Purpose of processing	Legal basis	Further explanation of the purpose of processing, related processing operations and legitimate interests pursued [1]
1. Provision of banking products and services	Performance of a contract, compliance with a legal obligation, consent and a legitimate interest	The processing of personal data for the purposes of providing banking products and services covers, among other things, the following operations, areas and procedures of the Bank: **Identification of clients and their representatives.** This includes personal data processing in connection with the following: (i) Completion of initial client questionnaires, including identification and contact details of the client or the client's representative; (ii) collection of data by making copies of identity documents of the client or the client's representative; (iii) registration of the client and/or the client's representative in the Bank's central system; (iv) collection and check of additional information (e.g. a document demonstrating the representative's authorisation to act on behalf of the client); (v) specification of the type of client (e.g. natural person, business natural person, legal entity, minor client or legally incapacitated client); (v) check of the existence of bankruptcy proceedings or other similar proceedings; (vi) repeated check of data validity in subsequent transactions; (vii) data check against an identity document; (ix) biometric data processing for client identification purposes; (x) data change procedures with regard to the data of the client or the client's representative. **Bank accounts (deposit products).** This includes personal data processing in connection with the following: (i) Acceptance of the General Business Terms and Conditions and conclusion of the contractual agreement for a particular deposit product; (ii) preparation, entry into and settlement of deposit product transactions between the Bank and the client; (iii) opening, administration and management of a bank account; (iv) bank account servicing and technical support. **Credit products.** This includes personal data processing in connection with the following: (i) Consideration of an application for a credit or a credit card received directly from the client or the client's representative; (ii) client check by way of enquiries to bank and non-bank registers, including registers of third parties (such as the Social Security Fund); (iii) enquiries concerning the client's income (a series of questions prescribed in the relevant Decree of the Ministry of Justice of the Slovak Republic); (iv) check of the client's creditworthiness (ability to repay a credit) based on the Bank's approved risk model; (v) approval of a maximum credit limit based on the Bank's approved risk model; (vi) conclusion of loan/mortgage loan/credit card agreements, including the acceptance of the Bank's General Business Terms and Conditions; (vii) management of a credit product, including the draw-down and repayment. **Real estate checks.** This includes personal data processing in connection with the following: (i) Checks, using multiple sources and registers, of the condition of real estate involved in banking transactions (e.g. as the collateral securing a mortgage loan); (ii) processing of personal data of persons indicated in the certificate of title as the owners of the real estate; (iii) preparation and consideration of expert appraisals of the real estate; (iv) identification and assessment of the real estate in the Bank's internal system; (v) posting of data to contractual documentation (credit products). **Electronic banking.** This includes personal data processing in connection with the following: (i) Banking applications and internet banking, in particular George Slovakia, George GO Slovakia, SLSP mToken and Business 24; (ii) provision of banking products and services by any other remote/electronic means, including through the website www.slsp.sk and e-shop; (iii) client identification procedures (refer to the above) as part of digital onboarding; (iv) generation of login and identification data in the various applications; (vi) remote acceptance of contractual documentation. **Collective investment (Asset Management)** This includes personal data processing in connection with the following: (i) Disclosure of personal data to Asset Management Slovenskej sporiteľne, správ. spol., a. s., the asset management company of SLSP; (ii) opening of the client's asset account or a list of unit holders with the asset management company; (iii) placement of the client's orders with the asset management company; (iv) data exchange with, and mandatory data reporting to, securities depositories and exchanges; (v) record-keeping of holders of securities and security interests for the purposes of unit certificates; (vi) signing of documentation in the Bank's branches. **Securities (Treasury)** This includes personal data processing in connection with the following: (i) Data collection through so-called investment

		questionnaires, to the extent of the questions specified in the Decree of the Ministry of Finance of the Slovak Republic of 19 December 2017; (ii) collection of other data under the Securities Act (e.g. Certificates of Birth); (iii) advising in connection with trading in securities; (iv) record-keeping of the client' transactions in securities; (v) record-keeping of communication with the client under the Securities Act; (vi) dispute resolution with clients under EMIR; (vii) compliance with ISDA standards in connection with transactions in derivatives; (viii) keeping of a register of covered bonds; (iv) execution of the client's transaction orders. **The Bank's risk model.** This includes personal data processing in connection with the following: (i) Statistical processing of data of clients and their loan repayment history; (ii) risk rating of individual transactions; (iii) use of standard and extended credit register services; (iv) monitoring of relevant gazettes (bankruptcies, insolvencies and reports); (v) generation of unique identification and authentication codes of clients; (vi) calculation and adjustment of offers for concrete clients. **Payment transactions.** This includes personal data processing in connection with the following: (i) Execution and processing of domestic and international payments, including processing accuracy checks; (ii) necessary exchange of accessory payment details with banks, payment service providers and card companies within the SEPA and SWIFT systems; (iii) handling of complaints concerning the processing of payment services; (iv) provision and collection of information concerning erroneous payments; (v) provision of payment services; (vi) mandatory disclosure of data to third-party providers under PSD2; (vii) mandatory disclosure of data to the National Bank of Slovakia; (viii) inter-bank transfers; (ix) production and personalisation of payment cards. **Financial intermediation.** This includes personal data processing in connection with the following: (i) Intermediation of insurance for banking products and services (e.g. loan or payment card insurance) where the Bank acts as a financial agent authorised to act as such by its banking licence; (ii) data exchange with insurance companies being the Bank's contractual partners that provide services to the Bank's clients; (iii) compliance with the legal obligations of a financial agent arising from the Financial Intermediation and Advising Act and other relevant laws. **Registers.** This includes personal data processing in connection with the following: (i) Provision of data to and use of data of the NBS Register of Bank Loans and Guarantees under Section 38 of the Banks Act; (ii) keeping of the Bank's own register of clients under Section 92(7) of the Banks Act and provision of data of such register to other banks; (iii) provision of data to and use of data of the shared banking register (SBCB – Slovak Banking Credit Bureau, s.r.o.) under Section 92a of the Banks Act; (iv) provision of data to and use of data of the shared register of basic banking product consumers within the meaning of Section 92b of the Banks Act; (v) provision of data to and use of data of registers established under the Housing Loans Act and the Consumer Credits Act; (vi) update, rectification and erasure of data in the relevant registers. **Compliance.** This includes personal data processing in connection with the following: (i) Customer care procedures under AML regulations; (ii) identification, verification and check of facts under AML regulations; (iii) detection and reporting of suspicious financial transactions to the Financial Intelligence Unit and other competent authorities; (iv) action such as blocking of funds or suspension of payment transactions; (v) comparison of data obtained from various inter-governmental sanction lists or other lists; (vi) prevention of fraud and fraudulent transactions in financial market; (vii) filing of criminal complaints and provision of support and cooperation to public authorities in their action or evidence-taking in connection with suspected fraud; (viii) processing of aggregate loss data in connection with operational risk quantification; (ix) law enforcement authorities' enquires; (x) documentation of the Bank's operations; (xi) implementation of an internal control system and execution of regular internal/external audits at the Bank. **Customer care.** This includes personal data processing in connection with the following: (i) Provision of regular technical and information support to clients via the Call Centre, a branch or a personal banker, or communication through a chatbot; (ii) recoding of phone conversations with clients and client identity checks; (iii) handling of clients' general filings, complaints or claims; (iv) activity of the Bank's ombudsman available to clients for the referral of any matters; (v) any communication, whether by post, electronic means or telephone or in person, in connection with the processing operations mentioned above and sending of so-called service messages; (vi) processing and settlement of any bank charges according to the Bank's current pricelist, or crediting of any gains (such as interest or return) to the client's account; (vii) preparation, conclusion and execution of

		transactions and contractual agreements with clients; (viii) administration and control of contractual obligations between the client and the Bank; (ix) provision of value-added accessory services to the Bank's client, including the provision of so-called optional add-ons in the George application, such as a financial manager and a monthly summary that help the client to obtain an enhanced overview of the financial expenditure and receipt categories; (x) internal administration activities of the Bank or Erste Group, including without limitation transfers of personal data within Erste Group for internal administration purposes, including the processing of clients' or employees' personal data; (xi) obtaining clients' feedback with the aim of enhancing the quality of banking products and services and aligning them with clients' needs, requirements and preferences and new banking trends; (xii) assistance services that support the onboarding of potential clients who interrupt or fail to complete the necessary onboarding process, including using previously provided contact data. Such processing may include any other processing operations, areas or procedures which are inevitable for attaining the purpose of the provision of banking products and services. **Data sharing and use within ERSTE Group in connection with cross-border payment operations**. This includes the processing of personal data during the provision of data within the ERSTE Group in connection with cross-border payments, which is due to the sharing of the common IT infrastructure providing a platform for payment systems of some ERSTE Group banks (including the Controller). Such shared use of data enables the Controller to streamline and facilitate payments to clients' accounts held in third-country bank outside the ERSTE Group, e.g. from ERSTE Group's own funds that are held in bank accounts held outside ERSTE Group in such third countries. **Streamlining of the identification of clients and their representatives within ERSTE Group through AML data sharing**. This includes personal data processing in connection with the following: (i) Compatible use of the personal data which are processed by the Controller primarily for compliance purposes to carry out customer due diligence under AML laws (identification, verification and fact-checking according to AML laws) in connection with the Controller's pursuit of its legitimate interests, as well as for the identification of clients and their representatives within ERSTE Group; (ii) sharing of the personal data which are processed by the Controller primarily for compliance purposes and for purposes related to the identification of clients and their representatives within ERSTE Group, which includes the provision and receipt of personal data concerning important natural persons of the Bank's corporate clients (e.g. members of corporate bodies, ultimate beneficial owners, company members, shareholders) to/from members of 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; (iii) sharing of personal data within ERSTE Group through the "Compliance Advanced Analytics Platform and Services" (CAPS) group software platform for machine learning model development, client portfolio examination and analysis, financial crime risk analysis and related automated reporting aimed at optimising the efficiency and effectiveness of regulatory requirements concerning financial crime in the banking sector. **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**. This includes the processing of personal data to the extent of the payer's name, the payer's payment account number and the payer's address for all transfers of funds, irrespective of their amount, to the payee's payment service provider established within or outside the EU, where the payer address data may be provided in excess of the minimum requirements laid down in Article 5(2) and Article 6(2) of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on data accompanying transfers of funds and repealing Regulation (EC) 1781/2006. **The Bank's risk model – SIMS - Clients**. The processing concerned relates to the Controller's existing corporate clients or entities being examined in connection with the negotiation of the provision of a banking service. E.g. statutory representatives of corporate clients. The processing operation involves the processing of data obtained from Slovenská informačná a marketingová spoločnosť, a. s. ("SIMS"), which is an intelligence agency providing specialised analytical and structured intelligence services focused on economic, business and factual intelligence. SIMS obtains personal data to the extent of legally published data from official publicly available sources, such as the Statistical Office and state and other public registers. The basic part of the Controller's processing operations taking place in relation to the Bank's risk model is at the same time carried out on the legal basis of fulfilling legal obligations under Article 6(1)(c) of GDPR. Pursuant to the Act No 483/2001 on banks,

		the Bank is required to have its own risk model, which is subject to control and approval by the NBS and to adjustments by the Bank's to be aligned with its actual business. For this reason, the application of the Bank's risk model is an essential part of data processing in the provision of banking products and services. The broader context of this data processing is that the risk model protects the integrity of the financial sector by not allowing the Bank (especially in relation to credit or mortgage products) to carry out operations that pose a risk. However, the processing of data in connection with the application of the Bank's risk model represents a legitimate interest of the Bank in relation to the above-mentioned processing operations.
2. Legal and contractual purposes	Performance of a contract and a legitimate interest	The processing of personal data for the purposes of proving, pursuing and defending legal claims covers, among other things, the following operations, areas and procedures of the Bank: **Collection of receivables** This includes personal data processing in connection with the following: (i) Sending of payment demands and reminders; (ii) initiation of debt enforcement proceedings; (iii) initiation of court proceedings (payment order or action for performance); (iv) debt assignment to a third party; (v) legal representation of the Bank in relevant proceedings; (vi) exercise of a pledge or lien; (vii) conclusion of reconciliation arrangements, acknowledgements of debt, settlement arrangements or payment schedules. **Litigations, legal proceedings and enquiries.** This includes personal data processing in connection with the following: (i) Any court proceedings, irrespective of the Bank's procedural status; ii) any administrative, criminal or other proceedings and controls irrespective of the Bank's procedural status; (iii) provision of mandatory cooperation to courts, law enforcement authorities, administrative authorities, arbitration tribunals or mediators (refer, in particular, to Section 91 (4) of the Banks Act; (iv) notarisation of deeds; (v) non-court dispute resolution (e.g. through arbitration or mediation); (vi) conclusion of reconciliation arrangements, acknowledgements of debt or settlement arrangements; (vii) evidence-taking in support of legal claims; (viii) communication with courts, public authorities, parties in proceedings and their representatives; (ix) legal representation and advising by law firms; (x) obtaining expert opinions. **Administration of contractual agreements.** This includes personal data processing in connection with the following: (i) Conclusion and performance of any contractual agreement between the Bank and a third party; (ii) approval and revision of contracts and agreements by the Legal Department; (iii) communication between the parties, including the processing of data of the parties' contact persons and statutory representatives; (iv) central record-keeping of internal and external powers of attorney; (v) central record-keeping of supplier-customer contractual arrangements between the Bank as a business and third parries (i.e. outside the provision of banking products and services). **Asset management.** This includes personal data processing in connection with the following: (i) Management, maintenance and improvement of the Bank's movable and immovable assets; (ii) conclusion and record-keeping of lease agreements and other contractual agreements involving real estate; (iii) legal settlement of rights to real estate. **GDPR.** This includes personal data processing in connection with the following: (i) Handling of data subjects' requests and related communication; (ii) record-keeping of consents, objections or consent withdrawals; (iii) obtaining data subjects' opinions, e.g. in connection with impact assessment;
		(iv) reporting and documentation of personal data breaches; (v) keeping records of instruction or information; (iv) validation of previously granted personal data processing consents after a longer period, if appropriate, or a request for a new personal data processing consent in cases where the data subject has previously granted his/her consent and it is appropriate given the current circumstances (e.g. where a longer period has elapsed, or where the expectations of the data subject regarding processing could be different as the Controller's current request is more specific, etc.). **Administration of legal affairs.** This includes personal data processing in connection with the following: (I) Typical agenda of the Legal Department, such as preparation of opinions on contractual agreements, debt recovery or preparation of legal claims and petitions to initiate court proceedings; (ii) reviews of legal matters or advice; (iii) reporting of various matters to public authorities (including reporting administrative offences, criminal offences or insured losses/claims); (iv) use of legal representation or legal advice provided by law firms; (v) performance of due diligence, including the provision of data by potential buyers and their advisors, e.g. in connection with selling a business, stock or portfolio of the Bank; (vi) administration of corporate affairs and performance of all obligations under the Commercial Code (e.g. records of and invitations to general

		meetings, annual reports); (vii) obtaining, renewal and record-keeping of any licences, approvals, certificates of qualification or education in the Bank's usual regulatory compliance process.
3. Implementation of security measures to prevent fraud	Compliance with a legal obligation and a legitimate interest	The processing of personal data for the purposes of implementing security measures to prevent fraud covers, among other things, the following operations, areas and procedures of the Bank: **Strong access authentication**. This includes the processing of personal data in the Fraud Prevention System (FPS): (i) Implementation of strong customer authentication (SCA) for the client's access to the George desktop/mobile application, internet banking or dedicated API for connection to third-party providers (TTP), for the placement or confirmation of payment orders and other remote transactions posing a high risk of fraud; (ii) creation, analysis and use of clients' behavioural profiles to support SCA of electronic banking service users based on the definition and analysis of signals which reflect the mode of use and behaviour of the users of banking applications and systems; (iii) analysis and use of risk signals in the identification, authentication and authorisation of the data subject's accesses to particular electronic banking services and functionalities and in security level assessment in the authorisation of payments. **Automated individual decision-making.** This covers sets of automated processing operations in the FPS systems resulting in granting or rejecting access to the internet banking or the George mobile application, or a decision to make an individual risk assessment and examination of the initiated transaction, or stopping the initiated transaction. **IT security and development** This covers the combination and use of the data processed for this purpose, including risk signals, also for compatible IT security and development purposes in fulfilling legal obligations under Article 32 of GDPR, the RTS Regulation, the PSD2 Directive or the Banks Act, or in situations where the Bank's legitimate interest in such processing is overriding.
4. IT security and development	Compliance with a legal obligation and a legitimate interest	The processing of personal data for the purposes of IT security and development covers, among other things, the following operations, areas and procedures of the Bank: **Access right management.** This covers personal data processing in connection mainly with the following: (I) Assignment and withdrawal of and changes to access rights and roles for the various systems and applications of the Bank, which also includes the use of Service Desk or the ticketing system for the management of internal IT affairs; (ii) data integration and strengthening of users' and clients' access rights using technological solutions based on Identity Access Management (IAM); assignment, change and renewal of forgotten or compromised passwords for the Bank's internal systems or banking applications for clients (iv) keeping of a disabled user's data for a certain period following the withdrawal of the user's access rights in order to prevent attempts for misusing the user's login identity; (v) use of the so-called two-factor authentication of data subjects' access when conforming client transactions, or employees' access to an internal network of the Bank from an external, non-Bank environment via VPN, or other activities posing a higher risk; (vi) use of personal data to verify human action and distinguish it from attacks of so-called bots integrated in internet banking services; (vii) application of processes linked to status verification.

		Security incident management and evaluation of reported suspicions. This covers personal data processing in connection mainly with the following: (i) management and documentation of personal data breaches in accordance with GDPR, which may include reporting necessary personal data to the main supervisory body or processing personal data of the data subject to whom the Bank is obligated to report the breach according to Article 34 of GDPR; (ii) export, obtaining and use of log data concerning a specific event and persons involved, or log data directly concerned with the behaviour of a specific user at a specific time as a part of forensic analysis in the investigation of causes of and liability for a security incident.. **Monitoring of users and devices.** This covers personal data processing which typically includes the systematic monitoring and analysis of various data that contain personal data, mainly for the: (i) Use of a set of technology, procedures and allocated professionally skilled personnel of the Bank's Security Operation Centre (SOC) for the purposes of Security Information and Event Management (SIEM), which includes, in particular, security analysis of so-called suspicious events systematically generated in form of alerts on the basis of processing a large amount of data from various sources (e.g. systems, applications, external vulnerability databases, logs from different application tier levels of the information and communication technologies used by the Bank, computer networks, electronic communication metadata, etc.); (ii) comparison of personal data of the Bank's IT users with (personal) data identified as compromised using credible security software tools of the Bank, and further use of such tools for enhancing the security of the Bank and its clients (e.g. to block phishing attack e-mails, compromised credit cards used by an existing client, compromised databases offered for sale on Darkweb, etc.); (iii) generation of so-called log data from the monitoring of behaviours of the Bank's IT users, both internally (e.g. in relation to employees and authorised contractor staff) and externally (in relation to clients using banking services, users downloading banking applications etc.) at all levels of systems, applications and networks to the extent technically feasible; (iv) use of anti-theft functionalities to delete remotely, via the Internet, the contents of the work-related electronic mails in the employee's mailbox available in his/her mobile device (smartphone) in case of loss or theft of the device; (v) monitoring of the sharing of electronic files by specifically privileged users with access rights to external data warehouses of appointed processors. **Profiling and use of AI technology.** This covers personal data processing typically including the following: (i) Making applications available to users on the basis of digital risk assessment and, where appropriate, blocking a device temporarily if there is a larger number of signals or defined threats which may change and adapt dynamically over time (e.g. logging from a non-standard IP address/country or during non-working hours or from an unknown device) (so-called zero trust concept); (ii) defining risk criteria and events associated with the automated evaluation and analysis of large amounts of (personal) data in order to automatically generate alerts for security personnel, which may also be developed with the use of so-called machine learning methods incorporated in the artificial intelligence present within certain external security software solutions used by the Bank to analyse data and various events observed within internal systems. **IT development, improvement and testing.** This covers personal data processing typically including the following: (i) Personal data processing required for the development, improvement or testing of internal banking systems, applications and their functionalities, including the development, improvement and testing of technical security measures to reflect the current state of the art and technological advancement; (ii) personal data processing required for the internal control penetration testing or security auditing for ISO certification purposes in order to verify the functioning, reliability and adequacy of applied security measures.

		Use of data processed by FPS. This covers the combination and use of data processes for the implementation of security measures to prevent fraud, including risk signals, and also for compatible IT security and development purposes, subject to compliance with the legal obligations of the Bank as the controller within the meaning of Article 32 of GDPR. **Compatible processing for the purposes of proving, pursuing and defending legal claims:** this includes personal data processing which typically covers, among other things, the following operations, areas and procedures of the Bank: (i) Necessary processing taking place as a part of demonstrating the implementation of security measures and their practical use to the main supervisory body and other competent supervisory bodies which exercise the supervision of personal data processing across the Bank's group; (ii) necessary processing taking place as a part of security audits in situations where the Bank is the processor and the controller requires an audit to be carried out; (iii) necessary processing taking place as a part of security reviews and audits of the Bank's processors if, because of the nature, context and purposes, this cannot be performed without personal data processing; (iv) the use of data generated through the application of security measures (such as logs) in response to data subjects' requests made in connection with the exercise of their rights under GDPR; (v) disclosure of personal data processed for the purpose of IT security and development in connection with a request for the provision of support and cooperation to other units of the Bank which are responsible for the handling of requests made by public authorities in the performance of their legal obligations (e.g. courts, law enforcement authorities).
5. Whistleblowing	Compliance with a legal obligation	The processing of personal data for whistleblowing purposes covers, among other things, the following operations, areas and procedures of the Bank: (i) Taking steps in connection with the protection of whistleblowers (i.e. persons reporting information on wrongdoings) by the employer in accordance with Article 7 of the Act No 54/2019; (ii) receipt, consideration and record-keeping of reports within the internal report examination system, including retaining the reports received for a period of three years; (iii) making audio recordings of calls to the special whistleblowing hotline.
6. Accounting and taxation purposes	Compliance with a legal obligation	The processing of personal data for accounting and taxation purposes covers, among other things, the following operations, areas and procedures of the Bank: (i) Record-keeping and use of accounting documents in accordance with Section 35 of the Act No 431/2002 on accounting and on amendments to certain laws; (ii) retention of documents in accordance with Section 76(1) of the Value Added Tax Act No 422/2004; (iii) any personal data processing necessary for compliance with a taxpayer's obligations under the Income Tax Act No 595/2003, as amended; (iv) any personal data processing necessary for compliance with a taxpayer's obligations under the Act No 563/2009 on tax administration (Tax Code) and on amendments to certain laws; (v) any personal data processing necessary for compliance with a taxpayer's obligations under the Act No 359/2015 on the automatic exchange of information on financial accounts for tax administration purposes, which may also include the disclosure of personal data associated with financial accounts opened with the Bank to tax administration authorities of other member States of the EU, or of the United States of America under the Agreement between the United States of America and the Slovak Republic to Improve International Tax Compliance and to Implement FATCA (Foreign Account Tax Compliance Act), including its annexes..
7. Protection of property and persons	A legitimate interest and compliance with a legal obligation	The processing of personal data for the purposes of protection of property and persons covers, among other things, the following operations, areas and procedures of the Bank: **CCTV systems.** This covers the monitoring of (i) areas accessible to the public in the Bank's defined facilities, including the Bank's branch network; and (ii) ATMs and exchange offices (Article 93a(7) of the Banks Act) by CCTV systems.

		Access control and recording systems at entrances to designated areas of the Bank's premises This covers the (i) monitoring and use of data concerning Bank employees' and visitors' entries in designated protected areas, such as reserved areas in branches and the head office, tills, parking sites, ATMs, vaults or reserved premises of the Bank, which may also involve the check of the employee's photo integrated in his/her chip card; (ii) processing of limited data from the machine-readable part of the identification card (name, surname or number of the identity document) by automated means, together with data of the entry and exit times of visitors in relation to certain premises of the Bank. **GPS monitoring of company vehicles** This covers the geolocation monitoring of company vehicles used in connection with the performance of work duties or cash transport, which may also include the real-time tracing and instant location of a monitored vehicle. Employees' private travels, where permitted, may be monitored only to the extent the employee voluntarily chooses not to restrict the monitoring (i.e. not to enable the relevant system function using a push-button in the vehicle of the function of which the employee was instructed and the instruction documented/) and gives the Bank his/her specific informed consent to such monitoring and the related personal data processing; non-giving of such consent does not have any adverse implications for the employee. **Use of private security services.** This covers any personal data processing necessary for the proper performance of contractual agreements between the Bank and private security service (PSS) entities providing their security services to the Bank, which includes in particular the following: (i) Processing of personal data and identity checks of the PSS staff in connection with their cash handling action; (ii) other provision of services by PSS entities which involves necessary personal data processing in connection with the safeguarding of persons and property (e.g. accompanying the Bank's employees at auctions, enforcement proceedings or risk-involving court hearings, or guarding designated premises of the Bank).
8. Marketing and PR purposes	Consent and a legitimate interest	The processing of personal data for marketing and PR purposes covers, among other things, the following operations, areas and procedures of the Bank: **Targeted advertising (direct marketing)** This includes personal data processing in connection with the following: (i) Creation, adaptation and distribution of direct marketing mailings (e-mail, text messages, push-notifications); (ii) creation, adaptation and distribution of leaflets or targeted printed forms of marketing materials; (iii) creation, adaptation and displaying of advertisements on social networks; (iv) creation, adaptation and displaying of advertising banners; (v) creation, adaptation and displaying of offers in applications or internet banking; (vi) profiling clients' behaviours for on-line marketing purposes. **Use of marketing tools** This includes personal data processing in connection with the following: (I) Analysis of visitor, success and conversion rates (e.g. using tools such as Google Analytics, Facebook Ads Manager etc.); (ii) use of social-network or third-party plug-ins (such as FB/Google Login); (iii) client identification upon logging into a protected zone; (iv) use of various analytical tools based on cookies, pixels, SDK, web beacons etc., as explained in the Bank's "Cookies Policy"; (v) marketing research and surveys. **Awareness and reputation enhancement (PR).** This includes personal data processing in connection with the following: (i) Maintenance of the Bank's/SLSP Group's profiles on social networks and the related interaction with users; (ii) organisation of events, including making photos and video recordings; (iii) posting of contents, photos or video recordings in social media; (iv) awareness and goodwill enhancement (PR purposes); (v) organisation of consumers competitions, including with partners. **Offer for the refinancing of a credit product secured by real estate (cross-sell 1):** This covers the processing of personal data from the Real Estate Registry concerning the data subject's (Bank client's) ownership of real estate, including data on existing debts and other customer information on the data subject's use of services in order to identify a suitable group of clients with a higher likelihood of a positive response to relevant direct marketing communication and the Bank's offer of credit products that could be used e.g. to refinance the client's existing loan product, or for the renovation, furnishing or conversion of the real estate.

		This may also include involvement of the Retail Risk Department through the intermediary Slovenská informačná a marketingová spoločnosť, a.s. (SIMS) which monitors on the Controller's behalf changes in the data registered in the Real Estate Registry and retrieves data that are relevant to the Bank's clients and uploads them automatically to the Bank's systems where persons to be contacted with a direct marketing offer for loan refinancing are identified (e.g. the Controller's clients having a loan from the Controller that is secured by real estate which is at the same time pledged in favour of another bank). The form of such marketing may vary and it is planned to prefer a personal contact as part of the service provided to clients by the branch network, personal bankers and other forms of customer care, but the direct form of marketing through electronic communication (email, banking applications) is not excluded. **Offer of a credit product to a client with an unsecured loan (cross-sell 2):** This covers the processing of personal data from the Real Estate Registry concerning the data subject's (Bank client's) ownership of real estate, including data on existing debts and other customer information on the data subject's use of services in order to identify a suitable group of clients with a higher likelihood of a positive response to relevant direct marketing communication and the Bank's offer of credit products that could be used e.g. to refinance the client's existing loan product, or for the renovation, furnishing or conversion, or even financing of the purchase, of the real estate. This may also include involvement of the Retail Risk Department through the intermediary Slovenská informačná a marketingová spoločnosť, a.s. (SIMS) which monitors on the Controller's behalf changes in the data registered in the Real Estate Registry and retrieves data that are relevant to the Bank's clients and uploads them automatically to the Bank's systems where persons to be contacted with a direct marketing offer for loan refinancing are identified (e.g. the Controller's clients having a loan from the Controller that is secured by real estate which is at the same time pledged in favour of another bank).
9. Statistical purposes	Initial purposes within the meaning of Article 89 of GDPR	The processing of personal data for statistical purposes covers, among other things, the following operations, areas and procedures of the Bank: (i) Preparation of statistical outputs, statements, reports, analyses and various working and analytical inputs for the Bank's internal statistical purposes and for the statistical purposes of the National Bank of Slovakia, other authorities and legal entities; (ii) generation of anonymised and aggregated statistical data from the personal data processed for other legitimate personal data processing purposes which have a valid legal basis and of which data subjects were properly informed in accordance with Recital 50 and Article 89 of GDPR.
10. Archiving in public interest	Compliance with a legal obligation, or initial purposes within the meaning of Article 89 of GDPR	The processing of personal data for the purposes of archiving in public interest covers, among other things, the following operations, areas and procedures of the Bank: (i) Keeping of registry records for such retention times as specified in the Bank's Registry Management Plan; (ii) record-keeping of incoming post; (iii) destruction of registry records upon expiry of applicable retention times; (iv) transfer of archived documents to state archives; (v) record discarding proceedings; (vi) retrieval and use of registry or archive documents, subject to meeting compatibility test requirements (e.g. for the purposes of proving, pursuing and defending legal claims).

[1] The underlined parts of the text refer to the activities/operations/areas covered by the processing taking place on the basis of legitimate interests.