PRIVACY NOTICE

Effective for the data processing from 18 September 2026

1. General information on data protection and processing

1.1. Who is the data controller?

Erste Bank Hungary Zrt. (registered seat: H-1138 Budapest, Népfürdő u. 24-26.; website: www.erstebank.hu, email: erste@erstebank.hu; telephone: +36 (1) 298-0222, fax: +36 (1) 272-5160; hereinafter: "**Bank**" or "**Data Controller**") processes Your personal data either in the capacity of data controller or intermediary assigned by a third party data controller to carry out data processing activities (and also to act as intermediary for financial, auxiliary financial or investment services (hereinafter: **"Intermediary"**) or in the capacity of joint data controller with a third party company.

The Bank has a qualifying holding (100% ownership interest) in the following subsidiaries, which, together with the Bank shall mean the members of the Erste Bank Group (hereinafter jointly referred to as: **"Subsidiaries"**):

- Erste Befektetési Zrt. (registered seat: H-1138 Budapest, Népfürdő u. 24-26., Floor 8)
- Erste Lakás-takarékpénztár Zrt. (registered seat: H-1138 Budapest, Népfürdő u. 24-26.)
- Erste Jelzálogbank Zrt. (registered seat: H-1138 Budapest, Népfürdő u. 24-26.)
- Erste Ingatlan Kft. (registered seat: H-1138 Budapest, Népfürdő u. 24-26.)

The parent company of the Bank (a legal person possessing a qualifying holding in the Bank): Erste Group Bank AG (registered seat: Am Belvedere 1, 1100 Vienna, Austria).

1.2. Why is data privacy important?

Data privacy is a fundamental right. Similarly to freedom or security, you have the right to the protection of Your data.

Your personal data can contain a wide range of information about you: they may as well relate to your hobbies, preferences and aspirations. Such things are, of course, worth protecting. Yet Erste can only improve the customized service it provides to its customers if it is aware of its customers' preferences. It is important for Erste to cooperate with its customers to find ways to manage their data in the best interests and under the supervision of its customers. In processing personal data, Erste makes every effort to ensure the highest level of protection in accordance with applicable data protection and information security requirements.

In this notice, you will find and learn, among other things, about the data processing activities carried out by Erste as data controller, your data protection rights and the steps you can take to enforce your data protection rights.

1.3. What legislation applies to my data privacy rights? What is the GDPR and what does it regulate?

If we process Your personal data that qualifies You as a person identified or identifiable by the Bank (regardless of the purpose, legal title or duration of the processing of processing personal data), You shall be considered a Data Subject under the provisions of the governing

data protection legislation, and shall be entitled to the rights set forth in the governing data protection legislations, in particular, "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; "GDPR")" and Act CXII of 2011 on Informational Self-determination and Freedom of Information ("Info Act") regarding the processing and the protection of personal data (hereinafter together: rights related to the processing of personal data).

1.4. Basic concepts of data protection

What is personal data?

Personal data means any information relating to an identified or identifiable natural person, a co-called 'Data subject. E.g. a person's name or identifier, IBAN or account number. (For further detail, refer to Article 4(1) of the GDPR.)

What is data processing?

Processing means any operation or set of operations which is performed on 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 by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (For further detail, refer to Article 4(2) of the GDPR.)

Further definitions

Data Subject shall mean an identified or identifiable natural person (under Article 4(1) of the GDPR).

Consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Third Country shall mean any country other than the Member States of the European Union, Iceland, Liechtenstein and Norway is a third country.

Former Employee shall mean a natural person who worked for the Bank under an employment contract but is currently not employed by the Bank.

Employee shall mean a natural person who works for the Bank under an employment contract (under Section 34 (1) of Act I of 2012 on the Labour Code, hereinafter the Labour Code).

Employer shall mean a person having legal capacity that employs employees under employment contracts (under Section 33 of the Labour Code).

1.5. What is the Privacy Notice about?

This Privacy Notice contains information on the processing of the personal data related to all Data Subjects on the one hand, as well as additionally specific rules regarding the processing of the personal data related to each Data Subjects on the other hand. Certain rules of data processing are also included in the Business Rules of the Bank and the Bank shall also

undertake and make all effort to ensure that the Data Subject, prior to the commencement of the processing of personal data, get acquainted with that part of this Privacy Notice that concerns him/her. The Bank shall publish this Privacy Notice on its website at: https://www.erstebank.hu/hu/adatkezelesi and also make it accessible at its branches. The Bank may prepare an extract of this Privacy Notice regarding the various types of Data Subjects and may make it possible for the Data Subject affected by the processing of its personal data to make a declaration regarding that the preliminary information concerning the processing of personal data has been provided and his /her acknowledgement thereof by way of signing this document or an extract thereof.

This Privacy Notice shall apply to personal data processing activity(ies) carried out by the Bank as of the date specified in the header. The Privacy Notice effective at the time of the personal data processing carried out by the Bank prior to this Privacy Notice shall govern such processing of personal data by the Bank.

The Bank shall be entitled for the unilateral amendment of this Privacy Notice at any time. The amendment shall be applicable to personal data processing performed under the previous Privacy Notice of the Bank in respect of the new parts of the amendment (otherwise processing of such personal data shall be subject to the rules prevailing upon the commencement of the processing of the personal data), whereas personal data processing commenced following the amendment of the Privacy Notice shall be entirely governed by the amended Privacy Notice (which shall be deemed the Privacy Notice in force upon the commencement of the processing of the personal data in respect of these Data Subjects). The Bank shall make accessible all amendments of the Privacy Notice on its website https://www.erstebank.hu/hu/adatkezelesi. If the amendment is driven by legislative changes or by an administrative decision, or if the amendment does not concern issues relating to the processing of personal data (e.g. a change in the data protection officer or any other technical amendment) the change shall also apply to personal data processed prior to such amendment.

2. What do I have to know about the processing of my personal data at Erste?

2.1. The contact details of the Data Protection Officer:

In relation to the processing of your personal data you can contact the Data Protection Officer of the Bank in writing. Name and contact details of the data protection officer of the Bank: dr. Zsolt Misky; email: adatvedelem@erstebank.hu; mailing address: 1138 Budapest, Népfürdő utca 24-26.

2.2. Regulatory authority competent in data protection matters:

You can make a complaint in connection with processing by Erste or any data processor engaged by Erste to the Hungarian National Authority for Data Protection and Freedom of Information (contact details: (www.naih.hu), registered seat: 1055 Budapest, Falk Miksa utca 9-11. mailing address: 1363 Budapest, PO Box. 9, +36 (1) 391-1400, fax: +36 (1) 391-1410, email: ugyfelszolgalat@naih.hu), or the competent court.

2.3. Whose data is processed by Erste?

The Data Subjects of personal data processed in connection with our activities are typically:

1. **Customer:** means all the natural persons who use financial services / auxiliary financial services (the "**Service**") provided by the Bank as a financial institution

(Section 160 (2) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings, hereinafter the "**Banking Act**"),

2. **Applicant:** means all the natural persons who contact the Bank to receive Services, but who decide not to use such Services (Section 160 (2) of the Banking Act),
3. **Co-debtor, payment guarantor, a natural person providing other security:** means a person involved in the performance of a contract for financial service / auxiliary financial service (the "**Contract**") in addition to the debtor Customer, who shall be liable on behalf of /in addition to the debtor Customer upon a failure by the debtor Customer to satisfy its payment obligations under and as set forth in the Contract,
4. **Authorised representative:** means a natural person who acts on behalf of another natural or legal person as set forth in Section 6:11 of Act V of 2013 on the Civil Code, hereinafter the "**Civil Code**",
5. **Payer**: means a natural person making a cash deposit onto the customer's account maintained with the Bank,
6. **Beneficiary**: a natural or legal person who is the recipient of the funds constituting the subject of the payment transaction (Section 2 (12) of Act LXXXV of 2009 on payment services, hereinafter the "**Payment Services Act**"),
7. **Contact Person:** the person on behalf of the party entering into a Contract with the Bank as being specified in the Contract for the purpose of keeping contact,
8. **Employee**
9. **Former employee**
10. **Other Data Subject** (in particular, a person who signs up to a newsletter, contracted partner's contact person, contact person of a contracted partner, contact person of a potential entrepreneur/corporate client who is a natural person) All Data Subjects who are not classified as Data Subject specified in Clause III 1) through 9) of this Privacy Notice are included in this category.

The Bank shall process the personal data (including the contact data as well) provided by the Data Subject as a data related to the Data Subject (the check of which shall not be a duty of the Bank), except the case when the Data Subject provides the Bank with a declaration that the concerned personal data is not related to it, whereby the Data Subject shall ensure that the Bank has lawful right to process the personal data not related to it but to another entitled person. The Data Subject shall declare in these cases that if he or she provides Erste Bank Hungary Zrt. with data that is not related to him or her, then he or she has already informed the Data Subject that he or she has shared data with respect to him or her with the Bank, and the Data Subject has already information – based on the privacy notice of the Erste Bank at https://www.erstebank.hu/hu/adatkezelesi - on how Erste Bank processes data obtained not from the Data Subject. If a third party indicates to the Bank in relation to a contact managed by the Bank regarding the Data Subject that the Data Subject is not available at that contact, the Bank shall be entitled to inform thereabout the Data Subject at another contact managed by the Bank and to request that the Data Subject modify its particular contact details, and the Bank may restrict / erase / anonymize the processing of personal data challenged by a third party, even if it provides a service to the Data Subject for the given contact, in order that the Bank shall not process a third party related personal data without authorization.

2.4. What are the purposes and legal bases for processing my data?

- **Processing for the performance of a contract or actions taken at your request before entering into a contract**
  The services that Erste provides to its customers depend on the specific contact, e.g. loan contact, account contact, lease contact, insurance brokerage or George contact. For example, Erste may process customer data to enable customers to log in to George, manage their account online and carry out transactions. The scope of such processing is set out in the contractual

documents and the Business Rules and General Terms and Conditions in effect from time to time.

- **Processing for the fulfilment of a legal obligation**
  Personal data processing may also take place in the case and scope where the processing of personal data is necessary for compliance with a legal obligation. Such mandatory processing may occur, for example, in the following cases: Customer due diligence obligations under the rules on the prevention and combating of money laundering and terrorist financing, retention obligations under accounting rules, processing necessary for fraud prevention/fraud management.

- **Processing based on legitimate interest**
  If certain conditions are met, Erste may carry out processing on the basis of legitimate interests in order that the controller or a third party can pursue their legitimate interest.

- **Processing based on your consent**
  If there is no contract, legal obligation or legitimate interest, processing may also be lawful if the Data Subject has given his or her consent. The scope and content of such processing will always depend on the specific consent on a case-by-case basis. The Data Subject may withdraw his or her consent at any time for the future. The withdrawal of consent shall however not affect the lawfulness of processing based on consent before its withdrawal. This means that withdrawal of consent has no retrospective effect.

- **Processing for statistical purposes**
  The Bank may use your anonymized personal data (i.e. that may not be linked to the Data Subject) for statistical purposes.

2.5. Is there any other data processed about me in addition to the data collected from me?

In this Privacy Notice, we inform the Data Subject of the means applied for processing the personal data obtained from the Data Subject, learned by the Bank through the actions of the Data Subject and from conclusions drawn by the Bank regarding the Data Subject. If Your personal data processed by the Bank were not made available to the Bank by You, the Bank provides specific information under Article 14 of the GDPR, with the exception of the case(s) contained in Article 14 (5) of the GDPR. If the personal data was obtained from You as a Data Subject, that types of personal data related to You and processed by the Bank are contained in the forms via the completion thereof we manage Your personal data.

2.6. Do I have to provide my personal data? What if I do not want to do so?

For the establishment of a business relationship between the Data Subject and the Bank, the Bank shall be obliged to process the personal data of the Data Subject required by law and necessary for the fulfilment of a contract and for the establishment of a business relationship under the provisions of the law. In view of this, if the Data Subject may fail to provide the personal data required for the fulfilment of the contract or required by law, the Bank may refuse to provide certain services. In all other cases, we shall only process your data with a Data Subject consent, which you may provide only on a voluntary basis.

2.7. How long does Erste process my personal data?

If we are subject to an obligation to erase personal data, we comply with such erasure obligation by way of factual, final and irreversible destruction / anonymisation and take measures for the full destruction of the documents to be destructed under such erasure obligation. If the irrevocable and final erasure / anonymisation takes place in the course of our regular erasure procedure, we will not send separate information to the Data Subject about the implementation of the erasure, but will inform the Data Subject whether we maintain record of the Data Subject's personal data or not within the frame of exercising the right to access by the Data Subject. If the Data Subject submits an individual request for erasure, the Bank shall separately inform the Data Subject about the implementation of the irrevocable and final erasure / anonymisation (if the erasure is possible, otherwise about the reasons for refusal / partial implementation of the erasure). If the personal data requested to be erased by the Data Subject is the Data Subject's contact which we exclusively manage in relation to the Data Subject, we shall inform the Data Subject of the future erasure / anonymisation at this contact and the erasure shall be implemented thereupon by the Bank.

3. Information on Erste's data processing

3.1. Information on the processing of all Data Subjects' personal data

3.1.1. If the Bank has the right to process personal data, the Bank may also process under such right all related paper-based or electronic documents containing the Data Subject's relevant personal data through the entire duration of the processing of personal data contained in such documents.

Paper-based documents generated in the branch network in connection with customer relationships and the conclusion, maintenance and termination of account, credit and card agreements are digitalised and prepared for archiving within a closed process that also uses artificial intelligence. The documents are subsequently processed and stored in accordance with the Bank's standard internal procedures.

3.1.2. We inform the Data Subject that the duration of processing personal data by the Bank shall be extended (with the period of processing the following personal data, or with the outstanding time of such period) if, upon the expiration of the duration of the processing of personal data available to the Bank, criminal proceedings, claim management or such other proceedings are in progress against the Data Subject in the course of which the processing of personal data by the Bank is necessary for asserting its legal claim / for complying with a legal obligation of the Bank / a legitimate interest of the Bank exists for this purpose.

Cases of (further) processing of Your personal data, form and purpose of such processing	Duration of the personal data processing	Legal basis of the personal data processing
1) Upon a judgement adopted in civil proceedings for the benefit of the Bank, imposing a payment obligation on the opposing party or upon a settlement reached by the parties if recovery has not been achieved / the payment obligation has not been fulfilled.	5 years after the judgement becomes final (limitation of the enforcement right), upon claims arising from a labour relationship, duration is 3 years, except if such period of limitation is interrupted or suspended. The limitation of the right of enforcement will be	The legitimate interest of the Bank based on Section 57 of Act LIII of 1994 on Judicial Enforcement and on Section 286 of Act I of 2012 on the Labour Code - the Labour Code

	interrupted by any action of enforcement.	
2) (i) Regarding a judgement adopted in a litigation in favour of the Bank, imposing a payment obligation on the opposing party if recovery has been achieved in favour of the Bank, (ii) Upon a financial claim awarded to the claimant against the Bank if there has been recovery in favour of the claimant, (iii) Upon a settlement reached with the Bank (either in or outside a litigation) if the party under a payment obligation has fulfilled such payment obligation.	8 years following the year of adopting the annual accounts prepared for the year of issuance of the last accounting certificate related to the Contract (that is also considered the termination of the Contract) (under Section 169 (2) of the Accounting Act)	Completion of the legal obligation set out in Section 169 (2) of the Accounting Act
3) (i) Upon a judgement adopted in a litigation not imposing a payment obligation, irrespective of whether the Bank or the opposing party has been condemned, (ii) Upon a settlement not containing a payment obligation (where the settlement is reached either in or outside a litigation).	5 years after the judgement becomes final except if such period of limitation is interrupted or suspended	The legitimate interest of the Bank based on Section 6:22 of Act V of 2013 on the Civil Code.
4) Ongoing litigation	Over the entire duration of the litigation and subject to the outcome thereof, for the relevant retention period set forth in Points 1)-3) of this table	The legitimate interest of the Bank based on Section 6:22 of Act V of 2013 on the Civil Code.
5) Debt collection (recovery) to collect overdue, defaulted contractual claims of the Bank	Until the successful objection by the Data Subject, however, no later than 8 years following the year of adopting the bank's annual accounts on the year when the Bank's claim becomes due or the full contract concluded between the Bank and the Data Subject terminated.	Based on the Bank's legitimate interest in recovering its legal claim; Article 6 (1) (f) of GDPR
6) Data protection request(s) / application(s) by a Data Subject concerning the processing/protection of the Data Subject's personal data and the response(s) provided by the Bank thereto, official inquiry and response(s) provided thereto, including the information regarding the request and the response provided thereto	5 years following the date of the response letter provided to the request	The legitimate interest of the Bank based on Section 6:22 (1) of Act V of 2013 on the Civil Code.

5) Data categories processed within the course of debt collection (recovery) activity:

Data category	Non-exhaustive list of data
Data from official documents	Personal identification card, address card, passport, driving license etc. number.
Personal identification data	Customer, authorised representative, guardian, custodian, statutory representative, birth name, given name, place and date of birth, etc.
Demographic data	Citizenship
Contact details	Permanent and mailing address, telephone number, e-mail address, etc.
Legal proceeding related data	Litigious and non-litigious proceedings, public notary and enforcement proceeding
Death and inheritance related data	Acting public notary, heirs' data, estate assets, creditors of the estate, number, content of the formal transfer decision, etc.
Data of real estate provided as security	Address, location, lot number, value of the real estate
Credit data	Product type, maturity, currency, interest, credit purpose, credit line, subsidy related financial data, instalment frequency, instalments, contract number, etc.
Data affected by complaint management	Complaint, response to complaint, etc.
Debt collection data	Payment notice, telephone conversation

Further personal data processing related to claim management:

The purpose of the processing of your personal data, designation of processed data	Legal basis of the personal data processing	Duration of the personal data processing
Audio recording for quality assurance of phone conversations for the purpose of claim management	Consent provided under Article 6(1)(a) of the GDPR	Until the withdrawal of consent, and with respect of data processing in Clause IV.1) 14, until the successful objection by the Data Subject or, failing that, no later than 8 years following the year of adoption of the Bank's annual accounts on the year when the claim that expired under the contract concluded between the Bank and the Data Subject or the full claim ceased.
Back-testing of personal meet-ups for the purpose of debt management	Consent provided under Article 6(1)(a) of the GDPR	Until withdrawal of consent or, failing that, 1 (one) year from the date of audio recording
Notification address provided for debt management purposes	Consent provided under Article 6(1)(a) of the GDPR	Until withdrawal of consent or, failing that, 5 (five) year from the date of the home address

Data of the questionnaire on the data subject's current financial situation and future ability to pay in the context of a suspension of loan repayments.	Consent provided under Article 6(1)(a) of the GDPR	Until withdrawal of consent or, failing that, 5 (five) years from the completion of the questionnaire
Personal data (declarations) provided in order to obtain a payment facilitation (as a modification of the contract) or a replacement loan (so-called restart), to establish eligibility, in particular personal data relating to the Data Subject's ability to pay, financial situation, insolvency.	Consent provided under Article 6(1)(a) of the GDPR	Consent may be withdrawn pending the outcome of the assessment of payment facilitation. If a payment facilitation is granted, 8 (eight) years after the year of adoption of the annual accounts for the year of issuance of the last accounting document relating to the Contract or the Amendment to the Contract (the termination of the Contract shall also be deemed as such). (Pursuant to Section 169 (2) of the Accounting Act.) If the payment facilitation is not granted, the duration of the personal data processing shall be 5 (five) years upon the failure to enter into an Amendment to the Contract (from the date of refusal in the case of refusal) based on the legitimate interest of the Bank under Section 166/A (2), (3) of the Banking Act.
E-mail address, telephone number provided for payment facilitation (rescue package)	Consent provided under Article 6(1)(a) of the GDPR	Until withdrawal of consent or, failing that, 5 (one) year from the date of recording of the personal data

Data relating to the Data Subject's current declared financial situation, income, household in connection with the settlement of a cancelled, overdue loan/facility/negative account balance	Consent provided under Article 6(1)(a) of the GDPR	Consent may be withdrawn pending assessment of the offer. In the case of the acceptance of the offer, 8 (eight) years after the year of adoption of the annual accounts for the year of issuance of the last accounting document relating to the Contract (the termination of the Contract shall also be deemed as such). (Pursuant to Section 169 (2) of the Accounting Act.)

The electronic data contained in the litigation records of the Bank regarding the parties to the litigation and the adjudicated issue (with the exception of documents stored electronically) are not erased / anonymised in consideration of the legitimate interest of the Bank (res iudicata can be evidenced). Based on the Bank's legitimate interest, the personal data of customers with foreign currency-based contracts may be processed for an additional five years beyond the retention period specified in Act C of 2000 on Accounting. The purpose of this extended processing is to ensure the proper handling of potential legal disputes, the enforcement of legal claims, and the conclusion of related settlements.

Documents constituting ownership claim will not be erased considering that ownership claims are not subject to limitation.

If the Bank is obliged to issue personal data to a person other than the Data Subject in compliance with the Data Subject's right to Data portability, the Bank shall inform and warn such recipient third person in the scope of this Privacy Notice that the personal data issued by the Bank concerning the Data Subject shall not be used for his/her own purposes and such personal data may be only processed in compliance with the applicable data protection legislation, and observing the principle of purpose limitation. The Company does not accept liability for the third-party usage of personal data adequately transmitted to a third person at the Data Subject's request.

3.2. Specific rules regarding the processing of personal data of each Data Subjects

If you are a customer, co-debtor, payment guarantor or other natural person providing security,

- i.e. you are a natural person defined in Clauses 2.3.1 and 2.3.3 of the Privacy Notice, your personal data will be processed by the Bank as follows:

The Bank shall process the personal data of Data Subjects under this Clause as data categorised as banking secret under Section 160 (1) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings, the Banking Act, in accordance with the rules of the

Banking Act on bank secrets in addition to complying with the provisions of laws on the protection of personal data

I. Processing for the performance of a contract or actions taken at your request before entering into a contract:

The purpose of the processing of Your personal data	Legal basis of the personal data processing	Duration of the personal data processing
1. Processing is necessary for preparatory purposes concerning the conclusion of a contract with the Bank that is at the request of the Data Subject, prior to the conclusion of the contract.	Article 6 (1)(b) of GDPR, processing of personal data before the conclusion of the Contract for the purpose of concluding the Contract	In the case of a failure to conclude the Contract and if the customer due diligence has been already started under point 7 of the table, but the contract has not been concluded, for 5 (five) years from the failure to conclude the Contract based on Section 166/A (2) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings - the Banking Act, for 6 (six) months in the lack thereof. If there has been a change in the personal data of the Data Subject within this 6 (six)-month period based on a consultation with the Data Subject, we calculate this 6 (six) months period from the date of the change in the case of all changes.
2. Processing of personal data for the performance of a Contract whereto the Data Subject is a party	Article 6 (1)(b) of GDPR, processing of personal data necessary for the performance of the Contract	In case of a Contract that has been concluded, 8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of Act C of 2000 on Accounting – the "Accounting Act").
3. Pre-assessment (i.e. the preliminary assessment of the entitlement regarding the Bank's product applied for by You based on the personal data provided by You	Article 6 (1)(b) of GDPR, processing of personal data before the conclusion of the Contract for the purpose of concluding the Contract	In case of the conclusion of a Contract, 8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related

		accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of the Accounting Act. In the case of failure to conclude the Contract, till the expiry of retention period under point 1 of the table.
4. Data processing required for the performance of the Contract concluded with the Bank (including the processing of personal data in addition to the personal data set forth in Clause 5 of Chapter 3 below for the purpose of possible debt collection and also the e-mail address and telephone number personal data provided by the online personal loan application, as well as in the contracts concluded for electronic services (eg George, Elektra, SMS services), or thereafter changed with regard to the contract for these services, and the e-mail address provided or modified for the purpose of requesting or performing certain services under a contract for the provision of financial services.	Article 6 (1)(b) of GDPR, processing of personal data necessary for the performance of the Contract	8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of the Accounting Act).
5. Automated decision-making by online personal loan, credit card or bank account application	Data processing in order to take the actions under Article 6 b) and 22(2) a) of the GDPR necessary in accordance with the preamble (71) of the GDPR for the conclusion of the Contract between the Bank and the Data Subject, and for the conclusion of the Contract between the Bank and the Data Subject	Till the submission of an objection by the Data Subject under Article 22 (3) of the GDPR
6. Personal data processed in connection with booking appointments for personal, video or – in the case of premium customers – telephone consultations via the George app (the fact that an appointment has been booked, its date and time, location, information entered in the comments field, the name of	*Article 6(1)(b) of the GDPR: processing of personal data necessary for the performance of a contract*	*Eight (8) years following the year in which the annual accounts relating to the year of issue of the final accounting document in connection with the Contract (which also includes the termination of the Contract) were approved (pursuant to*

the chosen adviser, and the type of case selected)		*Section 169(2) of the Accounting Act)*
7. As part of the services provided by the George electronic channel under contract: conducting video consultations; documenting the client's statements and the content of the consultation; supporting the contract conclusion process; in the event of a contract being concluded, verifying the conclusion and content of the contract; and enforcing the associated rights and obligations. Scope of data processed: Audio and video recordings made during the video consultation (the voice and image of the adviser and the client), verbal statements made during the consultation, a screen recording of the adviser's screen, and the content of related electronic chat messages.	*Article 6(1)(b) of the GDPR – the fulfilment of the Electronic Services Contract and Data Sheet (including the General Terms and Conditions, the Digital Services Notice and the Video Consultation Service – Notice of Terms of Use), and – in the event of a contract being concluded – the preparation and performance of the individual contract concluded within the framework of the video consultancy service.*	*Eight (8) years following the year in which the annual accounts relating to the year in which the final accounting document relating to the Contract was issued (which also includes the termination of the Contract) were approved (pursuant to Section 169(2) of the Accounting Act).*

- Automated decision-making

  We inform the Data Subject that we only issue decision based on automated data processing by using Your personal data in case of online applications for personal loans and credit cards (the "automated decision-making") that is necessary for the conclusion or completion of the contract between the Data Subject and the Bank. The Bank shall not include special categories of personal data in automated decision-making. In the course of such automated decision-making, we check (as per the logic applied in the automated decision-making) Your age, income, regular income, employer, data stored in the Central Credit Information System, credit exposure, repayment behaviour regarding other credit. If the Data Subject satisfies the minimum criteria, we assess the risk involved in entering into a contract with the Data Subject, implement the risk rating of the Data Subject, the result thereof will affect the eligible credit amount or may result in the approval or the rejection of Your application.

  A decision based on data processing automated on the "green branch" is being made within the course of the application for account package, which is necessary for the conclusion or the fulfilment of the contract between the Data Subject and the Bank. There is no manual process step on the "green branch" on the side of the Bank that would require a human intervention. Each step of the application is automated, the automated decision is based on the processing of the data of the Applicant recorded thereby on the product application interface and stored in the banking systems. The online bank account process shall require an automated decision-making because it provides the benefits from rapidity. The Bank shall not include special categories of personal data in automated decision-making.

You shall have the right to request an assessment of the decision made on the basis of automated decision-making process by the Bank's experts, and to share your position as well as to submit an objection in this regard which shall be made at any contact points specified under Clause 2 of Chapter 4 of the Privacy Notice. In this case, the Bank shall examine your application and inform you thereafter.

If you do not want the decision made during the online application to apply to you, you can submit the personal loan, credit card or account package application in person at any of our bank branches in this case, and you shall be entitled to share your position or objections with the Bank.

- We inform the Data Subject that we shall be entitled to process personal data underlying the Intermediary activity as Intermediary carrying out financial, auxiliary financial / investment / auxiliary investment / insurance / payment intermediation activities in the interest, in the name and on behalf of the principals defined in Clause 5 of this Privacy Notice.
- If You have entered into a Contract with the Bank that requires the use of a telephone number (e.g. Text message service) and/or of an email address, in that case we process such personal data on the legal basis and for the duration set out in point 4 of the above table for the purpose of performing the Contract, unless You change Your relevant contact data in the form of contract amendment (whereupon the Bank shall erase/anonymise the former personal data on a final and irreversible basis).

II. Processing for the fulfilment of a legal obligation:

The purpose of the processing of Your personal data	Legal basis of the personal data processing	Duration of the personal data processing
8. Fulfilment by the Bank of customer due diligence set out in Sections 6, 7 of Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing ("AML Act"), which obligation the Bank may meet through the GIRinf0 service provided by GIRO Zrt.	Performance of a legal obligation under Section 6 and 7 of the AML Act.	8 (eight) years from the termination of the business relationship or performance of the transaction order (Sections 56, 57 of the AML Act). During the entire retention period of the Contract (i.e. 8 years following the year of adopting the annual accounts prepared for the year of issuance of the last Contract related accounting certificate (the termination of the Contract shall also be deemed as such)) (under Section 169 (2) of Act C of 2000 on Accounting - the "Accounting Act").
9. Copying documents for the full performance of the obligation to conduct customer due diligence as	Performance of a legal obligation under Section 7 (8) of the AML Act.	8 (eight) years from the date of termination of the business relationship or

set out in Sections 7 (8) of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (the AML Act)		from the date of performance of the transaction (Sections 56, 57 of the AML Act) 8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued during the entire retention period of the Contract (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of Act C of 2000 on Accounting – the "Accounting Act").
10. Data transfer to and query from the Central Credit Information System – based on a statutory obligation –	Sections 5 (2) and (7) of Act CXXII of 2011 on the Central Credit Information System (the KHR Act) – compliance with legal obligation	8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of Act C of 2000 on Accounting – the "Accounting Act").
11. Processing of personal data for risk management (loan assessment) purposes	Fulfilment of legal obligations under Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings, the "Banking Act", § 98 (1), (2), § 99 (3), Government Decree 361/2009 (XII.30.)	8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 of Act C of 2000 on Accounting – the "Accounting Act").
12. Quality control / quality assurance	Fulfilment of legal obligations under § 107 (1), (2), § 108 (5), e), i) Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings - the "Banking Act".	8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 of Act C of

		2000 on Accounting – the "Accounting Act").
13. Fraud prevention / fraud management	Fulfilment of legal obligations under § 107 d), g), § 165 (5) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings - the "Banking Act".	Within the limitation period of the claims arising of payment transaction (Section 165 (5) of the Banking Act)
14. Device information processed within the course of using the George App for fraud prevention/fraud management purposes: operating system type and version number, the security state of the device (e.g., whether the operating system has been modified through rooting or jailbreaking*), list of applications installed on the device (particularly, but not exclusively the softwares which enable remote access), and IP address used by the customer while using electronic channels (George) * Modified operation system: the state of the device when the defense of integrity is violated and becomes accessible, the state of the device is broken, on an Android device it is rooted, on an iOS device (iPhone or iPad) it is jailbroken.	Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open communication standards (SCAr.)	5 years from the date the data origination from 01.03.2022, for customers activating George's electronic channels
15. Complaint management (the complaint, the response thereupon and documentation regarding the complaint)	Fulfilment of legal obligations under § 288 (3) CCXXXVII of 2013 on Credit Institutions and Financial Undertakings - the "Banking Act".	5 (five) years upon the date of the response to the complaint under Section 288 (3) of the Banking Act
16. Audio recording for the purpose of making a declaration with legal effect (for example entering into a contract), or submitting a complaint	Section 288 (2) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings - the "Banking Act", Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MIFID 2 Directive) – compliance with legal obligation	Regarding a declaration having legal effect, if it results in entering into a contract, during the entire retention period of the contract, (that is, 8 years following the year of adopting the annual accounts prepared for the year of issuance of the last Contract related accounting certificate (the termination of the Contract shall also be deemed as such)) (under Section 169 (2) of Act C of 2000 on Accounting - the "Accounting Act").

		In case of a complaint, 5 (five) from the response made to the complaint
17. Processing of personal data classified as special category personal data if such personal data are actually used but in any event for the duration of such use.	Upon Your consent provided under Section 9 (2) a) of the GDPR or a legislative authorisation provided under Article 9 (2)(b)-(j) of the GDPR	Till the fulfilment of the data processing purpose / withdrawal of the consent. In the case of biometric signature, 8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of Act C of 2000 on Accounting – the "Accounting Act").
18. Disclosure of connections in the United States of America / CRS member states	Act XIX of 2014 on the Promulgation of the Agreement between the Government of Hungary and the Government of the United States of America to Improve International Tax Compliance (FATCA), Act CXC of 2015 on the Promulgation of the Multilateral Agreement between the Competent Authorities on the Automatic Exchange of Financial Account Information and Act XXXVII of 2013 on Certain Rules of International Public Administration Cooperation Related to Taxes and Other Public Duties	10 years from the date of termination of the legal obligation to provide the required data under Section 3/D (5) of Act XXXVII of 2013
19. Personal data of the beneficial owner	Fulfilment of customer due diligence set out in Sections 8, 9 of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (the "AML Act")	8 (eight) years following the termination of the business relationship or the execution of the transaction order (Sections 56 and 57 of the AML Act)
20. Receipt, management of whistle-blowing complaint, operation of the whistle-blowing system	Act XXV of 2023 on Complaints and Notifications of Public Interest and on the Rules for Reporting Abuses, § 18, § 26	If a public interest disclosure proves to be unfounded or no further measure is necessary, the Bank shall erase the data of the investigation within 60 (sixty) days of such disclosure made If a measure is applied further to the

		investigation, also including measures related to legal proceedings or disciplinary measures against whistle-blowers, the Bank will process data related to the disclosure until the final closing of the proceedings launched on grounds of the relevant disclosure, at the latest.
21. Processing of data for the purpose of preventing market abuses upon legislative authorization	Article 11 (5) d) of the 596/2014 MAR (Regulation on Market Abuses), Article 4 (1) a of EU Regulation 2016/960 on market sounding activities, Article 18, 19 (5) of the MAR	5 (five) years – Article 11 (8), 18 (5), 28 of the MAR
22. Other customer due diligence measures (data on business relationships, management of changes to data, data updates) and monitoring of customer relationships	Fulfilment of the obligation to conduct customer due diligence set out in Sections 10, 11 and 12 of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (the "AML Act") and Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings the "Banking Act" § 107	8 (eight) years from the termination of the business relationship or performance of the order for the transaction (Sections 56, 57 of the AML Act). During the entire retention period of the Contract (i.e. 8 years following the year of adopting the annual accounts prepared for the year of issuance of the last Contract related accounting certificate (the termination of the Contract shall also be deemed as such)) (under Section 169 (2) the Accounting Act).
23. Customer due diligence (checking the source of funds and assets)	Fulfilment of the legal obligation due diligence set out in Sections 9/A 16 (3) and 16/A of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing/A")	8 (eight) years upon the termination of the business relationship, and the completion of the transaction order (Section 56 and 57 of the AML Act)
24. Customer due diligence (checking the politically exposed person status)	Fulfilment of the legal obligation set out in Section 9/A of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing ("AML Act")	8 (eight) years upon the termination of the business relationship, and the completion of the transaction order (Section 56 and 57 of the AML Act)
25. While using the electronic banking sites accessible to customers as users (e.g. Erste	Fulfilment of legal obligations pursuant to Section 3 (1) c), d) and f) of Government	In respect of customers using the electronic channel, for 5 years from

Retail/Corporate NetBank, Erste Retail/Corporate MobileBank, George Web and George App, Erste Electra System, API), the IP address and the electronic site identifier used by the customer are processed for the purpose of serving requests from public authorities.	Decree No. 42/2015 (12.III.) under § 67 (1)/A (1) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings - the "Banking Act".	the date the data was generated.
26. Queries related to the Central Credit Information System ("KHR") [Data listed in Section 5(7)(b) of Act CXXII of 2011 on the Central Credit Information System (the "KHR Act"), in particular identification data; so-called negative information (e.g. data on late payments, defaults, fraud, abuse)] and data transfer - based on a legal obligation -	Article 6(1)(c) of the GDPR, fulfilment of a legal obligation: relevant provisions of Act CXXII of 2011 on the Central Credit Information System (the "KHR Act") (in particular: §§ 5-6; §§ 11-13)	8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of Act C of 2000 on Accounting – the "Accounting Act").
27. Erste Group Bank AG (registered seat: Am Belvedere 1. A-1100 Vienna) as a member with a controlling interest in the Data Controller for the purpose of exercising certain rights of Erste Group Bank AG in relation to its controlling interest, for the purpose of fulfilling the reporting obligations of the Bank to Erste Group Bank AG (the Bank's parent company), for the purpose of requesting a decision or for the purpose of providing follow-up information	Fulfilment of legal obligations under § 164 (3) (e) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings - the "Banking Act".)	8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of Act C of 2000 on Accounting – the "Accounting Act").
28. From 1 July 2025, the transfer to the Central Abuse Filtering System (GIRO Zrt.) of the data specified in § 55/D of Act LXXXV of 2009 on the Provision of Payment Services (Pft.) and in Annex 2 (e.g.: type of payment transaction, amount, amount of payment request, currency, content of message, identifier of cash substitute payment instrument, location identifier)	GDPR Article 6 (1) (c), legal obligation: pursuant to Act LXXXV of 2009 on the Provision of Payment Services (Payment Services Act), § 55/D.	8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of Act C of 2000 on Accounting – the "Accounting Act").

Processing of special categories of personal data

Under Article 9 of the GDPR, we process special categories of personal data (that is, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation only if the Data Subject has given explicit consent to the processing of such special categories of personal data for one or more specific purpose(s), unless EU or Member State legislation excludes data processing based on consent and except if any legal basis for the processing of special categories of personal data set forth in Article 6 (b)-(j) exist on our side. We process Your special category personal data (even in case of Your consent) solely for the purpose of data processing You have consented to and only as long as such purpose exists. We process Your biometric signature for the purpose of ensuring the electronic signature of documents that may be signed electronically, and the handover of documents in electronic form, and the authentic identification of the signatory person using the electronic signature facility. In the case of processing a biometric signature as personal data, we process Your biometric signature for 8 years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of the Accounting Act.

The Customer may withdraw its consent to the register of the biometric data by the Bank at any time within the biometric signature process. If the Customer withdraw the consent, it shall not concern the lawfulness of the earlier data processing, so the contracts concluded, declaration made so shall remain valid and effective even after the withdrawal, those are available for the Customer until the Erste electronic channels contract concluded with the Bank remains in force. We process the Customer's biometric data / biometric signature within the retention period of the Electronic documents, set out in the legislation and in the Privacy Notice of the Bank, linked to the document, we do not use it for other purposes after the withdrawal of the consent.

The Data Controller have made an impact assessment before the commencement of the processing of biometric signature to see how the data processing affects the protection of personal data and have also assessed the risks of data processing related to the rights and freedoms of the data subjects. Based on the assessment, it can be concluded that the existing risks and the chances of possible abuses are very low, considering that the Data Controller ensures the protection of bank secrecy and personal data by applying the necessary technical and organizational measures in accordance with data security and information security regulations.

In consideration of the above, we request You not to provide the Bank with special category personal data without providing Your consent to the Bank for the processing thereof (where such consent shall also contain the purpose in respect of which You authorise the Bank to process data) because, in lack of Your explicit consent containing the purpose of data processing as well, the Bank will not have the right to access and thus to apply such personal data by the adoption of its decisions. We shall immediately erase /anonymise such personal data without reading if we establish that You have not provided Your consent to the Bank to the processing of Your special category personal data.

Device information processed within the course of using the George App for fraud prevention/fraud management purposes: operating system type and version number, the security state of the device (e.g., whether the operating system has been modified through rooting or jailbreaking*), list of applications installed on the device (particularly, but not exclusively the softwares which enable remote access), and IP address used by the customer while using electronic channels (George)

The data processing is based on the legal requirements of the Payment Services Act and SCAr., the purpose of which is to prevent and investigate fraud. Data related to the Bank and the customer are stored for 8 years, while data related to transactions, use of instruments and data generated by the Bank (scoring) are stored for 1 year.

The Bank uses transaction monitoring mechanisms to detect payment fraud, which are capable of monitoring payment transactions and certain non-payment transactions (e.g. Netbank login) in real time, while they are being executed, via remote channels. Due to the acceleration of digital services, fraudulent use can be effectively detected and prevented by automated monitoring and decisions (automated decision making), which may result in the rejection of the payment transaction. The Data Subject has the right to object to automated decision-making.

Furthermore, in order to filter out payment transactions that were not approved by clients or were approved through deception, it is necessary to establish customer profiles. This means collecting customer-related information such as the typical geographic location of the usage (IP address, geolocation data), typical characteristics of previous payments, software data of the user's devices, etc.

Our Bank also uses supervised machine learning models to risk assess the complex data (customer profiles, fraud patterns) available during transaction monitoring.

Data transfer to the Central Abuse Filtering System (GIRO Zrt.)

As of July 1, 2025, the Bank will transfer to GIRO Zrt. the data specified in Act LXXXV of 2009 on the provision of payment services, relating to HUF payment orders to be processed, settled, and executed in the payment system, as well as foreign currency and cross-border transfer orders submitted to the Bank, and HUF and foreign currency transfer orders between the Bank's own clients, for the purpose of supporting the detection and prevention of fraud related to payment transactions.

III. Processing based on legitimate interest:

The purpose of the processing of Your personal data	Legal basis of the personal data processing	Duration of the personal data processing
29. Performance of monitoring mandatory for banks with respect of data categories in addition to the ones set out in Section 10 of Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing ("AML Act"), which obligation the Bank may meet through the GIRinf0 service provided by GIRO Zrt.	Legitimate interest of the Data Controller under Article 6(1)(f) of the GDPR	Until a successful objection by the Data Subject, or, failing this, until the Bank's legitimate interest persists, i.e. for 8 (eight) years from the termination of the business relationship or the execution of the transaction order in accordance with the provisions of § 56 and 57 of the AML Act.
30. Processing of personal data for claims management purposes e-mail, telephone number, voice recording / Processing of telephone numbers for quality assurance purposes related to claims management	Upon the legitimate interest of the Bank in the recovery of legitimate claims; Article 6 (1)(f) of GDPR	5 years from the cessation of any overdue claim outstanding under the contract between the Bank and the Data Subject or the entire claim. If the Bank assigns the claim, then, with regard to the provisions of Article 6:22

		(1) of Act V of 2013 on the Civil Code, 5 (five) years from the date of assignment.
31. Profiling for direct marketing purposes	Legitimate interest of the Data Controller under Article 6(1)(f) of the GDPR	Successful objection by the Data Subject, in the lack thereof, till the Bank has a legitimate interest
32. Market research activities (see Section X, point 58) Selection and contact of customers for the purpose of preparing such activities (data processed: contact details, access to the George Web/App depending on the subject of the market research, product data, usage habits).	Pursuant to Article 6(1)(f) of the GDPR, the Bank's legitimate interest is: to identify respondents who can provide the most relevant answers.	Until a successful objection by the data subject, or, in the absence thereof, until the Bank's legitimate interest ceases to exist.
33. Processing of telephone number personal data for the purpose of compiling a contact list, marketing list	Legitimate interest of the Data Controller under Article 6(1)(f) of the GDPR	Successful objection by the Data Subject, in the lack thereof, till the Bank has a legitimate interest
34. The processing of video recordings captured by the video surveillance system installed on the premises of Erste Bank Hungary Zrt. is carried out for the purposes of ensuring the uninterrupted provision of the Bank's services, protecting human life, physical integrity and personal freedom, as well as business, banking and securities secrets, preventing acts against property, and reconstructing security incidents.	Pursuant to Article 6(1)(f) of the GDPR, the Data Controller's legitimate interest is: the Bank's interest in ensuring the uninterrupted provision of the services it offers, and in protecting human life, physical integrity, personal freedom, business, banking and securities secrets, and property.	50 (fifty) days from the date of recording, unless (i) the recording is used in ongoing administrative, judicial or internal proceedings – in which case until the proceedings are finally concluded – or (ii) the data subject exercises their right to restrict data processing – in which case, until the restriction remains in force.
35. Smooth acquisition of business customers of Commerzbank Zrt., including joint solicitation of business customers	Legitimate interest of the Data Controller under Article 6(1)(f) of the GDPR.	Until a successful objection by a Data Subject, in the absence thereof, until the existence of a legitimate interest of

by the Bank and Commerzbank Zrt.		the Bank, ie at the latest until the conclusion of a contract with business customers or the completion of the portfolio transfer.
36. Analysis of voice records for the below purposes: (i) improvement of the quality of Erste services (ii) review of the Erste services quality (iii) complaint prevention (iv) decreasing the number of incoming calls (v) increasing the customer satisfaction as regards the Erste services (vi) customer retention (vii) customer education	Legitimate interest of the Data Controller under Article 6(1)(f) of the GDPR	Voice record being subject to analysis: 93 days Data and results of the analysis: 455 days
37. Displaying George Tips for financial education on George App	Pursuant to Article 6(1)(f) of the GDPR, the Data Controller has a legitimate interest in ensuring that customers' financial awareness	Until a successful objection by a Data Subject, in the absence thereof, until the existence of the contract for internet banking and mobile application services, i.e. the legitimate interest of the Bank. Each George Tip is deleted after 35 days.
38. Displaying materials that enhance financial awareness in the Fit section of George App for the purpose of financial education.	Pursuant to Article 6(1)(f) of the GDPR, the Data Controller has a legitimate interest in ensuring that customers' financial awareness	Until a successful objection by a Data Subject, in the absence thereof, until the existence of the contract for internet banking and mobile application services, i.e. the legitimate interest of the Bank.
39. Display travel-related features in the Travel Hub function of George App for customer satisfaction and educational purposes, and display a currency converter calculator using the National Bank of Hungary exchange rate.	Legitimate interest of the Data Controller under Article 6(1)(f) of the GDPR	Until a successful objection by a Data Subject, in the absence thereof, until the existence of the contract for internet banking and mobile application services, i.e. the legitimate interest of the Bank.

40. During the automated processing of HUF transfer orders submitted in paper form at the branch network, the order provided by the Customer is first digitised (scanned). Subsequently, the data indicated on the order (name, bank account number, transaction details) are automatically extracted by a closed system using artificial intelligence, both during the training of the system and its subsequent operation. Thereafter, the transfer order is processed in accordance with the traditional procedures and control mechanisms.	Legitimate interest of the Data Controller under Article 6(1)(f) of the GDPR	The data are deleted from the artificial intelligence system immediately after processing, but no later than within 5 days. In the event of a successful objection by the Data Subject, the data are deleted from the artificial intelligence system following receipt of the objection
41. Email notifications regarding the status of the requested appraisal service	Pursuant to Article 6(1)(f) of the GDPR, the Data Controller's legitimate interest, which is linked to ensuring the transparency of the appraisal process	Until a successful objection by the data subject, or, in the absence thereof, until the Bank's legitimate interest ceases to exist, for a period of 8 (eight) years from the termination of the business relationship or the fulfillment of the assignment
42. Generation of device- and session-level risk scores by the ThreatMark fraud prevention system for the purpose of risk-based, real-time assessment of electronic payment transactions. As part of its data processing activities, the Bank records the following data whilst you are using your mobile banking app: • user ID (pseudonym), • GPS coordinates, • keystroke dynamics, • browser events (blur, focus, movement), • device information (device model, operating system, manufacturer, unique device identifiers), • malware signatures, • a list of mobile applications running on the device (in hashed form), • IP address,	This is in the legitimate interests of the Data Controller and the data subject, pursuant to Article 6(1)(f) of the GDPR. The Data Controller's legitimate interest: preventing electronic payment fraud and protecting customers' funds and access to their bank accounts. The data subject's legitimate interest: protecting their own assets, access to their bank accounts and personal data against unauthorised transactions. A balancing test has been carried out.	The retention periods for each data category are as follows: • user ID: 3 months • device information: 6 months • list of mobile applications: 1 month • IP address: 6 months • GPS coordinates: 2 weeks • source URL for logging into online banking: no retention, real-time processing only • malware signatures: no retention, real-time processing only • keystroke dynamics: 2 weeks

• the source URL used to access the online banking service. The Bank's aim is to protect your funds and access to your banking services against payment fraud and unauthorised access.		• browser events (blur, focus, movement): 2 weeks **Right to object:** You have the right to object to the processing of your data pursuant to Article 21(1) of the GDPR. The Bank will examine your objection on a case-by-case basis and notify you of the outcome within 30 days. The Bank may continue to process your data despite your objection if it demonstrates that there are compelling legitimate grounds for doing so which take precedence over your interests, rights and freedoms. In relation to this data processing, such compelling legitimate grounds include, in particular: (i) due to the operational logic of the ThreatMark fraud prevention system, which is based on aggregated data samples at device and session level, the exclusion of a single data subject would directly jeopardise the accuracy of the system as a whole and, consequently, the protection of the funds of other customers who have not lodged an objection; (ii) in the absence of device information, real-time fraud prevention is not comprehensive, which breaches the Bank's statutory obligations [PSD2, EBA RTS 2018/389];

		(iii) data processing is based on pseudonymous user identifiers and device fingerprints; it does not involve the processing of data linked to a directly identified natural person, and therefore the impact on the data subject's privacy is moderate.
43. Credit card application forms completed in paper format at external sales locations, together with the documents and identification papers related to the application, are scanned. Subsequently, the data provided (basic personal identification data, demographic data, identification document data, contact details, customer declarations, basic transaction data; HR data; credit data, including basic loan application data, repayment data, disbursement data, credit assessment data, and income data; company data; and account-related data, including basic bank account information) are automatically extracted by a closed system that also uses artificial intelligence (both during the training of the system and its subsequent operation). Thereafter, the credit card application is processed in accordance with the standard processes and controls.	Legitimate interest of the Data Controller under Article 6(1)(f) of the GDPR	The data are deleted from the artificial intelligence system immediately after processing, but no later than within 5 days. In the event of a successful objection by the Data Subject, the data are deleted from the artificial intelligence system following receipt of the objection
44. When recording or updating a customer's personal data within the branch network, it is necessary, for identification purposes, to photograph and store the customer's identification documents. The data contained in these documents (name; birth name; mother's birth name; place of birth; date of birth; nationality; gender; identification document number for domestic individuals – identity card/passport/driving licence, address card; expiry date of the identification document; permanent address) are automatically captured,	Legitimate interest of the Data Controller under Article 6(1)(f) of the GDPR	The data are deleted from the artificial intelligence system immediately after processing, but no later than within 5 days. In the event of a successful objection by the Data Subject, the data are deleted from the artificial intelligence system following receipt of the objection

evaluated, and processed by a closed system that also uses artificial intelligence (both during the training of the system and its subsequent operation). The extracted data are then recorded in the bank's systems in accordance with the standard operating procedures otherwise applied by the bank.		

- We inform the Data Subjects entering our registered seat, premises and branches and those using our ATMs that a **continuous image recording is being applied at our registered seat, premises, branches and ATMs** for the protection of human life, physical integrity, personal freedom, business, banking- and securities secrets as well as for personal and property security purposes upon our legitimate interests concerning personal, property and banking security. We process such image recording in accordance with the governing legislative provisions and our relevant policy on physical security.
- **Profiling**
  The Bank may carry out profiling for direct marketing purposes on the basis of its legitimate interest for direct marketing under point (47) of the Preamble of the GDPR (for the compilation of a target group of recipients to be contacted for marketing purposes).

- Further information on data processing related to the use of the **IT system that credit institutions and insurers have in place for the registration of housing insurance and the provision of security in the form of credit protection** (the so-called DLT system for the registration of housing insurance, which provides IT support for the business process of registration of housing insurance and the provision of security in the form of credit protection using shared ledger[1] technology) is available **here**.
- **Direct marketing**
  The Bank may contact a Data Subject in accordance with Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing, upon the conditions set forth therein, either itself or via its authorised representative for the purpose of research or direct marketing. For this purpose, the Bank may contact natural persons at their telephone numbers listed in public telephone directory databases, not marked as restricted. The Data Subject of such contact may object to such contacts. We keep records of the persons who objected to be further contacted by the Bank for such purpose or its authorised representative.

- **The Data Controller shall perform an analysis of the voice records based on speech and data analysis, including a profiling of the bank administrator**, by using a comprehensive performance and quality management system. The application shall analyse customer service conversations, shall recognize the words spoken, and other factors

[1] Distributed database technology in which data modification transactions, data and program code providing the business logic are stored redundantly between operator nodes. The block-chain component of the technology ensures data integrity protection.

that may affect the quality of customer service and the performance of the administrator.

As part of the analysis, the system shall perform objective measurements related to the call (measuring, for example, the length of the call, the percentage of speech by the administrator and the customer, the percentage of silence or words spoken at a given time, and the number of certain predefined words), whereupon it shall calculate averages, shall compile statistics to monitor, improve, and evaluate the efficiency (performance) of the administrator. A textual description shall be made about the sound material; this shall make it possible to search for specific words, which is suitable, for example, for checking the provision or appropriate quality of mandatory information (quality assurance, education).

Based on the above data, the bank staff in charge shall perform sortings (for example, for calls that are significantly different from the average or that contain certain words, such as "complaint") by the system and shall listen again all or part of the calls collected, controlling thereby the performance of the administrator or the proper handling of requests and questions from the customer. The verification shall require the recording of call statistics (call date, customer ID).

Sound analysis software has no self-learning capability. It is a pre-parameterized system, ie. it is able to complete a more reliable search and to display the search results based on the criteria (parameters) specified by Erste. The system shall not make an automated decision, it shall analyse the calls as specified above and organize them into groups according to the set parameters.

The above operation of the system shall allow Erste to analyse the data for the full range of incoming calls and primarily on the basis of objective criteria. (Without this, verification and analysis would only be possible by listening back to randomly selected calls, which would drastically reduce the possibility of error detection.)

The purpose of data processing shall be to ensure an adequate and effective control of the quality of Erste's services (primarily telephone customer service) (to ensure service quality) and a further improvement thereof for a strengthened efficiency and customer satisfaction (which facilitates customer retention as well) and to prevent possible internal abuse. Within these goals, the analyses shall also focus on the prevention of complaints, the reduction of the number of calls, customer education and related process improvements.

In view of the above and as a result of the balance of interests carried out by the Data Controller, Article 6 (1) (f) GDPR, the Data Controller's legitimate interest in data processing shall provide legal basis for data processing. The personal data processed during this data processing are: date of call, customer ID (telephone number or banking customer number), basic type of call: incoming or outgoing call, text description of audio material, length of call, productivity data: the percentage of customer's speech, silence and conversation on each other as well as other non-classifiable time, the rate of words number per minute. Erste shall not process or analyse health data (eg emotional or mental state) during voice analysis.

The retention period for audio material suitable for analysis shall be 93 days, and the retention period for additional personal data listed above shall be 455 days.

The audio materials and results shall be stored and analysed on Erste's own device, which can only be accessed by authorized employees of Erste or data processors.

Data processors involved in data processing:

Data processor	Contact details	Activities
eSense Human Resources Szolgáltatñ Nyrt.	1138 Budapest, Madarász Viktor u. 47-49, Building 1 (06 1) 555 1585	We provide temporary employees employed by eSense with access to the calls they analyse and the related analysis and data.
Xdroid Kft.	1031 Budapest, Záhony u. 7- Building C Floor 2 (06 1) 240 4867	Software maintenance, updates and bug fixes

The Data Subject shall be entitled for objection in connection with the data processing. An objection against voice analysis may be shared during the call with the administrator managing the call, and an objection may also be submitted afterwards in manners listed in point C) of II.2.

In the event of an objection or request for deletion (exercise of the "right to be forgotten"), the voice recording and the analysis results stored in the sound analysis system shall be deleted by Erste.

Erste shall ensure the access to the results of the voice analysis (request for a copy) upon a request at one of the contact points listed in paragraph II.2) C).

In case of a notification for data correction or a comment, Erste shall record the relevant information in the voice analysis system, depending on the outcome of the investigation.

In case of an objection or a request for access, correction or deletion, please provide the call identification data for ensuring traceability (date of call, customer's telephone number, TeleBank ID in case of identified call).

Data Subjects shall not be entitled to the "right of data portability" defined in Article 20 of the GDPR in the context of this data processing.

- **Detailed rules on video surveillance at Erste Bank Hungary Zrt. premises**

  Scope of data subjects

  Persons entering or present at the Bank's head office, premises or branches (hereinafter referred to as the 'monitored area'). The Bank collects personal data directly from the data subject.

  Scope of data processed

The image of the data subject entering the monitored area, their activities visible in the recording (e.g. movement), and the location and time of the recording.

Purpose of processing personal data

The recording and storage of video footage is carried out to ensure the uninterrupted provision of the services offered by the Bank, to prevent acts against human life, physical integrity, personal liberty or property, and to prevent breaches of business, banking and securities secrecy, as well as to reconstruct security incidents occurring in connection with the above.

Technical and organisational measures

Access to the video recordings is restricted solely to authorised persons designated by the Bank for this purpose. The Bank implements appropriate technical and organisational measures to ensure the security of personal data in accordance with Article 32 of the GDPR.

Legal basis for the processing of personal data

The legal basis for the processing of video footage is the Bank's legitimate interest, as set out in Article 6(1)(f) of the GDPR: the Bank's interest in ensuring the uninterrupted provision of the services it offers, and in protecting human life, physical integrity, personal freedom, as well as business, banking and securities secrets, and property.

Duration of personal data processing

In the absence of any use, **50 (fifty) days** from the date of recording of the video footage.

Data processors

The Bank engages data processors to operate the video surveillance system; these data processors carry out security maintenance, fault-finding and manned security duties. The data processors may access personal data solely within the framework of the data processing agreement concluded with the Bank and in accordance with the Bank's instructions.

The data processors engaged are: **Name of data processor**	**Registered office**	**Company registration number**	**Activity**
Criterion Security Technology Ltd.	51/b Teve Street, 1139 Budapest	01-10-041569	Security technology maintenance and repair
Criterion Security Solutions Ltd.	51/b Teve Street, 1139 Budapest	01-09-422007	Manned guarding services

Data transfer

Data transfer to third countries

The Bank does not transfer the data subject's personal data to a third country (outside the European Economic Area) or to an international organisation.

Data transfer to public authorities

The Bank may be required by law to hand over video footage to the relevant authority (in particular the police, the public prosecutor's

office or the courts) in the context of a criminal investigation, court proceedings or other official proceedings. In such cases, the legal basis for the data transfer is Article 6(1)(c) of the GDPR (compliance with a legal obligation).

Rights of data subjects and submission of requests

A data subject appearing in video footage may request access to their personal data, the erasure of such data, **the restriction of data processing** – including where the data subject requests restriction rather than erasure for the purpose of asserting legal claims – and **may object to the processing of their data**.

Further information on data subjects' rights can be found in the chapter entitled 'My rights in relation to Erste's data processing' in the Bank's Data Protection Notice.

IV. Processing based on Data Subjects' consent:

The purpose of the processing of Your personal data	Legal basis of the personal data processing	Duration of the personal data processing
45. Data transfer to the Central Credit Information System – based on the consent of the Data Subject	Article 6 (1)(a) of GDPR, consent of the Data Subject	5 years from the start of the retention period under Sections 8 (2) of Act CXXII of 2011 on the Central Credit Information System (the "KHR Act")
46. For the purpose of sending direct marketing (advertising) inquiry on behalf of the Bank and its Subsidiaries, sending an offer on behalf of the Bank Depending on the content of the consent, through the following channels or any of them: Postal letter, Electronic mail, Telephone, SMS, Online platforms (online banking, mobile app services, push notifications, websites used for advertising)	Article 6 (1)(a) of GDPR, consent of the Data Subject	Till the fulfilment of the data processing purpose / till the withdrawal of the consent, in the lack thereof, during the whole retention period of the Contract,(i.e. 8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued - the termination of the Contract shall also be deemed as such - under Section 169 (2) of Act C of 2000 on Accounting - the "Accounting Act"
47. Processing of contact details regarding the person interested in the service (e-mail address, telephone number, facebook username, viber username) (except for the e-mail address and telephone number personal data provided by the online personal loan application, as well as in the contracts concluded for electronic services (eg Netbank,	Article 6 (1)(a) of GDPR, consent of the Data Subject	Till the fulfilment of the data processing purpose / till the withdrawal of the consent, in the lack thereof if a Contract has been entered into, during the whole retention period of the Contract, (i.e. 8 (eight) years following the year of adopting the annual accounts prepared

Elektra, SMS services), or thereafter changed with regard to the contract for these services)		for the year when the last Contract related accounting certificate has been issued - the termination of the Contract shall also be deemed as such - under Section 169 (2) of Act C of 2000 on Accounting - the "Accounting Act". If the Contract has not been concluded within 6 (six) months upon the commencement of the personal data processing (except for the case, if there is a change in the data within the 6 (six) months), if there has not been concluded a Contract with the Data Subject. If there has been a change in the personal data of the Data Subject within this 6 (six) months period upon consultation with the Data Subject, we calculate this 6 (six) months period from the date of amendment in case of all changes. If the Contract has not been concluded, the duration of the personal data processing shall be 5 (five) years upon the failure of the conclusion of a Contract (from the date of refusal in case of refusal) based in the legitimate interest of the Bank upon the Section 166/A (2), (3) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings - the "Banking Act".
48. Verification of the authenticity of documents/instruments related to the application/Contract and the verification by the Bank of the fulfilment of the obligation specified in the Contract through the GIRinfO service provided by GIRO Zrt.	Article 6 (1)(a) of GDPR, consent of the Data Subject	Till the fulfilment of the data processing purpose / till the withdrawal of the consent, in the lack thereof if a Contract has been entered into, during the whole retention period of the Contract, (i.e. 8 (eight) years following

		the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued - the termination of the Contract shall also be deemed as such - under Section 169 (2) of Act C of 2000 on Accounting - the "Accounting Act". If the Contract has not been concluded within 6 (six) months upon the commencement of the personal data processing (except for the case, if there is a change in the data within the 6 (six) months), if there has not been concluded a Contract with the Data Subject. If there has been a change in the personal data of the Data Subject within this 6 (six)-month period upon an alignment with the Data Subject, we calculate this 6 (six) months period from the date of amendment in case of all changes. If the Contract has not been concluded, the duration of the personal data processing shall be 5 (five) years upon the failure of the conclusion of a Contract (from the date of refusal in case of refusal) based in the legitimate interest of the Bank upon the Section 166/A (2), (3) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings - the "Banking Act".
49. Processing of personal data classified as special category personal data if such personal data are actually used but in any event for the duration of such use.	Upon Your consent provided under Section 9 (2) a) of the GDPR or an legislative authorisation provided under Section 9 (2) b)-j) of the GDPR	Till the fulfilment of the data processing purpose / withdrawal of the consent. In case of biometric signature, 8 (eight) years following the year of adopting the

		annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of Act C of 2000 on Accounting – the "Accounting Act").
50. Data transfer outside an EEA member state (if used by the Bank) and this fact specifically appears in this Privacy Notice.	Consent given by the Data Subject under Article 6 (1)(a) of the GDPR or the conclusion of an agreement for data processing under Article 45(1), 46(1) of the GDPR and under Article 28 of the GDPR in case of a data processor.	Regarding a consent based data transfer, until the fulfilment of the data processing purpose / the withdrawal of the consent provided by the Data Subject, or, in other cases, as long as the conditions set forth in Article 45 (1) / Article 46 (1) of the GDPR exist / until the termination of the data processing agreement, whichever occurs first
51. Automated decision-making in case of individual case(s) (with the exception of the online personal loan, credit card or bank account applications)	Upon the legal basis of Article 22(2)(c) of the GDPR (explicit consent of the Data Subject)	Till the fulfilment of the data processing purpose / till the withdrawal of the Data Subject's consent, but no longer than till the end of the full retention period of the Contract
52. Audio recording for other purposes (audio recording other than for complaint management purposes in point 14 and for claims management purposes in point 27 of the table)	On the legal basis of Article 22 (2)(c) of the GDPR (explicit consent of the Data Subject)	The full duration of the Contract
53. Image and voice recording (video recording) for direct electronic customer due diligence purpose	Data Subject's consent (under of Section 17(4) a) and 18(1) of the MNB Decree No. 26/2020 (VIII. 25.))	Regarding a declaration having legal effect, if it results in contracting, during the entire retention period of the contract, (that is, 8 years following the year of adopting the annual accounts prepared for the year of issuance of the last Contract related accounting certificate (the termination of the Contract shall also be deemed as such)) (under Section 169 (2) of Act C of 2000 on Accounting - the "Accounting Act").

54. Processing of personal data like name, e-mail, telephone number provided within the course of the online booking, for the data processing period of this purpose	Consent provided under point a. of Article 6(1) of the GDPR	Till the fulfilment of the data processing purpose / withdrawal of the consent
55. Development of personalized offers via the George App for participants of the Moneyback Benefit program	Consent provided under point a. of Article 6(1) of the GDPR	Until the withdrawal of the consent or till the deactivation of the Benefit Program, Erste shall retain them for 5 years from the withdrawal of the consent under this chapter or the deactivation of the Benefit Program based on its own legitimate interest.
56. Audio recording when using the Live Assist service available on the George App and George Web, or image recording in the event of an error message to troubleshoot/investigate the error	Consent provided under point a. of Article 6(1) of the GDPR	5 years after the date of service provision
57. Direct contact with the employer of the loan applicant - by phone/email - for the purpose of verifying the content of documents related to the loan applicant's employment and income (e.g., loan application, employer's certificate, bank statement) and obtaining further information (e.g., amount and composition of salary; incapacity for work; duration and nature of employment). Processed personal data: information necessary for asking questions, employer identification and contact details.	Consent provided under point a. of Article 6(1) of the GDPR	Till the fulfilment of the data processing purpose / till the withdrawal of the consent. Thereafter, the retention of data: if a Contract has been entered into, during the whole retention period of the Contract, (i.e. 8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued - the termination of the Contract shall also be deemed as such - under Section 169 (2) of Act C of 2000 on Accounting - the "Accounting Act". If the Contract has not been concluded within 6 (six) months upon the commencement of the personal data processing (except for the case, if there is a change in the data within the 6 (six) months), if there has not been concluded a Contract with the Data Subject. If there has been a change in the personal data of the

		25 Data Subject within this 6 (six) months period upon consultation with the Data Subject, we calculate this 6 (six) months period from the date of amendment in case of all changes. If the Contract has not been concluded, the duration of the personal data processing shall be 5 (five) years upon the failure of the conclusion of a Contract (from the date of refusal in case of refusal) based in the legitimate interest of the Bank upon the Section 166/A (2), (3) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings - the "Banking Act".
58.Transmission of identifier data to external digital platforms (Google*, Meta*, Adform***) for the purpose of displaying personalized content in marketing campaigns run by the Bank. For Google and Meta, the transmitted identifier is the email address; for Adform, it is a unique identifier. Consent for data transmission is managed separately by the Bank for each channel. Google*: By transmitting the email address, the user may see personalized advertisements across various Google services, such as Google Search, YouTube, and the Google Display Network. Meta** (Facebook and Instagram): By transmitting the email address, the user may see personalized advertisements on the Facebook and Instagram platforms. Adform***: By transmitting identifiers created specifically for this purpose, the user may see	Article 6 (1)(a) of GDPR, consent of the Data Subject	Until the purpose of data processing is fulfilled or until consent is withdrawn. In the absence of such withdrawal, until the termination of the contractual relationship.

personalized advertisements across advertising networks managed by Adform. This means Erste Bank ads may appear on various websites and applications based on the user's interests, as part of the Adform advertising network.		
59. Use of browsing data to provide personalized financial offers. When the advertising cookie setting is enabled during a visit to erstebank.hu, browsing data collected on the Bank's websites and advertising platforms (such as visited pages and time spent on them) may be linked to banking customer data (e.g. banking activities, services mediated by the Bank, demographic data, etc.) after logging in through an identified channel (e.g. George Web).	Article 6 (1)(a) of GDPR, consent of the Data Subject	Until the purpose of data processing is fulfilled or until consent is withdrawn. In the absence of such withdrawal, until the termination of the contractual relationship.
60. Use geolocation data to display the National Bank of Hungary exchange rate of the currency corresponding to your location in the Travel Hub function of George App.	Article 6 (1)(a) of GDPR, consent of the Data Subject	Until the purpose of data processing is fulfilled or until consent is withdrawn. In the absence of such withdrawal, until the termination of the contractual relationship.
61. When activating the Click to Pay service, the email address, telephone number, mailing address provided for contact purposes, and credit card details (credit card number, CVC code, expiration date) will be processed and transferred to Visa Inc. which latter ensures technical compliance.	Article 6 (1)(a) of GDPR, consent of the Data Subject	Until consent is withdrawn, or in the absence of such withdrawal, until the termination of the contractual relationship.
62. Market research activities (measuring customer satisfaction, assessing efficiency, preference surveys, testing): measuring and increasing customer satisfaction, developing new and existing products/services, and managing and analyzing customer names, contact information, and results obtained during market research activities for the purpose of increasing efficiency. In the case of certain market research	Consent pursuant to Article 6(1)(a) of the GDPR	Until consent is withdrawn, or for 5 years in the absence of such withdrawal. Unless the wording of the consent specifies a different retention period.

activities, processing of audio/video recordings.		
63. **Display Name** – the abbreviated name (nickname) provided by the user, processed in order to ensure that the form of address used in correspondence, messages, the app and our other electronic communication channels is personalised and easy to read, particularly in the case of long official names or personal names containing name suffixes.	Consent pursuant to Article 6(1)(a) of the GDPR	Until the purpose of data processing has been fulfilled or consent is withdrawn; failing that, until the termination of the contractual relationship.

64. The following data processing in relation to the Central Credit Information System ("KHR"):

Data receipt pursuant to Section 5 (7) a) of Act CXXII of 2011 on the Central Credit Information System (the "KHR Act") [in particular: identification data and so-called positive information, e.g. type of contract stored in the KHR, amount, date of conclusion, date of termination, etc.] on the basis of consent pursuant to Section 5 (3) of the KHR Act.	Article 6 (1)(a) of GDPR, consent of the Data Subject	8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of the Accounting Act).
The transfer of data pursuant to Section 9 (2) of Act CXXII of 2011 on the Central Credit Information System (the "KHR Act") - based on the consent of the Data Subject (in this case, the data processed by the Bank is only the consent to the processing of the Data Subject's data by the financial undertaking managing the KHR for a maximum period of five years after the termination of the contractual relationship).	Article 6 (1)(a) of GDPR, consent of the Data Subject	8 (eight) years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the Contract shall also be deemed as such) (under Section 169 (2) of the Accounting Act).

See the table above for specific rules on the withdrawal of consents under the KHR Act:

- Under the applicable law a consent under Section 5(3) of the KHR Act may only be withdrawn in writing.

- Under the applicable law a consent under Section 9(2) of the KHR Act may only be withdrawn in writing; until the termination of the contractual relationship, through the Bank, and thereafter directly contacting the financial undertaking managing the KHR.

If (any of) Your personal data are processed by the Bank based on Your consent as per the above table, we process Your personal data under such consent, until the withdrawal thereof / or if the purpose of data processing has been implemented previously, until the implementation of the data processing purpose, or in lack thereof, as long as any legal basis exist for the Bank for processing Your personal data (except if this Privacy Notice sets a period shorter than that for the processing of certain consent based personal data processing by the Bank). Withdrawal of the consent shall cover the period after the withdrawal of the consent, processing of personal data falling before this period shall not be affected by the withdrawal of the consent. You may withdraw your consent at any time without a reasoning by providing the Bank with any legal notice to the Bank, in particular by telephone, in written or electronic way / form or in person at our bank branch.

- Having Your consent thereto as set out in Article 6 (1)(a) of the GDPR, we process Your personal data provided in the course of using the applications made available by us through an on-line platform, in principle until the withdrawal of Your consent. You may withdraw your consent at any time without a reasoning, by way of providing the Bank with any legal notice, in particular by telephone, in written, electronic way / form or in person at our bank branch. Photograph(s) uploaded to such applications may only be uploaded to the application with the consent of the Data Subject(s) visible thereon. It is the responsibility of the user authorized to use the application to obtain the consent and to prove its existence, and the liability for all damages occurring related to the uploading of the image and the obligation to delete the image from the application shall be on the burden thereof. If there is any doubt about the lawfulness of the use of the image, the Data Controller shall be entitled, but not obliged, to take measures to delete the image.

- The Bank shall process the personal data (name, telephone number, e-mail address) provided on the website thereof during the online booking, on the legal basis of Data Subject consent as per point a) of Article 6(1) of the GDPR, in principle, until the completion of the data processing purpose or the withdrawal of the Data Subject's consent. In the latter case, the consent withdrawal methods described above provided related to the applications usable on the online interface shall apply.
- We may do voice recordings with a Data Subject's prior express consent which may be managed till the withdrawal of such consent, but till the end of the retention period relevant for the other personal data processed with regard to the Data Subject, the latest (unless otherwise required by this Privacy Notice). You may withdraw your consent at any time without a reasoning by providing the Bank with any legal notice to the Bank, in particular by telephone, in written or electronical way / form or in person at our bank branch.
- Direct marketing
  Under Section 6 (1) of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities

("**Commercial Advertising Act**"), we inform the Data Subjects that we only send (commercial) advertisements (definition: Section 1 (d) of the Commercial Advertising Act) to natural persons as recipients by means of direct marketing (thus, in particular, via electronic correspondence or other equivalent means of individual communication, with the exception of the addressed postal advertising and telephone contact made via a non-automized telephone calling system), either ourselves or via our agent if the relevant Data Subject as the recipient of such advertising has given its prior, clear and specific consent thereto. We keep records of the personal data of natural persons who make an explicit declaration of consent. Personal data entered into these records relating to the recipients of advertising may be processed only in accordance with and until the withdrawal of the declaration of consent (but in any event until the date set in Clause 35 of Chapter 3 and may be transferred to a third party only upon the prior approval of the Data Subject given as required by law. Withdrawal of the consent shall cover the period after the withdrawal of the consent, processing of personal data falling before this period shall not be affected by the withdrawal of the consent.

- **Detailed rules for data processing of Moneyback Benefit Program Persons cooperating in the Benefit Program**

  For the organization of the Benefit Program, Erste has a cooperation with Erste Digital GmbH (registered office: Am Belvedere 1, 1100 Vienna, Austria; company identification number: 396294k) and with Dateio s.r.o. service provider (registered office: Czech Republic, Prague 5, postal code: 150 00, Beniškové 1285/7, Košiře, company identification number: 02216973, registered in the Commercial Register of the Municipal Court of Prague in the Czech Republic, section C / registration number: 216820) hereinafter referred to as the **Service Providers**

  Scope of the processed data

  Customer data: e-mail address, telephone number, account number, customer ID (indirect ID of customers), year of birth, no (female / male), information on whether the payment will be received in a bank account (yes / no), name / identifier of the employer provided by the Organizer for contact purposes.

  Benefit Program data: registration status (active / inactive customer, account registration / closing date) of the Benefit Program

  Card data: unique ID of the Card, debit / credit Card, number of marked Cards, Card status (active / inactive), business / normal Card, details of the Organizer's account where the Card was issued,

  Transactional data: transaction channel (automatic teller machine, POS or WEB), cash / card payment, value / amount of payment, date / time of payment, description of payment, details of the card acceptor (eg name, country); information about the merchant (e.g. name, category).

  Purpose and manner of data processing

  Erste and the Service Providers shall process the personal data of the

Participants as per point 3 for the purpose of the Benefit Program, within the framework of which, the Service Providers shall develop aggregated segments by processing and combining the available data. Discounted Offers shall be compiled thereupon for segment groups and thus for the Participants belonging thereto. The Offers shall apply only to products promoted under the Benefit Program and shall only be available to Participants through channels approved in the Participation Conditions Policy of the MoneyBack Benefit Program.
In order to fulfil the above purposes, the Service Providers shall be entitled to make the personal data partially or in full available to another organization belonging to their company group.

Joining the Benefit Program shall not be considered as a consent for marketing promotions, the Organizer, Service Providers and Merchant Partners participating in the Benefit Program shall only be entitled to display Merchant Partner offers to Participants in the George App interface as specified in the Benefit Program.

The Participants data shall therefore be processed with a view to the implementation of the Benefit Program (with the purpose of joining the Benefit Program, ensuring the operation of the online platform and the mobile application, development of segment groups based on transaction data, providing personalized offers detailed above) after joining thereto.

For the preparation of offers, the personal data of the Participants registered in the Benefit Program (data of purchases paid by card) shall be transferred for analysis to the Service Providers, including the Transaction Data as of a period corresponding the specified period, ie 1 (one) year prior to joining the Benefit Program. In a limited number of cases, such Transaction Data may allow Service Providers to identify Participants.

The following must be taken into account when selecting Offers:
Previous purchases from merchants like Partner Merchants;
The distance between the Customer and any store participating in the Program (where the mobile application is used and the geographic location feature is activated); the relevant distance is determined by the nature of the products or services offered by the Partner Merchants;
Customer's online shopping habits;
The existence of previous purchases paid for with the Card in the stores of the Partner Merchants;

For the fulfilment of the above-mentioned purposes, Erste Bank may transfer certain categories of personal data outside Hungary, the European Union / European Economic Area. In case of a transfer outside the European Union / European Economic Area, Erste Bank shall transfer the personal data in accordance with the general terms and conditions adopted by the European Commission or other guarantees required by applicable law.

The personal data of Customers having joined the Benefit Program shall also be processed anonymously for statistical purposes to generate such aggregated data such as for example the number of Customers having joined the Program, the number of customers with active offers, the number of customers using the George App Mobile Application over a period of time.

Participant shall have the opportunity to enable the geolocation feature in order to locate the nearest stores of Partner Merchants that have joined the Benefit Program. In this case, the processing shall also extend to the location data with the consent of the Participant, which shall be deemed to be provided if this function is enabled. Consent may be withdrawn at any time by disabling the feature, without prejudice to any processing operations performed prior to the withdrawal of the consent.

Legal basis for processing

Consent by Participants made by joining to the Benefit Program on the George App interface pursuant to Article 6 (1) (a) of the GDPR.
The data processing consent is required for the participation in the Benefit Program and for the implementation of the Program and the achievement of the related goals, while the refusal of the consent shall lead to the impossibility to participate in or to operate the Benefit Program.
The Participant shall have the right to withdraw his / her consent at any time by disabling the Moneyback Benefit Program in the George App under the Profile / MoneyBack menu item, the withdrawal shall result in the termination of participation in the Benefit Program.
Withdrawal of consent shall not affect the lawfulness of the data processing prior to the withdrawal.

Duration of data processing

Erste shall process the personal data referred to in point 3 till the withdrawal of consent or the deactivation of the Benefit Program, or, under paragraph 2.G of chapter II, for 5 years from the withdrawal of consent or deactivation of the Benefit Program upon Erste's legitimate interest.

- **Detailed rules of data processing for the Click To Pay service**

1. Collaborating organizations in service provision

To provide the Click to Pay service, Erste Bank acts in cooperation with Visa Inc., the service provider that puts in place the technical conditions that are necessary for the operation of Click to Pay service (registered seat: 900 Metro Center Boulevard, Foster City, CA 94404, USA, hereinafter referred to as the Service Provider).

2. Categories of personal data concerned in data processing

Customer data: e-mail address, telephone number, mailing address transferred by the Bank as contact details.

Card details: card number, expiration date of the card

3. Purpose of data processing

The Bank and the Service Provider shall process the Customer' personal data as per the provisions of Clause 2 for the purpose of service provision.

The purpose of data processing is the use of the Click to Pay service in order to execute online card payments quickly and securely. The activation and use of the Click to Pay service does not qualify as consent to marketing solicitation.

4. Method of data processing

This data shall be managed jointly by the Bank and the Service Provider (where each company is responsible for the use of this data).

The Bank shall transfer the data specified in Clause 2 to the Service Provider via an encrypted channel of communication for the use of the Click to Pay service (activation, data modification) or the cancellation of the service.

The Service Provider shall store the data specified in Clause 2 and use it for online card payments in a manner where the Service Provider shall display the bankcards associated with the e-mail address whenever the Customer selects the Click to Pay option during payment and enters their e-mail address. Once the Customer has selected the bankcard preferred for payment, the Service Provider shall initiate card payment with the chosen bankcard. Consequently, payment is made in a secure manner, without manually entering card details.

A detailed description of the Service Provider's use of personal data is provided in the Notice that is available at the following link: https://www.visa.hu/hasznalati-feltetelek/visa-globalis-adatvedelmi-ertesites.html

The personal data of Customers using the service shall further be processed in an anonymized form for statistical purposes in order to produce aggregated data (for example, the number of Customers having activated the service).

5. Legal basis of data processing

The transfer of data shall be based on the consent pursuant to Article 6(1)(a) of the GDPR given by the Customers in the George App when activating the Click to Pay service.

Consent to data processing is required to use the service and achieve the associated goals, while any refusal to consent will render the use or operation the Click to Pay service impossible.

The Customer has the right to withdraw their consent at any time by canceling the Click to Pay service in the George App. The withdrawal of consent shall not affect the lawfulness of data processing performed prior to the time of withdrawal.

6. Duration of the data processing:

The Bank shall store the personal data listed in Clause 2 as set out in this Notice.

The Service Provider shall retain the data specified in Clause 2 for three months following the withdrawal of consent or the cancellation of the

service on the basis of the Service Provider's legitimate interests (settlement of claims submitted by Customers who have canceled the service and use of the data as factual evidence in the event of legal proceedings).

If you are an applicant (i.e. you are contacting the Bank to use the service but have not yet used the service),

i.e. you are a natural person defined in Clause 2.3.2 of the Privacy Notice, your personal data will be processed by the Bank as follows:

The Bank shall process the personal data of the Data Subject submitting an application as data categorised as banking secret under Section 160 (2) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings, the "Banking Act", in accordance with the provisions of the Banking Act on the protection of bank secrets, in addition to complying with the provisions of laws on the protection of personal data.

I. If the Bank has conducted credit assessment in Your respect, in the course of which it has commenced Your identification in compliance with the AML Act, but we have rejected Your credit application, the Bank shall process Your personal data and the documents containing those for 5 (five) years following the failure of the Contract based on its legitimate interest set forth in Section 166/A (2) of the Banking Act and, thereafter the Bank shall erase/anonymise Your personal data on a final and irreversible basis.

If the processing of Your personal data by the Bank is solely based on Your consent (and no other legal basis exist for the Bank to process Your personal data), the Bank shall process Your personal data until the fulfilment of the purpose of data processing but in any event no longer than up to 6 (six) months and thereafter the Bank shall erase /anonymise Your personal data on a final and irreversible basis.

II. In case You express Your intention, interest, wish towards the Bank to conclude a Contract, but the Bank or its Intermediary has not started the due diligence under the AML Act for the conclusion of the Contract, the Bank may process Your personal data (with Your consent) till 6 (six) months upon the receipt of the personal data, or, if You have withdrawn Your consent within this period of time, till the withdrawal of such consent, whereafter the Bank shall erase /anonymise Your personal data on a final and irreversible basis.

III. Applicants are also subject to marketing-related data processing based on their consent, as detailed in point IV.

The purpose of the processing of Your personal data	Legal basis of the personal data processing	Duration of the personal data processing
A) Transmission of identifier data to external digital platforms (Google*, Meta*, Adform***) for the purpose of displaying personalized content in marketing campaigns run by the Bank. Depending on the content of the consent, through the following	Article 6 (1)(a) of GDPR, consent of the Data Subject	Until the purpose of data processing is fulfilled or until consent is withdrawn. In the absence of such withdrawal, for 6 months following the provision of the data. If a contractual relationship

channels or any of them: Postal letter, Electronic mail, Telephone, SMS, Online platforms (online banking, mobile app services, push notifications, websites used for advertising) For Google and Meta, the transmitted identifier is the email address; for Adform, it is a unique identifier. Consent for data transmission is managed separately by the Bank for each channel. **Google***: By transmitting the email address, the user may see personalized advertisements across various Google services, such as Google Search, YouTube, and the Google Display Network. **Meta****: (Facebook and Instagram): By transmitting the email address, the user may see personalized advertisements on the Facebook and Instagram platforms. **Adform*****: By transmitting identifiers created specifically for this purpose, the user may see personalized advertisements across advertising networks managed by Adform. This means Erste Bank ads may appear on various websites and applications based on the user's interests, as part of the Adform advertising network.		also exists, then until its termination.
B) One-time callback response to a specific inquiry about a service.	Article 6 (1)(a) of GDPR, consent of the Data Subject	Until the purpose of data processing is fulfilled or until consent is withdrawn. In the absence of such withdrawal, for 6 months following the provision of the data. If a contractual relationship also exists, then until its termination.
C) Use of browsing data to provide personalized financial offers.	Article 6 (1)(a) of GDPR, consent of the Data Subject	Until the purpose of data processing is fulfilled or until consent is withdrawn. In the absence of such withdrawal, for 6

When the advertising cookie setting is enabled during a visit to erstebank.hu, browsing data collected on the Bank's websites and advertising platforms (such as visited pages and time spent on them) may be linked to banking customer data (e.g. banking activities, services mediated by the Bank, demographic data, etc.) after logging in through an identified channel (e.g. George Web).		months following the provision of the data. If a contractual relationship also exists, then until its termination.

How can I manage my consents (as an applicant) related to direct marketing communications, visibility on external digital platforms (Google, Meta, Adform), and the use of my browsing data?

In the case of a request submitted via a microsite, previously provided settings can be modified or withdrawn through the web interface linked in the confirmation email sent after the request, or via any of the contact options listed in point 4.2.

If the consent for "visibility on digital service provider platforms" referred to in points A–D is withdrawn as described above, Google and Meta will no longer use the transmitted email addresses to display marketing messages from the Bank and its subsidiaries. Adform will also cease processing the identifier created for this purpose.

If you are a beneficiary, a contractual contact person, other assisting third party of the contracting party (in particular an interpreter, translator), and an authorised representative for the purpose of concluding or performing the contract,

i.e. you are natural person defined in Clauses 2.3.4, 2.3.6 and 2.3.7 of the Privacy Notice your personal data will be processed by the Bank as follows:

The Bank shall process the personal data of Data Subjects under this Clause as data deemed banking secret under Section 160 (1) of the Banking Act, in accordance with the rules of the Banking Act on bank secrets in addition to complying with the rules on the protection of personal data.

The purpose of the processing of Your personal data	Legal basis of the personal data processing	Duration of the personal data processing
Processing of personal data and documents that may include personal data concerning the Beneficiary of the Contract, the Contact Person specified in the Contract, and other contributors of the Contracting party (in particular the interpreters and translators), and the Authorized Representatives acting for the	Based on the legitimate interest of the party entering into a contract with the Bank, under Article 6 (1) f) of the GDPR	During the entire duration of the Contract (ie 8 years following the year of adopting the annual accounts prepared for the year when the last Contract related accounting certificate has been issued (the termination of the

conclusion, performance of the Contract.		Contract shall also be deemed as such - under Section 169 (2) of Act C of 2000 on Accounting – the "Accounting Act").

If you are a payer

i.e. you are a natural person defined in Clause 2.3.5 of the Privacy Notice, your personal data will be processed by the Bank as follows:

The Bank shall process the personal data of Data Subjects under this Clause as data deemed banking secret under Section 160 (1) of the Banking Act, in accordance with the rules of the Banking Act on bank secrets, in addition to complying with the provisions on the protection of personal data.

The purpose of the processing of Your personal data	Scope of relevant data	Legal basis of the personal data processing	Duration of the personal data processing
Fulfilment by the Bank of the obligation to conduct customer due diligence set out in Sections 6, 7 and 14 of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing ("**AML Act**")	a) surname and given name, b) birth surname and given name, c) citizenship, d) place and date of birth	Performance of a legal obligation under Sections 6, 7 and 14 of the AML Act.	8 (eight) years from the recording of the personal data (the completion of the transaction order) (Section 56 and 57 of the AML Act)
Performance of a legal obligation under Sections 6, 7 and 14 of the AML Act	Recording of data pursuant to Sections 7, § 8, § 9 and § 9/A of the the AML Act (personal identification data, copies of documents, PEP declaration, declaration of beneficial ownership)	Performance of a legal obligation under Sections 6, 7 and 14 of the AML Act	8 (eight) years from the recording of the persona data (the completion of the transaction order) (Section 56 and 57 of the AML Act)

If you are in the category of Other Data Subjects

i.e. you are a natural person defined in Clause 2.3.10 of the Privacy Notice, your personal data (and the documents containing such personal data (if any)) will be processed by the Bank as follows:

I. If the processing of Your personal data by the Bank is solely based on Your consent (and no other legal basis exist for the Bank to process Your personal data), the Bank shall process Your personal data until the fulfilment of the purpose of data processing but in any event no longer than up to 6 (six) months and thereafter the Bank shall erase /anonymise Your personal data on a final and irreversible basis.

II. As other Data Subjects, the Bank is entitled to process your personal data in addition to your consent or, in the absence of your consent, on a legal basis pursuant to Chapter 2, Clause 4 of this Privacy Policy, for a lawful processing purpose, and as long as such legal basis and processing purpose exists, after which he Bank will permanently and irretrievably delete/anonymise your personal data.

III. Promotional Outreach to Potential Entrepreneurial/Corporate Clients via Direct Marketing:

For the purpose of direct business acquisition, the Bank may contact potential entrepreneurial or corporate clients using email addresses and telephone numbers listed in the databases of Opten Informatikai Kft. and Dun & Bradstreet Hungary Kft., as well as contact details available on company websites. Once these data are recorded in the Bank's system, the Bank will notify the company—using one of the contact methods available in the database or on the website—about the data registration and the possibility to object.
The Bank maintains a record of companies that have expressed their objection, and such companies will no longer receive promotional direct marketing communications.
The legal basis for data processing is the Controller's legitimate interest pursuant to Article 6(1)(f) of the GDPR. The duration of data processing lasts until a successful objection is received, or in the absence thereof, until the Bank's legitimate interest ceases to exist, but for no longer than one year.

If you are a contact person, employee or other data subject of Commerzbank's business customers in connection with the Bank's acquisition of Commerzbank Zrt.

Your personal data (including, in particular, delivery agents, beneficial owners, politically exposed persons of corporate clients, natural person providing security for corporate banking products) (and any document(s) containing such personal data, including, in particular, the personal identification data of natural person data subjects, contact data, customer identification data necessary to prevent and deter money laundering and terrorist financing, other related personal data) will be processed by the Bank as follows (information before data processing).

The source of the data subjects' personal data under this Clause is Commerzbank Zrt. The Bank acquires/has acquired the information on the corporate clients of Commerzbank Zrt. in accordance with Section 164(e) of the Banking Act, and Sections 117(9), 120(f) and 140(1) of the Investment Act. The interest of the Bank acknowledged by the Hungarian National Bank is that the transferor bank (Commerzbank Zrt.) provides the transferee bank (the Bank) with customer data so that the transferee bank (the Bank) can continue to provide the contractual services to customers. In addition to the rules on the protection of personal data, the Bank shall process the personal data of the data subjects under this Clause as bank secrets under Section 160(1) of the Banking Act and/or business secrets or securities secrets under Sections 117 and 118 of the Investment Act, in accordance with the confidentiality obligations thereof.

The data shall be processed until a successful objection by the data subject or, failing that, until the Bank's legitimate interest exists, i.e., until the conclusion of a contract with Commerzbank Zrt.'s corporate clients, or until the portfolio transfer has been completed at the latest. Thereafter, the personal data will continue to be processed by the Bank for additional purposes and under the legal basis set out in this Privacy Notice.

If you are a data subject visiting the Bank's website

I. Visitor: A Visitor is a person (data subject) who visits the Bank's website without providing any personal data and without engaging with the Bank for the purpose of using its services. **The website operated by the Bank may automatically save information about your device while you are using the website (from which no personal data may be inferred about You), and the Bank may place so called cookies thereon for the purpose of**

- collecting information about Your device,
- ensuring that such information can assist You to assist you in using the Bank's websites
- , or
- using such information to optimise advertising contents available on the website and other web pages.

The detailed rules on the use of the cookies is available at the below website: https://www.erstebank.hu/hu/cookie-policy https://www.erstebank.hu/hu/cookie-policy

II. Processing of the personal data of contact persons, authorised representatives and other contributors in respect of contracts concluded by the Bank for non-financial /auxiliary financial services

The processing of personal data of contact persons, authorised representatives and other contributors designated in a contract entered into between the Bank and a service provider under Act V of 2013 on the Civil Code (hereinafter the "**Civil Code**") is deemed to be processed for the purpose of keeping contact based on the legal basis of performing the contract existing between the Bank and the other party to the contract, in the interest of the party on whose behalf the relevant natural person acts and serves this purpose. The Bank processes the personal data of contact persons, authorised representatives and other contributor natural persons as personal data of Other Data Subjects during the entire retention period of the contract existing between the Bank and the service provider that has entered into a contract with the Bank, where such retention period is 5 years following the termination of the contractual relationship between the Bank and the service provider if there is no dispute between the Parties (and if the limitation period is not interrupted or suspended), except if such Other Data Subject objects to the processing of his/her personal data with the Bank. Upon a successful objection to the processing of the personal data of contact persons, authorised representatives or other contributor natural persons, the Bank terminates the processing of the personal data of such Data Subjects.

III. Processing of former employees' personal data by the Bank

Former employees' personal data may be processed by the Bank for the purpose, on the legal basis of and for the duration set out in this Clause, by means described in the General part of this Privacy Notice.

1. According to Section 99/A of the Act LXXXI of 1997 on Social Security Pension Benefits (Social Security Act), the Bank as employer shall retain the labour documents containing data regarding the social security relationship, duty period relating to the employee as beneficiary or ex-beneficiary of the social security, or the earnings, income that may be taken into consideration by the establishment of the pension benefits, for five years from reaching the retirement age relevant for the beneficiary or ex-beneficiary of the social security. We process these personal data with the purpose of complying with our legal obligations.

2. The Bank processes other personal data and the documents containing such other personal data in connection with the employment

relationship of a Data Subject described in this Clause and the relevant personal data for 3 years following the termination of the employment contract under Section 286 (1) of Act I of 2012 on the Labour Code (the "Labour Code"), with the exception of personal data processed under a legal basis being the Data Subject's consent. The Bank processes personal data processed under the consent of Data Subjects described in this Clause until the withdrawal of consent but in any event for up to 3 years following the termination of the employment contract as set forth in Section 286 (1) of the Labour Code.

IV. Processing of personal data of applicants for job offers

We process the personal data of the Data Subject completing a registration on the Career portal of the Bank (http://karrier.erstebank.hu) (including the documents attached by the Data Subject completing the registration and the personal data contained therein) for the below data processing purposes and within the following duration:

- to consider the application of the Data Subject to the specific job within the selection process, from the application till the closure of the selection, but no longer 1 (one) year,

- to consider this personal data by filling the positions opening at the Bank, to contact the registered Data Subject at the contact details provided by the registration with new positions possibly becoming actual, till 1 (one) year from the last application of the Data Subject to a specific position.

The Data Subject may register his or her data and may attach his or her Curriculum Vitae (with his or her photo) as document in a manner and format offered at http://karrier.erstebank.hu. If the registrant Data Subject provides a specific personal data by the registration, or attach a document containing specific personal data, the Data Controller shall inform the Data Subject that it shall not be entitled to process this personal data in the lack of the explicit consent made by the Data Subject, and the Data Controller shall immediately erase / delete this type of personal data after receiving thereof (if the registrant Data Subject does not provide the Data Controller with its explicit consent to the processing of such specific personal data). The Data Controller call the Data Subject not to provide access for the Data Controller to specific personal data (in the lack of its consent), because the Data Controller do not process such personal data of the Data Subject without the consent thereof. Only the Human Resources Management area of the Bank and the managers concerned with the selection procedure have access to the data provided by the Data Subject.

The Data Subject shall be entitled to change its password ensuring the usage of the surface, or the registered personal data at any time, and to terminate the access at any time. We call the attention of the Data Subject completing a registration that erase of the registration completed by the registrant Data Subject and the personal data contained therein can be done by the Data Subject in the account set up by the registration and can also initiate it via electronic mail sent to karrier@erstebank.hu e-mail address.

The Data Subject shall acknowledge that we may transfer Your personal data provided at the Career portal to contractual third parties as Data Controller, for the purpose of application to job offers, for the conclusion of targeted employment to use video interview platform service (Indivizo Zrt.), and to fill in The Predictive Index® surveys.

Nexum Magyarország Kft. (registered seat: 6722 Szeged, Gyertyámos u 13.; company registration number: 06-09-004861) is the data processor engaged by the Bank.

We may specify and disclose more detailed information for the Data Subject applying for position on the application surface.

V. Use of Facebook, Viber, banking widget surface

We ensure for the Data Subjects to request information regarding our services both at Facebook and Viber user interfaces and at our website. These interfaces cannot be used for lodging complaints and for sending privacy related requests, Data Subjects may only make requests thereby regarding the issuance of or questions concerning the general data not deemed banking or other types of secrets. We process the personal data provided in the course of using these portals upon consent provided by the Data Subject, until the withdrawal of such consent by the Data Subject, or in lack thereof, for 6 months after the relevant personal data have been recorded in our systems. Upon the expiry of this period, the Bank will finally and irreversibly erase /anonymise Your personal data (if no other legal basis exist for the processing of such personal data by the Bank).

Information concerning special Data Subjects (in particular, persons below the age of 16, natural persons providing data classified as special)

I. Persons **below the age of 16** shall be considered children under the GDPR.

> We only process personal data in relation to information society related services offered directly to children if the child is over the age of 16. Where the child is below the age of 16, we do the processing of the children's personal data only if and to the extent that consent is provided or authorised by the person holding the custody rights concerning the child.

II. We process **personal data regarding decisions on the declaration of criminal liability and offences and the related security measures** in the scope permitted by Hungarian law (if the Bank is deemed complainant or plaintiff in respect of the relevant offence or asserts a civil law claim in the criminal proceeding). If the Bank did not file a civil law claim in the criminal proceeding, we process such data until the decision adopted in the criminal proceeding becomes final, otherwise (if a civil law claim has been lodged) for 5 years after the judgement becomes final (that is, until the limitation of the right of enforcement) except if such period of limitation is interrupted or suspended (in this case, in compliance with Section 57 on the Act on Judicial Enforcement and with Section 286 of the Labour Code).

III. In accordance with applicable legislation, the Bank may purchase **databases containing personal data from service providers having a contractual relationship** with the Bank and if a Data Subject is recorded in such database, the Bank may contact the Data Subject at its contact details listed in the database, in compliance with legislative provisions applicable to the relevant contact to be made.

IV. The Bank may contact business organisations for the purpose of direct marketing (advertising) at the e-mail address and telephone number of such **business organisations indicated for contact keeping**, in compliance with the applicable legislative provisions.

4. My rights in relation to Erste's data processing

4.1 What rights do I have in relation to data protection?

We inform You that You as Data Subject have **the following rights in connection with the protection / processing of Your personal data by the Bank**:

If Your personal data is processed by the Bank, in connection therewith,

1. You may request access to personal data related to You, by way of requesting information from the Bank regarding Your personal data processed thereby. Information and copies of the processed data shall be provided free of charge (Right to access personal data),
2. You may request the rectification / supplement of personal data related to You without undue delay if Your personal data processed by the Bank are incorrect / incomplete. (**Right to rectification**). If exercising the right to rectification / supplementing of personal data would result in a change to personal data contained in Your Contract entered into with the Bank, that may be done by Data Subject as specified in the Business Rules of the Bank regarding contract amendment, or in lack thereof, in compliance with the legislative provisions in force or as set out by Your Contract with the Bank regarding the contract amendment;
3. You may initiate the erasure of all or only of Your certain personal data processed by the Bank (**Right to erasure**). Under this right, You may obtain to erasure / anonymisation of Your personal data on a final and irreversible basis (and to destruct / anonymise the documents containing the personal data of the Data Subject involved in such deletion) by the Bank, in respect of which

   3.1 the processing purpose for which the Bank as Data Controller collected or processed Your personal data no longer exists and no other legal basis exists for the personal data processing by the Bank and the personal data have not been erased / anonymised, or
   3.2 the processing of Your personal data is based on Your consent provided to the Bank and You have withdrawn such consent from the Bank in accordance with this Privacy Notice (and no other legal basis provided by law exists for the Bank for the processing of personal data),
   3.3 You have lawfully objected to the processing of Your personal data and no overriding purpose exists for the continued processing of Your personal data by the Bank,
   3.4 according to Your position, the processing of Your personal data is unlawful.

   Under Article 11 of the GDPR, we inform You that if no data processing purpose exists for the Bank that requires / permits the processing of the data of the Data Subject by the Data Controller, following the erasure / anonymisation of the relevant personal data, the Bank may only retain the customer identification numbers of Data Subjects (in respect of Data Subjects having customer identification numbers) so that the Bank is able to verify, upon a possible disagreement that the erasure / anonymisation has been completed by the Bank. The Data Subject shall provide its customer identification number to facilitate the verification of such erasure; in lack thereof, the Bank will be only able to inform the Data Subject or the party lawfully requesting information regarding the Data Subject that the Bank does not process any personal data regarding the Data Subject at that point in time.
   Instead of erasure, the Bank shall block the personal data of the Data Subject if the Data Subject requests so or if it can be

assumed on the basis of the information available to the Bank that an erasure would infringe the legitimate interests of the Data Subject. Personal data blocked for this reason may be processed only as long as the purpose for data processing that excluded the erasure of such personal data exists.

4. You may request the restriction of the processing of personal data concerning You, designating the scope of personal data to be restricted ("**Right to the Restriction of Data Processing**"). Under this right You may obtain restricted processing of Your personal data by the Bank if You contest the accuracy thereof or if, in Your view, the data processing is unlawful, nevertheless, You are against the erasure of the personal data, or if the Bank as Data Controller does not need the personal data for the purpose of processing but You need the same for the submission or assertion or the protection of legal claims.
5. You may request the Bank to specify the recipients whom it had informed of such rectification or erasure of data or of the restriction of data processing,
6. You may withdraw Your consent to the data processing at any time if Your consent shall mean the legal basis for the processing of Your personal data by the Bank ("**Right to the withdrawal of consent**"). We may process Your personal data following the withdrawal of Your consent, if processing is necessary for the Bank to comply with its legal obligation or on the basis of its legitimate interests, if the pursuit of such interests is proportionate to the limitation of the right regarding the privacy personal data,
7. 7. You have the right to receive Your personal data provided by You to the Bank in a structured, commonly used, machine readable format. You / a third person lawfully authorised by You may request the Bank to transfer such data to another data controller (if data is processed by the Bank on the basis of Your consent or of a contract with the Bank, in which You are one of the contracting parties and if the relevant data are processed using automated means; ("**Right to Data Portability**"). We inform You that, at this point in time, the Bank is unable to satisfy the request You / the third person lawfully authorised by You submitted on Your behalf regarding Your personal data provided to the Bank (that is, Your application regarding the acceptance of the personal data proposed to be recorded by the Bank) considering that no data processing procedure or a purpose for processing exists for the Bank that would facilitate the satisfaction of Your request and the processing of Your personal data limited to the relevant purpose, thus the Bank is currently not entitled to receive the data carrier containing Your personal data provided to it and to process the personal data stored thereon,
8. You may contest a decision if the Bank uses automated individual decision-making ("**Right to contest**"),
9. You may object to the processing of Your personal data by the Bank on legal basis of legitimate interest or on grounds relating to Your particular situation in the cases defined in the GDPR ("**Right to object**");
10. Regarding the lawfulness of the processing of Your personal data by the Bank, You may initiate the procedure of the Hungarian National Authority for Data Protection and Freedom of Information (abbreviated name: NAIH, registered seat: 1055 Budapest, Falk Miksa utca 9-11. mailing address: 1363 Budapest, PO Box. 9., website: www.naih.hu, telephone: +36 (1) 391-1400, fax: +36 (1) 391-1410, central e-mail

address: ugyfelszolgalat@naih.hu) or seek judicial remedy ("**Right to Redress**");

4.2 How can I file a claim with respect to the above?

As a Data Subject You may submit to the Bank Your questions / requests regarding the exercise of Your rights related to the processing of personal data at the following **contact details:**

1. In writing, in a letter sent to the address of the registered seat of the Bank (Erste Bank Hungary Zrt.; 1138 Budapest, Népfürdő utca 24-26.) (the application form regarding the processing of personal data is attached as Annex no. 1 to this Privacy Notice),
2. In a written application submitted at any branch of the Bank,
3. Verbally made via a recorded telephone line using the telephone customer service of the Bank (Telebank telephone number: +36 (1) 298-0222; to key customers: +36 (1) 298-0196),
4. In an e-mail message sent to erste@erstebank.hu,
5. In an electronic message forwarded from the George platform.

4.3 What information should I provide to this end?

With a view to the Bank's obligation regarding the protection of personal data/ banking secrets / securities' secrets / insurance secrets / business secrets, we shall complete the appropriate identification of the Data Subject in line with its capacity (customer, applicant etc.) in accordance with this Privacy Notice, and shall only be entitled to complete the application / request of the Data Subject only after the (proper level) identification of the Data Subject, upon the fulfilment of the Data Subject's application regarding the processing of personal data.

We accept requests / applications regarding the processing of personal data submitted by means of standard forms issued by NAIH for applications / requests to be submitted by the Data Subject, if the personal data to be provided thereon have been completed in full. If this request has been submitted in paper form, it shall also be signed by the Data Subject. If the Data Subject has not provided all personal data necessary for identification in the request, the Bank shall call on the Data Subject to supplement its personal data to facilitate a response to be provided to the request / application.

We provide the Data Subject with an application form on the personal data processing to submit the written applications as an Annex No. 1 to this Privacy Policy, whereby the Data Subject can submit its written application to the Bank by filling it. As per this Privacy Notice, we however accept written applications of the Data Subject other than this form as well.

The request of the Data Subject under Clauses 4.1-4.7 of Chapter 2 of this Privacy Notice for the processing of personal data shall include (beside the standard form issued by the NAIH) at least the surname and given name, place and date of birth, mother's birth name and the address of the Data Subject.

Application of the employee or former employee of the Bank for the processing of personal data shall include (beside the standard form issued by the NAIH) at least the surname and name, birth name, place and date of birth, Mother's maiden name and the social insurance number with regard to the Data Subject.

We may request the application of the Data Subject (Other Data Subject) under Clause 4.10 of Chapter 2 of this Privacy Notice in written form, (beside the standard form issued by the NAIH) by way of listing the types of personal data (processed data, for example name, e-mail address, telephone number) provided to and processed by the Bank, and by specifying the reason / purpose of data processing by the Bank.

If a Data Subject has submitted his or her request related to the processing of personal data contrary to the above and the Bank was not able to identify the relevant Data Subject appropriately as required for data security and/or for the protection of banking secrets (as specified in this Privacy Notice), the Bank may request the Data Subject to provide further personal data, and upon a failure or non-fulfilment of such request, the Bank shall not be able to respond to the request. That period of time from starting from the Bank's request for the provision of the necessary personal data / for the performance of a lacking activity until the provision of the personal data shall not be included in the calculation of the due date for responding to the request.

4.4 How long does it take to process my request?

The Bank shall perform requests regarding the processing of personal data / respond to such requests without undue delay, but in any event **within one month** following the submission thereof. This one-month period may be extended by two further months, taking into account the complexity and the number of requests, where the Bank shall inform the Data Subject of any such extension within one month of submission / receipt of the request to / by the Bank.

4.5 How does Erste respond to data subjects' requests for exercising their rights?

In the case of the Data Subjects falling within the scope of Clauses 4.1 to 2.4.7 of Chapter 2 of this Privacy Notice - the Customer, the Applicant, the Debtor, the payment guarantor , other natural person providing security, the Authorised Representative, the Payer, the Beneficiary and the Contact Person - the Bank will respond as follows:

The Bank shall comply with the Data Subject's request in connection with the processing of personal data by sending a reply by post. If attachment of copies shall become necessary concerning the response, this duty shall be fulfilled by the Bank by way of delivering a password-protected electronic data carrier to the Data Subject by post (as an annex to the basic information). The Bank shall deliver the password necessary for the use of the electronic data carrier and the information for the use of the password in a separate letter by post (in a so called password letter), in addition to the information letter, at least one working day following the delivery of the basic information letter. (Due to the Bank's obligation to protect banking secret and information security duties) the Bank shall only send the Data Subject information classified as personal data in an encrypted e-mail if the Data Subject expressly requests the e-mail delivery and even in this case, we shall fulfil the electronic delivery only to the e-mail address available to us, in a password-protected delivery if it is technically possible due to the size of any attachments. In this case, we shall deliver the password to the Data Subject necessary to access to the encrypted content via another contact channel data processed by us other than e-mail (telephone number, mailing address) or in any other identifiable manner. Information on the use of the password shall be included in the information that contains the password.

The Bank shall respond to that Data Subject's request via the George interface, if the Data Subject has submitted it via this channel or has requested such a response in a subsequently verifiable manner. If the size of the documents to be sent attached to the response letter may not allow a response via the George interface, a response shall be sent by way of attaching an encrypted CD to a postal mail, as described above.

The requests of Data Subjects falling within the scope of Clauses 4.8 to 4.10 of Chapter 2 of this Privacy Notice - the employee or former employee of the Bank, and the Other Data Subject - concerning personal data processing that involves the transfer of personal data regarding the Data Subject, shall be fulfilled by the Bank by way of delivering a response via post if the mailing address of the Data Subject is being processed. If attachment of copies shall become necessary concerning the response, this duty shall be fulfilled by the Bank by way of delivering a password-protected electronic data carrier to the Data Subject by post (as an annex to the basic information). The Bank shall deliver the password necessary for the use of the electronic data carrier and the information for the use of the password in a separate letter by post (in a so called password letter), in addition to the information letter, at least one working day following the delivery of the basic information letter. An employee or former employee of the Bank, and the Other Data Subject shall only be sent information classified as personal data in an encrypted e-mail if the Data Subject expressly requests the e-mail delivery or if the Data Subject's request has been received by e-mail and the Data Subject provides the Bank with a contact channel other than the e-mail (e.g. telephone number, mailing address) in order to send the password required to open the reply letter containing the personal data, or in case of contact information regarding the Data Subject other than the e-mail address is already being processed by the Bank and it is technically possible due to the size of any attachments. In this case, the Bank will send the password to the Data Subject via the contact channel other than e-mail. Information on the use of the password shall be included in the information that contains the password.

If the Data Subject has not received the postal letter (i.e. if the return receipt is returned to the Bank with a signal of not sought / received), the Bank will try to send the letter to the Data Subject once more, thus fulfilling its obligation to ensure the enforcement of the Data Subject's privacy rights, thereafter, the Bank shall resume the delivery of items that could not been received twice, only at the repeated request of the Data Subject.

If the Bank is under the obligation to disclose personal data regarded as banking secret to a third person within the frame of exercising the Right to portability, the Bank shall complete a request / application submitted in the form of a document or public document with full probative force under legislative provisions applicable to the protection of banking secrets, in compliance with Section 161 (1) of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings **("Banking Act").**

4.6 Will it cost me anything to assert my data protection rights?

No, Erste fundamentally fulfils such requests free of charge.

If, in the scope of his or her right related to the processing/protection of its personal data, set out in Clause 1.1 of Chapter 4 of this Privacy Notice, the Data Subject requests the issuance of a copy of such a document processed by the Bank, where the Bank's right to process / protect the Data Subject's personal data does not cover the issuance thereof, we inform the Data Subject to that effect and notify it that the Bank can fulfil the relevant request charging a service fee announced in respect of the relevant service and the Bank shall fulfil such request by the Data Subject after the Data Subject has indicated that it requests the issuance of the relevant copy also being aware of the relevant charge.

4.7 What options do I have to submit a complaint?

An application by a Data Subject regarding the processing of personal data shall not be considered by the Bank as a complaint but, if the Data Subject makes a complaint in its application regarding the processing of personal data that is in accordance with the applicable legislative provisions and the complaint handling regulations of the Bank, the Bank may respond to the request regarding the processing of personal data and to the complaint submitted by the Data Subject in a single notice (where adequate information is provided). If, following information provision by the Bank regarding the processing of

personal data / a response provided by the Bank to another request regarding the protection of personal data, the Data Subject makes a complaint as set forth in the complaint handling policy of the Bank, where such complaint is not related to the processing of personal data, the Bank shall process and respond to such request as a complaint.

5. Is Erste permitted to transfer my data?

Pursuant to Article 13 (1)(e) of the GDPR, we inform You that we transfer Your personal data to the following categories of recipients on the below legal basis:

5.1 Within its financial-, auxiliary financial activity, the Bank may transfer the Data Subject's personal data to the data processors assigned by the Bank for outsourced activity and specified in Annex No. 1 to the actual version of the Erste Bank's Business Rules (the "**Annex No. 1 to the Business Rules on Financial Services**") based on the Section 164 j) of the Banking Act and the data processing agreement concluded with the person doing the outsourced activity. The effective version of Annex 1 of the Business Rules is available at https://gate.erstebank.hu/uzletszabalyzat. Purpose of this data transfer is the fulfilment of the activity as outsourced activity as of the Annex No. 1 of the Business Rules on Financial Services to be performed by the particular data processor, and the duration thereof shall be last till the fulfilment of the data processing purpose.

5.2 Based on Section 161 c) of the Banking Act, we (may) transfer Your personal data to company(ies) dealing with debt collection and having contractual relationship with the Bank for the purpose of debt collection defined herein for the period necessary for the fulfilment of the data processing purpose.

5.3 Based on Section 164 q) of the Banking Act, we transfer Your personal data necessary for the fulfilment of a contract arranged by an Intermediary for intermediated financial service to the Intermediary being in contractual relationship with the Bank, for the period necessary for the fulfilment of the data processing purpose. The list of intermediaries that have a contractual relationship with the Bank is available on the website of the Hungarian National Bank at http://www.mnb.hu/felugyelet/engedelyezes-es-intezmenyfelugyeles/piaci-szereplok-keresese/kozvetitok-keresese. Intermediaries are entitled upon their contract with the Bank to transfer the personal data lawfully acquired during their intermediary activity.

5.4 In accordance with Section 164 d) of the Banking Act and the data processing contract, we may complete a transfer of personal data relating to the Data Subject to the auditor authorized by the Bank or to the responsible asset controller, to legal experts (individual lawyer and law office) having contractual relationship with the Bank or to other experts for the purpose of audit / legal, or other expert activity till the fulfilment of this purpose.

In case the Data Subject's consent is the legal basis for the data processing by the recipient as data processor, we shall inform the data processor about the withdrawal of the Data Subject's consent, whereupon the data processor shall no longer be entitled to process the data of the Data Subject that is being subject to its consent. We shall notify the data processor, if fulfilment of other duty becomes necessary for the data processor based on a request for the erasure / anonymise, correction, freezing of the personal date relating to the Data Subject or other personal data processing request.

5.5 We may assign our claim towards the Data Subject, whereby we transfer all data and document relevant to the debt of the Data Subject to the assignee upon the assignment contract (unless otherwise agreed by the assignor and the assignee in the assignment contract). Under Section 169 (2) of the Accounting Act, we process the accounting certificates relating to the assignment, and the underlying documentation for 8 years following the year

of adopting the annual accounts prepared for the year when the assignment related accounting certificate has been issued.

5.6 We may transfer Your personal data to the authorities having jurisdiction and competence, if the relevant legislation requires us to process these personal data, or if the authority having jurisdiction and competence has delivered us a proper request.

In the frame of ensuring the enforcement of Your access rights, we also inform You (upon Your request) in addition to the information on the recipient categories (by providing the company name and registered seat data) about such recipients whom Your personal data is / has been transferred.

5.7. Open banking (API channel) related data transfer

For the performance of the duties of the Payment Initiation Service Provider (hereinafter: PISP), the Account Information Service Provider (hereinafter: AISP), the Card Based Payment Instrument Issuers (CBPII) (hereinafter together: third party payment service provider – TPP) set out in Sections 31, 31/A, 38/A of Act LXXXV of 2009 in Payment Services, the Bank shall transfer the personal data necessary for the fulfilment of its TPP services, if the Data Subject has preliminary provided the TPP with its consent thereto.

In case of a retail customer, the Bank shall automatically provide access to the Indirect Electronic Channel (API) by default, without explicit request by the Data Subject, if the Account Holder has an Internet banking service and his / her Payment Account is accessible online. The Indirect Electronic Channel (API) and the TPP may be prohibited in accordance with the relevant General Terms and Conditions.

The Bank shall automatically provide access to the Indirect Electronic Channel (API) by default, without the Data Subject's specific order in case of retail customer, if the Account Holder has an internet banking service and its Payment Account is available online. The Indirect Electronic Channel (API) and the TPP may be prohibited in accordance with the relevant General Terms and Conditions.

The Bank may transfer the Data Subject's personal data included in the table below to the third-party payment service provider (TPP):

Service Provider	Purpose of data transfer	Personal data concerned with the data transfer
Account Information Service Provider (AISP)	Account list query	IBAN number currency account category (for example: current account) date of account opening
	Account balance query (regarding one specific account)	booked balance available balance locked balance
	Account history query (regarding one specific account)	The booked transaction in the query interval, or the live locks on the account, if the given day (query day) falls in the query interval
Payment Initiation Service Provider (PISP)	Payment initiation service	Query of the status of a payment order submitted via API,

		Withdrawal status of an ad hoc value date HUF order
CBPII Card Based Payment Instrument Issuer	Query of the coverage availability (related to card based payment transaction)	The Bank shall provide only 'yes' or 'no' information as a result of the Query.

5.8 Data provision by Erste Wizz credit card application

We inform You that Your personal data provided by the application for the Erste Wizz credit card are transferred to the WIZZ Air Hungary Ltd. (Registered seat: 1103 Budapest, Kőér utca 2/A, Building B II-V) based on the legal title of contract performance for a period necessary for the implementation of the data processing purpose.

5.9 Data transfer related to the Erste Student Loan Account Fee Package

The Framework Agreement for the Erste Student Loan Account Fee Package (hereinafter the Erste Student Loan Account) is only available to an Account Holder who has a student loan in accordance with the terms and conditions set out by Student Loan Centre Corporation [in Hungarian: "Diákhitel Központ Zrt"] or whose eligibility for a student loan has been confirmed by the Student Loan Centre Corporation and who has made a declaration as to the utilisation of an Erste Student Loan Account. Upon opening and closing of an Erste Student Loan Account, the Bank shall transmit the data detailed below to Student Loan Centre Corporation in order that Student Loan Centre Corporation can enter them into its records for the purpose of verifying the eligibility conditions.

The transfer of data is made for the purpose of the performance of the contract (Article 6 (1)(b) GDPR), in respect of the following data:
(1) Erste Student Loan Account bank account number,
(2) Date of opening of the Erste Student Loan Account
(3) Date of termination of the Erste Student Loan Account
The period of retention of the transferred data by Student Loan Centre Corporation shall be governed by the Privacy Notice of the Student Loan Centre Corporation in effect from time to time.

5.10 Data transfer in connection with collecting Erste Shopping Credit Card points

The condition for collecting Erste Shopping Credit Card points is that the Cardholder must have a valid Tesco Clubcard. When applying for the Erste Shopping Credit Card, the Cardholder shall provide the Tesco Clubcard number on the application form. The Bank shall provide the data detailed below to Tesco-Global Áruházak Zrt. in order to credit the points collected to the Cardholder's Clubcard balance.

The legal basis for the date transfer is the performance of a contract regarding the following data (Article 6(1)(b) GDPR): (1) the Clubcard card number, (2) the amount of points collected in a given period. Tesco-Global Áruházak Zrt.'s current Privacy Notice is applicable to the storage period of the data concerned by the data transfer.

5.11 The Data Controller informs the Data Subject that personal data relating to the use of the digital service George (George Digital Platform - George Web, George App) are processed for the purpose of providing our services and for the performance of the contract with you (Article 6(1)(b) GDPR). As indicated in Annex 1 to the Terms of Service, Amazon Web Services, the public cloud service provider under contract with Erste Digital GmbH, as data processor, processes the following personal data for the purpose of providing the service: name, address, account information, credit card details, financial transactions. Amazon Web Services processes data in the Republic of Ireland, Germany and Austria. The personal data is stored in the cloud hosted by Amazon Web Services, and compliance with the outsourcing requirements of the Banking Act is a guarantee of the adequacy of the processing performed by the data processor.

5.12 Data transfer to third country / international organization

In case of a data transfer to a third country or to an international organization, the Data Controller shall ensure an adequate level of protection for the transfer in accordance with the provisions of the GDPR and other European Union and national legislation.

5.12.1

Data transfers to other external digital platforms (Data Subjects: Client, Applicant)

Transmission of identifier data to external digital platforms (Google*, Meta*, Adform***) for the purpose of displaying personalized content in marketing campaigns run by the Bank. For Google and Meta, the transmitted identifier is the email address; for Adform, it is a unique identifier.

The data transfers to Google Ireland Limited, Meta Platforms Ireland Limited, and Adform A/S are considered intra-EU data transfers. However, under the Data Privacy Framework, Google and Meta may, in certain cases, transfer the email addresses to their data centers located in the United States.