DATA PROTECTION POLICY

(hereinafter referred to as ***"the Policy")***

of

BIOSYN
(REGISTRATION NUMBER: 2021/657597/07)
(hereinafter referred to as ***"the Company'***)

LEGISLATIVE BACKGROUND

The Republic of South Africa has made tremendous efforts to implement laws and regulations relating to the protection of personal information and data. The right to privacy is protected by South Africa's Constitution. Additionally, the Electronic Communications and Transactions Act, Act 25 of 2002 (hereinafter referred to as **"ECTA"**) contains a number of regulations that control the electronic acquisition of personal data, however compliance is optional. These provisions of the ECTA pertaining to the protection of personal information were repealed on 30 June 2021.

The Protection of Personal Information Act, Act 14 of 2013 (hereinafter referred to as ***"POPIA")*** was promulgated into law on November 26, 2013. On **1 July 2021** all sections of POPIA were completely operative, with the exception of Section 58. The implementation of Section 58, however, was delayed until 1 February 2022. The scope of the POPIA's application is broad, and it affects everyone in the country who processes personal data and information.

The Consumer Protection Act, Act 68 of 2008 (hereinafter referred to as the **"CPA"),** which was passed in 2011, covers telephone-based direct marketing of both goods and services to consumers, must also be taken into account when analyzing data privacy. Although it may appear that the CPA's restrictions on direct marketing and unsolicited communications overlap with those of POPIA, POPIA only applies in the case of unsolicited electronic communications.

The POPIA sets out the standards regarding accessing and processing of any personal information belonging to any individual or entity (hereinafter referred to as **"data subject").** According to POPIA, "processing" includes gathering, receiving, logging, organizing, retrieving, using, disclosing, or distributing any personal information about a data subject.

The POPIA's purpose is to implement the constitutional right to privacy while weighing that right against conflicting rights and interests to information access.

ISO (the International Organization for Standardization) and **IEC** (the International Electrotechnical Commission) forms the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001 or as a guidance document for organizations implementing commonly accepted information security controls.

The standard ISO/IEC 27002:2013 information technology - security techniques - code of practice for information security controls, has been revised under **ISO/IEC 27002:2022** Information security, cybersecurity and privacy protection - information security controls edition.

ISO/IEC 27002:2022 is a guidance document and is designed to be used as a reference for selecting controls while implementing an Information Security Management System (ISMS) based on ISO/IEC 27001 or as a guidebook for organizations implementing commonly accepted information security controls

South Africa recognizes the international standard under SA National Standards as published in the Government Gazette under the Standards Act, Act 29 of 1993.

The General Data Protection Regulation (hereinafter referred to as **"GDPR"**) is one of the most wide-ranging pieces of legislation passed by the EU. The GDPR was designed to protect personal data linked to individuals. The GDPR applies to controllers or processors established in the EU, regardless of whether the processing takes place in the EU or not. GDPR applies to any entity (any person, business, or organization) that collects or processes personal data from any person in the European Union.

OVERVIEW

The development and advancement of sophisticated control and security systems is a result of the increased and stricter requirements for security measures in the business environment. These systems increasingly rely on biometric data, like fingerprinting, voice recognition, retinal scanning, etc., distinctively identifying an individual permitting entry into and exit from a physical location, program, system, or network. Employee biometric information must be obtained in order for an employer to apply such control measures, which raises the issue of whether employees can be coerced into providing biometric information.

POPIA gives specific guidelines on how to handle biometric data. According to POPIA, it is generally prohibited to collect an employee's personal information unless the processing is authorised by law or is done with the employee's consent. The employer must be sure and put procedures in place to ensure that no unauthorised access to the biometric information occurs, and they may only use the biometric information for the exact purpose for which consent was given.

The employment contract may contain a provision for consent for the processing of biometric information. The explanation of the justifications for obtaining and processing such biometric data, as well as the repercussions for the employee should no consent be given, should follow along with the request for consent. Employees may object to the use of such biometric data and employer must make clear the repercussions of such actions. Depending on the employer's security requirements, these repercussions could range from additional security measures being used to confirm an employee's identity to the employee not being granted access to the premises or systems, and consequently being unable to provide his services effectively. This could result in termination for performance failure. When biometric access and security measures are necessary for a job's performance, it's crucial to let prospective employees know before hiring them that providing their biometric data is a requirement for employment and that, should they refuse to provide it or give it permission to be used, their employment contract may be terminated as a direct result.

THE AIM

The core purpose of this policy is to create effective and visible guidelines to ensure that the Company complies with all applicable local and international legislation and good practices during the processing of personal information belonging to any data subject.

This Policy regulates the processing of personal information and sets forth the requirements with which the Company undertakes to comply when processing personal information pursuant to undertaking its operations and fulfilling its contractual obligations in respect of client, data subjects and third parties.

The Company places a high value on the privacy of every person and entity with whom is interacts or engages and therefore acknowledges the need to ensure that personal information is handled with reasonable standard of care as may be expected from the Company. The Company is committed to ensuring that it complies with the requirements of POPIA, and also with the terms of the GDPR to the extent that is applies.

This Policy aims not only to inform data subjects about how the Company processes personal information, but also to establish a standard by which the Company and its employees and representatives shall comply in as far as processing personal information is concerned.

THE PROTECTION OF PERSONAL INFORMATION

1 TERMS AND DEFINITIONS

'the Company' means Biosyn;
'biometrics' means a technique of personal identification that is based on physical, physiological or behavioral characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
'client' means any natural person or entity that the Company renders services to in terms of a contractual agreement;
'consent' means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
'Constitution' means the Constitution of the Republic of South Africa, 1996;
'data subject' means the person to whom personal information relates;
'data processing laws' means the Protection of Personal Information Act; The Consumer Protection Act; Electronic Communications and Transactions Act; Promotion of Access to Information Act; Standards Act; Data Protection Act of Botswana; Guidelines per the SA National Standards (ISO/SANS 27002:2014); ISO/IEC27002:2022 Information security, cybersecurity and privacy protection - information security controls edition;
'data protection officer' means a person appointed as the main representative on data protection matters in terms of POPIA;
'electronic communication' means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;
'employee' means all permanent -, temporary-, fixed term- and casual employees, Directors, Shareholders, authorised third party representatives and agents acting for or on behalf of the Company;
'in writing' means written, printed, lithographed, telefaxed, via e-mail or represented by any other substitute for writing, whether hard copy or electronic or otherwise;
'operator' means a person who processes personal information for a responsible party in terms of a contract or mandate;
'person' means a natural person or a juristic person;

'personal information' means information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including, but not limited to –

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

'POPIA' means the Protection of Personal Information Act, Act 14 of 2013;

'processor' means a person who processes personal information for a responsible party in terms of a contract or mandate;

'processing' means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

'public record' means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

'record' means any recorder information –

(a) regardless of the form or medium, including any of the following:

(i) writing on any material;

(ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorder or stored;

(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing;

(v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

(b) in the possession or under the control of a responsible party;

(c) whether or not it was created by a responsible party; and

(d) regardless of when it came into existence;

'Regulator' means the Information Regulator established in terms of Section 39 of the POPIA;

'Republic' means the Republic of South Africa;

'responsible party' means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

'special personal information' means all information relating to a person's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information or criminal behavior.
'**Ubiquitous'** means something exists in many places simultaneously at the same time.

2 APPLICATION OF THE POLICY

2.1 The Policy applies to any and all of the following persons:

2.1.1 Employees of the Company; including permanent-, temporary-, fixed term- and casual employees.
2.1.2 Directors and shareholders;
2.1.3 Authorised operators, third party representatives and agents acting for or on behalf of the Company.

2.2 Every employee involved in processing personal information for or on behalf of the Company must read, understand and comply with the Policy at all times in the course of performing any task in the scope of their duties.

2.3 The Company shall provide adequate resources, systems and processes in the workplace for all employees, including regular internal training, to ensure that all employees understand all procedures, protocols, duties and obligations under the Policy and all relevant data processing laws.

2.4 Compliance with the Policy is mandatory and any breach shall result in disciplinary action.

3 OBLIGATIONS AND RESPONSIBILITIES

The Company must ensure that –

3.1 Only personal identifiable information that is necessary for a clear, explicit, and legal purpose is processed.
3.2 All personal data processing is carried out in a legal, ethical, and transparent manner.
3.3 All personal data is accurately processed and periodically updated.
3.4 Any processing of personal information is adequate, pertinent, and restricted to what is required.
3.4 Any personal identifiable information that it processes is not maintained in a way that makes it possible to identify data subjects for any longer than is required to fulfill the relevant purposes.
3.5 It takes the necessary technological and organizational precautions to safeguard the security of the personal data it processes, protect it from unauthorized or unlawful processing, and prevent accidental loss, destruction, or damage.
3.6 Data subjects are able to exercise their legal rights in connection to their personal data, and the Company must permit this.

4 CONSENT

4.1 The Company must always have a legitimate basis and purpose in order to acquire and process personal information for any particular purpose.

4.2 It is not always necessary to obtain consent to process a data subject's personal information. Under the following conditions, the Company will be permitted by the data processing regulations to legitimately handle a data subject's personal information without the data subject's consent:

4.2.1 The processing is required for the execution of a contract to which the data subject is a party;
4.2.2 The Company needs to process the data in order to fulfill certain legal requirements;
4.2.3 The processing is done to safeguard the subject's legitimate or vital interests, the interests of the Company or third party, or both.
4.2.4 The processing is necessary to carry out tasks in the public interest, carry out official duties, or exercise official authority.

4.3 If the processing of a data subject's personal information is necessary for reasons not listed above, then the data subject must agree to the processing by way of consent to the processing of its personal data to ensure that such processing is legal. The data subject must be aware of the personal information that will be processed, the method in which the information will be obtained and stored, and the reason for the personal information.

4.4 The consent by the data subject must be freely given, without conditions.

4.5 When a data subject's consent is necessary to process their personal information, they have the right to revoke that consent at any time. It will be important to inform the data subject of the consequences of the revocation, i.e. that the Company will not be able to continue its relationship with the data subject. If consent is revoked, the Company will no longer be permitted to continue processing such personal information from the date of such revocation. It is required that the revocation by the data subject be in writing.

4.6 The data processing laws makes a distinction between special personal information (usually referred to as sensitive personal data) and personal information. The data subject's race, ethnicity, political affiliation, religious or philosophical beliefs, union membership, genetics, biometrics, health, sex life, or sexual orientation are considered special personal information.

4.6.1 In terms of the POPIA, in order to process special personal information, it is required by the Company to justify the processing by proving that:

4.6.1.1 the data subject has given consent for the processing of the special personal information in writing;
4.6.1.2 the processing is essential for the creation, exercise, or defense of a legal right or obligation;
4.6.1.3 the processing is required to fulfill a legal duty under international public law;
4.6.1.4 the data subject knowingly made the information public by means of publication of the information on any social platform or in any other manner;
4.6.1.5 when processing is done based on race or ethnicity and is done in order to identify data subjects and only when doing so is necessary for that purpose; to comply with legislation intended to protect or advance individuals or groups of individuals, who have been previously disadvantaged by unfair discrimination;
4.6.1.6 the Regulator has granted authorisation to process specific special personal information, if doing so is in public interest.

4.6.2 Under the GDPR, one of the following conditions must be met before any data or information is processed:

4.6.2.1 the data subject consented to the processing;
4.6.2.2 processing is a necessity for the purpose of carrying out the obligation and exercising specific rights of the Company or of the data subject in the field of employment, social security and social protection law;
4.6.2.3 processing is a necessity to protect the legitimate interest of the data subject or of another natural person where the data subject is physically incapable of giving consent;
4.6.2.4 the Company is an organization with a political, philosophical, religious, or trade union goal, and the processing is done in the course of its legitimate business operations, provided that the processing only pertains to current or former members of the organization, or to people who regularly interact with it in connection with its objectives, and that the personal data is not disclosed outside the organization without the subjects' consent;
4.6.2.5 the processing relates to personal information which is clearly made public by the data subject;
4.6.2.6 the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
4.6.2.7 the processing is required for legitimate purposes of the public interest, in accordance with legal standards that respect the core principles of data protection and provide for appropriate and targeted safeguards for the data subject's fundamental rights and interests;
4.6.2.8 the processing is required for preventative or occupational medicine, for the evaluation of an employee's working capacity, for medical diagnosis, for the provision of health or social care or treatment, or for the management of health or social care systems or services in accordance with the law or in accordance with a contract with a health professional, provided that the Company takes appropriate and specific measures to protect the fundamental rights and interests of the data subjects;
4.6.2.9 the processing is necessary for public interest reasons in the area of public health, such as protecting against serious cross-border health threats or ensuring high standards of quality and safety of healthcare, medicines, or medical devices, on the basis of law that provides for suitable and specific measures to safeguard the rights of the data subject.

4.7 It is the responsibility of the client to obtain consent from the data subject prior to processing any personal data and information to the Company. The client shall keep the consent on record and can be requested by the Company’s Data Processing Officer for assessment and validity.

5 MINIMISATION

The personal information that every operator processes on the Company's behalf must be sufficient, pertinent, and kept to a minimum given the purposes for which it is to be used. Any operator is only permitted to handle personal data that is strictly essential for carrying out the specified purpose and any associated obligations and tasks, and not for any other uses. A person shall face disciplinary action for accessing excessive amounts of personal information that is unnecessary, to which they are not authorized, or to which they have no legitimate reason to have access. In some cases, this behavior may also be illegal and result in civil or criminal liability or administrative fines.

6 STORAGE OF DATA

In order to mitigate any risks, storing personal data for a longer period of time may make data breaches more serious and increase the costs associated with such storage. When the purpose for which it was gathered has passed, the Company will continue to follow its policies and procedures to make sure that personal data is deleted or destroyed after a reasonable amount of time.

7 DATA SHARING

Any operator handling personal data on the company's behalf are not allowed to share the data to outside parties unless:

7.1 consent have been obtained by the data subject;

7.2 the data subject has been informed in advance by way of notice that the personal information will be shared with another; and

7.3 prior to receiving the personal information, the individual or entity receiving it, if acting as an operator or processor has otherwise agreed to keep the personal information confidential and to use it only for the purpose for which it was shared under a data transfer agreement.

8 DATA TRANSFERS OUTSIDE OF SOUTH AFRICA OR THE EUROPEAN ECONOMIC AREA (EEA)

The laws governing data processing forbid the transfer of personal data outside of South Africa, the UK, and/or territories in the EEA, including the transmission, sending, viewing, or accessing of personal data within or to another country, unless:

8.1 the data subject consents to such processing; or

8.2 the jurisdiction receiving the personal information offers the same degree of protection for the data subject(s) as is mandated by South Africa's, the UK's, and/or EEA-affiliated territories' data processing regulations.

9 RIGHTS OF THE DATA SUBJECT

9.1 The laws governing data processing give data subjects a range of rights over their personal information, including the ability to access and modify that information. The Company has implemented certain processes to give effect to the rights of a data subject, and all enquiries will be dealt with directly to the relevant Company’s Data Processing Officer of the client, and no other person.

9.1.1 REVOCATION

When providing consent for the processing of personal information, a data subject has the right to revoke that consent at any time. The revocation will only be effective as of the date it is made, and it will not affect the legality of the processing of the data subject's personal information to which the consent applied prior to the revocation.

9.1.2 RIGHT TO BE INFORMED

A data subject has the right to know why their personal information is being processed, as well as what kind of personal information will be processed, the reason for the processing, who will receive their personal information and whether it will be sent outside of the country in which it is being processed or stored. The client is responsible to ensure that a data subject is fully informed.

9.1.3 AMENDMENT OF DATA

Every data subject has the right to request that outdated, incorrect, or incomplete personal information be updated or corrected. The client's Data Protection Officer must provide in writing all amendment requests.

9.1.4 DELETION OF DATA

In the following situations, a data subject has the right to request that the Company delete the personal information that it has collected about them:

9.1.4.1 it is no longer necessary for the company to keep that personal information with regard to the purpose(s) for which it was originally collected or processed;

9.1.4.2 the data subject wishes to revoke their consent;

9.1.4.3 the data subject objects to the Company's holding and processing of their personal data, and there is no overriding legitimate purpose to permit the Company to continue doing so;

9.1.4.4 the personal data has been handled unlawfully; or

9.1.4.5 the Company must remove personal data in order to adhere to a specific legal requirement.

All requests for deletion must be dealt with, and the data subject must be informed of the deletion, within one month of receipt of the request. In the case of complicated requests, the time frame may be extended by up to two months. The data subject must be informed if more time is needed. The client's Data Protection Officer must provide in writing all deletion requests.

9.1.5 PERSONAL INFORMATION BREACH

A data subject must be informed when a personal information security breach affects their personal data. The Company will inform the Data Protection Officer of the Client that will be responsible to delay the notice to the effected data subject.

9.1.6 RIGHT TO OBJECT

9.1.6.1 A data subject has the right to file a complaint or an objection over the processing of their personal data, provided that the complaint or objection outlines and addresses the Company's violation of the data processing laws or regulations. The client's Data Protection Officer must provide in writing all complaints or objections.

9.1.6.2 Upon receipt of a complaint or objection is received, the Client Company's Data Processing Officer will make an effort to hear the issue out and find a solution; if that fails, they will escalate the complaint or objection to the Company.

9.1.6.3 The Company will access the complaint or objection and provide a report to the Data Processing Officer of the Client.

9.1.6.4 In the event that the parties are unable to resolve the matter, the data subject will have the right to refer the complaint to the appropriate supervisory authority, such as the Information Regulator in the case of an alleged POPIA violation or infringement or the Information Commissions Officer in the case of an alleged GDPR violation or infringement.

10 DATA PROTECTION OFFICER

The Company must appoint a suitable Data Protection Officer by way of written appointment by the Directors of the Company. The Data Protection Officer has the authority to appoint and delegate specific tasks to Deputy Data Protection Officer.

The Data Protection Officer of the company will be responsible for the following:

10.1 developing, implementing and overseeing a Company-wide personal information processing framework, various personal information processing policies and procedures, including this Policy;
10.2 ensuring compliance with this Policy, the various personal information processing policies, and the applicable data processing laws;
10.3 arranging and implementing data protection training for all directors, employees, operators and processors who process personal information on the Company's behalf;
10.4 providing ongoing guidance and advice on the processing of personal information;
10.5 ensuring the implementation and compliance with all operational and technological data protection standards;
10.6 be authorized to initiate disciplinary proceedings against any employee who violates any technological and/or organizational and/or operational data protection standard, rule, custom, instruction, policy, practice, and/or protocol (verbal, in writing, or otherwise) applicable in any department or area of the Company's operations;
10.7 examining and approving any contracts or agreements with third parties that may handle or process data subject information;
10.8 Attend to data subjects' requests and queries about their respective data subject rights, including requests for access to their personal data or information;
10.9 coordinating with and/or cooperating with any regulators, investigators, or officials who may be looking into a data privacy issue;
10.10 Report any breach to the Company and advise on the process and responsibilities of the Company.

11 IT MANAGER

The Company shall appoint a suitable IT Manager that will be responsible for the following:

11.1 carrying out cyber security risk assessments, including baseline risk assessments for all of the Company's information activities;
11.2 ensuring the implementation of adequate and effective IT operational and technological data protection procedures and standards in order to address all IT security risks;

11.3 ensuring that all systems, services, and equipment used for data processing and/or storage adhere to internationally acceptable security and data safeguarding standards and are regularly updated to remain compliant with such standards;

11.4 issuing appropriate, clear, and regular rules and directives, whether for the Company as a whole or a specific part thereof, department, person, or level of persons in relation to any aspect of the Company's work, including password protocols, data access protocols, access to certain data sign-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications, and equipment that will or may be used under any circumstances;

11.5 evaluating any third-party services that the Company is considering or may acquire to process or store data, such as cloud computing services, and ensuring that appropriate and effective operational and technological data protection procedures and standards are in place to address all IT security risks that these external service providers may present.

12 EXTERNAL SERVICE PROVIDER

The Company will utilize the professional services of a secure offsite cloud based hosting company known as Absolute Hosting. Absolute Hosting owns and hosts its infrastructure and services from Tier 4 Data Centers within Samrand, South Africa. Absolute Hosting is compliant in terms of POPIA, GDPR and relevant data protection laws and provides a high standard of Cyber Security.

When necessary, to achieve the purposes for which the personal information was originally collected and processed, the Company may disclose personal information to Absolute Hosting. The Company will enter into a written agreement with Absolute Hosting to ensure that they comply with the applicable data protection laws in connection with the processing of personal information provided to them from time to time by the Company. The Company will retain personal information it has processed, in an electronic or hardcopy format on its own accord and will only be transferred to Absolute Hosting, in their capacity as external service provider to the Company and they will not have access to the personal information stored.

13 SECURING PERSONAL INFORMATION

The Company has implemented appropriate, reasonable physical, organizational, contractual, and technological security measures to protect the integrity and confidentiality of personal information, including safeguards against loss or theft, unauthorised access, disclosure, copying, use, or modification of personal information in accordance with applicable data protection laws.

In addition, in accordance with applicable data protection laws, the Company will take steps to notify the relevant Regulator(s) and/or any affected data subjects in the event of a security breach, and will do so as soon as reasonably possible after becoming aware of any such breach.

Regardless of any other provisions of this Policy, it should be noted that the transmission of personal information, whether in person, via the internet, or any other digital data transferring technology, is not completely secure. Although the Company will take all appropriate, reasonable measures to safeguard the integrity and confidentiality of the personal information it processes, the Company makes no guarantees that its security system is completely secure or error free.

Therefore, the Company cannot guarantee the security or accuracy of the information (whether it be personal information or not) which it collects from any data subject.

14 INDEMNITY

The Client shall indemnify, defend, and hold harmless the Company against any liability, damage, loss, or expense (including reasonable attorney's fees and expenses of litigation) incurred by or imposed upon any of the Company's indemnitees in connection with any third party claims, suits, actions, demands or judgments under any theory of liability (including without limitation actions in the form of tort, warranty, or strict liability) resulting from or arising out of the practice or use of any of the Company's technology or joint technology (or any part thereof) by the Client, its affiliates or any of their sub licensees, or concerning any product, process, or service that is made, used, or sold pursuant to any right or license granted by the Company to the Client under any contractual agreement, other than in the event of a claim resulting from or arising out of a breach of the representations and warranties by the Company under any contractual agreement by the Company or any fraud or intentional misconduct by any of the Company's indemnitees.

15 NON-COMPLIANCE

Any transgression of the Policy shall be investigated and may result in disciplinary action against the relevant offender.

16 CONTACTS

All comments, questions, concerns and complaints regarding personal information or this Policy should be sent via email to the Data Protection Officer.

DATA PROTECTION OFFICER	
ADDRESS	
TELEPHONE NUMBER	
EMAIL	