

HYPO NOE LANDESBANK FÜR NIEDERÖSTERREICH UND WIEN AG PRIVACY POLICY AND CLIENT INFORMATION PURSUANT TO ARTICLES 13 AND 14 GDPR

Last revised on 1 July 2023

We, HYPO NOE Landesbank für Niederösterreich und Wien AG ("HYPO NOE"), hereby inform you about how we process your personal data in connection with our business relationship with you and about the rights you have under data protection law. The contents and scope of the specific data processing activities will depend on the products and services you have requested or which have been agreed with you.

1. CONTROLLER

The controller of your personal data is:

HYPO NOE Landesbank für Niederösterreich und Wien AG

FN [Business Register Number] 99073 x,
Regional Court [*Landesgericht*] St. Pölten
Address: Hypogasse 1, 3100 St. Pölten
Phone +43 (0)5 90 910-0
@ datenschutz@hyponoe.at

Contact details for HYPO NOE's Data Protection Officer:

Address: Hypogasse 1, 3100 St. Pölten
Phone +43(0)5 90 910-2203
@ datenschutz@hyponoe.at

2. PROCESSING OUR CLIENTS' PERSONAL DATA

2.1 Which data is processed by us as part of the client relationship and from which source does it originate?

We process personal data which we receive in the course of a business relationship or from you as a potential user of our services on a product-related basis. We also process data that we have lawfully received from public sources (e.g. the Austrian Land Register [*Grundbuch*], the Austrian Business Register [*Firmenbuch*], the Austrian Register of Associations [*Vereinsregister*] or the internet) or from debtors' lists or credit agencies (e.g. Kreditschutzverband von 1870, KSV 1870 Information GmbH).

The processed personal data includes your personal details (e.g. name, address, contact details, date and place of birth, nationality), identification data (e.g. ID document details) and authentication data (e.g. specimen signature). Moreover, it may include order data (e.g. payment orders), data from the fulfilment of our contractual obligations (e.g. transaction data from payment transactions), information on your financial status (e.g. credit information, scoring and/or rating data), advertising and marketing data, documentation data (e.g. consultation reports), register data, image and sound files (e.g. video or telephone recordings), information from your electronic communication with the bank (e.g. apps, cookies), processing results which the bank itself generates, and data for the fulfilment of statutory and regulatory requirements. Please find a list of the categories of personal data arranged by product/service in Annex I at the end of this Privacy Policy.

2.2 Purposes of and legal bases for data processing

For the performance of the **contractual obligations (Article 6(1)(b) of the General Data Protection Regulation (GDPR))** your data will be processed for the following purposes:

- carrying out financial transactions;
- providing and negotiating banking transactions;
- advising on and managing of financial services;
- advising on and managing of insurance services;
- advising on and negotiating of securities transactions;
- acceptance and forwarding of securities orders for processing;
- advising on and managing of lease transactions;

In the course of our activities we are subject to a number of **regulatory requirements**, which may also constitute personal data processing. They are, inter alia, contained in the following laws and regulations:

- Austrian Banking Act [*Bankwesengesetz/BWG*]
- Regulation (EU) No 575/2013 (CRR)
- Austrian Act on the Prevention of Money Laundering in the Financial Market [*Finanzmarkt-Geldwäschegesetz/FM-GwG*]
- Austrian Securities Supervision Act [*Wertpapieraufsichtsgesetz/WAG*]
- Delegated Regulation (EU) No 2017/565
- Austrian Accounts Register and Inspection of Accounts Act [*Kontenregister- und Konteneinschaugesetz/KontRegG*]
- Austrian Capital Outflow Reporting Act [*Kapitalabfluss-Meldegesetz/KapAbfLG*]
- Austrian Market Abuse Regulation [*Marktmissbrauchsverordnung/MAR*]
- Austrian Stock Exchange Act [*Börsegesetz/BörseG*]
- Austrian Act on Deposit Guarantee and Investor Compensation Schemes [*Einlagensicherungs- und Anlegerentschädigungsgesetz/ESAEG*]
- Austrian Stock Corporations Act [*Aktiengesetz/AktG*]

On the basis of **legal obligations (Article 6(1)(c) GDPR)** we will process the following data, among others:

- identification of beneficial owners as part of anti-money laundering checks and transmission to the Austrian Federal Office of Criminal Investigations [*Bundeskriminalamt*] (*FM-GWG*), where appropriate;
- transmission of personal data to the Financial Market Authority, the Austrian Central Bank (OeNB) or the Federal Ministry of Finance (e.g. central credit register as defined in Section 75 *BWG*, account register as defined in the *KontRegG*, capital outflow reports as defined in the *KapAbfLG*, or post-trade transparency as defined in Article 20 *et seq.* of Regulation (EU) No 600/2014);
- analyses of available personal data as part of risk control (e.g. rating of the credit risk as defined in the CRR) and for internal regular and comprehensive checks of whether the entire business is lawful, proper and expedient (internal audit; Section 42 *BWG*);
- processing of enquiries by courts and public authorities in connection with (potential) adult guardianships, decedents' estates, invalidation procedures, criminal matters and levy of execution, ward money or covered bonds;
- where required, transmission of account details to Einlagensicherung AUSTRIA Ges.m.b.H. (ESA) in connection with deposit protection and quarterly transmission of test data, which will only be stored for the duration of the test runs (*ESAEG*);
- comparison of personal data to sanctions lists published by public agencies (e.g. the European Union or the United Nations Security Council).

In connection with your **consent pursuant to Article 6(1)(a) GDPR** we will process your personal data only in accordance with the purposes described in the declaration of consent and within the scope defined therein. On the basis of your consent we will process your data for marketing purposes (see section 3).

For safeguarding **legitimate interests as defined in Article 6(1)(f) GDPR** of the bank or of third parties data will be processed beyond actual performance of the contract, including in the following cases:

- Collection of personal data from the Register of Small Loans [*Kleinkreditevidenz/KKE*] and the warning list of Kreditschutzverband of 1870 (*KSV*) and transmission of personal data to *KKE* and *KSV*. There is a legitimate interest in particular prior to entering into transactions that involve a risk of financial loss. Performing credit checks serves to protect the bank from losses in the lending business and at the same time offers the possibility to protect borrowers from excessive indebtedness by providing advice. Please note that, due to the material significance the information networks that were set up for performing credit checks before the GDPR entered into force have for credit checks required under regulatory provisions and consumer protection provisions, there is, in principle, no right to object, not least because of the weighing of interests provided for in the last sentence of Article 21(1) GDPR;
- Measures to prevent and combat fraud. The legitimate interest is the prevention of criminal offences and the protection of the assets of the clients and the bank; moreover, HYPO NOE is required by law to analyse security-relevant incidents such as cases of fraud
- CCTV surveillance: The legitimate interest is the protection of the safety and assets of the clients and the bank and the protection of employees against criminal offences;

- Syndicated financing;
- As part of legal action and defence of legal disputes;
- Internal analyses for identifying market opportunities and client potential;
- Measures for business control and further development of products and services;
- Marketing (by post) or market and opinion surveys to the extent that you have not objected to the use of your data for these purposes pursuant to Article 21 GDPR;
- The debit card allows cardholders to prove vis-à-vis third parties that they have attained a specific age that is relevant to the third party (e.g. due to youth protection regulations regarding the purchase of tobacco products). The third party will obtain the bank's confirmation in this respect by means of the debit card which is presented for this purpose by the data subject in person or to technical equipment.

2.2.1 Data processing in HYPO NOE 24/7 Internet Banking

HYPO NOE 24/7 Internet Banking allows our clients to take care of their banking business online. When you open a HYPO NOE product we will provide you with your personal access details for HYPO NOE 24/7 Internet Banking. In order for us to be able to access your personal banking details you will first have to authenticate yourself using the access details. The authentication and all other data transmissions will be carried out via an encrypted https connection. The data will be processed in our data centre, Accenture TiGital GmbH.

The HYPO NOE 24/7 Internet Banking app constitutes the entire functions of HYPO NOE 24/7 Internet Banking in one app.

The HYPO NOE 24/7 Internet Banking app uses a number of features of your mobile phone/tablet. The HYPO NOE 24/7 Internet Banking app will also access the camera (for capturing QR codes, FaceID), the fingerprint sensor (Touch ID), the network connection (for using web content), the location (only for location retrieval in the branch and ATM finder), system tools (for push messages), the memory (for running the 24/7 Internet Banking app), the deactivation of the standby mode and the control of the vibration alarm. These features will be accessed for you to be able to use the app's features. The personal data stored on your mobile device will not be accessed or processed. Consent to use of the features is given when downloading or updating the app. Withdrawal of consent to certain features means having to accept considerable restrictions on the HYPO NOE 24/7 Internet Banking app or the fact that the same cannot be used. The features will only be accessed where this is absolutely necessary for the app to carry out a specific action.

By means of **Piwik PRO** tracking data is collected and stored in an anonymised form in HYPO NOE 24/7 Internet Banking for optimisation purposes. The tracking data is anonymised by truncating the IP address, which is stored exclusively in the bank's data centre and not disclosed to third parties. You can deactivate tracking in the internet banking under "My banking" at any time.

HYPO NOE apps require the use of **push messages**. This makes it possible to display information from the app directly on your mobile phone/tablet. The push notification system of your operating system will be used. It cannot be excluded that the provider of the operating system of your mobile phone/tablet will obtain this data and then transmit it to the United States of America. If you do not want this, you should contact your provider directly. Please note that you may not be able to receive push messages due to a fault. Even if they have been deleted on the mobile phone/tablet, push messages may still be retrieved in the app.

Co-browsing is a guided live presentation for client support purposes. It allows physically separated parties (the bank and the client) to simultaneously and jointly navigate content in a browser window. The bank is not able to view or access information outside the browser window.

2.2.2 Data processing in the HYPO NOE ID app

The HYPO NOE ID app supports strict customer authentication which, according to Directive (EU) 2015/2366, is required during login and signing of orders in online banking. You may download the HYPO NOE ID app from your preferred app store and install it on your mobile device (iOS, Android) or your Windows computer (Windows 10 or higher). When logging into HYPO NOE 24/7 Internet Banking or the

HYPO NOE apps and when signing orders, several encrypted codes will be sent to the HYPO NOE ID app.

You will be notified thereof by push messages. After logging into the HYPO NOE ID app the correct code must be chosen by tapping on it to complete login or sign the order.

When signing orders, the data that is characteristic of the transaction will be displayed in the HYPO NOE ID app in addition. This data allows you to check the order once more.

2.2.3 Data processing in the HYPO NOE Pay app

If you wish to use this service please note the Privacy Policy for the HYPO NOE Pay app at <https://www.hyponoe.at/services/mobiles-bezahlen/hypo-noe-pay>.

2.3 Transmission of your personal data

See section 5.

2.4 Storage period

We will store your above personal data for the purposes stated and for the duration of the business relationship (from negotiating and handling up to termination of the contract) and beyond in accordance with the statutory retention and documentation duties. They are, inter alia, contained in:

- the Austrian Business Code [*Unternehmensgesetzbuch/UGB*],
- the Austrian Fiscal Code [*Bundesabgabenordnung/BAO*],
- the Austrian Banking Act [*Bankwesengesetz/BWG*],
- the Austrian Act on the Prevention of Money Laundering in the Financial Market [*Finanzmarkt-Geldwäschegesetz/FM-GwG*], and
- the Austrian Securities Supervision Act [*Wertpapieraufsichtsgesetz/WAG*].

In addition, with regard to the storage period the statutory periods of limitation must be observed, which, for example according to the Austrian Civil Code [*ABGB*], may be up to 30 years in certain cases (the general statutory period of limitation is three (3) years), as well as guarantee and warranty periods.

3. MARKETING ACTIVITIES

3.1 Which data is processed by us in connection with marketing activities and from which source does it originate?

In addition to general contact details we process personal data which we have lawfully received from you as part of a (potential) business relationship on a product-related basis. See ANNEX II.

3.2 Purposes of processing

In connection with marketing activities your data will be processed for the following purposes:

- preparation of individual offers regarding banking, lease and insurance products tailored to your needs;
- enhancement of our portals, apps and self-service terminals;
- development of banking, lease and insurance products tailored to your personal needs;
- invitations to events of HYPO NOE and its subsidiaries;
- sending information in connection with products and services via different channels (letter, fax, electronic mail) and providing such information by phone
- carrying out price draws and the like.

3.3 Legal basis for processing

Where we process your personal data based on your **consent (Article 6(1)(a) GDPR)**, such consent will determine the purpose and scope of data processing. Consent may be withdrawn at any time, making future processing inadmissible. In line with the Austrian Telecommunications Act [*Telekommunikationsgesetz/TKG*] electronic mail for direct marketing purposes will only be sent if you have given your express consent to the same (Section 174 *TKG*). This also applies to marketing calls. You may withdraw your consent with effect for the future at any time.

The bank has an **overriding legitimate interest (Article 6(1)(f) GDPR)** in the following cases, among others:

- sending of advertising material of HYPO NOE and its cooperation partners by post
- analysis of marketing activities. The legitimate interest is the measuring of the efficiency of our marketing activities and provision of suitable products to specific recipients in a goal-oriented manner;
- analysis of business relationships. The legitimate interest is an assessment of the need for products and offering of suitable products to certain recipients in a goal-oriented manner. In addition, this analysis is a material part of HYPO NOE's risk control;
- analysis of payment behaviour. The legitimate interest is the enhancement of our portals, applications and self-service terminals. In addition, these analyses are essential to prevent money laundering activities and fight terrorist financing;
- analysis of visits to the website. The legitimate interest is an assessment of the need for products and the provision of suitable products to certain recipients in a goal-oriented manner;
- Please note that you have a right to object (see section 9).

3.4 Transmission of your personal data

See section 5 in this respect.

3.5 Storage period

Regarding data applications that you have consented to your personal data will be processed for as long as you do not withdraw your consent (see section 8). Furthermore, we will store the data for the purposes stated for the duration of the business relationship (from negotiating and handling up to termination of the contract) and beyond in accordance with the statutory retention and documentation duties. We will erase the data as soon as the legitimate purposes cease to exist.

4. OMBUDSPERSON ACTIVITIES FOR DATA SUBJECTS

If you consult HYPO NOE's ombudsperson as a neutral mediator who offers free assistance to private clients of HYPO NOE regarding the resolution of disputes, we will process some of your personal data.

4.1 Categories of processed data

See ANNEX III.

4.2 Purposes of processing

Your data will be processed for the following purposes:

- identifying the subject matter of the dispute;
- drafting proposals for a settlement;
- storing for documentation purposes and archiving;
- if consent has been given, disclosure to public conciliation boards, courts and/or administrative authorities;
- aggregated reporting to the Financial Market Authority.

Your data will be provided to us directly by you (in particular by communication via email or other means of communication) or we will collect it ourselves, for example in the course of conversations.

4.3 Legal basis for processing

We will process your data on the following basis:

- on the basis that it is required for performance of a contract to which the data subject is a party or for implementing necessary pre-contractual measures upon the data subject's request, namely an agreement to carry out the ombudsperson activities, pursuant to **Article 6(1)(b) GDPR**;

- on the basis that it is necessary for complying with legal obligations to which we are subject, pursuant to **Article 6(1)(c) GDPR**;
- on the basis of your consent to processing of your data (**Article 6(1)(a) or Article 9(2)(a) GDPR**).

4.4 Transmission of your personal data

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

- legal professionals;
- public conciliation boards, courts and administrative authorities;
- external IT service providers;
- cooperation partners.

4.5 Storage period

We will only store your data until termination of the information and support relationship and, beyond that, for as long as this is necessary to fulfil our statutory obligations and on the basis of other statutory retention periods or due to any legal disputes in which the data may be required as evidence. For withdrawal of consent see section 8.

5. DATA RECIPIENTS

Within HYPO NOE your data will be disclosed to persons and/or departments/offices/agencies that need the same for fulfilling contractual, statutory and/or regulatory obligations, as well as due legitimate interests or processing activities based on your consent.

For performance of the contract we also cooperate with cooperation partners who also receive personal data to the extent that they require the same for handling the business relationship, e.g. for the purpose of selling debit or credit cards, building society savings contracts or loan agreements or insurance contracts.

Moreover, processors instructed by us (including but not limited to providers of IT services and back office services) will receive your data to the extent that they need such data for rendering their relevant agreed service. All processors have been put under a contractual obligation to treat your data as confidential and to process the same only in connection with the provision of their service.

Other third parties will obtain your data if this is necessary for performance of the contract or due to legal requirements, e.g. recipients of money transfers and their payment services provider.

Please be informed that HYPO NOE, being an Austrian bank, is required to maintain banking secrecy pursuant to Section 38 *BWG*. This means that we are required to maintain secrecy about any and all information entrusted or made accessible to us by you solely on the basis of our business relationship with you and that we are not allowed to disclose or exploit it unless you have given your express written consent to disclosure or we are entitled or obliged to do so by law. In this connection recipients of personal data may be other credit or financial institutions or similar institutions to which we transmit data for handling the business relationship with you (depending on the contract, these may be correspondent banks, stock exchanges, custodian banks or credit agencies).

Where there are statutory obligations we must transmit your personal data to public agencies or institutions (e.g. the Austrian Financial Market Authority, the Austrian Central Bank (OeNB), the European Banking Authority, the European Central Bank or tax authorities).

In connection with the performance of the contract or in connection with fulfilling data applications on the basis of a declaration of consent disclosure of your personal data may be necessary (e.g. to guarantors in connection with loan agreements; to syndicate partners or other credit or financial institutions for fulfilling syndicated financing or assignment arrangements; to legal counsel). Financing may also require disclosure of the provided data, including, without limitation, to the European Central Bank, the Austrian Central Bank, Oesterreichische Kontrollbank AG, the European Investment Bank or the European Bank for Reconstruction and Development.

5.1 Is data transmitted to third countries or international organisations?

Since we occasionally process data in a third country outside the European Union (EU) or the European

Economic Area (EEA) and since this is done by using the services of third parties, we have implemented suitable and appropriate safeguards in order to keep the disclosure of data to the relevant third country in compliance with data protection law (e.g. adequacy decisions, Binding Corporate Rules or conclusion of standard data protection clauses). Upon request we will transmit a copy of these appropriate safeguards if we process your data in third countries or have the same processed there. This is only done if it is necessary for us to fulfil our (pre-)contractual obligations, on the basis of express consent, on the basis of a legal obligation or on the basis of our legitimate interests.

5.2 Account information service provider and payment initiation service provider

If you instruct an account information service provider or a payment initiation service provider to render a payment service, we will disclose the data provided for by law of the accounts defined by you to the same for allowing the same to render the payment service ordered. No additional personal data will be transmitted (in particular no sensitive data such as security-relevant PINs). For further information on the way in which the account information service provider or payment initiation service provider processes the transmitted data and on the rights you may assert vis-à-vis the account information service provider or payment initiation service provider please contact the same directly.

6. PROFILING AND AUTOMATED DECISION-MAKING (IN PARTICULAR CREDIT CHECK AND TRANSMISSION OF DATA TO THE REGISTER OF SMALL LOANS)

We do not resort to automated decision-making as defined in Article 22 GDPR to bring about a decision on establishing and performing the business relationship.

Prior to granting a loan a credit check (credit scoring) will be performed. Statistical peer groups are used to assess the default risk of people seeking loans. The score value calculated is intended to enable a prognosis regarding the likelihood with which a loan applied for is expected to be paid back. For calculating this score value your master data and details on your general financial situation and your payment behaviour will be used. In the case that the default risk is too high, the application for a credit will be rejected, an entry in the Register of Small Loans kept by Kreditschutzverband of 1870 will be made, where appropriate, and an internal warning note will be issued. In line with a decision of the Data Protection Authority, the fact that an application for a credit was rejected will be shown in the Register of Small Loans kept by Kreditschutzverband of 1870 for a duration of 6 months.

Please note that, due to the material significance that the information networks that were set up for performing credit checks before the GDPR entered into force have for the credit check required by regulatory provisions and consumer protection provisions, there is, in principle, no right to object, not least because of the weighing of interests provided for in the last sentence of Article 21(1) GDPR.

7. YOUR RIGHTS IN CONNECTION WITH PERSONAL DATA

Among other things, applicable law entitles you to

- check whether and which of your personal data is stored by us and to obtain copies of the same;
- request rectification, completion or erasure of your personal data if it is incorrect or has been processed unlawfully;
- obtain from us a restriction on processing of your personal data;
- object, under specific circumstances, to processing of your personal data or to withdraw your consent to processing that was previously given; such a withdrawal does not affect the lawfulness of the processing done up until the time of withdrawal (see section 8);
- request data portability;
- know the identity of third parties to whom your personal data is transmitted and to lodge a complaint with the Data Protection Authority (www.dsb.gv.at) or a regulatory authority of another EU Member State, in particular in the country of your place of residence or work.

8. WITHDRAWAL OF CONSENT

You may withdraw your previously given consent at any time. Your withdrawal must preferably be

addressed to your client services agent of HYPO NOE or to the data protection officer via email to datenschutz@hyponoe.at.

Your personal data will be processed for as long as you do not withdraw your consent.

Please note that withdrawal applies *ex nunc*, which means that the lawfulness of the data processing based on consent done up until the time of the withdrawal will not be affected by it. However, HYPO NOE complies with the erasure obligations defined in Article 17 GDPR.

9. OBJECTION

Please note that you have a right to object to processing of personal data concerning you which we process on the basis of overriding interests at any time on grounds relating to your particular situation; this also applies to profiling that is based on those provisions. If this is the case, HYPO NOE will stop processing this personal data unless we are able to demonstrate compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject or unless the processing serves the assertion, exercise or defence of legal claims. Please note that an exemption applies to data applications for credit checks that have been set up as information networks (see section 6).

If personal data is processed for direct marketing purposes, you will have the right to object to processing of personal data concerning you for the purpose of such marketing at any time; this also applies to profiling to the extent that it is related to such direct marketing.

10. OBLIGATION TO DISCLOSE THE DATA

We request that you disclose personal data which is necessary for establishing and performing the business relationship and which we are required to collect by law. If you do not wish to do so we will not be able to enter into a business relationship or conclude the relevant contract with you and/or to continue the same, which is why we have to terminate existing contractual relationships in that case. Data that is not necessary or not legally required for establishing or performing the contract does not have to be disclosed. You may give your consent to marketing activities voluntarily; upon request to datenschutz@hyponoe.at we will be pleased to send you the relevant form.

ANNEX I. CATEGORIES OF PROCESSED DATA - PRODUCTS

PLEASE NOTE: The present list is a general presentation of the data that is usually collected and processed in connection with the respective products. This does not mean that we will actually store or process all of the said data in any case. If you would like to obtain personalised information you may do so in connection with your right of access as defined in Article 15 GDPR.

1. CURRENT ACCOUNTS

- Client: Salutation/gender, name, home address, date of birth, email address, phone number, signature, banking details, identification data (i.e. ID document details or audio and video files when using online video identification), proof of citizenship, residence permit, registration data, marital status, proof of assets, tax number, employer, duration of employment, living situation, family relations, data regarding payments to your account as well as withdrawals and other payment references and money transfer data (payee, IBAN and payment service provider of the payee), client number, signatory number, account number, remittance information, account statements/transaction data of your own bank and the third-party bank, payor, payment behaviour, payment reminder behaviour, terms, means of payment used, consumer behaviour, saving targets and saving behaviour, balance, debit card data
- Payee: Salutation/gender, name, banking details, payment reference, remittance information, IBAN and payment service provider of the payee
- Payor: Name, banking details, payment reference, remittance information, IBAN and payment service provider of the payor

2. SAVING

Salutation/gender, name, home address, date of birth, email address, phone number, proof of assets, banking details, identification data (i.e. ID document details and audio and video files when using online video identification), registration data, marital status, data from credit agencies, saving targets and saving behaviour

3. INVESTING

Salutations/gender, name, home address, date of birth, email address, phone number, proof of assets, banking details, identification data (i.e. ID document details and audio and video files when using online video identification), registration data, residence for tax purposes, order data, phone recordings in connection with securities orders, securities account number, clearing account, securities portfolio, authorisations to operate/sign on the account or legal representation (e.g. in the case of minors or adult guardianships), consultation reports, in connection with the investor profile "knowledge and experiences" in the respective forms of investment (such as, e.g., number and volume of past transactions), financial situation (asset structure plus the relevant source of income as well as liabilities), investment objectives (including data on the duration and purpose of the investment, special investment requests and payment mode), risk appetite and risk category of the client

4. LOANS

4.1. Loans

- Borrower: Salutation/gender, name, home address, date/place of birth, proof of citizenship, email address, phone number, signature, proof of assets, income information (including, without limitation, pay slips), monthly expenses, amount of the different liabilities, (collateral) security and its value, other assets, credit history, credit information, rating, banking details, terms, identification data, registration data, marital status, number of dependants, employer, duration of employment, school education, data from credit agencies
- Guarantor: Salutation/gender, name, home address, date of birth, email address, phone number, proof of assets, (collateral) security, banking details, identification data, registration data, data from credit agencies

- Escrow agent/authorised representative: Salutation/gender, name, address, banking details, identification data, phone number, email address
- Lessee/Tenant of the properties financed: Name, identification data, list of rent payments

4.2. Operating loans

- Company: Company name, business address, Business Register Number, excerpt from the Business Register, trade licence
- Persons authorised to operate/sign on the account: Salutation/gender, name, address, identification data, phone number, email address

5. INSURANCE

Salutation/gender, name, home address, date/place of birth, proof of citizenship, email address, phone number, proof of assets, banking details, identification data, registration data, marital status, number of dependants, employer, health data (depending on the insurance company, answers to health questionnaires, medical documents such as reports/letters from physicians and hospitals, laboratory and histological findings/reports, medical certificates, medical histories, discharge papers, treatment data must be sent to the relevant insurance company), advisory service reports

ANNEX II CATEGORIES OF PROCESSED DATA - MARKETING ACTIVITIES

Marketing activities concerning clients and prospective clients

1. GENERAL DATA

Salutation/gender, name; company name, latest address and communication data (address, phone numbers, email addresses), risk class of securities, data obtained during consultancy meetings, such as your interests, plans, budget; use of the newsletter and potential interests resulting from perusal of the same.

2. DATA ON THE BANKING, LEASE AND INSURANCE PRODUCTS PURCHASED

Products purchased (e.g. account, securities, deposits, financing, credit cards, lease, insurance), means of payment used (e.g. cards, cheques, bills of exchange), payment behaviour and payment transactions (e.g. payee/payor, amount, purpose, type and frequency of account movements, consumer behaviour), allocations made in internet banking, saving targets and saving behaviour, recommendations/references, account balances, terms (e.g. interest rates, charges, commissions)

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

Type of use (frequency, time, place/location analyses), features used for all HYPO NOE apps and portals used for banking transactions, including software (internet banking), IP addresses

4. ADDITIONAL DETAILS REQUIRED FROM NATURAL PERSONS

Date of birth, marital status, identification data (i.e. ID documents), living situation, income, employer, occupation, education, family relations, other persons in the household

5. ADDITIONAL DETAILS REQUIRED FROM LEGAL PERSONS

Business Register data (e.g. industry, size, legal form, business/corporate relations), financial documents (e.g. balance sheets, budgets and income statement)

ANNEX III CATEGORIES OF PROCESSED DATA - OMBUDS OFFICE

1. GENERAL DATA

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

2. REQUIRED DOCUMENTS

Documents handed over, statement of release from banking secrecy, correspondence