Tomorrow

Data Privacy Policy
Tomorrow Mobile Banking

App of Tomorrow GmbH

I. Introduction

With "Tomorrow" we provide you with a mobile app that you can download from the "Apple App Store" or for Android from the "Google PlayStore" to your mobile device.

With the following information we want to give you as a "data subject" an overview of the processing of your personal data by us as well as your rights from the data protection laws.

Your personal data will always be processed in accordance with the Generell Data Protection Regulation (GDPR) and all applicable country-specific data protection regulations. We have implemented numerous technical and organizational measures to ensure the highest possible protection when processing your personal data.

II. Scope

This privacy statement applies solely to our Tomorrow app.

III. Controller

Controller within the GDPR is:

Tomorrow GmbH
Neuer Pferdemarkt 23
20359 Hamburg
Deutschland
Email: support@tomorrow.one
Website: www.tomorrow.one

IV. Data Protection Officer

If you have any questions or suggestions regarding data protection issues, you can contact our data protection officer at any time:

Niklas Hanitsch

c/o secjur GmbH

Steinhöft 9

20459 Hamburg

Telefon: +49 40 228 599 520

E-Mail: dsb@secjur.com

V. Transmission and disclosure of personal data

Within the scope of our activities, we transmit personal data to external parties (e.g. persons, companies or legally independent organizational units). You can find details on this below under "Services used" with the respective service providers.

VI. Data processing in third countries

We process personal data in a third country. These are countries outside the European Union (EU) and the European Economic Area (EEA). We only process data in third countries where an adequate level of data protection exists in accordance with Art. 44-49 GDPR. You can find details on this in this privacy policy for the respective third-party providers.

VII. Download the Tomorrow app

You can download our app from the Apple App-Store and the Google Playstore. In doing so, a data transfer to Google or Apple will take place.

Provider

Apple App-Store: Apple Inc., Infinite Loop, Cupertino, CA 95014, USA (Apple).

Google Playstore: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland, Mother Company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Google).

Purpose of processing

- Provision of our App
- Offering our contractual services

Legal basis

- Performance of a contract or implementation of pre-contractual measures (Art. 6 Para. 1 Cl. 1 letter b. GDPR)
- Legitimate interest (Art. 6 Para. 1 Cl. 1 letter f GDPR). Our legitimate interest corresponds to the above-mentioned purposes.

Privacy Policy of Apple and Google

You can find further information on data processing in the privacy policy of Apple: https://www.apple.com/legal/privacy/de-ww/ and Google: https://policies.google.com/privacy

VIII. Cooperation with Solaris

We work closely with our cooperation partner of Solaris SE, Anna-Louisa-Karsch-Straße 2, 10178 Berlin, Germany (Solaris). All data that we collect from you in the course of the

registration for the use of the Tomorrow app and which at the same time serves the execution of the customer contract with Solaris, we forward to Solaris.

Legal basis

- Performance of a contract or implementation of pre-contractual measures (Art. 6 Para. 1 Cl. 1 letter b. GDPR). Solaris needs your data to fulfill the payment service framework contract concluded with you. Only when Solaris executes the customer contracts on our behalf will we be able to fulfill our contract with you to manage the account via the Tomorrow app.

Joint Controllers according to Art 26 GDPR

For certain processing operations, Solaris and Tomorrow jointly determine the purposes and means of processing the data. For this purpose, we have concluded an jpint controller agreement with Solaris for data processing in accordance with Art.26 DS-GVO. This contract states, among other things, that you can assert all your rights regarding the processing of your data against us and Solaris.

Main content of the agreement

The processing of your personal data in connection with the provision of banking services is generally the responsibility of Solaris. Tomorrow is responsible for all other data processing, e.g. in the context of the provision of functions of the Tomorrow app.

We have regulated in the contract with Solaris that you can assert all your rights in relation to the processing of your data against us and Solaris. Tomorrow is the primary point of contact for your concerns.

In addition, Solaris and Tomorrow are committed to informing each other of any data breaches that come to our attention.

Privacy policy of Solaris

You can find further information on data processing in the privacy policy of Solaris: https://www.Solaris.com/content/partner/kundeninformation_zur_datenverarbeitung_englisch_v1.5.1.pdf

IX. Registration

1. Registration

Description of the processing

Before you can open an account via our Tomorrow app, you need to register on our website. Afterwards you create a user profile.

Processed data

- Your first and last name
- Your e-mail address
- Your nationality
- The country in which you have your permanent residence
- Employment status
- Your date of birth
- Your birthplace

- Your gender
- The country in which you are taxable
- Whether you are taxable in the USA
- Your tax identification number (optional)
- Your invitation code
- Your password

In addition, we process the following personal data during the registration process:

- Browser types and versions used
- the operating system used by the accessing system
- the website from which an accessing system reaches our website (so-called referrer)
- the sub-websites, which are accessed via an accessing system on our website
- the date and time of access to the website
- an IP address
- the Internet service provider of the accessing system.

Legal basis

- Performance of a contract or implementation of pre-contractual measures (Art. 6 Para. 1 Cl. 1 letter b. GDPR)

2. Confirmation email

If you register to open an account in the Tomorrow app with your email address, we will send you an email to the address you provide with a confirmation link (double opt-in procedure). By opening this link you confirm that you are the owner of the email address you provided and that no unauthorized person is misusing your email address.

Processed data

- The time of sending our confirmation e-mail
- The time of opening the confirmation link
- Your IP address

Legal basis

- Performance of a contract or implementation of pre-contractual measures (Art. 6 Para. 1 Cl. 1 letter b. GDPR)

3. Sendgrid

We use SendGrid to send you the confirmation email.

Provider

SendGrid Inc., 1801 California Street, 1801 California St, Denver (USA).

Data protection outside the EU/ EEA

We have concluded standard data protection clauses with Sendgrid

Privacy policy of SendGrid

You can find further information on data processing in the privacy policy of SendGrid: https://www.twilio.com/legal/privacy

4. Registration via CHECK24

We offer you the possibility to register with us via CHECK24. For this you can enter your personal data at Check24, which are necessary for the registration at Tomorrow. CHECK24 then sends us this data and your date of birth, which you entered when creating your CHECK24 account. We will send you a confirmation e-mail where you have to create a password and enter your date of birth for security reasons. We process your personal data to facilitate the registration process for you. We also process your date of birth to verify your identity.

Provider

CHECK24 Vergleichsportal GmbH, Erika-Mann-Str. 62-66, 80636 Munich, Germany (CHECK24)

Legal basis

Legitimate interest (Art. 6 Para. 1 Cl. 1 letter f GDPR). The legitimate interest corresponds to the purposes stated above.

Privacy policy of CHECK24

You can find further information on data processing in the privacy policy of CHECK24: https://www.check24.de/popup/datenschutz/

X. Identification procedure

1. Generell information

You enter into a payment services framework agreement with Solaris on our behalf. Due to the Money Laundering Act ("GwG"), our cooperation partner, Solaris, as a banking institution, is obliged to verify your identity and age when you open an account. For the identification we use the Video-Ident-Procedure and Bankident-Procedure.

2. Video ident procedure

The identification with a valid ID document is carried out via Video-Ident-Procedure. During the registration process for our Tomorrow app, you will be directed to the video identification process via a link.

The actual procedure itself is carried out by the provider IDnow GmbH, Auenstraße 100, 80469 Munich ("IDnow") on behalf of Solaris (order processing). The information you provide

during the registration process is transmitted to IDnow so that IDnow can verify its accuracy using the Video ID process. Since the Video ID process is a prerequisite for the delivery of the services offered by us related to your mobile banking. A secure video connection is established between your mobile device and IDnow. For this purpose, it is necessary that you allow IDnow temporary access to your camera and microphone of your cell phone. For example, IDnow employee can see you through the camera of your cell phone. In the following your ID document, which you have to hold in the camera, will be checked and compared with the data you entered during registration.

Photographs and, if necessary, video recordings of your identity card will be taken to prove that you have completed the procedure. Particular attention is paid to the integrity, authenticity and security features. You will also be asked to read the number of your identity document. Parts of the conversation will also be recorded and stored for this purpose. Once the verification is complete, the data is sent to Solaris. Your ID document's information about size and eye color is blacked out by IDnow before it is sent to Solaris.

Legal basis

- Performance of a contract or implementation of pre-contractual measures (Art. 6 Para. 1 Cl. 1 letter b. GDPR)
- Processing is necessary for compliance with a legal obligation to which the controller is subject (Art. 6 Para. 1 Cl. 1 letter c GDPR).
- Consent (Art. 6 Para. 1 Cl. 1 letter a GDPR), if you have given your consent to Solaris. At the beginning of the video call, you will be asked for your consent by the IDnow employee who will verify your identity to make and process the recordings of you. Consent can be revoked at any time with effect for the future.

Privacy policy of Solaris SE and ID-Now

You can find further information on data processing in the privacy policy of Solaris: https://www.solarisgroup.com/customer-information/germany/de-iban/english/customer-information-on-data-processing-germany-de-iban-english-v1.8-clean.pdf and ID-Now**:** https://www.idnow.io/de/datenschutz/

3. Banking ident procedure

In the Bankident procedure, you can enter your personal data and specify a reference account. You then initiate a microtransaction in the cent range from your bank account, thereby legitimizing yourself as the account holder. In the last step, you receive an SMS-TAN, which is used to create a qualified electronic signature. In order to carry out the bank identification procedure, Solaris works together with Swisscom AG, Alte Tiefenaustraße 6, CH-3050 Bern (Swisscom) and SafeNed-Fourthline B. V., Tesselschadstraße 12, 1054 ET, Amsterdam (fourthline).

Legal basis

- Contract fulfillment and implementation of pre-contractual measures (Art. 6 para. 1 p. 1 lit. b DS-GVO)
- Fulfillment of a legal obligation (Art. 6 para. 1 p. 1 lit. c DS-GVO in conjunction with the GWG)

Privacy Policy of Solaris, fourthline and Swisscom

You can find further information on data processing in the privacy policy of Solaris: https://www.solarisgroup.com/customer-information/germany/de-iban/english/customer-information-on-data-processing-germany-de-iban-english-v1.8-clean.pdf, fourthline: https://www.fourthline.com/privacy-statement and Swisscom: https://www.swisscom.ch/de/privatkunden/rechtliches/datenschutz.html

XI. Fraud prevention and anti-money laundering checks

When you register via our app to use the banking services provided by Solaris, and on an ongoing basis while you use such services, Solaris will perform a risk assessment for fraud prevention and anti-money laundering purposes. For such purposes, Solaris uses SEON Technologies Kft. (Rákóczi út 42. 7. em., Budapest 1072, Hungary) as a service provider under a data processing agreement with Solaris in accordance with Art. 28 GDPR. For the processing activities described in this section, we have entered into a joint controllership agreement with Solaris (Art. 26 GDPR). We will provide you with further information at any time upon request.

In order to perform the risk assessment, we collect and transfer to Solaris the following browser data, device data, traffic data and location data from your device: IP address including type (e.g. commercial, mobile line, university) and whether it is listed as harmful, TOR value, VPN, proxy, number of accessories attached to your device, whether your phone is muted or not, device system's volume, country code and name of carrier (a) associated with the SIM card and (b) the device is currently using, device model type and unique identifier, system uptime, iCloud token, version and name of device given by the user in iOS settings, when the device last booted in UNIX time format and UTC time zone, country code and ID associated with device, cookie session ID, and browser details / settings including scrolling behavior.

Solaris may add additional information and will then transfer such data to SEON along with your email address, name and phone number for performance of a risk analysis regarding potential fraudulent or other illicit activities.

SEON analyses this personal data based on a mathematically-statistically recognised and proven procedure and will provide Solaris with a fraud risk score. As part of the analysis, SEON may perform email analysis, social media lookup or address profiling.

Based on the analysis and risk score, you will be able to complete your registration, be rejected as a new customer, or may be guided through an extended registration process. The decision-making process is automated. If you want to challenge the automated decision and want to have a human review of this automated decision, you can get in touch with us by contacting hello@tomorrow.one. Once you have given your consent and are onboarded, Solaris will continuously collect the above data and perform additional risk analysis via SEON for ongoing fraud risk assessment.

The legal basis of the processing is your consent and the implementation of necessary steps for entering into a contract requested by you (Art. 25 TTDSG, Art. 6 (1) lit. a, Art. 22 (2) lit. a GDPR). [As a new Customer...] While you are free to give your consent, you cannot use the banking service provided by Solaris without consenting, because the fraud prevention and anti-money laundering check is necessary for a secure provision of the banking services by Solaris. As a licensed bank, Solaris has a statutory obligation to fight money laundering by setting up a functioning risk management system and internal security measures as well as an ongoing screening of customers' activities (sections 4, 6 and 10 of the German

Anti-Money-Laundering Act). You can withdraw your consent at any time by email to hello@tomorrow.one, but without consent you will not be able to continue using Solaris' services.

Your personal data will be stored until the purposes of processing these data as set forth above have been achieved, and be deleted within 12 months after performance of the risk assessment at the latest, unless statutory retention obligations apply (e.g. under anti-money laundering, commercial or tax law).

XII. Transmission of your identification data for the use of other services

1. Generell information

Within the scope of using our app, we offer you an investment service with custodian banks or other service providers. For this purpose we cooperate with various custodian banks, where you can conclude custodian contracts or create a portfolio. If you use the service offered by us, we will pass on your stored portfolio data including your identification data to our cooperation banks. This saves you the need for further identification procedures, for example. You can find our current cooperation partners under **3.**

Legal basis

- Consent (Art. 6 Para. 1 Cl. 1 letter a GDPR)

2. Cooperation with Wiwin and Effecta

Wiwin is a cord-investing platform through which one can invest in sustainable projects. As a contractually bound agent in the sense of § 2 para. 10 of the Kreditwesengesetz (KWG), Wiwin cooperates with Effecta GmbH, Am Sportplatz 13, 61197 Florstadt (Effecta). Effecta acts as a liability umbrella for, among other things, crowd-investment platforms and organizes the entire regulatory process.

Provider

Wiwin GmbH & Co. KG, Schneebergerhof 14, 67813 Gerbach (Wiwin)

Privacy policy of Wiwin

You can find further information on data processing in the privacy policy of Wiwin: https://www.wiwin.de/datenschutzerklaerung

Privacy policy of Effecta

You can find further information on data processing in the privacy policy of Effecta: https://www.effecta-gmbh.de/datenschutzerklaerung

XIII. Joint bank account

We offer you the possibility of sharing a bank account. For this purpose, you as the account holder can grant a power of attorney to another Tomorrow customer. After the recipient of the power of attorney confirms this, you can use the account together, check the account balance, make transactions and each receive your own card.

Legal basis

- Contract fulfillment and implementation of pre-contractual measures (Art. 6 para. 1 p. 1 lit. b DS-GVO) for the account holder.
- Consent (Art. 6 para. 1 p. 1 lit. a DS-GVO) for the authorization recipient.

XIV. Bank account change service

Provider

finleap connect GmbH, Gaußstraße 190c, 22765 Hamburg, Germany (finleap connect).

Description and purpose of the processing

You have the possibility to use the bank account change service of finleap connect to change from your current bank to Tomorrow. Basically, you can work directly with finleap connect to make the change without our involvement. But we also offer you the possibility to forward your data directly to finleap connect. If you use this service, we process personal data of you.

Processed data

- Name
- Adress
- Date of birth
- IBAN

Legal basis

- Performance of a contract or implementation of pre-contractual measures (Art. 6 Para. 1 Cl. 1 letter b. GDPR)

Privacy policy of finleap connect

You can find further information on data processing in the privacy policy of finleap connect: https://connect.finleap.com/nutzer-datenschutzerklaerung/

XV. CO2-Footprinting

With our Tomorrow CO2-Footprinting we calculate your personal CO2 footprint based on your shopping behavior. For this we work together with ecolytiq.

Provider

ecolytIQ GmbH, Geusenstr. 8, 10317 Berlin, (ecolytIQ).

Processed data

- Unique & random profile ID
- Transaction details (date and time, amount, description, category code/ MCC)
- Classification in terms of consumption habits
- Targeting in terms of consumption profiles
- Personal consumption/transaction history

- Responses from feedback loops (e.g. specifying your diet)

Legal basis

- Performance of a contract or implementation of pre-contractual measures (Art. 6 Para. 1 Cl. 1 letter b. GDPR)

- If you were already a customer of Tomorrow before the introduction of CO2 footprinting, your consent is the legal basis for the data processing (Art. 6 Para. 1 Cl. 1 lit. a GDPR).

Privacy policy of ecolytiq

You can find further information on data processing in the privacy policy of ecolytiq: https://ecolytiq.com/privacy-policy/

XVI. Push Notifications

1. Generell information

We will send you push notifications. Push notifications are messages that appear on your smartphone even if you are not actively using our app.

Processed data

- Meta and communication data (e.g. Device ID)

Purpose of processing

- Notification of functionalities of our App

Legal basis

- Consent (Art. 6 Para. 1 Cl. 1 letter a GDPR)

Opt-out possibility

You can disable the sending of push notifications at any time in the appropriate settings of your device

2. Firebase Cloud Messaging

Firebase Cloud Messaging is a cross-platform cloud solution for messaging and notification for Android and iOS.

Provider

Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, mother company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Google).

Data protection outside the EU/EEA

We have agreed with Google standard privacy clauses of the European Commission

Privacy policy of Google

You can find further information on data processing in the privacy policy of Google: https://firebase.google.com/support/privacy

XVII. Contact

1. Generell information

We offer you different ways to contact us (e.g. by e-mail, chat or telephone).

Processed data

- inventory data (e.g. first and last name, address)
- Contact information (e.g. e-mail address, phone number)
- Meta and communication data (e.g. IP address)
- Content data (e.g. entered text content, photographs, videos)

Purpose of the processing

- Answering contact requests
- Communication

Legal basis

- Performance of a contract or implementation of pre-contractual measures (Art. 6 Para. 1 Cl. 1 letter b. GDPR), if your request is based on pre-contractual measures or on an existing contract with us.
- Legitimate interest (Art. 6 Para. 1 Cl. 1 letter f GDPR) If your inquiry is independent of contractual or pre-contractual measures, our legitimate interests constitute the legal basis. The legitimate interest corresponds to the above-mentioned purposes.

2. Google

For sending and receiving emails we use e-mail accounts located on Google servers.

Provider

Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland, Mutterunternehmen: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Google).

Data protection outside the EU/ EEA

We have concluded standard data protection clauses with Google.

Privacy Policy of Google

You can find further information on data processing in the privacy policy of Google: https://safety.google/privacy/data/

3. Freshchat

Freshchat serves the purpose of live chat communication between you and Tomorrow.

Provider

Freshworks Inc., 2950 S. Delaware Street, Suite 201, San Mateo CA 94403, USA (Freshworks).

Data protection outside the EU/ EEA

We have concluded standard data protection clauses with Freshworks: https://www.freshworks.com/data-processing-addendum/

Privacy Policy of Freshchat

You can find further information on data processing in the privacy policy of Freshchat: http://freshworks.com/privacy

4. Ultimate.ai

We use a chat bot to communicate with you. A chat bot is a software that answers your questions and informs you about news. The chat bot tries to find answers to your questions.

Provider

ultimate.ai GmbH, Ritterstraße 12-14, 10969 Berlin, Germany

Privacy policy of Ultimate.ai

For more information, please read the privacy policy of Ultimate.ai: https://www.ultimate.ai/privacy-policy

XVIII. Tomorrow IBAN Scanner

1. Generell information

To make the transfer process easier for you, our app offers you the possibility to scan the recipient's e-mail address or IBAN. This way you don't have to type in the IBAN or the e-mail address manually when you want to make a bank transfer. There is the possibility to make a bank transfer using the email address of the recipient if the recipient is also a customer of Tomorrow.

Processed data

- IBAN of the recipient
- Recipient's e-mail address

The scan itself is not saved. This ensures that no other personal data is processed.

Purpose of the processing

- Simplification and optimization of the payment process

Legal basis

- Consent (Art. 6 para. 1 cl. 1 lit. a DS-GVO) for access to your camera and the processing of your personal data

- Legitimate interests (Art. 6 para. 1 cl. 1 letter f DS-GVO) for the IBAN and the e-mail address of the payee. The legitimate interest corresponds to the above-mentioned purposes.

2. Google Play Service "MLKIT

To use the scan function we use a Software Development Kit (SDK). This is a collection of programming tools and program libraries for the development of a software. Specifically, we use the Google Play Service "MLKIT" (Machine Learning Kit) from Google. Due to the concrete way of implementation, no personal data will be passed on to third parties.

Provider

Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (Google).

Data protection outside the EU/ EEA

We have agreed with Google standard privacy clauses of the European Commission

Privacy policy of Google

You can find further information on data processing in the privacy policy of Google: https://safety.google/privacy/data/

XIX. Web Analysis and Optimization Services

1. Generell Information

We conduct analytics to evaluate the usage and functionality of our app. In doing so, we are able to process your interests, certain behavioral patterns or demographic data. This allows us to analyze how you use our app and its content and functions. User profiles can be created as part of the analysis. Additionally we use tools for error analysis.

Processed data

- Usage data (e.g. websites visited, interest in content, time of access)
- Meta and communication data
- Location data

Purpose of the processing

- Range measurement and tracking
- Evaluation of visitor behavior and profiling
- Improving our offer and offering customer-friendly services

2. Bugsnag

Bugsnag allows us to analyze and categorize errors that caused our app to malfunction or crash.

Provider

Bugsnag Inc. 110 Sutter St., Suite 1000, San Francisco, California 94104, USA (Bugsnag).

Processed data

- Device information (device ID, user settings, location information, mobile operator and operating system)
- Details of the page visited at the time of the error
- Time of error

Legal basis

- Legitimate interest (Art. 6 para. 1 Cl. 1 letter f GDPR). Our legitimate interest corresponds to the above-mentioned purposes.
- Consent (Art. 6 Para. 1 Cl. 1 letter a GDPR)

Data protection outside the EU/ EEA

We have agreed with Bugsnag standard data protection clauses of the European Commission:

Privacy policy of Bugsnag

You can find further information on data processing in the privacy policy of Bugsnag: https://docs.bugsnag.com/legal/privacy-policy

3. Flagsmith

Flagsmith is an analysis platform that helps us analyze the usage of our app and display crash reports to improve our app.

Provider

Bullet Train Ltd trading as Flagsmith, 86-90 Paul Street, London Ec2A 4NE.

Processed data

- Marketing Reference ID
- Subscription Type

Legal basis

- Legitimate interest (Art. 6 para. 1 Cl. 1 letter f GDPR). Our legitimate interest corresponds to the above-mentioned purposes.

Privacy policy of Countly

You can find further information on data processing in the privacy policy of Flagsmith: https://flagsmith.com/privacy-policy/

4. Adjust

Adjust works with a variety of partners and can thus document the path a customer takes from an advertisement on a smartphone to the installation of the Tomorrow app. Thereby we are able to measure the success of our advertising

Provider

Adjust GmbH, Saarbrücker Str. 37A, 10405 Berlin, Germany (Adjust).

Description and purpose of the processing

Processed data

- Device information (device identifier, user settings, location information, mobile carrier, and operating system).
- Hashed IP address Mobile identifiers such as the Advertising ID for iOS (IDFA),
- Google Advertising ID or similar mobile identifiers
- Installation and initial opening of an app on the mobile device
- Interaction within an app (e.g., in-app purchases, registration)
- Information about which ads you have seen or clicked on
- Additionally, for the Unbotify / Fraud product: sensor data including touch events, text change counting, accelerometer, gyroscope, bat- tery, light sensor, device hardware specifications, and operating system version.

Legal basis

- Legitimate interest (Art. 6 para. 1 Cl. 1 letter f GDPR). Our legitimate interest corresponds to the above-mentioned purposes.

Privacy policy of Adjust

You can find further information on data processing in the privacy policy of Adjust: https://www.adjust.com/terms/privacy-policy/

5. Braze

We use the services of Braze for marketing purposes such as newsletter marketing and push messages. This enables us to optimize our marketing efforts.

Provider
Braze, Inc., 318 West 39th Street, 5th Floor New York, NY 10018, USA (Braze).

Processed data

- Communication data (e.g. e-mail address)
- Interaction data
- Metadata (e.g. push tokens or the IP address)

Legal basis
Legitimate interests (Art. 6 para. 1 p. 1 lit. f DS-GVO). The legitimate interest corresponds to the purposes mentioned above.

Data protection outside the EU/ EEA
- We have agreed to standard European Commission data protection clauses with Braze: https://privacy.google.com/businesses/processorterms/mccs/

- In addition, Braze publishes a transparency report: https://www.braze.com/company/legal/transparency-report

Braze Privacy Policy
For more information, see Braze's privacy policy: https://www.braze.com/company/legal/privacy

6. Mixpanel

We use services from Mixpanel to track user behaviour in our offers. This enables us to optimise and further develop our services.

Provider

Mixpanel, Inc., 405 Howard St., Floor 2, San Francisco, CA 94105, USA (Mixpanel).

Processed data

- Device information (device identifier, user settings, location information, mobile carrier, and operating system).
- App version,
- IP address.
- Dwell time on specific page

Legal basis

- Legitimate interests (Art. 6 Abs. 1 S. 1 lit. f DS-GVO). The legitimate interest corresponds with our purpose of processing.

Data protection outside the EU/ EEA

- We have agreed to standard European Commission data protection clauses with Mixpanel:
- In addition, Mixpanel has taken further security measures to protect your personal information.

Privacy Policy of Mixpanel

You can find further information on data processing in the privacy policy of Mixpanel: https://mixpanel.com/privacy/

XX. Google Pay and Apple Pay

We offer you the possibility to pay contactless with Google Pay or Apple Pay. This allows you to carry out transactions easily and securely within a "contactless" payment process.

1. Google pay

Provider

Google Pay is Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

Processed data

- Card, authentication and transaction data (e.g. date, time, transaction amount)
- Data for the security of payment transactions.

- Name
- Adress
- Phonenumber

Purpose of processing

- Enabling a contactless and simplified payment method
- Risk of fraud and abuse.

Legal basis

- Performance of a contract or implementation of pre-contractual measures (Art. 6p ara. 1 Cl. 1 letter b. GDPR)
- Legitimate interest (Art. 6 para. 1 Cl. 1 letter f GDPR). Our legitimate interest corresponds to the above-mentioned purposes.

Data protection outside the EU/ EEA

We have agreed with Google standard data protection clauses of the European Commission

Privacy policy of Google

You can find further information on data processing in the privacy policy of Google: https://payments.google.com/payments/apissecure/get_legal_document?ldo=0&ldt=privacynotice&ldl=de and https://policies.google.com/privacy

2. Apple Pay

Provider

Apple, One Apple Park Way, Cupertino, CA 95014, USA (Apple).

Apple does not store any original credit, debit or prepaid cards added to Apple Pay or any transaction data that could be traced back to you. Furthermore, Apple stores only a part of the actual card and device account number as well as a card description.

Purpose of processing

- Enabling a contactless and simplified payment method
- Risk of fraud and abuse

Legal basis

- Performance of a contract or implementation of pre-contractual measures (Art. 6p ara. 1 Cl. 1 letter b. GDPR)
- Legitimate interest (Art. 6 para. 1 Cl. 1 letter f GDPR). Our legitimate interest corresponds to the above-mentioned purposes.

Data protection outside the EU/ EEA

We have agreed with Apple standard data protection clauses of the European Commission

Privacy policy of Apple

You can find further information on data processing in the privacy policy of Apple: https://support.apple.com/de-de/HT203027

XXI. Content Delivery Network (CDN)

1. Generell information

Our website uses a CDN. This is a network of powerful servers that cache content in different locations around the world. A CDN enables us to provide content in the shortest possible time and to relieve the web host by distributing the data traffic. Static content that all website visitors receive in the same form, such as video content from streaming services or code frameworks. Dynamic content is first adapted to the user and only created at the moment of the request. This includes content that is personalized and delivered via web applications, e-mail or online stores. To use the latter, information about the website visitor must first be transmitted to the CDN.

Processed data

- Usage data (e.g. websites visited, time of access)
- Meta and communication data (e.g. IP address)
- Content data (e.g. entered text content, photos, videos)

Purpose of the processing

- Provision of content within the shortest possible time
- Relief of the web host by distributing the data traffic

Legal basis

- Legitimate interest (Art. 6 para. 1 Cl. 1 letter f GDPR). Our legitimate interest corresponds to the above-mentioned purposes.

2. Amazon Web Services (AWS)

Provider

Amazon Web Services Inc., 410 Terry Avenue North, Seattle, WA 98109-5210, USA (Amazon).

Data protection outside the EU/ EEA

We have concluded standard data protection clauses with Amazon: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Privacy Policy of Amazon

You can find further information on data processing in the privacy policy of Amazon: https://d1.awsstatic.com/legal/privacypolicy/AWS_Privacy_Notice_German_2020-08-15.pdf

Further information on data processing

https://aws.amazon.com/de/compliance/germany-data-protection/

XXII. Cloud Service Provider

1. Generell information

We use cloud services accessible via the Internet and executed on the servers of the respective providers. In this context, a back-up of your registration data is stored on servers.

Processed data

- All registration data (IX. Registration / Creating a user profile / inventory data)

Purpose of processing

- Keep a backup of your data to prevent data loss

Legal basis

- Legitimate interests (Art. 6 Para. 1 Cl. 1 letter f. GDPR).

2. Hetzner Cloud

Provider

Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany (Hetzner).

Privacy policy of Google

You can find further information on data processing in the privacy policy of Google: https://www.hetzner.de/rechtliches/datenschutz

XXIII. Rights of the data subject

1. Confirmation

You have the right to ask us to confirm whether personal data concerning you is being processed

2. Right of access by the data subject (Art. 15 GDPR)

You have the right to receive from us at any time and free of charge information about the personal data stored about you as well as a copy of this data in accordance with the statutory provisions.

3. Right to retrification (Art. 16 GDPR)

You have the right to request the correction of incorrect personal data concerning you. You also have the right to request the completion of incomplete personal data, taking into account the purposes of the processing.

4. Right to erase (Art. 17 GDPR)

You have the right to demand from us that personal data concerning you be deleted immediately if one of the reasons provided by law applies and if the processing or storage is not necessary.

5. Right to restriction of processing (Art. 18 GDPR)

You have the right to demand that we restrict processing if one of the legal requirements is met.

6. Right to data portability (Art. 20 GDPR)

You have the right to receive the personal data concerning you that you have provided us in a structured, common and machine-readable format. Furthermore, you have the right to have this data communicated to another person in charge, without hindrance from us, to whom the personal data has been made available, provided that the processing is based on the consent pursuant to Art. 6 Para. 1 letter a GDPR or Art. 9 Para. 2 letter a GDPR or on a contract pursuant to Art. 6 Para. 1 letter b GDPR, and provided that the processing is carried out with the aid of automated procedures, unless the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority delegated to us. In addition, when exercising your right to data transfer in accordance with Art. 20 Para. 1 GDPR, you have the right to request that personal data be transferred directly from one responsible party to another, insofar as this is technically feasible and provided that this does not affect the rights and freedoms of other persons.

7. Right to object (Art. 21 GDPR)

You have the right to object at any time, for reasons arising from your particular situation, to the processing of personal data concerning you that is carried out on the basis of Article 6 para. 1 letter e (data processing in the public interest) or f (data processing based on a balancing of interests) of the DPA. This also applies to profiling based on these provisions within the meaning of Art. 4 No. 4 GDPR.

If you lodge an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate reasons for processing which outweigh your interests, rights and freedoms, or unless the processing serves to assert, exercise or defend legal claims. In individual cases we process personal data for the purpose of direct marketing. You may at any time object to the processing of personal data for the purpose of such advertising. This also applies to profiling, insofar as it is connected with such direct advertising. If you object to us processing your personal data for the purposes of direct marketing, we will no longer process the personal data for these purposes.

In addition, you have the right to object, for reasons arising from your particular situation, to the processing of personal data relating to you which is carried out by us for scientific or historical research purposes or for statistical purposes in accordance with Art. 89 para. 1 of the GDPR, unless such processing is necessary for the performance of a task carried out in the public interest. You are free to exercise your right of objection in connection with the use of information society services, notwithstanding Directive 2002/58/EC, by means of automated procedures involving the use of technical specifications.

8. withdrawal of a data protection consent

You have the right to withdraw your consent to the processing of personal data at any time with effect for the future.

9. complaint to a supervisory authority

You have the right to complain to a supervisory authority responsible for data protection about our processing of personal data.

XXIV. Storage period of personal data

We process and store your personal data only as long as the purpose of storage requires it or as long as it is required by law. If the purpose of storage ceases to apply or if a prescribed storage period expires, the personal data is routinely blocked or deleted in accordance with legal requirements. The criterion for the duration of storage of personal data is the respective legal retention period. After the period has expired, the corresponding data is routinely deleted if it is no longer required for the fulfillment or initiation of a contract.

XXV. Actuality and changes of the privacy policy

This data protection declaration is currently valid and has the following status: March 2022. If we further develop our website and our offers or if legal or official requirements change, it may be necessary to amend this data protection declaration. You can view the current data protection declaration at any time on the website under https://www.tomorrow.one/en-EU/privacy-policy/