Data Protection

Data Protection Policy

Table of Contents

1 OVERVIEW

1.1 Policy Statement

BIOSEC SOLUTIONS (hereinafter referred to as the "Company") needs to collect personal information to effectively carry out our everyday business activities and to provide the products and services defined by our business type. Such data is collected from employees, users, customers, suppliers and clients and includes (but is not limited to), name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information and bank/credit card details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations.

Where applicable, we are committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR), and any other relevant data protection law, company policies and guidelines (herein collectively referred to as "the data protection laws").

The Company has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities, and we operate a 'Privacy by Design' approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

1.2 Purpose

The purpose of this policy is to ensure that the Company meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individuals' best interest.

The data protection laws include provisions that promote accountability and governance and as such the Company has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimize the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

1.3 Applicability

This Privacy Notice is applicable, for all intent, purposes, rights and obligations, to the processing of personal data of data subjects that fall under the EU GDPR. However, data subjects and users of our services that are not covered by the GDPR may, directly or indirectly and without any legal right or claim, enjoy the benefits of the measures that we have put in place.

1.4 Scope

This policy applies to all staff within the Company (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in Nigeria or overseas). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

2 DEFINITIONS AND ABBREVIATIONS[1]

- "Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.
- "Binding Corporate Rules" means personal data protection policies which are adhered to by the Company for transfers of personal data to a controller or processor in one or more third countries or to an international organisation.
- "Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- "Cross Border Processing" means processing of personal data which: -
    - takes place in more than one Member State; or
    - which substantially affects or is likely to affect data subjects in more than one Member State
- "Data controller" means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- "Data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- Data Processing Agreement (or "DPA"): contract between the Controller and the Processor, containing all the mandatory information requested by the GDPR.
- "Data protection laws" means for the purposes of this document, the collective description of the GDPR; and any other relevant data protection law, company policies and guidelines.
- Data Protection Notice (or "Privacy Notice"): a document intended for the Data Subject containing the mandatory information requested by the GDPR.
- DPIA: Data Protection Impact Assessment;
- DPM: Data Protection Manager
- DPO: Data Protection Officer
- "Data subject" means a living natural person, who is the subject of personal data
- EEA: European Economic Area
- ERM: Enterprise Risk Management
- FDPIA: Full Data Protection Impact Assessment, as described by the GDPR
- "GDPR" means General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data.

[1] See also art. 4 "Definitions" of the GDPR.

- "Genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- IDPIA: Initiative-Based Data Protection Impact Assessment.
- "Personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- (Personal) Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed
- PII: Personal Identifiable Information (concept similar to Personal Data).
- Portability: right for a Data Subject to receive his/her Personal Data in a structured, commonly used and machine-readable format.
- Privacy Notice: see above "Data Protection Notice"
- Privacy Shield: Data Protection framework between the EU and the USA
- "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- Processor: natural or legal person processing data on behalf of a Controller;
- "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- RACI: Responsible, Accountable, Consulted, Informed;
- "Recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- Record of Processing: the record of processing activities, as described by the GDPR
- Special Categories of Personal data (or "Sensitive Data"): data revealing racial or ethnic origin, political opinions, religious of philosophical beliefs, trade union membership, genetic and biometric data, data concerning health or data concerning a person's sex life or sexual orientation.
- Sub-Processor: natural or legal person (sub-)processing Personal Data on behalf of a Processor
- "Supervisory Authority" means an independent public authority which is established by a Member State
- "Third Party" means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

3 Data Protection Law

The GDPR is applicable to all companies located in EU/EEA, doing business in Europe, or simply involved in the processing of personal data of data subjects residing in the EU/EEA.

Where applicable and as required by the Regulation on the processing of personal data of individuals resident in the EU/EEA, we comply with the requirements of the EU GDPR. For the sake of convenience, this policy only refers to the (article/Recital numbers of) the GDPR.

3.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) (EU)2016/679) was approved by the European Commission in April 2016 and applies to all EU Member States from 25th May 2018. As a 'Regulation' rather than a 'Directive', its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As the Company processes personal information regarding individuals (data subjects), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

All Biosec Solutions personnel who hold or process personal data must comply with the data protection principles and conditions for processing described in the GDPR and summarized on this policy document.

3.1.1 Personal Data

Information protected under the GDPR is known as “personal data” and is defined as: -

“Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

The Company ensures that a high level of care is afforded to personal data falling within the GDPR’s ‘special categories’ (previously sensitive personal data), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the ‘Special categories of Personal Data’ the GDPR advises that: -

“Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.”

3.1.2 The GDPR Principles

Article 5 of the GDPR requires that personal data shall be: -

a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’)

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

Article 5(2) requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles' ('accountability') and requires that firms show how they comply with the principles, detailing and summarizing the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

3.2 The Data Protection Authority (DPA)

The Data Protection Authority (DPA) is the independent regulatory office who reports directly to European Data Protection Board, EDPB, and whose role it is to uphold information rights in the public interest. They have oversight for the General Data Protection Regulation.

The DPA is empowered to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals, and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws, the DPA, has roles, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws.

The Company and its DPO are registered and appear on the Data Protection Register under the Belgian Data Protection Authority (Supervisory Authority) as a controller of personal information.

4 Data Protection Policy

4.1 Objectives

As required by the EU GDPR we are committed to ensuring that, where applicable, personal data are processed by the Company in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority. We ensure the safe, secure, ethical and transparent processing of personal data and have stringent measures to enable affected data subjects to exercise their rights.

The Company has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

With reference to the EU GDPR and affected data subjects, the Company ensures that: -

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws
- Business practice, function and process carried out by the Company, is monitored for compliance with the data protection laws and its principles
- Personal data is only processed where we have verified and meet the lawfulness of processing requirements
- We only process special category data in accordance with the GDPR requirements
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested
- Employees are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations and how they apply to their specific role and the Company
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection
- We have appointed an EU Representative / Data Protection Officer, who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR
- We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance

- We provide clear reporting lines and supervision with regards to data protection
- We store and destroy all personal information, in accordance with our retention policy and schedule which has been developed from the legal, regulatory and statutory requirements and suggested timeframes
- Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Employees are aware of their own rights under the data protection laws
- We maintain records of processing activities in accordance with the Article 30 requirements
- We have developed and documented appropriate technical and organisational measures and controls for personal data security and have a robust Information Security program in place

4.2 Governance Procedures

4.2.1 Accountability & Compliance

Due to the nature, scope, context and purposes of processing undertaken by the Company, we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures through our documentation and practices.

Our main governance objectives are to: -

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all employees
- Identify key stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the designated person(s) has sufficient access, support and budget to perform the role
- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that the Company in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated information security policies.

4.2.2 Privacy by Design

We operate a 'Privacy by Design' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. Whenever the Company creates a new process, product, service or any other product resulting in the processing of personal data, it shall integrate data protection in the design of the processing. We have developed controls and measures (detailed below), that help us enforce this ethos.

4.2.2.1 Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be 'limited to what is necessary', which forms the basis of our minimalist approach. We only obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

4.2.2.2 Pseudonymisation

We utilise pseudonymisation where possible to record and store personal data in a way that ensures it can no longer be attributed to a specific data subject without the use of separate, additional information (personal identifiers).

4.2.2.3 Encryption

We utilise encryption as a further risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

4.2.2.4 Restriction

Our *Privacy by Design* approach means that we use company-wide restriction methods for all personal data activities. Restricting access is built into the foundation of the Company's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information.

4.2.2.5 Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options. Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time we hold it.

Refer or request our Data Protection by Design by Default Policy & Procedures for further details.

4.2.3 Information Audit

To enable the Company to fully prepare for and comply with the data protection laws, we have carried out data protection information audit to better enable us to record, categorise and protect the personal data that we hold and process.

The audit has identified, categorised and recorded personal information obtained, processed and shared by our company in our capacity as a controller and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Disclosures and Transfers

Refer or request our Compliance & audit policy for further details**.**

4.2.4 Legal Basis for Processing (Lawfulness)

Where the EU GDPR applies, at the core of personal information processing activities undertaken by the Company, is the assurance and verification that we are complying with Article 6 of the regulation and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is, where applicable, provided to the data subject and Supervisory Authority as part of our information disclosure obligations. Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: **-**

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is 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 a legal obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).

4.2.5 Processing Special Category Data

Special categories of Personal Data are defined in the data protection laws as: -

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

Where the Company processes any personal information classed as special category or information relating to criminal convictions, we do so in accordance with Article 9 of the GDPR regulations.

We will process special category data where: -

- The data subject has given explicit consent to the processing of the personal
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim

- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1).

Refer or request our Retention Policy for further details.

4.2.6 Records of Processing Activities

As an organisation that processes special category data, the Company maintains records of all processing activities and maintains such records in writing, in a clear and easy to read format and readily available to the Supervisory Authority upon request.

We continually review and maintain all such activities to ensure that we will record such information as detailed in GDPR Article 30 where: -

1. Processing personal data could result in a risk to the rights and freedoms of individual
2. The processing is not occasional
3. We process special categories of data or criminal convictions and offences

Acting in the capacity as a controller, our internal records of the processing activities carried out under our responsibility, contain the following information: -

- Our full name and contact details and the name and contact details of our Data Protection Officer. Where applicable, we also record any joint controller and/or the controller's representative
- The purposes of the processing
- A description of the categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data has or will be disclosed (including any recipients in third countries or international organizations)
- Where applicable, transfers of personal data to a third country or an international organization (including the identification of that third country or international organization and where applicable, the documentation of suitable safeguards)
- Where possible, the envisaged time limits for erasure of the different categories of data
- A general description of the processing security measures as outlined in section 12 of this document (pursuant to Article 32(1) of the data protection laws)

4.2.6.1 Maintaining the Record of processing Activities, RoPA

The Company maintains our RoPA periodically or when a significant change has taken place in our processes, purposes or means of processing. The Company has designated the RoPA Owner, who has developed a process to monitor our processes and implement the necessary updates on the RoPA. The process includes but not limited to the following.

1. Determine whether an initiative create a new personal data processing
2. Determine whether the initiative introduce the processing of a new category of personal data
3. Determine whether the initiative introduce a new third party to the processing of personal data
4. Determine whether the initiative change the way personal data is processed in any way
5. Gather information about the processing
6. Define the categories of personal data processed
7. Define the categories of data subject concerned by the possessing
8. Implement the necessary changes, update the RoPA and document changes accordingly

4.2.7 Third-Party Processors

The Company utilise external processors for certain processing activities (where applicable). We identify, categorise and record all personal data that is processed outside of the company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. Such external processing includes (but is not limited to**): -**

- IT Systems and Services
- Legal Services
- Payroll
- Hosting or Email Servers
- Credit Reference Agencies

We have strict due diligence and Know Your Customer procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain company documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

We audit their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance.

The continued protection of data subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

We draft Service Level Agreements (SLAs) and contracts with each processor as per the services provided and have a dedicated Processor Agreement template that details: -

- The processors data protection obligations
- Our expectations, rights and obligations

- The processing duration, and aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

The Processor Agreement and any associated contract reflects the fact that the processor: -

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third country or an international organisation (unless required to do so by a law to which the processor is subject)
- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists the Company in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments
- When requested, deletes or returns all personal data to the Company after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to the Company all information necessary to demonstrate compliance with the obligations set out in the agreement and contract
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract
- Informs the Company immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

4.2.8 Data Retention & Disposal

The Company have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and prioritises the protection of the personal data in all instances.

Please refer or request our Data Retention & Erasure Policy for full details on our retention, storage, periods and destruction processes.

4.3 Data Protection Impact Assessments (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the Company. We therefore utilise several measures and tools to reduce

risks and breaches for general processing. However, where processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where the Company must or are considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we always carry out a Data Protection Impact Assessment (DPIA) (sometimes referred to as a Privacy Impact Assessment).

Pursuant to Article 35(3) and Recitals 84, 89-96, we consider processing that is likely to result in a high risk to include: -

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)
- Processing on a large scale of special categories of data
- Processing on a large scale of personal data relating to criminal convictions and offences
- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV)
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual
- Those involving the use of new technologies
- New processing activities not previously used
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects
- Processing activities making it difficult for the data subject(s) to exercise their rights

Carrying out DPIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: -

- Avoided
- Reduced
- Accepted

Please refer or request our DPIA Procedures for further details.

4.4 Data Subject Rights

4.4.1 Consent & The Right to be Informed

The collection of personal and special category data is fundamental to the performance of the business activities of the Company and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.

The data protection law defines consent as; 'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

Where processing is based on consent, the Company have reviewed and revised all consent mechanisms to ensure that only the necessary data for valid consent is collected and that the Company adhere to EU GDPR requirements.

Please, refer or request our Consent guidelines/Procedures document for details.

4.4.2 Personal Data Not Obtained from the Data Subject

Where the Company obtains and/or processes personal data that has not been obtained directly from the data subject, the Company ensures that the information disclosures contain in Article 14 are provided to the data subject within 30 days of our obtaining the personal data (except for advising if the personal data is a statutory or contractual requirement).

In addition to the information disclosures in section 8.1.4, where personal data has not been obtained directly from a data subject, we also provide them with information about: -

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources

Please refer or request our Consent Guidelines for further details

4.4.2.1 Employee Personal Data

As per the data protection law guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Staff Handbook and Employee Privacy Notice, which informs them of their rights under the data protection laws and how to exercise these rights and are provided with a Privacy Notice specific to the personal information we collect and process about them.

4.4.3 Privacy Notice

The Company defines a Privacy Notice as a document, form, webpage or pop-up that is provided to individuals at the time we collect their personal data (or at the earliest possibility where that data is obtained indirectly).

Our Privacy Notice provides individuals with the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

We have a link to our Privacy Notice on our website and provide a copy of physical and digital formats upon request. The notice is the customer facing policy that provides the legal information on how we handle, process and disclose personal information.

Our privacy Notice is drafted by the Data Protection Officer using the data protection laws requirements.

The notice is easily accessible, legible and is available in several formats, dependant on the method of data collection: -

- Via our website
- Linked to or written in full in the footer of emails

- Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face
- In employee contracts and recruitment materials
- Verbally via telephone or face-to-face
- Via SMS
- Printed media, adverts and financial promotions
- Digital Products/Services
- On Mobile Apps
- Automated phone service

Please refer or request our Privacy Notice for further details

Please refer or request our Employee Privacy Notice for further details.

4.4.4 The Right of Access

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 (collectively, The Rights of Data Subjects), in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity (i.e. verbally, electronic).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

Please refer or request our Data Subject Access Rights Policy and Procedures for detailed information.

4.5 Security & Breach Management

Alongside our 'Privacy be Design' approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. We provide detailed measures and controls to protect personal information and to ensure its security from consent to disposal. We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk. We carry out information audits to ensures that all personal data held and processed by us is accounted for and recorded, alongside DPIA assessments as to the scope and impact a data breach could have on data subject(s).

Whilst every effort and measure are taken to reduce the risk of data breaches, the Company has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and communication to the data subjects (where applicable).

Please refer to our Data Breach Policy & Procedures for specific protocols.

4.6 Transfers & Data Sharing

The Company takes proportionate and effective measures to protect personal data held and processed by us, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is subject to our data protection methods, including those described in our Privacy by Design and Default Guidelines.

We use approved, secure methods of transfer and have designated an EU Representative / Data Protection Officer, DPO as required by the GDPR. All data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible. The Data Protection Officer authorises all transfers and verifies the security methods and measures.

Please refer or request our Data Transfer Policy and Procedures for further details.

4.7 Audits & Monitoring

This policy and procedure document detail the extensive controls, measures and methods used by the Company to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct. In addition to these, we also carry out regular audits and compliance monitoring processes that are detailed in our Compliance Monitoring & Audit Policy & Procedure, with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The Data Protection Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimisation methods are frequently reviewed, and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Data Protection Officer and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to: -

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- Ensure that implemented data processing processes, registers and records are maintained and updated
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance

- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data
- To monitor compliance with the data protection laws and demonstrate best practice

Please refer or request our Compliance Policy & Audit Monitoring for further details.

4.8 Training

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. Our Training & Development Policy & Procedures Policy detail how new and existing employees are trained, assessed and supported and include: -

- GDPR awareness, Training and Assessment Tools
- Coaching & Mentoring
- 1:1 Support Sessions
- Access to GDPR policies, procedures, checklists and supporting documents

Employees are continually supported and trained in the data protection laws requirements and out own objectives and obligations around data protection.

Please refer or request our Training & Development policy for further details.

4.9 Penalties

The Company understands its obligations and responsibilities under the data protection laws and recognises the severity of breaching any part of the law or Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. We recognise that: -

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations (Chapter IX) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

4.10 Responsibilities

The Company has appointed an EU Representative / Data Protection Officer, whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPO will work in conjunction with the Compliance Officer, IT Manager and Training Officer to ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.

The DPO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.