



Invest in building your wealth with every purchase.

Privacy Policy for the App

Introduction	3
1 Whose personal data does Pigtie process?	3
2 Who is responsible for the processing of my personal data?	3
3 Which personal data does Pigtie process?	3
4 How does Pigtie obtain my personal data?	5
5 For which purposes does Pigtie process personal data and which bases apply to this?	6
5.1 To enter into a business relationship and conclude a contract with you	6
5.2 To maintain the business relationship with you and carry out orders	7
5.3 To protect your interests and ours	8
5.4 To develop and improve our products and services	9
5.5 For advertising and marketing purposes and to maintain the business relationship with you	10
5.6 To conclude and terminate contracts with suppliers and business customers	11
5.7 To comply with legal obligations	11
5.8 For our corporate management	11
5.9 For archiving purposes	12
6 Where and for how long does Pigtie store my personal data?	12
7 Does Pigtie also process special categories of personal data?	13
8 Does Pigtie make automated decisions about me?	13
9 Who at Pigtie has access to my data?	13
10 Does Pigtie also use personal data for other purposes?	13
11 Does Pigtie pass my personal data on to third parties and to other countries outside the EU?	14
12 Provision of the mobile app and use of the mobile app	14
Description and scope of the data processing	14
Legal basis for the data processing	15
Purpose of the data processing	15
Duration of storage	15
12.1 Video identification by an identity verification service provider	15
12.2 MessageBird	16
12.3 Adjust	16
12.4 Analytics through Google Firebase	16
12.5 Notifications (push notifications)	17
12.6 Customer support	17
13 What rights do I have at Pigtie?	18
13.1 Right to information	18
13.2 Right of access and rectification	18
13.3 Right to erasure of your data	18
13.4 Right to restriction of processing	18
13.5 Right to data portability	18
13.6 Right to object to processing on the basis of a legitimate interest	18
13.7 Right to object to direct marketing	18
14 Where can I turn with a question or complaint?	19
15 Can Pigtie change this document?	19
Annex 1: List of third-party providers	19

Note on this translation. This document is an English translation of our German "Datenschutzerklärung zur App", provided for your convenience. The authoritative version is the German one, which you can find at www.pigtie.de/datenschutz and in the app. In the event of any discrepancy, the German version prevails.

Introduction

Pigtie processes personal data. At this point we would like to inform you about this clearly and unambiguously.

In this privacy policy we answer the most important questions about the processing of your personal data by Pigtie. If you have any questions about this privacy policy, you are welcome to contact us.

In addition to this privacy policy, our privacy policy for the website also applies.

IMPORTANT: This document already covers the personal data that we will process once we provide the investing function. This document is therefore more detailed than it currently needs to be. Should you have any questions, please contact us at any time at hello@pigtie.de.

As we talk about the processing of your personal data in this privacy policy, we would first like to inform you about what we mean by the terms "personal data" and "processing".

Personal data: all data that says something about you, directly or indirectly. For example your name and your (email) address, but also your date of birth or your transaction data.

Processing: everything that can be done with personal data, such as collection, but also storage, use and deletion of your data.

1 Whose personal data does Pigtie process?

We process personal data of people with whom we have, want to enter into, or have had a direct or indirect business relationship.

This is personal data of:

- customers,
- people who show an interest in our products and services, or
- people who are connected with a company or organisation with which we have, would like to have, or have had a relationship.

2 Who is responsible for the processing of my personal data?

Pigtie is responsible for the processing of your personal data.

3 Which personal data does Pigtie process?

Type of data	What kind of data is this?	Examples of Pigtie's use of this data
Direct or indirect identification data	Name, address, telephone number, email address, data contained in your identity document.	For identification, to assess whether we can accept you as a customer, or to contact you.

Type of data	What kind of data is this?	Examples of Pigtie's use of this data
Data about and relating to contracts	Data about your financial situation and the index fund (risk profile) with which you invest.	In order to be able to carry out orders for you.
Payment and transaction data	Information about the person to whom you have paid amounts or from whom you have received a payment, and about the time and place of the payment. We also collect the IBANs and BICs as well as turnover data of the bank accounts (recipient and sender names, amount, reference, etc.) or personal identification characteristics (customer number, etc.).	In order to be able to calculate how much in roundups we have to reserve for you per payment. To show in the app where and when you made this payment. After your express consent to the display of unexpected income, in respect of which you can decide whether or not to invest it.
Special categories of personal data, criminal law data and your social security number	Data from which your place of birth is apparent, as well as data from which your political opinions may be apparent, and your social security number.	We use your social security number in order to report the balance of your investments to the tax office. We collect data about your country of birth for the purposes of counter-terrorism and on the basis of tax obligations. It is possible that details about your political opinions, religion or health appear in your transaction data. Pigtie never uses this data for Pigtie's services.
Telephone recordings, online chat records, stored emails and interactions on social networks.	Conversations that we have with you and that you have with us by telephone or in the chat. This also applies to emails that you send us and that we send you, comments, videos, photos, likes and public messages that you publish on our social networks. Our encrypted communication with you via messenger services is also included.	We may use the conversation recordings, emails and chat conversations to combat fraud, on the basis of legal obligations, for quality objectives, to provide evidence, to improve our service and for the training, supervision and assessment of our employees. We may use the comments, videos, photos, likes and public messages in order to answer questions, post comments, and share information on a website not managed by us or on social media. Above all, this allows us to develop our chatbot further and to build up our chat data set with which we train our chatbot.
Data that says something about the use of our website and the app. Also data about, or the use of, emails that we send you.	See also the cookie page in this regard, IP address, data about the device with which you use our website or app.	In order to be able to use our app and website, and to combat fraud. To improve our website. To offer targeted advertising or banners.

Type of data	What kind of data is this?	Examples of Pigtie's use of this data
Data that we receive from other business partners.	Data that we receive from companies to which you have given consent to pass on data (for example finAPI, Facebook and Google).	To check whether you have debts, and to check who you are and where you live. To contact you or to propose offers to you.
Data that we pass on to other business partners.	Data that we make available to other business partners. This helps us to provide our services. Data in respect of which you have asked us to pass it on to another business partner. Data that we have to pass on to the supervisory authority.	We are obliged to forward certain (financial) data to the tax office and our supervisory authorities (Chamber of Industry and Commerce for Munich and Upper Bavaria, Bundesbank, Federal Financial Supervisory Authority, European Central Bank, German Federal Cartel Office and German data protection authority). Other business partners (for example marketing-related companies) that process data on our behalf, because we engage them for our services, also have access to this data.
Data that we need in order to combat fraud, for your and our security, and to prevent money laundering and the financing of terrorism.	Location data, transaction data, identity data, cookies, IP address and data about the device with which you use our website or app.	In order to comply with legal obligations and to prevent the financial sector, Pigtie or our employees from becoming victims of fraud. To protect Pigtie or the sector and to protect financial interests. We use your deposit and expenditure data, for example, to monitor transactions. These may stand out, for example, because you differ from the average deposit and withdrawal behaviour. We may use your IP address, device data and cookies for security purposes.

4 How does Pigtie obtain my personal data?

We obtain your data from you yourself, for example when you conclude a contract with us or contact us via our app, website, email or telephone. We also receive data from you through your use of our services, for example when depositing into and opening your Pigtie account or when calculating your roundups.

We may also receive your data from other financial institutions in the context of combating fraud, money laundering and the financing of terrorism. In addition, we may receive data from public sources such as public registers, the internet and social networks with a public profile. We may also receive data from other parties with whom we cooperate, for example via a list of public figures and people on insolvency lists. Sometimes we receive data because you have given third parties consent to pass data on to us.

5 For which purposes does Pigtie process personal data and which bases apply to this?

For the sake of clarity, we would first like to inform you about what we mean by the terms “purposes” and “bases”.

Purposes: what we process your personal data for; what we want to achieve with it. You can read about these in detail under 5.1 to 5.9.

Bases: why we process your personal data. This is necessary in order to perform the contract that you have concluded with Pigtie, either because you have given us consent or because we are legally obliged to do so.

In addition, we sometimes have a legitimate interest in processing your data. In this case we weigh Pigtie's interests against the interference with your privacy. Our interests include, for example, the following:

- We combat fraud in order to avoid damage to us, but also to the financial sector;
- We have to keep our internal accounts properly, take measures in the context of corporate taxation and review our internal processes;
- We have an interest in direct marketing in order to increase the number of Pigtie customers;
- We would like to keep you up to date about new products or existing products that, in our view, could be of interest to you.

We weigh our interest or the interest of third parties against your interest and your right to privacy. For example, we will then check whether we cannot achieve the same objective in another way without using your data, and whether we really need all of your personal data. If we want to use sensitive data and your right to privacy is more likely to be infringed, we will be slower to use your data on the basis of a legitimate interest.

Sometimes it is not clear from the law exactly what obligations we have to process your data. In addition, the obligation may not be contained in a law, or the law may not apply directly to us. If we nevertheless use data in such situations, we do so on the basis of a legitimate interest.

The legal basis for any data processing is Art. 6(1) GDPR.

5.1 To enter into a business relationship and conclude a contract with you

Purposes

If you become a customer of ours or would like to acquire a new product or service, we need your personal data. For example, we have to carry out an investigation in order to determine whether we can accept you as a customer.

For this purpose we may also use information about you that we receive from others.

If you would like to become a customer of ours, but also if you are already a customer of ours, we consult databases that indicate whether or not you have ever been involved in money laundering or the financing of terrorism.

We also subject you to a check against national and international sanctions lists.

We may also use the data that we receive from you and have stored about you for analyses, in order to determine whether you are eligible for a particular product or service. In addition, we may store a copy of your identity card when we enter into a business relationship with you.

Bases

In most cases we process your data because we are legally obliged to do so. But if this legal obligation does not apply directly to Pigtie, we have a legitimate interest in processing your data for these purposes. We may also process your data because this is necessary for the conclusion of your contract.

5.2 To maintain the business relationship with you and carry out orders

Purposes

If you are a customer of ours, we want to offer you good services. For this purpose we process personal data. We use your name, your telephone number and your email address, for example in order to stay in contact with you and to send you overviews of the status of your investments and the transactions you have made. We may also create recordings, for example of telephone calls and chat sessions. This is done, among other things, for the purposes of quality assurance, for training purposes and in the context of providing evidence. We may then also pass your data on to third parties. You can find a current list of third-party providers in the annex.

We process transaction data that you have passed on to us — only with your express consent — in order to be able to offer you Pigtie services. We use the data for credits or debits to your bank account. This also includes bank data including the IBANs and BICs as well as turnover data of the bank accounts (recipient and sender names, amount, reference, etc.) or personal identification characteristics (customer number, etc.), in order to identify unexpected income or to calculate your roundups. When taking up a service, you give your consent once for access to your account and once for the service (in order, for example, to calculate and/or invest roundups or unexpected income). On the basis of this one-off consent, we can always view this data.

Bases

We process data because this is necessary in order to perform the contract with you, but also because we have a legal obligation to do so, for example when investing in an index fund. If you do not provide us with certain information, we cannot perform the contract, as we cannot comply with our legal obligations.

In a number of cases we have a legitimate interest in processing your data, for example when creating telephone recordings (except when transmitting orders, where we may make recordings because this is required by law).

We only process transaction data after we have received your express consent in this regard and you have passed your transaction data on to Pigtie.

We then process your data, for example, in order to calculate and/or invest your roundups or your unexpected income. Do you not give permission for the investment and/or calculation of roundups and/or unexpected income? Then this has consequences for our services towards you, as we cannot then provide these services for you. If you do not pass your transaction data on to Pigtie, we cannot, for example, carry out debits from your bank account and cannot show you any unexpected income. As a customer, you can withdraw your consent to the processing at any time via the app.

Pigtie is bound by law to a maximum period for access to your transaction data. This maximum period is 90 days. Once the maximum period has expired, we may no longer be able to provide some services for you in full.

If you are not a Pigtie customer yourself (for example if you are a joint account holder) and consent to the sharing of transaction data has been given, you can send an email to Pigtie in order to withdraw your consent to the processing. You can also have your bank block Pigtie's access to the transaction details of your bank account.

5.3 To protect your interests and ours

Purposes

In order to protect your interests and ours as well as those of the financial sector, we may process personal data; for example, in order to combat or investigate fraud. For this purpose we or third parties may, for example, consult the country and sanctions lists of the Financial Action Task Force and have personal data recorded in them.

Customer investigation

It is not only when taking up a customer relationship that we or third parties check whether we can accept you as a customer. During the customer relationship too, we have to investigate whether you can continue to be our customer. For this purpose we process personal data. For example, a deposit into your Pigtie account or a withdrawal from your Pigtie account may give rise to further investigations.

Prevention of money laundering and the financing of terrorism

We have to prevent the misuse of the financial system through, for example, the concealment and movement of assets of illegal origin and the financing of terrorism. Such criminal activities can threaten not only the reputation and soundness of Pigtie, but also endanger the integrity and stability of the entire financial centre.

If we establish facts that indicate such misuse, we have to report this without undue delay to the Financial Intelligence Unit.

Under certain conditions, accounts, securities accounts or safe deposit boxes held by you at credit institutions based in Germany may also be traced and transmitted to the respective requesting parties, above all law enforcement authorities.

You can find detailed information and further links here:

https://www.bafin.de/DE/Aufsicht/Geldwaeschepraevention/geldwaeschepraevention_node.html

https://www.zoll.de/DE/Fachthemen/FIU/fiu_node.html

<http://www.fatf-gafi.org/>

In the following, reference will be made to a “third party”. This third party is either the custodian bank at which you open your Pigtie account or the verification service provider with which we check that you really are you.

If you would like to become a Pigtie customer, but also if you are already a Pigtie customer, we or a third party consult databases that indicate whether or not you have ever been involved in money laundering or the financing of terrorism. Not all Pigtie employees or employees of the third party can view these databases. If a Pigtie employee or an employee of the third party carries out a query during customer onboarding, that employee only sees whether or not there is an entry. If an entry is included in the databases, the compliance officer of Pigtie or of the third party assesses, on the basis of information from the databases or information available to them, whether you can become a customer.

If there is cause to do so (for example in the case of fraud at Pigtie), we or the third party may have you included in the database. We or the third party will then pass information about you on to third parties so that they can assess whether you should be included in the databases. The competent authority in this regard is the Financial Intelligence Unit of the customs authority.

We or the third party also consult lists of persons held by authorities. Sometimes financial institutions are not permitted to do business with these persons. It may also be that these persons require additional attention from financial institutions.

We or the third party can view the databases that indicate whether or not you have ever been involved in money laundering or the financing of terrorism, but we or the third party can also have your personal data recorded in these databases. If we or the third party have your data recorded in these databases, we or the

third party will inform you about this. Do you not agree with this recording? Then you can object to us or request the rectification or erasure of your data from us or from the third party.

Public sources

We or the third party consult public sources such as public registers, newspapers and the internet in order to prevent fraud and misuse and to protect Pigtie.

Fraud

In the context of combating fraud, we or the third party may use information that you have made available to us, for example your deposit and withdrawal behaviour in your Pigtie account. The supervisory authority also requires this of us.

In combating cybercrime and hacker attacks, such as botnets, we or the third party make data about you available to other parties that deal with cybercrime. We do this when we see that your security or that of the financial sector may be at risk. However, we only do this if we have concluded agreements with these parties on the careful use of your data. As set out in the sub-section "Prevention of money laundering and the financing of terrorism", we check whether you appear in databases that indicate whether or not you have ever been involved in money laundering or the financing of terrorism.

We create recordings and may store them, for example of telephone calls, email traffic and chat sessions. We do this in the context of fraud investigation. We may also do this where we are legally obliged to do so; for example to provide evidence, for quality assurance, and for further training, coaching and employee assessment.

Bases

We process your data because this is necessary in order to comply with a legal obligation. Where we are not under a direct legal obligation to pass on your data, we rely on the legitimate interest of Pigtie, of the financial sector or of our customers and employees.

5.4 To develop and improve our products and services

Purposes

In order to be able to offer you good services, we work continuously on the development and improvement of our products and services. In some cases we process personal data for this purpose; for example when you ask a question about a product, but also in order to be able to examine the use of the Pigtie app and the Pigtie website by means of in-app and website analytics. In doing so, we establish connections to third-party systems such as Google Analytics and Firebase Analytics in order to be able to process and analyse data. This allows us to create customer profiles and interest profiles. We do this by using cookies and comparable techniques, with the aim of improving our website and app.

By analysing personal data, we see how our products and services are used by you. We also use the results of the analyses, for example, to divide customers into groups. In this way we can create customer and interest profiles. If you use the Pigtie app, for example, you receive tips on using the app. You can object to this at any time.

If we establish that you are not using our services, or not using them fully, we may ask you what the reason for this is. We use your contact details for this purpose. We may do this for three months after you have ended the service with us.

If you no longer wish to be contacted by us, you can unsubscribe at any time via a link in the email, or tell us by email, telephone or chat that you do not wish to be contacted.

Bases

We process your data because we have a legitimate interest in doing so.

We may also ask for your consent to be allowed to process your data for the development and improvement of our products and services.

Do you not give us consent for the development and improvement of our products and services? Then this has no influence on our services towards you. You can withdraw the consent you have given at any time.

5.5 For advertising and marketing purposes and to maintain the business relationship with you

Purposes

We process your personal data for the purposes of customer care, advertising or marketing; for example, in order to inform you about a new product or a function that could be of interest to you, or to be able to respond better to your wishes. We also use links to social networks and other digital (advertising) networks for the purposes of sales promotion and marketing.

We use your contact details in order to send you information about products and services when you create a Pigtie account or leave personal data with us, such as your email address.

In addition, we may also contact you after you have ended your business relationship with Pigtie. You can unsubscribe from these marketing communications quickly and easily at any time by clicking the “Unsubscribe” link at the end of all newsletters and mailings.

We may also use the data we have stored about you in order to carry out analyses. With the help of these analyses we are able to improve the services for you. We may connect your use of our website with the information known to us about you in order to improve our services and to show you relevant advertising.

Do you not wish to be contacted for commercial purposes?

You can object to the processing of personal data with Pigtie yourself. To do so, simply write an email to hello@pigtie.de.

In addition, you can find out about personalised online advertising at www.youronlinechoices.com. You can also prevent websites from placing cookies on your computer, tablet or mobile phone. To do this you have to change your browser settings. You can also choose other settings for cookies here, for example that you receive a warning when cookies are set. You have to adjust these settings separately for each browser that you use. If you do not accept cookies from www.pigtie.de, it is possible that you will be asked again on every visit to the website whether you want to accept cookies.

Opting out of your marketing identifier

If you use our app, we collect a unique identifier of your device for marketing purposes (this is the Advertising Identifier on iOS devices and the Google Ad ID on Android devices). This identifier applies solely to your device and does not contain any personal data such as your name, your telephone number or your email address.

Using the settings on your device, you can determine yourself how these identifiers are used, including the option of resetting them. You can find an explanation of this on the website of your device's operating system:

- Apple iOS
- Android

We also cooperate with social networks and other digital platforms in order, for example, to place a relevant advertisement. For this purpose we share, among other things, an identifier with these platforms. Whether or not you receive these advertisements depends on your settings on these platforms (with Facebook, for example, you go to Settings > Ads).

We process your data together with providers of social network services if, for example, you post comments, videos, photos, likes and public messages on our social media company page, or post comments about Pigtie on a website or in a social network that is not managed by us. We use your data in order to write a comment

or share information. For the data processing by the social network provider, we refer you to the website of these providers (such as Facebook, Instagram, WhatsApp, etc.).

Bases

We process your data because we have a legitimate interest in doing so. We may also ask for your consent to process your data for advertising and marketing purposes. Do you not give us your consent to this? Then this has no influence on our services for you. You can withdraw your consent via any channel (website, app) at any time. Each channel has its own settings for accepting marketing cookies or not. If you want to withdraw your consent for all channels, you have to do this separately for each channel.

5.6 To conclude and terminate contracts with suppliers and business customers

Purposes

If you have contact with Pigtie in the course of your work, we may process your personal data; for example, in order to determine whether or not you are permitted to represent your company, or to grant you access to our office.

Bases

We process your data in order to perform the contract concluded with you, because we are legally obliged to do so, or because we have a legitimate interest in doing so.

5.7 To comply with legal obligations

Purposes

On the basis of certain (international) laws and regulations, we have to collect data about you. On the basis of the German Act on the Prevention of Money Laundering and the Financing of Terrorism, for example, we have to carry out a (more detailed) investigation if you have certain assets or if there is an unusual deposit into or withdrawal from your Pigtie account.

Laws and regulations may also oblige us to forward data about you to a governmental body or a supervisory authority; for example to the Federal Financial Supervisory Authority or the Bundesbank. As we have to comply with legal obligations and contracts, we have to pass on data about you to the German or a foreign tax authority. In addition, we have to process personal data in the context of our duty of care where there is a reason to do so.

Creation and storage of recordings

We make recordings of, for example, telephone calls, email traffic and chat sessions, and may store these. We do this in order to comply with legal obligations, for example in the context of financial investment brokerage. We may also do this for the purposes of providing evidence, quality assurance, combating and investigating fraud, and training, coaching and assessing employees.

Bases

We process your data because this is required by law, or because we would otherwise be unable to perform the contract concluded with you, or where we have a legitimate interest in processing your data in order to comply with a legal or other statutory obligation.

5.8 For our corporate management

Purposes

As a financial investment broker, we consider it important and necessary that we have a good overview of our customer relationships. This also includes knowing whether you cooperate with other parties that may pose a risk. In order for us to obtain this overview and then be able to take measures, we process your personal data.

In addition, we use data in order to record and improve our business processes, so that we can assist you better or make our processes more efficient. Insofar as this is possible, we will first anonymise or pseudonymise your data.

Audits and investigations

We also use your data to carry out (internal) audits and investigations, for example in order to investigate whether new rules have been properly implemented or to record risks.

Bases

We process your data because this is required by law or because we have a legitimate interest. The processing of your data may also be necessary for the performance of the contract concluded with you.

5.9 For archiving purposes

Purposes

We do not collect more personal data than is necessary in the context of the purposes stated above. If we do not retain the data for these purposes, we may nevertheless retain the data for archiving purposes. This means that the data is used only in court proceedings or for historical, statistical or scientific purposes.

Bases

When processing personal data for the purposes of archiving, scientific or historical research or for statistical purposes, we rely on the legitimate interest of Pigtie, of the financial sector or of our customers and employees.

6 Where and for how long does Pigtie store my personal data?

Your personal data is stored carefully and for no longer than necessary for the purpose for which it is processed.

In general, we only process personal data for as long as this is necessary in order to fulfil our contractual and legal obligations. Data processing is necessary, among other things, for the performance and settlement of the contract, including the defence and enforcement of civil law claims within the relevant limitation periods. Limitation periods can be up to thirty years under §§ 195 et seq. of the German Civil Code; the standard limitation period is three years. In addition, tax, commercial, fiscal and other statutory retention obligations must be observed. The periods provided for there for retention/documentation are six to ten years plus the assessment limitation period of a further four years. In order not to infringe statutory provisions or lose the opportunity to enforce a claim or defend ourselves against one, we reserve the right to delete the data only after the expiry of the last period that legitimises the storage of the data.

As a guideline, it can be said that in most cases this is seven (7) years after the end of the contract or of your business relationship with Pigtie. Sometimes the retention period is longer or shorter, for example at the request of the supervisory authority, or if you have lodged a complaint.

In that case the period for retaining this complaint data is five (5) years. Another example is that we store telephone conversations for a maximum of six (6) months. For your transaction data that you forward to Pigtie, for example, the rule is that it is removed from the Pigtie systems after thirteen (13) months at the latest, or earlier if you switch off the roundups investing or calculation function or terminate your contract with Pigtie. If you no longer want Pigtie to have access to the transaction data of your analysis account, you can withdraw consent for the use of your transaction data. You can do this via the Pigtie app.

Your personal data and transaction data are stored in encrypted form in a data centre in Germany (Frankfurt) and processed in Belgium. For encryption we rely on AES, the most secure encryption method in the world. All data is transmitted via an encrypted SSL/TLS connection.

7 Does Pigtie also process special categories of personal data?

Special categories of personal data are sensitive data, for example your social security number or data about a possible criminal past. Pigtie may obtain access to databases that indicate whether or not you have ever been involved in money laundering or the financing of terrorism, and may have criminal law data processed for this purpose. The purpose of these databases is to protect the interests of financial institutions and their customers.

We also process special categories of personal data in the context of the transaction data that you share with Pigtie via your current account, for example if you make a payment at a pharmacy or transfer money to a political party. Data about your health or your political opinions can be derived from this. Pigtie does not use this data for its own service.

We only process special categories of personal data where we are obliged to do so by law, with your consent, or where you ask us to. Do you request us to record special categories of personal data about you, or do you make this data public yourself? In this case we only process this data where it is necessary for the service.

8 Does Pigtie make automated decisions about me?

Automated decisions are decisions about you that are made by computers and no longer by people. The law permits Pigtie to use automated decisions, including the creation of profiles. However, certain rules apply to this. Does a decision have legal consequences for you? Or can this decision cause you problems? In this case we may not make an automated decision about you, unless this takes place in the context of a contract that you would like to conclude with Pigtie, or where it is legally permissible, or where you give your consent to it. In such situations you have the right to consult someone from Pigtie.

You also have the right to object. You can also request us to stop having the decision made by computers.

Pigtie does not currently make any fully automated decisions about you that could affect you to a significant degree.

9 Who at Pigtie has access to my data?

Within Pigtie, your personal data can only be used by employees who need access to it because of their position.

Our employees and, of course, we ourselves are bound by a duty of confidentiality.

10 Does Pigtie also use personal data for other purposes?

If we want to use data for a purpose other than the one for which it was originally processed, this is only possible where there is a close connection between the two purposes.

11 Does Pigtie pass my personal data on to third parties and to other countries outside the EU?

Your data is passed on to third parties outside Pigtie where we are legally obliged to do so, because we have to perform a contract with you, or because we engage another service provider, for example in the context of combating fraud, preventing money laundering, preventing the financing of terrorism and improving the services for you as a customer, as well as in the context of our duty of care.

We pass your personal data on to third parties where we are obliged to do so, for example to (European) supervisory authorities such as the Federal Financial Supervisory Authority, the Bundesbank, the European Central Bank or the tax office.

We also pass on information where this is necessary in order to fulfil the agreements made with you. This may mean that data is transmitted to other parties in countries that do not have the same level of protection for personal data as the European Union. If your personal data is processed in a country with a different level of protection, this may, for example, result in your personal data being examined by the competent national authorities of the countries in which this data is located.

We also pass your data on to third parties that we need in the context of our service, for example to debt collection agencies, bailiffs and lawyers.

Sometimes we engage other parties/business partners that process personal data on our behalf; for example business partners that carry out market research on behalf of Pigtie or business partners that store data for us. These business partners must first be classified by us as sufficiently reliable. We can only engage other business partners where this fits the purpose for which we have processed your personal data, for example for advertising and marketing purposes or for the provision of IT services. In addition, business partners can only receive our engagement where certain agreements have been made with us, demonstrably appropriate security measures have been taken, and confidentiality is guaranteed. Your personal data may also be exchanged with other parties that we engage in order to carry out our business activities or provide our services.

If we ourselves pass your data on to third parties outside the European Union, we take additional measures to protect your data. Not all countries outside the European Union have the same rules for protecting your data as are mandatory within the European Union. Do we use the services of third parties outside the EU? Does the country in which this business partner is located not, in the view of the European Commission, offer adequate protection for the processing of personal data? In this case we will only forward personal data where there are other appropriate safeguards, such as contractual arrangements approved by the European Commission or on the basis of the "Privacy Shield" (USA).

In accordance with the right of access, you will find a list of recipients in the annex to this privacy policy.

12 Provision of the mobile app and use of the mobile app

Description and scope of the data processing

When downloading the mobile app, the necessary information is transferred to the app store, in particular the user name, email address and customer number of your account, the time of the download, payment information and the individual device identifier. We have no influence over this data collection and are not responsible for it. We only process the data insofar as this is necessary for downloading the mobile app onto your mobile end device. When using the mobile app, we collect the personal data described below in order to enable convenient use of the functions. If you would like to use our mobile app, we collect the following

data, which is technically necessary for us in order to offer you the functions of our mobile app and to ensure stability and security:

- IP address
- Date and time of the request
- Time zone difference from Greenwich Mean Time (GMT)
- Content of the request (specific page)
- Access status / HTTP status code
- Volume of data transferred in each case
- Website from which the request originates
- Operating system and its interface
- Language and version of the browser software

On installation, our mobile app generates a device key, which uniquely identifies your mobile end device in order to pair it with the user account. For advertising purposes we use the so-called “Advertising Identifier” (IDFA). This is a unique but non-personalised and non-permanent identification number for a particular end device, which is provided by iOS. The data collected via the IDFA is not linked with other device-related information. We use the IDFA in order to provide you with personalised advertising and to be able to evaluate your usage.

Legal basis for the data processing

The legal basis for the temporary storage of this data and of the log files is Art. 6(1)(f) GDPR, as we have a legitimate interest as the responsible app provider. An additional legal basis in the context of providing our service is Art. 6(1)(b) GDPR.

Purpose of the data processing

The above data is stored in log files in order to ensure the functionality of our mobile app. Only in this way can we genuinely guarantee the security of our information technology systems (for example in order to detect attacks). We also continuously improve the website in order to make it appealing. We need the further data in order to be able to provide the app and the associated services.

Duration of storage

The above data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. Where data is collected in order to provide the website, this is usually the case once the respective session has ended.

Where data is stored in log files, this is the case after seven days at the latest. Storage beyond this period is possible — in that case the user’s IP address is deleted by us or rendered unrecognisable in such a way that it is no longer possible to attribute it to the calling user and the data contained no longer relates to an identifiable person.

12.1 Video identification by an identity verification service provider

Description, purpose and scope of the data processing

In order to facilitate the opening of the account, we offer a video identification procedure for the identification required under the relevant statutory provisions. The video identification is carried out on behalf of and exclusively for the purposes of the custodian bank, expected to be by WebID Solutions GmbH, Friedrichstraße 88, 10117 Berlin, Germany (“WebID”), a company specialising in this. The data processing by WebID takes place as a service provider/processor, and WebID is likewise obliged to comply with all applicable data protection provisions. For the purpose of the video identification, the custodian bank makes available personal data of

the customer (name, date of birth, address, email address, telephone number and preferred language), which is forwarded by us to WebID. In the course of the video identification procedure, a WebID employee then takes photographs of the customer and their identity document (passport, identity card) via the camera of the customer's device. The photographs of the identity document are subsequently transmitted via us to the custodian bank in order to complete the identification, enable the account to be opened and comply with the custodian bank's retention obligations.

Legal basis for the data processing

The legal basis for the data processing is Art. 6(1)(a) and (c) GDPR (consent and legal obligation).

12.2 MessageBird

Description, purpose and scope of the data processing

In order to pair the user's end device with the account, we use the services of MessageBird to send SMS messages to the mobile phone number. In doing so, the user's mobile phone number and a standard message are transmitted.

Legal basis for the data processing

The legal basis for the data processing is Art. 6(1)(f) GDPR (legitimate interest). We have an interest in ensuring and guaranteeing the technical processes, for example pairing an end device with a user account. An additional legal basis for this is Art. 6(1)(b) GDPR (performance of the contract). Further information on the data processing: we have concluded a data processing agreement with MessageBird. MessageBird is a company in the Netherlands, operates under Dutch law and is therefore subject to EU data protection law. You can find MessageBird's privacy policy here: <https://www.messagebird.com/de-de/datenschutz>

12.3 Adjust

When the app is used, we deploy the analysis technology "adjust.io" of Adjust GmbH, Saarbrücker Str. 38a, 10405 Berlin. On our behalf, adjust.io collects and uses the IP address and — unless deactivated by the user in the system settings of their device — temporary device identification numbers. This data is pseudonymised immediately after it is collected and before it is processed further.

It is therefore not possible to draw direct conclusions about you as a person. The information collected through this use is used solely to analyse the function and use of the app, for example by creating aggregated evaluations and graphics on the number of visits and the number of pages accessed per user.

Legal basis for the data processing

The legal basis for the data processing is Art. 6(1)(f) GDPR (legitimate interest). We have a legitimate interest in the provision of effective advertising measures.

Purpose of the data processing

We use this information for our own market research and to optimise our own advertising measures.

Further information on the data processing

You can find further information about the purpose and scope of the data collection and the further processing and use of the data in Adjust's privacy policy at <https://www.adjust.com/privacy-policy/>. The collection and storage of data by Adjust can be deactivated at any time with effect for the future at <https://www.adjust.com/opt-out>.

12.4 Analytics through Google Firebase

Description and scope of the data processing

We use the Firebase technology provided by Google (Google Ireland Limited ("Google"), Gordon House, Barrow Street, Dublin 4, Ireland). Firebase is part of the Google Cloud Platform and, in addition to a real-time database, offers further services:

- Firebase Analytics enables the analysis of the use of our offering. This records information about the use of our app, transfers it to Google and stores it there. For this, Google uses the end device's advertising ID. Google will use the information referred to in order to evaluate the use of our app in anonymised form and to provide further services to us associated with the use of apps.
- Firebase Crash Reporting serves the stability and improvement of the app. In doing so, information about the device used and the use of our app is collected (for example the timestamp of when the app was started and when the crash occurred), which enables us to diagnose and resolve problems.
- Firebase Cloud Messaging serves to enable the transmission of push notifications or so-called in-app messages (messages that are only displayed within the app). In doing so, a pseudonymised push reference is assigned to the mobile end device, which serves as the target for the push notifications or in-app messages.

Legal basis for the data processing

The data processing takes place on the basis of Art. 6(1)(f) GDPR (legitimate interest). We have a legitimate interest in the provision of a functioning and optimised mobile app that provides a certain standard of convenience and technology.

Purpose of the data processing

We use the data processing for the purpose of providing a functional app that corresponds to the state of the art. With the data that is evaluated in anonymised form, we obtain the necessary information that enables us to offer an appealing presentation of our content.

Further information on the data processing and option to object

Where possible, Google Firebase uses servers located in the EU for these services. However, it cannot be ruled out that data is also transferred to the USA. Google has joined the EU-US Privacy Shield, a data protection agreement between the EU and the USA.

In your device settings you can restrict the use of the advertising ID (iOS: Privacy -> Advertising -> Limit Ad Tracking; Android: Account -> Google -> Ads). Push notifications can be deactivated and reactivated at any time in the settings of the mobile end device.

12.5 Notifications (push notifications)

In order to support you as effectively as possible in managing your accounts and contracts, we send you helpful push notifications on your smartphone, such as your weekly roundups. To provide this function we use the Firebase Cloud Messaging technology from Google Firebase. The push notifications are sent to your smartphone by Apple Inc. ("Apple"), One Infinite Loop, Cupertino, California 95014, USA, or by Google Firebase ("Google"), 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

12.6 Customer support

In order to organise and handle our customer support as effectively as possible, we use the software of WhatsApp Inc., 1601 Willow Road Menlo Park, California 94025, USA ("WhatsApp"). As a customer you have the option of contacting us with enquiries via various channels, such as email, Facebook, Instagram or WhatsApp.

FrontApp channels all customer enquiries into one application and helps us to organise customer enquiries with flags (for example in progress or resolved), in order to be able to resolve your enquiry as quickly as possible.

UserEcho serves as a community where you can submit new ideas and discuss them with us.

You can use WhatsApp in order to clarify questions about the use of the Pigtie services in a direct chat with our customer service staff.

13 What rights do I have at Pigtie?

13.1 Right to information

This privacy policy is intended to inform you about what Pigtie does with your data. Sometimes we provide more or different information outside this privacy policy; for example, when we have your data recorded in databases that indicate whether or not you have ever been involved in money laundering or the financing of terrorism. Pigtie will then — where this is permissible — inform you about this separately. If there are further reasons to inform you in addition to the privacy policy, we will do so. We can do this by email, letter or in another way.

13.2 Right of access and rectification

You can ask us whether, and if so which, of your data we process. We are then obliged to give you access to the data that we have processed about you. Do you believe that your personal data has been processed incorrectly or incompletely? Then you can request us to change or supplement the data (rectification).

13.3 Right to erasure of your data

You can request us to delete the data we have stored about you. We do not always have to do this, for example not where we still have to store your data on the basis of legal obligations.

13.4 Right to restriction of processing

You can request us to temporarily restrict the processing of the personal data we have stored about you. This means that we temporarily process less of your data.

13.5 Right to data portability

You have the right to request information from us that you have made available to us in the context of the contract with us or with your consent, in a structured and machine-readable form, in order to receive it or have it transferred to a third party. If you want the data to be passed on directly to a third party, this is only possible where it is also technically feasible. Sometimes you can also retrieve data that you have made available to us yourself, for example your current transaction data: you can consult this via the app.

13.6 Right to object to processing on the basis of a legitimate interest

If we process your data because we have a legitimate interest in doing so, you can object to this. We will then carry out a new assessment in order to determine whether your data may in fact no longer be used for this purpose. We will stop the processing if your interests carry more weight than our interests. We will then inform you about our decision.

13.7 Right to object to direct marketing

You have the right to request us to no longer use your data for direct marketing. It may be that you can only object to contact via a particular channel, for example if you no longer wish to be contacted by telephone but would still like to receive our newsletters. We will then ensure that you are no longer contacted via this particular channel.

Have you addressed one of the requests described above to us? Then we will respond to such a request within one month of receipt.

We may ask you to specify your request for access in more detail; for example if you ask us for access to the telephone recordings. We may then ask you for search criteria such as the time, the number and where the call was made from. In very specific cases we may extend the period within which we respond to a maximum of three months. We will then keep you informed about the progress of your request.

We may ask you to identify yourself when you address a request to us. For example in the case of a request for access. We want to be sure that we pass the data on to the right person. If, for example, we have doubts about your identity or doubts about the security of transmitting your data, we may ask you to come to our office in order to prove your identity and have it checked by us, or to collect your data securely.

It may be that we cannot comply with your request, for example because the rights of others would be infringed, or because the law, the public prosecutor's office or another official body does not permit this, or because we have weighed the interests and the interests of Pigtie or others in processing the data take precedence. We will then also inform you about this.

Do we update your data? Or do we delete your data on request? Then we will inform you about this. Where necessary, we will also inform the recipients of your data in this regard.

14 Where can I turn with a question or complaint?

If you have questions or complaints about the processing of personal data by Pigtie, you can lodge a complaint. You can also contact Pigtie's data protection officer and the data protection officer of your state.

Contact details for lodging a complaint with Pigtie:

hello@pigtie.de

Contact details of Pigtie's data protection officer:

johannes@pigtie.de

Telephone number: +49 176 43 62 40 26

Contact details of the data protection officer of the State of Bavaria:

Prof. Dr. Thomas Petri

Postfach 22 12 19

80502 Munich

<https://www.datenschutz-bayern.de/>

15 Can Pigtie change this document?

Yes, our privacy policy may change from time to time. If there are new data processing techniques, we will adapt the privacy policy accordingly. If these changes are also important for you, we will draw your attention to them or inform you about the changes in a conspicuous general manner. You can always find the most recent version of our privacy policy at www.pigtie.de and in the app. You can also view earlier versions on our website.

Annex 1: List of third-party providers

- Google G Suite
- Facebook
- Facebook Analytics
- Instagram
- WhatsApp
- Firebase Analytics & Notifications (incl. Crashlytics) and Google Cloud
- Google Analytics
- Google AdWords

- Google Remarketing
- YouTube
- ActiveCampaign
- finAPI
- Slack
- Heroku
- Adjust
- Hotjar
- Twitter
- Custodian bank (not yet determined)
- Identity verification service provider (not yet determined)