Data Protection Policy Statement

1. Introduction

1.1. Background to the UK-General Data Protection Regulation ('UK-GDPR')

- This Policy is based on the UK-GDPR and the ICO's guidance on the UK-GDPR and also complies with the Data Protection Act 2018, which defines the law of processing data on identifiable living people and most of it does not apply to domestic use. Anyone holding personal data for other purposes is legally liable to comply with this Act, with a few notable exceptions.
- This Policy applies to all personal information processed by, or on behalf of our Company.
- All personal data must be handled and dealt with appropriately however it is collected, recorded and used, and whether it is on paper, in electronic records or recorded in other formats, on other media, or by any other means. It includes information held on computers (including email), paper files, photographs, audio recordings and CCTV images.
- The purpose of this Policy is to help you understand what personal data our Company collects, why we collect it and what we do with it. It will also help you to identify what your rights are and who you can contact for more information, to exercise your rights or to make a complaint.

1.2. Definitions according to Article 4 of the UK-GDPR

- **Personal data** – 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;
- **Data controller** – 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;
- **Data processor** – means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **Processing** – 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;

- **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;
- **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;
- **Child** – the UK-GDPR defines a child as anyone under the age of 13 years old. The processing of personal data of a child shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
- **Third party** – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- **Filing system** – means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- **Third country**– means a country or territory outside the United Kingdom.

2. Data Protection Policy Statement

2.1. Top Magic Limited is committed to compliance with all relevant domestic laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information we collect and process in accordance with the UK-GDPR.

2.2. Compliance with the UK-GDPR is described by this Policy and other relevant policies such as the Information Security Policy (ISP) along with connected processes and procedures.

2.3. The UK-GDPR and this Policy shall apply to all of our Company's data processing functions, including those performed on customers', clients', employees', suppliers', and partners' personal data, and any other personal data the organisation processes from any source.

2.4. Our Company has established objectives for data protection and privacy, which are in the **Personal Information Management System (PIMS).**

2.5. Top Magic Limited shall be responsible for reviewing the register of data processing annually in the light of any changes to the Company activities and to any additional requirements identified by means of **Data Protection Impact Assessment (DPIA).**

2.6. This Policy applies to all Employees/Staff/Contractors/Clients/Partners and third-party providers of our Company. Any breach of the UK-GDPR will be dealt with as described under our **Data Breach Notification Procedure** and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.7. Partners and any third parties working with or for our Company, and who have or may have access to personal data, will be expected to have read, understood and to comply with this Policy. No third party may access personal data held by our Company without having first entered into a **Data Confidentiality Agreement,** which imposes on the third-party obligations no less onerous than those to which our Company is committed, and which gives us the right to audit compliance with the agreement.

3. Personal Information Management System & Information Security Policy (PIMS/ISP)

3.1. To support compliance with the UK-GDPR, our Board has approved and supported the development, implementation, maintenance and continual improvement of a documented PIMS, which is integrated within the ISP, for our Company.

3.2. All our Employees/Staff and third-party providers identified in the inventory are expected to comply with this Policy and with the PIMS/ISP that implements this Policy. All Employees/Staff will receive appropriate training.

3.3. **Scope:**
The scope of the PIMS will cover all of the PII (Personally Identifiable Information) that the organisation holds including PII that is shared with external organisations such as suppliers, cloud providers, etc.

3.4. In determining its scope for compliance with the UK-GDPR, we consider:

- any external and internal issues that are relevant to our purpose and that affect our ability to achieve the intended outcomes of its PIMS/ISP;
- specific needs and expectations of interested parties that are relevant to the implementation of the PIMS/ISP;
- organizational objectives and obligations;
- the organisation's acceptable level of risk; and
- any applicable statutory, regulatory, or contractual obligations.

3.5. The PIMS is documented within the ISP system, maintained in our Intranet. Our Company's objectives for compliance with the UK-GDPR are consistent with this Policy, measurable, take into account UK-GDPR privacy

requirements and the results from risk assessments and risk treatments, monitored, communicated and updated as appropriate.

4. Responsibilities & Roles under the General Data Protection Regulation

4.1. We are a data controller for staff and marketing data and a data processor for client data under the UK-GDPR.

4.2. All those in managerial or supervisory roles throughout our Organisation are responsible for developing and encouraging good information handling practices within our Company.

4.3. Top Magic Limited and our Board of Directors for the management of personal data within our Company and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes development and implementation of the UK-GDPR as required by this Policy, and security and risk management in relation to compliance with the Policy.

4.4. The Legal Compliance Department has been appointed to take responsibility for our Company's compliance with this Policy on a day-to-day basis and has direct responsibility for ensuring that our Company complies with the UK-GDPR.

4.5. The Legal Compliance Department shall have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

4.6. Compliance with data protection legislation is a responsibility of and obligation for all our Employees/Staff who process personal data.

4.7. Our Company's Training Policy sets out specific UK-GDPR training and awareness requirements in relation to specific roles of our Employees/Staff generally.

4.8. Our Employees/Staff are responsible for ensuring that any personal data about them and supplied by them to our Company is accurate and up-to-date.

5. Data Protection Principles

5.1. All processing of personal data must be conducted in accordance with the data protection principles as set out in Articles 5 and 6 of the UK-GDPR. Our

policies and procedures are designed to ensure compliance with the principles.

5.2. **Personal data must be processed lawfully, fairly & transparently**

- **Lawfully** – you must identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example, consent.
- **Fairly** – in order for processing to be fair, the data controller has to make sure that personal data are handled in ways that the data subject would reasonably expect and not use it in ways that have unjustified adverse effects on it.
- **Transparently** – Transparent processing is about being clear, open and honest with people from the start about who you are, and how and why you use their personal data. We ensure that we tell individuals about our processing in a way that is easily accessible and easy to understand. You must use clear and plain language.

5.3. **The specific information that must be provided to the data subject must, as a minimum, include:**

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the DPO (if a DPO is appointed) or the contact details of the relevant Department to appointed by the Organisation to responsible to establish GDPR compliance);
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the categories of personal data concerned;
- any further information necessary to guarantee fair processing.

5.4. **Personal data can only be collected for specific, explicit and legitimate purposes**

- Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- The **Privacy Procedure** sets out the relevant procedures.

5.5. **Personal data must be adequate, relevant and limited to what is necessary for processing**

- The Legal Compliance Department is responsible for ensuring that we do not collect information that is not strictly necessary for the purpose for which it is obtained.
- All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or a link to privacy statement and approved by the Legal Compliance Department.
- The Legal Compliance Department will ensure that, on an annual basis all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

5.6. **Personal data must be accurate and kept up to date with every effort to erase or rectify without delay**

- Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. The Legal Compliance Department is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
- Employees/Staff/clients/contractors and third-party providers should be required to notify the Company of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Company to ensure that any notification regarding change of circumstances is recorded and acted upon.
- The Legal Compliance Department is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
- On at least an annual basis, the Legal Compliance Department will review the retention dates of all the personal data processed by our Company, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the **Information Disposal Policy**.
- The Legal Compliance Department is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If our Company decides not to comply with the request, the Legal Compliance Department must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

5.7. **Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.**

- Where personal data is retained beyond the processing date, it will be

minimised/ encrypted/ pseudonymised in order to protect the identity of the data subject in the event of a data breach. Personal data will be retained in line with the ISP and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

- The Legal Compliance Department must specifically approve any data retention that exceeds the retention periods defined in the ISP and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

5.8. **Personal data must be processed in a manner that ensures the appropriate security**

- The Legal Compliance Department will carry out a Data Protection Risk Assessment (DPIA) taking into account all the circumstances of our Company's controlling or processing operations.
- In determining appropriateness, the Legal Compliance Department should also consider the extent of possible damage or loss that might be caused to individuals (e.g., staff or customers) if a security breach occurs, the effect of any security breach on the Company itself, and any likely reputational damage including the possible loss of customer trust.

5.9. When assessing appropriate technical measures, the Legal Compliance Department shall consider the following:

- Password Protection
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to the Company's procedures.

5.10. When assessing appropriate organisational measures, the Legal Compliance Department shall consider the following:

- The appropriate training levels throughout our Company;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection clause in employment contracts;
- Identification of disciplinary action measures for data breaches;

- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Adoption of a Clear Desk Policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employees' own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site.

5.11. These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Our Company's compliance with this principle is contained in its PIMS, which has been developed in line with the ISP.

5.12. **The controller must be able to demonstrate compliance with the UK-GDPR's other principles (accountability)**

- The UK-GDPR includes provisions that promote accountability and governance. These complement the UK-GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.
- Our Company will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

6. Personal Data Individuals' Rights

6.1. Each individual shall have the following rights regarding data processing, and the data that is recorded about them:

- To make access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the UK-GDPR.

- To take action to rectify, block, erase or destroy inaccurate data.
- To request the supervisory authority to assess whether any provision of the UK-GDPR has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

6.2. Our Company ensures that individuals may exercise these rights by making data access requests as described in the **Acceptable Use Agreement**, which shall include the Subject Access Request Procedure. This procedure also describes how our Company will ensure that its response to the data access request complies with the requirements of the UK-GDPR.

6.3. Individuals shall also have the right to complain to the Company related to the processing of their personal data, handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

7. Consent

7.1. Our Company understands "consent" to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

7.2. Our Company understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

7.3. There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

7.4. For sensitive data, explicit written consent of individuals must be obtained unless an alternative legitimate basis for processing exists.

7.5. In most instances, consent to process personal and sensitive data is obtained routinely by the Company using standard consent documents e.g., when a new

client signs a contract, or during induction for participants on programmes.

7.6. Where our Company provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 13. Our Company does not routinely process data in this category.

8. Security of Data

8.1. All Employees/Staff are responsible for ensuring that any personal data that our Company holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by our Company to receive that information and has entered into a confidentiality agreement.

8.2. All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Company's Policies.

8.3. Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of the Company. All Employees/Staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

8.4. Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

8.5. Personal data may only be deleted or disposed of in line with the **Information Retention procedure.** Manual records that have reached their retention date are to be shredded and disposed of as "confidential waste". Hard drives of redundant PCs are to be removed and immediately destroyed.

9. Disclosure of Data

9.1. The Company must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party.

9.2. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for the conduct of our Company's business.

10. Retention & Disposal of Data

10.1. The Company shall not keep personal data in a form that permits identification of data subjects for longer a period than it is necessary, in relation to the purpose(s) for which the data was originally collected.

10.2. The Company may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

10.3. The retention period for each category of personal data will be set out in the **Information Retention procedure** along with the criteria used to determine this period including any statutory obligations the Company has to retain the data.

10.4. The Company's information retention and information disposal procedures apply in all cases.

10.5. Personal data must be disposed of securely in accordance with the sixth principle of the UK-GDPR. Any disposal of data will be done in accordance with the secure disposal procedure.

11. Data Transfers

11.1. On 28 June 2021 the EU Commission adopted decisions on the UK's adequacy under the EU's General Data Protection Regulation (EU GDPR) and Law Enforcement Directive (LED). In both cases, the European Commission has found the UK to be adequate. This means that most data can continue to flow from the EU and the EEA without the need for additional safeguards.

11.2. All exports of data from the UK and the European Economic Area (EEA) to non-European Economic Area countries (referred to in the UK-GDPR as "third countries") are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

11.3. The broader area of the EEA is granted "adequacy" on the basis that all such countries are signatories to the GDPR. The non-EU EEA member countries (Liechtenstein, Norway and Iceland) apply **EU regulations through a Joint Committee Decision.**

11.4. **Binding Corporate Rules:**

The Company may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that the Company is seeking to rely upon**.**

11.5. **Model Contract Clauses:**

The Company may adopt approved model contract clauses for the transfer of data outside of the UK and the EEA. If the Company adopts the model contract clauses approved by the relevant supervisory authority there is an automatic recognition of adequacy.

11.6. **Exceptions:**

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the individual has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the individual and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

12. Data Inventory

12.1. The Company has established a Data Inventory and Data Flow process as part of its approach to address risks and opportunities throughout its UK-GDPR compliance project. The Company's Data Inventory and Data Flow determines:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;

- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Company throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

12.2. Our Company is aware of any risks associated with the processing of particular types of personal data:

- The Company assesses the level of risk to individuals associated with the processing of their personal data. **Data Protection Impact Assessments** (DPIAs) are carried out in relation to the processing of personal data by the Company, and in relation to processing undertaken by other organisations on behalf of the Company.
- The Company shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this Policy.
- Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, our Company shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.
- Where, as a result of a DPIA it is clear that the Company is about to commence processing of personal data that could cause damage the Company and/or distress to the data subjects, the decision as to whether or not the Company may proceed must be escalated for review to the Legal Compliance Department.
- The Legal Compliance Department shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.
- Appropriate controls will be selected, as appropriate and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the Company's documented risk acceptance criteria and the requirements of the UK-GDPR.