Data Privacy Policy

Our privacy policy describes what personal data neon Switzerland AG collects about you and otherwise processes when you use the neon app. Personal data is any information relating to an identified or identifiable natural person. This personal data is protected by data protection law and, in certain circumstances, through bank customer confidentiality.

Your personal data is only transmitted to third parties if this is necessary for the purpose of contract processing, if you have given your prior consent or if legal provisions permit or require this.

We inform you that the transfer of data via the internet (e.g. through communication by email) can involve security vulnerabilities. Absolute protection of the data against access by third parties is not possible.

This policy may be updated at any time, and we will always notify you of any changes. The current version of the privacy policy is available here as a PDF file.

1. Responsible party
When you use the neon app, your personal data is collected, processed and used by:

neon Switzerland AG, Badenerstrasse 557, 8048 Zurich, Switzerland («neon»), email: help@neon-free.ch. More information about neon is provided in the legal notice of our price list.

2. Scope and definition

This data privacy policy applies only to the use of the neon app and any personal information that may be collected and stored, for example as part of notified recording of telephone conversations with our employees, in order to comply with our legal obligations or for neon's business purposes.

This data privacy policy explicitly does not apply to:

- Visiting and the use of the neon website. Further information on data protection relating to the use of the neon website can be found in the applicable data privacy policy on our website;

- other websites to which you will be directed via a link.

If you only use our services for informational purposes, or do so without a bank account, we do not collect any personal data, with the exception of data that your browser or end device transmits to facilitate your visit to our website.

3. Legal bases for data processing
We collect, process and use your personal data in a lawful way and in good faith. Depending on the respective purpose of the data processing, neon processes your personal data on the following legal bases:

a. Contractual obligations
neon processes personal data with primary priority as part of initiating or executing contracts with you, in particular to manage, run, maintain and improve the neon app and services offered on it.

b. Legal obligations
neon is required to comply with applicable laws and may be required by law or an official order to provide information, report your personal data or hand over your personal data.

c. Safeguarding legitimate interests
Where required, neon processes your personal data for purposes not related to the actual performance of the contract, in order to safeguard its own legitimate interests or those of third parties, e.g. to monitor and control money laundering and other operational risks, for planning, product development and statistical purposes, for marketing and market research purposes, to provide adequate information about neon's range of services and to safeguard and secure neon's claims if any receivables are owed to neon or to you, and to ensure your safety and that of neon's employees.

d. Consent
For further processing purposes not related to the actual performance of the contract (e.g. sending newsletters), the processing of your personal data can be based on your consent, which you can withdraw at any time.

4. Which personal data does neon collect and process?
neon endeavours to only store as much data concerning you as we require to be able to offer you the complete range of features at the highest possible security level. neon collects and processes personal data so that we are able to offer you use options in accordance with the contract. Your personal data will only be shared with third parties if we are legally obliged to do so, if you have given your prior consent to this, or if these third parties are able to assert a legitimate interest. We need your explicit consent for additional offers that require your personal data to be further processed. This applies in particular to the use of mobile payment solution providers.

a. neon app login
After registering via neon or Hypothekarbank Lenzburg AG, you can then log in to the app using the contract number or your email address and a login code.

b. Identification via fingerprint and facial recognition
The neon app allows you to log in using fingerprint and facial recognition if the device you are using supports this function. In this case, neither neon nor the neon app will receive your biometric data. If you require further information on how identification by fingerprint or facial recognition works, please contact the relevant provider of this function.

c. Data collection and processing when opening and using a neon bank account
Master data. The following personal data is collected, used, processed and stored during onboarding for the purpose of opening a neon bank account with Hypothekarbank Lenzburg AG and using neon services:

- First and last name
- Date of birth
- Place of birth / place of origin
- Gender
- Marital status
- Email address
- Nationality
- Home address
- Mobile phone number
- Sound and image recordings (e.g. telephone calls or picture or video recordings)
- Commercial ownership & use
- Tax domicile and US tax liability
- Copy of ID document
- Type of ID document
- Date issued
- ID number.

Account management. The neon app displays your personal data such as your account details, IBAN, name, email address, mobile phone number and home address.

Transactions and card transactions. The neon app enables you to transfer money (including transfer, recurring payment, direct debit) or withdraw money, receive credit balances, always have an up-to-date overview of your account and pay with your neon card (collectively referred to as "transactions"). The data entered or otherwise received for a transaction is transmitted in encrypted form to and from Hypothekarbank Lenzburg AG. neon stores the following data in order to be able to display the information in the neon app and to offer all neon app functions: data entered during a transaction, which vary depending on the type of transaction (your IBAN and the data of the counterparty: Name, account number/ IBAN/ BIC, address, reference number if applicable), additional data if applicable such as «Merchant Category», location of the «Point of Sale», location of the ATM, amount and currency, posting text (free text field with additional information such as payment purpose if applicable), posting date, status, type of transaction (card payment, transfer, direct debit/debit etc.), and transaction data exchanged via the interfaces (transaction ID, name of the bank, bank code, location of the bank, date of the transaction order, type of transaction, date of execution of the transaction, amount of the transaction incl. currency, credit balance of the account after execution of the transaction, success of the execution of the transaction, fees incurred for the transaction at the bank), collectively referred to as «transaction data».

The neon app provides an overview of all transactions that are performed using your neon app and the neon bank account with Hypothekarbank Lenzburg AG. In all cases, neon stores the transaction data of all transactions in encrypted form.

Closing your account. If you close your neon bank account with Hypothekarbank Lenzburg AG, neon will continue to store your customer data for a period of five years in order to prevent misuse.

Properly uninstalling the neon app will result in all data generated by the neon app locally on your device being deleted. Should you request it, we subsequently erase all personal data (name, address, transactions, etc.) from productive systems, if permitted by law.

With respect to data stored by unstructured means, such as tickets for questions relating to technical issues or data that has been backed up, neon cannot guarantee complete erasure.

Notifications. If you use the neon app, you will be able to activate the «Notifications» feature to receive current information about your account, such as transactions (credits and debits), budget alerts and account balance updates. To use this feature, neon requires the login code of your neon bank account, which is stored in a secure data centre. This function uses the Apple Push Notification Service provided by Apple Inc. («Apple»), the Google Cloud Messaging Service from Google Inc. («Google») or the HUAWEI Push Service from Huawei Device Co., Ltd. («Huawei»). If you use SwatchPay or GarminPay, the relevant terms and conditions of these providers shall apply. If you require further information on how these functions operate, please contact the relevant provider of the function. Neon will send you a relevant notification compatible with the operating system of your device. Notification will in all cases be transmitted in encrypted form.

d. Identification procedure

Hypothekarbank Lenzburg AG is legally bound to verify your identity via a valid identification document when you open an account and to store certain details of the identification document. For this purpose, we offer you digital identification options that are carried out in accordance with the criteria of FINMA Circular 2016/7 «Video and Online Identification» («FINMA RS») of the Swiss Financial Market Supervisory Authority FINMA («FINMA»). Although the user generally has a choice between online and video identification, in certain cases neon may prescribe the method.

Video identification is performed on behalf of neon and Hypothekarbank Lenzburg AG by Intrum AG, Eschenstrasse 12, 8603 Schwerzenbach (hereinafter «Intrum»). Identity is verified by means of a web-based video identification procedure using an encrypted transmission channel.

On completion of the video identification procedure, Intrum will send you a text message containing a «transaction number» or «TAN». As instructed by Intrum, you confirm the correctness of the data that you have entered in the app via the entry field provided, as well as your identity, and you accept the respective GTCs and contractual conditions of Hypothekarbank Lenzburg AG, neon and Intrum.

Online identification is carried out by Hypothekarbank Lenzburg AG. which also relies on services provided by Intrum. Your identity is confirmed, in part, using an electronic copy of your identification document transmitted in encrypted form.

Hypothekarbank Lenzburg AG will send you a TAN by text message for online identification. By entering the TAN in the entry field provided by the app, you confirm the correctness of the data that you have entered in the app, as well as your identity, and you accept the respective GTCs and contractual conditions of Hypothekarbank Lenzburg AG, neon and Intrum.

For both procedures (video identification and online identification) neon transfers your personal data (first and last name, date and place of birth, nationality, email address, gender, mobile number, place of residence, preferred language) to Intrum. To verify that the video identification procedure has been carried out correctly, Intrum requires access to the camera on your terminal device and must be able to take photos of you and the front and back of your ID card or the front of your passport and, if applicable, your residence permit. These photos are transmitted to Hypothekarbank Lenzburg AG.

The conversation between you and Intrum is recorded and saved for statutory verification purposes. At the outset of the video identification, Intrum will request your express consent to create photos and record the conversation. Intrum AG transfers the data to Hypothekarbank Lenzburg AG and it is then deleted from Intrum's servers after 90 days at the latest.

To continue with the online identification process, the app must be able to access the back camera on your device so photos of you as well as the front and back of your Swiss identification card or your alien's identity card can be taken. These photos, as well as any discrepancies that we discern between your personal data and details taken from your identification card or passport, will be transferred from Intrum to neon and Hypothekarbank Lenzburg AG. This data will be deleted from Intrum's servers after 90 days at the latest.

For online identification, Intrum is tasked with verifying the authenticity of the identification card or passport that you present. For this purpose, Intrum uses a prescribed electronic process to check the integrity and the respective optical security features of the identification document. If the security features are not clearly visible or if any anomalies should become apparent, the photos taken during this process may be subject to manual checking by Intrum.

Customer support. For customer support, neon uses the systems from the company Freshworks Inc., San Mateo, California. So that neon can always give you the best possible help, the following information is stored exclusively for the purpose of support services: name, first name, email, contract number, product type, language, telephone number. The data thus stored will be stored in a data processing centre in the European Union in accordance with the

applicable contractual data protection provisions. More information is available here. neon keeps a record of all communications between you and our customer support team, whether we communicate by email or chat or telephone, to help improve our ability to assist you with future enquiries.

The 24-hour customer support phone line in connection with use of the card is operated directly via Hypothekarbank Lenzburg AG.

5.   Which data does the neon app produce?

Based on the data indicated above, neon can offer you additional functions. This currently includes automatically categorising your transactions and statistics for your account movements over set periods of time and for set recipients, as well as giving you the option of sending money to other neon customers via the address book feature and mobile payment services.

Categories. neon automatically categorises all your transactions, in particular expenses, for you. The neon app automatically assigns transactions to a certain category (e.g. expenses to «rent», «travel», income to «salary»), e.g. via the account number, the payment reference or the name of the recipient. You can reassign completed transactions to other categories at any time. By assigning transactions to a category, the neon app can assign the total transactions made over a period of time to a specific category on a percentage basis.

Usage data. neon collects, processes, uses and stores data that is generated when using the neon app in order to improve the user experience and prevent misuse. In particular, this includes the IP address, screen resolution and operating system of the device used for the call, the date and time of the call, duration of visit to the site and the content called up during a site visit (collectively «usage data»).

Payments to other neon customers. neon gives you the option of sending money to other neon customers in a straightforward way. These are called «peer-to-peer-payments». If you want to do this, the neon app asks you whether you want to allow access to your address book so that other customers can be found using their telephone number.

«Invite friends». neon gives you the option to invite your friends to neon. After a successful invitation, the name of the inviter and the invited person can be displayed to the other customer (e.g. as details of a payment effected by neon). To this extent, I agree to the disclosure of my personal data to the invitee or the invited person and release neon from its confidentiality obligations in this respect.

Mobile payment services. To be able to use mobile payment services from Google, Samsung and Apple, your account information is converted into an encrypted token, which is used to authorise payments with these services. Your personal data will be shared with the respective providers of the mobile payment services, as these providers provide the technological basis for this.

6.   Does neon use non-personal (anonymous) data?

Non-personal (anonymous) data, such as statistics concerning the device you are using or transaction data, cannot be used to identify you personally. We use such data to continuously optimise the performance and offerings of the neon app.

7.   What does neon do to protect your personal data?

Communication between neon and Hypothekarbank Lenzburg AG is fully encrypted using the standardised TLS/SSL protocol.

Data security. All transactions are always processed via an interface layer based on a secure application programming interface («Open

API») of Hypothekarbank Lenzburg AG and neon respectively. All bank transaction data is stored at Hypothekarbank Lenzburg AG's data centre or Swiss data centres. These are ISO27001 certified. We are governed by the Swiss Data Protection Act and take appropriate technical and organisational security measures to protect your personal data from unauthorised access and misuse.

8.   How are third-party services used?

As with banks, we rely on the services of carefully selected third parties, such as our data centre. Your personal data is always protected.

Third-party providers. In order to use technical or organisational services provided by third parties that we require in order to meet the purposes set out in this Privacy Policy or for our other business activities, your personal data may be stored in the systems of these service providers, such as your transaction data, which is stored in encrypted form in an ISO27001 certified data centre in Switzerland, but also personal data stored within the customer support systems of Freshworks Inc., San Mateo, California in accordance with the applicable data protection regulations in a data centre in the European Union. Our service providers are bound by the respective data privacy laws and are also contractually obliged to process personal data exclusively on our behalf and in accordance with our instructions. We oblige our service providers to comply with technical and organisational measures to ensure that personal data is protected.

9.   What about analysis services and tracking technologies?

To enable statistical analysis of your usage behaviour, neon uses carefully selected analysis services and tracking technologies from Google. The data collected in this way is anonymised. The only data collected is how the neon app is used, e.g. page views and loading times, but never personal or customer-identifying data or content. The data transmitted to Google is not merged with other Google data. The data collected in this way is exclusively used for troubleshooting and optimising the customer experience.

The collected information about usage of the neon app is transferred to Google servers, generally in Europe, and stored there for a maximum of 14 months (to allow comparison of app performance throughout this period). The data is not used for any other purpose or transferred to third parties.

You can find further information in the data privacy policy and functionalities of Google.

10.   What about emails?

Whenever we send you an email, you have the option to unsubscribe from additional product information or emails – the exception is emails required for maintaining or terminating the customer relationship, e.g. updates to our general terms and conditions («GTC»).

For the purpose of sending emails, neon saves your email address, first name and chosen language and, where necessary, saves customer segment attributes with our service provider who sends the emails. This service provider is contractually bound to provide an adequate level of data protection.

11.   Is my personal data transmitted abroad and how is it protected there?

Notification and transmission of personal data to third-parties carefully selected by us inside and outside of Switzerland takes place if this is necessary to provide services (e.g. for payment orders), if this is required by law (e.g. as part of the automatic exchange of information) or if you have consented to this. neon ensures (e.g. through the use of corresponding standard contractual clauses of the

European Commission) that the recipients of personal data guarantee an adequate level of data protection at all times and wherever located.

As part of providing customer support, all personal data as described in section 4 is stored in a data centre in the European Union via the systems of the company Freshworks Inc., San Mateo, California in accordance with the General Data Protection Regulation (GDPR).

12. Retention period for personal data

We process and store your personal data for the entire duration of the business relationship (from initiation, account opening to termination of a contract) and beyond in accordance with the statutory retention and documentation obligations. It is possible that personal data will be retained for the period during which claims can be asserted against our company and insofar as we are otherwise legally obliged to do so or if legitimate business interests require this (e.g. for evidence and documentation purposes). As soon as your personal data is no longer required for the purposes stated above, it will be deleted or anonymised to the extent possible.

For operational data (e.g. system protocols, logs), shorter retention periods of twelve months or less generally apply.

13. Rights of the data subject

Duty to provide information. Upon request, neon will provide you with information about all personal data stored about you, recipients or categories of recipients who have received personal data about you from us, and the purpose of the data storage. If your personal data that we have stored is not accurate, we kindly ask that you

contact customer support so that we are able to correct it without delay. You have the option of changing any data yourself in the neon app. You also have a right to block, erase or destroy this data. We reserve the right to apply any restrictions provided for by law.

If you have given your consent to the use of data, you can revoke this consent at any time with future effect. Revocation of consent may result in our services no longer being available to you without restriction or the user relationship being terminated. We will inform you in advance of any resulting costs.

Customer support. For help using the neon app or for general questions about this privacy policy and data protection at neon, you can contact our support team anytime at help@neon-free.ch or by post at neon Switzerland AG, Badenerstrasse 557, 8048 Zurich, Switzerland.

14. Entry into force

This Data Privacy Policy is immediately effective. neon reserves the right to make changes to it at any time. You will be notified of these changes by email and they shall be deemed accepted after 30 days in the absence of any objections having been submitted. If no notice of objection is received within this period, beginning at the point upon which the email message is received, the amended terms and applies shall be deemed to have been agreed and accepted.

In the course of the notice of changes to the Data Privacy Policy, neon shall inform the customer separately of their right to object, the objection period and the implication of the customer not raising an objection.

Links in the document:

- neon data privacy policy app: https://www.neon-free.ch/media/neon_app_privacy_policy.pdf

- neon legal notice: http://www.neon-free.ch/de/impressum/

- neon data privacy policy website: https://www.neon-free.ch/media/neon_datenschutz_website_en_de.pdf

- Apple Push Notification Service: https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-de-ww.pdf

- Google Cloud Messaging Service: https://cloud.google.com/terms/data-processing-terms?hl=de

- Huawei Push Service: https://developer.huawei.com/consumer/de/doc/10134

- Freshworks Inc.: https://www.freshworks.com/de/

- Data privacy policy of Freshworks: https://www.freshworks.com/de/dsgvo/

- Data privacy policy and functionalities of Google: https://www.google.com/policies/privacy