Online and Mobile Banking Privacy Notice

Last updated: January 2022

Deutsche Bank recognizes the importance of protecting the privacy of the personal information which has been transmitted to us. We believe that the confidentiality and protection of information entrusted to us by our clients and Online Banking and Mobile Banking users (online users) is one of our fundamental responsibilities. We have been safeguarding our clients' privacy for decades by maintaining strict standards of security and procedures which are specially designed to prevent misuse of this information. This Privacy Notice describes how we, DB UK Bank Limited ("Deutsche Bank"), located at 23 Great Winchester Street, London EC2P 2AX as controller collect and process personal data and other information relating to our clients and their authorised representatives or agents ("you"), when using eBanking services via Online Banking (https://dwouk.db.com) and Mobile Banking. You may wish to refer in addition to the more general Privacy Notice issued to clients of Deutsche Bank, which is available here: https://deutschewealth.com/en/uk/regulatory_information.html

1. What categories of Personal Data do we collect and process?

We collect and process information by which you can be identified ("Personal Data").

This information includes the following Personal Data when you log into Online or Mobile Banking: user name, password and code generated via hard or soft token ("Log-in Data"). You will be provided with the Log-in Data from us when you sign up for the eBanking services. The code will be generated by the token when logging in.

Besides your log-in credentials, we also process the Personal Data available in your eBanking account: such as statements, portfolio data, and transaction data ("Account Data").
We also collect device and usage information, which includes information specific to the device used to access and browse Online and Mobile Banking (including language preferences) ("Usage Information").

2. Why does Deutsche Bank collect Personal Data and what is the legal basis?

We process the personal data in compliance with the provisions of the UK General Data Protection Regulation (UK GDPR)and any other applicable data protection laws..

We collect and process your Log-in Data and Account Data to provide you with the eBanking services and to better serve your financial needs (e.g so that you can access your account statements online)and to administer our business.

We collect, retain and use Usage Data about you for the purposes of better serving you, e.g. to remember your language preferences.

The legal basis for the processing of Log in Data and Account Data is either that this is necessary for the performance of our contract with you or that this necessary for the legitimate interests of the Bank, our client or another party in connection with that contract.. The legal basis for Usage Data are our legitimate interests which are the following: to maintain the performance of Online and Mobile Banking and to analyse usage.

We may also process your Personal Data on the legal basis that this is necessary to meet our legal and compliance obligations, such as in relation to the prevention and detection of financial crime, or for our legitimate interests, such as with regard to risk management and information security.

We may also use your Personal Data to provide you with marketing information about our products or those of our affiliates within Deutsche Bank Group where we consider this may be of interest to you. Again, this is on the legal basis of our legitimate interests

Subject to your rights referred to below, the provision of Personal Data is compulsory. If you do not provide your Personal Data, you cannot use Online Banking and Mobile Banking.

3. How long will Personal Data be stored?

In general terms, we retain your personal data as long as necessary for the purposes for which we obtained it. In making decisions about how long to retain data we take account of the following:

- The termination date of the relevant contract or business relationship;
- Any retention period required by law, regulation or internal policy;
- Any need to preserve records beyond the above periods in order to be able to deal with actual or potential audits, tax matters or legal claims.

4. What are cookies and how do we use them?

Deutsche Bank is committed to the continuous improvement of our services. We use so-called tracking technologies such as cookies and tags for statistical purposes and to improve user experience.
Technically, a cookie is a small text file that is used to store information about a website visit for a limited period of time. The stored information consists of at least two components, the name of the cookie and its content, including the accessed webpages.
Cookies are used to improve the end-user experience by using the former mentioned tracking technologies. Users can configure their browser to prevent or warn against cookies. However certain functions or services might not be available in this case.

5. Who will have access to my Personal Data?

The Personal Data gathered will be stored by Deutsche Bank Switzerland and only accessed by the team responsible for you. In some cases your relationship manager may be employed by a different Deutsche Bank group company. Personal Data will be shared with internal service providers, located in Switzerland (which is deemed by the UK government to have an essentially similar level of data protection laws to the UK ("adequacy")), that provide general IT operations such as application management services. The service providers will process your data on our behalf as data processors and subject to contracts containing appropriate security and confidentiality obligations. It will only be used according to the purpose for which the data has been collected. We reserve the right to disclose your information where required by law, to cooperate with regulators or law enforcement authorities or to protect our rights and property as permitted by law.

6. How is Personal Data protected?

Pages where we collect Personal Data from our website visitors are usually encrypted with your browser's internal encryption module. These pages, as well as the internet banking-system of Deutsche Bank are certified by international accredited certification institutions. Deutsche Bank has implemented additional, comprehensive security procedures for our internet-banking-system. A firewall is deployed as a means to prevent external access to account information from Deutsche Bank's system. We also deploy multiple layers of encryption and other security measures to prevent unauthorised access to client information.

If at any time you are not satisfied with our procedures to protect your privacy or if you have questions regarding the collecting and/or use of your Personal Data or regarding this privacy notice, feel free to contact us.

7. Do we conduct any profiling?

"Profiling" in this context means using an automated process to analyse personal data in order to assess or predict aspects of a person's behaviour. We may use profiling in the following circumstances:

- To help identify potential cases of financial crime;
- To provide you with information on DB products and services that seem likely to be of interest;

- To assess creditworthiness (where automated credit scoring based on a mathematically and statistically recognised and proven procedure assists us with our decision making and ongoing risk management).

8. Your rights

Pursuant to applicable data protection law you may have the following rights:

a. Right of access
You may have the right to obtain from us confirmation as to whether or not Personal Data concerning you is processed, and, where that is the case, to request access to the Personal Data. The access information include – but are not limited to – the purposes of the processing, the categories of Personal Data concerned, and the recipients or categories of recipient to whom the Personal Data have been or will be disclosed.
You may have the right to obtain a copy of the Personal Data undergoing processing. For further copies requested by you, we may charge a reasonable fee based on administrative costs.

b. Right to rectification
You may have the right to obtain from us the rectification of inaccurate Personal Data concerning you. Depending on the purposes of the processing, you may have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.

c. Right to erasure ("right to be forgotten")
Under certain circumstances you may have the right to require us to erase your Personal Data.

d. Right to restriction of processing
Under certain circumstances you may have the right to require us to restrict the processing of your Personal Data. In this case the respective data may only be processed by us for certain purposes.

e. Right to data portability
Under certain circumstances you may have the right to receive Personal Data which you have provided to us, in a structured, commonly used and machine-readable format and you may have the right to transmit this to another entity.

f. Right to object
Under certain circumstances, such as where we process your Personal Data on the basis of legitimate interests – see section 2 above) you may have the right to object, on grounds relating to your particular situation, at any time to the processing of your Personal Data, including profiling, by us and we can be required to stop processing your Personal Data.

g. Right not to be subject to automated decision making.

This enables you to ask us not to make a decision about you that affects your legal position (or has some other significant effect on you) based purely on automated processing of your data. We do not as a rule make decisions of this nature based solely on automated processing and without any human assessment whatsoever. We would notify you specifically if we did.

If you have any concerns about our use of your personal information, or if you would like to exercise your data subject rights you may discuss this with your Relationship Manager or contact our Data Protection Officer at the following address: FAO the Data Protection Officer, DB UK Bank Limited, 23 Great Winchester Street, London EC2P 2AX or you can use the following email address dpo@db.com

You can also complain directly to the UK data protection regulator, the Information Commissioner's Office (ICO). The details to submit a complaint can be found on the ICO website at the following address: https://ico.org.uk/make-a-complaint/.

Various
We reserve the right to modify this Privacy Notice at any time. Nevertheless, we will actively inform you about any significant changes to this notice. .