BIOMETRIC SOLUTIONS LIMITED

DATA PROTECTION POLICY

12A MANNINGS HILL ROAD, KINGSTON 8, JM WI, TELEPHONE: (876) 620-8321-2

DATA PROTECTION POLICY
BIOMETRIC SOLUTIONS LIMITED

1.0 Policy Statement

Further to the enactment of the Data Protection Act 2020, Biometric Solutions has implemented internal systems and guidelines to secure the privacy rights of its clients and staff. This policy applies to both staff and clients and outlines the means by which the personal information collected and processed by Biometrics Solutions as a Data Controller is kept safe and secure. In the provision of our suite of services, we are required to collect, disclose and use personal information of clients. Additionally, there may be instances whether by law, consent or legitimate purposes, that information may be shared with third parties. In any such circumstance you will be advised in advance as to the nature and purpose for the disclosure and the utmost diligence will be applied to ensure the preservation and confidentiality of the information.

While personal information is usually collected at the time of engagement, there may be instances where information is collected at various points of engagement. This is particularly true for existing clients or members of staff who maybe requested to provide updated or additional personal information.

At all times, it is our commitment to not take more information than is required, to not keep that information for longer than is required and to not share that information with third parties outside of the exemptions permitted by law. In all instances where information will be shared, the relevant data subject will be advised. Further, each member of staff is responsible for the protection of all data stored and accessed whether electronically or in physical format.

Our Data Protection Policy is guided by the Data Protection Act and subscribes to the eight data protection principles, namely:

1. Fairness and lawfulness;
2. To obtain personal information for limited specific and required purposes and to ensure it will not be processed outside of the stated purposes.
3. To limit personal data processed to only personal data that is relevant and not excessive
4. To ensure that the personal data of the data subject is accurate
5. To retain personal data no longer that is required or necessary
6. To ensure that the transfer of data is limited to jurisdictions with adequate data protection and privacy framework.

7. To implement appropriate internal and technical measures to secure personal data.

8. Ensure the preservation of the rights of the data subject.

2. Definitions (pursuant to the Data Protection Act 2020)

Biometric Data: in relation to an individual, means any information relating to the physical, physiological or behavioural characteristics of that individual, which allows for the unique identification of the individual, and includes—

(a) physical characteristics such as the photograph or other facial image, finger print, palm print, toe print, foot print, iris scan, retina scan, blood type, height, vein pattern, or eye colour, of the individual, or such other biological attribute of the individual as may be prescribed; and

(b) behavioural characteristics such as a person's gait, signature, keystrokes or voice.

Data Controller: means any—

(a) person; or

(b) public authority,

who, either alone or jointly or in common with other persons determines the purposes for which and the manner in which any personal data are, or are to be, processed, and where personal data are processed only for purposes for which they are required under any enactment to be processed, the person on whom the obligation to process the personal data is imposed by or under that enactment is for the purposes of this Act a data controller

Data Processing: in relation to information or personal data means obtaining, recording or storing the information or personal data, or carrying out any operation or set of operations (whether or not by automated means) on the information or data, including—

(a) organisation, adaptation or alteration of the information or data;

(b) retrieving, consulting or using the information or data;

(c) disclosing the information or data by transmitting, disseminating or otherwise making it available; or

(d) aligning, combining, blocking, erasing or destroying the information or data, or rendering the data anonymous.

Data Processor: in relation to personal data, means any person, other than an employee of the data controller, who processes the data on behalf of the data controller.

Data Subject: means a named or otherwise identifiable individual who is the subject of personal data, and in determining whether an individual is identifiable account shall be taken of all means used or reasonably likely to be used by the data controller or any other person to identify the individual, such as reference to an identification number or other identifying characteristics (whether physical, social or otherwise) which are reasonably likely to lead to the identification of the individual;

Personal Data: (a) means information (however stored) relating to—

(i) a living individual; or

(ii) an individual who has been deceased for less than thirty years, who can be identified from that information alone or from that information and other information in the possession of, or likely to come into the possession of, the data controller; and

(b) includes any expression of opinion about that individual and any indication of the intentions of the data controller or any other person in respect of that individual;

Sensitive Personal Data: means personal data consisting of any of the following information in respect of a data subject—

(a) genetic data or biometric data;

(b) filiation, or racial or ethnic origin;

(c) political opinions, philosophical beliefs, religious beliefs or other beliefs of a similar nature;

(d) membership in any trade union;

(e) physical or mental health or condition;

(f) sex life;

(g) the alleged commission of any offence by the data subject or any proceedings for any offence alleged to have been committed by the data subject.

3. What kinds of data do we process?

In order to deliver our services and to effectively manage our legal obligations, we may ask to be provided with certain personally identifiable information such as:

i. Full name of Client/employee
ii. Telephone number (home and cell)
iii. Address
iv. NIS (employee only)
v. TRN
vi. Occupation
vii. Address of place of employment
viii. Telephone number (work)
ix. Email address
x. Banking details
xi. Company name
xii. Company TRN
xiii. Company Address

4. Purpose for data collection

4.1 Data is collected from our clients for the purpose of performing contractual obligations and to meet service deliverables as per requests. The information may also be required to ensure efficacy in the products and software being marketed and supplied to clients as per client specifications. Generally, the information will be required as a key part of our "know your client" on-boarding and to comply with all applicable laws.

4.2 All data collected with respect to our staff is for the purpose of compliance with existing labour laws, legitimate purpose and by consent. As such, the collection, maintenance and use, will be solely for management and administrative purposes. This personal data is usually collected during recruitment and stored to facilitate the payment of remuneration, provision of staff benefits and welfare, and the general management of staff. Staff data is secured by limited accessibility by the Human Resource Management Team and the CEO of Biometric and to a lesser extent the Payroll Department.

4.3 During recruitment, additional sensitive personal data may be collected. The situations for additional data will include instances such as criminal record checks or requests for medical and health information where by law the company is required to make special provisions under the Disability Act of Jamaica 2014.

5. How do we use your data?

The Biometric Solutions Limited may use your personal data for the following purposes:

i. To provide and maintain our services to you.

ii. For the performance of our contract with you. This will include the general management of your account, the development, compliance and undertaking of the purchase contract for the products, items or services, general software management and maintenance of the system purchased from us.

iii. To contact you by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.

iv. For marketing and promotional goods/information.

v. To evaluate and improve our Service, products, services, marketing and your experience.

6. Retention of your Personal Data

6.1The Company will retain your personal data only for as long as is necessary for the purposes set out in this Policy. We will retain and use your personal data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

6.2 In all instances, we do not retain the information of clients for longer than a period of seven (7) years after the performance of the contract and for staff, for a period of ten (10) years after separation.

6.3 All Personal and sensitive Information shall be disposed of at the end of the relevant period including information stored electronically. Physical documents will be disposed of by shredding or returning to the client or employee as applicable.

7. Transfer of your Personal Data

7.1 Your information, including Personal Data, is processed at the Company's operating offices and by the product supplier in the United States of America. As such, your information is transferred to and maintained on secured servers located outside of Jamaica. The servers are secured using Microsoft Azure and Amazon

7.2 Your consent to this Policy followed by Your submission of such information represents Your agreement to that transfer. The Company will take all steps reasonably necessary to ensure that Your data is treated securely and in accordance with this Policy and no transfer of Your Personal Data will take place to any organization or a country unless there are adequate controls in place including the security of your data and other personal information.

8. Storage and Security

8.1 All members of the staff are required to operate with the utmost confidentiality with respect to client's and employees' personal and sensitive information. We employ the following general strategies to ensure the foregoing:

a. Restrict and monitor access to sensitive data
b. Develop transparent data collection procedures
c. Train employees in online privacy and security measures
d. Build secure networks to protect online data
e. Ensuring that any data-processing software and antivirus software used by the company are effectively maintained and up-to-date;
f. Selecting data processors who sufficiently guarantee that they have adequate security measures in place and will report security breaches;
g. Implement and maintain strategies to restore the availability of and access to, personal data in a timely manner in the event of a physical or technical incident.
h. Establish clear procedures for reporting privacy breaches or data misuse
i. Include contract clauses or communicate statements on how we handle data
j. Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

8.2 In all instances, where files are kept in a physical form, they are held in locked file cabinets and where electronically held, only shared with the members of the team who are actively working on the matter.

8.3 Security of personal data is further secured by limiting access to our IT Servers to only authorized members of staff, access to computers and databases are password protected; relevant staff members use unique passwords and are not permitted to disclose passwords and personal data is never stored on portable devices.

8.4 Biometric Solutions further employ additional security measures against unauthorized access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The Security of personal data is governed by the Guidelines accompany this Policy at Appendix I.

9 Protection of Data Subject Rights

9.1 At all times the rights of the client or employee over their personal and sensitive information as outlined in the Data Protection Act shall be preserved. These shall include the following:

i. The right to view/access your personal data

ii. The right to be informed as to the use of your personal data

iii. The right to correct or delete data as permitted by law. Provided always that any request for access, change and or deletion must be in writing.

iv. The right to object to the continued use and processing of your data within the provisions of the law. Provided that the any such request is made in writing and with the understanding that it may impact the continued provision of our services to you.

9.3 Biometric Solutions will employ all available strategy and technologies in ensuring the safety and security of the personal data of clients and staff, there may be instances where a breach may occur. In every such instance the breach shall be reported immediately to the Data Protection Officer, who shall collect all information concerning the data subject, the nature of the data affected by the breach, the date and time of the breach, how the breach was identified and if applicable who reported the breach, and provide a report.

9.4 Where a data breach has occurred, the data subject must be notified immediately. Any report shall include the following:

i. description of type/nature of the personal data;

ii. how the personal data breach occurred;

iii. date and time the personal data breach occurred;

iv. what data was involved;

v. measures taken by Biometric Solutions to mitigate the impact and effect of the personal data breach;

9.4 Where a data breach has occurred, the Office of the Information Commissioner shall be notified within 72 hours of the identification of the breach and shall include the information outlined in the Guidelines to this policy.

10 Policy Review

This policy shall be reviewed every three (3) years or at such other time as may be required by law or the CEO may deem appropriate.

APPENDIX I

DATA PROTECTION GUIDELINES

1. General principles

i. Members of staff shall ensure that personal data is processed and handled in accordance with this Policy and the Data Protection principles and standards.

ii. Members of staff collectively and individually have the responsibility to ensure that personal data is collected, stored, shared and used appropriately.

iii. Members of staff shall only access personal data which is required for the completion of duties. Where a member of staff is found to have accessed personal data outside of the scope of their core function, the member of staff shall be subject to disciplinary proceedings.

iv. Members of staff are required to familiarize themselves with the requirements of the Data Protection Act and the terms of this policy.

v. Members of staff shall be required to attend all training initiatives coordinated by the Management Team of Biometric Solutions.

vi. Members of Staff are prohibited from informally sharing personal data whether internally or externally. For the avoidance of doubt, personal data shall not be shared without the explicit instructions of the Supervisor, Manager or CEO.

vii. Biometric Solutions shall ensure that the transfer of personal data is limited to jurisdictions with a regulatory framework that recognizes and protects personal data privacy.

viii. Biometric Solutions shall ensure that the personal data of staff and clients are up to date and accurate. To this end, regular audits of the information being processed shall be conducted and the personal data amended accordingly.

ix. Members of staff should ensure that client and other members personal data are not discussed in open spaces and or within the hearing of unauthorized staff or third parties.

x. In the processing of Client's personal information, the following rules must be adhered to:

a. the individual has consented to the processing; or the processing is required by law; or
b. the processing is necessary for the legitimate interests and/or performance of the service contract; or

c. the processing is necessary to comply with any legal obligation; or
d. the processing is necessary for the purposes of a legitimate interests to meet any contractual obligations and requests of the client; or
e. the processing is necessary to protect/preserve the interests of the client.
f. the processing is required to comply with any obligation by a government authority.

xi. In the processing of employee's personal information, the following rules must be adhered to:

a. the individual has consented to the processing; or the processing is required by law; or
b. the processing is necessary for the legitimate interests and/or performance of the contract of employment; or
c. the processing is necessary to comply with any legal obligation; or
d. the processing is necessary to comply with any obligation with government bodies.

xii. Members of staff shall ensure the safety and confidentiality of information within his/her control and or custody by ensuring the following:

a. Files are kept in a locked secure file cabinet whenever they are not in use.
b. Documents/information being removed from a file shall be destroyed immediately.
c. Electronic files are to be secured by strong passwords, which shall not be shared with other team members
d. Personal data while in use should be secured to prevent view by third parties or other members of staff.
e. Personal Data for clients and other members of staff should not be stored on personal devices or sent via personal emails.
f. Personal Data for staff and clients should only be stored on approved/official servers which are secured.
g. Printed documents should be retrieved immediately to prevent them being viewed by third parties or other members of staff not authorized to access the personal data.
h. Computer screens should be locked whenever the member of staff is away from his/her desk and at the end of each day.
i. Ensure the security of personal data against loss by frequently backing using the approved procedures.
j. Ensure that personal data is encrypted prior to the transfer of the personal data.
k. Where personal data is stored on a removable media, these should be kept secured and locked away when not in use.
l. Prior to the disclosing of any personal data request and receive the approval of the Supervisor, Manager and or CEO.

2. Data Breach Report

2.1 Where a breach of personal data has occurred the member of staff reporting the breach must advise the Data Protection Officer of the following to facilitate the preparation of a Data Breach Report:

a. Details of the breach, including the date and time.
b. Date and time the breach was detected;
c. The type of Data involved and its sensitivity;
d. The number of individuals affected by the breach;
e. Whether the Data were encrypted.
f. Who identified the breach and how
g. How the personal data was being processed at the time of the breach

2.2 The Data Protection Officer shall prepare and submit a report within 48 hours of being notified of a breach to facilitate the Data Subject being advised. The report shall include the details of the breach as well as the security measures which were in place and how the breach was identified.

2.3 Pursuant to the Data Protection Act, all breaches must be reported to the Office of the Information Commissioner (OIC) within 72 hours of the identification of the breach. Any such report shall include:

a. the facts surrounding the security breach;

b. a description of the nature of the security breach, including the categories, number of data subjects concerned, and the type and number of personal data concerned;

c. the measures taken or proposed to be taken to mitigate or address the possible adverse effects of the breach;

d. the consequences of the breach; and

e. the name, address, and other relevant contact information of the Data Protection Officer.

3. Data Impact Assessment Report

3.1 Within three (3) months of the end of any registration period, the Data Protection Office shall prepare an Impact Assessment Report for submission to the OIC.

3.2. The Report shall include the following:

a. a detailed description of the envisaged processing of the personal data and the purposes of the processing, specifying, where applicable, the legitimate interest pursued by the data controller;

b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c. an assessment of the risks to the rights and freedoms, of data subjects; and

d. the measures envisaged addressing the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Act, taking into account the rights and legitimate interests of data subjects and other persons concerned.