

# C Conditions for the Use of Electronic Services.

## 1. General conditions.

### 1.1 Scope.

The General Terms and Conditions governing the use of the electronic services of GKB shall apply to all electronic services of GKB (including the use of technical interfaces connecting systems of GKB with systems of third parties [e.g. connections to financial applications or banking platforms]; hereinafter referred to as the “Services”) that may now or in the future be required by the Client or the Client’s authorised representative (hereinafter referred to collectively as the “User”), unless otherwise specified in the Special Conditions for the Services concerned.

For the individual Services the Special Conditions shall also apply, as well as any conditions published on the GKB website (including product descriptions, overviews of Services and user manuals).

In the event of any conflict between the General Terms and Conditions, the Special Conditions for the applicable Services or any conditions on the GKB website, the Special Conditions shall apply first, then the General Terms and Conditions and then the conditions noted on the GKB website, in that order.

## 1.2 Access to the Services.

Technical access to the Services takes place via the User’s device. The hardware (including mobile devices such as smartphones) and software (apps in particular) used for access are deemed to be end devices. The User selects the provider (for internet, telecommunications, etc.). The end device must at least meet the minimum requirements indicated on the current GKB website or elsewhere.

Any person identifying themselves on the basis of the authentication keys referred to in the applicable Special Conditions has access to the Services.

GKB reserves the right to exchange or alter authentication keys at any time and will give the User suitable notification in advance.

GKB will send the authentication keys to the communicated mailing address of the User. The Client acknowledges and agrees that GKB cannot control who receives and uses the authentication keys. In the case of legal entities and/or delivery to a business address, the Client is responsible for monitoring the receipt of the authentication keys and their use.

As part of the two-step login procedure, GKB is authorised for security reasons to make the User's name/company name known when the valid authentication key is entered during the first step.

Any person who identifies themselves under the conditions noted above (self-identification) shall be considered by GKB as authorised to use the Services. GKB may therefore permit them to call up data and draw funds and may accept instructions or orders and legally binding communications from them, within the framework and scope of the Services used by the User, without any further verification of their authorisation.

GKB has the right to decline to perform Services for security reasons where it has legitimate doubts and to insist the User identify themselves through other means (e.g. by providing a signature or by means of a personal meeting).

The Client must inform their authorised representatives on the content of these provisions on electronic Services and ensure that they comply with all obligations hereunder.

The Client acknowledges unconditionally all transactions carried out in connection with the use of the electronic Services or technical interfaces using the Client's authentication keys or those of the Client's authorised repre-

sentative(s). In addition, all instructions, orders and notifications reaching GKB in this way shall be deemed to have originated from and been approved by the Client.

### 1.3 User's duty of care.

#### a) In connection with the authentication keys.

**The User shall immediately change the first password issued to them by GKB and agrees to change it regularly.** Passwords must not be easy to guess.

The User shall keep the authentication keys secret and protect them from misuse by unauthorised persons. In particular, authentication keys must not be saved unprotected on an end device. The authentication keys must also not be given to third parties or otherwise made accessible. Multiple authentication keys for using Services must be kept separately.

E-mails, text messages or other messages allegedly originating from GKB and requesting the disclosure of authentication keys (e.g. by entering user names, contract numbers or passwords) may not be responded to. GKB must be informed of these immediately.

If there is any reason to suspect that **unauthorised third parties have gained knowledge of one or more of the authentication keys of the User**, the User must **switch or change the authentication key immediately**. If this is not possible, the User **must arrange for access to the relevant Services to be blocked immediately or do so themselves**. New authentication keys should be requested from GKB if necessary.

In the event of irregularities, the User must not log in or, if already logged in, must terminate the connection immediately and contact GKB. Personal authentication keys must only be sent to GKB. Clients may only log in on GKB's login page and never on a third-party website.

The Client shall be responsible for all losses arising from the use – including any wrongful use – of the User's authentication keys, provided that GKB has exercised normal due care and diligence.

**b) In connection with the User's end device.**

The User must take suitable protective measures to minimise the risk of unauthorised access to their end device (e.g. over public electronic networks such as the internet). In particular, operating systems and browsers must be kept updated,

i.e. the User must install the software updates and security patches provided by the respective providers immediately. In addition, the standard security precautions for public electronic networks must be taken, e.g. using an anti-virus program and installing a firewall and keeping them updated. It is the responsibility of the User to stay informed of the latest state-of-the-art security precautions and the security tips provided on the GKB website and to take the recommended security measures.

If there is reason to believe **that unauthorised third parties may have gained access to the User's end device**, the User **must notify GKB immediately**.

The User must check any hardware and software provided for their use by GKB immediately upon receipt and report any defects to GKB at once. In the absence of any such reports to GKB, the hardware or software shall be deemed approved by the User.

**c) In connection with data input.**

The User shall check that all the data that they have entered is complete and correct. This applies in particular when scanning invoices. Responsibility for the data sent by the User remains with the Client until it has been received by the GKB system.

If the User has issued an order electronically to GKB (e.g. payment order, stock market order, etc.) and, after issuing the order, the User establishes that GKB has not or has only partly carried out the order in accordance with the User's instructions, the User shall immediately, but within one month at the latest, submit a complaint, failing which the said omission or erroneous execution shall be deemed to be approved.

#### 1.4 Security of Services, liability waiver.

Due to the encryption used, in principle it is not possible for any unauthorised person to see confidential client information. Nonetheless, absolute security cannot be guaranteed for either GKB or the User, even in the case of security precautions which conform to the latest technology. The User's end device, their network and/or third-party systems used by the User form part of the system. However, they are outside the control of GKB and may constitute a weak point in the system.

The Client accepts the following risks and hereby agrees to take due note of the security information placed on the website for the respective Services or made available to the User in any other form and shall immediately take any security measures recommended:

- Inadequate systems knowledge and inadequate security precautions may facilitate unauthorised access (e.g. inadequately protected storage of data on hard disk, file transfers).
- When using a network (e.g. the internet, a mobile network), there is a risk that viruses, etc. could infect the end device when it connects to the network. Suitable software available on the market can support the User's security precautions.
- It is imperative that the User uses software only from trusted sources.
- The network operator or software provider has the technological ability to profile the User's internet traffic and to see with whom the User has been in contact.
- It is possible for a third party to gain access to the User's equipment unnoticed while Services are being used.

GKB makes no warranty that the User will have unrestricted access to or unrestricted use of the Services. GKB also cannot guarantee that the internet will always be fully operational. GKB further cannot guarantee that information sent by it at the User's request using electronic communication channels (e.g. e-mail, SMS, app, technical interfaces) will reach the User within a reasonable period of time.

GKB exercises normal due care and diligence when displaying and transmitting data, information, notifications, etc. (hereinafter “data”) that it provides as part of the Services. **GKB disclaims any further warranty and liability for the correctness, completeness or current relevance of the data. In particular, account and custody account details (account balances, statements, transactions, etc.) and generally accessible information such as stock prices or exchange rates shall be deemed to be provisional and not legally binding. The data contained in the Services shall not constitute a binding offer, unless expressly described as such.**

GKB furthermore disclaims any responsibility for the content of external websites to which there may be links from the publicly accessible content of the e-Banking and mobile banking channels. These websites are entirely beyond the control of GKB. Connections to these websites and their content are established at the Client’s own risk.

GKB assumes no liability for the User’s end device, technical access to the respective Services, the software and hardware required for this purpose or third-party systems used by the Client. Likewise, GKB assumes no liability for any defects in any software it provides, e.g. via data carriers, downloads, etc., for the accuracy or completeness of data transmitted via a technical interface (e.g. ac-

count balance), for the misconduct of third-party providers or their systems, or for the interruption or restriction of Services.

The Services are provided via an open network accessible to anybody (e.g. by internet, telephone network etc. ). GKB cannot accept liability for any loss or damage arising from use of the public network. In particular, GKB accepts no liability for loss or damage incurred by the Client as a result of transmission errors, technical faults, interruptions, outages, delays (especially in processing), illegal interference with network and/or telecommunications installations, overloading of network and/or telecommunication installations, disruptions, interruptions or other faults of the network and/or telecommunications operators.

If any security risks are discovered, GKB reserves the right at all times to suspend the Services until the risks have been eliminated. GKB also reserves the right to interrupt the Services for maintenance work. GKB accepts no liability for any loss or damage resulting from any such interruption or blocking of access.

GKB accepts no liability for loss or damage incurred by the Client as a result of the Client's failure to perform their contractual obligations to third parties, or for indirect or consequential damage such as profit foregone or claims from third parties.

GKB accepts no liability for loss or damage resulting from minor negligence on the part of support staff going about their normal duties.

### 1.5 Transaction confirmation.

In order to increase security, GKB reserves the right to request a transaction confirmation from the User to confirm the order.

**In such cases, the User is obliged to compare the data sent by GKB to their end device with the original order or original document and to check that it is correct.** If the User believes that the data transmitted by GKB is correct, the User must, if the User wishes to issue the corresponding order to GKB, confirm the order (e.g. by entering the code provided by GKB). **If the User believes that the data transmitted by GKB is incorrect, the User must abort the transaction. If the User does not confirm the order, the order shall be deemed not to have been issued by the User and it will not be processed by GKB.**

### 1.6 Blocking of access.

The Client may have GKB block access by the Client or the Client's authorised representative to any of GKB's Services.

Such blocking may be requested during normal business hours or the hours when the relevant Service is available. Until such a block has become effective within the customary period of time, the Client shall bear the risk of any misuse of the authentication keys for using the Services.

The block or interruption may be lifted at the request of the Client.

GKB is entitled to block access by the Client and/or one or all authorised representatives to any single one or all of the Services as well as the connection to systems via the technical interface at any time without having to provide reasons and without prior notice.

### 1.7 Terms applying to powers of attorney and authorisations.

When a power of attorney is granted pursuant to the list of authorised signatories at GKB, the authorised representative is also permitted to use electronic Services of GKB. The removal of the signatory powers conferred on an authorised representative, as set

out in the list of authorised signatories at GKB, shall automatically have the effect of terminating any permission to use the Services. If authorisation is granted to a third party to use the Services other than under the list of authorised signatories at GKB, this authorisation must be revoked separately.

In addition, the death of the User or the User's incapacity to act – notwithstanding any other entries in the Commercial Register and publications – does not automatically mean that any authorisations that have been granted are terminated or that it is no longer possible to use the Services. In this case, an express revocation of the authorisation is required or a specific request for blocking must be made. In the event of the Client's death, GKB shall have the right to place restrictions on the disposal of the deceased Client's assets and block access to Services.

### **1.8 Bank-client confidentiality and data protection.**

The User is aware that Swiss bank-client confidentiality applies only within Switzerland and that any data sent and/or stored outside Switzerland will not enjoy this protection.

The User is aware that data is transmitted via an open network that is accessible to the

public. Data may thus be transmitted across borders, unchecked, even if both sender and recipient are in Switzerland. The User also accepts that information from GKB which the User receives separately via electronic communication channels (e.g. e-mail, SMS, push notification) is generally unencrypted, which means that bank-client confidentiality and data protection are not guaranteed. Even in encrypted transmissions, the sender and recipient are not encrypted. Third parties may therefore be able to see that a banking relationship exists.

The downloading, installation and use of apps provided by GKB on an end device create points of contact with third parties (including the operator of the App Store). They may indicate that a client relationship exists with GKB. Third parties (e.g. device manufacturers, network operators) may be able to draw conclusions about the existence of a business relationship with GKB. Data transmissions may cross international borders, even if the User is located in Switzerland. The User acknowledges this and releases GKB from its duty of confidentiality in this respect.

By activating technical interfaces, the Client consents to GKB exchanging data (e.g. account information) with the third-party providers they have activated. Third-party systems may be located abroad and the ex-

change may not use end-to-end encryption. The Client releases GKB from the obligation to maintain bank-client confidentiality and any other confidentiality obligations in this regard.

### **1.9 Foreign jurisdictions/import and export restrictions.**

The offering of Services to Users abroad may be subject to restrictions under local laws, with consequent limitations on the Services provided. GKB shall be entitled to modify, limit, or discontinue the range of Services available abroad at any time and without prior notice.

The User acknowledges that they may under certain circumstances be contravening rules of their country of domicile, including, for example, sanctions or current restrictions on imports or exports (particularly as regards the authentication keys or encryption algorithms contained therein), or other foreign legislation, by using Services from outside Switzerland. It is the User's responsibility to ascertain the situation. If in doubt, the User should refrain from using Services or importing/exporting authentication keys. GKB disclaims all liability in this respect.

### **1.10 Reservation of statutory provisions.**

Any statutory provisions governing the operation and use of telecommunications equipment and networks are reserved.

### **1.11 Fees.**

GKB charges a fee for the individual Services based on the list of fees, which is available for viewing at any time. The fees and changes in fees will be notified in a suitable manner.

The Client will be notified of any such changes in writing or in another suitable manner. They shall be deemed approved unless the Client gives notice of termination for the product or Service in question within 30 days of notification. Any notice or withdrawal periods specified in special conditions or agreements are reserved.

GKB has the power to debit an account of the Client's with any charges that may be applicable.

### 1.12 Termination.

The Client, the Client's authorised representative as indicated in the list of authorised signatories at GKB, and GKB may terminate any or all GKB electronic Services at any time without notice. Unless otherwise instructed by the User, GKB shall be entitled, but not obliged, to process pending orders at the time of termination. GKB is also authorised to remove access to Services without prior notice if the User has not used them for twelve successive months.

### 1.13 Contact.

Information about the Client Service for electronic Services is provided on the websites of the respective Services. The Client Service is available during normal business hours and during the service times indicated on the website.

### 1.14 Amendments to these Conditions.

GKB reserves the right to change these Conditions, those of the respective Services, the range of Services offered and any conditions shown on GKB's website at any time. The Client will be informed in advance in writing or in another suitable manner. If the Client does not object within 30 days of notification

in writing or another form demonstrable by text, the changes shall be deemed approved.

If the Client objects, they may terminate the business relationship with immediate effect. Any notice or withdrawal periods specified in special conditions or agreements are reserved.

Any amendment to these Conditions shall always take effect the next time the Service is used after the change has come into effect.

The latest version is available on the internet ([gkb.ch/rechtlichehinweise](http://gkb.ch/rechtlichehinweise)).

## 2. Special Conditions for the Use of e-Banking Services and Technical Interfaces.

### 2.1 Scope and Services offered.

The Special Conditions are in addition to and/or amend the General Terms and Conditions for the use of the electronic Services and apply to all e-Banking Services provided by GKB.

The various e-Banking Services offered by GKB are described in the relevant product brochures and on the GKB website.

The User can activate technical interfaces (e.g. application programming interfaces) in accordance with the Services agreed with GKB. Through these technical interfaces, the User can connect to and use software or other third-party services (e.g. connection to financial applications or banking platforms) in conjunction with the Services provided by GKB (e.g. e-Banking). The Client consents to data being exchanged and displayed via these interfaces and platforms, including in particular account information (e.g. IBAN, account holder, account balance and transactions). Depending on the range of Services provided, these interfaces may also be used to receive or forward instructions (e.g. payment orders). GKB may assume that the instructions are correct and have been issued by authorised persons. The Client is responsible for access to the systems of GKB or third parties and shall not hold GKB liable for any loss or damage or claims by third parties.

GKB reserves the right to make changes to its range of Services.

## 2.2 Technical access.

Technical access to the e-Banking Services is over the internet or app, via a provider selected by the User or through any other new communication media.

Access to e-Banking Services and/or technical interfaces is granted to those who have identified themselves during use by entering their personal details (e.g. contract number) or by using financial software as well as by entering security features (e.g. password, password supplement, PIN or biometric authentication).

GKB uses mobile device technology for the biometric check. GKB cannot influence or control this technology and cannot view the biometric data stored on the mobile device. Accordingly, the authorised User must ensure that they are the only person whose biometric data is stored on the mobile device. The authorised User must also protect their mobile device against third-party access and deactivate the GKB mobile banking app immediately if their mobile device is lost.

## 2.3 Stock market orders.

As a general rule, stock market orders can be entered by a User in GKB e-Banking at any time. **However, stock market orders cannot be processed at all times or always immediately after being entered.** The hours of operation are published on [gkb.ch](http://gkb.ch) or can be obtained from the GKB Client Service.

Before placing a stock market order, the User undertakes to consult the current version of

the “Risks involved in trading financial instruments” brochure as well as the information on risk provided for the e-Banking Services. The “Risks involved in trading financial instruments” brochure has been published at [gkb.ch/risiken-in-handel-mit-finanzinstrumente](http://gkb.ch/risiken-in-handel-mit-finanzinstrumente) and may be obtained in hard copy from GKB.

If the User issues stock market orders, the User shall comply with the relevant standards governing the transaction and applicable to the stock exchange concerned. The User confirms that they are familiar with the usual terms and established practices and in particular with the structures and **risks of the individual financial instruments**. The User acknowledges that where a stock market order is issued via e-Banking, GKB is unable to check whether the financial instrument to which the transaction relates is appropriate or suitable for the Client. This shall apply in particular to stock market orders issued by the Client on their own initiative and **without individual advice** from GKB and executed by GKB as “**execution only**” transactions. In “execution only” transactions, the User and GKB expressly waive any explanations, suitability tests and appropriateness checks by GKB. This information is only provided here and will not be repeated at the time of such transactions. If individual advice is required, the client advisor should be contacted.

## 2.4 Secure communication channel.

Users can use the e-Banking Services of GKB to communicate with GKB via a secure communication channel. Messages from the User to GKB are processed during GKB’s normal business hours. If offered, the User may also send documents to GKB digitally. GKB uses the secure communication channel for example for product and service information, offers, recommendations, surveys, safety news, events, competitions and general communications.

The e-Banking Services may include functions that enable the User to activate the use of an electronic communication channel not operated by GKB (e.g. e-mail, text messages, push notifications). Communication via such channels is generally unencrypted.

The User is responsible for storing notifications and documents received electronically or for saving them outside of the e-Banking Services. The User acknowledges that GKB is entitled to delete notifications and documents in the e-Banking Services once the maximum available storage space has been reached or after a defined period of time has elapsed.

The User acknowledges that the notifications are not available for stock market and payment orders nor for time-critical matters in

general. The Client must use the standard functions and/or the channels provided for this purpose.

Notifications from the Bank shall be deemed to have been duly delivered when they are stored in the Client's inbox. The Client undertakes to take note of the notifications addressed to them in a timely manner.

### **3. Specific provisions for automated categorisation of transactions.**

#### **3.1 Scope.**

These provisions govern the legal relationship between GKB and Clients who use automated categorisation of transactions (hereinafter referred to as "Categorisation"). They supplement and/or amend the General Terms and Conditions Governing the Use of Electronic Services and the Special Conditions for the Use of e-Banking Services.

#### **3.2 Services offered.**

Categorisation is part of electronic Services. It helps Clients manage their finances. Transfers and payments by debit and credit card are assigned to specific categories, and income and expenses are displayed graphically, which helps to keep personal budgets and

savings goals in mind. Clients can adjust the expense categories to suit their needs, add their own information to transactions and search according to various criteria. If the Client does not agree to the use of automated transaction Categorisation, they acknowledge that they cannot use the e-Banking and mobile banking Services.

#### **3.3 Data protection.**

For the automated Categorisation of transactions, GKB uses the technical infrastructure of an external service provider, which is subject to the duty of confidentiality. GKB does not forward any data to this provider or any other external service providers that could in any way allow conclusions to be drawn about the identity of persons.

GKB is entitled to process this data to support the Client's financial management and for its own purposes, in particular for risk management and marketing purposes, and to augment it with other data known to GKB concerning the Client in question.

### 3.4 Credit card details.

Principal card holders and additional card holders have consented to the use of their credit card data for Categorisation purposes, unless they have explicitly revoked their consent given to Visa Card Services AG. Card holders can only see their own data unless the additional card holder has consented to their data being shown to the principal card holder and/or vice versa. The credit card data transmitted by Visa Card Services AG are treated by GKB in the same way as data the Client provides directly to GKB.

### 3.5. Liability.

As Categorisation is largely automated, individual information or assignments may be subject to errors. GKB accepts no liability for the data and analyses displayed within Categorisation being accurate, complete or up to date. This also applies to data and information relating to credit card transactions transmitted by Visa Card Services AG. They are outside the control of GKB.

The information provided by Categorisation does not constitute advice, nor does it constitute an invitation to or recommendation for transactions or investments. GKB accepts no liability for decisions taken by the Client based on Categorisation.

GKB accepts no liability for the availability or integrity of content stored by its Clients. Saving illegal content is not allowed. GKB reserves the right to delete such content without prior notice.

### 3.6 Amendments.

GKB is entitled to change the functional scope of Categorisation at any time without prior notice.

### 3.7 Revocation of the provision of credit card data.

As a cardholder, the Client can revoke the transfer of credit card data by Visa Card Services AG. In this case, Visa Card Services AG will no longer transmit any transaction data to GKB. The analysis and processing of data within the scope of electronic Services will thereafter take place without credit card data. The Client acknowledges that cancellation of the credit card by the principal card holder will always result in the credit card data of any additional card holders no longer being transmitted to GKB.