

# NOTES ON DATA PROTECTION AT FIDOR BANK AG

I. Privacy policy for the website of Fidor Bank AG

II. Privacy policy for the Fidor Smart Banking App

III. Data protection information on the changes by the PSD2

IV. Data protection information according to Art. 13, 14 GDPR of Fidor Bank AG

## I. PRIVACY POLICY FOR THE WEBSITE OF FIDOR BANK AG

### 1. General information and principles of data processing

We are pleased that you are visiting our website. The protection of your privacy and the protection of your personal data, the so-called personal data, when using our website is important to us.

According to Art. 4 No. 1 GDPR, personal data is all information relating to an identified or identifiable natural person. This includes, for example, information such as your first and last name, your address, your telephone number, your e-mail address, but also your IP address.

Data that cannot be related to your person, such as through anonymization, are not personal data. Processing (e.g. collection, storage, reading, retrieval, use, transmission, deletion or destruction) pursuant to Art. 4 No. 2 GDPR always requires a legal basis or your consent. Processed personal data must be deleted as soon as the purpose of the processing has been achieved and there are no longer any statutory storage obligations to be met.

Here you will find information about the handling of your personal data when you visit our website. In order to provide the functions and services of our website, it is necessary for us to collect personal data about you.

We also explain to them the type and scope of the data processing, the purpose and the corresponding legal basis and the respective storage period.

This privacy policy only applies to this website under the domain [fidor.de](https://fidor.de). It does not apply to other websites to which we merely refer through a hyperlink.

We cannot be responsible for the confidential treatment of your personal information on these third party websites as we have no control over whether these companies comply with the privacy policy. Please inform yourself about the handling of your personal data by these companies directly on these web pages.

## **2. Who is responsible for data processing?**

Responsible for the processing of your personal data is the

**Fidor Bank AG**  
Sandstr. 33  
80335 Munich  
Germany

Head Office: +49 89 189 085 233  
Fax: +49 89 189 085 199

E-mail: [info@fidor.de](mailto:info@fidor.de)  
Internet: [www.fidor.de](http://www.fidor.de)

Represented by the Board of Directors: Boris Joseph, Pascal Cirelli, Stephan Spannagl

## **3. How can you contact our Data Protection Officer?**

If you have any questions regarding data protection, you can also contact our Data Protection Officer at any time:

**Dr. Georg Schröder, LL.M.**  
**Data Protection Officer**

legal data  
Schröder Rechtsanwaltsgesellschaft mbH

Prannerstr. 10  
80333 Munich  
Germany

Tel.: +49 89 954 597 520  
Fax: +49 89 954 597 522

E-mail: [datenschutz@fidor.de](mailto:datenschutz@fidor.de)

## **4. Provision and use of the website / server log files**

### **a) Nature, scope and purpose of data processing**

If you use this website without transmitting data to us in any other way (e.g. by registration or use of the contact form), we collect technically necessary data via server log files, which are automatically transmitted to our server, among other things:

- IP address
- Date and time of the request
- Name and URL of the retrieved file
- Website from which access is made (referrer URL)
- Access status / HTTP status code
- Browser type
- Language and version of the browser software
- Operating system

This processing is technically necessary in order to be able to display our website to you. We also use the data to ensure the security and stability of our website.

### **b) Legal basis**

The legal basis for this processing is Art. 6 Para. 1 lit. f) GDPR. The processing of the mentioned data is necessary for the provision of a website and thus serves the protection of a legitimate interest of our company.

### **c) Storage period**

As soon as the personal data mentioned is no longer required to display the website, it will be deleted. The collection of data for the provision of the website and the storage of data in log files is mandatory for the operation of the website. Consequently, there is no possibility for the user to object to this aspect. A further storage can take place in individual cases, if this is legally prescribed.

## **5. Use of cookies**

### **a) Nature, scope and purpose of the data processing**

We use cookies to facilitate and improve the use of our website. Cookies are small files containing text information that are stored on a computer when a website is visited via the web browser. This serves the recognition of a session, for example when logging in permanently to a website.

Some functions of our website cannot be offered without the use of technically necessary cookies. Other cookies, on the other hand, allow us to perform various analyses. For example, some cookies may recognise the browser you are using when you return to our website and transmit various information to us. We use

cookies to facilitate and improve the use of our website. For example, we can use cookies to make our website more user-friendly and effective for you by, for example, tracking your use of our website and determining your preferred settings (e.g. country and language settings). If third parties process information via cookies, they collect the information directly via your browser. However, cookies do not damage your terminal device. They cannot run programs or contain viruses. Various types of cookies are used on our website, the nature and function of which are explained below.

### **Temporary cookies / session cookies**

So-called temporary cookies or session cookies are used on our website, which are automatically deleted as soon as you close your browser. This type of cookie makes it possible to record your session ID. This makes it possible to assign different requests from your browser to a common session and it is possible to recognize your terminal device during later website visits.

### **Permanent cookies**

So-called permanent cookies are used on our website. Permanent cookies are cookies that are stored in your browser for a longer period of time and can transmit information. The respective storage period varies depending on the cookie. You can delete permanent cookies independently via your browser settings.

### **Third-party cookies**

We use analytical cookies to monitor anonymous user behaviour on our website.

We also use advertising cookies. These cookies can be used to track user behaviour for advertising and targeted marketing purposes.

Social media cookies allow you to connect to your social networks and share content from our website within your networks.

### **Configuration of browser settings**

Most web browsers are preset to accept cookies automatically. However, you can configure your browser so that it only accepts certain cookies or no cookies at all. However, we would like to point out that you may then no longer be able to use all the functions of our website.

You can also delete cookies already stored in your browser via your browser settings. It is also possible to set your browser so that it notifies you before cookies are stored. Since the different browsers can differ in their respective

functionalities, we ask you to use the respective help menu of your browser for the corresponding configuration options.

Disabling the use of cookies may require the storage of a permanent cookie on your computer. If you subsequently delete this cookie, you must deactivate it again if you do not want the use of other cookies.

### **b) Legal basis of data processing**

Due to the purposes described, the legal basis for the processing of personal data using cookies is Art. 6 Para. 1 lit. f) GDPR. If you have given us your consent to the use of cookies on the basis of a notice ("cookie banner") provided by us on the website, the legal basis is also Art. 6 Para. 1 lit. a) GDPR.

### **c) Storage period**

As soon as the data transmitted to us via cookies is no longer required for the purposes described above, this information is deleted. A further storage can take place in individual cases, if this is legally prescribed.

## **6. Use of pixels / partner programs**

### **Tracking pixel**

#### **a) Nature, scope and purpose of data processing**

We also use so-called pixels from various providers and affiliate programs for the purpose of user tracking. Pixels, also called tracking pixels, web beacons or web bugs, are small, invisible files on web pages. Pixels can be used to recognize and share certain types of information on your computer system, such as the contents of cookies, the time and date of a page view, and a description of the page where the pixel is located. A transaction can thus be assigned to a specific publisher or affiliate (see below).

#### **b) Legal basis of data processing**

The legal basis for data processing are our legitimate advertising interests in accordance with Art. 6 Para. 1 lit. f) GDPR. If you have given your consent, the legal basis is Art. 6 Para. 1 lit. a) GDPR.

#### **c) Storage period**

The storage period of the respective tool can be seen in our cookie banner.

## Affiliate networks

### a) Nature, scope and purpose of data processing

We integrate elements (especially advertisements) from partner networks in the field of affiliate marketing into our website. When calling up these advertising banners, the user is redirected to external partner sites.

Affiliate marketing is based on the placement of advertisements from advertising companies (advertisers) on the websites of third parties (publishers). By displaying advertisements from partner sites, we become active as publishers in this sense. The mediation of advertisements from an advertiser to a publisher (both so-called "affiliates") takes place via affiliate networks. Affiliate networks are also responsible for assigning the clicks on advertisers' banner ads to the publisher's pages in order to enable performance-based compensation for the publisher.

For this purpose, the respective affiliate network sets a cookie on the user's end device. With the help of this cookie, the network usually collects the following data: User ID, IDs of the participating partner sites, advertising material ID, time stamp.

The purpose of processing is the handling of commission payments in relation to the affiliate network and advertisers.

If you do not want cookies from affiliate networks to be set, you can set your browser to not accept cookies. In addition, you can delete cookies at any time in the settings of your browser.

Insofar as we use affiliate networks located outside the EU or the EEA, these are obliged to adhere to a data protection standard that essentially corresponds to the European standard on the basis of so-called EU standard contract clauses.

We set links to partner sites from the following affiliate networks:

- **Adcell**  
(Firstlead GmbH, Rosenfelder Str. 15-16, 10315 Berlin)  
Privacy policy:  
<https://www.adcell.de/datenschutz>
- **Admitad**  
(Admitad GmbH, Lise-Meitner-Str. 8, 74074 Heilbronn)  
Privacy policy:  
<https://account.admitad.com/de/privacy/>
- **Adtraction**  
(Adtraction Deutschland GmbH, Eichhornstraße 3, 10785 Berlin)  
Privacy policy:  
<https://adtraction.com/about-us/privacy-policy>

- **AWIN**  
(AWIN AG, Eichhornstraße 3, 10785 Berlin)  
Privacy policy:  
<https://www.awin.com/de/datenschutzerklärung>
- **a-net**  
(The a-net GmbH, Oskar-von-Miller-Ring 20, 80333 Munich)  
Privacy policy:  
<https://www.the-a-net.com/imprint>
- **communicationAds**  
(communicationAds GmbH & Co. KG, Karlstraße 9, 90403 Nuremberg)  
Privacy policy:  
<https://www.communicationads.net/aboutus/privacy/>
- **financeAds**  
(financeAds GmbH & Co. KG, Karlstraße 9, 90403 Nuremberg)  
Privacy policy:  
<https://www.financeads.net/aboutus/datenschutz/>
- **Financequality**  
(netzeffekt GmbH, Theresienhöhe 28, 80339 Munich)  
Privacy policy:  
<https://www.financequality.net/datenschutz/>
- **Impact Radius**  
(Impact Tech, Inc., Empire State Building, 350 Fifth Avenue, 36th floor, New York, NY 10118, USA)  
Privacy policy:  
<https://impact.com/privacy-policy/>
- **Moneytrax**  
(Moneytrax GmbH, Max Bruch Str. 4, 80939 Munich)  
Privacy policy:  
<https://moneytrax.net/datenschutz/>
- **NetSlave**  
(NetSlave GmbH, Simon-Dach-Str. 12, 10245 Berlin)  
Privacy policy:  
<https://www.netslave.de/datenschutz-2019.html>

With regard to the affiliate network financeAds, we act both as a publisher and as an advertiser. This means that we do not only publish advertisements of partners on our website, but also place advertisements on partner sites ourselves. We therefore also set cookies on our website in order to recognize the user on partner sites and to be able to send him our offers there.

## **b) Legal basis of data processing**

The legal basis for data processing are our legitimate advertising interests in accordance with Art. 6 Para. 1 lit. f) GDPR.

## **c) Storage period**

The data collected by the affiliate networks is not processed by us.

The cookie we set within the financeAds network has a duration of 60 days.

## **Further partner programs / direct cooperations**

### **a) Nature, scope and purpose of data processing**

In addition, we also link to partner sites without the use of affiliate networks. In this case, the external partner is informed via the link that the user has been forwarded from our site. Other data is not transmitted to the partner site, but is collected directly on the partner site after the redirection, e.g. the IP address of the user. The purpose of the processing is again to enable performance-based remuneration from us as a publisher.

In case of direct cooperation, your data entered with one cooperation partner may also be made available to the other cooperation partner in order to fulfill the purpose of the cooperation. We enter into cooperations with partner sites in such cases if we wish to link our services to the offerings of third parties, e.g. by placing our products on the platform of a third party and enabling a transaction with us directly on the third party platform. We can be both the data transmitting and the data receiving cooperation partner.

We are involved in direct cooperations with the following partner sites:

- **Affiliate School**  
(Inh. Christopher Hauffe, Aachener Straße 113, 40233 Düsseldorf)  
Privacy policy:  
<https://www.affiliateschool.de/datenschutz/>
  
- **Amazon**  
(Amazon Europe Core S.à.r.l., 38 avenue John F. Kennedy, 1855 Luxembourg)  
Privacy policy:  
[https://www.amazon.de/gp/help/customer/display.html?ie=UTF8&nodeId=201909010&ref\\_=footer\\_privacy](https://www.amazon.de/gp/help/customer/display.html?ie=UTF8&nodeId=201909010&ref_=footer_privacy)



- **Cryptotax**  
(21 Consulting GmbH, Hauptstraße 72, 82380 Peißenberg)  
Privacy policy:  
<https://cryptotax.io/datenschutz/>
- **Currencyfair**  
(CurrencyFair Limited, Head Office, Colm House, 91 Pembroke Road, Ballsbridge, Dublin 4, D04 EC42 Ireland)  
Privacy policy:  
<https://www.currencyfair.com/trust/privacy-policy/>
- **DPV**  
(DPV Deutscher Pressevertrieb GmbH, Am Baumwall 11, 20459 Hamburg)  
Privacy policy:  
<https://www.dpv.de/datenschutz>
- **Finanzcheck**  
(FFG FINANZCHECK Finanzportale GmbH, Admiralitätstraße 60, 20459 Hamburg)  
Privacy policy:  
<https://www.finanzcheck.de/uber-uns/datenschutz/>
- **Optiopay**  
(OptioPay GmbH, An den Treptowers 1, 12435 Berlin)  
Privacy policy:  
<https://www.optiopay.com/privacy-policy/>
- **Remind.me**  
(remind me GmbH, Torstraße 19, 10119 Berlin)  
Privacy policy:  
<https://www.remind.me/internal/datenschutzerklaerung>
- **Sumup**  
(SumUp Limited, Block 8, Harcourt Centre, Charlotte Way, Dublin 2, D02 K580 Ireland)  
Privacy policy:  
[https://sumup.de/datenschutzbestimmungen/?fcam\\_rc=bbc8c8qwmu7hcofwn0a35c7lk](https://sumup.de/datenschutzbestimmungen/?fcam_rc=bbc8c8qwmu7hcofwn0a35c7lk)
- **VÖB**  
(VÖB-Service GmbH, Godesberger Allee 88, 53175 Bonn)  
Privacy policy:  
<https://www.voeb-service.de/kontakt/datenschutz/>

## b) Legal basis of data processing

The legal basis for data processing are our legitimate advertising interests in accordance with Art. 6 Para. 1 lit. f) GDPR. If you have given your consent, the legal basis is Art. 6 Para. 1 lit. a) GDPR.

### **c) Storage period**

The data collected by the partner sites is not processed by us.

As far as we receive data entered by you from partner sites, the respective storage periods described in this privacy policy apply.

## **7. Data collection for the implementation of pre-contractual measures and for the fulfilment of contracts**

### **a) Nature scope and purpose of data processing**

In the pre-contractual area and at contract conclusion we collect personal data about you. This applies, for example, to first and last name, address, e-mail address, telephone number or bank details.

Furthermore, we also use your personal data within the scope of identification and TAN procedures, in particular within the scope of the so-called pushTAN procedure, in which a pushTAN is sent to your smartphone for the identification and protection of a transaction. The data transfer of the pushTAN is performed via a separate app on your smartphone.

The processing of your personal data for the purpose of contractual performance is also explained in detail in IV. – Data protection information according to Art. 13, 14 GDPR of Fidor Bank AG.

### **b) Legal basis of data processing**

We collect and process this data exclusively for the purpose of executing the contract or fulfilling pre-contractual obligations. The legal basis for this is Art. 6 (1) (b) GDPR. If, in addition, you have given your consent, the additional legal basis is Art. 6 Para. 1 lit. a) GDPR.

This applies in particular to the processing of your personal data in connection with the delivery of a pushTAN.

### **c) Storage period**

The data shall be deleted as soon as they are no longer necessary for the purpose of their processing.

In addition, there may be legal storage obligations, for example commercial or fiscal storage obligations according to the German Commercial Code (HGB) or the German Tax Code (AO). If such storage obligations exist, we block or delete your data at the end of these storage obligations.

## **8. Registration option**

### **a) Nature, scope and purpose of data processing**

You can register on our website. When you register, we collect and store the data you enter in the input mask (e.g. last name, first name, e-mail address). Your data is not passed on to third parties.

Your registration is required for the use of certain content and services on our website or for the performance of a contract or for the implementation of pre-contractual measures. After registration, you are free to modify the personal data provided during registration at any time or - subject to statutory retention obligations - to have them completely deleted from our database.

### **b) Legal basis of data processing**

In the case of consent, the legal basis for processing is Art. 6 Para. 1 lit. a) GDPR. If your registration serves to prepare the conclusion of a contract, Art. 6 Para. 1 lit. b) GDPR is the additional legal basis.

### **c) Storage period**

The data collected during registration are stored by us as long as you are registered on our website and are then deleted. Legal retention periods remain unaffected. In addition, your registered personal data will be deleted if you delete your user account on our website. If your registration data and other data are necessary for the performance of a contract to which you are a party, or for the implementation of pre-contractual measures, the data will only be deleted when they are no longer required for the performance of the contract or the implementation of pre-contractual measures.

## **9. Application possibility**

### **a) Nature, scope and purpose of data processing**

You can apply on our website or by e-mail. When you apply, we collect and store the data that you enter into the input mask or that you send us by e-mail.

### **b) Legal basis of data processing**

We process your data only for the purpose of processing your application. A passing on to third parties does not take place. The legal basis for the processing is Art. 88 Para. 1 GDPR in connection with § 26 BDSG (German Federal Data Protection Act) and additionally Art. 6 Para. 1 lit. b) GDPR.

If you give us your consent to be included in our applicant pool, the legal basis is Art. 6 Para. 1 lit. a) GDPR.

### **c) Storage period**

If we are unable to offer you a job, we will store your data for a maximum of six months after completion of the application process, taking into account Section 61b Para. 1 ArbGG (German Law on Employment) in conjunction with Section 15 AGG (General Equal Treatment Act). The start of the period is the date of receipt of the lit. of notice of rejection.

If you have given us your consent to be included in our applicant pool, we will store your data for a maximum of two years.

### **d) Data transfer**

Your data will only be sent to those departments that are involved in the decision (responsible personnel or specialist departments, management, works council).

Other data recipients may be those for whom you have given us your consent for data transmission.

## **10. Comment function**

### **a) Nature, scope and purpose of data processing**

On our website you can write and comment articles. If you write or comment on a contribution, we collect and store the data you enter in the input mask. In addition to the comments you leave, we also store and publish information about the time you enter your comments and any user names (pseudonyms) you have chosen. Furthermore, the IP address assigned to the person concerned by the Internet Service Provider (ISP) is stored. Your data is not passed on to third parties.

The processing of the data transmitted by you (e.g. the IP address) is necessary to display your comment on our website. Besides, the processing serves security purposes, e.g. in the event that the person concerned violates the rights of third parties by submitting a comment or posts illegal content.

This collected personal data will not be passed on to third parties unless such a passing on is prescribed by law or serves the legal defence of the controller.

### **b) Legal basis of data processing**

The legal basis for the processing of personal data transmitted when using the comment function is Art. 6 Para. 1 lit. a) GDPR, if and to the extent that you have given your consent. You can revoke this consent at any time. The legality of the data processing operations that have already taken place remains unaffected by the revocation. Another legal basis is Art. 6 Para. 1 lit. f) GDPR.

We have a legitimate interest in the processing if third party rights are violated or illegal content is posted. This serves the security, if someone writes illegal contents in comments and contributions (insults, forbidden political propaganda etc.).

### **c) Storage period**

The comments and the associated data (e.g. IP address) are stored and remain on our website until the commented content has been completely deleted or the comments have to be deleted for legal reasons.

## **11. Contact options by e-mail**

You can contact us via e-mail on our website.

### **a) Nature, scope and purpose of data processing**

You can contact us by e-mail. Our data collection is limited to the e-mail address of the e-mail account used by you to contact us and to the personal data that you have made available to us at any time during the contact process. The purpose of the data processing is the possibility to answer your request properly.

### **b) Legal basis of data processing**

The legal basis for this is Art. 6 Para. 1 lit. f) GDPR. We have a justified interest in the processing of the above-mentioned personal data in order to be able to process your request properly.

### **c) Storage period**

The duration of the storage of the above data depends on the background of your contact. Your personal data will be deleted on a regular basis if the purpose of the communication no longer applies and storage is no longer necessary. This can result, for example, from a processing of your request. If the contents of your email are subject to a contractual relationship, longer statutory retention periods may apply.

## **12. Data processing for the fulfilment of legal obligations and for our own legitimate purposes**

### **a) Nature, scope and purpose of data processing**

In addition, personal data may be passed on to consultants (e.g. lawyers, tax consultants) or the criminal prosecution authorities or processed internally to ensure the functionality and security of the IT systems.

In addition, we may be obliged to pass on your data to other public authorities and institutions (e.g. prosecutor's office, police, supervisory authorities, tax office, social insurance agencies, etc.).

The purpose of processing is the assertion or defence of legal claims, the prevention and prosecution of criminal offences and the guarantee of IT security.

In addition, processing may be aimed at the fulfilment of legal obligations.

### **b) Legal basis of data processing**

The legal basis of the processing is Art. 6 Para. 1 lit. f) GDPR according to our legitimate interest in the performance of the above-mentioned purposes.

Insofar as there is a legal obligation to disclose, the legal basis is Art. 6 Para. 1 lit. c) GDPR.

### **c) Storage period**

The data will be deleted immediately after the purpose has been achieved, subject to statutory storage obligations and further processing mentioned in this data protection declaration.

## **13. Newsletter**

### **a) Nature, scope and purpose of data processing**

On our website you have the possibility to subscribe to a free regular e-mail newsletter in order to send you the newsletter regularly, we need your e-mail address from you.

In connection with the newsletter dispatch a passing on of your data takes place if necessary to our newsletter service provider who is active in the way of the order processing for us. Your data is not passed on to third parties.

For the newsletter dispatch we use the so-called double opt-in procedure.

This means that we will not send you an e-mail newsletter until you have expressly confirmed that you agree to receive the newsletter. We will then send you a confirmation e-mail asking you to confirm that you wish to receive future newsletters from us by clicking on the appropriate link.

This serves to ensure that only you yourself as the owner of the e-mail address provided can register for the newsletter. Your confirmation must be sent promptly after receipt of the confirmation e-mail, otherwise your newsletter subscription will be automatically deleted from our database.

When you subscribe to the newsletter, we collect and store the data you enter in the input mask (e.g. last name, first name, e-mail address).

When you register for the newsletter, we also save your IP address entered by the Internet Service Provider (ISP) as well as the date and time of registration in order to be able to track any possible misuse of your e-mail address at a later point in time. In the confirmation e-mail sent for control purposes (double opt in the e-mail), we also store the date and time of the click on the confirmation link and the IP address registered by the Internet Service Provider (ISP).

The data collected by us when registering for the newsletter will be used exclusively for the purpose of advertising the newsletter.

## **b) Legal basis of data processing**

In accordance with Art. 6 Para. 1 lit. a) GDPR and § 7 Para. 2 No. 3 UWG (German Unfair Competition Act), the processing of your e-mail address for newsletter dispatch is based on the declaration of consent voluntarily given by you in the following and revocable at any time for the future. In addition, the processing is based on Art. 6 Para. 1 lit f) GDPR due to legitimate interests of us to document the evidence of the necessary consent.

## **c) Storage period**

Your e-mail address will be stored as long as you have subscribed to the newsletter. After unsubscribing from the newsletter your e-mail address will be deleted unless you have expressly consented to further use of your data or another legal basis for data processing applies.

## **14. Social Media Platforms**

We also integrate social media platforms partly via links behind the respective logo graphics of the provider of the social media platform. Here, no data is automatically transferred to the providers, but only when you want to switch to the social media platform and actively click on the link. We have no influence on which data is collected and transmitted and how the providers process or use it.

If you are logged in to your user account on a social network when you access our profile page, the operator of the social network may be able to assign the information collected during your visit to your personal account. If you want to avoid that the collected information can be directly assigned to your user account, you have to log out of the respective social network before accessing our profile page.

If you access our profile page on a social network, the operator of the social network can also set cookies on your end device, regardless of whether you have an account with the network or whether you are logged in there. Cookies are data packets that mark the user's end devices with a specific identifier. Cookies are set primarily to enable us to display personalised advertising to visitors to social networks, including our profile pages. This is done, for example, by showing the user ads on social network pages from social network advertising partners whose websites the user had previously visited. Cookies also enable us to compile statistics on the use of our profile page (e.g. number of page views, user categories). If we receive such statistical analyses from the operator of the social network, the data is previously anonymised by the operator, i.e. it is not possible for us to assign usage data to an individual user.

The purpose of processing your data on our profile page with the respective social network is to inform you about our offers and services and to answer any enquiries on our profile page. The legal basis for the processing is Art. 6 Para. 1 lit. f GDPR. In this respect, public relations work is covered by our legitimate interests within the meaning of the provision.

Private messages that you send us via social networks will be deleted after 2 years after the last communication with you. Public posts from you (e.g. in our timeline) will always remain permanently published until you explicitly request their deletion.

In accordance with the case law of the European Court of Justice, we are jointly responsible with the operator of the respective social network for the operation of our profile page and the inclusion of social plugins with regard to compliance with data protection regulations. Within this framework, the operator of the social network provides the corresponding IT infrastructure as well as the social network website and is basically the primary contact person when it comes to processing your data on the social network pages (e.g. information or deletion). However, you can also assert your legal rights against us. In this case we will forward your requests to the operator of the social network.

Social media platforms that we integrate in this way are currently:

- **Facebook**



Provider: Facebook Ireland Limited,  
4 Grand Canal Square, Dublin 2 D02 X525, Ireland  
<https://www.facebook.com/about/privacy/>

- **Twitter**

Provider: Twitter International Company,  
One Cumberland Place, Fenian Street, Dublin 2 D02 AX07, Ireland  
<https://twitter.com/de/privacy>

- **Instagram**

Provider: Facebook Ireland Limited,  
4 Grand Canal Square, Dublin 2 D02 X525, Ireland  
<https://help.instagram.com/519522125107875>

- **YouTube**

Provider: Google Ireland Limited,  
Gordon House, Barrow Street, Dublin 4 D04 E5W5, Ireland  
<https://policies.google.com/privacy?hl=en-DE&fg=1>

- **LinkedIn**

Provider: LinkedIn Ireland Unlimited Company,  
Wilton Place, Dublin 2 D02 AD98, Ireland  
[https://www.linkedin.com/legal/privacy-policy?trk=d\\_org\\_guest\\_company\\_overview\\_footer-privacy-policy](https://www.linkedin.com/legal/privacy-policy?trk=d_org_guest_company_overview_footer-privacy-policy)

- **Xing**

Provider: New Work SE,  
Dammtorstraße 30, 20354 Hamburg, Germany  
<https://privacy.xing.com/en/privacy-policy>

## 15. Tracking and analysis tools

We use tracking and analysis tools to ensure continuous optimisation and design of our website to meet your needs. Through the use of tracking and analysis measures, it is also possible for us to statistically record the use of our website by visitors and to further develop our online presence for you through the knowledge gained thereby.

If you have given us your consent to the use of cookies on the basis of a notice ("cookie banner") provided by us on the website, the legality of the use is additionally governed by Art. 6 Para. 1 lit. a) GDPR.

In addition, we may have a legitimate interest in optimising our online presence so that the use of tracking and analysis tools may in some cases be permissible under Art. 6 Para. 1 lit. f) GDPR.

If the providers of the tools transfer the data outside the EU / EEA, the recipients are obliged to comply with an appropriate data protection standard on the basis of so-called EU standard contractual clauses. In addition, a transfer to a third country may also take place due to the recognition of an adequate level of data protection by the European Commission.

The tracking and analysis tools we use are listed in our cookie banner. Such tools that require your consent are only activated when the respective setting in the cookie banner is checked and saved. You can change or revoke the settings you have made at any time.

## **16. Additional tools**

### **Google Maps**

#### **a) Nature, scope and purpose of data processing**

We integrate the maps of the service Google Maps. Google Maps ist a service of Google Ireland Ltd, Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Irland, E-mail: support-deutschland@google.com ("Google").

We use Google Maps to show you maps on our website, especially for directions. This allows us to display interactive maps directly on our website and enables you to use the map function conveniently.

Google stores your data as user profiles and uses them for the purposes of advertising, market research and / or the design of its website in line with requirements.

Such evaluation is carried out in particular (even for users who are not logged in) for the purpose of providing demand-oriented advertising. The evaluation is also carried out to inform other users of the social network about your activities on our website.

If you use the Google Maps component integrated on our website, Google will store a cookie on your end device via your Internet browser and process the following data:

- The operating system
- Information about the browser type and version used
- Information about your Internet service provider
- Your IP address

- Date and time of access
- Websites from which you came to our website
- Websites that you visit through our website

This occurs regardless of whether Google provides a user account that you are logged in to or whether there is no user account. If you're logged in to Google, your information will be directly associated with your account. If you do not want your profile to be associated with Google, you will need to log out.

#### **b) Legal basis of data processing**

The legal basis is your consent according to Art. 6 Para. 1 lit. a GDPR.

#### **c) Storage period**

The stored data are deleted by us as soon as they are no longer needed for our purposes mentioned above.

#### **d) Right to objection**

You have a right of objection to the formation of these user profiles. This is to be addressed to Google.

You can prevent the transfer of data to Google by disabling JavaScript in your browser settings. In that case, you will not be able to use Google Maps on our website.

Learn more about the Google Maps Terms of Use:  
<https://policies.google.com/terms?gl=DE&hl=en>

Learn more about the Additional Terms of Service of Google Maps:  
[www.google.com/intl/en\\_US/help/terms\\_maps.html](http://www.google.com/intl/en_US/help/terms_maps.html)

For more information see Google's privacy policy:  
<https://policies.google.com/privacy?hl=en>

### **Google Fonts**

#### **a) Nature, scope and purpose of data processing**

We use external fonts from Google on this website. Google Fonts is a service of Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, Tel: +353 1 543 1000, Fax: +353 1 686 5660, E-Mail: [support-deutschland@google.com](mailto:support-deutschland@google.com) ("Google").

The integration of these web fonts is done by a server call. This can also be a Google server in the USA. In this case, the server is informed which of our Internet pages you have visited. The IP address of your end device is also processed by Google.

The purpose of using Google Fonts is the uniform representation of fonts.

#### **b) Legal basis of data processing**

The legal basis is Art. 6 Para. 1 lit. f) GDPR. Our legitimate interest lies in the optimisation and economic operation of our Internet presence.

#### **c) Storage period**

The data collected by Google due to the use of Google Fonts will not be processed by us.

#### **d) Right of objection**

You have the right to object to the creation of these user profiles. This should be addressed to Google.

You can find more information in Google's privacy policy, which you can download here: <https://www.google.com/policies/privacy/>

## **17. Credit bureaus**

We make use of the services of credit agencies (e.g. SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden, Germany [https://www.schufa.de/en/schufa-information/schufa-information\\_en.jsp](https://www.schufa.de/en/schufa-information/schufa-information_en.jsp)), Creditreform Boniversum GmbH, Hammelfelddamm 13, 41460 Neuss, Germany (the data protection declaration of Creditreform Boniversum GmbH can be found here <https://www.boniversum.de/eu-dsgvo/for-consumers-information-under-eu-gdpr/?lang=en>) within the framework of the entire business relationship with you, insofar as this is necessary and permissible to safeguard our legitimate interests or the legitimate interests of third parties or to fulfil statutory obligations. This includes in particular:

- Transmission of the data collected from you concerning the application, execution and termination of business relations as well as data concerning non-contractual behaviour or fraudulent behaviour.
- Data exchange to determine creditworthiness or default risks and the requirements for the garnishment protection account or base account.
- Measures to prevent money laundering and terrorist financing or the prevention and investigation of criminal offences.

The information obtained from the credit agencies forms the basis for the decision on credit applications (including credit cards) and serves to minimise financial risks for all parties involved. Information can also be obtained outside a credit request, e.g. when opening an account and issuing debit cards, if this is necessary to reduce financial risks.

It is also possible that the decision on the opening of an account or the credit application is automatically taken by the computer system on the basis of the information obtained. Negative information leads to a rejection of the account opening, the card application or the credit application.

The legal basis of data processing is Art. 6 Para. 1 lit. f) GDPR. Insofar, our legitimate interest is the safeguarding of our business activities with the help of creditworthiness data. Besides, the data exchange with credit bureaus helps protect third parties in the course of their commercial activities.

## **18. What rights do you have with regard to data protection?**

Here you will find your rights regarding your personal data. Details can be found in Articles 7, 15-22 and 77 GDPR. You can contact the responsible office (point 2) or the Data Protection Officer (point 3) in this regard.

### **a) Right to revoke your data protection consent pursuant to Art. 7 Para. 3 S. 1 GDPR**

You can revoke your consent to the processing of your personal data at any time with effect for the future. However, this shall not affect the lawfulness of the processing carried out until revocation.

### **b) Right to information pursuant to Art. 15 GDPR**

You have the right to request confirmation as to whether we process any personal data concerning you. If this is the case, you have the right to information about this personal data as well as other information, e.g. the processing purposes, the recipients and the planned duration of storage or the criteria for determining the duration.

### **c) Right to rectification and completion pursuant to Art. 16 GDPR**

You have the right to demand the correction of incorrect data without delay. Taking into account the purposes of the processing, you have the right to request the completion of incomplete data.

### **d) Right to deletion ("right to be forgotten") pursuant to Art. 17 GDPR**

You have the right to have your data deleted if processing is not necessary. This is the case, for example, if your data is no longer necessary for the original purposes, if you have withdrawn your declaration of consent under data protection law or if the data have been unlawfully processed.

### **e) Right to limitation of processing pursuant to Art. 18 GDPR**

You have the right to limit the processing, e.g. for the duration of the assessment if you are of the opinion that the personal data is incorrect, or if you have objected to processing. Besides, you can demand limitation of processing if you do not wish for your data being actively used, but reject a deletion, e.g. if you still need the data for a legal dispute.

#### **f) Right to data transferability pursuant to Art. 20 GDPR**

You have the right to receive your personal data in a structured, common and machine-readable format.

#### **g) Automated decision in individual cases including profiling pursuant to Art. 22 GDPR**

You have the right not to be subject to a decision based exclusively on automated processing, including profiling, except in the exceptional circumstances mentioned in Art. 22 GDPR.

An automated decision making including profiling does not take place with us. Should we use these procedures in individual cases, we will inform you of this separately if this is required by law.

#### **h) Complaint to a data protection supervisory authority pursuant to Art. 77 GDPR**

You can also file a complaint with a data protection supervisory authority at any time, for example if you believe that the data processing does not comply with data protection regulations.

The competent data protection supervisory authority is the following:

#### **Bavarian State Office for Data Protection Supervision**

P.O. Box 1349  
91504 Ansbach  
Germany

Telephone: +49 (0) 981 180093-0  
Fax: +49 (0) 981 180093-800

E-mail: [poststelle@lda.bayern.de](mailto:poststelle@lda.bayern.de)

Homepage: <http://www.lda.bayern.de>

## **19. Which data are you obliged to provide?**

As part of our business relationship, you must provide the personal information necessary to establish and conduct a business relationship and to fulfil the contractual obligations associated therewith, or which we are required by law to collect. Without this information, we will generally not be able to enter into or execute the contract with you.

If you are authorized to represent a third party, you must provide us with the personal data that are necessary for the collection and execution of a representation / authorisation and the fulfilment of the associated contractual obligations or which we are legally obliged to collect. Without this data, we usually have to reject you as an authorised representative or cancel an existing authorisation.

In particular, we are obliged under the provisions of money laundering law to identify you on the basis of your identification document before establishing the business relationship or the power of representation / authorisation and to collect and record your name, place of birth, date of birth, nationality, address and identification data. To enable us to comply with this legal obligation, you must provide us with the necessary information and documents in accordance with the Money Laundering Act and notify us immediately of any changes arising in the course of the business relationship. If you do not provide us with the necessary information and documents, we may not establish or continue the business relationship you have requested or set up or continue the power of representation / authorisation you have requested.

## **20. Is profiling taking place?**

We partially process your data automatically with the aim of evaluating certain personal aspects (profiling). For example, we use profiling in the following cases:

- Due to legal and regulatory requirements, we are obliged to combat money laundering, terrorist financing and property-threatening crimes. Data evaluations are also carried out (e.g. in payment transactions). These measures also serve to protect you.
- In order to be able to provide you with targeted information and advice on products, we use evaluation tools. These enable needs-based communication and advertising, including market and opinion research.
- We use scoring to assess your creditworthiness. The probability with which a customer will meet its payment obligations in accordance with the contract is calculated. For example, income, expenses, existing liabilities, occupation, employer, length of employment, experience from the previous business relationship, contractual repayment of previous loans and information from credit agencies can be included in the calculation.

The scoring is based on a mathematically-statistically recognised and proven procedure. The calculated scores support us in making decisions in the context of product closures and are included in ongoing risk management.

## **21. Information on the right of objection under Article 21 GDPR**

### **Right of objection in individual cases**

You have the right to object at any time, for reasons arising from your particular situation, to the processing of personal data concerning you carried out pursuant to Article 6 Para. 1 lit. e) GDPR (data processing in the public interest) and Article 6 Para. 1 lit. f) GDPR (data processing on the basis of a balancing of interests), including profiling based on this provision within the meaning of Article 4 No. 4 GDPR.

If you file an objection, we will no longer process your personal data unless we can prove compelling legitimate reasons for the processing that outweigh your interests, rights and freedoms, or the processing serves the assertion, exercise or defence of legal claims.

### **Right to object to the processing of data for direct marketing purposes**

In individual cases we process your personal data in order to operate direct advertising. You have the right at any time to object to the processing of personal data concerning you for the purpose of such advertising; this also applies to profiling in so far as it is connected with such direct advertising.

If you object to the processing for purposes of direct marketing, we will no longer process your personal data for these purposes.

### **Addressee of an objection**

The objection can be made without form (best with the subject "Objection") under indication of your name, your address and your date of birth and should be addressed to:

**Fidor Bank AG**  
Sandstr. 33  
80335 Munich  
Germany

Head Office: (089) 189 085 233  
Fax: (089) 189 085 199

E-mail: [info@fidor.de](mailto:info@fidor.de)



## **II. PRIVACY POLICY FOR THE FIDOR SMART BANKING APP**

### **1. Who is responsible for data processing?**

Responsible for the processing of your personal data is the

**Fidor Bank AG**  
Sandstr. 33  
80335 Munich  
Germany

Head Office: +49 89 189 085 233  
Fax: +49 89 189 085 199

E-mail: [info@fidor.de](mailto:info@fidor.de)  
Internet: [www.fidor.de](http://www.fidor.de)

Represented by the Board of Directors:  
Boris Joseph, Pascal Cirelli, Stefan Spannagl

## **2. How can you reach our Data Protection Officer?**

If you have any questions regarding data protection, you can also contact our Data Protection Officer at any time:

**Dr. Georg Schröder, LL.M.**  
**Data Protection Officer**

legal data

Schröder Rechtsanwaltsgesellschaft mbH  
Pranner Straße 10  
80333 Munich

Tel: +49 89 954 597 520  
Fax: +49 89 954 597 522

E-mail: [datenschutz@fidor.de](mailto:datenschutz@fidor.de)

## **3. What are the features of the App?**

### **Registration and device binding**

You can log in to the Fidor Smart Banking app using your e-mail address and password, which you use for your Fidor account. In addition, you can log in with your fingerprint, which is stored locally and encrypted on your device.

Your Fidor account can only be linked to one Fidor Smart Banking App at a time (so-called device binding). This ensures that unauthorised third parties cannot gain insight into your account transactions.

### **View account transactions**

In the Fidor Smart Banking App, you can view your current account balance as well as track the transactions that have taken place on the account (e.g. credits, transfers).

## **Banking**

The Fidor Smart Banking App includes all banking functions that are also available to you on your Fidor account page accessible via web browser (transfers, standing orders, scheduled transfers).

In addition, you can make transactions directly to contacts from your address book (e.g. if you do not know their IBAN).

## **Digital credit card**

In the Fidor Smart Banking App you can deposit your credit card provided by Fidor Bank in digital form. In this way, you can pay in retail directly with your smartphone and do not need your physical card for this. In the card management within the app, you can also activate or deactivate your card, view your card details, set payment limits and block the card if necessary.

## **Fidor Cash Map**

In the Fidor Smart Banking App, you can display the nearest Fidor Bank partners in whose stores you can withdraw cash from your Fidor account or deposit it there. For this purpose, the location of your device is determined and processed locally on your device if you grant the corresponding authorisation.

## **Call customer service**

You can call Fidor Bank's customer service directly from the Fidor Smart Banking App. The corresponding phone number is automatically entered and dialed in the phone app of your smartphone. A manual switch to the phone app is not necessary for this.

## **Push notifications**

If you grant the appropriate authorisation, you can have account-related notifications (e.g. successful completion of a transaction) delivered to your smartphone as a push notification. This means that the notification is not only delivered when you open the app, but the moment it is retrieved by the app in the background. The app constantly checks for new push notifications so that they can be displayed immediately.

## **TAN procedure**

If you want to make a transfer via the Fidor Smart Banking App, you will also receive the corresponding transaction authentication number (TAN) as a push notification via the app. You can use the TAN to authorize and initiate the transaction.

#### **4. What permissions does the APP require?**

To fulfill the purposes outlined above, the Fidor Smart Banking App requires the following authorisations:

- Access to the address book
- Access to location information
- Access to the phone function
- Access to the device ID
- Access to network communication functions
- Access to NFC (Near Field Communication) functions

You can change permissions once granted at any time later in the system settings of your smartphone.

#### **5. What data do we use and how long do we keep it?**

For the provision of our service within the Fidor Smart Banking App, we primarily use the data that you have provided to us yourself or that is generated during the intended use of the app. This includes in particular:

- First name, last name
- Address
- E-mail address
- Phone number
- Password
- IBAN, BIC
- Credit card data
- Account balance
- Transaction history
- Standing orders
- Random one-time TANs
- Contacts in the address book

The data required for the display of account transactions and the processing of transactions corresponds to the data that is processed when you use your Fidor account via a web browser.

If you have activated authentication using your fingerprint, this is stored in encrypted form on your terminal device and managed locally by the manufacturer of your smartphone. Fidor Bank does not gain knowledge of the content of biometric data.

In principle, we keep your personal data for as long as is necessary to achieve the contractually intended purpose. This regularly corresponds to the duration of the account contract with you. In addition, there may be legal obligations to retain data e.g. in accordance with the German Banking Act (KWG), the Money Laundering Act (GwG), the Securities Trading Act (WpHG), tax laws (including the Fiscal Code (AO), Value Added Tax Act (UstG), Income Tax Act (EstG)) and banking supervisory requirements (e.g. the European Central Bank, the European Banking Supervisory Authority, the Deutsche Bundesbank and the Federal Financial Supervisory Authority).

## **6. What is the legal basis for the processing?**

We process your personal data managed via the Fidor Smart Banking App, in particular your account and transaction data, to fulfill the underlying bank account contract. The legal basis for the processing is thereby Art. 6 (1) lit. b GDPR. Insofar as we process data for the fulfillment of legal obligations (e.g. of statutory retention obligations), the legal basis is Art. 6 (1) lit. c GDPR. If we obtain separate consent from you to a specific processing, your data will be processed on the basis of Art. 6 (1) lit. a GDPR. Otherwise, the legal basis for processing is Art. 6 (1) lit. f GDPR. Such use of your data is based on legitimate interests of Fidor Bank or third parties (e.g. use of consulting services of business consultants and lawyers or enforcement or defense of legal claims).

## **7. To whom will your data will be disclosed?**

Before downloading the Fidor Smart Banking App, you must log in to either the Google Play Store (in the case of Android devices) or the Apple App Store (in the case of Apple devices) and accept the terms and conditions of the respective provider. Google or Apple process personal user data in this process. Details on this can be found in the privacy statements of the providers at:

### **Google:**

<https://policies.google.com/privacy>

### **Apple:**

<https://www.apple.com/de/legal/privacy/>

If you have activated the receipt of push notifications via the Fidor Smart Banking App, we use the "Google Firebase" service for this purpose, which is offered by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4 D04 E5W5, Ireland ("Google"). For the purpose of assigning push notifications to an end device, unique ID numbers can be created as pseudonyms and transmitted to Google for the delivery of the notifications. There is no transmission of contents of the push notifications to Google (i.e. in particular not of the TAN or associated transaction details). If data is transferred to recipients in third countries (e.g. to Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA), these are obligated to comply with a data protection standard that essentially corresponds to the European standard on the basis of so-called EU standard contractual clauses. Further information on data protection at Google can be found at: <https://policies.google.com/privacy>

Otherwise, your personal data will only be passed on for the following purposes:

We will only pass on your personal data to third parties if:

- you have given your express consent in accordance with Art. 6 para. 1 lit. a) GDPR,
- this is legally permissible and required according to Art. 6 para. 1 lit. b) GDPR for the fulfilment of a contractual relationship with you or the implementation of pre-contractual measures,
- there is a legal obligation under Art. 6 para. 1 lit. c) GDPR to pass on such information. We are legally obliged to transmit data to state authorities (e.g. financial authorities, financial supervision, tax authorities, criminal prosecution authorities),
- the disclosure pursuant to Art. 6 para. 1 sentence 1 lit. f) GDPR is necessary to safeguard legitimate business interests and to assert, exercise or defend legal claims and there is no reason to assume that you have an overriding legitimate interest in not disclosing your data, or
- we use so-called contract processors in accordance with Art. 28 GDPR when processing us by external service providers who have been obliged to handle their data with care. We use such service providers primarily in the areas of IT, logistics, telecommunications, sales, marketing and debt collection.

A data transfer to places in states outside the European Union (so-called third states) takes place, insofar as

- it is necessary for the execution of your orders (e.g. if a payment is to be made to an account-holding institution established in a third country),
- it is required by law (e.g. tax reporting obligations), or
- you have given us your consent.

When transferring your personal data to external entities in third countries, i.e. outside the EU or the EEA, we ensure that these entities treat your personal data with the same care as within the EU or the EEA. We only transfer personal data to third countries where the EU Commission has confirmed an adequate level of

protection or where we ensure the careful handling of personal data through contractual agreements or other appropriate guarantees.

## **8. What rights do you have with regard to Data Protection?**

Here you will find your rights regarding your personal data. Details can be found in Articles 7, 15-22 and 77 GDPR. You can contact the responsible office (point 1) or the Data Protection Officer (point 2) in this regard.

### **a) Right to revoke your data protection consent pursuant to Art. 7 Para. 3 S. 1 GDPR**

You can revoke your consent to the processing of your personal data at any time with effect for the future. However, this shall not affect the lawfulness of the processing carried out until revocation.

### **b) Right to information pursuant to Art. 15 GDPR**

You have the right to request confirmation as to whether we process any personal data concerning you. If this is the case, you have the right to information about this personal data as well as other information, e.g. the processing purposes, the recipients and the planned duration of storage or the criteria for determining the duration.

### **c) Right to rectification and completion pursuant to Art. 16 GDPR**

You have the right to demand the correction of incorrect data without delay. Taking into account the purposes of the processing, you have the right to request the completion of incomplete data.

### **d) Right to deletion ("right to be forgotten") pursuant to Art. 17 GDPR**

You have the right to have your data deleted if processing is not necessary. This is the case, for example, if your data is no longer necessary for the original purposes, if you have withdrawn your declaration of consent under data protection law or if the data have been unlawfully processed.

### **e) Right to limitation of processing pursuant to Art. 18 GDPR**

You have the right to limit the processing, e.g. for the duration of assessment if you are of the opinion that the personal data is incorrect, or if you have objected to processing. Besides, you can demand limitation of processing if you do not wish for your data being actively used, but reject a deletion, e.g. if you still need the data for a legal dispute.

**f) Right to data transferability pursuant to Art. 20 GDPR**

You have the right to receive your personal data in a structured, common and machine-readable format.

**g) Automated decision in individual cases including profiling pursuant to Art. 22 GDPR**

You have the right not to be subject to a decision based exclusively on automated processing, including profiling, except in the exceptional circumstances mentioned in Art. 22 GDPR.

**h) Complaint to a data protection supervisory authority pursuant to Art. 77 GDPR**

You can also file a complaint with a data protection supervisory authority at any time, for example if you believe that the data processing does not comply with data protection regulations.

The competent data protection supervisory authority is the following:

**Bavarian State Office for Data Protection Supervision**

P.O. Box 1349  
91504 Ansbach  
Germany

Telephone: +49 (0) 981 53 1300

Fax: +49 (0) 981 180093-800

E-mail: [poststelle@lda.bayern.de](mailto:poststelle@lda.bayern.de)

Homepage: <http://www.lda.bayern.de>

### **III. DATA PROTECTION INFORMATION ON THE CHANGES BY THE PSD2**

The Second Payment Services Directive ("PSD2") and its implementation into German law will bring some changes in the field of online banking.

The most visible is the introduction of two-factor authentication. As soon as you want to log in to the online banking of your Fidor account via your internet browser, not only the input of user name and password is required but also the confirmation of the log in via a mTAN. The same applies to payments created in a web browser after login. However, the login in the Fidor Smart Banking App still does not require a mTAN. If a payment is to be made via the Fidor Smart Banking App, you will receive a pushTAN. The payment is then released by wiping on the device.



In addition, with your express consent, your account and transaction data may be forwarded to third party payment service providers to fulfill the purposes assumed by these service providers towards you. These payment service providers can basically be divided into payment initiation services and account information services. Payment initiation services can be located between the Fidor Bank as a credit institution and a marketplace, e.g. an online shop, and in this case they take over the payment processing without you having to log in to your Fidor account or provide the marketplace with your account data. Fidor Bank provides the account data required for the transaction to the payment initiation service via a PSD2 interface. With the help of account information services you can, e.g. have the relevant information on your bank accounts, including your Fidor account, displayed in an aggregated way. To do this, the account information service retrieves the data of your Fidor account via the PSD2 interface of Fidor Bank.

Further information about the changes due to the PSD2 can be found on our FAQ page: <https://www.fidor.de/psd2-fur-privat-und-geschaeftskunden>

## **IV. DATA PROTECTION INFORMATION ACCORDING TO ART. 13, 14 GDPR OF FIDOR BANK AG**

Our activities also require the collection and processing of personal data. Below we would like to give you a brief overview of how your personal data is processed by us and what rights you are entitled to under the EU General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG). Which data is processed in detail and how it is used depends largely on the services requested or agreed, so you may not be concerned with information in this document.

Please also pass on the information to current and future authorized representatives and beneficial owners as well as any co-obligated parties of a loan. These include, for example, beneficiaries in the event of death, authorized signatories or guarantors.

## 1. Who is responsible for data processing?

Responsible for the processing of your personal data is the

### **Fidor Bank AG**

Sandstr. 33  
80335 Munich  
Germany

Head Office: (089) 189 085 233

Fax: (089) 189 085 199

E-mail: [info@fidor.de](mailto:info@fidor.de)

Internet: [www.fidor.de](http://www.fidor.de)

Represented by the Board of Directors: Boris Joseph, Pascal Cirelli, Stefan Spannagl

## 2. How can you contact our Data Protection Officer?

If you have any questions regarding data protection, you can also contact our Data Protection Officer at any time:

### **Dr. Georg Schröder, LL.M.** **Data Protection Officer**

legal data  
Schröder Rechtsanwaltsgesellschaft mbH  
Prannerstr. 10  
80333 Munich  
Germany

Tel.: +49 89 954 597 520

Fax: +49 89 954 597 522

E-mail: [datenschutz@fidor.de](mailto:datenschutz@fidor.de)

## 3. Which data do we use and from which sources do they originate?

We collect your personal data when you contact us, e.g. as an interested party, authorized representative, applicant or customer. That is: In particular, if you are interested in our products, submit applications or use our products and services within the framework of an existing business relationship. In addition,

we process – to the extent necessary for the provision of our services – personal data which we obtain from publicly accessible sources (e.g. debtor directories, land registers, commercial and association registers, press, Internet, transparency registers) or which are transmitted to us by other companies of the Fidor Bank Group or by other third parties (e.g. a credit agency) with permission.

Relevant personal data in the interested party process, when entering master data, in the course of authorization, as co-obligated party of a loan (e.g. guarantor), etc. can be: Personal data (name, address and other contact details (mainly e-mail address, telephone number), date and place of birth and nationality, marital status, gender, legal capacity, occupational group, employer if applicable and type and duration of employment relationship, residential status (property / rent), identification data (e.g. ID card data), authentication data (e.g. signature sample), tax ID, SCHUFA score, FATCA status and EU basic account identification.

In addition, this may also include the following types of data: Order data (e.g. payment order), data from the fulfilment of our contractual obligations (e.g. turnover data in payment transactions), tax information, information on your financial situation (e.g. creditworthiness data, scoring rating data, origin of assets, income / surplus calculations, balance sheets, business analyses, etc.), information and records on knowledge and / or experience with securities, interest rate and currency products / money investments (MiFID status: (e.g. land register excerpts, property valuations), advertising and sales data (including advertising scores, information on participation in direct marketing measures, contact channel, date, occasion and result of the consultation, (electronic) copies of correspondence, newsletter opt-in (this is saved during the double opt-in process): IP address, date and time of registration and date and time of clicking on the confirmation link in the confirmation e-mail and IP address), community data (data that you share with other customers and the public within the Fidor community, such as your questions / answers, profile information, photo, etc.), documentation data (e.g. consultation protocol) and other data comparable to the categories mentioned.

#### **4. For what purposes will your data be processed and on what legal basis?**

We process personal data in accordance with the provisions of the European Data Protection Basic Regulation (GDPR) and the Federal Data Protection Act (BDSG):

##### **a) For the fulfilment of contractual obligations (Art. 6 Para. 1 lit. b) GDPR)**

The processing of personal data is carried out to provide banking transactions and financial services within the framework of the execution of our contracts

with our customers or to carry out pre-contractual measures, which take place at your request.

The purposes of data processing depend primarily on the specific product you are using (e.g. account, credit, etc.) and may include, but are not limited to, needs analyses, advice, asset management and support, and the execution of transactions. Further details for the purpose of data processing can be found in the respective contract documents and terms and conditions. Within the scope of fulfilling contractual obligations, data is also exchanged with credit card providers if a credit card is applied for and made available via Fidor Bank AG. This also includes automatic data exchange as part of the Mastercard® Automatic Billing Updater (ABU) database to minimize the rejection of card payments when credit card data expires or changes are made.

#### **b) In the context of balancing interests (Art. 6 Para. 1 lit. f) GDPR)**

If necessary, we process your data beyond the fulfilment of contractual obligations to protect the legitimate interests of us or third parties.

Examples of this are:

- Consultation and data exchange with credit agencies (e.g. SCHUFA, Creditreform Boniversum GmbH) to determine creditworthiness and default risks in the credit business,
- Testing and optimisation of procedures for needs analysis
- for the purpose of direct customer contact, advertising or market and opinion research, provided that you have not objected to the use of your data,
- Assertion of claims and defence in legal disputes,
- Ensuring the IT security and IT operations of our company and its contractual partners,
- Prevention and investigation of criminal offences,
- Video surveillance to ensure building and plant safety and the safety of our employees,
- Measures for building and plant security (e.g. access controls),
- Measures for business management and further development of services and products,
- Risk management in our company and in affiliated companies.

#### **c) Based on your consent (Art. 6 Para. 1 lit. a) GDPR)**

If you have given us your consent to the processing of personal data for certain purposes (e.g. use of telephone and e-mail or postal address for advertising purposes, dispatch of invitations to sales events or newsletters), the legality of this processing is given on the basis of your consent. A given consent can be revoked at any time. The revocation of the consent does not affect the legality of the data processed until the revocation.

**d) To fulfil our legal obligations (Art. 6 Para. 1 lit. c) GDPR) or in the public interest (Art. 6 Para. 1 lit. e) GDPR)**

As a bank, we must meet a wide range of legal requirements (e.g. under the German Banking Act (KWG), the Money Laundering Act (GwG), the Securities Trading Act (WpHG), tax laws (including the Fiscal Code (AO), Value Added Tax Act (UstG), Income Tax Act (EstG)) and banking supervisory requirements (e.g. the European Central Bank, the European Banking Supervisory Authority, the Deutsche Bundesbank and the Federal Financial Supervisory Authority). The purposes of processing include, but are not limited to, credit checks, identity and age checks, prevention of fraud and money laundering, compliance with tax control and reporting obligations, evaluation of your expertise, experience and knowledge of financial assets, and evaluation and management of risks to our company and its affiliates.

## **5. To whom will your data be transmitted?**

Within our company, those departments that need your data to fulfil our contractual and legal obligations will have access to it.

We will only pass on your personal data to third parties if:

- you have given your express consent in accordance with Art. 6 Para. 1 lit. a) GDPR,
- this is legally permissible and required according to Art. 6 Para. 1 lit. b) GDPR for the fulfilment of a contractual relationship with you or the implementation of pre-contractual measures,
- there is a legal obligation under Art. 6 Para. 1 lit. c) GDPR to pass on such information. We are legally obliged to transmit data to state authorities (e.g. financial authorities, financial supervision, tax authorities, criminal prosecution authorities),
- the disclosure pursuant to Art. 6 Para. 1 sentence 1 lit. f) GDPR is necessary to safeguard legitimate business interests and to assert, exercise or defend legal claims and there is no reason to assume that you have an overriding legitimate interest in not disclosing your data, or
- we use so-called contract processors in accordance with Art. 28 GDPR when processing us by external service providers who have been obliged to handle their data with care. We use such service providers primarily in the areas of IT, logistics, telecommunications, sales, marketing and debt collection.

A data transfer to places in states outside the European Union (so-called third states) takes place, insofar as

- it is necessary for the execution of your orders (e.g. if a payment is to be made to an account-holding institution established in a third country),
- it is required by law (e.g. tax reporting obligations), or
- you have given us your consent.

When transferring your personal data to external entities in third countries, i.e. outside the EU or the EEA, we ensure that these entities treat your personal data with the same care as within the EU or the EEA. We only transfer personal data to third countries where the EU Commission has confirmed an adequate level of protection or where we ensure the careful handling of personal data through contractual agreements or other appropriate guarantees.

## **6. How long are your data stored?**

We process and store your personal data as long as it is necessary for the fulfilment of our contractual and legal obligations. Please note that our business relationship with you may last for many years.

If the data are no longer necessary for the fulfilment of contractual or legal obligations, they are regularly deleted, unless their - temporary - further processing is necessary for the following purposes:

- Fulfilment of commercial and tax retention obligations: These include the German Commercial Code (HGB), the German Tax Code (AO) and the Money Laundering Act (GwG). The time limits for storage and documentation specified there are between two and ten years.
- Preservation of evidence within the framework of the statutory statute of limitations. According to Sections 195 et seq. of the German Civil Code (BGB), these limitation periods can be up to 30 years, whereby the regular limitation period is three years.

## **7. What rights do you have with regard to data protection?**

Here you will find your rights regarding your personal data. Details can be found in Articles 7, 15-22 and 77 GDPR. You can contact the responsible office (point 1) or the Data Protection Officer (point 2) in this regard.

### **a) Right to revoke your data protection consent pursuant to Art. 7 Para. 3 S. 1 GDPR**

You can revoke your consent to the processing of your personal data at any time with effect for the future. However, this shall not affect the lawfulness of the processing carried out until revocation.

### **b) Right to information pursuant to Art. 15 GDPR**

You have the right to request confirmation as to whether we process any personal data concerning you. If this is the case, you have the right to information about this personal data as well as other information, e.g. the processing purposes, the recipients and the planned duration of storage or the criteria for determining the duration.

**c) Right to rectification and completion pursuant to Art. 16 GDPR**

You have the right to demand the correction of incorrect data without delay. Taking into account the purposes of the processing, you have the right to request the completion of incomplete data.

**d) Right to deletion ("right to be forgotten") pursuant to Art. 17 GDPR**

You have the right to have your data deleted if processing is not necessary. This is the case, for example, if your data is no longer necessary for the original purposes, if you have withdrawn your declaration of consent under data protection law or if the data have been unlawfully processed.

**e) Right to limitation of processing pursuant to Art. 18 GDPR**

You have the right to limit the processing, e.g. for the duration of the assessment, if you are of the opinion that the personal data is incorrect, or if you have objected to processing. Besides, you can demand limitation of processing if you do not wish for your data being actively used, but reject a deletion, e.g. if you still need the data for a legal dispute.

**f) Right to data transferability pursuant to Art. 20 GDPR**

You have the right to receive your personal data in a structured, common and machine-readable format.

**g) Automated decision in individual cases including profiling pursuant to Art. 22 GDPR**

They have the right not to be subject to a decision based exclusively on automated processing, including profiling, except in the exceptional circumstances mentioned in Art. 22 GDPR.

An automated decision making including profiling does not take place with us. Should we use these procedures in individual cases, we will inform you of this separately if this is required by law.

**h) Complaint to a data protection supervisory authority pursuant to Art. 77 GDPR**

You can also file a complaint with a data protection supervisory authority at any time, for example if you believe that the data processing does not comply with data protection regulations.

The competent data protection supervisory authority is the following:

**Bavarian State Office for Data Protection Supervision**

P.O. Box 1349  
91504 Ansbach  
Germany

Telephone: +49 (0) 981 180093-0

Fax: +49 (0) 981 180093-800

E-mail: [poststelle@lda.bayern.de](mailto:poststelle@lda.bayern.de)

Homepage: <http://www.lda.bayern.de>

## **8. Which data are you obliged to provide?**

As part of our business relationship, you must provide the personal information necessary to establish and conduct a business relationship and to fulfil the contractual obligations associated therewith, or which we are required by law to collect. Without this information, we will generally not be able to enter into or execute the contract with you.

If you are authorised to represent us, you must provide us with the personal data that are necessary for the collection and execution of a representation / authorisation and the fulfilment of the associated contractual obligations or which we are legally obliged to collect. Without this data, we usually have to reject you as an authorised representative or cancel an existing authorisation.

In particular, we are obliged under the provisions of money laundering law to identify you on the basis of your identification document before establishing the business relationship or the power of representation / authorisation and to collect and record your name, place of birth, date of birth, nationality, address and identification data. To enable us to comply with this legal obligation, you must provide us with the necessary information and documents in accordance with the Money Laundering Act and notify us immediately of any changes arising in the course of the business relationship. If you do not provide us with the necessary information and documents, we may not establish or continue the business relationship you have requested or set up or continue the power of representation / authorisation you have requested.

## **9. Is profiling taking place?**

We partially process your data automatically with the aim of evaluating certain personal aspects (profiling). For example, we use profiling in the following cases:

- Due to legal and regulatory requirements, we are obliged to combat money laundering, terrorist financing and property-threatening crimes. Data evaluations are also carried out (e.g. in payment transactions). These measures also serve to protect you.



- In order to be able to provide you with targeted information and advice on products, we use evaluation tools. These enable needs-based communication and advertising, including market and opinion research.
- We use scoring to assess your creditworthiness. The probability with which a customer will meet its payment obligations in accordance with the contract is calculated. For example, income, expenses, existing liabilities, occupation, employer, length of employment, experience from the previous business relationship, contractual repayment of previous loans and information from credit agencies can be included in the calculation.

The scoring is based on a mathematically-statistically recognised and proven procedure. The calculated scores support us in making decisions in the context of product closures and are included in ongoing risk management.

## **10. Information on the right of objection under Article 21 GDPR**

### **Right of objection in individual cases**

You have the right to object at any time, for reasons arising from your particular situation, to the processing of personal data concerning you carried out pursuant to Article 6 Para. 1 lit. e) GDPR (data processing in the public interest) and Article 6 Para. 1 lit. f) GDPR (data processing on the basis of a balancing of interests), including profiling based on this provision within the meaning of Article 4 No. 4 GDPR.

If you file an objection, we will no longer process your personal data unless we can prove compelling legitimate reasons for the processing that outweigh your interests, rights and freedoms, or the processing serves the assertion, exercise or defence of legal claims.

### **Right to object to the processing of data for direct marketing purposes**

In individual cases we process your personal data in order to operate direct advertising. You have the right at any time to object to the processing of personal data concerning you for the purpose of such advertising; this also applies to profiling in so far as it is connected with such direct advertising.

If you object to the processing for purposes of direct marketing, we will no longer process your personal data for these purposes.

### **Addressee of an objection**

The objection can be made without form (best with the subject "Objection") under indication of your name, your address and your date of birth and should be addressed to:

**Fidor Bank AG**

Sandstr. 33  
80335 Munich  
Germany

Head Office: (089) 189 085 233

Fax: (089) 189 085 199

E-mail: [info@fidor.de](mailto:info@fidor.de)