Recommendations to use content

Short text (verified on other customers to pass Google Play requirements):

In order to ensure the security of transactions and prevent fraudulent actions the Bank has the right to transfer to "Kaspersky" (JSB "Kaspersky", address: 125212, Moscow, Leningradskoe shosse, 39A, building 2, BC "Olympia Park") the following data: model of the Client's mobile device; operating system version; unique identifiers; geographic location of the Client's mobile device; mobile network data; data on all applications installed on the Client's device. Privacy Policy Kaspersky is located at: www.kaspersky.com/Products-and-Services-Privacy-Policy

For user in compliance with your in-app disclosure must accompany and immediately precede a request for user consent and, where available, an associated runtime permission. You may not access or collect any personal or sensitive data until the user consents. The app's request for consent:

- Must present the consent dialog clearly and unambiguously;
- Must require affirmative user action (e.g., tap to accept, tick a check-box);
- Must not interpret navigation away from the disclosure (including tapping away or pressing the back or home button) as consent; and
- Must not use auto-dismissing or expiring messages as a means of obtaining user consent.

Extended text (if the short version is not enough):

In order to ensure the security of transactions and prevent fraudulent actions the Bank has the right to transfer to "Kaspersky" (JSB "Kaspersky", address: 125212, Moscow, Leningradskoe shosse, 39A, building 2, BC "Olympia Park") the following data: Software, End Product, Data Subject and Environment identifiers (device identifiers, IMSI, IMEI, device firmware identifiers, software installations identifiers, software versions, OS, user identifier and user login in End Product); data of the use of authentication functionality on the device by a fingerprint (data about support for this functionality by the device, data on activation / deactivation of functionality, data about the fact of fingerprint change used for authentication on the device); installed applications data (file names, package names, paths, permissions, certificates, source, used libraries, date and time of installation, application reputation); device location data (coordinates, coordinates precision); active network connections (GPRS, GPS, Wi-Fi); device roaming, network connections data (IP addresses, MAC addresses, URLs, HTTP referrer data, SSID, VPN connection data); fingerprint of device properties (device firmware and hardware properties, display characteristics, sensors properties, network connection data, current settings, current security settings, location, system settings, webView settings, webGl data, canvas fingerprint,); files data (size, name, path, file MD5 hash sum); SensorEvent data; Privacy Policy Kaspersky is located at: www.kaspersky.com/Products-and-Services-Privacy-Policy

The declared purpose is achieved by:
- detecting use of the Data Subject’s account by third parties,
- detecting interception of the work session of the Data Subject with the End Product,
- detecting unauthorized or unspecified data modification,
- detecting suspicious activities on Data Subject’s device,
- detecting insecure wireless connections on Data Subject’s device,
- detecting malware and fake applications on Data Subject’s device,
- detecting vulnerable modifications in Data Subject’s device firmware.

For user in compliance with your in-app disclosure must accompany and immediately precede a request for user consent and, where available, an associated runtime permission. You may not access or collect any personal or sensitive data until the user consents. The app's request for consent:

- Must present the consent dialog clearly and unambiguously;
- Must require affirmative user action (e.g., tap to accept, tick a check-box);
- Must not interpret navigation away from the disclosure (including tapping away or pressing the back or home button) as consent; and
- Must not use auto-dismissing or expiring messages as a means of obtaining user consent.

Examples based on other clients

Permissions for all Android versions (example of other banks)	
Bank A	**Bank B**
Contacts: • Search for accounts on the device • Change contacts • View contacts	**Contacts**: • Search for accounts on the device • Change contacts • View contacts
Location: • Approximate location (network based) • Exact location (based on network and GPS signals)	**Location**: • Approximate location (network based) • Exact location (based on network and GPS signals)
Wi-Fi connection data: • View Wi-Fi connections	**Wi-Fi connection data:** • View Wi-Fi connections
Device ID and Call Data: • Получение данных о статусе телефона	**Device ID and Call Data:** • Получение данных о статусе телефона
Storage: • View data on USB storage • Change / delete data on USB storage	**Storage**: • View data on USB storage • Change / delete data on USB storage
Phone number: • Receiving data on the status of the phone	**Phone number:** • Receiving data on the status of the phone
Photos / Media / Files: • View data on USB storage • Change / delete data on USB storage	**Photos / Media / Files:** • View data on USB storage • Change / delete data on USB storage
Identity data: • Search for accounts on the device	**Identity data:** • Search for accounts on the device
Microphone: • Audio recording	No
Camera • Photo and video filming	**Camera** • Photo and video filming
Other: • Receiving data from the Internet • Establishing a connection with Bluetooth devices • View network connections • Access to Bluetooth settings • Prevent the device from going to sleep • Flash control • Connecting / disconnecting Wi-Fi network • Unlimited internet access • View Google service configuration • NFC-module control • Startup when the device is turned on • Vibration function control • Change audio settings	**Other**: • Receiving data from the Internet • View network connections • Prevent the device from going to sleep • Flash control • Connecting / disconnecting Wi-Fi network • Unlimited internet access • View Google service configuration • Startup when the device is turned on • Vibration function control

Data collected by Kaspersky Fraud Prevention:

EXHIBIT 1. ADDITIONAL CONDITIONS REGARDING DATA PROCESSING

This Exhibit 1 along with the End User License Agreement for the Software, in particular in the Section “Conditions regarding Data Processing” specifies the conditions, responsibilities and procedures relating to the transmission and

processing of the data, indicated in this Exhibit 1. Carefully read the terms of this Exhibit 1, as well as all documents referred to herein.

When the End User configures the Software to use transmission of data of Data Subjects, the End User is fully responsible for ensuring that the processing of personal data of Data Subjects is lawful, particularly, within the meaning of Article 6 (1) (a) to (1) (f) of Regulation (EU) 2016/679 (General Data Protection Regulation, "GDPR") if the Data Subject is in the European Union, or applicable laws on confidential information, personal data, data protection, or similar thereto.

Data Protection and Processing
Data received by the Rightholder from Data Subjects during use of the End Product of the End User are handled in accordance with the Rightholder's Privacy Policy published at: http://www.kaspersky.com/Products-and-Services-Privacy-Policy.

Purpose of Data Processing
The Rightholder will process data to protect the Data Subject against information and network security threats when the Data Subject uses the End Product of the End User.
The declared purpose is achieved by:
- detecting use of the Data Subject's account by third parties,
- detecting interception of the work session of the Data Subject with the End Product,
- detecting unauthorized or unspecified data modification,
- detecting suspicious activities on Data Subject's device,
- detecting insecure wireless connections on Data Subject's device,
- detecting malware and fake applications on Data Subject's device,
- detecting vulnerable modifications in Data Subject's device firmware.

The Rightholder will also process data to activate the Software within the End Product of the End User and to verify legitimate use of the Software by the Data Subject.

Processed Data
During use of the End Product of the End User by the Data Subject, the Rightholder will automatically receive and process the following data:
Software, End Product, Data Subject and Environment identifiers (device identifiers, IMSI, IMEI, device firmware identifiers, software installations identifiers, software versions, OS, user identifier and user login in End Product); data of the use of authentication functionality on the device by a fingerprint (data about support for this functionality by the device, data on activation / deactivation of functionality, data about the fact of fingerprint change used for authentication on the device); installed applications data (file names, package names, paths, permissions, certificates, source, used libraries, date and time of installation, application reputation); device location data (coordinates, coordinates precision); active network connections (GPRS, GPS, Wi-Fi); device roaming, network connections data (IP addresses, MAC addresses, URLs, HTTP referrer data, SSID, VPN connection data); fingerprint of device properties (device firmware and hardware properties, display characteristics, sensors properties, network connection data, current settings, current security settings, location, system settings, webView settings, webGl data, canvas fingerprint,); files data (size, name, path, file MD5 hash sum); SensorEvent data.

Purpose of Data Processing
The Rightholder will process data to detect and eliminate errors in the service.

Processed Data
During use of the End Product of the End User by the Data Subject, the Rightholder will automatically receive and process the following data:
Logs data (public methods calls, system and service API errors, service information about services operation, requests and responses to Kaspersky Fraud Prevention servers).

Examples of mentioning the collected data in EULA of banking applications:

BANK A

CONSENT TO PROCESSING PERSONAL DATA

I, being a client of _____ (hereinafter referred to as the “Bank”), freely, by my will and in my interest, give specific, informed and conscious consent to the processing of the following information relating to my personal data, incl. biometric personal data, including banking secrecy, namely:
 full name; year, month, date, place of birth; citizenship; floor;
 data of the identity document (type, series, number, by whom and when issued), including their copies;
 address: place of residence, place of registration, place of work;
 taxpayer identification number;
 insurance number of the individual personal account, information on the state of the individual personal account of the insured person;
 information about employment, labor activity (including information about seniority, income and expenses), marital status, property status, education, profession;
 data of the driver's license, including its copy;
 information about phone numbers of which I am a subscriber and / or user; information about the communication services provided by operators (including information about the location of subscriber equipment when receiving communication services, information about traffic, services provided and their payment), information about the results of their processing, including the organization of a communication channel between the Bank and me using phone numbers of which I am a subscriber and / or user; data about me as a subscriber of a cellular operator, including the following information: the fact of changing the phone number, international identifier of the SIM card, its replacement, the fact of reissuing to a third party or transferring to another operator with the number being preserved; on the fact of termination of the contract for the provision of communication services, suspension and resumption of the provision of communication services; about the fact of connection of call and message forwarding services; about the fact of a change in the settlement system between the operator and the subscriber; on the fact of receipt by the cellular operator of the subscriber's refusal to transfer information to the Bank on any of the listed events;
 information about my e-mail addresses, username on the Internet, information about the account (account) created on the Bank's website or mobile application; metadata, cookie data, cookie identifiers, IP addresses, browser and operating system information;
 information about my bank accounts and cards, operations carried out on them;
 amount of debt to the Bank, other creditors;
 information from the credit history, other information previously provided to the Bank (including information containing bank secrets);
 photographic image and video image;
 audio recording of voice;
 information provided by me to the Bank, including through communication channels, information received from the Internet and / or from other publicly available sources of personal data, and / or from third parties, including government bodies, state information systems, a unified system identification and authentication, the Pension Fund, including through the system of interdepartmental electronic interaction.

The processing of personal data can be carried out using automation tools or without them, including collection, recording, systematization, accumulation, storage, clarification (update, change), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction of personal data, including in the information systems of the Bank, and performing other actions provided for by Federal Law No. 152-FZ of July 27, 2006 "On Personal Data".
The purpose of processing personal data is:
exercise by the Bank of any rights and obligations related to the fulfillment of the requirements of the legislation of the Russian Federation, agreements, provisions of the Bank's internal documents and corporate standards for the identification and study of Clients;
 consideration by the Bank of the possibility of concluding any contracts and agreements with me, making a decision on the offer of services and services;
 checking the accuracy of the information I specified, obtaining the Client's personal data from other authorized sources;

 checking and assessing solvency and creditworthiness for making a decision on concluding a loan agreement and / or an agreement that ensures the fulfillment of obligations to repay the loan, further performance of the agreement (s), obtaining the results of such an assessment, a scoring score (individual rating), including characterizing indicators the quality of performance by an individual of his obligations to creditors, the presence or absence of factors indicating the possible conduct of the procedures used in the insolvency (bankruptcy) case and other indicators of reliability;
 negotiating the terms of contracts and agreements with the Bank, concluding contracts and agreements with the Bank;
 using the Bank's services, making settlements on the Client's operations and ensuring the security of transfers, including those made using bank cards;
 providing information on the performance of contracts and ongoing transactions on accounts and bank cards;
 submission to the International Payment System / Payment System World / organization providing the Payment Mobile Service, information about the operations performed by the Client through the Payment Mobile Service, as well as information for the purpose of tokenization of the Card;
 making money transfers through the Fast Payment System / Sberbank Payment and Transfer System;
 payment by the Client for goods, works, services of third parties through the Bank's branches, using the ___ Internet Bank, __Mobile services, ___Payment money transfers, online stores, payment terminals, cash desks receiving payments, ATMs and other devices. The list of third parties - recipients of payments is determined by the Bank;
 purchase by the Client of goods, other property, including property rights, works, services of third parties, including other credit organizations, management companies, brokers, forex dealers, insurance organizations, telecom operators, appraisal companies, leasing companies, organizations, providing legal and other services;
 improving the quality of service by the Bank, organizing the improvement of the Bank's software;
 promotion of goods, works, services on the market by making direct contacts by means of communication, by telephone, via a mobile radiotelephone network and in any other way, chat, sending SMS messages, sending messages via instant messaging services, mailing by e-mail , sending Push notifications, and in any other way, the Client bears all the risks associated with the fact that the sent messages may become available to third parties;
 creation of information data systems, analysis, modeling, forecasting, construction of mathematical models, construction of scoring models, their use and transfer of information processing results to third parties, analysis of aggregated and anonymous data, statistical and research purposes;
 collection of overdue debts to the Bank under any contract or agreement;
 provision of services to the Bank by third-party organizations for storing client documents, creating, storing, transferring electronic copies of these documents, including recognition of scanned images of these documents;
 Investigation of controversial transactions, including in the case of depositing cash to the account through software and hardware devices of third-party organizations;
 promotion of the Bank's products and services, including the transmission of information and advertising messages about the Bank's services by making direct contacts using communication means, conducting incentive events, including lotteries, contests, games and other advertising campaigns organized by the Bank;
 promotion of products and services of third parties, including the transmission of information and advertising messages about the services of third parties by making direct contacts using communication means, conducting incentive events, including lotteries, contests, games and other promotions organized by third parties;
 registration in incentive programs (bonus programs) or in other programs for individuals conducted by the Bank or organizations cooperating with the Bank in the framework of issuing partner cards, as well as the implementation of these programs, receipt of premium service by the Client;
 for the purpose of Authentication in the Call Center "_____-Consultant"
 queuing in the queue management system in the Bank's branches;
 other purposes that will be indicated in the agreements concluded between me and the Bank on the provision of banking products and services, other documents, including for the implementation of the opportunities provided for by Federal Law No. 422-FZ dated November 27, 2018.

The Client agrees and authorizes the Bank to provide in whole or in part the listed personal data to the tax authority in order to obtain information about the Client's taxpayer identification number by accessing the Find Your TIN resource posted on the official website of the Federal Tax Service on the

Internet, as well as to receive it by contacting to the resource "Find out your TIN" data on the Client's taxpayer identification number.
The Client agrees and authorizes the Bank to transfer, in whole or in part, any information and (or) documents to the competent authorities and / or financial and credit institutions in which the Bank has correspondent accounts, at their request, in order to carry out settlements on the Client's operations
The Client agrees and authorizes the Bank to receive the Client's personal data in the required volume from the Ministry of Digital Development, Communications and Mass Media of the Russian Federation (Ministry of Telecom and Mass Communications of Russia) through the Unified Information System for the purpose of considering the possibility of providing the Client with the Bank's services, concluding contracts and agreements with the Bank.
The Client agrees that the Bank sends a request on its behalf to the FIU through the SMEW to obtain information on the status of his individual personal account of the insured person and to provide the specified information to the Pension Fund of the Russian Federation through the SMEV to the Bank for its subsequent processing by the Bank (including recording, accumulation, systematization, storage, retrieval , use, disposal) in order to assess his solvency for making a decision on concluding a consumer loan agreement with him and providing loans. This consent to request and receive information from the FIU is valid for six months from the date the request is sent and the information is received from the FIU by the Bank, either until the Bank makes a final decision to conclude or refuse to conclude a consumer loan agreement with the Client (if such a decision is made before the expiration of six months).
The Client agrees that the Bank receives information from the credit bureau about the main part of the Client's credit history in accordance with Federal Law No. 218-FZ dated 30.12.2004 "On Credit Histories" in order to check the Client's reliability by the Bank and / or for the Bank to form regarding the Client's loan offers, the Bank's decision to provide the Client with a loan (s), the conclusion with the Client and further support (execution) of contracts.
In case of concluding a consumer loan agreement with the Bank, the Client agrees to interact with third parties, information about which has been provided to the Bank for the purpose of returning overdue debt.
The Client agrees to receive advertising, provide him with information and offer products of the Bank and / or third parties by sending to e-mail addresses, telephone calls, SMS messages to telephone numbers, via the mobile radiotelephone network and in any other way.

The Client confirms that he has received the written consent of individuals, whose personal data may be contained in the documents and information received by the Bank from the Client, for the processing of personal data of such individuals, in form and content in accordance with the legislation of the Russian Federation on personal data. At the same time, the Client, in turn, provides the Bank with his consent and the corresponding right to process the personal data of these personal data subjects in order to provide the Bank's services under contracts and assumes the risks associated with the use by him and the above personal data subjects of unprotected communication channels in correspondence with the Bank.
For the above purposes, the Client agrees to the processing of the listed personal data and information constituting a bank secret, _____ and / or third parties with whom the Bank has an agreement, containing a condition on the processing of personal data and information constituting a bank secret to the extent necessary for the execution of the agreement, as well as a condition on confidentiality and non-disclosure of information, including the list of which is posted on the Bank's website _____ (“List of third parties that process the personal data of the Clients on the basis of the agreements concluded with the Bank, the Clients' consent ”).
A client who is a user of the subscriber number specified in the agreement with the Bank (hereinafter referred to as the "User"), in order to provide the Bank with services, agrees to the telecom operators specified in the list posted on the Bank's website _____ ("List of third parties who process the personal data of the Clients on the basis of the agreements concluded with the Bank, the agreements of the Clients "), for the processing of phone numbers, the user of which is the User, information about the communication services provided by the operators (including information about the location of the subscriber equipment when receiving communication services, payment for communication services), information about the identifiers of the subscriber equipment and the transfer of this information or the result of their processing to the Bank, including the organization of the Bank's communication channel using the phone numbers used by the User.
Consent to the processing of personal data can be revoked by the subject of personal data by contacting the Bank branch. If the subject of personal data withdraws consent to the processing of personal data, the Bank has the right to continue processing personal data without the consent of the subject of personal data if there are grounds specified in the Federal Law of July 27, 2006 No. 152-FZ "On Personal Data", including for storage personal data provided for by the legislation of the Russian

Federation, in order to fulfill the terms of any agreement concluded between the Client and the Bank or to comply with the requirements of the legislation of the Russian Federation.
The Bank processes the Client's personal data during the entire period of validity of agreements, contracts, including the Agreement on Comprehensive Banking Services for Individuals in _____, concluded with the Bank, as well as within 10 years from the date of termination of the parties' obligations under the agreements.

BANK C

I, freely, by my will and in my own interest, in accordance with the Federal Law dated July 27, 2006 No. 152-FZ "On Personal Data", I give my consent to the _____ for processing
personal data including collection, recording, systematization, accumulation, storage, clarification (update, change), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction of personal data.
Personal data is provided by the Client for the purpose of executing contracts, obtaining information about the contract, obtaining information about other products and services Bank, using any means of communication, including telecommunications and postal departure. Personal data is provided by the Client in order to transfer it to the Bank Russia, JSC "National System of Payment Cards", Banks - participants in settlements in The Fast Payment System and other settlement participants of the Fast Payment System, posted on the website https://sbp.nspk.ru/, to transfer funds using the Fast Payments System from the moment you connect to the Fast Payment System payments using the Mobile Bank.

The list of personal data for the processing of which I consent:
1.surname, name, patronymic (current and all previous), gender, date of birth, place birth, citizenship, details of identity documents (current and all the previous ones); permanent or temporary registration address and actual address residence, contact phone numbers (home, mobile, work), address e-mail, insurance number of an individual personal account (SNILS), taxpayer identification number (TIN) / TIN (if any), family position, information on family composition, information on social status (including details of the state certificate for maternity (family) capital (if availability), information about education, attitude to military service, place of work, position held, information on sources of income, information on average monthly income and expenses, property status, information on financial transactions, information on social benefits.

2. for the Bank to process my Biometric personal data (including, but, not limited to photo, video, fingerprints of both hands) in order to conducting my identification and authentication, including in remote services.
In order to ensure the security of transactions and prevent fraudulent actions the Bank has the right to transfer to "Kaspersky Lab" (JSC "Kaspersky Lab", address: 125212, Moscow, Leningradskoe shosse, 39A, page 2, BC "Olympia Park") the following data: model of the Client's mobile device; operating system version; unique identifiers; geographic location of the Client's mobile device; mobile network data; data on all applications installed on the Client's device. Privacy Policy AO Kaspersky Lab is located at: www.kaspersky.com/Products-and-Services-Privacy-Policy.
This consent is provided from the moment of signing the contract and is valid within five years after the fulfillment of contractual obligations. After the specified the period of validity of the consent is considered to be extended for every next five years if lack of information about his recall.
I have been advised that for revocation