Privacy Policy

1. Purpose

1.1 This Policy defines requirements to ensure compliance with laws and regulations applicable to GPEX (the "Company") collection, use, processing, and transfer of Personal Data.

2. Scope

2.1 GPEX is committed to complying with the applicable Data Privacy and Protection requirements in the countries in which it operates.

2.2 This policy is based upon the UK Data Protection Act 1998 and the General Data Protection Regulation (GDPR) which operates within EU Regulation 2016/679, which provide a robust generic model for global Data Protection and privacy compliance.

2.3 This Policy applies to all Company full and part time employees, agency employees, and all suppliers and clients who receive Personal Data from the Company, have access to Personal Data collected or processed by the Company, or who provide information to the Company, regardless of geographic location.

2.4 As a policy commitment, the Company will not process Personal Data without notification to the Data Protection authorities in jurisdictions which require such notification. To ensure compliance with the regulations the Company will correctly establish its status for all Data Processing as either a Data Controller, or Data Processor acting for another Data Controller.

3. Compliance

3.1 The Company's data compliance program will be overseen by the GDPR Team.

3.2 The GDPR Team will implement the company's Data Protection procedures as well as any duties required by applicable law, including:

3.2.1 Determining whether notification to one or more Data Protection authorities is required as a result of the Company's Data Processing activities, then making any required notifications, and keeping such notifications current.

3.2.2 Designing and implementing ongoing programs for training employees in Data Protection rules and procedures.

3.2.3 Establishing procedures and standard contractual provisions for obtaining compliance with this Policy by clients, suppliers, and third parties who receive Personal Data from the Company, have access to Personal Data collected or processed by the Company, or who provide information to the Company, regardless of geographic location.

3.2.4 Establishing mechanisms for periodic audits of compliance with this Policy, implementing procedures, and applicable law.

3.2.5 Establishing, maintaining, and operating a system for prompt and appropriate responses to Data Subject requests.

3.2.6 Establishing, maintaining, and operating a system for the prompt and appropriate automatic disclosure to the relevant authorities and Data Subjects of any loss of Personal Data.

3.2.7 Informing senior managers, officers, and directors of the Company of the potential corporate and Personal civil and criminal penalties which may be assessed against the Company and/or its employees for violation of applicable Data Protection laws.

3.2.8 Ensuring that the risk management plans in relation to Data Protection are implemented effectively and promptly.

3.2.9 Ensuring that adequate assurance regarding the effectiveness of Data Protection procedures and audits is provided to the Board and management.

4. Data Protection Principles

4.1 The Company has adopted the following principles to govern its use, collection, and transmittal of Personal Data, except as specifically provided by this Policy or as required by applicable laws:

4.1.1 Personal Data shall only be processed fairly and lawfully.

4.1.2 Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes.

4.1.3 Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed.

4.1.4 Personal Data shall not be collected or processed unless one or more of the following apply:

4.1.4.1 The Data Subject has provided Consent (See definition of Consent in Appendix A);

4.1.4.2 Processing is necessary for the performance of a contract directly with the Data Subject, or to which the Data Subject is an employee of a party;

4.1.4.3 Processing is necessary for compliance with a Company legal obligation;

4.1.4.4 Processing is necessary in order to protect the vital interests of the Data Subject;

4.1.4.5 Processing is necessary for legitimate interests of the Company or by the third party or parties to whom the Data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject.

4.2 Appropriate physical, technical, and procedural measures shall be taken to:

4.2.1 Prevent and/or to identify unauthorised or unlawful collection, Processing, and transmittal of Personal Data; and

4.2.2 Prevent accidental loss or destruction of, or damage to, Personal Data.

5. Transfers to Third Parties

5.1 Personal Data shall not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to establish and maintain the required level of Data Security.

5.2 Personal Data may be communicated to third persons only for reasons consistent with the purposes for which the Data were originally collected or other purposes authorised by law.

5.3 All transfers of Personal Data to third parties for further Processing shall be Subject to written agreements.

5.4 EU Personal Data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless the transfer is made to a country or territory recognised by the EU as having an adequate level of Data Security.

5.5 Subject to the provisions of the above, Personal Data may be transferred where any of the following apply:

5.5.1 The Data Subject has given Consent to the proposed transfer;

5.5.2 The transfer is necessary for the performance of a contract between the Data Subject (Personally or via his employing company) and the Company;

5.5.3 The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Company and a Third Party;

5.5.4 The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defence of legal claims;

5.5.5 The transfer is required by law;

5.5.6 The transfer is necessary in order to protect the vital interests of the Data Subject.

6. Prevention of Non-Complying IT Systems

6.1 The Company's GDPR Team shall establish a procedure for assessing the impact of any new or existing Technology on the privacy and security of Personal Data.

6.2 No new system or new version of an existing system shall be made available for use until the GDPR team has confirmed there would be no breach of any Data Protection of other legal requirement or regulation.

7. Sources of Personal Data

7.1 Personal Data shall be collected only from the Data Subject unless the nature of the business purpose necessitates collection of the Data from other persons or bodies.

7.2 If Personal Data are collected from someone other than the Data Subject, the Company must have confirmation, in writing, from the supplier of the Data that the Data Subject has provided Consent to the transfer to the Company.

8. Data Subject Rights

8.1 Data Subjects shall be entitled to obtain the information about their own Personal Data upon a request made in writing to the Company who will establish a system for logging each request under this Section as it is received and noting the response date.

8.2 The Company shall provide its response to a request above within a month from the date of the written request, provided the request is not extremely complex in nature.

8.3 Data Subjects shall have the right to require the Company to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

8.4 The Company may establish reasonable fees to cover the cost of responding to requests that are manifestly unfounded, or excessive, or repetitive.

9. Sensitive Data

9.1 Sensitive Personal Data should not be processed unless:

9.1.1 Such Processing is specifically authorised or required by law.

9.1.2 The Data Subject expressly and unambiguously Consents.

9.1.3 Where the Data Subject is physically or legally incapable of giving Consent, but the Processing is necessary to protect a vital interest of the Data Subject. This exemption may apply, for example, where emergency medical care is needed.

9.1.4 Data relating to criminal offenses may be processed only by or under the control of the Admin Department.

10. Data Quality Assurance

10.1 Personal Data must be kept only for the period necessary for permitted uses. The Company has established local Record Retention Policies which determine applicable timescales for Data deletion.

10.2 Personal Data shall be erased if their storage violates any Data Protection rules or if knowledge of the Data is no longer required by the Company, or at the request of the Data Subject.

11. Third Party Processors

11.1 Where the Company relies on third parties to assist in its Processing activities, the Company will choose a Data Processor who provides sufficient security measures and take reasonable steps to ensure compliance with those.

12. Written Contracts for Third Party Processors

12.1 The Company shall enter into a written contract with each Data Processor requiring it to comply with Data privacy and security requirements imposed on the Company under local legislation.

13. Audits of Third Party Data Processors

13.1 As part of the Company's internal Data auditing process, the Company shall conduct periodic checks on processing by third party Data Processors, and in particular relating to the hand-off procedures for the Data especially in respect of security measures.

14. Notice to Directors, Managers, and Officers of Potential Sanctions for Non-Compliance

14.1 The GDPR Team shall notify directors, managers, and other officers of the Company that:

14.1.1 Failure to comply with relevant Data Protection legislation may trigger criminal and civil liability, including fines, imprisonment, and damage awards; and

14.1.2 They can be personally liable where an offence is committed by the Company with their Consent or connivance, or is attributable to any neglect on their part.

5. Data Security

15.1 The Company has a Data Security Management policy, under which it shall adopt physical, technical, and organisational measures to ensure the security of Personal Data, including the prevention of their alteration, loss, damage, unauthorised Processing or access, having regard to the nature of the Data, and the risks to which they are exposed by virtue of human action or the physical or natural environment. These measures will be documented within the Data Security Policy, which will be reviewed at least annually, or when necessary to reflect significant changes to security arrangements.

15.2 Adequate security measures should include all of the following:

15.2.1 Prevention of unauthorised persons from gaining access to Data Processing systems in which Personal Data are processed.

15.2.2 Preventing persons entitled to use a Data Processing system from accessing Data beyond their needs and authorisations.

15.2.3 Ensuring that Personal Data in the course of electronic transmission during transport or during storage on a Data carrier cannot be read, copied, modified or removed without authorisation.

15.2.4 Ensuring that Personal Data are protected against undesired destruction or loss.

15.2.5 Ensuring that Data collected for different purposes can and will be processed separately.

15.2.6 Ensuring that Data are not kept longer than stipulated in the Data Retention Policy, including by requiring that Data transferred to third persons be returned or destroyed.

16. Compliance Measurement

16.1 The GDPR Team shall establish a schedule for and implement a Data Protection compliance audit. The GDPR Team, shall devise a plan and schedule for correcting any identified deficiencies within a fixed, reasonable time.

16.2 The Company shall review annually its Data collection, Processing, and Security practices and shall determine what Personal Data The Company is collecting including that held in manual systems that constitute "Relevant Filing Systems"

16.3 The information collected in this annual review shall be delivered to the GDPR Team for review and appropriate action including, without limitation, the following:

16.3.1 Making recommendations for improvement to policies and procedures in order to improve compliance with this Policy and applicable law.

16.3.2 Satisfying the requirements for self-certifying compliance within local Data Protection Authorities.

17. Implementation

17.1 This Policy shall be available to employees on the company noticeboard, and shall be made available to others via the Company's website.

17.2 The GDPR Team, will develop a timeline and program for implementing this Policy.

17.3 This Policy may be revised at any time but at least annually by the GDPR Team. Notice of significant revisions shall be provided to employees via the noticeboard and to others via the Company's website.

Appendix A

Glossary

Consent: Consent means "any freely given specific and informed indication of his wishes by which the Data Subject signifies agreement to Personal Data relating to him being processed."

Nevertheless, Consent may be obtained by a number of methods. These may include clauses in employment contracts, check boxes on replies to application or purchase forms, and click boxes on online forms where Personal Data are entered.

In most European Union countries, Consent to the Processing of Sensitive Personal Data needs to be clear and unequivocal. This generally means that some form of specific, active Consent) is required.

Data: Data (whether or not having an initial capital letter) as used in this Policy shall mean information which either:

- is being processed by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should be processed by means of such equipment;
- is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System;
- does not fall within any of the above, but forms part of a readily accessible record covering an individual.

Data therefore includes any digital Data by computer or automated equipment, telephone recordings, and any manual information which is part of a Relevant Filing System.

Data Controller: Data Controller means a person who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed.

Data Processor: Data Processor means any person, other than an employee of the Data Controller, who processes the Data on behalf of the Data Controller. A company may be a Data Processor if defined as such under contractual terms with the Data Controller.

Data Subject: Data Subject means the person to which Data refers. Data Subjects include customers and web users, individuals on contact /e-mailing lists or marketing Databases, employees, contractors and suppliers.

Personal Data: Personal Data means Data related to a living individual who can be identified from those Data or from those Data and other information in the possession of, or likely to come into the possession of, a Data Controller or Data Processor. Personal data does not include information that has been anonymized, encoded or otherwise stripped of its identifiers, or information that is publicly available, unless combined with other non-public personal information.

Processing: Processing covers a wide variety of operations relating to Data, including obtaining, recording or holding the Data or carrying out any operation or set of operations on the Data, including:

- Organisation, adaptation, or alteration;
- Disclosure by transmission, dissemination, or otherwise; and
- Alignment, combination, blocking, erasure, or destruction.

Relevant Filing System: Relevant Filing System means any set of information relating to individuals, whether kept in manual or electronic files, structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Therefore any digital Database and/or organised manual files relating to identifiable living individuals fall within the scope of Data Protection laws and regulations, while a Database of pure statistical or financial information (which cannot either directly or indirectly be related to any identifiable living individuals) will not.

Sensitive Data: Sensitive Data means Personal Data containing information as to the Data Subject's:

- Race or ethnic origin;
- Religious beliefs or other beliefs of a similar nature;
- Political opinions;
- Physical or mental health or condition;
- Sexual history or orientation;
- Trade union membership;
- Commission or alleged commission of any offense and any related court proceedings.

Technology: Technology is to be interpreted broadly, to include any means of collecting or Processing Data, including, without limitations, computers and networks, telecommunications systems, video and audio recording devices, biometric devices, closed circuit television, etc.