

Data Protection

*How we handle your data, and your rights
– Information pursuant to articles 13, 14
and 21 of the General Data Protection
Regulation
(GDPR) –*

Dear client,
dear client,

The purpose of this letter is to inform you about the processing of your personal data by DZ HYP AG, and about your claims and rights pursuant to data protection law. The particular products and services you have ordered or agreed upon, as well as the scope of our business relationship, are generally what determines how and what personal data will be processed and used in each individual case.

1. Who is responsible for data processing, and whom should I contact?

The data controller is:

DZ HYP AG

Rosenstrasse 2
20095 Hamburg, Germany
Telephone: +49 40 3334-0
Fax: +49 40 3334-1111

Sentmaringer Weg 1
48151 Munster, Germany
Telephone: +49 251 4905-0
Fax: +49 251 4905-5555

E-mail: info@dzhyp.de

You can contact our corporate Data Protection Officer at:

DZ HYP AG
Rosenstrasse 2
20095 Hamburg, Germany
Telephone: +49 40 3334-2311
E-mail: datenschutz@dzhyp.de

2. What type of sources and data do we use?

We process personal data that we receive from you as part of our business relationship. Where necessary to provide our services, we also process personal data that we have received lawfully (e.g. to execute orders, fulfil contracts or where you have provided us with consent) from other entities of the German Cooperative Financial Network, or from other third parties (e.g. from SCHUFA). Furthermore, we process personal data that we have lawfully obtained from public sources (e.g. debtors' list, land register, register of companies or associations, press, media) and are permitted to use.

Relevant personal data includes personal information (name, address, and other contact details; date and place of birth and nationality), identification data (e.g. official ID data) and authentication data (e.g. a specimen signature). It may also include order-related data (e.g. a payment order), data resulting from us fulfilling a contractual obligation (e.g. payment data, loan facility, product data – e.g. from deposit-taking, lending, or custody business), information concerning your financial situation (e.g. credit quality, scoring/rating information, source of assets), marketing and sales data, documentation data (e.g. records of advisory discussions), data from public registers, as well as other data similar to the categories mentioned.

3. Why do we process your data (processing purpose), and on what legal basis?

We process personal data in accordance with the provisions set out in the EU General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (*Bundesdatenschutzgesetz* – "BDSG"):

3.1 to perform contractual obligations (article 6 (1)(b) of the GDPR)

Personal data is processed (as defined in article 4 (2) of the GDPR) for the purposes of providing or intermediating banking and other financial services as well as transactions in real estate – in particular, to fulfil the contracts we have with yourselves (or to make pre-contractual arrangements) and to execute your orders, as well as in connection with all activities necessary for the operation and administration of a bank and financial services provider.

The primary purposes of the data processing have to do with the specific kind of product (e.g. accounts, credits, securities, deposits, brokerage) and may include things like needs analyses, advisory services, asset management or advisory services, or executing transactions.

Specific details about the purpose of the data processing can be found in the relevant contractual documentation, our General Terms and Conditions of Business and General Loan Terms.

3.2 to determine the balance of interests (article 6(1)(f) of the GDPR):

Where necessary, the extent to which we process your data extends beyond the actual performance of a contract in pursuance

of the legitimate interest of the Bank or a third party. Examples:

- Consulting and exchanging data with credit reference agencies (such as SCHUFA) to determine credit or default risks, or to analyse the needs in connection with seizure-protected accounts ("*Pfändungsschutzkonto*"), or basic accounts;
- testing and optimising the process for conducting a needs analysis for the purposes of direct contact with clients;
- advertising or market and opinion research, so long as you have not objected to your data being used;
- enforcing legal rights and defending our position in legal disputes;
- safeguarding the Bank's IT security and operations;
- preventing and investigating offences;
- video surveillance is used to collect evidence of criminal offences and thus serves to protect clients and staff, as well as the exercise of domiciliary rights;
- measures relating to building and premises security (e.g. access control);
- measures relating to the assertion of our right to exclude people from our premises;
- measures relating to the management of our business and developing products and services.

3.3 where you have given consent (article 6 (1)(a) of the GDPR)

Where you have consented to your personal data being processed for specific purposes (e.g. sharing information within the

Cooperative Financial Network/DZ BANK Group, analysing payment data for marketing purposes), the consent serves as the basis for lawfully processing your personal data in accordance with article 6 (1)(a) of the GDPR. Once given, consent may be revoked at any time. This also applies to withdrawing consent given before the GDPR came into force, i.e. before 25 May 2018, such as under the clause permitting the procurement of data from SCHUFA.

Please note that the withdrawal will only apply going forwards. This means that data processing prior to the withdrawal will not be affected.

3.4 for compliance with a legal requirement (article 6(1)(c) GDPR) or in pursuit of the public interest (article 6(1)(e) GDPR):

In addition, as a bank, we are subject to various different legal obligations, such as statutory requirements (including the German Banking Act (*Kreditwesengesetz*), Anti-Money Laundering Act (*Geldwäschegesetz*), Securities Trading Act (*Wertpapierhandelsgesetz*), tax laws) as well as banking regulatory requirements (including those set out by the European Central Bank, the European Banking Authority, Deutsche Bundesbank and the German Federal Financial Services Supervisory Authority). Purposes of data processing include aspects such as assessing credit quality, checking identity and age, preventing fraud and money laundering, complying with tax auditing and reporting requirements, as well as evaluating and managing risks.

4. Who receives my data?

The parties that have access to your personal data within the Bank are those that

need access so they can perform the Bank's contractual and legal obligations. Processors (as defined in article 28 of the GDPR) we have instructed may also receive data for the purposes set out above; this includes companies involved in financial services, IT, logistics, printing, telecommunications, debt collection, advisory/consultancy services, marketing and sales.

In terms of transferring data to recipients outside of our Bank, under the General Terms and Conditions (*Allgemeine Geschäftsbedingungen*) agreed upon between yourselves and the Bank, we are – first and foremost – required to keep confidential all client-related facts and analyses of which we are aware. We may only share information about you where there is a legal requirement to do so, and where we have your consent, where we are authorised to issue a status report (*Bankauskunft*). In these circumstances, the recipients of personal data can include, for example:

- public bodies and institutions (e.g. Deutsche Bundesbank, the German Federal Financial Supervisory Authority, the European Banking Authority, the European Central Bank, tax authorities) where a statutory or regulatory requirement to do so applies;
- other banks or financial services providers, or similar entities to whom we transfer personal data in order to conduct our business relationship with you (according to the particular contract – e.g. DZ BANK Group entities or members of the Cooperative Financial Network, syndicate partners, correspondent banks, custodian

banks, exchanges, credit reference agencies).

Other recipients include parties with whom you have authorised us to share your data or where you have waived banking confidentiality by way of an agreement or consent.

5. How long is my personal data stored?

To the extent necessary, we process and store your personal data during the course of our business relationship; this includes the initiation and settlement of contracts. Bear in mind that our business relationship may constitute a continuing obligation set to last for several years.

Over and above this, we are subject to various record-keeping and documentation obligations, including under the German Commercial Code (*Handelsgesetzbuch* – "HGB"), the German Fiscal Code (*Abgabenordnung* – "AO"), the German Banking Act (KWG), the German Anti-Money Laundering Act (GwG), and the German Securities Trading Act (WpHG). The time periods set out in these acts require record-keeping or documentation for between two and ten years.

Furthermore, the length of storage is also determined by reference to statutory limitation periods: pursuant to sections 195 et seqq. of the German Civil Code (*Bürgerliches Gesetzbuch* – "BGB"), limitation periods can span up to 30 years, although the usual limitation period expires after three years.

6. Is data transferred to any third-party country or an international organisation?

Data is only transferred to third countries (countries outside the EU) where doing so is necessary to execute your orders (e.g. payment instructions or securities orders), required by law, or where you have provided consent. We will provide separate information in this context, to the extent prescribed by law.

7. What are my data protection rights?

Every affected person has the right of **access** under Article 15 of the GDPR, the right to **rectification** under Article 16 of the GDPR, the right to **erasure** under Article 17 of the GDPR, the right to **restriction of processing** under Article 18 of the GDPR, [the right to object under Article 21 of the GDPR], and the right to **data portability** under Article 20 of the GDPR. There is also the right to lodge a complaint with a supervisory authority (Article 77 of the GDPR).

8. Am I under any duty to provide information?

As part of our business relationship, you only have to provide us with the personal data required to establish and conduct a business relationship, or information we are required to obtain by law. Without this data, we will generally have to decline entering into a contract or executing an order, or to cease performing obligations under an existing contract and terminate it.

In particular, we are required under anti-money laundering regulations to identify you (e.g. by reference to your ID documentation) in order to begin our business relationship. This includes collecting and verify-

ing your name, place and date of birth, nationality, and residential address. To comply with these legal obligations, you have to provide us with the necessary information and documentation required pursuant to the GwG, and immediately bring our attention to any subsequent changes arising over the course of our business relationships. If you do not provide us with the necessary information and documentation, we are prohibited from entering into a business relationship with you as requested.

9. How much of the decision-making process is automated in each individual case?

As a rule, we do not use any fully automated decision-making processes for the purpose of deciding upon the establishment and maintenance of a business relationship (article 22 of the GDPR). Should we use such a procedure in individual cases, we will provide you with a separate notification that we are doing so, where we are legally required to do so.

10. To what extent is my data used for profiling (scoring)?

Some of the personal data we process is processed automatically, with the aim of analysing certain personal aspects (profiling). We carry out profiling in the following cases:

Due to legal requirements, we have a duty to prevent money laundering, terrorist financing, and fraud. As part of this process, we analyse data (such as payments). These measures are also designed to protect you.

We use scoring as part of our process for assessing your creditworthiness. This includes calculating the probability that a client will not comply with his or her payment obligations as contractually required. These calculations take into account aspects such as income situation, expenses, existing debt, profession, length of employment, prior business relationship experiences, due contractual repayment of previous loans as well as information from credit agencies. The scoring system is based on a mathematically and statistically recognised and accepted procedure. The resulting scores help us to make a decision about product transactions, and are incorporated into our ongoing risk management.

Information about your right to object
under article 21 of the General Data Protection Regulation (GDPR)

You have the right to object at any time, for reasons relating to your particular situation, to the processing of personal data concerning you where the data processing is based on article 6(1)(e) of the GDPR (data processing in the public interest) and article 6(1)(f) of the GDPR (data processing to determine the balance of interests).

If you lodge an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds which override your interests, rights and freedoms, or where the processing serves to establish, exercise or defend legal claims.

If you object to us processing your personal data for direct marketing purposes, we will cease to do so.

Right to object when you have given your consent

You also have a right to object regarding future data processing on the basis of consent as defined by article 6 (1)(a) in conjunction with article 7 of the GDPR, and with regard to the processing of special categories of personal data pursuant to article 9 (2)(a) of the GDPR (such as data concerning racial or ethnic origin, political opinions, religious or philosophical convictions, or trade union membership; as well as concerning genetic or biometrical data for the unique identification of a natural person, health data, or data concerning sexual orientation).