Data protection information under the EU General Data Protection Regulation (GDPR) for “natural persons”

This information is applicable for current and potential clients of Bank Vontobel AG (hereinafter referred to as “Vontobel” or “we”).

Vontobel is committed to complying with bank-client confidentiality and data protection laws and regulations and thus to ensuring the protection and confidentiality of your Personal Data. The following information provides an overview of how we process your Personal Data and your rights under data protection laws and regulations. Which specific data are processed and how they are used depends largely on the services requested or agreed in each case. However, we process data about individuals (“Personal Data”), including data about employees and contractors of our suppliers (“Affected Persons”).

Please also forward this information to current and future authorized representatives and beneficial owners, as well as to any co-obligors under a loan. These include, for example, beneficiaries in the event of death, commercial attorneys-in-fact and guarantors.

1. Who is responsible for the data processing and who can I contact in this regard?

The following entity (including its branches) is responsible for data processing:

Bank Vontobel AG
Gotthardstrasse 43
CH-8022 Zurich
Switzerland
Phone: +41 58 283 71 11
E-mail: vontobel.group@vontobel.com

You can also contact our corporate Swiss and/or Group Data Protection Officer (DPO):
- Group DPO: dpo.vontobelgroup@vontobel.com
- Swiss DPO: dpo.ch@vontobel.com

2. What source and what type of data do we process?

We process Personal Data that we receive from you in your capacity as an Affected Person in the context of our business relationship. Should it be necessary for the provision of our services, we process Personal Data that we lawfully (for example, to execute orders, perform contracts or on the basis of your consent) receive from other entities within the Vontobel Group or third parties (such as private commercial databases). We also process Personal Data from publicly available sources (for example, debtor directories, land registers, commercial registers and registers of associations, the press and the Internet) which we lawfully obtain and are permitted to process.

Furthermore, in our dealings with current and potential Affected Persons we process Personal Data, such as name, address and other contact details (telephone, e-mail address), title, date of birth, gender, nationality, marital status, partner type data (employed / self-employed), identification data (such as ID, tax ID), certification data (such as specimen signature), contract related data (such as sales data in payment transactions), order data including online banking (such as payment orders), and information regarding your financial situation (such as creditworthiness data, scoring/rating data, origin of assets), CVs, criminal records or any other information publicly available or accessible through third party providers. In addition to the categories mentioned, we also process advertising and sales data (including advertising scores), documentation data (such as consultation protocols) and other data comparable with the above categories.

3. Does Vontobel collect special categories of data (Art. 3 (c) FADP; Art. 9 GDPR)?

To the extent that we process any special categories of data relating to Affected Persons, we will do so if the processing is necessary for the establishment, exercise or defense of a legal claim, for reasons of substantial public interest or if you have given your explicit consent to Vontobel to process that data (where legally permissible). In that sense, we might process biometric data that is classified as sensitive Personal Data (Art. 4 (14), Art. 9 (1) GDPR). In this respect, your explicit consent will be required in a separate procedure in order to obtain a biometric identification (for example, Touch ID) or other biometric identification to use it for access to certain applications.

4. For what purpose do we process your data and on what legal basis?

We process the aforementioned Personal Data in compliance with the provisions of the EU General Data Protection Regulation (GDPR) and the Swiss Federal Act on Data Protection (FADP):

4.1. For fulfillment of contractual obligations (Art. 13 (2) (a) FADP; Art. 6 (1) (b) GDPR)

Data is processed in order to provide banking business and financial services in the context of performing our contracts with our clients or to perform pre-contractual measures that occur as part of a request. The purposes of data processing are primarily in compliance with the specific product (such as bank account, credit, saving with building societies, securities, deposits and client referral) and can include needs assessments, advice, asset management and support, as well as carrying out transactions. You can find additional details about the purposes of data processing in the relevant contract documents and terms and conditions.

4.2. For compliance with a legal obligation (Art. 13 (1) FADP; Art. 6 (1) (c) GDPR) or in the public interest (Art. 6 (1) (e) GDPR)

We are also subject to various legal obligations (globally and locally), namely, statutory requirements (such as the Swiss Banking Act, Collective Investment Schemes Act, Anti-Money Laundering Act, Mortgage Bond Act, financial supervisory ordinances and circulars, and tax laws) and bank regulatory requirements (for example, Swiss National Bank and FINMA). Other purposes of processing include assessment of creditworthiness, identity and age verification, anti-fraud and anti-money laundering measures, the fulfillment of tax law control and reporting obligations, as well as the assessment and management of risks within the bank and the Group.

4.3. For the purposes of safeguarding legitimate interests (Art. 13 (1) FADP; Art. 6 (1) (f) GDPR)

Where necessary, we process your data beyond the actual performance of our contractual obligations in order to safeguard the legitimate interests pursued by us or a third party, which does not unduly affect your interest or fundamental rights and freedoms. Besides the following examples, we also obtain Personal Data from publicly available sources for client acquisition purposes:

- Consulting and exchanging data with information offices (for example, the debt register) to investigate creditworthiness and credit risks in credit business and the requirement for an account maintained with a basic non-sizable balance and basic accounts;
- Reviewing and optimizing procedures for needs assessment for the purpose of direct client discussions;
- Marketing or market and opinion research, unless you have objected to the use of your data;
- Asserting legal claims and defense in legal disputes;
- Guarantee of IT security and IT operations;
- Prevention and clarification of crimes;
- Video surveillance to protect the right of owners of premises to keep out trespassers, for collecting evidence in hold-ups or fraud, or to prove availability and deposits, for example, at ATMs and office entrances;
- Measures for building and site security (for example, access controls);
- Measures for ensuring the right of owners of premises;
- Measures for business management and further development of services and products;
- Group risk management.

For all the data processing foreseen in points 4.1. – 4.3. the legal basis for the data processing is constituted by the necessity of carrying out a legal obligation. Therefore, in those cases it is not necessary to obtain your prior consent to process this data.

4.4. On the basis of your consent (Art. 13 (1) FADP; Art. 6 (1) (a) GDPR)

Insofar as you have consented to the processing of Personal Data for specific purposes (such as transfer of data within the Group, analysis of trading activities for marketing purposes, etc.), the lawfulness of such processing is based on your consent. Any consent granted may be revoked at any time. This also applies to the revocation of declarations of consent that are granted to us prior to the entry into force of the GDPR, that is, prior to May 25, 2018.

Please be advised that the revocation shall only have effect for the future. Any processing that was carried out prior to the revocation shall not be affected thereby.

5. Who receives your data?

Within Vontobel, the units given access to your data are those which require them in order to perform our contractual, legal and regulatory obligations. Service providers and vicarious agents employed by us can also receive access to data for the purposes given if they maintain banking confidentiality and comply with our written instructions under data protection law and regulations. These are companies in the categories of banking services, IT services, logistics, printing services, telecommunications, collection, advice and consulting, sales and marketing.

With regard to transferring data to recipients outside Vontobel, it must first of all be noted that as a bank we are under a duty to maintain secrecy about any client-related facts and evaluations of which we may have knowledge (banking confidentiality pursuant to our general terms and conditions; Art. 47 Swiss Federal Banking Act). We may only disclose information about you if we are legally required to do so, if you have given your consent, if we are authorized to provide bank information and / or if processors commissioned by us guarantee compliance with banking secrecy and the provisions of the FADP / GDPR).

Under these requirements, recipients of Personal Data might be, for example:

- Public authorities and institutions (such as Swiss National Bank, financial supervisory ordinances, financial authorities, criminal prosecution authorities) insofar as a statutory or official obligation exists;
- Other companies within Vontobel for risk control due to statutory or official obligations;
- Other credit and financial service institutions, comparable institutions and processors to which we transfer your Personal Data in order to perform any business relationship with you (specifically, processing of bank references, support / maintenance of EDP / IT applications, archiving, document processing, callcenter services, compliance services, controlling, data screening for anti-money laundering purposes, data destruction, purchasing / procurement, space management, real estate appraisals, loan processing services, collateral management, collection, payment card processing (debit cards, / credit cards), customer management, marketing, media technology, reporting, research, risk controlling, expense accounting, telephony, video identification, website management, investment services, share register, fund management, auditing services and payment transactions).

Other recipients of data might be any units for which you have given your consent to the transfer of data or with respect to which you have exempted us from banking secrecy by agreement or consent.

6. Is data transferred to any third country or international organization?

Data will only be transferred to countries outside Switzerland and the EU or the EEA (so-called third countries) if this is required for the execution of your orders (such as payment and securities orders), prescribed by law (such as reporting obligations under tax law), if you have given us your consent, or in the context of commissioned data processing. If service providers in a third country are used, they are obligated to comply with the data protection level in Switzerland and Europe in addition to written instructions by agreement of the EU standard contractual clauses.

We take seriously our obligation to ensure that any transfers outside the EU or the EEA are only made to entities that can demonstrate equivalence in standards of security and other relevant data processing requirements.

7. For how long will my data be stored?

We process and store your Personal Data as long as it is necessary for the performance of our contractual and statutory obligations. In this regard, it should be noted that our business relationship is a continuing obligation designed to last for several years. We have processes in place to review, at various points, the different categories of data that we hold to ensure that we do not hold these for an excessive period of time.

If the data are no longer required for the performance of our contractual and statutory obligations, they are regularly deleted, unless their further processing – for a limited time – is necessary for other legal purposes, such as:

- Compliance with record retention periods under commercial and tax laws: These include the Swiss Code of Obligations (OR) in conjunction with the Accounting Ordinance, the Federal Act on Direct Taxation, the Federal Act on Value Added Taxation, the Federal Act on Harmonization of Direct Taxes of Cantons and Municipalities, the Federal Act on Stamp Duties, the Federal Act on Withholding Tax, the Money Laundering Act (AMLA) and the Federal Banking Act. The periods for storage and documentation specified therein might vary;
- Preservation of evidence and/or all forms of relevant information when litigation is reasonably anticipated, which requires us to keep records for an undefined period of time.

8. Data protection rights

8.1. In general

Every data subject has the right to access (Art. 8 FADP; Art. 15 GDPR), the right to rectification (Art. 5 FADP; Art. 16 GDPR), the right to erasure (Art. 5 FADP; Art. 17 GDPR), the right to restrict processing (Art. 12, 13, 15 FADP; Art. 18 GDPR), the right to object (Art. 4 FADP; Art. 21 GDPR), and if applicable, the right to data portability (Art. 20 GDPR). Furthermore, if applicable, you have the right to lodge a complaint with an appropriate data privacy regulatory authority (Art. 77 GDPR). The rights are dependent on the lawful basis selected for holding the particular data.

You may revoke your consent to the processing of Personal Data at any time. This also applies to the revocation of declarations of consent that are granted prior to the entry into force of the EU General Data Protection Regulation, that is, prior to May 25, 2018. Please be advised that the revocation will only take effect in the future. Any processing that was carried out prior to the revocation shall not be affected thereby.

8.2. Ad hoc right of objection (Art. 21 GDPR)

You have the right to object, on grounds relating to your particular situation, at any time to the processing of Personal Data concerning you which is based on processing in the public interest (Art. 6 (1) (e) GDPR) and for the purposes of safeguarding legitimate interests (Art. 6 (1) (f) GDPR); this includes any profiling based on those provisions within the meaning of Art. 4 (4) GDPR. If you submit an objection, we will no longer process your Personal Data unless we can give evidence of mandatory, legitimate reasons for the processing, which outweigh your interests, rights, and freedoms, or where the processing serves the enforcement, exercise, or defense of interests. Please note that in such cases we will not be able to provide services or maintain a business relationship.

8.3. Right to object to the processing of data for marketing purposes

In certain cases, we process your Personal Data for direct marketing purposes. You have the right to object at any time to the processing of Personal Data concerning yourself for such marketing purposes, which includes profiling to the extent that it is related to direct marketing. If you object to processing for direct marketing purposes, we will no longer process your Personal Data for such purposes.

9. Am I under any obligation to provide data?

Within the scope of our business relationship, you must provide Personal Data which is necessary for the initiation and execution of a business relationship and the performance of the associated contractual obligations, or which we are legally obligated to collect. As a rule, we would not be able to enter into any contract or execute an order without these data or we may no longer be able to perform an existing contract and would have to terminate it.

In particular, provisions of money laundering law require that we verify your identity before entering into the business relationship, for example, by means of your identity card, and that we record your name, place of birth, date of birth, nationality and your residential address. In order for us to be able to comply with this statutory obligation, you must provide us with the necessary information and documents and notify us without undue delay of any changes that may arise during the course of the business relationship. If you do not provide us with the necessary information and documents, we will not be allowed to enter into or continue your requested business relationship.

10. To what extent is automated decision-making (including profiling) carried out?

As a rule, we do not make decisions based solely on automated processing as defined in Art. 22 GDPR to establish and implement the business relationship. If we use these procedures in individual cases, we will inform you of this separately, provided that this is prescribed by law. In such a case, you will have a right to object to these procedures under certain circumstances.

11. Is profiling used within Vontobel?

In some cases, we process your data automatically with the aim of evaluating certain personal aspects (profiling). For example:

- We are required by law to take anti-money laundering, anti-fraud and anti-terrorism financing measures, as well as measures related to offenses that pose a danger to assets. Data evaluations are also carried out (in payment transactions, among other things) in this context. These measures also serve to protect you;
- In order to provide you with targeted information and advice on products, we use evaluation tools. These enable demand-oriented communication and advertising, including market and opinion research.

12. How do we protect Personal Data?

All personnel accessing Personal Data must comply with the internal rules, policies and processes in relation to the processing of any Personal Data to protect them and ensure their confidentiality. They are also required to follow all technical and organizational security measures put in place to protect the Personal Data.

We have also implemented adequate technical and organizational measures to protect Personal Data against unauthorized, accidental or unlawful destruction, loss, alteration, misuse, disclosure or access, as well as against all other unlawful forms of processing. These security measures have been implemented taking into account the state of the art of the technology, their cost of implementation, the risks presented by the processing and the nature of the Personal Data, with particular care for sensitive data.

13. Contact

Please also let us know if we do not meet your expectations with respect to the processing of Personal Data or if you wish to complain about our data protection practices; this gives us the opportunity to examine your issue and make improvements, where necessary. In any of these cases, please send us a clear request in writing, together with a clearly legible copy of a valid official ID document (for example, passport or ID card), to the entity or one of the DPOs named in section 1. We will acknowledge receipt as soon as received, examine your issue and reply in good time. If a full response will take more than one month, taking into account the complexity and number of the requests, we will advise you of this.

14. Other legislation aspects

In order to comply with other legislation, for example, Directive 2014/65/EU of the European Parliament (MIFID II), we must in some of our legal entities record telephone conversations with reference to operations concluded in the performance of our services. For further information about the treatment of your Personal Data in this regard, please see our complete information at: www.vontobel.com/mifid.

15. Changes to the Privacy Policy

This data protection information was last updated on May 14, 2018. It may be subject to change. Any future change or additions to the processing of Personal Data as described above affecting you will be communicated to you through the appropriate channel (for example, it will be posted on our website).