SLOVENSKÁ sporiteľňa

Information on Personal Data Processing

(under Articles 13 and 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR))

Controller

Slovenská sporiteľňa, a.s., Tomášikova 48, 832 37 Bratislava, Registration ID 00151653, registered in the Commercial Register of Bratislava I District Court, Section: Sa, File No 601/B (hereinafter referred to as "Bank").

Telephone number: 0850 111 888 e-mail address: info@slsp.sk website: www.slsp.sk

Data Protection Officer

JUDr. Richard Főldeš, Head of Legal Services Division
Mailing address: Odbor právnych služieb, Slovenská sporiteľňa, a.s., Tomášikova 48, 832 37 Bratislava
E-mail-address:

Purpose and legal basis of personal data processing

Purpose of personal data processing	Legal basis
Provision of the Bank's products and services	Performance of a contract (with a client), compliance with a legal obligation[1], consent and a legitimate interest
Legal and contractual purposes	Performance of a contract (with a business partner) and a legitimate interest
Implementation of security measures to prevent fraud	Compliance with a legal obligation[2] and a legitimate interest
IT security and development	Compliance with a legal obligation[3] and a legitimate interest
Whistleblowing	Compliance with a legal obligation[4]

Accounting and taxation purposes	Compliance with a legal obligation[5]
Protection of property and persons	A legitimate interest and compliance with a legal obligation[6]
Marketing and PR purposes	Performance of a contract and a legitimate interest
Statistical purposes	Initial purposes within the meaning of Article 89 of GDPR
Archiving in public interest	Compliance with a legal obligation [7] or initial purposes within the meaning of Article 89 of GDPR

[1] In particular, the Act No 483/2001 on banks and other regulations and guidelines governing the financial/banking market
[2] In particular, the Act No 492/2009 on payment services implementing the so-called "PSD 2 Directive", which is available at https://eur-lex.europa.eu/legal-content/sk/TXT/?uri=CELEX%3A32015L2366 (hereinafter "**PSD 2 Directive**") and the so-called RTS Regulation, which is available at https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32018R0389&from=EN and other regulations and guidelines governing the financial/banking market
[3] In particular, Article 32 of GDPR; Articles 3c, 28c and 28d of the Act No 492/2009 on payment services
[4] Act No 54/2019 on the protection of whistleblowers
[5] In particular, the Act No 431/2002 on accounting; Act No 595/2003 in income tax; Act No 222/2004 on value added tax and other laws governing accountancy and taxes
[6] In particular, Article 38a and Article 93a(7) of the Act No 483/2001 on banks
[7] Act No 395/2002 on archives and registries

For a more detailed explanation of the above purposes and relevant processing operations please refer to the enclosed Second-Tier Information document.

Legitimate interests we pursue

Purposes of processing	Legitimate interests pursued
Provision of the Bank's products and services	▪ Identification of clients and their representatives; ▪ Client care; ▪ The Bank's risk model; ▪ Use of client information registers; ▪ Fraud and loss prevention and cooperation with law enforcement authorities; ▪ Data sharing and use within ERSTE Group in connection with cross-border payment operations; ▪ Real estate checks ▪ Streamlining of the identification of clients and their representatives within ERSTE Group through AML data sharing; ▪ Provision of payer address data to the payees' payment service providers in connection with transfers of any funds both across the EU/EEA and outside the EU/EEA.
Legal and contractual purposes	▪ Collection of receivables ▪ Litigations, legal proceedings and enquiries

	▪ Administration of contractual agreements ▪ Asset management ▪ GDPR ▪ Administration of legal affairs
Implementation of security measures to prevent fraud	▪ Strong access authentication in the FPS system
IT security and development	▪ Access right management; ▪ Security incident management and evaluation of reported suspicions; ▪ Monitoring to prevent confidentiality and integrity breaches and the gaining of access to important data and personal data through unauthorised access to electronic communication networks, malware distribution, denial-of-service attacks and damage to important assets of the Bank's infrastructure; ▪ Performance of software development, improvement and testing in order to ensure reasonable security, user friendliness and functionalities of the software required for the effective provision of modern banking services
Marketing and PR purposes	▪ Targeted advertising (direct marketing) ▪ Use of marketing tools ▪ Awareness and reputation enhancement (PR)
Protection of property and persons	▪ CCTV systems ▪ Access control and recording systems at entrances to designated areas of the Bank's premises ▪ GPS monitoring of company vehicles ▪ Use of private security services

A more detailed categorisation and explanation of legitimate interest can be found in the enclosed "Second Tier Information" document.

Personal data collection

A client must provide his/her personal data to the Bank to the extent required by the relevant law. For example:

- Based on Section 89(2) of the Banks Act, a client of the Bank is required to prove his/her identity and the Bank is required to refuse to execute a transaction where the client's anonymity is requested, except transactions referred to in Article 89(5) of that Act; or

- Based on Section 89(4) of the Banks Act, clients are required to provide ownership-related information in respect of funds exceeding EUR 15,000.

A number of laws are in place which require the Bank to collect or process certain personal data of clients, while such laws may not necessarily provide the obligation of clients to comply with requests for personal data or tolerate the processing concerned. Where there is a legal obligation of the client to provide data to the Bank and of the Bank to process such data, the Bank cannot proceed on the matter or execute the transaction unless and until such obligation is complied with. In certain cases the Bank is even obligated to report the matter to authorities.

Where the legal basis for processing the client's personal data is a legitimate interest, as referred to in Article 6(1)(f) of GDPR, the client is obligated to tolerate such processing, while also having the right to effectively object to such processing, which objection may lead to the processing being limited or ceased or continued, depending on circumstances. More information concerning this right can be found in the highlighted specific section "Data subjects' rights in personal data processing"

Where the legal basis of processing is consent to personal data processing within the meaning of Section 6(1)(a) of GDPR, the provision of personal data by the client is never mandatory and it is always done on a voluntary basis.

If we enter into a contract with you, the provision of your personal data may be made a contractual obligation, particularly for the purposes of sufficient identification of the parties to the contract or communication between them. The decision to enter into a contract or negotiation is always voluntary. While the provision of personal data is voluntary, non-provision may result in the contract being not concluded and the service sought not provided.

If the Client refuses to provide to the Bank personal data -:

- which are requested under relevant legislation, the Bank will not execute the banking transaction;
- which are inevitable for a contract to be concluded or performed, the conclusion, amendment or termination of, as applicable, or the provision of a particular performance under the contract will be impossible;
- which are inevitable for consent-based processing, the processing will be impossible.

Source of personal data

The Bank will obtain data directly from the Bank's client or from other clients, third parties (e.g. another bank, a legal representative, attorney in law or another authorised person, public authorities, financial institutions providing contact data to the Bank for the purposes of entering into a contract, courts, bailiffs, ...), relevant registers established under current laws, or from public sources in connection with the pursuit of the Bank's legitimate interests; or if such data is required for performing a contract or entering into a pre-contract arrangement, from providers of services based on public data and public sources of data, or from other persons, to the extent a legal basis exists for the collection of such data by the Bank.

In certain cases it is almost impossible or disproportionally difficult to inform you individually about the specific sources from which we collect information. Therefore, below please find information about the most frequent sources from which we collect data:

Source of personal data	**Personal data collected from an external source**	**Purpose of subsequent data processing at the Bank**
Common Banking Information Register (CBIR)/SBCB – Slovak Banking Credit Bureau, s.r.o.	▪ Personal identity data including the name, surname, permanent address, temporary address, birth registration number, if assigned, date of birth, nationality, type and number of identity document and a photo from the identity document, and for a business natural person also the address of the place of business, line of business, designation of the official register or other official records in which the business natural person is entered and the registration number; ▪ Contact telephone number, fax number and e-mail address; ▪ Documents and data proving and demonstrating (i) the client's capacity to fulfil the obligations arising from the transaction; (ii) the required security for the obligations arising from the transaction; (iii) the authorisation for representation if the person is a representative; (iv) the fulfilment of any other requirements and conditions applicable to the entry into or execution of the transaction under the Banks Act or other specific law, or agreed with the bank or the branch of a foreign bank, as applicable; ▪ Personal data entered in the register of natural persons pursuant to the Act No 253/1998 on the registration of residence of citizens of the Slovak Republic and the Register of Inhabitants of the Slovak Republic; ▪ Personal data from the register of identity cards pursuant to the Act No 224/2006 on identity cards.	Provision of the Bank's products and services

Various public registers, as further specified by SIMS, a.s. here: https://sims.as/gdpr.php, and SIMS, a.s. which collects and processes the information on our behalf	▪ The categories of common personal data kept in the relevant public registers, or aggregated analytical data generated from them; ▪ Personal data of real estate owners and other persons referred to in folios/certificates of title.	Provision of the Bank's products and services
The other bank which kept a current account for you if you apply for the transfer of your account (refer to "Account Transfer Information")	▪ Common identification and contact details, information on the payment account in the old bank and the scope of payment transactions which the data subject requests to be transferred, including information as to whether he/she requests the closing of the payment account in the old bank or transfer of a specific amount of funds from the payment account in the old bank without closing; ▪ Standing payment orders, direct debit authorisations, account protection against direct debits, and existing payment orders and direct debit payment orders with a due date after the date of transfer of the payment account; ▪ The amount and distribution of funds held in the current account in the old bank, if you also request their transfer.	Provision of the Bank's products and services
Courts, lawyers, executors, experts, parties to legal disputes or other interested persons authorised to submit various information and personal data for the proceedings, or public registers (e.g. Real Estate Registry, Commercial Register, Trade Register, Commercial Gazette, Register of Financial Statements, lists of debtors of the Social Insurance Fund and the public health insurance funds, Bankruptcy Register, etc.)	▪ Any common categories of personal data that are necessary in order to properly attain the purpose of the pursuit of legitimate interests in connection with evidencing, defending and enforcing the Bank's legal claims (e.g. administration of legal affairs, litigations, proceedings and inquiries).	Legal and contractual purposes
The members of the ERSTE Group, including in particular: Erste Group Bank AG, Erste Bank Austria, Erste Bank Novi Sad, Erste & Steiermärkische Bank, Erste Bank Hungary, Česká sporiteľňa, as, Banca Comerciala Romania	▪ Any common categories of personal data necessary to streamline the identification of clients and their representatives through sharing AML data and/or data obtained in the anti-money laundering and anti-terrorist financing processes; ▪ Any common categories of personal data necessary for the provision of customer care and for the Bank's internal administrative purposes; ▪ Any common categories of personal data required for the sharing and use of data within ERSTE Group in connection with cross-border payment operations.	Provision of the Bank's products and services
Internet access provider	▪ Common categories of personal data to identify a participant in electronic communication based on a dynamic IP address in the event of serious cyberattacks against the Bank.	Legal and contractual purposes

Categories of personal data concerned

The scope and categories of personal data to be processed will be as implied by the particular contract/pre-contract arrangement, relevant law or legitimate interest, or as explicitly specified in the client's consent. The Bank shall process, in particular, common personal data categories and any specific personal data categories will be processed only if additional conditions therefor are fulfilled, as referred to in Article 9(2) of GDPR.

Common categories of personal data processed by the Bank include, without limitation, the following:

- Identification and contact details of clients and other persons collected in connection with contractual arrangements;
- Identification details of clients collected in connection with the client identification and verification (as an anti-money laundering measure);
- Identification details of clients collected from identification documents (e.g. client identification in a branch or upon entering the Bank's protected premises), including a photo;
- Birth registration number collected in accordance with the conditions laid down in Section 78(4) of the Personal Data Protection Act No 18/2018;
- Data contained in CCTV recordings (made upon entering the Bank's protected premises);
- Data concerning the solvency and risk level of a client collected from shared bank and non-bank registers);
- Identification and operational data collected in connection with the client authentication for internet-banking or mobile applications or other electronic services of the Bank;
- All banking transaction data concerning the client, including orders and the Bank's communication with the client; or
- Data concerning the use of the Bank's websites and social network profiles, collected through direct communication or by means of cookies, as further explained in a specific document (https://cdn0.erstegroup.com/content/dam/sk/slsp/www_slsp_sk/documents/osobne-udaje/vyuzivanie-suborov-cookies.pdf?forceDownload=1).

The Bank also processes certain specific personal data categories, in particular biometric data, for purposes of the individual identification of a natural person. The basis of such processing is an express consent.

Data retention period

The Bank retains a client's personal data in a form allowing the identification of the client as the data subject only until it is needed for the purposes for which the personal data are processed. To that end, the Bank has specified the following retention times, or criteria for the determination of the applicable retention time, provided that the general retention times may be reduced or extended if the circumstances of a particular case so require:

Purpose of processing	General data retention period
Provision of the Bank's products and services	During the contractual relationship with the client and ten years after its termination, with the proviso that they will be destroyed no later than in the next two years (the total retention period can thus reach up to 12 years).
Legal and contractual purposes	During the contractual relationship with the client and ten years after its termination, with the proviso that they will be destroyed no later than in the next two years (the total retention period can thus reach up to 12 years).
Implementation of security measures to prevent fraud	For the time of use of electronic/mobile banking services
IT security and development	For the time of use of electronic/mobile banking services

Whistleblowing	Three years of the date of receipt of the report[9]
Accounting and taxation purposes	Ten years following the year in which the accounting document containing the personal data was created.[10]
Protection of property and persons	13 months as a general rule (particularly for recordings from CCTV systems referred to in Sections 93a(7) and 38a(2) of the Banks Act); 15 days for other CCTV systems; 2 years for access records
Marketing and PR purposes	Until the consent is withdrawn, or for one year from the beginning of processing
Statistical purposes	For the duration of initial purposes of processing
Archiving in public interest	For the duration of initial purposes of processing, or the mandatory period provided in law, or the period provided in the Bank's Registry Management Plan

[9] Article 11(1) of the Act No 54/2019 on the protection of whistleblowers

[10] Article 35(3) of the Act No 431/2002 on accounting, as amended.

Provision, access and disclosure of personal data

The personal data of the Bank's client will not be provided or made available to a third party, except as may otherwise be provided in a special law or agreed between the Bank and the Bank's client, or necessary for the fulfilment of contractual/pre-contractual obligations or the pursuit of the Bank's legitimate interests.

The Bank does not publish any personal data.

Categories of recipients of personal data

The list of recipients of personal data is provided in each relevant law under which the Bank is required to provide the personal data concerned (it may include, for example, courts, law enforcement authorities, bailiffs, official receivers, public authorities, the National Bank of Slovakia, banks, credit registers), or is explicitly specified in the consent granted by the data subject, where applicable. For personal data provided under a contract between the Bank and the client or under the client's order, the recipients are specified in such contract or order.

A list of the Bank's processors and a list of third parties to which data may be transferred by the Bank are published on the Bank's website in the "Personal Data" section, the "List of Processors of Slovenská sporiteľňa, a.s. and Other Recipients" document.

Cross-border transfer of personal data

The Bank's cross-border transfers of personal data to third countries (i.e. countries other than the EU Member States, Norway, Iceland and Lichtenstein) are limited to necessary cases and they are always performed in accordance with GDPR requirements. The Bank uses services of certain leading providers such as Google, LLC.,

Facebook, Inc., Microsoft Corporation or other data importers, as appropriate, particularly for marketing and statistic purposes. Those providers and their equipment are located in the United States of America. Since the Court of Justice of the European Union of the EU-US invalidated the Privacy Shield mechanism (http://curia.europa.eu/juris/document/document.jsf;jsessionid=48EBC070398FA667894F99C798FFCEE4?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=17767094), the United States of America have been treated as a third country that does not ensure an adequate level of protection. If we perform personal data transfers to third countries (such as the USA), we require the provision of additional personal data protection safeguards (such as conclusion of contractual clauses or existence of binding corporate rules). The contractual clauses are as provided in the model transfer agreement approved by the EU Commission (for the text please refer to https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32021D0914). Entities transferring data outside the EU are not allowed to deviate materially from the text thereof. The contractual clauses were declared by the Court of Justice of the EU a valid and applicable legal instrument. However, we make efforts to obtain additional safeguards wherever we deem it appropriate in view of the rulings of the Court of Justice of the EU. We provide information on concrete third-country data importers and the applicable guarantees upon request.

Automated individual decision-making, including profiling

The Bank uses certain forms of automated individual decision-making and profiling in the product approval process and the loan pre-approval process Accordingly, this section is relevant to the purpose of providing banking products and services and the sub-purpose of providing credit products.

The data used in the client profiling include those obtained by the Bank from the client's application for a product, data obtained in accordance with the laws in force from external sources (e.g. Credit Register or the Social Insurance Fund) and, also, data from the client's use of the Bank's other banking products and services. Those data altogether are used to create the client's risk profile. Based on the client's risk profile, the assessment of the application for a product or of a credit line amount is made using automated decision-making with such consequences that the product is provided to the data subject on standard terms, or subject to acceptance of higher guarantee/security requirements, or in an amount other than requested, or is not provided at all.

Profiling elements are also used in the implementation of fraud prevention measures in order to ensure strong authentication when an account is accessed or a transaction ordered through the Bank's electronic banking services, and thus ensure deposit protection and account protection against fraudulent misuse by unauthorised persons and perpetrators of cyber crime. The data from the Client's transactions are used in this case that enable the identification of the level of security of electronic payments, as foreseen by the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU; and Regulation (EU) No Repealing Directive 2007/64/EC; and Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council as regards regulatory technical standards for strong customer authentication and common and secure open communication standards (hereinafter "RTS Regulation"). A check is made when a client attempts to access electronic services as to whether any predefined risk signals are present that might indicate possible fraudulent misuse of the client's account, means of payment and/or electronic money. Based on the data thus obtained and evaluated, the transaction is classified as a normal one or a risky one. A normal transaction is confirmed by the client by clicking the relevant transaction field, while a risky transaction is confirmed by the client using the SMS key/mToken. In none of the cases mentioned above is the transaction processed automatically, without confirmation by the client. Based on a fully automated evaluation of a large number of diverse risk signals, the client's access to and basic command of the account via Internet banking services and the George application may be temporarily disabled and automatic reports may be generated to initiate an investigation of the potentially fraudulent/illegal behaviour indicating a possible misuse of the account and/or means of payment and/or funds of the data subject, including contacting the client through the client centre.

Automated decision-making and profiling are also used in the process of selecting clients for a targeted range of products and services.

The data subject has the right not to be subject to a decision based solely on automated individual decision-making (i.e. an algorithm-based decision of a computer program without any human intervention), including profiling, and the right to demand appropriate measures to be taken by the Bank (e.g. human intervention by the Bank and/or an opportunity for the client to express his/her position or to legally contest the decision); the exercise of this right does not imply, however, the Bank's obligation to approve a banking product for the client. The foregoing does not apply if the decision is permitted by the EU law or the law of the Slovak Republic and, at the same time, it provides adequate measures to safeguard the protection of rights and freedoms and legitimate interests of the data subject.

Data subject's rights in personal data processing

The data subject has the right to object to the processing of his/her personal data which the Bank processes on a legitimate/pubic interest basis, or to processing for marketing purposes, including profiling, in accordance with Article 21 GDPR. If you make an objection or request us to do so, we will be pleased to present to you the conclusions of our balance test proving the overriding status of the legitimate interest pursued.

We are committed to personal data protection and, therefore, we are making efforts to ensure the security of personal data through measures and by giving the data subject the possibility to exercise his/her rights under GDPR via an electronic or written or personal request. Requests concerning data subjects' rights may be delivered by electronic means or in writing using the data protection officer's contact details provided above. We recommend that every such request should include an as detailed as possible explanation of what right(s) afforded by GDPR the data subject seeks to exercise and what purposes of processing the request relates to, where applicable, and he data subject's identification details (for identity verification the data subject's identification details (for identity verification). Where the request is too general, we must require clarification and this extends the one-month time limit for handling a complaint.

GDPR lays down general conditions concerning the execution of rights by data subjects. However, their existence does not automatically mean that that the exercise of each right will automatically be granted by the Bank since exceptions may apply to a particular case, or the exercise of a particular right may be linked to the fulfilment of specific conditions which may not always be fulfilled. The Bank examines each request, including in the context of applicable legislation.

The client or data subject has the following rights vis-à-vis the Bank as the controller:

- Right to withdraw at any time consent to data processing previously granted, provided that this will not prejudice the lawfulness of any personal data processing made prior to the withdrawal; Right to have access to his/her personal data in accordance with Article 15 of GDPR;
- Right to have any incorrect or incomplete personal data rectified and/or completed in accordance with Article 16 of GDPR;
- Right to have his/her personal data processed by the Bank erased in accordance with Article 17 of GDPR;
- Right to the restriction of personal data processing in accordance with Article 18 of GDPR;
- Right to the notification of rectification, erasure or restriction of personal data to other recipients in accordance with Article 19 of GDPR;
- Right to the transmission/portability of data provided to the Bank in a structured, machine-readable format which are processed by automated means and on the basis of a contract or consent in accordance with Article 20 of GDPR;
- Right to object in accordance with Article 21 of GDPR;
- Right not to be subject to automated individual decision-making in accordance with the conditions provided in Article 22 of GDPR. For more information please refer to the section on automated individual decision-making and profiling.

Also, every data subject has the right to file a complaint with the supervisory authority, which is the Office for Personal Data Protection of the Slovak Republic, and/or a petition to initiate proceedings under Section 100 of the Act No 18/2018 on personal data protection. More information on data subjects' rights and templates of requests can be obtained from the Office for Personal Data Protection. As the data subject, you also have the right to complain to any other supervisory authority in an EU Member State where you have your habitual residence or place of work, or where the place of the alleged GDPR breach is located.

Contact details of the supervisory authority of the Slovak Republic:

Úrad na ochranu osobných údajov Slovenskej republiky [*Office for Personal Data Protection of the Slovak Republic*]
47 585 12
820 07 Bratislava 27
Slovak Republic
statny.dozor@pdp.gov.sk
+421 2 32 31 32 14

Slovenská sporiteľňa, a.s.