LAFIA.IO DATA PRIVACY POLICY

Contents

LAFIA.IO DATA PRIVACY POLICY

i. Aim of the Data Protection Policy

ii. Scope and amendment of the Data Protection Policy

This Data Protection Policy applies to Lafia.io and its employees. The Data Protection Policy extends to all processing of personal data. Anonymised data, e.g., for statistical evaluations or studies, is not subject to this Data Protection Policy. This Data Protection Policy can be amended in coordination with the Data Protection Officer and the Chief Executive Officer under the defined procedure for amending policies. The amendments will be reported immediately using the process for amending policies.

iii. Application of national laws

This Data Protection Policy comprises the internationally accepted data protection principles without replacing the existing national laws. It supplements the national data protection laws. The relevant national law will take precedence if it conflicts with this Data Protection Policy, or it has stricter requirements than this Policy. The content of this Data Protection Policy must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed.

Lafia.io is responsible for compliance with this Data Protection Policy and legal obligations. If there is reason to believe that legal obligations contradict the duties under this Data Protection Policy, the Data Protection Officer should be informed. In the event of conflicts between national legislation and the Data Protection Policy, Lafia.io will work to find a practical solution that meets the purpose of the Data Protection Policy.

iv. Principles for processing personal data

a. Fairness and lawfulness

When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed legally and fairly.

b. Purpose limitation

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

c. Transparency

The data subject must be informed of how their data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of or informed of:

- The identity of the Data Controller;
- The purpose of data processing; and
- Third parties or categories of third parties to whom the data might be transmitted.

d. Data minimisation

Before processing personal data, you must determine whether and to what extent the processing of personal data is necessary to achieve the purpose for which it is

undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

e. Storage limitation

Personal data should only be stored for as long as they are needed. Data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit the protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

f. Accuracy

Personal data on file must be correct, complete, and – if necessary – kept up to date. Appropriate measures must be in place to ensure that inaccurate or incomplete data are deleted, corrected, supplemented, or updated.

g. Confidentiality and integrity of data

Personal data must be secured with appropriate organisational and technical measures to prevent unauthorised access, illegal processing, or sharing, as well as accidental loss, modification, or destruction.

h. Lawfulness

i. Reliability of data processing

Collecting, processing, and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing, and using the personal data is to be changed from the original purpose.

1. Customer and partner data

1.1. Data processing for a contractual relationship

Personal data of the relevant prospects, customers, and partners can be processed to establish, execute, and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Before a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfil other requests of the prospect that relate to contract conclusion. Prospects can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospects must be complied with.

1.2. Data processing for advertising purposes

If the data subject contacts Lafia.io to request information (e.g., request to receive information material about a product), data processing to meet this request is permitted.

Customer loyalty or advertising measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research,

provided that this is consistent with the purpose for which the data was initially collected. The data subject must be informed about the use of his/her data for advertising purposes. If data is collected only for advertising purposes, the disclosure from the data subject must be voluntary. The data subject shall be informed that providing data for this purpose is voluntary. When communicating with the data subject, consent shall be obtained from him/her to process the data for advertising purposes. When giving consent, the data subject should be given a choice among available forms of contact, such as regular mail, email, and phone.

If the data subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

1.3. Consent to data processing

Data can be processed if the consent of the data subject is validly obtained. Before giving consent, the data subject must be informed. The declaration of consent must be obtained in writing or electronically for documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

1.4. Legal obligation

The processing of personal data is also permitted if national legislation requests, requires, or allows this. The type and extent of data processing must be necessary for the legally authorised data processing activity and must comply with the relevant statutory provisions.

1.5. Performance of contract

Personal data can be processed to fulfil the performance of a contract between Lafia.io and a customer or partner. Such a contract must contain a data processing clause or accompanied with a data processing agreement. Existing contracts should have an addendum incorporating the provisions of the Regulation.

1.6. Legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest in Lafia.io. Legitimate interests are generally of a legal (e.g., collection of outstanding receivables) or commercial nature (e.g., avoiding breaches of contract). Personal data may not be processed for a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection. Before relying on legitimate interest as a legal basis, Lafia.io must conduct a Legitimate Impact Assessment (LIA) and must be documented.

1.7. Processing of highly sensitive data

Sensitive personal data can be processed only if the law requires this, or the data subject has given express consent. This data can also be processed if it is mandatory for asserting, exercising, or defending legal claims regarding the data subject. If there are plans to process sensitive data, the Data Protection Officer must be informed in advance.

1.8. Automated individual decisions

Automated processing of personal data that is used to evaluate certain aspects (e.g., credit- worthiness) cannot be the sole basis for decisions that have adverse legal consequences or could significantly impair the data subject. The data subject must be informed of the facts and results of automated individual decisions and the possibility to respond. To avoid erroneous decisions, a test and plausibility check must be made by an employee.

1.9. User data and internet

If personal data is processed and used on websites or in apps, the data subjects must be informed of this in a privacy notice and, if applicable, information about cookies. The privacy notice and any cookie information must be integrated so that it is easy to identify, directly accessible, and consistently available for the data subjects.

If user profiles (tracking) are created to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy notice. Personal tracking may only be affected if it is permitted under the law or upon the consent of the data subject. If tracking uses a pseudonym, the data subject should be given a chance to opt-out in the privacy notice.

If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access

2. Employee data

2.1. Data processing for the employment relationship

In employment relationships, personal data can be processed if needed to initiate, carry out, and terminate the employment agreement. When initiating an employment relationship, the applicants' data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with third parties.

In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorised data processing apply.

If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws have to be observed. In cases of doubt, consent must be obtained from the data subject.

There must be legal authorisation to process personal data that is related to the employment relationship but was not originally part of the performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, contract, consent of the employee, or the legitimate interest of the company.

2.2. Legal Obligation

The processing of personal employee data is also permitted if national legislation requests, requires or authorises this. The type and extent of data processing must be necessary for the legally authorised data processing activity and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

2.3. Collective agreements on data processing

If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorised through a collective agreement. Collective agreements are pay scale agreements or agreements between employers and employee representatives, within the scope allowed under the relevant employment law. The agreements must cover the specific purpose of the intended data processing activity and must be drawn up within the parameters of national data protection legislation.

2.4. Consent to data processing

Employee data can be processed upon the consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for documentation. In certain circumstances, consent may be given verbally, in which case it must be appropriately documented. In the event of informed, voluntary provision of data by the relevant party, consent can be assumed if national laws do not require express consent. Before giving consent, the data subject must be made fully aware of the purpose for which his data is being processed.

2.5. Legitimate Interest

Personal data can also be processed if it is necessary to enforce a legitimate interest in Lafia.io. Legitimate interests are generally of a legal (e.g., filing, enforcing or defending against legal claims) or financial (e.g., valuation of companies) nature.

Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection.

Control measures that require the processing of employee data can be taken only if there is a legal obligation to do so, or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the company in performing the control measure (e.g., compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion and cannot be performed unless appropriate. The legitimate interest of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law (e.g., rights of co-determination for the employee representatives and information rights of the data subjects) must be taken into account.

2.6. Processing of sensitive data

Sensitive personal data can be processed only under certain conditions. Sensitive personal data is data about racial and ethnic origin, political beliefs, sexual orientation, biometric data, religious or philosophical beliefs, union membership, and the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive, or the content of the data categories can be filled out

differently. Moreover, data that relates to a crime can often be processed only under special requirements under national law.

The processing must be expressly permitted or prescribed under national law. Additionally, processing can be permitted if the responsible authority must fulfil its rights and duties in the area of employment law. The employee can also expressly consent to the processing.

If there are plans to process highly sensitive data, the Data Protection Officer must be informed in advance.

2.7. Automated decisions

If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g., as part of personnel selection or the evaluation of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee. To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation and that this evaluation is the basis for the decision. The data subject must also be informed of the facts and results of automated individual decisions and the possibility to respond.

2.8. Telecommunications and internet

Telephone equipment, email addresses, intranet, and the internet, along with internal social networks, are provided by the company primarily for work-related assignments. They are a tool and company resource. They can be used within the applicable legal regulations and internal company policies. In the event of authorised use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

There will be no general monitoring of telephone and email communications or intranet/ internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to Lafia.io's network that block technically harmful content or that analyse the attack patterns. For security reasons, the use of telephone equipment, email addresses, the intranet/internet, and internal social networks can be logged for a temporary period. Evaluations of this data from a specific person can be made only in concrete, justified cases of suspected violations of laws or policies of Lafia.io. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as the company's policies.

v. Transmission of personal data

Transmission of personal data to recipients outside or inside Lafia.io is subject to the authorisation requirements for processing personal data under this Section **V**. The data recipient must be required to use the data only for the defined purposes.

If data is transmitted to a recipient outside Lafia.io situate in another country, this recipient must agree to maintain a data protection level equivalent to this Data Protection Policy. This does not apply if the transmission is based on; the explicit consent of the data subject, contract on behalf of the data subject or between Lafia.io and a data subject. A legal obligation of this kind can be based on the laws of the country transmitting the data. In the alternative, the laws of the country of the company can acknowledge the purpose of

data transmission based on the legal obligation of a third country. If a third party transmits data to Lafia.io, it must be ensured that the data can be used for the intended purpose.

Also, the data subject is entitled to assert his or her rights against Lafia.io. In the event of claims of a violation, the company exporting the data must document to the data subject that the company importing the data in a third country (if the data is further processed after receipt) did not violate this Data Protection Policy.

In the case of personal data being transmitted from Lafia.io to a third-party company located in another country, the data controller transmitting the data shall be held liable for any violations of this Policy committed by the entity located in a third country concerning the data subject whose data was collected in Nigeria, as if the violation had been committed by the data controller transmitting the data.

vi. Contract data processing

Data processing on behalf of a data controller means that a provider is hired to process personal data, without being assigned responsibility for the related business process. In these cases, a data processing agreement must be concluded with external providers. The client retains full responsibility for the correct performance of data processing. The provider can process personal data only as per the instructions from Lafia.io. When issuing the order, the following requirements must be complied with; the department placing the order must ensure that they are met.

a. The provider must be chosen based on its ability to cover the required technical and organisational protective measures.

b. The order must be placed in writing. The instructions on data processing and the responsibilities of the client and provider must be documented.

c. The contractual standards for data protection provided by the Data Protection Officer must be considered.

d. Before data processing begins, Lafia.io must be confident that the provider will comply with the duties. A provider can document its compliance with data security requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated regularly during the term of the contract.

e. In the event of cross-border contract data processing, the relevant national requirements for disclosing personal data abroad must be met.

vii. Rights of the data subject

Every data subject has the following rights. Their assertion is to be handled immediately by the responsible unit and cannot pose any disadvantage to the data subject:

a. The data subject may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose. If there are further rights to view the employer's documents (e.g., personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected. In ensuring that this right is not violated, Lafia.io shall publish its privacy notice on its website and on every data collection point;

b. If personal data is transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients;

c. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented;

d. The data subject can object to the processing of his or her data for purposes of advertising or market/opinion research. The data must be blocked from these types of use;

e. The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed;

f. The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

Refer to procedure on data subject rights

viii. Confidentiality of processing

Any unauthorised collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorised to carry out as part of his/her legitimate duties is unauthorised. The “need to know” principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a thorough breakdown and separation, as well as the implementation of roles and responsibilities.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorised persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

ix. Processing security

Personal data must be safeguarded from unauthorised access and unlawful processing or disclosure, as well as accidental loss, modification, or destruction. This applies regardless of whether data is processed electronically or in paper form, before the introduction of new methods of data processing, particularly new IT systems, technical and organisational measures to protect personal data must be defined and implemented. These measures must be based on state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification).

In particular, the responsible department can consult with its Information Security Officer (ISO) or anyone exercising a similar function and the Data Protection Officer. The technical and organisational measures for protecting personal data are part of Corporate Information Security management and must be adjusted continuously to the technical developments and organisational changes.

x. Data protection control

Compliance with the Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits, assessment, and other controls. The performance of these controls is the responsibility of the Data Protection Officer and other company units with audit rights or external auditors hired. The results of the data protection controls must be reported to the Board. The Board must be informed of the initial results as part of the related reporting duties. On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data protection authority can perform its controls of compliance with the regulations of this Policy, as permitted under national law.

xi. Data protection incidents

All employees must inform their supervisor or the Data Protection Officer immediately about cases of violations against this Data Protection Policy or other regulations on the protection of personal data (data protection incidents). The manager responsible for the function or the unit is required to inform the Data Protection Officer immediately about data protection incidents.

In cases of:

- improper transmission of personal data to third parties;
- improper access by third parties to personal data; or
- loss of personal data

The required company reports (Information Security Incident Management/Incident Management Form) must be made immediately so that any reporting duties under national law can be complied with. *Refer to Data Breach Response Policy.*

xii. Responsibilities and sanctions

The executive body of Lafia.io is responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements and those contained in the Data Protection Policy for data protection are met (e.g., national reporting duties). The management staff is responsible for ensuring that organisational, HR, and technical measures are in place so that any data processing is carried out following data protection. Compliance with these requirements is the responsibility of the relevant employees.

The relevant executive body must designate the Data Protection Officer. The Data Protection Officer is the contact person on-site for data protection. They can perform checks and must familiarise the employees with the content of the data protection policies. Management is required to assist the Data Protection Officer with their efforts. The departments responsible for business processes and projects must inform the Data Protection Officer in good time about new processing of personal data. For data processing plans that may pose unique risks to the individual rights of the data subjects, the Data Protection Officer must be informed before processing begins. This applies, in particular, to compassionate personal data. The managers must ensure that their employees are sufficiently trained in data protection.

Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted in Nigeria and other countries with extra-territorial laws and result in claims for compensation of damage. Violations for which individual employees are responsible can lead to sanctions under employment law.

xiii. Data Protection Officer

The Data Protection Officer, being internally independent of professional orders, works towards compliance with national and international data protection regulations. The Leader is responsible for the Data Protection Policy and supervises its compliance. Lafia.io's Board of Management appoints the Data Protection Officer. The Data Protection Officer shall promptly inform the Management of any data protection risks.

Data subjects may approach the Data Protection Officer at any time to raise concerns, ask questions, request information, or make complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially and promptly. Decisions made by the Data Protection Officer to remedy data protection breaches must be upheld by the Management of the company in question. Inquiries by supervisory authorities must always be reported to the Data Protection Officer through Lafia.io.

xiv. Definitions

a. **Consent** is the voluntary, legally binding agreement to data processing.

b. **Data** is anonymised if no one can ever trace personal identity, or if the personal identity could be recreated only with an unreasonable amount of time, expense, and labour.

c. **Data protection incidents** are all events where there is justified suspicion that personal data is being illegally captured, collected, modified, copied, transmitted, or used. This can pertain to actions by third parties or employees.

d. **Data subject** under this Data Protection Policy is any natural person whose data can be processed.

e. **Sensitive personal data** is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership, or the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive, or the content of the data categories can be structured differently. Moreover, data that relates to a crime can often be processed only under special requirements under national law.

f. **Personal data** is all information about particular or definable natural persons. A person is definable, for instance, if the personal relationship can be determined using a combination of information with even incidental additional knowledge.

g. **Processing** personal data means any process, with or without the use of automated systems, to collect, store, organise, retain, modify, query, use, forward, transmit, disseminate or combine and compare data. This also includes disposing of, deleting and blocking data and data storage media.

h. **Data Controller** is the legally independent company of Lafia.io, whose business activity initiates the relevant processing measure.

i. **Third countries** under the Data Protection Policy are all nations outside Nigeria. This does not include countries with a data protection level that is considered sufficient by NITDA or relevant supervisory authority.

j. **Third parties** are anyone apart from the data subject and the Data Controller.

k. **Transmission** is all disclosure of protected data by the responsible entity to third parties.