1. Item

With this data protection notice we inform you about the processing of your personal data by us if you the user is 4M

We will also explain to you the information provided under the EU General Data Protection Regulation (GDPR).

rights to which you are entitled.

The 4M and the web interface are hereinafter referred to collectively as “4M”.

Our general data protection information also applies.

2. Person responsible and data protection officer

We are responsible, **company: MIK Technology GmbH, address: Kirschallee 57, 14469 Potsdam, telephone: +49 15124154416**

Contact details of the data protection officer: **Address: Berlinerstr . 55.10713 Berlin, if necessary telephone: +49 15124154416 of the data protection officer**

3. User account and master data

To use 4M, you need a user account. You can either create this yourself or we can create it for you.

The following master data is assigned to the user account:

• Access data (e.g. email and password)

To use 4M, your mobile number or email address is required.

We can also use your email address within 4M for system-related emails, e.g. notifications of changed data protection notices or workflow notifications (e.g. approvals granted). As part of the registration process, you may receive an email containing a verification code to your email address. This is to ensure that the email address is assigned to you.

We generally store the master data in 4M for the duration of your user account. Your data will also be deleted if you or we delete your user account, for example if we discontinue 4M as a whole or you decide that you no longer want to use 4M .

Within 4M, your contact details are generally not visible to all other 4M users.

Providing your data for the user account is optional. However, you cannot use 4M without your data.

3.1 The application currently collects the following information, which the user must (can) enter independently when using the application:

–phone

–e-mail

–Full name (optional)

–Gender (optional)

–Country of current residence (optional)

The information is necessary for the operation of the application and is stored on the company's server. The user can delete his profile and stop working with the application at his own discretion. Currently, after deleting a profile, we delete all information about the user from the server database and then no longer store any information.

3.2 To verify the User's age, the Application uses a third party called Veriff Private Company (Veriff), which specializes in providing online verification services (https://www.veriff.com). The data protection guidelines can be found at the following link : https://veriff.com/privacy-notice. The main task of the service for us is solely to determine the user's date of birth, which we store on our application server.

3.3 How the Veriff service interacts with our application:

3.3.1. The application has program code installed in the form of a library from Veriff

3.3.2. To start identifying, we send a request to the Veriff server through the Veriff API and initiate a session (we receive a unique identifier tied to the verification of a specific document, but not to the user).

3.3.3 The Veriff programming code is executed in the application and begins validating the user's documents (at this point our application no longer receives data). In this phase, the Veriff library communicates with the Veriff servers (the user submits snapshots of their documents and face).

3.4. After verification of the documents and verification by Veriff that the person matches the information in the documents, the documents are processed. The service uses facial data to compare whether the photo in the documents matches the person's physical (biometric) face to determine that no one else is trying to download another person's documents.

3.5 Our application accesses the Veriff API, receives the following information from user documents and stores it on its server:

- Full name

- Birth date

Our application does not store images of the user's face.

3.6 Please note that pursuant to the agreement concluded between 4M and Veriff , all personal data for the provision of the Veriff Services, including data about individuals, will be processed by 4M as data controller and Veriff will act as data processor . Veriff therefore processes the data on behalf of and under the responsibility of 4M.

3.7 In order to be able to process personal data on behalf of 4M, Veriff, as data processor, commissions other companies (sub-service providers) to provide services. Subservice providers commissioned by Veriff therefore act as subservice providers of 4M. Media files are processed by Google Cloud EMEA and Amazon Web Services EMEA SARL. The legal relationships with these companies are governed by data processing agreements.

The reasons for passing on the personal data to third parties: the sub-service providers are commissioned to provide services to Veriff so that Veriff can provide its services to 4M.

The maximum data retention period is 90 days in accordance with Veriff 's data retention plan for 4M's services. Veriff will not store personal data longer than stipulated by 4M in accordance with the agreements concluded with Veriff .

3.8. Information on how to contact the data protection officer at Veriff legal@veriff.com

From their privacy policy: “We only retain personal data for as long as data retention is required by law or contract or is necessary to provide our services or protect against legal claims. After the retention period has expired, we will permanently delete or anonymize personal data.”

4. Individual functions

Below we explain how your data is handled when you use individual 4M functions. This may also describe functions that are not (yet) available to you.

5. Notifications on mobile devices (push notifications)

We can send you push notifications to your device if it uses the iOS or Android operating system. Push notifications are messages that are displayed on your device even when you are not using the 4M. This is therefore a function of the operating system provider and not of 4M itself.

We use push notifications, for example to inform you about incoming messages. 4M can also be used without the push function.

In order to deliver the push notifications, we must hand over the content of the notifications to a technical service from your operating system provider. In the case of devices with an Android operating system, this is Google Ireland Limited Gordon House, Barrow Street Dublin 4. Ireland and is part of the " Firebase Cloud Messaging" service, for iOS it is Apple Inc., One Apple Park Way, Cupertino , California, USA , 95014. Your device is technically addressed using a pseudonymous code that your operating system provider provides to us and which only applies to 4M and your specific device. We do not provide the operating system provider with any information that directly identifies you, such as your name or email address.

The basis for data transfer to the USA, as an unsafe third country within the meaning of the GDPR, is the provision of the push functionality you expressly request, Art. 49 Paragraph (1) b) GDPR (contract execution).

6. Data processing for analysis purposes

6.1. Server log files (web interface)

In principle, we do not keep server log files. We only activate this when necessary in case of troubleshooting. In this case:

When you access an individual page of the web interface, our web servers record the address (URL) of the page accessed, the date and time of access, any error messages and, if applicable, the operating system and browser software of your device in a log file and the website from which you visit us.

We use the log file data exclusively to ensure the functionality of our services (e.g. error analysis, ensuring system security and protection against misuse) and after the problem has been resolved, deleted after 7 days at the latest or shortened so that no personal reference can be established.

To the extent that log file data can be qualified as personal data in individual cases, the legal basis for processing the log file data is our legitimate interest (error analysis, ensuring system security and protection against misuse).

6.2. Usage statistics

We do not collect anonymous statistics about which functions and pages are used and how often.

7. System permissions

4M requires the following system authorizations on your device and uses them as follows:

Camera: to capture photos you take in 4M and send to us for transmission to Veriff 's ISP for review .

Internet access: to communicate with our servers, for example to retrieve content.

Geolocation access: to determine your location when using 4M proximity finder

8. Additional information on the obligation to provide data, legal basis, data recipients and storage period

Unless stated otherwise in this data protection notice:

8.1. Obligation to provide

You are not obliged to provide personal data.

8.2. Data recipients and data exports

Your data will be sent to the responsible departments within the company responsible for data protection, e.g. the human resources department.

For the technical operation of the servers to manage push messages and to provide the web interface, we can use technical service providers bound to instructions within the EU as part of so-called order processing, in particular for the operation and maintenance of the server on which your data is stored and the web interface can be provided.

Unless otherwise stated in this data protection notice, we will not transfer your data to countries outside the EU and the EEA for which the EU Commission has not determined that they guarantee a level of data protection appropriate to the EU (no transfer to so-called “unsafe third countries”)).

8.3. Storage period

We measure the storage period for your data based on the specific purposes for which we use the data. In addition, we are partly subject to legal retention and documentation obligations, which arise in particular from the Commercial Code (HGB) and the Tax Code (AO). Finally, the storage period is also determined by the statutory limitation periods, which, for example, according to Sections 195 ff. of the German Civil Code (BGB), are usually three years.

On the device on which you installed the 4M, the data stored by the 4M will be deleted if

• You uninstall 4M

• Your user account ends or is deleted.

To the extent that your data is stored on our server in the backend, the explanations in this data protection notice apply.

9. Your GDPR Rights

By law, we are obliged to inform you about your rights under the GDPR. We explain these rights below. You are entitled to these rights under the conditions of the respective data protection regulations. The following presentation does not grant you any further rights.

9.1 . Information

You have the right to request confirmation from us as to whether we are processing personal data relating to you; If this is the case, you have the right to information about this personal data and to the information listed in detail in Art. 15 GDPR.

9.2 . Correction

You have the right to request that we immediately correct incorrect personal data concerning you and, if necessary, complete incomplete personal data, Art. 16 GDPR.

9.3 . Delete

You have the right to request that we delete personal data concerning you immediately if one of the reasons listed in detail in Article 17 GDPR applies, e.g. B. if the data is no longer needed for the purposes pursued.

9.4 . Restriction of processing

You have the right to request that we restrict processing if one of the conditions listed in Article 18 GDPR is met, e.g. B. if you have objected to the processing, for the duration of our review.

9.5 . Data portability

Under certain conditions, you have the right to receive, transmit and - if technically feasible - have the data relating to you that you have provided to us in a structured, common and machine-readable format, Art. 20 GDPR.

9.6 . Complaint

Regardless of other administrative or judicial remedies, you have the right to lodge a complaint with a supervisory authority if you believe that our processing of personal data concerning you violates the GDPR, Article 77 GDPR. You may exercise this right with a supervisory authority in the Member State of your residence, your place of work or the place of the alleged infringement. The contact details of the supervisory authorities in Germany can be found at https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html .

9.7 . Revocation (of consent)

If you have given us data protection consent, you have the right to revoke it at any time with future effect. This also applies to data protection consent that you gave us before the GDPR came into force.

9.8 . Right of withdrawal

You also have the right to object, which is explained at the end of this document.

10. Appendix: Explanations of terms

10.1. Terms

Below we explain some legal and technical terms used in this data protection notice.

a) Processor :

Processors are service providers who process your data for specific purposes and instructions according to our specifications.

b) Personal data:

Personal data (data) is any information relating to an identified or identifiable natural person.

c) Processing:

Processing of personal data is any process related to personal data, e.g. collecting it via an online form, storing it on our servers or using it to contact us.

d) IP address:

The IP address is a number that your Internet provider assigns to your device temporarily or permanently. With a complete IP address, it is possible to identify the connection owner in individual cases, for example using additional information from your Internet access provider.

10.2. Legal basis

The GDPR only allows the processing of personal data if there is a legal basis. We are required by law to inform you of the legal basis for processing your data.

Below we will explain the terms used.

Legal basis / designation / explanation

Art. 6 Para. 1 lit. a) GDPR / Consent / This legal basis allows processing if and to the extent that you have given us your consent.

Art. 6 Para. 1 lit. b) GDPR / Performance of contract / This legal basis permits processing to the extent that this is necessary to fulfill a contract with you, including pre-contractual measures (e.g. execution of the employment contract).

Art. 6 Para. 1 lit. f) GDPR / legitimate interests / According to this legal basis, we are permitted to process data to the extent that this is necessary to protect our legitimate interests (or those of third parties) and your conflicting interests do not outweigh them. Unless otherwise stated, our interests lie in pursuing the stated processing purposes.

Your right to object

You also have the right to object to the processing of personal data concerning you at any time for reasons arising from your particular situation, provided that we base the processing on Art. 6 Para. 1 lit e . or f GDPR. We will then no longer process this data unless we can demonstrate compelling legitimate reasons for the processing that outweigh your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims (Article 21 GDPR).

If we use your personal data for direct advertising (e.g. via email), you have the right to object at any time to the use of your data for these purposes. This also applies to profiling insofar as it is related to direct advertising. Profiling means the use of personal data to analyze or predict certain personal aspects (e.g. interests).