



Science • Sustainability • Social Impact

An ISO 9001-2015 Company

Data Privacy Policy

1. Objective

The purpose of this policy is to maintain the privacy of, and protect the personal information of employees, contractors, vendors, interns, associates, customers and business partners of Banka BioLoo Limited, and ensure compliance with laws and regulations applicable to Banka BioLoo Limited (hereafter referred to as “BANKA” or “the Company”).

2. Scope

This policy is applicable to all Banka employees, contractors, vendors, interns, associates, customers and business partners, who may receive personal information, have access to personal information collected or processed, or who provide information to Banka, regardless of geographic location. All employees of BANKA are expected to support the privacy policy and principles, when they collect and / or handle personal information, or are involved in the process of maintaining or disposing of personal information. This policy provides the information to successfully meet the Company’s commitment towards data privacy.

All partner firms and any third party working with or for BANKA, and who have or may have access to personal information, will be expected to have read, understood and comply with this policy. No third party may access personal information held by the Company, without having first entered into a confidentiality agreement.

3. Responsibilities

The owner for the Data Privacy Policy shall be the Data Privacy Officer. The Data Privacy Officer shall be responsible for maintenance and accuracy of this policy. Any queries regarding the implementation of this policy shall be directed to the Data Privacy Officer. This policy shall be reviewed for updates by Data Privacy Officer on an annual basis. Additionally, the data privacy policy shall be updated in-line with any major changes within the organization’s operating environment or on recommendations provided by internal/ external auditors.

4. Policy Compliance

Compliance to the data privacy policy shall be reviewed on an annual basis by Privacy Review Team to ensure continuous compliance monitoring through the implementation of compliance measurements and periodic review processes.

In cases where non-compliance is identified, the Data Privacy officer shall review the reasons for such non-compliance, along with a plan for remediation and report them to Privacy Review Team. Depending on the conclusions of the review, need for a revision to the policy may be identified. In instances of persistent non-compliance by the individuals concerned, they shall be subject to action in accordance with the Management’s decision.

5. Data Privacy Principles

This policy describes generally acceptable privacy principles (GAPP) for the protection and appropriate use of personal information at BANKA. These principles shall govern the use, collection, disposal and transfer of personal information, except as specifically provided by this Policy or as required by applicable laws.

- **Notice:** BANKA shall provide data subjects notice about how it collects, uses, retains, and discloses personal information about them.
- **Choice and Consent:** BANKA shall give data subjects the choices and obtain their consent regarding how it collects, uses, and discloses their personal information.
- **Rights of Data subject:** BANKA shall provide individuals the right to control their personal information, which includes the right to access, modify, erase, restrict, transmit, or object to certain uses of their information, and for withdrawal of earlier given consent to the notice.
- **Collection:** BANKA shall collect personal information from data subjects only for the purposes identified in the privacy notice / SoW / contract agreements and only to provide requested product or service.
- **Use, Retention and Disposal:** BANKA shall only use personal information that has been collected for the purposes identified in the privacy notice / SoW / contract agreements and in accordance with the consent that the data subject shall provide. BANKA shall not retain personal information longer than is necessary to fulfil the purposes for which it was collected, and to maintain reasonable business records. BANKA shall dispose the personal information once it has served its intended purpose or as specified by the data subject.
- **Access:** BANKA shall allow data subjects to make inquiries regarding the personal information about them, that BANKA shall hold and, when appropriate, shall provide access to their personal information for review, and/or update.
- **Disclosure to Third Parties:** BANKA shall disclose personal information to third parties / partner firms only for purposes identified in the privacy notice / SoW / contract agreements. BANKA shall disclose personal information in a secure manner, with assurances of protection by those parties, according to the contracts, laws and other segments, and, where needed, with consent of the data subject.
- **Obligations for Sub-processor:** Where a processor (vendor or third party acting on behalf of BANKA's data processor) engages another processor (sub-processor) for carrying out specific processing activities on behalf of BANKA (controller), the same data protection obligations as set out in the contract or other legal act between BANKA and the processor shall be imposed on the sub-processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of General Data Protection Regulation (GDPR). Where the sub-processor fails to fulfil its data protection obligations, the initial processor (relevant vendor or third party, acting on behalf of BANKA's data processor) shall remain fully liable to BANKA for the performance of that sub-processor's obligations.
- **Security for Privacy:** BANKA shall protect personal information from unauthorized access, data leakage and misuse.
- **Quality:** BANKA shall take steps to ensure that personal information in its records is accurate and relevant to the purposes for which it was collected.

- **Monitoring and Enforcement:** BANKA shall monitor compliance with its privacy policies, both internally and with third parties, and establish the processes to address inquiries, complaints and disputes.

6. Notice

Notice shall be made readily accessible and available to data subjects, before or at the time of collection of personal information or otherwise, notice shall be provided as soon as practical thereafter. Notice shall be displayed clearly and conspicuously, and shall be provided through online (e.g., by posting it on the intranet portal, website, sending emails, newsletters, etc.) and / or offline methods (e.g., through post, courier, etc.). All the websites (including Intranet portals), and any product or service that collects personal information internally, shall have a privacy notice.

Privacy notices may include:

- the organization's operating jurisdictions; third parties involved; business segments and affiliates; lines of business; locations;
- types of personal information collected; sources of information; who is collecting the personal information, including contact information;
- the purpose of collecting the personal information;
- assurance that the personal information will be used only for the purpose identified in the notice and only if the implicit and / or explicit consent is provided, unless a law or regulation specifically requires, otherwise;
- any choices the data subject have regarding the use or disclosure of the information; the process and data subject shall follow to exercise the choices;
- the process for a data subject to change contact preferences and ways in which the consent is obtained;
- collection process and how the information is collected; how the information is used, including any onward transfer to third parties;
- retention and disposal process for personal information; assurance that the personal information to be retained only as long as necessary to fulfil the stated purposes, or for a period specifically required by law or regulation and will be disposed of securely, or made anonymous, post the identified purpose is completed;
- process of accessing personal information; the costs associated for accessing personal information (if any); process to update / correct the personal information; the resolution of disagreements related to personal information; how the information is protected from unauthorized access or use;
- how users will be notified of changes made to privacy notice;
- disclosure process for third parties; the assurance that the personal information is disclosed to third parties only for the purpose identified; the remedial actions in place for any misuse of personal information by the third parties;
- security measures in place to protect the personal information; ways of maintaining quality of personal information;
- monitoring and enforcement mechanisms in place; description of the complaint channels available to data subjects; how the internal personnel, key stakeholders and the customers can contact the Company related to any privacy complaints or

- breaches; relevant contact information and / or other reporting methods, through which the complaints and/or breaches could be registered;
- consequences of not providing the requested information.

7. Choice and Consent

Choice refers to the options the data subjects are offered regarding the collection and use of their personal information. Consent refers to their agreement to the collection and use, often expressed by way in which they exercise a choice option.

- BANKA shall establish systems for the collection and documentation of data subject consents to the collection, processing, and/or transfer of personal data.
- Data subjects shall be informed about the choices available to them with respect to the collection, use, and disclosure of personal information.
- Consent shall be obtained (in writing or electronically) from the data subjects before or at the time of collecting personal information or as soon as practical thereafter.
- The changes to a data subject's preferences shall be managed and documented. Consent or withdrawal of consent shall be documented appropriately.
- The choices shall be implemented in a timely fashion and respected. If personal information is to be used for purposes not identified in the notice / SoW / contract agreements at the time of collection, the new purpose shall be documented, the data subject shall be notified, and consent shall be obtained prior to such new use or purpose.
- The data subject shall be notified if the data collected are used for marketing purposes, advertisements, etc.
- BANKA shall review the privacy policies of the third parties, and types of consent of third parties before accepting personal information from third-party data sources.

8. Collection of Personal Information

Personal information may be collected online or offline. Regardless of the collection method, the same privacy protection shall apply to all personal information.

Personal information shall not be collected, unless either of the following is fulfilled:

- the data subject has provided a valid, informed and free consent;
- processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject, prior to entering into a contract;
- processing is necessary for compliance with the organization's legal obligation;
- processing is necessary in order to protect the vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in public interest;
- data subjects shall not be required to provide more personal information than is necessary for the provision of the product or service that data subject has requested or authorized. If any data not needed for providing a service or product are requested, such fields shall be clearly labelled as optional. Collection of personal information shall be avoided or limited when reasonably possible;
- personal information shall be de-identified when the purposes of data collection can be achieved without personally identifiable information, at reasonable cost;

- when using vendors to collect personal information on the behalf of BANKA, it shall ensure that the vendors comply with the privacy requirements of BANKA as defined in this policy;
- BANKA shall, at minimum annually, review and monitor the information collected, the consent obtained and the notice / SoW / contract agreement identifying the purpose;
- the project team/support function shall obtain approval from the IT security team before adopting the new methods for collecting personal information electronically;
- BANKA shall review the privacy policies and collection methods of third parties before accepting personal information from third party data sources.

9. Use, Retention and Disposal

- Personal information may only be used for the purposes identified in the notice / SoW / contract agreements, and only if the data subject has given consent;
- Personal information shall be retained for as long as necessary for business purposes, identified in the notice / SoW / contract agreements at the time of collection, or subsequently authorized by the data subjects;
- When the use of personal information is no longer necessary for business purposes, a method shall be in place to ensure that the information is destroyed in a manner sufficient to prevent unauthorized access to that information or is de-identified in a manner sufficient to make the data non-personally identifiable;
- BANKA shall have a documented process to communicate changes in retention periods of personal information required by the business to the data subjects, who are authorized to request those changes;
- Personal information shall be erased, if their storage violates any of the data protection rules or if knowledge of the data is no longer required by BANKA or for the benefit of the data subject. Additionally, BANKA has the right to retain the personnel information for legal and regulatory purpose, and as per applicable data privacy laws.
- BANKA shall perform an internal audit on an annual basis to ensure that personal information collected is used, retained and disposed of in compliance with the organization's data privacy policy.

10. Access

BANKA shall establish a mechanism to enable and facilitate exercise of data subject's rights of access, blockage, erasure, opposition, rectification, and, where appropriate or required by applicable law, a system for giving notice of inappropriate exposure of personal information.

- Data subjects shall be entitled to obtain the details about their own personal information upon a request made and set forth in writing. BANKA shall provide its response to a request within 72 hours of receipt of written request.
- The data subjects shall have the right to require BANKA to correct or supplement erroneous, misleading, outdated, or incomplete personal information.

- Requests for access to, or rectification of personal information shall be directed, at the data subject's option, to the manager of the projects team or support function responsible for the personal information.
- The privacy coordinators shall record and document each access request as it is received and the corresponding action taken.
- BANKA shall provide personal information to the data subjects in a plain simple format, which is understandable (not in any code format).

11. Disclosure to Third Parties

Data Subject shall be informed in the privacy notice / SoW / contract agreement, if personal information shall be disclosed to third parties / partner firms, and it shall be disclosed only for the purposes described in the privacy notice / SoW / contract agreements and for which the data subject has provided consent.

- Personal information of data subjects may be disclosed to the third parties / partner firms only for reasons consistent with the purposes identified in the notice / SoW / contract agreements or other purposes authorized by law.
- BANKA shall notify the data subjects prior to disclosing personal information to third parties / partner firms for purposes not previously identified in the notice / SoW / contract agreements.
- BANKA shall communicate the privacy practices, procedures and the requirements for data privacy and protection to third parties / partner firms.
- The third parties shall sign an NDA (Non-Disclosure Agreement) with BANKA before any personal information is disclosed to the third parties partner firms. The NDA shall include the terms on non-disclosure of customer information.

12. Security

Information security policy and procedures shall be documented and implemented, to ensure reasonable security for personal information collected, stored, used, transferred and disposed of by BANKA.

- Information asset labelling and handling guidelines shall include controls specific to the storage, retention and transfer of personal information.
- Management shall establish procedures that maintain the logical and physical security of personal information.
- Management shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards.
- Individuals noticing or becoming aware of any breach of personal data shall notify the DPO, by emailing at it@bankabio.com, within 2 hours. It shall be the DPO's responsibility to analyze and act on the intimation of the same, within 24 hours.

13. Quality

BANKA shall maintain data integrity and quality, as appropriate, for the intended purpose of personal data collection, and use and ensure data are reliable, accurate, complete and current. For this purpose, the DPO and privacy co-ordinators shall have

systems and procedures in place to ensure that personal information collected is accurate and complete for the business purposes, for which it is to be used.

14. Monitoring and enforcement

- BANKA shall perform a periodic review of all the complaints related to data privacy to ensure that all the complaints are resolved in a timely manner, and resolutions are documented and communicated to the data subjects.
- An escalation process for unresolved complaints and disputes shall be designed and documented.
- Communication of privacy incident / breach reporting channels and the escalation matrix shall be provided to all the data subjects.
- Employees with inquiries or complaints about the processing of their personal information shall first discuss the matter with their immediate supervisor. If the employee does not wish to raise an inquiry or complaint with an immediate manager, or if the manager and employee are unable to reach a satisfactory resolution of the issues raised, the employee shall bring the issue to the attention of the Grievance Officer, emailing it@bankabio.com).
- Customers / third parties with inquiries or complaints about the processing of their personal information shall bring the matter to the attention of the Grievance Officer in writing. Any dispute concerning the processing of the personal information of non-employees shall be resolved through arbitration.
- Privacy Review Team shall conduct an internal audit annually (at minimum) to ensure compliance with the established privacy policies and applicable laws.
- The internal audit shall consist of the review of the following:
 - o personal information collected from data subjects;
 - o the purposes of the data collection and processing;
 - o the actual uses of the data;
 - o disclosures made about the purposes of the collection and use of such data;
 - o the existence and scope of any data subject consents to such activities;
 - o any legal obligations regarding the collection and processing of such data; and
 - o the scope, sufficiency, and implementation status of security measures.
- The Data Privacy Officer, along with Privacy Coordinators, shall take actions on the findings from the internal audit, and work on the recommendations for improvement of the privacy posture.
- Any change made to the policy shall be communicated to all the employees, the stakeholders and the customers / clients.