consumer Protection]

5.4 Duration of data processing: the Company is obliged to keep the complaint and the reply for 5 years, or limit the processing to the duration of the legitimate interest of the data subject not to delete the complaint and the reply, if the complaint and the reply are no longer needed for the purposes of data processing, but the data subject requires the complaint and the reply before the expiry of the retention period for the establishment, exercise or defence of legal claims [the retention period is determined in accordance with the provisions of the Act on Credit Institutions and Financial Undertakings of 2013 on the protection of the rights of the data subject]. CCXXXVII of 2007, § 288 (3) shall apply]

5.5 Data source: former holder of the claim (for data transferred in the course of an assignment), data subject

5.6 Addressees: representative, data processor, court, authority

5.7 Data processor: Reisswolf Budapest Kft., PCS-SYSTEM Kft.

5.8 The fact of transfer of personal data to third countries or international organisations: -

5.9 The fact of automated decision-making, including profiling: -

6. Contact

6.1 Purpose of data management: to contact and maintain contact, thereby facilitating the settlement of the debt, to provide accurate information on the current amount of the debt, the possibility of a settlement agreement, to raise awareness of the conditions for its conclusion, to provide information on possible debt management steps, their costs and, in the event of non-payment, the continuing increase in the debt, as well as where and how the debt can be settled

6.2 Data processed: address, postal address, e-mail address, telephone number
6.3 Legal basis for processing: consent, except for address data, where the performance of the contract
6.4 Duration of data processing: until consent is withdrawn or, in the absence of consent, at the latest until the recovery activity is terminated, and in the case of address data, at the latest 8 years from the date of termination of the recovery activity, given that this data is contained in accounting documents, in particular contracts, settlement and instalment agreements, cash flow statements, bank statements, cash receipts, property and cost-related court decisions, judgments with the force of res judicata [in the latter case, the retention period is determined in accordance with the provisions of the Act on Accounting of 2000. C Act C of 2006, § 169 (2) shall apply]
6.5 Data source: data subject, former claim holder, address registry
6.6 Addressees: representative, data processor
6.7 Data processor: Express Profit Balance Kft., Reisswolf Budapest Kft., PCS-SYSTEM Kft., TC&C Kft., Digicom Média Kft., Magyar Telekom Nyrt.
6.8 The fact of transfer of personal data to third countries or international organisations: -
6.9 The fact of automated decision-making, including profiling: -

7. Skip tracing

7.1 Purpose of data processing: to request data from the register containing personal, address and notification address data in order to pursue the legitimate interests of the Company
7.2 Data processed: address, notification address
7.3 Legal basis for processing: legitimate interest (The interest test is set out in Annex 3 to the Prospectus)
7.4 Identification of legitimate interest: the Company has a legitimate interest in processing the address data which is necessary for the enforcement of claims and the maintenance of contact
7.5 Duration of data processing: the Company will process the address data provided by the registration authority for a maximum of 8 years from the date of termination of the recovery activity
7.6 Data source: personal data and address register
7.7 Addressees: representative, data processor, court, public authority and enforcement body
7.8 Data processor: Reisswolf Kft., TC&C Kft.
7.9 The fact of transfer of personal data to third countries or international organisations: -
7.10 The fact of automated decision-making, including profiling: -

8. Contracting, assumption of debt

8.1 Purpose of data processing: agreement on payment facilities, establishment of a settlement agreement between the parties, making a declaration necessary for the assumption of a debt
8.2 Data processed: name, name at birth, mother's name, place and date of birth, address, file number, client number, type and identification number of the contract (on which the claim is based), capacity of the client (debtor, co-debtor, guarantor, debtor in rem, debt assumor, etc.), capacity of representative (agent, guardian, custodian, legal representative), amount and currency of instalment, due date, method and frequency, amount of discount, order for payment file number, enforcement file number, bailiff file number, final decision number, date of finality, date of assignment, title, amount, composition of debt (principal, interest, costs)
8.3 Legal basis for processing: performance of contract
8.4 Duration of processing: 8 years at the latest from the termination of the recovery activity, given that the document containing these data is an accounting document [the retention period is governed by Article 169 (2) of Act C of 2000 on Accounting]
8.5 Data source: concerned
8.6 Addressees: representative, data processor, court, public authority and enforcement body
8.7 Data processor: Reisswolf Kft.
8.8 The fact of transfer of personal data to third countries or international organisations: -

8.9 The fact of automated decision-making, including profiling: -

9. Preservation of evidence

9.1 Purpose of processing: to fulfil the obligation to keep records
9.2 Data processed: accounting voucher data [e.g. name, name at birth, mother's name, place and date of birth, address, file number, contract number (client number), bailiff file number, order for payment file number, court file number, NYUFIG basic number, amount and currency of instalment, due date, method and frequency, title, amount, composition of debt (principal, interest, costs), bank account number, amount and date of payment, payer ID, etc.]
9.3 Legal basis for processing: fulfilment of a legal obligation [the legal basis is governed by Section 169 (2) of Act C of 2000 on Accounting]
9.4 Duration of data processing: 8 years at the latest from the termination of the recovery activity [the retention period is governed by Section 169 (2) of Act C of 2000 on Accounting]
9.5 Data source: former holder of the claim, data subject, court, authority and enforcement body, employer
9.6 Addressees: representative, implementing body, data processor, auditor
9.7 Data processor: Reisswolf Kft.
9.8 The fact of transfer of personal data to third countries or international organisations: -
9.9 The fact of automated decision-making, including profiling: -

10. Purchase and sale of real estates

10.1 Purpose of data processing: to conclude sale and purchase contracts for real estate to be sold or purchased by EOS KSI Kft. and to provide the data necessary for the transfer of ownership and its registration.
10.2 Data processed: name, name at birth, mother's name, place and date of birth, address, capacity of representative (proxy, guardian, guardian, legal representative), in the case of auction sale, the auction transaction data, identification and descriptive data of the property, data contained in the contract of sale of the property.
10.3 Legal basis for processing: performance of the contract
10.4 Duration of data processing: 8 years at the latest from the date of the sale and purchase contract, given that the document containing these data is an accounting document [the retention period is governed by Article 169 (2) of Act C of 2000 on Accounting]
10.5 Data source: public land register concerned
10.6 Recipients: court, authority
10.7 Data processor: Reisswolf Kft.
10.8 The fact of transfer of personal data to third countries or international organisations: -
10.9 Fact of automated decision-making, including profiling: -

11. Sending a commercial newsletter

11.1 Purpose of data processing: sending newsletters to Clients or potential partners, informing them about current information on the Company's services, news, events.
11.2 Data processed: name, telephone number, e-mail address
11.3 Legal basis for processing: the collection of personal data is based on the voluntary consent of the data subject
11.4 Duration of processing: until consent is withdrawn
11.5 Data source: concerned
11.6 Recipients: -
11.7 Data processor: -
11.8 The fact of transfer of personal data to third countries or international organisations: -
11.9 The fact of automated decision-making, including profiling: -

12. Data management related to the prevention of money laundering and

terrorism (due diligence, management of beneficial ownership declaration)

12.1 Purpose of processing:The Data Controller processes personal data for the purposes of carrying out mandatory customer due diligence measures as defined by law, identifying the customer, risk classification of the customer, verifying the identity of the customer, and for the purpose of identifying and monitoring the purpose and nature of the business relationship and the transaction.
12.2 Scope of data processed: data pursuant to Articles 7 (2)-(3), 8 (2), 9 of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter: Pmt.)
12.3 Legal basis for data processing: fulfilment of a legal obligation (Art. 6 of the Data Protection Act)
12.4 Duration of processing: data will be kept for a maximum of 8 years after the business relationship has ended.
12.5 Data source: data subject or customer of the Company
12.6 Recipients may include: supervisory body, police, NAV investigative authority, TEK, administration, national security service, NAV KI PEI financial information unit, customs and other authorities, Refinitiv One World Check
12.7 Data processor: -
12.8 The fact of transfer of personal data to third countries or international organisations: -
12.9 The fact of automated decision-making, including profiling: -

13. Data processing for the prevention of money laundering and terrorism - for low-risk customers

13.1 Purpose of processing:The Data Controller processes personal data for the purposes of carrying out mandatory customer due diligence measures as defined by law, identifying the customer, risk classification of the customer, verifying the identity of the customer, and for the purpose of identifying and monitoring the purpose and nature of the business relationship and the transaction.
13.2 Scope of data processed: data pursuant to Article 7 (2) (a) (ab), (ad), (ae) and (b) (bd) and (be) of the Act on the Protection of Personal Data.
13.3 Legal basis for processing: the legitimate interest of the Data Controller to perform its legal obligations more effectively, based on the Risk Sensitive Approach of the Data Controller pursuant to Article 15 of the GDPR (Article 6 (1) (f) GDPR).
13.4 Duration of processing: data will be kept for a maximum of 8 years after the business relationship has ended.
13.5 Data source: data subject or customer of the Company
13.6 Recipients may include: supervisory body, police, NAV investigative authority, TEK, administration, national security service, NAV KI PEI financial information unit, customs and other authorities, Refinitiv One World Check
13.7 Data processor: -
13.8 The fact of transfer of personal data to third countries or international organisations: -
13.9 The fact of automated decision-making, including profiling: -

14. Data processing for the prevention of money laundering and terrorism - processing of identity documents for high-risk customers

14.1 Purpose of processing: verification of the identity of the beneficial owners of high-risk customers
14.2 Scope of data processed: identity document data
14.3 Legal basis for processing: legitimate interest of the Controller in legal compliance (Article 6(1)(f) GDPR)
14.4 Duration of processing: the data will be deleted immediately after verification.
14.5 Data source: data subject or customer of the Company
14.6 Recipients may include: supervisory body, police, NAV investigative authority, TEK, administration, national security service, NAV

KI PEI financial information unit, customs and other authorities, Refinitiv One World Check

14.7 Data processor: -

14.8 The fact of transfer of personal data to third countries or international organisations: -

14.9 The fact of automated decision-making, including profiling: -

15. Data management for the prevention of money laundering and terrorism - control activity on the source of funds and assets

15.1 Purpose of processing: to ensure that the funds of the Data Controller derived from economic activities originate from legal sources and that their origin can be verified

15.2 Data processed: personal identification data; data on the source of funds

15.3 Legal basis for processing: the legitimate interest of the Data Controller to be able to verify the legal origin of the source of funds and at the same time to ensure legal compliance (Article 6(1)(f) GDPR)

15.4 Duration of processing: data will be kept for a maximum of 8 years from the date of filtering.

15.5 Data source: concerned

15.6 Recipients may include: supervisory body, police, NAV investigative authority, TEK, administration, national security service, NAV KI PEI financial information unit, customs and other authorities, Refinitiv One World Check

15.7 Data processor: -

15.8 The fact of transfer of personal data to third countries or international organisations: -

15.9 The fact of automated decision-making, including profiling: -

16. Data management for the prevention of money laundering and terrorism - control activity on the source of funds and assets

16.1 Purpose of processing: to ensure that the funds of the Data Controller derived from economic activities originate from legal sources and that their origin can be verified

16.2 Scope of data processed: personal identification data; data on the source of funds; in the case of a legal person client, the title

16.3 Legal basis for data processing: fulfilment of legal obligations (Article 16/A (1) (a) (ac) of the Hungarian Banking Act, or in the case of payments of HUF 10 million or more, Article 24 (4) of MNB Regulation No.26/2020 (VIII. 25.)

16.4 Duration of processing: data will be kept for a maximum of 8 years from the date of filtering.

16.5 Data source: data subject or customer of the Company

16.6 Recipients may include: supervisory body, police, NAV investigative authority, TEK, administration, national security service, NAV KI PEI financial information unit, customs and other authorities, Refinitiv One World Check

16.7 Data processor: -

16.8 The fact of transfer of personal data to third countries or international organisations: -

16.9 The fact of automated decision-making, including profiling: -

17. Data management in relation to the prevention of money laundering and terrorism - monitoring tasks

17.1 Purpose of processing: to check the data and documents available and to ensure that the customer's risk level is up to date in the event of changes, and in addition to check the data every year for high-risk customers and every 5 years for low-risk customers, and to contact the data subject in this respect.

17.2 Scope of data processed: data available pursuant to Articles 7-10 of the Data Protection Act, contact details

17.3 Legal basis for data processing: fulfilment of a legal obligation (Art. 12 of the Data Protection Act)

17.4 Duration of processing: data will be kept for a maximum of 8 years after the business relationship has ended.

17.5 Data source: data subject or customer of the Company

17.6 Recipients may include: supervisory body, police, NAV investigative authority, TEK, administration, national security service, NAV KI PEI financial information unit, customs and other authorities, Refinitiv One World Check

17.7 Data processor: -
17.8 The fact of transfer of personal data to third countries or international organisations: -
17.9 The fact of automated decision-making, including profiling: -

III. Rights concerned

1. Right of access

1.1 In order to exercise the right of access, the data subject shall, upon request, be informed by the Company whether his or her personal data are processed by the Company itself or by a processor acting on its behalf or at its instructions.
1.2 All data subjects should have the right to know in particular

- the purposes for which personal data are processed
- the categories of personal data concerned
- where possible, the period for which the personal data are processed
- the recipients of the personal data
- the rights of the data subject, including the right to administrative redress
- information on the source of the data
- the circumstances in which the personal data breaches occurred in relation to the processing of the data subject's personal data, their effects and the measures taken to deal with them
- the fact of transfer of personal data to third countries or international organisations and the appropriate and suitable safeguards
- the logic underlying the automated processing of personal data, and
- the possible consequences of the processing, at least where it is based on profiling, and that
- be informed about all this.

1.3 The Company shall provide the information free of charge, without undue delay, but in any event within 25 days of receipt of the request, in writing by post or, if the data subject has submitted the request by electronic means, by electronic means.
1.4 If the Company fails to act on the data subject's request, it shall inform the data subject without delay, but no later than 25 days from the date of receipt of the request, of the reasons for the failure to act and of the right to lodge a complaint with the National Authority for Data Protection and Freedom of Information (hereinafter referred to as "the Authority") and to seek judicial remedy.

2. Right to rectification

2.1 In order to exercise the right of rectification, the Company shall, if the personal data processed by it or by a processor acting on its behalf or at its instructions are inaccurate, incorrect or incomplete, without undue delay, in particular at the request of the data subject, rectify or correct them or, if compatible with the purposes of the processing, supplement them with additional personal data provided by the data subject or with a declaration by the data subject on the personal data processed.
2.2 The Company is obliged to correct any inaccurate data, if the necessary data are available (e.g. from public records).
2.3 If the Company rectifies personal data processed by it or by a processor acting on its behalf or at its instructions, it shall inform the processor to which it transmitted the personal data concerned by the rectification of the personal data of the fact of the rectification and of the rectified personal data.
2.4 If the Company fails to act on the data subject's request, it shall inform the data subject without delay and at the latest within 25 days of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with the Authority and to seek judicial remedy.

3. Right to erasure

3.1 In order to enforce the right to erasure, the Company will delete the personal data of the data subject without undue delay if.

- the processing is unlawful, in particular where the processing is contrary to the data protection principles, the purpose of the processing has ceased or the further processing is no longer necessary for the purpose of the processing, the period laid down by law, an international treaty or a legally binding act of the European Union has expired or the legal basis for the processing has ceased and there is no other legal basis for the processing
- the data subject withdraws his or her consent to the processing and there is no other legal basis for the processing
- the erasure of the data has been ordered by law, an EU act, the Authority or a court
- the personal data must be erased in order to comply with a legal obligation under Union or national law applicable to the Company; or
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing.

3.2 The above rule on the erasure of personal data does not apply where the processing is necessary to comply with a legal obligation or to present, exercise or defend a legal claim.

3.3 If the Company deletes personal data processed by it or by a processor acting on its behalf or at its instructions, it shall notify the processors to which it transmitted the data prior to such action of the fact and the content of such action, in order to enable them to implement the deletion in respect of their own processing.

3.4 If the Company fails to act on the data subject's request, it shall inform the data subject without delay and at the latest within 25 days of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with the Authority and to seek judicial remedy.

3.5 The Company will inform all recipients to whom or with whom the personal data have been disclosed of the erasure, unless this proves impossible or involves a disproportionate effort. Upon request, the Company will inform the data subject of these recipients.

4. Right to restriction of processing

4.1 In order to enforce the right to restriction of processing, the Company restricts the processing of data

- where the data subject contests the accuracy or correctness of personal data processed by the Company or by a processor acting on its behalf or at its instructions and the accuracy or correctness of the personal data processed cannot be established beyond reasonable doubt, for the period necessary to resolve the doubt.
- the processing is unlawful and the data subject opposes the erasure of the data and instead requests the restriction of their use for the duration of the legitimate interest justifying the non-deletion (e.g. to bring a legal claim)
- the data subject has objected to the processing, in which case the restriction applies for the period until it is established whether the legitimate grounds of the Company prevail over the legitimate grounds of the data subject.

4.2 During the period of the restriction of processing, the Company or the data processor acting on its behalf or under its instructions may carry out processing operations other than storage with the personal data subject's consent, for the purposes of the data subject's legitimate interests or as provided for by law, international treaties or binding European Union acts.

4.3 The Company shall inform in advance the data subject at whose request the processing has been restricted of the lifting of the restriction of processing.

4.4 If the Company fails to act on the data subject's request, it shall inform the data subject without delay and at the latest within 25 days of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with the Authority and to seek judicial remedy.

4.5 The Company will inform all recipients to whom or with whom it has disclosed the personal data of the restriction, unless this proves impossible or involves a disproportionate

effort. Upon request, the Company will inform the data subject of these recipients.

5. Right to data portability

5.1 Where personal data are processed by automated means, the data subject shall have the right to obtain the personal data concerning him or her which he or she has provided to the Company in a structured, commonly used, machine-readable and interoperable format and to transmit them to another controller.

5.2 This right may be exercised where the data subject has provided the personal data on the basis of his or her consent or where the processing is necessary for the performance of a contract. This right may not be exercised where the legal basis for the processing is other than consent or a contract.

5.3 The data subject has the right to have data transmitted directly between controllers, where technically feasible.

5.4 The Company will comply with the request free of charge, without undue delay and in any event within 25 days of receipt of the request. If the Company fails to act on the data subject's request, it shall inform the data subject without delay and at the latest within 25 days of receipt of the request of the reasons for the failure to act and of the possibility to lodge a complaint with the Authority and to exercise his or her right of judicial remedy.

6. Right to object

6.1 Any data subject should also have the right to object to the processing of data relating to his or her particular situation, even if the personal data can be lawfully processed because the processing is necessary for the legitimate interests of the Company or a third party. In such a case, the Company may no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

6.2 The Company shall explicitly draw the attention of the data subject to the right to object at the latest at the time of the first contact with the data subject and shall display the information clearly and separately from any other information.

6.3 The Company will comply with the request free of charge, without undue delay and in any event within 15 days of receipt of the request. If the Company fails to act on the data subject's request, it shall inform the data subject without delay and at the latest within 15 days of receipt of the request of the reasons for the failure to act and of the possibility to lodge a complaint with the Authority and to exercise his or her right of judicial remedy.

6.4 If the Company agrees to the objection, it will cease processing and notify the objection or its action to all those to whom it has previously transferred the data.

7. Right to administrative redress

7.1 Anyone may lodge a complaint with the Authority to initiate an investigation on the grounds that there has been or is an imminent threat of a breach of rights in relation to the processing of personal data. The request must inform the Authority of any circumstances that may be relevant for the conduct of the investigation.

7.2 The Authority will only investigate the complaint of the data subject if he or she has already contacted the Company prior to his or her notification to the Authority in relation to the exercise of the rights indicated in the notification.

Contact details:
National Authority for Data Protection and Freedom of Information
Address: 1055 Budapest, Falk Miksa utca 9-11.
Mailing address: 1363 Budapest, Pf. 9.
Phone: +36 1 391-1400 Fax: +36 1 391-1410

E-mail: ugyfelszolgalat@naih.hu
Website: http://naih.hu

Activity: telephone exchange and telephone system maintenance

8. Right to judicial remedy

8.1 Irrespective of the decision of the Authority, the data subject may bring an action against the Company before the competent court of the place of establishment in the event of a violation of his/her rights, as a result of which, in addition to the court enforcing the exercise of the data subject's rights by ordering the Company to do so, the data subject may claim damages or compensation for damages.

IV. Data processors, contact details

1. Reisswolf Budapest Kft.

Headquarters: 1097 Budapest, Illatos út 6.
Company registration number: 01-09-715780
Registered by: the Commercial Court of the Metropolitan Court of Budapes
Tax number: 13039673-2-43

Activity: physical destruction of data stored on data media

2. Digicom Media Ltd.

Registered office: 6724 Szeged, Nádas utca 15/A.
Company registration number: 06-09-008823
Registered by: the Szeged Court of Szeged
Tax number: 13137180-2-06
Activity: bulk SMS
Activity: telephone directory enquiry

3. TC&C Ltd.

Head office: 1155 Budapest, Wesselényi u 35.
Company registration number: 01-09-168656
Registered by: the Company Court of the Metropolitan Court of Budapest
Tax number: 10780370-2-42