

## **HYPO NOE Landesbank für Niederösterreich und Wien AG**

### **Privacy policy and information pursuant to Articles 13 and 14 GDPR**

Date: 01/03/2019

We, HYPO NOE Landesbank für Niederösterreich und Wien AG (“HYPO NOE”), hereby inform you how we will process your personal data and what rights you have under applicable data protection legislation. The content and scope of the specific processing depends on the products and services requested by and/or agreed with you.

#### **1. CONTROLLER RESPONSIBLE FOR PROCESSING**

Responsible for the processing of your personal data:

##### **HYPO NOE Landesbank für Niederösterreich und Wien AG**

Company register number 99073 x, St. Pölten Regional Court (*Landesgericht St. Pölten*)

Address: Hypogasse 1, 3100 St. Pölten

T +43 (0)5 90 910-0

@ [datenschutz@hyponoe.at](mailto:datenschutz@hyponoe.at)

Contact details of HYPO NOE’s **data protection officer**:

Address: Hypogasse 1, 3100 St. Pölten

T +43(0)5 90 910-2203

@ [datenschutz@hyponoe.at](mailto:datenschutz@hyponoe.at)

#### **2. AS SOON AS YOU BROWSE OR VISIT OUR WEBSITE (WWW.HYPONOE.AT), WE WILL PROCESS SOME OF YOUR PERSONAL DATA.**

##### **2.1 Use of our website**

As soon as you browse or visit our website ([www.hyponoe.at](http://www.hyponoe.at)), we will process some of your personal data.

###### **2.1.1 Categories of processed data**

While you browse or visit our website, the following personal data will be processed:

- date and time of access to a page of our website;
- your IP address;

- name of the accessed file and time of access;
- volume of data transferred;
- whether access was successful;
- name and version of browser used;
- website (URL) you visited before;
- certain cookies.

### 2.1.2 Purposes of data processing

Your data is processed for the following purposes:

- to give you with the best experience while visiting our website, including offering you all the relevant information and services and making improvements and adjustments;
- to produce usage statistics;
- to detect, prevent and investigate attacks on/against our website;
- to display personalised site recommendations;

### 2.1.3 Legal basis of data processing

We process your personal data based on

- your consent to the processing of your personal data (Article 6(1a) GDPR) and section 96 (2) Austrian Telecommunications Act (*Telekommunikationsgesetz*, TKG);
- our compelling legitimate interest pursuant to Article 6 (1f) GDPR, which is to make our website more user friendly and to prevent potential attacks.

### 2.1.4 Transfer of your personal data

See item 3.

### 2.1.5 Storage period:

Generally, we store processed data until consent has been revoked. Data may be stored longer or may have to be stored longer to investigate attacks on/against our website, and beyond that, only until relevant limitation periods, statutory retention periods or legal disputes, if any, have ended where the data is needed as evidence.

### 2.1.6 Cookies

Cookies are small text files that enable us to determine frequency of use and number of users on our website. You can disable acceptance of cookies via your browser settings. Please have a look at the instructions provided by your browser's manufacturer to see how individual settings work. Should you disable certain technical and/or functional cookies, this may limit the functionality of our website. Moreover, the cookie banner, which is displayed when you first open our website and which you can open again at any time by clicking on a link in the website's footer, allows you to separately select which types of cookies our website may use and to which extent. Please note that certain cookies which are necessary to properly display the website (but do not contain any personal data) cannot be unselected as they are required cookies. Other cookies – in particular those regarding preferences, statistics and marketing – will be used only with your prior consent. The settings you have selected and any consent you may have granted can be edited or revoked at any time by accessing the cookie banner.

For further details on these cookies and how you can change your cookie settings, please refer to: <https://www.hyponoe.at/de/cookie-hinweis>

## 2.2 Clients

Depending on what is required for any specific product, we process personal data we legitimately received from you in the context of a (potential) business relationship or from publicly accessible sources (e.g. land register, company register, central register of associations, internet) or from registers of debtors (e.g. Kreditschutzverband von 1870 [KSV]) or from credit reference agencies (e.g. CRIF GmbH).

### 2.2.1 Categories of processed data

See ANNEX I.

### 2.2.2 Purposes of data processing

Your data is processed for the following purposes:

- wealth management;
- financial transactions;
- providing and brokering of banking transactions;
- advice on and management of financial services;
- advice on and management of insurance services;
- advice on and management of securities transactions;
- advice on and management of lease transactions.

In the course of our activities we are subject to a great number of regulatory requirements, which may also entail the automated processing of personal data. In this respect, we are obligated to take the following actions (non-exhaustive list):

- Identifying beneficial owners within the scope of checks for preventing money laundering and, if required, transferring such data to the Federal Criminal Police (Financial Markets Anti-Money Laundering Act, FM-GwG);
- transferring personal data to the Financial Market Authority (FMA), the Austrian central bank or the Federal Ministry of Finance (e.g. central credit register pursuant to section 75 Banking Act, accounts register pursuant to the Accounts Register and Inspection of Accounts Act, capital outflow reports pursuant to the Capital Outflow Reporting Act or post-trade transparency pursuant to Article 20 et seqq. MiFIR);
- evaluating existing personal data in the context of risk management (e.g. assessment of credit risks pursuant to CRR) and for the ongoing and comprehensive internal review

of the legality, regularity, efficiency and expediency of the entire undertaking (internal audit; section 42 Banking Act);

- Processing requests from courts and public authorities in connection with (potential) legal guardianship for adults, estates, cancellation of shares, criminal cases, enforced debt collection, money held in trust for wards, and covered bonds;
- monitoring all securities orders and transactions to determine potential market manipulations (MAR and Austrian Stock Exchange Act);
- if necessary, transferring account data to Hypo-Haftungs-Gesellschaft m.b.H within the scope of the statutory deposit guarantee scheme and transferring test data on a quarterly basis (stored only for the duration of the tests being performed) (Federal Act on Deposit Guarantee Schemes and Investor Compensation, ESAEG);
- comparing personal data against sanctions lists published by public bodies (e.g. by the European Union or by the United Nations Security Council).

Your data stated in ANNEX I - item 1. are automatically analysed and prepared for the purpose of a better presentation. This includes the full indexing of your data and **categorisation of turnover**. Categorisation of turnover means the allocation of turnover to individual categories in the case of electronic payment. Subsequently, the data is used for preparing personalised offers, provided that you agree to their processing.

If you agree to participate in a **peer group comparison** and the related transfer of data, your data stated in ANNEX I - item 1. will be processed as follows: A peer group is a group that is comparable based on certain characteristics, e.g. sex, date of birth, marital status, income, expenses, persons living in a household, children, country, federal state. In the case of a peer group comparison, data of the participating persons will be passed on and compared in an anonymised form. The calculated reference values are provided to all participants. Please note that most persons participating in the peer group comparison participate in Austria, which is why the results might not be conclusive for other countries of residence.

#### 2.2.2.1 HYPO NOE 24/7 Internetbanking

HYPO NOE 24/7 Internetbanking makes it possible to execute bank transactions via the Internet. When you opt for service of HYPO NOE, we will send you your personal log-on details for the HYPO NOE 24/7 Internetbanking. You first have to authenticate yourself with these log-on details to get access to your personal banking data. This authentication and all further data transfers are executed through an encrypted https connection. The data are processed at ARZ Allgemeines Rechenzentrum GmbH.

The HYPO NOE 24/7 Internetbanking app comprises the entire range of features of HYPO NOE 24/7 Internetbanking in one app.

The HYPO NOE 24/7 Internetbanking app uses numerous functions of your mobile phone / tablet. The HYPO NOE 24/7 Internetbanking app will use the camera (to record QR codes, FaceID), the fingerprint sensor (ShortPIN), the network connection (to use the web content), the location (only for queries regarding the location of branches and cash dispensers), the system tools (for push notifications), the memory (to execute the 24/7 Internetbanking app), the “deactivation of standby mode” and “vibration alarm control”. This access is necessary in order for the functions of the banking app to be used. In this context, the personal data stored on your device are neither accessed nor processed. Consent to use the functions is given by way of downloading or updating the app. Any revocation of certain functions is only possible with heavy restrictions on the use of the HYPO NOE 24/7 Internetbanking app and / or by not using the app. The functions are accessed only if this is absolutely necessary for the execution of a particular action by the app.

With respect to HYPO NOE Internet banking, tracking data are collected and stored in anonymised form with the help of **Piwik PRO** for optimisation purposes. The tracking data are anonymised by shortening the IP address, stored exclusively in the data centre of the bank and not passed on to third parties. You can deactivate tracking at any time in the Internet banking under “My banking”.

The HYPO NOE 24/7 Internetbanking app uses **push notifications**. This makes it possible for information from the app to be displayed directly on your mobile phone / tablet. The push notification system of your operating system is used for this purpose. It cannot be ruled out that the provider of the operating system of your mobile phone / tablet receives these data and transfers them to the USA. If you do not want this to happen, you should contact your provider directly. Please note that you might not receive push notifications in case of a service disruption. If push notifications are deleted on your mobile phone / tablet, they can still be accessed via the app.

**Co-browsing** is a live demonstration used to support the client. Through this feature, content within one browser window can be jointly and simultaneously navigated by parties that are physically apart (the bank and the client). The bank can neither view nor access information outside of this browser window.

### 2.2.2.2 HYPO NOE Multibanking

We ensure that the personalised security features assigned to you are not accessible to any other parties than you and the necessarily involved payment service provider, and that the data are transferred through secure and efficient channels.

The data created within HYPO NOE Multibanking are visible to the registered user and are used exclusively for account information services. Other persons authorised to operate the respective (securities) account do not have access to it, as long as we do not provide and you do not activate a separate feature for sharing data. The data created by HYPO NOE Multibanking is stored by us for the duration of use of HYPO NOE Multibanking by the respective user. If HYPO NOE Multibanking is deactivated all data entered up to this point will be deleted.

If the business relationship is terminated by the client or if HYPO NOE multibanking is deactivated by the user, all data stored in HYPO NOE Multibanking will be deleted, i.e. the financial products of third-party entities added by the user as well as all data created in HYPO NOE Multibanking. This shall, however, not apply for data subject to statutory retention requirements.

### 2.2.2.3 HYPO NOE ID app

The HYPO NOE ID app is an alternative option to transmit transaction authorisation numbers (TANs) to approve logins and for the signing of transactions. This app is a separate application you have to download and install on your respective devices. When signing a transaction using the HYPO NOE ID app, an encrypted TAN is provided directly in the HYPO NOE ID app. You will be alerted to this through a push notification. This app will provide a recap of the key transaction data, making it possible to review the order to be placed. As with all signing procedures, the TAN is only valid for one login or transaction.

### 2.2.3 Legal basis of data processing

- To fulfil our (pre-)contractual obligations (Article 6 (1b) GDPR).

We process your personal data to carry out banking transactions, financial services and insurance services. Furthermore, we process your personal data to the extent necessary to fulfil the contracts entered into with you.

- To fulfil the legal obligations we are subject to (Article 6 (1c) GDPR).

In addition, we process personal data to comply with regulatory requirements, such as the ones set out in the:

- Austrian Banking Act (*Bankwesengesetz, BWG*)
  - Capital Requirements Regulation (CRR)
  - Austrian Financial Markets Anti-Money Laundering Act (*Finanzmarkt-Geldwäschegesetz, FM-GwG*)
  - Austrian Securities Supervision Act (*Wertpapieraufsichtsgesetz, WAG*)
  - Austrian Accounts Register and Inspection of Accounts Act (*Kontenregister- und Konteneinschaugesetz, KontRegG*)
  - Austrian Capital Outflow Reporting Act (*Kapitalabflussmeldegesetz, KapAbflG*)
  - Market Abuse Regulation (MAR)
  - Austrian Stock Exchange Act (*Börsegesetz, BörseG*)
  - Act on Deposit Guarantee Schemes and Investor Compensation (*Einlagensicherungs- und Anlegerentschädigungsgesetz, ESAEG*)
- Based on compelling legitimate interests pursuant to Article 6 (1f) GDPR.

The bank has a compelling legitimate interest, for instance in the following cases:

- Collecting of personal data from *Kleinkreditevidenz*(KKE) and the warning list maintained by the *Kreditschutzverband von 1870* (KSV) and transfer of personal data to KKE and KSV; A legitimate interest exists, in particular, prior to entering into transactions with a risk of financial default. Creditworthiness checks protect the bank from losses in its lending business and, at the same time, enable it to advise borrowers in a bid to protect them from becoming over-indebted. Please note that, given how important these information sharing systems - which existed already before the GDPR entered into force - are for checking creditworthiness as required by consumer protection and regulatory law, no right to object exists in this case, as can be derived from the balancing of interests requirement as stipulated in Article 21 (1) last sentence GDPR.
- Measures to prevent and combat fraud: The legitimate interest is to protect the client's and the bank's assets;
- Video surveillance: The legitimate interest is to protect the client's and the bank's assets and the employees against criminal offences;
- Syndicated financing;



- Recording of phone calls: The legitimate interest is to protect the client's and the bank's assets (e.g. in cases of complaints); if the phone calls are recorded in the context of securities orders, there is also a legal obligation to fight market manipulation and to secure client orders;
- Internal evaluations to identify market opportunities and client potential;
- Disclosure to group companies;
- Evidence vis-à-vis third parties of persons having attained a certain age (e.g. due to youth protection regulations regarding the purchasing of tobacco products).

#### 2.2.4 Transfer of your personal data

See item 3.

#### 2.2.5 Storage period:

We store your personal data for the stated purposes for the duration of our business relationship (from contract negotiations to ongoing handling until the termination of contract) and beyond that in accordance with legal retention or documentation requirements, such as the ones set out in the:

- Austrian Company Code (*Unternehmensgesetzbuch*, UGB)
- Austrian Federal Tax Code (*Bundesabgabenordnung*, BAO);
- Austrian Banking Act (*Bankwesengesetz*, BWG);
- Austrian Financial Markets Anti-Money Laundering Act (*Finanzmarkt-Geldwäschegesetz*, FM-GwG);
- Austrian Securities Supervision Act (*Wertpapieraufsichtsgesetz*, WAG).

We also have to comply with legal limitation periods, which can - for example pursuant to the Austrian Civil Code (ABGB) - be up to 30 years in certain cases (the general limitation period is 3 years), as well as with warranty periods.

## 2.3 Marketing activities

### 2.3.1 Categories of processed data

See ANNEX II.

### 2.3.2 Purposes of data processing

Your data is processed for the following purposes:

- To create bespoke offers for banking, lease and insurance products tailored to your needs (e.g. in the course of categorising your data - see item 2.2.2.);
- to improve our portals, apps and self-service terminals;
- to develop bank, lease and insurance products, tailored to your personal needs;
- to safeguard against/prevent identity theft, i.e. fraudulent use of your identity;
- to invite you to events hosted by HYPO NOE and its subsidiaries;
- to send you information on products and services (also for marketing purposes) via phone, fax or electronic mail (e-mail, text messages, messenger services);
- to hold raffles/promotional competitions;

### 2.3.3 Legal basis of data processing

- If you have given your consent (Article 6 (1a) GDPR).

If we process personal data based on your consent, such consent determines the purpose and extent of the processing. Consent may be revoked at any time, resulting in any future processing becoming prohibited.

- Based on compelling legitimate interests pursuant to Article 6 (1f) GDPR.

The bank has a compelling legitimate interest, for instance in the following cases:

- Analysis of marketing activities: The legitimate interest is to measure the efficiency of our market activities and to offer suitable products to specific recipients in a targeted manner;
- Analysis of business relationships: The legitimate interest is to survey demand for products and to offer suitable products to specific recipients in a targeted manner; moreover, such analysis is a material part of HYPO NOE's risk management;
- Analysis of payment behaviour: The legitimate interest is to improve our portals, apps and self-service terminals. Such analyses are also material for preventing money laundering and terrorist financing;
- Analysis of visits to our website: The legitimate interest is to survey demand for products and to offer suitable products to specific recipients in a targeted manner;

- Analysis of security incidents (e.g. cases of fraud): The legitimate interest is to prevent criminal offences and protect the client's and HYPO NOE's assets. What is more, HYPO NOE is obligated by law to do so.

Please note that you have a right to object (see item 7).

#### 2.3.4 Transfer of your personal data

See item 3.

#### 2.3.5 Storage period:

In the context of data applications to which you have consented, your personal data will be processed until such consent is revoked (see item 6). We store your personal data for the stated purposes for the duration of our business relationship (from contract negotiations to ongoing handling until the termination of contract) and beyond that in accordance with legal retention or documentation requirements,. As soon as such legitimate purposes cease to exist, we will delete the data.

### 2.4 Ombudsman activities for data subjects

If you contact HYPO NOE's ombudsman as a neutral mediator who helps retail clients to resolve disputes for free, this will also involve some of your personal data being processed.

#### 2.4.1 Categories of processed data

See ANNEX III.

#### 2.4.2 Purposes of data processing

Your data is processed for the following purposes:

- determining the matter in dispute;
- drawing up settlement proposals;
- documentation and archiving;
- if consent has been given, transfer to public conciliation bodies, courts and administrative authorities;
- aggregated reports to the Financial Market Authority (FMA);

Your data are either provided by you directly (in particular by communicating with us via e-mail or other means of communication) or we collect the data ourselves, e.g. in the course of conversations.

### 2.4.3 Legal basis of data processing

We process your personal data

- 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;
- to fulfil the legal obligations we are subject to (Article 6 (1c) GDPR);
- Based on your consent to the processing of your personal data (Article 6(1a) or Article 9(2a) GDPR).

### 2.4.4 Transfer of your personal data

In as far as necessary for the purposes stated above, we will transfer your data to the following recipients:

- legal consultants;
- public conciliation bodies, courts and administrative authorities;
- external IT service providers.

### 2.4.5 Storage period:

We will store your personal data only until our information and business relationship has ended, or beyond that, only as long as is necessary to fulfil our legal obligations or until statutory retention periods or legal disputes, if any, have ended where the data is needed as evidence. On the revocation of consent, see item 6.

## 3. TRANSFER OF YOUR PERSONAL DATA

### 3.1 Data transfer within Austria

Your data will be provided to those employees or departments of HYPO NOE which need your data to fulfil contractual, legal and supervisory obligations, to pursue legitimate interests and for processing based on your consent.

We have to transfer your personal data to public bodies and institutions (e.g. Austrian Financial Market Authority, Austrian central bank, European Banking Authority, European Central Bank, tax authorities) if we are obligated to do so by law.

A transfer of your personal data might also be required in the context of fulfilment of contract and/or data applications used based on your declaration of consent, (e.g. to guarantors of loan agreements; to consortium partners or other credit of financial institutions to fulfil syndicated financing or assignments; to legal representatives). In cases of financing, the data provided by you might also have to be transferred, for instance, to the European Central Bank, the Austrian central bank, Österreichische Kontrollbank (OeKB), the European Investment Bank and the European Bank for Reconstruction and Development.

We will share your personal data with the following companies within the group:  
<https://www.hyponoe.at/de/ihre-hypo-noe/konzerngesellschaften>

Moreover, processors commissioned by us (in particular IT and back office service providers) will receive your data if they need such data to provide their respective service. All processors are contractually obligated to treat your data as confidential and to process them only to the extent necessary to fulfil their service obligations.

Please note that HYPO NOE is an Austrian credit institution and thus obligated to observe banking secrecy pursuant to section 38 Banking Act (*Bankwesengesetz, BWG*). This means that we are prohibited from disclosing or exploiting any information you entrusted us with or made accessible to us based on our business relationship, unless you have expressly agreed to such disclosure in writing or we are legally entitled or obligated to do so.

### **3.2 International data transfer**

Some of the recipients stated above may be located, or process your personal data, outside of Austria. The level of data protection in other countries might not meet Austrian standards. However, we only transfer personal data to countries in respect of which the European Commission has decided that they offer an adequate level of data protection, or we take measures to ensure that all recipients offer an adequate level of data protection. We use standard contractual clauses for this purpose (2010/87/EC and/or 2004/915/EC).

Based on the Foreign Account Tax Compliance Act (FATCA), the bank is obligated to transfer tax relevant data of natural persons taxable in the USA to the US tax authorities. Admissibility of such data exchange is ensured through bilateral agreements.

In addition, it cannot be ruled out that personal data will be processed in third countries by service providers you selected (e.g. in the context of Internet banking by providers of operating systems you selected). If you do not want this to happen, you should contact your provider directly.

### **3.3 Account information service providers and payment initiation service providers**

Should you commission an account information service provider or a payment initiation service provider for the execution of a payment service, we will pass on to such service provider the legally required data of the accounts defined by you for the purpose of fulfilling the commissioned payment service. Data exceeding the scope of such legally required data will not be passed on (in particular, no sensitive data such as safety-related PIN codes). For further information on how the data transferred to the account information service provider or payment initiation service provider is processed and which rights you can exercise in relation to such processing, please contact the account information service provider or payment initiation service provider.

## **4. PROFILING AND AUTOMATED DECISION-MAKING (IN PARTICULAR CHECKING OF CREDITWORTHINESS AND TRANSFER OF DATA TO KLEINKREDITEVIDENZ)**

Before granting a loans, the bank checks the client's creditworthiness (credit scoring). We assess the default risk of people seeking loans based on statistical peer groups. The aim of the calculated score value is to enable a prognosis of how likely it is that the loan applied for will be paid back. To calculate that score value, we use your master data, data on your general financial situation and data on your payment history. If the default risk is too high, we will decline the application for a loan and this might lead to an entry in the Kleinkreditevidenz credit database of KSV 1870 as well as to an internal warning note. Loan applications that have been declined can be viewed in the Kleinkreditevidenz credit database of KSV 1870 for a duration of 6 months, pursuant to a decision of the Austrian Data Protection Authority.

Please note that, given how important these information sharing systems - which existed already before the GDPR entered into force - are for checking creditworthiness as required by consumer protection and regulatory law, no right to object exists in this case, as can be derived from the balancing of interests requirement as stipulated in Article 21 (1) last sentence GDPR.

## **5. YOUR RIGHTS IN CONNECTION WITH PERSONAL DATA**

Under applicable law, you have the right

- to check whether we have stored your personal data and what kind of data, and to receive copies of such data;
- to request rectification, supplementation or erasure of personal data which are incorrect or have not been processed in conformity with the law;
- to request from us to limit the processing of your personal data;
- under certain circumstances, to object to the processing of your personal data or to revoke any consent to the processing of your data given previously; however, any and all data processing activities performed so far shall remain unaffected thereby (see item 6);
- to request data portability;
- to know the identity of third parties to whom your personal data are transferred and to lodge a complaint with the Austrian Data Protection Authority ([www.dsb.gv.at](http://www.dsb.gv.at)) or the supervisory body of another EU member state, in particular where you have your place of residence or work.

## 6. REVOCATION OF CONSENT

Each of these consents may be revoked (in writing and electronically) at any time. To do so, send an e-mail to your account manager or the data protection officer at the following e-mail-address: [datenschutz@hyponoe.at](mailto:datenschutz@hyponoe.at).

Your personal data will be processed until further notice.

Note that revocation applies ex nunc, which means that data processing activities already performed under the consent will remain unaffected thereby. In this respect, HYPO NOE complies with the erasure obligations set out in Article 17 GDPR.

## 7. OBJECTION

Please note that you have the right to object to the processing of personal data which we process based on our compelling legitimate interests on grounds relating to your particular situation; this also applies to any profiling based on these provisions HYPO NOE will then no longer process such personal data unless HYPO NOE can demonstrate compelling legitimate grounds for such processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Please note that data applications used for checking creditworthiness and set up as an information sharing systems are exempt from this right to object (see item 4).

Where personal data are processed for direct marketing purposes, you have the right to object at any time to the processing of personal data concerning you for such marketing, which includes profiling to the extent that it is related to such direct marketing.

## **8. OBLIGATION TO DISCLOSE DATA**

Please provide the personal data which we need for establishing and managing the business relationship and which we are required to collect by law. If you do not agree to this, we are unable to enter into, or continue, a business relationship or the respective contract with you, which is why, in such case, we have to end any existing business relationship with you.

You do not have to disclose any data which are not required for entering into or fulfilling the contract or which are not required under law. You can give your consent for marketing activities; we will be pleased to send you the relevant form upon your request to [datenschutz@hyponoe.at](mailto:datenschutz@hyponoe.at).



## **ANNEX I. CATEGORIES OF PROCESSED DATA – CLIENTS**

NOTE: The list below is a general overview of data that are usually collected and processed in connection with the respective products. This does not mean that we will actually store or process all of these data. If you would like to receive more personalised information, you may request it in accordance with your right of access pursuant to Article 15 GDPR.

### **Products**

#### **1. CURRENT ACCOUNTS**

- Client: Salutation/gender, name, address, date of birth, e-mail address, phone number, signature, bank details, identification data (i.e. ID card data), proof of citizenship, residence permit, residence registration data, marital status, proof of assets, social security number, tax number, employer, duration of employment, living situation, family relations, data on deposits to and withdrawals from your account and other payment references and transfer data (payee, IBAN and payment service provider of payee), client number, signatory number, account number, intended use, account statements/turnover data of your own bank and the other bank, payor, payment and dunning history, terms and conditions, means of payment used, consumption behaviour, savings targets and savings history, account balance, debit cards data
- Payee: Salutation/gender, name, bank details, payment reference, intended use, IBAN and payment service provider of payee
- Payor: Name, bank details, payment reference, intended use, IBAN and payment service provider of the principal

#### **2. SAVINGS**

Salutation/gender, name, address, date of birth, e-mail address, phone number, proof of assets, bank details, identification data, residence registration data, marital status, data from credit reference agencies, savings targets and savings history

#### **3. INVESTMENTS**

Salutation/gender, name, address, date of birth, e-mail address, phone number, proof of assets, bank details, identification data, residence registration data, order data, recordings of telephone conversations in connection with securities orders, securities account number

## 4. LOANS

### 4.1. Consumer loan

- Borrower: Salutation/gender, name, address, date/place of birth, proof of citizenship, e-mail address, phone number, signature, proof of assets, details on income (in particular payroll), monthly spending, amount of various liabilities, collateral and its value, other assets, credit history, creditworthiness data, rating, bank details, terms and conditions, identification data, residence registration data, marital status, number of persons subject to maintenance obligations, employer, duration of employment, school education, data from credit reference agencies
- Guarantor: Salutation/gender, name, address, date of birth, e-mail address, phone number, proof of assets, collateral, bank details, identification data, residence registration data, data from credit reference agencies
- Trustee/Authorised agent: Salutation/gender, name, address, bank details, identification data, phone number, e-mail address
- Lessee(s) of funded properties: Name, identification data, list of rent payments

### 4.2. Operating loan

- Company: Company name, company address, company register number, company register excerpt, business licence
- Person authorised to operate or sign: Salutation/gender, name, address, identification data, phone number, e-mail address

## 5. INSURANCE

Salutation/gender, name, address, date of birth, proof of citizenship, e-mail address, phone number, proof of assets, bank details, identification data, residence registration data, marital status, number of persons entitled to maintenance payments, employer, health data

## **ANNEX II. CATEGORIES OF PROCESSED DATA - MARKETING ACTIVITIES**

### **Marketing with clients and interested parties**

#### **1. GENERAL DATA**

Salutation/gender, name, company name, state-of-the-art address and communication data (address, phone number, e-mail addresses), securities risk class, data obtained during advisory consultations, e.g. your interests, plans, household accounts, newsletter usage and interests deriving therefrom

#### **2. DATA ON BANK, LEASE AND INSURANCE PRODUCTS**

Products (e.g. account, securities, deposits, financing, credit cards, leases, insurance), means of payment used (e.g. cards, cheques, bills of exchange), payment history and payment transactions (e.g. payee/payor, amount, intended use, type and frequency of account movements, consumption behaviour), allocations made in online/electronic banking, savings targets and savings history, referrals, account balances, terms and conditions (e.g. interest rates, expenses, commission fees)

#### **3. DATA ON WEBSITES, APPS, CALL CENTRES, SELF-SERVICE TERMINALS**

Type of use (frequency, time, place, site/location analysis), functions used for all HYPO NOE apps and portals, including the software used for banking transactions (online/electronic banking), IP addresses

#### **4. FOR NATURAL PERSONS, ADDITIONALLY:**

Date of birth, marital status, identification data (i.e. ID card data), living situation, income, employer, job, education/training, family relations, other persons living in the same household

#### **5. FOR LEGAL ENTITIES, ADDITIONALLY:**

Data from the company register (e.g. industry, size, legal form, corporate relations), financial documents (e.g. balance sheets, forecasts, income statement)

## **ANNEX III. CATEGORIES OF PROCESSED DATA - OMBUDSMAN**

### **1. GENERAL DATA**

Name, salutation/gender, reason for complaint, employee/department concerned by the complaint

### **2. REQUIRED DOCUMENTS**

Documents handed over, consent to release from banking secrecy, correspondence