

Privacy Policy

(Version 1.9, date: 03.02.2020)

In this Privacy Policy, we shall inform you about the collection, use and processing of personal data when using our website <https://n26.com> (hereinafter: "Website"), our web application (hereinafter: "Web App") and our mobile app (hereinafter: "App"; jointly called: "Services"). Insofar as information refers exclusively to our Website, Web App or App, we shall explicitly point this out to you.

In this context, personal data means all detailed information about personal or factual circumstances of a specific or identifiable natural person, such as e.g. name, telephone number or address. We process your personal data either within our business relation if you are a N26 customer or when you are visiting our website for informative purposes. In addition to that - if necessary for providing our services - we transfer personal data to other companies within the N26 Group or other third parties (e.g. Schufa) who process your data permissibly (e.g. to execute orders or contracts or because of your given consent). Furthermore, we process personal data coming from publicly accessible sources (e.g. records of debtors, trade registers, registers of associations, media, press, internet). The collecting and processing of publicly available data is permitted.

When using additional N26 products or products of our business partners additional personal data might be collected, processed and stored. Please find details concerning the processing of additional data in the respective product category.

Please note that you are not obliged to transfer your information to us; however, if you don't, it will limit your ability to use our services – in particular, you will not be able to have a bank account with us.

Our Websites, Web App or App may contain links to other websites, links or apps of our partner networks or our affiliates. Please note that these links and destinations have their own privacy policies and that we do not take any responsibility or liability for them.

I. Responsible authority

The authority responsible for the collection, processing and use of personal data is:

N26 Bank GmbH, London Branch, a corporation established in Germany and authorised and supervised by the German Federal Financial Supervisory Authority (the "BaFin") and whose London Branch is subject to limited regulation by the UK Prudential Regulatory Authority and the Financial Conduct Authority ("we/us" or "N26").

N26 has appointed a Data Protection Officer, who is accessible via dataprotection@n26.com. Our DPO has a lot of important responsibilities - in particular:

- Supervising our compliance with the GDPR and other data protection laws
- Cooperating with UK supervisory authorities such as the Information Commissioner's Office (ICO)
- Examine internal audit and raise awareness of data protection topics

For the technical provision of our Services, N26 Bank, UK Branch is supported by N26 GmbH, Klosterstrasse 62, 10179 Berlin which is bound by its instructions.

II. Data we collect about you

We will collect and process the following data about you:

- Information you give us about you by filling in forms on our Website, Web App or App, or by corresponding with us (for example, by e-mail or via the chat functions on the Website, Web App or App). It includes information you provide when you register to use the App, download or register the App, subscribe to any of our services, enter into any transaction on the Website, Web App or App, participate in social media functions, enter a competition, promotion or survey and when you report a problem with our Website, Web App or App. If you contact us, we will keep a record of that correspondence. The information you give us may include your name, address, date of birth, e-mail address, phone number, the Device's phone number, username, password and other registration information, details of your bank account including the bank account number, bank sort code, IBAN, details of your debit card, relevant expiry dates and CVC, identification document numbers, copies of identification documents and any other information you provide us in order to prove your eligibility to use our services.
- Information we automatically collect each time you are visiting our Website, Web App or App:
 - technical information, including the internet protocol (IP) address used to connect your computer to the Internet, your login information, browser type and version, etc.;
 - information about your visit, including the full uniform resource locators (URL), clickstream to through and from our site (including date and time), device information etc.;
 - transaction information including date, time, amount, currencies used, exchange rate, beneficiary details, details and location of the merchant or ATMs associated with the transaction or messages sent or received with the payment, etc.;
 - information stored on your Device, including if you allow N26 access contact information from your address book.
- Information to help us deliver our service to you. We work closely with third parties in order to help us deliver our Service to you. These third parties are business partners (such as those we partner with to offer additional N26 Services), sub-contractors in technical, payment and delivery services, search information providers, advertising networks, analytics providers, fraud prevention agencies, credit rating agencies, customer service providers and developers. Information we may collect about you from such parties can include information which helps us to verify your identity or information relating to your payment transactions.
- The personal information we have collected from you will be shared with fraud prevention agencies who will use it to prevent fraud and money-laundering and to verify your identity. If fraud is detected, you could be refused certain services, finance, or employment. Further details of how your information will be used by us and these fraud prevention agencies, and your data protection rights, can be found by <https://www.cifas.org.uk/fpn>.

II. Data processing purpose and legal basis

We process your personal data in accordance with the General Data Protection Regulation (GDPR) if at least one of the following applies:

- The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Art. 6 1b) GDPR). Personal data is processed to conduct financial services and banking transactions in order to fulfill our contractual and pre-contractual obligations. These actions are only taken when requested by you. You find the data processing purpose in the respective product category as well as in the respective Product Terms and Conditions. The data processing can include requirement analysis, consultation, investment management, asset support as well as performing transactions.

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes (Art. 6 1a) GDPR).
In case you gave your consent to the processing of your personal data for specific purposes, the processing is permitted on the legal basis of your consent. Your consent is revocable at any time. If you revoked your consent any processing of your personal data will become unlawful after the revocation. This means that the previous processing of your data remains lawful. You may request information about your given consents at any time.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (Art. 6 1f) GDPR)
If necessary, we process your personal data beyond our contractual obligations in order to protect our legitimate interests or the legitimate interests of a third party, e.g.:
 - data access and data transfer to credit agencies (e.g. Experian) to determine credit risks, prevent criminal activity, etc.
 - examination and optimization of processes concerning requirement analysis and customer approach including customer segmentation and calculation of probability of closure
 - marketing or market and opinion analysis
 - enforcement of claims and defence within legal disputes
 - to ensure IT security
 - to prevent criminal acts
 - for business management and the development of services and products
 - risk management within the N26 Group
- Processing is necessary for compliance with a legal obligation to which the controller is subject (Art. 6 1c) GDPR) and processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 6 e) GDPR)
N26 is subject to several legal obligations as well as regulatory requirements. The purpose of processing your personal data is e.g. verification of your identity and age, prevention of money laundering and fraud, verification of your credit rating, control and reporting obligations due to financial crime laws, tax laws and the risk assessment of the N26.
- Processing on behalf of N26 Bank (Art. 28 GDPR): Where processing of personal data is carried out on behalf of N26 Bank we conclude a separate contract with the processor with respect to this processing. This contract ensures compliance with GDPR and defines sufficient guarantees for the implementation of appropriate technical and organisational measures, which ensure the protection of your rights.
- In terms of the transmission of data, including personal data, to recipients outside of N26 Bank, N26 Bank is subject to banking secrecy (see section 2 "Terms & Conditions - Basic Rules Governing the Relationship between Customer and the Bank"). N26 Bank only transmits data to third parties, when this is required by law, you consented to the transmission or N26 Bank is authorised to issue a bank reference. Under these conditions recipients of personal data may be
 - Public authorities and institutions (e.g. Deutsche Bundesbank, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), European Central Bank, Financial Authorities, Law Enforcement Agency),
 - Other Credit- and Financial Services Institutes or similar institutions, to which we transmit personal data that are necessary for the performance and processing of the business relationship,

- Other companies within the N26 Group for risk controlling due to legal or official obligation.
- Service providers who are processing personal data on behalf of N26 Bank (Art. 28 GDPR): Where processing of personal data is carried out on behalf of N26 Bank we conclude a separate contract with the processor with respect to this processing. This contract ensures compliance with GDPR and defines sufficient guarantees for the implementation of appropriate technical and organisational measures, which ensure the protection of your rights.

Further data recipients may be institutions, for which you consented to the data transmission and released N26 Bank from banking secrecy in this regard or for which N26 Bank is entitled to transmit personal data due to its legitimate interest.

III. Data processing within the framework of N26 products

1. Data collection and processing in case of opening and using the N26 current account

Amongst others, the following data will be collected, used and processed by N26 for the purpose of opening a current account with N26 ("Sign-up") and using the Services of N26:

- First name and surname
- Date of birth
- Place of birth
- Email address
- Nationality
- Registered address
- Mobile telephone number
- National Insurance number
- Identification document including (for details see "Identification process")
- Type of identification document
- Issue date
- ID number
- And issuing authority

Please note that it is not possible to open an account, if you don't provide your personal data.

In order to process transactions N26 receives personal data and transfers personal data according to Art. 4 of the European Funds Transfer Regulation to payers, recipients and other financial institutions.

2. Data transmission in the framework of Google Pay and Apple Pay

In order to be able to use the mobile financial services of Google and Apple, information concerning your current account is transferred to our processor Mastercard MPTS. The information is tokenized at Mastercard MPTS. The tokens are used to authorize and to perform transactions with one of the mentioned service providers. Your personal data will be shared with Alphabet Inc. (Google) or Apple Inc. as Google and Apple provide the technological basis. In case you deactivate these services, the token generated by MPTS is automatically deactivated and erased.

3. Data transmission in the framework of Mastercard Automatic Billing Updater Program

In order to be able to use the Automatic Billing Updater (“ABU”), information concerning your current account is transferred to our processor Mastercard Europe S.A. (“Mastercard S.A.”), 198/A Chaussée de Tervuren, 1410 Waterloo, Belgium. ABU provides automatic updates of information concerning your Mastercard to third party services you use and to which you subscribed with your Mastercard. By doing this ABU helps to reduce preventable card-not-present declines by changes of stored payment account information. For this purpose N26 Bank transmits Cardholder information (cardholder PAN and card expiration date) as well as payment information according to Art. 6 1b) GDPR to Mastercard S.A. Mastercard S.A. will process those Personal Data for the purpose of providing ABU, including hosting and maintaining the ABU database and checking authorization requests against the ABU database.

4. Data transmission within the framework of N26 You/Metal

In order to facilitate your insurance cover within the framework of N26 You/Metal, we collaborate with AWP P&C S.A. (branch for the Netherlands, which operates as Allianz Global Assistance Europe and is a member of Allianz Group). For this purpose, we will transmit your first name and surname, date of birth, email address, N26 reference number and registered address according to Art. 6 1b) GDPR to AWP P&C S.A.

5. Data transmission in the framework of Facebook Custom Audience

In order to display specific ads to our customers or to exclude them from specific campaigns we use Facebook Custom Audience. For this reason we transmit your pseudonymized email address to Facebook, which are deleted by Facebook promptly after the match process is completed. Legal basis is Art. 6 para. 1 lit. a GDPR. You can revoke your consent to this data processing at any time in the N26 Web app. You can find further information about Facebook Custom Audiences on <https://en-gb.facebook.com/legal/terms/customaudience>.

6. Processing in the framework of Moneybeam

In order to facilitate Moneybeam we have to process data from sender and recipient and certain transaction data according to Art. 6 para. 1 lit. b GDPR. Transaction data are the same as for a normal bank transfer with the difference that no IBAN is used, but an email address or phone number and that no data is transmitted to third parties. In order to use Moneybeam the users have to make themselves “visible” and allow access to their contact list. How this works you can see [here](#). This function is based on your consent according to Art. 6 para. 1 lit. a GDPR (see also section II.). You can revoke this consent in the app at any time.

7. Visibility and access to your phone’s contact list when using certain N26 features

In the context of using certain N26 features like MoneyBeam, MoneyRequest or Shared Spaces we ask you to (i) grant us consent to be visible to other N26 users as an N26 client and ii) to allow N26 to access your phone’s contact list. With the first consent you are releasing N26 Bank from banking confidentiality. Because by granting N26 permission to share your status being a N26 customer, we can display this information to your contacts from your contact list in the context of using the N26 features. The second consent will enable N26 to access your phone’s contact list and display which of your contacts are also N26 clients, provided they have likewise made themselves “visible” as such. You may revoke the consent to being visible by accessing the app and opt-out. How to manage your visibility is explained [here](#).

8. Data transmission in the framework of Open Banking

To comply with a request to access your N26 account for payment initiation services, account information services and confirmation on the availability of funds (“Open Banking Request”), your personal data is provided to authorised

third party payment service providers via our processor Token.io Ltd (“Token”), 10 John Street, London, United Kingdom. The personal data Token receives will include your IBAN, Bank Account ID and N26 User ID. If you submit an Open Banking Request we will transfer the requested data to the payment service provider via Token. We provide the personal data you request through a licensed third party described in this section on the basis that it is necessary to comply with our obligation under the Payment Services Regulation 2017 (PSR 2017) to provide an interface for communication with licensed payment service providers of your choice (Art. 6 1 c) GDPR) and that it is necessary to perform our obligations under the N26 current account contract (Art. 6 1 b) GDPR).

9. Data transmission in the framework of the Stripe Top Up Feature

In order to be able to use the Stripe Top Up Feature (“Top Up Feature”), account information is transferred to our processor Stripe Payments Europe Ltd. (“Stripe”), The One Building, 1 Grand Canal Street Lower, Dublin 2, Ireland. The Top Up Feature provides an easy method for new customers to add funds to their accounts instantly. For this purpose N26 Bank transmits information regarding certain of your payment details (which may include your cardholder name, email address, unique customer identifier, order ID, bank account details, payment card details, card expiration date, CVC code, date, time and amount of transaction, merchant name/ID and/or location) to Stripe. Stripe will also process your data in order to fulfil its legal obligations, like monitoring fraudulent payment transactions, know-your-customer obligations and anti-money-laundering screening. Stripe and N26 only exchange anonymized tokens and N26 never sees or stores your card details. The usage of the Top Up Feature is entirely voluntary for eligible customers and you can close it/choose not to utilise it at any point.

IV. Identification procedure

The execution of video and photo identification is performed either on behalf of N26 Bank by an external service provider or directly by employees of N26 GmbH or its subsidiaries on behalf of N26 Bank. In both cases, identity is established by means of a web-based video or photo identification procedure via an encrypted transmission path. In both cases, web-based video and photo identification, N26 Bank may transmit personal data to external service providers for the purpose of verifying your identity.

For the purpose of photo identification your personal data is collected as proof of your eligibility to use our services. The service provider will access the camera of your end device and take photographs of you and the front and rear sides of your personal identification document or the principal page of your passport.

If your country’s regulation requires video-ident procedure you will be asked to identify yourself directly via live video. During the video identity confirmation, the provider must ensure the authenticity of the personal identity document or passport presented by you. For evidentiary purposes the photographs as well as the live video will be recorded and retained as long as required by law. At the start of the video identification, the employee will ask for your express consent according to Art. 6 1a) GDPR to the taking of the photographs and the recording of the conversation.

V. Credit check and data transmission

N26 Bank may share your personal information with the three main credit reference agencies in the UK. Such information is shared for the purpose of N26 Bank’s legitimate interests and the legitimate interests of the relevant credit reference agency, including for the purpose of verifying your identity as well as checking your credit and payment history. For further information, including in relation to how these credit reference agencies

use personal data and their legal grounds under UK data protection law for handling personal data, please read the [Credit Reference Agency Information Notice](#).

VI. Social Plugins

1. Use of Facebook plugins

Plugins from the social network Facebook (Facebook Inc., 1601 Willow Road, Menlo Park, California, 94025, USA) are integrated in our Services. You can recognise the Facebook plugins from the Facebook logo or the “Like button” on our page. You can find an overview of the Facebook plugins here:

<http://developers.facebook.com/docs/plugins/>.

If you visit our Services and click on the Facebook plugin, a direct connection will be established between your browser and the Facebook server. Facebook thereby receives the information that you have visited our site with your IP address. If you click on the Facebook “Like button” while you are logged into your Facebook account, you can link the contents of our pages to your Facebook profile. Thereby, Facebook can associate the visit to our Services with your user account. We hereby point out that as provider of the Services, we do not receive any information on the contents of the data transmitted or their use by Facebook. You can find further information about this in Facebook’s Privacy Policy at: <http://de-de.facebook.com/policy.php>.

If you do not want Facebook to be able to associate the visit to our Services with your Facebook user account, please log out of your Facebook user account.

2. Use of Twitter

Functions of the Twitter service are integrated in our Services. These functions are offered by Twitter Inc., Twitter, Inc. 1355 Market St, Suite 900, San Francisco, CA 94103, USA. By using Twitter and the “re-tweet” function, the websites visited by you are linked to your Twitter account and announced to other users. Data are thereby also transmitted to Twitter.

We hereby point out that, as provider of the Services, we do not receive any information on the contents of the data transmitted or their use by Twitter. You can find further information about this in Twitter’s Privacy Policy at <http://twitter.com/privacy>.

You can change your Twitter privacy settings in the account settings at: <http://twitter.com/account/settings>.

3. Use of LinkedIn

Our Services use functions of the LinkedIn network. The provider is LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA (hereinafter: “LinkedIn”). If you visit our Services and click on the LinkedIn plugin (“recommend button”), a connection to the LinkedIn servers will be established. LinkedIn will be informed that you have visited our Services with your IP address. If you click on the LinkedIn “recommend button” and are logged into your LinkedIn account, it is possible for LinkedIn to associate your visit to our Services with your user account. We hereby point out that, as provider of the Services, we do not receive any information on the contents of the data transmitted and their use by LinkedIn.

You can find further information about this in LinkedIn’s Privacy Policy at:

<https://www.linkedin.com/legal/privacy-policy>

4. Use of Instagram

Functions of the Instagram service are integrated in our Services. These functions are offered by Instagram Inc., 1601 Willow Road, Menlo Park, CA, 94025, USA (hereinafter: "Instagram"). If you are logged into your Instagram account, you can link the contents of our pages with your Instagram profile by clicking on the Instagram button. Thereby, Instagram can associate the visit to our Services with your user account. We hereby point out that as provider of the Services, we do not receive any information on the contents of the data transmitted and their use by Instagram.

You can find further information about this in Instagram's Privacy Policy:

<https://help.instagram.com/155833707900388>

VII. Email newsletter

In our email newsletter, we inform you about our offers. If you would like to receive the email newsletter, we require an email address from you. We will only send you our newsletter if you expressly consent to this as you open an account (so called double opt-in). We will thereby check whether you are the holder of the email address given or its holder is in agreement with receiving the email newsletter. This storage solely serves as proof in case a third party misuses an email address and registers to receive the newsletter without the knowledge of the entitled party. These data will only be used for sending the email newsletter and will not be disclosed to third parties.

In our newsletter, we use the Remarketing functions of the Salesforce Marketing Cloud from the service provider salesforce.com, Inc. The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA (hereinafter: "Salesforce"). If you consent to receiving our newsletter and visit our site via a newsletter, Cookies will be set which will enable N26 to understand the customer's interest in the newsletter.

Furthermore, in the email newsletter, Salesforce uses so-called Web Beacons. Web Beacons (also called ClearGIFs or tracking pixels) are small graphics (approx. 1x1 size GIF files) which among other things are set on websites or in HTML emails in order to provide the website operators with a better understanding of visitors' interactions with the website. Web Beacons fulfil similar functions as Cookies, but they are not visible to the users. Information can be obtained via Web Beacons, in particular about whether the email was opened and whether the user's system is capable of receiving HTML emails.

You can revoke your consent to storage of the data and the email address, as well as their use for sending the email newsletter, at any time. The revocation can be made via a link in the newsletter or via a message to the contact options below.

The newsletter distribution is legally justified due to your prior qualified consent according to Art. 6 1a) GDPR.

VIII. Storage Security and international transfer

As we provide an international service your personal data may also be processed outside of the European Economic Area (EEA) so we can provide the N26 Services. We will need to process your personal data for instance to action a request made by you to execute an international payment, process your payment details, counter terrorist financing solutions, provide global anti-money laundering and ongoing support services. We will take all steps to ensure that your personal data is treated securely and in accordance with this privacy policy.

Insofar as N26 transmits data to states outside of the scope of application of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 for the protection of natural persons during the processing of personal data and for the free movement of data, N26 shall ensure that the recipient of the data guarantees an

appropriate level of data protection. In order to ensure an appropriate level of protection by the recipient of the data, we use the standard contracts of the European Union for the transmission of data outside the EU, as amended.

Unfortunately, the transmission of information via the internet is not fully secure. Although we will do our best to protect your personal data, we cannot warrant the security of your data transmitted to our Website, Web App or App; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

Certain Services include social networking, chat room or forum features. Ensure when using these features that you do not submit any personal data that you do not want to be seen, collected or used by other users.

IX. Profiling

If we should use the possibility of a fully automated person related decision in order to provide our services fast and easy and if it is legally required, we will inform you upfront. You have the right that an individual person is reviewing the result of this automated decision. We process your personal data partially automated to assess certain personal aspects (profiling).

This happens e.g. in the following situations:

- In order to combat money laundering, terrorist financing and other criminal acts, which endanger financial assets. To fulfill these duties, personal data (i.a. within payment transactions) is analyzed, in order to secure our client deposits.
- With targeted marketing we try to only make offers to you which are interesting for you and which meet your needs.
- In order to evaluate your credit rating, we use scoring. Within the scoring process we calculate how probable it is that the respective customer meets his payment obligations. For the calculations we use personal data such as your salary, your expenses, existing obligations, your job, duration of employment, experiences of former contractual relations, repayment of former credits as agreed upon, as well as credit agencies' information. Your scoring is the result of a mathematical-statistical procedure and it is necessary to fulfill the obligations of our credit contract (overdraft or N26 credit) according to Art. 22 2a) GDPR. The score results support our decision making, when a customer wishes to purchase an additional product and it is included in the current risk management.

X. Right of revocation

- Case-related right of revocation
You have the right to revoke the processing of your personal data, which is processed in accordance with Art. 6 1 e) and Art. 6 1 f) GDPR, at any time. This does also include profiling according to Art. 4 (4) GDPR. In case of your revocation your personal data is not processed any longer, except when we have legitimate reasons to continue the processing, which exceed your interests, rights and liberties or when the processing is necessary to enforce, exercise or defend legal claims. The processing of your personal data remains justified until the date of your revocation.
- Right of revocation concerning data processing for marketing purposes. In some cases, we process your personal data for direct advertising. You have the right to revoke the processing of your personal data for advertising purposes at any time. This also applies to profiling, in case it is connected to direct advertisement. In case you revoke the processing of your personal data for direct advertising purposes your personal data is not processed for this purpose. The processing of your personal data remains justified until the date of your revocation. The revocation can be made without a form requirement and

should be send to the following address:
E-mail: Dataprotection@n26.com

XI. Rights

You have the following rights concerning your personal data: right of access according to Art. 15 GDPR, right of rectification according to Art. 16 GDPR, right to erasure according to Art. 17 GDPR, right to restriction of the processing according to Art. 18 GDPR, right if revocation to according to 21 GDPR, as well as the right to data portability according to Art. 20 GDPR. In addition to that, according to Art. 77 GDPR you have the right to appeal e.g. the Information Commissioner's Office (www.ico.org.uk) or refer a complaint to the Financial Ombudsman Service (www.financial-ombudsman.org.uk). However, we would really much appreciate the chance to deal with your concerns before you approach a supervisory authority.

Please address any requests to:
E-mail: dataprotection@n26.com

XII. Deletion and retention periods

We are basically storing and processing your personal data only as long as it is necessary to perform our obligations under the agreement with you or as long as the law requires us to store it. That means, we keep your data as long as you are using N26 and for six years after that to comply with the law. In some cases of fraud or anti money laundering we may be obliged to store your data even longer. Further, if information may be impossible to permanently delete we will put that information beyond reasonable use. Please note that information you have shared with others on our Website, Web App or App may remain publicly available and information which you have transmitted to others, e.g. our partners, will be subject to their privacy policy.

XIII. Changes to Privacy Policy

We will post any changes we make to our Website, Web App and App and, if there are significant changes we will also let you know via email.