



JOB APPLICANT PRIVACY STATEMENT

2023

TABLE OF CONTENTS

- 1. INTRODUCTION 2
 - 1.1 General..... 2
 - 1.2 Definitions..... 2
- 2. WHAT DO WE DO WITH YOUR PERSONAL DATA? 3
 - 2.1 What is Personal Data?..... 3
 - 2.2 Which Personal Data may we process about you?..... 3
 - 2.3 What legal basis do we have for Processing your Personal Data? 4
 - 2.4 For what purposes does NIBC collect your Personal Data and what are our justifications of use?..... 4
 - 2.5 For what purposes does NIBC Process criminal Personal Data?..... 6
 - 2.6 How long is Personal Data retained?..... 6
 - 2.7 From where do we collect your Personal Data? 7
 - 2.8 Where do we keep your Personal Data? 7
 - 2.9 How does NIBC protect my Personal Data?..... 7
 - 2.10 Do we share your Personal Data?..... 8
- 3. WHAT ARE YOUR RIGHTS?..... 9
- 4. NIBC ENTITIES AND CONTACT DETAILS..... 11
 - 4.1 Contact details of our DPO 11
 - 4.2 Contact details of the relevant data protection authorities 11

1. INTRODUCTION

1.1 General

In applying to join NIBC, you will be providing us with certain Personal Data about yourself. The Data Controller for the Processing of Personal Data in the context of your application will be NIBC Bank N.V. (collectively “NIBC” or “we”).

NIBC values and respects the privacy of our potential employees. NIBC will Process your Personal Data carefully and in accordance with applicable rules and regulations.

This Job Applicant Privacy Statement describes how we use your Personal Data in our business when you apply for an employment (or equivalent) position at NIBC. We collect, use, disclose and otherwise Process Personal Data that is necessary for the purposes identified in this Job Applicant Privacy Statement or as permitted by law.

In this Job Applicant Privacy Statement we use a number of terms that have a specific meaning under applicable privacy rules (such as “Personal Data” or “Data Controller”). Paragraph 1.2 of this Job Applicant Privacy Statement contains an overview of these defined terms.

NIBC may from time to time implement changes to this Job Applicant Privacy Statement. The most recent version will at all times be available on the relevant NIBC websites. In case there are substantial changes to this Job Applicant Privacy Statement, NIBC will inform you (such as via the relevant NIBC websites or other means of communication usually used by us to communicate with you).

1.2 Definitions

Criminal Personal Data	Any Personal Data that provides information on a person’s criminal convictions, offences, or related security measures.
Data Controller	The legal person or body which, alone or in conjunction with others, determines the purposes of and means for Processing of Personal Data.
Data Processor	The legal person or body which Processes Personal Data on behalf of the Data Controller without being subject to the Data Controller’s direct control.
Data Protection Officer or DPO	The officer for the protection of Personal Data within NIBC.
DPO Office	The group of Employees engaged on a regular basis in the oversight, provision of advice and monitoring of data protection matters within NIBC.
GDPR	The European General Data Protection Regulation, EU 2016/679.
Personal Data	Any information relating to an identified or identifiable natural person. By way of example but not limitation, video and voice recording is also Personal Data if the video images or the voice recording is identifiable to an individual. If financial data (such as

	bank statements) relate to an individual, such data is considered Personal Data.
Processing of Personal Data (or Process)	Any operation or any set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Special Categories of Personal Data	Any Personal Data that provides information on a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
UK GDPR	The Data Protection Act 2018, together with the Retained Regulation (EU) 2016/679 by which the GDPR was brought within the laws of the United Kingdom following the United Kingdom's departure from the European Union.

2. WHAT DO WE DO WITH YOUR PERSONAL DATA?

2.1 What is Personal Data?

Personal Data is defined above. In summary, it includes any information relating to an identified or identifiable natural person, such as a name, address, email address, a CV or résumé etc.

2.2 Which Personal Data may we process about you?

As part of your recruitment process, we may Process the following Personal Data about you:

- a. Your contact information** ► including your name, home address (and proof of address), telephone number(s), personal email address, gender;
- b. Your employment history and experience** ► including your CV or résumé which may include your date of birth, availability, application form details, qualification certificates, training certificates, licenses, information about your education, information available on LinkedIn or other relevant social media, permission to work documentation, references from other employers and other data collected through interviews or other forms of assessment (to the extent permitted by law);
- c. Information required for pre-employment checks** ► e.g. qualification certificates, training certificates, licenses (to the extent permitted by law);
- d. Information resulting from pre-employment screening checks** ► e.g. results of pre-employment screening checks, qualification certificates, training certificates, licenses, information available on LinkedIn and other relevant social media, permission to work checks that we may carry out as part of the recruitment process (to the extent permitted by law); and
- e. Materials produced during recruitment** ► materials produced during the course of the recruitment process, including your name, correspondence, your

reasons for applying, any videos and presentations you provide us for the purposes of a recruitment assessment and any contemporaneous interview notes (whether made by you or the interviewer), about you (to the extent permitted by law).

If you are taken on to work at NIBC, other Personal Data will be collected and Processed about you in accordance with our Employee Privacy Statement.

2.3 What legal basis do we have for Processing your Personal Data?

NIBC only Processes your Personal Data for legitimate purposes. The use of your Personal Data will also be justified on the basis of one or more legal "Processing grounds" that are provided for in the GDPR and/or, as applicable, the UK GDPR.

The table below contains an explanation of the scope of the various legal Processing grounds available under the GDPR and/or, as applicable, the UK GDPR, for Processing of Personal Data on which NIBC relies:

Contract performance: where NIBC requires your Personal Data in order to enter into an employment contract with you.
Legitimate interests: where the Processing of your Personal Data is necessary in order to achieve legitimate interests of NIBC or a third party , except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of your Personal Data.
Our legal obligations: where we are required to Process your Personal Data under a statutory obligation, primarily as a result of our status as a regulated financial institution.
Consent: where you have consented to our use of your Personal Data (in which case you will have been presented with the opportunity to actively give your consent (or refuse to do so) in relation to any such use and you may withdraw your consent at any time by the method explained in the communication with you or, and in any event, by giving notice to our DPO).

For more information, we refer to paragraph 2.4. below.

2.4 For what purposes does NIBC collect your Personal Data and what are our justifications of use?

This paragraph specifies the purposes for which NIBC uses the various categories of Personal Data. The exact nature and scope of Personal Data we collect from you will depend on the circumstances. For each use, we note the applicable legal Processing grounds by which we justify the relevant use of your Personal Data:

- a. To handle your job application and to communicate with you ►** to communicate with you about the recruitment process and your application.
 - **Use justification:** contract performance, legitimate interests (NIBC's legitimate interest to communicate with you about your job application).

- b. To assess your suitability for the advertised role or other potential vacancies within NIBC ►** we and other organisations engaged by us may access and use your Personal Data to assess your skills, qualifications and interests against our roles and vacancies.
 - **Use justification:** contract performance, legitimate interests (to assess whether you are a suitable candidate for our organisation), consent if your

application is unsuccessful but you allow NIBC to keep your Personal Data on file for an extended period.

- c. Information to carry out pre-employment checks** ► if you are offered a job where a pre-employment check is required, we will ask you for information so that we can carry out pre-employment checks, including performing a Dow Jones Risk and Compliance Check or (in the Netherlands) requesting a certificate of good conduct (Verklaring Omtrent het Gedrag). In Germany a similar certificate of good conduct (Führungszeugnis) is requested, as well as a credit investigation report (Schufa-Auskunft). This information is necessary to enable us to confirm the identity of job applicants, their right to work in the relevant jurisdiction and to seek assurance as to their trustworthiness, integrity and reliability.
- **Use justification:** contract performance, legitimate interests (to assess whether your trustworthiness, integrity and reliability are beyond doubt), if and when applicable for a specific position: to comply with our legal obligations. For the Processing of Criminal Personal Data, please see below under paragraph 2.5 "For what purposes does NIBC Process Criminal Personal Data?".
- d. To comply with our legal obligations and cooperate with regulators** ► we may Process and disclose your Personal Data to cooperate with requests from regulators (including financial supervisory authorities), including, but not limited to, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), the Netherlands Authority for the Financial Markets (AFM), the Dutch Central Bank (DNB), the Information Commissioner's Office (ICO), the Financial Conduct Authority (FCA), the Prudential Regulation Authority (PRA), the National Bank of Belgium (Nationale Bank van België), the Belgian Financial Services and Markets Authority (FSMA), the Belgian Data Protection Authority (Gegevensbeschermingsautoriteit), the various German State Data Protection Authorities, the German Central Bank (Deutsche Bundesbank) and the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht). Personal Data may also be provided to the police pursuant to a judicial warrant.
- **Use justification:** legal obligations, legitimate interests (for NIBC's interests and to ensure the integrity and security of the financial sector). For the Processing of Criminal Personal Data, please see below under "For what purposes does NIBC Process Criminal Personal Data?".
- e. To defend our legitimate interests and to change our business structure** ► we may disclose Personal Data in connection with legal proceedings or investigations anywhere in the world to third parties, such as public authorities, law enforcement agencies, notaries, lawyers, liquidators, regulators and third party litigants (these third parties are not Data Processors on behalf of NIBC and will Process Personal Data for their own purposes). NIBC may also provide your Personal Data to any potential acquirer of or investor in any part of NIBC's business for the purpose of that acquisition or investment.
- **Use justification:** contract performance, legal obligations, legitimate interests (to enable us to cooperate with law enforcement and regulators and to allow NIBC to change its business). For the Processing of Criminal Personal Data, please see below under "For what purposes does NIBC Process Criminal Personal Data?".

f. To improve our job application procedure ►

- **Use justification:** legitimate interest (to ensure that NIBC has a streamlined job application procedure in place).

g. To deal with questions, requests, comments, concerns and/or complaints ► NIBC may Process Personal Data in order to deal with questions, requests, comments, concerns and/or complaints and respond to job applicants accordingly.

- **Use justification:** contract performance, legitimate interests (to enable you to raise your questions, requests, comments, concerns and/or complaints with NIBC and for NIBC to be able to address them accordingly), legal obligations (e.g. if you exercise your data protection rights).

h. To analyse and report on questions, requests, comments, concerns and/or complaints ►

- **Use justification:** legitimate interests (to ensure that NIBC is able to report on such queries and input it has received from relevant stakeholders which also allows us to improve our procedures).

More information on the balancing of interest test performed when we base Processing of Personal Data on our legitimate interests is available upon request (please see paragraph 4.1 below for our contact details).

2.5 For what purposes does NIBC Process criminal Personal Data?

If you are offered a job at NIBC, NIBC carries out pre-employment checks, including criminal background checks, for which purpose NIBC may, if and to the extent necessary, Process Personal Data relating to criminal convictions and offences. NIBC will always notify you prior to carrying out any such pre-employment checks.

- **Use justification:** NIBC shall only Process Criminal Personal Data when such Processing is authorised by applicable law. NIBC participates in incident registers and early warning systems that are under the control of official authorities.

2.6 How long is Personal Data retained?

We keep records of your Personal Data for no longer than is necessary for the purpose for which we obtained them and any other permitted linked purposes. NIBC keeps your Personal Data on file in order to complete the application process and/or for consideration for future employment opportunities.

If your application for employment is unsuccessful, we may hold your Personal Data on file for:

- four (4) weeks after the end of the relevant recruitment process for applicants applying for a job in the Netherlands.
- six (6) months after the end of the relevant recruitment process (i.e. the application date) for applicants applying for a job in Germany.
- twelve (12) months after the end of the relevant recruitment process for applicants applying for a job in the United Kingdom or in Belgium.

For persons applying for a job in the Netherlands or Germany: If you provide your consent to keep your Personal Data on file for an extended period, we will hold your data on file for a total of one (1) year.

At the end of the relevant period, or once you withdraw your consent, your Personal Data is deleted or destroyed as quickly as possible. In practice, this may mean that Personal Data is retained for a short period after the retention period has expired. Deletion or destruction of files may be suspended where longer retention of the Personal Data is required by law or to defend ourselves if we consider a complaint or dispute to be likely. If NIBC proceeds with employing you, the Personal Data which you have provided to NIBC during the application process will become part of your employee file.

2.7 From where do we collect your Personal Data?

We may obtain Personal Data from you directly or from third parties such as our business partners, employment agencies, past employers, educational institutions, credit reference and anti-fraud agencies, other background check agencies/organisations, sanctions and politically exposed persons screening lists, or public registers.

2.8 Where do we keep your Personal Data?

We primarily store your Personal Data on IT systems located in the Netherlands, the UK, Belgium and Germany. Some of these IT systems are outsourced to third parties. We have also engaged IT service providers who are situated outside the European Economic Area (EEA). All IT service providers act as Data Processors on behalf of NIBC. When we engage such Data Processors, we will ensure that data processing agreements are in place. For more information, please see below, under *"Do we share your Personal Data?"*.

If your Personal Data is transferred outside of the EEA we will, if and when necessary, use the EU model contractual clauses or other suitable data transfer mechanisms in order to ensure an appropriate level of protection. Furthermore, NIBC will assess whether any additional measures are necessary to guarantee an appropriate level of protection of your Personal Data. Please do not hesitate to contact our DPO if you wish to receive more information about the appropriate or suitable safeguards in place for data transfers outside of the EEA.

2.9 How does NIBC protect my Personal Data?

NIBC has implemented appropriate technical and organisational measures to secure the Processing of Personal Data. These safeguards vary depending on its sensitivity, format, location, amount, distribution and storage of the Personal Data, and include measures designed to keep Personal Data protected from unauthorized access. If appropriate, the safeguards include encryption during transmission and/or storage, firewalls, access controls, separation of duties, and similar security protocols. We restrict access to Personal Data to personnel and third parties that require access to such information for legitimate, relevant business purposes.

All our staff members, contractors and third parties who will have access to Personal Data on NIBC's instructions will be bound to confidentiality and we use access controls to limit access to individuals that require such access for the performance of their responsibilities and tasks.

NIBC has information security policies in place and its security policies and systems are frequently audited. As a regulated financial institution, NIBC has to comply with strict security requirements. NIBC takes the security of its IT infrastructure very seriously.

2.10 Do we share your Personal Data?

NIBC has engaged various Data Processors for the Processing of Personal Data on our behalf, including IT service providers and other business service providers.

Service providers accessing NIBC Personal Data act as Data Processors on behalf of NIBC. Where we engage Data Processors, we will ensure that data processing agreements are in place.

We may also share your Personal Data with other third party service providers as described in paragraph 2.4. *"For what purposes does NIBC collect your Personal Data and what are our justifications of use?"* who act as Data Controllers. NIBC obliges these third party service providers to handle your Personal Data confidentially.

Some of these third parties are situated outside the EEA. If Personal Data is transferred outside of the EEA, this will take place in accordance with the applicable data protection legislation. If and when necessary, we will implement additional legal safeguards governing such transfer, such as the use of EU model contractual clauses (or, if so required, equivalent protections required to comply with the UK GDPR), or other suitable data transfer mechanisms in order to ensure an appropriate level of protection. Furthermore, NIBC will assess whether any additional measures are necessary to guarantee an appropriate level of protection of your Personal Data. Certain (sectors in) countries outside the EEA have been approved by the European Commission as providing essentially equivalent protections as EEA data protection laws. The GDPR and the UK GDPR allow NIBC to freely transfer Personal Data to such countries: as at the date of this Job Applicant Privacy Statement the UK has also approved those same (sectors in) countries as providing essentially equivalent protections as UK data protection laws. Furthermore, NIBC will assess whether any additional measures are necessary to guarantee an appropriate level of protection of your Personal Data. Please do not hesitate to contact our DPO if you wish to receive more information about the appropriate or suitable safeguards in place for data transfers outside of the EEA.

Where NIBC discloses Personal Data in response to requests from regulators and law enforcement or security agencies, these regulators and law enforcement or security agencies will be acting as a Data Controller. NIBC will always assess the legitimacy of such requests before disclosing any Personal Data and only disclose the Personal Data required to comply with the request.

3. WHAT ARE YOUR RIGHTS?

Under the GDPR and/or (if applicable to you) the UK GDPR, you have the following rights in relation to your Personal Data:

- a. Subject Access:** You have a right to be provided with access to any Personal Data held about you by NIBC and to receive certain information about the Processing of your Personal Data.
- b. Rectification:** You can ask us to have inaccurate or incomplete Personal Data corrected or completed.
- c. Erasure:** You can ask us to erase Personal Data in certain circumstances and we will take reasonable steps to inform Data Controllers with whom we have shared your Personal Data that you have requested the erasure of any links to, copies or replication of your Personal Data.
- d. Restriction:** Under certain circumstances, you can ask us to restrict the Processing of (certain) Personal Data.
- e. Portability:** Under certain circumstances, you can ask us to transmit the Personal Data that you have provided to us and we still hold about you to you in a structured, commonly used and machine-readable format, e.g. to be able to send it to a third party.
- f. Raise a complaint:** If you have a complaint about the Processing of your Personal Data by NIBC, we will do our utmost to resolve it with you. You can raise a complaint about our Processing with the data protection authority in your jurisdiction. In the Netherlands, this is the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), in the UK, the Information Commissioner's Office (ICO), in Belgium, the Data Protection Authority (Gegevensbeschermingsautoriteit), and in Germany the respective German State Data Protection Commissioner responsible for your complaint. For relevant contact details, please see paragraph 4.2. below. If you live or work in another country of the European Union, you can file a complaint with the competent supervisory authority in that country.

In addition, under certain conditions, you have the right to:

- where Processing is based on consent, **withdraw your consent**. Please note that the withdrawal of your consent does not affect the lawfulness of the Processing of your Personal Data prior to the withdrawal of your consent;
- **object** to any Processing of Personal Data that NIBC justifies on the **legitimate interests** legal Processing ground, unless our reasons for undertaking that Processing outweigh any prejudice to your interests, rights and freedoms; and;

Please be aware that certain exceptions apply to the exercise of these rights and so you may not be able to exercise these rights in all situations. Exceptions may include safeguarding the public interest (e.g. the prevention or detection of crime), our interests (e.g. the maintenance of legal privilege) and possible third party interests. If we refuse your request, we will explain the reasons for the refusal.

Please contact our DPO Office should you wish to exercise any of your rights. Contact details of our DPO can be found below. More generally, any questions relating to this Job Applicant Privacy Statement can be directed to our DPO.

Please be aware that in order to prevent fraud and misuse, we may need to request specific information from you to help us confirm your identity. We may also contact you to ask you for further information in relation to your request.

We will deal with your request without undue delay and ultimately within a month after receipt of your request, we will inform you whether we can comply with it. This period may be extended by two months in specific cases, for example when a complex request is made. We will inform you of such an extension within one month of receipt of your request.

4. NIBC ENTITIES AND CONTACT DETAILS

4.1 Contact details of our DPO

NIBC has appointed a data protection officer for its legal entities and branches (a DPO). Please do not hesitate to contact our DPO in case you have any questions in relation to the Processing of Personal Data by NIBC:

Contact details:	NIBC Bank NV Data Protection Officer E: dpo@nibc.com
Regular mail	NIBC Bank N.V. Data Protection Officer At the address for the relevant NIBC Legal Entity or Branch Office listed below:

- NIBC Bank N.V. - Carnegieplein 4, 2517 KJ The Hague, the Netherlands
- NIBC Bank N.V. (Belgium) Rue Royale 71, 1000 Brussels, Belgium
- NIBC Bank N.V. (London) - 26th Floor, 99 Bishopsgate, London EC2M 3XD, United Kingdom
- NIBC Bank N.V. (Frankfurt) - MainTower, Neue Mainzer Strasse 52, D - 60311 Frankfurt am Main, Germany

4.2 Contact details of the relevant data protection authorities

Country:	The Netherlands, Autoriteit Persoonsgegevens
Address:	Postbus 93374 2509 AJ Den Haag Nederland
Contact details:	(+31) (0)70 888 85 00
Website:	https://autoriteitpersoonsgegevens.nl/nl/contact-met-de-autoriteit-persoonsgegevens/informatie-en-meldpunt-privacy

Country:	United Kingdom, Information Commissioner's Office
Address:	Wycliffe House Water Lane, Wilmslow Cheshire, SK9 5AF United Kingdom
Contact details:	(+44) (0)303 123 1113
Website:	https://ico.org.uk/global/contact-us/postal-addresses/

Country:	Belgium, Gegevensbeschermingsautoriteit
Address:	Drukpersstraat 35 1000 Brussel Belgium
Contact details:	(+32) (0)2 274 48 00

Website: <https://www.gegevensbeschermingsautoriteit.be/contact>

Country: Germany, Der Hessische Datenschutzbeauftragte für Datenschutz und
Address: Informationsfreiheit
Postfach 3163
65021 Wiesbaden
Germany

Contact details: (+49) (0)611 1408 0
Website: <https://datenschutz.hessen.de/%C3%BCber-uns/kontakt>
