Deutsche Bank

South Africa Privacy Policy

Version 3
March 2023

Table of Contents

1. Scope

Deutsche Bank AG Johannesburg operates as a branch of Deutsche Bank AG (registered in Germany). As a banking institution, there are various streams of information that flow through the business. Therefore, Deutsche Bank AG Johannesburg (DBJ) is a responsible party for ensuring the protection of the information it processes. DBJ is also responsible for ensuring the information processed by the various functionaries in DBJ remains private and confidential where required. DBJ cares about protecting the personal information entrusted to us. This policy describes the principles which govern the processing and protection of all personal information in DBJ.

The principles described in this policy apply to personal information related to **living natural persons and juristic persons** (each a "person"). The policy applies to all information both physical records and structured and unstructured electronic records.

The right to privacy is an enshrined constitutional right. The right to privacy which includes the right to privacy of communications[1] is an essential human right that is fundamental to human dignity and is not easily limited.

The protection of the right to privacy finds expression in the Protection of Personal Information Act ("POPIA") which sets out the principles which should govern the processing of personal information by responsible parties. DBJ is a branch of a bank within the European Economic Area that also lends guidance from the provisions set out in the General Data Protection Regulation ("GDPR") which form the basis of Group Policies.

2. Information Processing

Processing of information includes the collection, receipt, recording, and storing of information amongst other uses[2]. The processing of information is strictly governed by DB's established policy framework which consists of local policies and procedures and Group-owned policies. The local information office is responsible for ensuring the policy framework and controls are consistent with group principles as well as local legislation. DBJ ensures that all information it obtains and processes; is obtained in a legal and reasonable manner that doesn't unjustifiably infringe on the rights of the data subject. DBJ processes various kinds of personal information with legal justification including CCTV cameras for security purposes. Each function within the branch is accountable for the information in its control. Each function has a clear understanding of all the information in its purview and the purpose of this personal information in its control.

In terms of POPIA, there are only limited reasons for which personal information may be processed[3] –

- If consensually provided by the data subject
- Information required to conclude or perform the contractual obligation
- Information required by law
- Information is necessary for the protection of a legitimate interest of the data subject
- Information is necessary for the protection of a legitimate interest of a responsible party

[1] Section 14(c) of the Constitution of South Africa of 1996

[2] Section 1 of Protection of Personal Information Act 2013

[3] Section 11 of the Protection of Personal Information Act 2013

DBJ only processes information if it relates to at least one of the abovementioned purposes.

We use personal information for the following purposes (note this is not an exhaustive list of uses):

- Manage risk, detect, and prevent fraud, to meet the requirements of anti-money laundering and terrorist financing laws and regulations and other legal, regulatory and industry self-regulatory requirements. These purposes may lead us to (among other measures):
  - establish and verify your and our client's identity, confirming politically exposed person status and check it against money laundering, terrorist financing or similar watch lists established by regulatory agencies or similar bodies in South Africa and internationally; and
  - check and evaluate prospective clients and business principals' past dealings or accounts with us or our international branches and affiliates, including, for example, information about onboarding rejections, relationship terminations, suspicious financial activity reports and other information material to financial risk assessment and fraud prevention, generally using a person's personal information to protect DBJ and its employees from fraud and error.
- Comply with legal reporting requirements stipulated by legislation, in-country and cross-border;
- Customer profiling;
- Maintain business records for reasonable periods and meet legal and regulatory record retention requirements;
- Meet our responsibilities to you and/or our clients;
- Follow your and/or our clients' instructions;
- Tell you and/or our clients by telephone and/or electronic communication about services and products available within the Group;
- Make sure our business suits client needs;
- Maintaining employee records as to Group requirements and for reporting purposes to the Department of Labour;
- Cross-check your qualifications and experiences with the requirements of job positions either currently vacant or becoming vacant in the future;
- Conducting background checks, including criminal records and ITC;
- Maintain a record of visitors to our premises for the means of corporate security as well as Occupational Health and Safety;
- Complete all requirements stipulated by Deutsche Bank Vendor Risk Management Policy; and
- Otherwise with a person's consent, or as permitted or required by law.

Without personal information, we may not be able to provide or continue to provide our clients with the products or services that they need.

DBJ is part of the Deutsche Bank Group and detail on the Group's data privacy rules can be found at the below external web address

https://www.db.com/company/en/data-protection.htm

3. Consent

Most personal information collected by DBJ in the course of business is done so by consent, however, it is important to note that consent is not always a legal requirement for collected information in contrast to GDPR provisions. Consent is not required where one or more of Section 11 of POPIA purposes exist at the time of processing (i.e., consent is not required if the information is being processed by a requirement law). Although not legally required, where necessary and appropriate consent may be sought- with the bounds of such consent clearly articulated. Consent to the collection, use and disclosure of personal information may be given in various ways.

Consent can be expressed (for example, orally, electronically or on a form signed describing the intended uses and disclosures of personal information) or implied (for example, when you and/or a client provide information necessary for a service requested). Consent may be given by your authorized representative (such as a legal guardian or a person having power of attorney). By providing DBJ with your personal information, we will assume that you consent to our collection, use and disclosure of such information for the purposes identified or described in this Privacy Policy, or otherwise at the time of collection. Therefore, by providing personal information to DBJ, you consent to us processing your personal information as set out in this policy.

If you provide us with personal information about another person, we will assume that you have the consent of that individual or entity to enable us to collect, use or disclose their personal information to us as described in this Privacy Policy.

You may withdraw your consent to our collection, use and disclosure of personal information, subject to contractual and legal restrictions and reasonable notice, provided that any consent you have given for certain purposes (for instance, risk management, fraud prevention and similar legitimate purposes identified in this policy) will be valid for so long as necessary to fulfil those purposes. Note that if you withdraw your consent to certain uses of your personal information, we may no longer be able to provide certain of, or all of, our products or services. Consent cannot be withdrawn in relation to the provision of a credit facility after credit has been granted. Even if you withdraw your consent, DBJ will still process personal information if it is legally entitled to do so.

An agreement produced by DBJ which contains a provision on personal information, which is signed by a data subject is considered consent for the use of personal information by virtue of the assertion of the agreement as a whole. In certain circumstances, consent will be required as a standalone matter in the course of a business relationship.

4. Personal Information Request

A data subject may at any point request to confirm personal information processed or retained by DBJ with the intention to verify its correctness. The data subject may at any point give the notice to correct personal information or aspects of personal information processed and/or retained by DBJ.

Both the notice to withdraw consent and notice to correct must be in writing and may be channelled through the functionary that initiated processing or directly to the Information Officer {Johan Gibhard – johan.gibhard@db.com}. The notice needs to expressly detail the intention as well as the reason for the request.

5. Notification of Data Subject

All data subjects for whom personal information have been processed shall be notified of the processing of such information, the general purpose of the information and any relevant information on the processing- the form of the notification is not prescribed and will take different forms and varying levels of detail based on the context under which information is being processed.

6. Further Processing of Personal Information

DBJ is part of a wider group and therefore information may be transferred to or collected by affiliates/associates for the same purpose for which the information was first processed. Should the intended purpose shift - in consultation with the Information Officer the transferring functionary will seek consent (if not pre-agreed) as well as various information privacy assurances prior to further processing.

7. Information Security

The protection of the information entrusted to the branch is a crucial component of the data privacy framework. DBJ analyses all potential risks to the information and structures its controls and policies with those risks in mind in order to uphold the privacy and integrity of information in the branch's purview. Data Protection Procedure sets out the granular detail which guides data protection controls- the Data Protection Procedure speaks to the principle set out in this Policy and Group protection policies.

In the case of an information breach, DBJ has effective and efficient processes which ensure a limitation to the harm caused by such a leak. Regulatory notifications of security compromises will also occur timeously and in the correct prescribed reporting manner as set out by the Information Regulator. DBJ has documented processes from a functionary level that cascade up to the Information Officer which allows any information security incident to be dealt with in an organised, timeous and bona fides manner to limit the prejudice of affected parties.

Should a data subject be in possession of information that suggests a data breach of information has occurred via interaction with DBJ, the such data subject must promptly report such suspicion to the Information Officer {Johan Gibhard- johan.gibhard@db.com, +27(0)11 7757000.

Deutsche Bank AG Johannesburg maintains a breach recording mechanism which allows for the identification, rectification and ownership of security compromise matters. All matters relating to security compromise are overseen by the information officer who has escalation recourse to regional and global data protection forums.

In terms of section 3(4) of the Cyber Crimes Act of 2020, any person who intercepts data of a non-public nature unlawfully has committed a criminal offence. Where such interception is detected by DBJ, the branch, through the Information Officer is obliged to report to the South African Police Service all information in their purview as it relates to such breach.

8. Data Retention

DBJ will not retain the Personal Information of a data subject any longer than its original purpose or longer than what is mandated by law. DBJ is also subject to the Group Master Retention Schedule which also prescribes a minimum period for which certain information is required to be retained in the legitimate operational interest of the business. We may store personal information unless you object, but we usually store it for as long as we are legally obliged to do so. If you object, we will only store it if we are legally permitted or obliged to do so.

Each functionary is responsible for maintaining the information in their purview and ensuring that redundant personal and other information is destroyed in an un- reconstructible manner.

9. Data minimisation

DBJ will only process and use Personal Information only where it is necessary and relevant to fulfilling a particular legitimate and legal purpose, DBJ ensures the non-excessive processing of information and will not request personal information unless it is strictly necessary. If we cannot avoid using Personal Information, we will only use the particular information necessary for the intended, legitimate purpose. In particular:

- We will limit the Personal Information we share with others, both internally (including with other DB entities) and externally, to that which is expressly authorized to be shared

10. Data Accuracy

Personal Information will be kept accurate, complete and up to date. You undertake to only provide accurate and up-to-date Personal Information to DBJ and to inform us without delays of any changes. You as a data subject provider would be liable for any loss incurred or damage suffered by DBJ for relying on inaccurate information.

If we notice any inaccuracies in the Personal Information that we handle, or if an individual or entity notifies us of any inaccuracy or change in their Personal Information, we will correct these immediately or escalate to the relevant person/team to be rectified.

Each internal business division and infrastructure function will ensure that it has adequate procedures in place to amend incorrect information and document that correction has been completed.

11. KYC Information

Most personal information that DBJ would process would relate to Customer Due Diligence processes- which require DBJ to identify and verify the existence of our clients at various intervals. The following KYC information is gathered by the Client On-Boarding team and is mandatory in terms of the Financial Intelligence Centre Act 1 of 2017 ("FIC Act"). This information is voluntarily provided as well as sourced from reputable public sources of information. The FIC Act prescribes to an extent the levels of identification required for a particular client and also prescribes a minimum period for which this information may be retained.

How information is processed, protected, and retained is the responsibility of the Front Office as well as Client Lifecycle Management ("CLM").

12. Third parties/Service Providers

A significant part of the processes carried out as part of DBJ's operations is automated through systems offered by third-party agents or service providers who provide services on our behalf, including administrative, billing, compliance, reporting, information technology or other processing or custodial services. Agreements with such third parties address the minimum data protection standards except on behalf of DBJ. Some of these entities may be located outside of South Africa, including, without limitation, in the United States, the United Kingdom, Singapore, India and Germany. These countries may not have data protection laws similar to those in South Africa.

We take reasonable measures to ensure that any personal information that may be collected, used, disclosed, or otherwise processed by these service providers, agents and/or our affiliates/associates on our behalf is protected and not used or disclosed for purposes other than as directed by DBJ, subject to legal requirements in foreign jurisdictions applicable to those organizations, for example, lawful requirements to disclose personal information to government authorities in those countries.

13. Recording of Telephone Calls

We may monitor and/or record telephone conversations with our representatives for our mutual protection, to ensure that client instructions are carried out, to document DBJ's compliance with legal requirements and to ensure that service levels are maintained. We may also use voice recognition to enhance the customer experience, detect fraud or for other purposes relating to our business. As required by legislation governing our regulatory licenses DBJ is required to record and keep a record of trading-related as well as product-offering conversations with clients.

14. Surveillance Cameras and Recording

For the legitimate security interest of DBJ, we may monitor movement in and around our premises by closed-circuit television for our mutual security and protection, including safeguarding our domiciliary rights and collecting evidence in cases of robbery and fraud. We may also use face recognition techniques to identify perpetrators of wrongful or criminal acts.

15. Marketing by electronic or telephonic means

We may use personal information to inform you of our products, market trends, economic outlooks etc. No such marketing may occur without the prior consent of the data subject. Such permission may be later revoked.

16. Monitoring of electronic communications

We communicate with you through different methods and channels. Where permitted by law, we may record and monitor electronic communications to make sure that they comply with our legal and regulatory responsibilities and internal policies.

17. Rights of individuals and juristic persons

Individuals and entities are granted the below rights in terms of POPIA, and we will adhere to these rights:

- the right to be informed about how and why their Personal Information is used;
- the right to ask for copies of the Personal Information held (including information contained in emails, instant messages, notes etc.);
- the right to ask for any inaccuracies in their Personal Information to be corrected;
- the right to have their Personal Information erased (where no obligations to keep the data exist beyond the retention period). You may also request that your Personal Information be erased if e.g. the Personal Information is no longer necessary for the purposes for which it was collected if the processing is based on your consent and you withdraw your consent for a specific process and there is no other legal ground for processing your Personal Information if you object to the processing of Personal Information where we do not have an overriding legitimate interest, the processing is unlawful, or the Personal Information has to be erased to enable us to comply;
- the right to ask to stop Processing their Personal Information;
- the right to object to their Personal Information being used for direct marketing purposes;
- the right to have any Personal Information that they have provided to be transferred to another party; and
- the right not to be subjected to a fully automated decision-making process (i.e., a system-generated decision without any human input), where the outcome has a legal or similarly significant effect on the individual concerned.

All exercise of rights by a data subject will follow the same prescribed manner- for access to information all exercise of rights will be conducted through an application in terms of Deutsche Bank's AG Johannesburg's "Accessing out Information" Manual (see Obligations under Promotion of Access to Information Act). All exercises of rights will be assessed and dealt with by the Information Officer and/or the Deputy Information Officer. When an individual or entity exercises any of the above rights, we will respond to the request in a strict time frame (in many cases one month, meaning one month to carry out the requested action). Any fees associated with such a request will be communicated to the data subject as soon as the application is assessed and decided on.

18. Obligations under the Promotion of Access Information Act

In the promotion of the right to information, the Promotion of Access to Information Act ("PAIA") makes it possible for private and public bodies to request certain personal and private information from institutions that process and retain such information on limited grounds. The process in which a body may request information from DBJ is prescribed in the PAIA Manual which includes the cost of such request as well as information that needs to be provided at the time of the request.

19. Information Regulator

You also have the right to seek external resources or clarity through the Information Regulator, the contact details of the Information Regulator can be found below.

Website: https://www.justice.gov.za/inforeg/

Address:

33 Hoofd Street
Forum III, 3rd Floor Braampark
P. O Box 31533
Braamfontein, Johannesburg, 2017

Mr Marks Thibela
Chief Executive Officer
Tel No. +27 (0) 10 023 5207, Cell No. +27 (0) 82 746 4173
inforeg@justice.gov.za

20. Compliance

All internal Business and Infrastructure heads are personally responsible for implementing and maintaining respective control standards and governance procedures to ensure compliance with this policy.

21. Information Officer Contact details

Should any person have any queries on the Privacy Policy or any aspect related to personal information connected to DBJ, the details of the Information Officer and the Deputy Information Officer in his absence are as follows:

The **Information Officer** and **Head: Compliance**
Deutsche Bank AG Johannesburg Branch
Private Bag X9933
Sandton
2146

Telephone: (011) 775 7000

2nd Floor North Towers
140 West Street
Sandton
2196

Johan Gibhard: Information Officer and Head of Compliance
johan.gibhard@db.com

Mfundo Mathunjwa- Deputy Information Officer
Mfundo.mathunjwa@db.com

22. Right to change this Privacy Policy

This Privacy Policy may be revised from time to time. If we intend to use or disclose personal information for purposes materially different than those described in this policy, we will make reasonable efforts to notify affected persons, if necessary, including by revising this Privacy Policy. The policy will be published on our website at
https://country.db.com/south-africa/documents/Privacy_Policy_South_Africa.pdf?language_id=1

If you are concerned about how your personal information is used, you should contact us as described above to obtain a current copy of this policy. We urge you to request and review this Privacy Policy frequently to obtain the current version. The publication on our website and/or your continued use of our products and/or services and/or continued provision of personal information would constitute your acceptance of changes to the policy.

23. Glossary

Term	Definition
Consent	means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Direct marketing	means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: (a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or (b) requesting the data subject to donate any kind for any reason.
Electronic communication	means any text, voice, sound or image message sent over an electronic communications network that is stored in the network or the recipient's terminal equipment until it is collected by the recipient.
Filing system	means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.
Information Officer	of, or in relation to, a: (a) public body means an Information Officer or deputy Information Officer as contemplated in terms of section 1 or 17 of the Promotion of Access to Information Act; or (b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act. Johan Gibhard- johan.gibhard@db.com Tel: 27 (0)117757000
Person	means a natural person or a juristic person
Personal information	means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— (a) information relating to race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or The employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or another particular assignment to the person; (d) the biometric information of the person;

Term	Definition
	(e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
POPIA	means Act No. 4 of 2013: Protection of Personal Information Act, 2013
Processing	means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including— (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of Information.
Public record	means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
Record	means any recorded information: (a) regardless of form or medium, including any of the following: (i) Writing on any material; (ii) information produced, recorded, or stored by means of any tape-recorder, computer equipment, whether hardware or software or both or other the device and any material subsequently derived from information so produced, recorded or stored; (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; (iv) book, map, plan, graph or drawing; v) photograph, film, negative, tape or another device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, being reproduced; (b) in the possession or under the control of a responsible party; (c) whether or not it was created by a responsible party; and

Term	Definition
	(d) regardless of when it came into existence.
Regulator	means the Information Regulator established in terms of section 39 of POPIA;