DATA PROTECTION POLICY

1. Data Protection Policy

1.1 This policy sets out how Seven20 (“We”, “Us”, the “Company”) handles personal information in the course of its business activities. We recognise that we process personal information about a range of stakeholders and are committed to handling that information in a lawful, fair and transparent way in accordance with applicable data protection legislation, including the UK General Data Protection Regulation (“UK-GDPR”), the Data Protection Act 2018 and, where applicable, the EU General Data Protection Regulation (“EU-GDPR”).

1.2 In our client services, delivered via the Seven20 platform and related services, the Company acts as a **data processor** on behalf of its clients. Each client acts as the **data controller** in respect of candidate, contact and client-employee data processed in the platform and determines the purposes and means of that processing.

1.3 Separately, the Company acts as a **data controller** in relation to personal information it processes for its own business purposes, including information relating to its own employees, job applicants, contractors, suppliers, prospects and customers, as well as finance, marketing, CRM and platform telemetry data.

1.4 The types of personal information we may handle include details of current, past and prospective employees, interns, candidates, client contacts, client employees, prospects, suppliers and other stakeholders that we communicate or interact with in the course of providing and supporting our services. This information may be held on paper, in electronic form or in other media and is subject to legal safeguards which impose restrictions on how we may use that information.

1.5 We are committed to protecting the rights and freedoms of data subjects and to demonstrating accountability for our data protection responsibilities. We reserve the right to change or amend this policy from time to time to reflect changes in law, guidance or our processing activities. The most recent version will be made available to staff and, where appropriate, to clients.

---

2. Status of the Policy

2.1 This policy sets out how the Company complies with its data protection obligations and seeks to protect personal information relating to our workforce, candidates, platform users, client contacts, suppliers and other stakeholders (“Stakeholders”, “Data Subjects”). Its purpose is also to ensure that the Company understands and complies with the rules governing the collection, use, disclosure

and deletion of personal information to which we have access in the course of our work.

2.2 The Company is committed to being concise, clear and transparent about how it obtains and uses personal information and how (and when) it deletes that information once it is no longer required. This policy applies to all personal information processed by or on behalf of the Company, whether as controller or as processor.

2.3 Where the Company acts as a data processor on behalf of clients, this policy sets out the minimum internal standards it applies to protect client data. The detailed allocation of responsibilities between the client (as controller) and the Company (as processor) is set out in the relevant client contract and Data Processing Agreement ("DPA"), which shall prevail in the event of any inconsistency with this policy.

2.4 The Company has appointed a Data Protection Officer or Data Protection Manager ("DPO/M"), who is responsible for informing and advising the Company and its staff on data protection obligations, for monitoring compliance with those obligations and with the Company's policies, and for acting as a contact point for supervisory authorities and data subjects. The DPO/M reports regularly to senior management on data protection risks, incidents and compliance activities.

2.5 The Company also benefits from a formal data protection representation and advisory service based in Ireland, which acts as its representative and point of contact within the European Economic Area ("EEA") in relation to processing subject to EU-GDPR. Contact details for the DPO/M and the EEA representative are set out in the Company's Privacy Notice and may be updated from time to time without amending this policy.

2.6 All staff must read, understand and comply with this policy when processing personal information on behalf of the Company. Any breach of this policy may result in disciplinary action and, where appropriate, contractual or legal consequences.

---

3. Definition of Data Protection Terms

3.1 **Data** is information which is stored electronically, on a computer, in the cloud or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal data** (sometimes known as personal information) means any information relating to a living individual who can be identified from that information (or from that information and other information in our possession or likely to come

into our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.4 **Data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.

3.5 **Criminal records information** means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

3.6 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with data protection law. The Company is a data controller in relation to personal information which it processes for its own business purposes (for example HR, finance, marketing, CRM and platform telemetry data). In addition, each client is the data controller for the personal data it enters into or otherwise processes through the Seven20 platform and related client services.

3.7 **Data users** include employees and other individuals whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.8 **Data processors** are people or organisations that process personal data on behalf of a data controller and in accordance with that controller's documented instructions. The Company acts as a data processor when it processes personal data on behalf of a client in the context of providing the Seven20 platform and related services (including data about candidates who have applied to a client, client contacts and client employees). The Company may also engage third-party data processors (sub-processors) to assist it in delivering those services, subject to appropriate contractual safeguards.

3.9 **Data Protection Officer / Data Protection Manager (DPO/M)** means the person appointed by the Company to oversee and advise on compliance with data protection law and this policy. The DPO/M is responsible for educating the Company and its employees on important compliance requirements, training staff involved in data processing, and conducting or coordinating appropriate audits and reviews. The DPO/M also serves as a point of contact between the Company and supervisory authorities, and works alongside the Company's EEA-based representative in Ireland for matters falling under EU-GDPR. The Company may determine, from time to time, whether the position is a formally mandated DPO role under law or a Data Protection Manager role carrying equivalent responsibilities.

3.10 **Processing** information means obtaining, recording, organising, storing, amending, retrieving, disclosing, combining, restricting, erasing and/or destroying information, or using or doing anything with it.

3.11 **Pseudonymisation** means the processing of personal information in such a way that it cannot be attributed to a specific data subject without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual.

3.12 **Sensitive personal data** (sometimes known as “special categories of personal data”) includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership or non-membership, physical or mental health or condition, sexual life or sexual orientation, genetic information or biometric information (where used to identify an individual), or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require a lawful basis and a specific condition for processing under data protection law.

---

4. Data Protection Principles

4.1 The Company will comply with the following data protection principles when processing personal information:

- (a) We will process personal information lawfully, fairly and in a transparent manner.
- (b) We will collect personal information for specified, explicit and legitimate purposes only and will not process it in a manner that is incompatible with those purposes.
- (c) We will only process personal information that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- (d) We will keep personal information accurate and, where necessary, up to date, and will take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay.
- (e) We will keep personal information for no longer than is necessary for the purposes for which the information is processed.

- (f) We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

---

5. Basis for Processing Personal Information

5.1 In relation to any processing activity, we will, before the processing starts for the first time and then regularly while it continues:

- (a) Review the purposes of the particular processing activity and select the most appropriate lawful basis (or bases) for that processing, namely:
    - (i) the data subject has given consent;
    - (ii) the 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;
    - (iii) the processing is necessary for compliance with a legal obligation to which the Company is subject;
    - (iv) the 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.
- (b) Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. there is no other reasonable way to achieve that purpose).
- (c) Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.
- (d) Include information about both the purposes of the processing and the lawful basis for it in the relevant privacy notice(s).
- (e) Where sensitive personal information is processed, identify and document a lawful condition for processing that information (see clause 6).
- (f) Where criminal offence information is processed, identify and document a lawful condition for processing that information.

5.2 When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing in its own capacity as a controller, we will:

- (a) Conduct a legitimate interests assessment ("LIA") as set out in our internal templates and keep a record of it, to ensure that we can justify our decision.

- (b) If the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment ("DPIA") in our role as controller.
- (c) Keep the LIA under review and repeat it if circumstances change.
- (d) Include information about our legitimate interests in our relevant privacy notice(s).

---

6. Sensitive Personal Information

6.1 The Company may from time to time need to process sensitive personal information. We will only process such information if:

- (a) We have a lawful basis for doing so as set out in paragraph 5.1(a) above (for example, it is necessary for the performance of an employment contract, to comply with the Company's legal obligations or for the purposes of the Company's legitimate interests); and
- (b) One of the special conditions for processing sensitive personal information applies, for example:
    - (i) the data subject has given explicit consent;
    - (ii) the processing is necessary for the purposes of exercising or complying with employment law rights or obligations;
    - (iii) the processing is necessary to protect the data subject's vital interests and the data subject is physically or legally incapable of giving consent;
    - (iv) the processing relates to personal data which are manifestly made public by the data subject;
    - (v) the processing is necessary for the establishment, exercise or defence of legal claims; or
    - (vi) the processing is necessary for reasons of substantial public interest.

6.2 Before processing any sensitive personal information, staff must notify the DPO/M of the proposed processing so that the DPO/M may assess whether the processing complies with the above criteria.

6.3 Sensitive personal information will not be processed until the assessment referred to in paragraph 6.2 has taken place and the individual has been properly

informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.4 The Company will not carry out automated decision-making (including profiling) based solely on any individual's sensitive personal information.

6.5 The Company's Privacy Notice sets out the types of sensitive personal information that the Company processes, what it is used for and the lawful basis for the processing.

6.6 The Company will comply with the procedures set out in paragraphs 9.1 and 9.2 below in relation to sensitive personal information to ensure compliance with the data protection principles.

6.7 During the recruitment process, HR, with guidance from the DPO/M, will ensure that (except where the law permits otherwise):

- (a) During short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information unless strictly necessary and lawful.
- (b) If sensitive personal information is received without being requested (for example, included in a CV), no unnecessary record is kept and any references are redacted where feasible.
- (c) Any equal opportunities monitoring data is kept separate from the individual's application and not seen by those making recruitment decisions.
- (d) Health-related questions are asked only once a conditional offer of employment has been made, unless otherwise permitted by law.

6.8 During employment, HR, with guidance from the DPO/M, may process health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits.

---

7. Criminal Records Information

7.1 Criminal records information may be processed during the recruitment process before making a final decision to recruit. This information may be received from the candidate and from the Disclosure and Barring Service ("DBS") or equivalent bodies. We will only request such information where it is lawful and necessary for a role.

7.2 Criminal records information will be used only to make an informed recruitment or employment decision. If the candidate is successful, we will retain the information securely and only for as long as necessary and proportionate, typically up to six

years post-employment unless a different period is justified or required by law. If the candidate is unsuccessful, we will retain the information securely for a limited period (typically six months) and then destroy it, unless retention is required for legal reasons.

---

8. Data Protection Impact Assessments

8.1 Where the Company acts as a **data controller** and processing is likely to result in a high risk to individuals' rights and freedoms (for example, where the Company is planning to use a new form of technology, conduct large-scale or systematic monitoring, or introduce new features using AI/ML on personal data), the Company is responsible for carrying out an appropriate data protection impact assessment ("DPIA") before commencing the processing.

8.2 In its role as a **data processor** for client services, the Company does not determine whether a DPIA is required for the client's overall processing activities and is not responsible for performing the client's DPIA. The responsibility for assessing the need for, and carrying out, a DPIA in relation to the client's use of the Seven20 services rests with the client as data controller.

8.3 The Company will, however, provide reasonable assistance to clients in connection with any DPIA they choose, or are required, to undertake in relation to their engagement of the Seven20 services. This assistance may include, where appropriate and subject to confidentiality:

- (a) Providing information about the nature, scope, context and purposes of the processing carried out on behalf of the client.
- (b) Providing information about the systems, technical and organisational measures and sub-processors used to deliver the services.
- (c) Supporting the client in assessing risks to data subjects arising from the processing performed by the Company on the client's behalf.

8.4 Before any new processing activity or technology is introduced by the Company in its capacity as controller that may require a DPIA, the manager responsible must contact the DPO/M to ensure that an appropriate DPIA is carried out and that any required consultation with supervisory authorities is completed, particularly where processing may significantly affect UK or EEA data subjects.

---

9. Documentation and Records

9.1 The Company will maintain written records of its processing activities where required by law, including processing that may result in a risk to individuals' rights

and freedoms or that involves sensitive personal information or criminal records information. Such records will include, where applicable:

- (a) The name and contact details of the Company (and, where applicable, of any joint controllers, the Company's representative in the EEA and the DPO/M).
- (b) The purposes of the processing.
- (c) A description of the categories of data subjects and categories of personal data.
- (d) The categories of recipients to whom personal data have been or will be disclosed.
- (e) Where relevant, details of transfers of personal data to third countries or international organisations, including the identification of the transfer mechanism and safeguards.
- (f) Where possible, the envisaged retention periods for different categories of personal data.
- (g) Where possible, a general description of the technical and organisational security measures in place.

9.2 As part of its records of processing activities ("RoPA"), the Company will document, or link to documentation, on:

- (a) Information required for privacy notices.
- (b) Records of consent, where consent is relied upon.
- (c) Controller–processor contracts, including DPAs with clients and contracts with sub-processors.
- (d) The location of personal information within systems and services, including the Seven20 platform and supporting tools.
- (e) DPIAs and LIAs.
- (f) Records of data breaches and related investigations.

9.3 Where the Company processes sensitive personal information or criminal records information, it will maintain written records of:

- (a) The relevant purpose(s) for which the processing takes place, including (where required) why it is necessary.
- (b) The lawful basis and condition for processing.

- (c) Whether the Company retains and erases the personal information in accordance with its policy and, if not, the reasons for departing from the policy.

9.4 The Company will conduct regular reviews of the personal information it processes and will update its documentation accordingly. This may include consulting stakeholders across the business to obtain a complete picture of processing activities and reviewing policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

9.5 Records of processing activities will be maintained in electronic form so that they can be updated efficiently when processing activities change.

---

10. Privacy Notice

10.1 The Company will issue one or more privacy notices, from time to time, to inform stakeholders about the personal information that we collect and hold relating to them, how they can expect their personal information to be used, and for what purposes.

10.2 The Company will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

---

11. Individual Rights

11.1 Data subjects have the following rights in relation to their personal information, subject to certain legal conditions and exemptions:

- (a) To be informed about how, why and on what basis their personal information is processed, through appropriate privacy notices.
- (b) To obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request.
- (c) To have personal information corrected if it is inaccurate or incomplete.
- (d) To have personal information erased in certain circumstances (the “right to be forgotten”).
- (e) To restrict the processing of their personal information in certain circumstances.

- (f) To object to certain forms of processing, including processing based on legitimate interests and processing for direct marketing purposes.
- (g) To receive personal data they have provided in a structured, commonly used and machine-readable format and to transmit those data to another controller, where the processing is based on consent or contract and is carried out by automated means (the “right to data portability”).

11.2 Data subjects who wish to exercise any of these rights should contact the DPO/M via the contact details set out in the relevant privacy notice. The Company will normally respond to such requests within one month of receipt. This period may be extended by up to two further months where necessary, taking into account the complexity and number of requests; in such cases, the data subject will be informed of the extension and reasons for the delay.

11.3 Where the Company acts as a data processor on behalf of a client, data subjects will normally need to exercise their rights with the client (as controller). In such cases, the Company will promptly forward any rights requests it receives to the relevant client and will provide reasonable assistance to enable the client to respond, in accordance with the applicable DPA.

11.4 Data subjects also have the right to lodge a complaint with a supervisory authority if they believe that their data protection rights have been infringed. For data subjects in the UK, this is typically the Information Commissioner’s Office (“ICO”). For data subjects in the EEA, this will generally be the supervisory authority in their habitual residence, place of work or place of the alleged infringement. Details of relevant supervisory authorities are set out in the Company’s Privacy Notice.

---

12. Individual Obligations

12.1 Individuals are responsible for helping the Company keep their personal information up to date. Data subjects should let the Company know if information previously provided to the Company changes (for example, if a stakeholder moves house or bank account details change).

12.2 Stakeholders, particularly employees, may have access to the personal information of other stakeholders. The Company expects its staff to help meet its data protection obligations towards those individuals and to be aware that they may also enjoy the rights set out in paragraph 11.1.

12.3 Staff who have access to personal information must:

- (a) Only access the personal information that they are authorised to access and only for authorised purposes.

- (b) Only allow other Company staff to access personal information where they have appropriate authorisation.
- (c) Only allow individuals who are not Company staff to access personal information where they have specific authority to do so.
- (d) Keep personal information secure, including by complying with rules on access to premises, computer access, password protection, secure file storage and secure disposal, and other precautions set out in the Company's Information Security Policy.
- (e) Comply with Company security procedures, including:
    - (i) Access controls and door security; reporting any unknown individuals in secure areas.
    - (ii) Appropriate methods of disposal, such as shredding of paper documents and secure wiping of removable media where their use is permitted.
    - (iii) Ensuring that monitors do not display confidential information to unauthorised persons and logging off or locking screens when leaving equipment unattended.
- (f) Not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures (such as pseudonymisation, encryption or password protection) are in place.
- (g) Not store personal information on local drives or on personal devices, unless explicitly authorised and subject to appropriate security controls.

12.4 Staff must contact the DPO/M promptly if they are concerned or suspect that any of the following has taken place (or is taking place or is likely to take place):

- (a) Processing of personal data without a lawful basis or, in the case of sensitive personal information, without an applicable condition under paragraph 6.1(b).
- (b) Any data breach (see clause 15).
- (c) Access to personal information without proper authorisation.
- (d) Personal information not kept or deleted securely.
- (e) Removal of personal information, or devices containing personal information (or which can be used to access it), from the Company's premises without appropriate security measures.

- (f) Any other breach of this policy or of any of the data protection principles.

---

13. Information Security

13.1 The Company will use appropriate technical and organisational measures, in accordance with its Information Security Policy, to keep personal information secure and to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These measures may include, as appropriate:

- (a) Pseudonymising or encrypting personal information.
- (b) Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- (c) Ensuring that, in the event of a physical or technical incident, availability of and access to personal information can be restored in a timely manner.
- (d) Regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.
- (e) Implementing role-based access controls and the principle of least privilege, including multi-factor authentication for privileged accounts where feasible.
- (f) Applying secure development practices, vulnerability management, and periodic penetration testing for key systems, including the Seven20 platform, with remediation tracked and completed within defined timelines.

13.2 Where the Company uses external organisations to process personal information on its behalf, additional security and data protection arrangements will be implemented through written contracts to safeguard the security and confidentiality of personal information. In particular, such contracts will require that:

- (a) The organisation acts only on the documented written instructions of the Company.
- (b) Those processing the data are subject to appropriate confidentiality obligations.
- (c) Appropriate technical and organisational measures are applied to ensure the security of processing.
- (d) Sub-processors are only engaged with the prior consent of the Company and under a written contract imposing equivalent obligations.

- (e) The organisation assists the Company in providing data subjects with access to their personal information and in enabling data subjects to exercise their rights.
- (f) The organisation assists the Company in meeting its obligations in relation to the security of processing, the notification of data breaches and the conduct of DPIAs.
- (g) The organisation deletes or returns all personal information to the Company at the end of the contract, at the Company's choice, unless retention is required by law.
- (h) The organisation submits to audits and inspections by the Company (or its appointed auditors), provides the Company with information necessary to demonstrate compliance, and promptly informs the Company if it believes an instruction infringes data protection law.

13.3 The Company will maintain a documented list of key sub-processors and their locations, and will make this information available to clients in accordance with the applicable DPA. Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is materially altered, the relevant staff must seek approval of its terms by the DPO/M or an appropriate delegate.

---

14. Storage and Retention of Personal Information

14.1 Personal information (including sensitive personal information) will be kept securely in accordance with the Company's Information Security Policy.

14.2 Personal information should not be retained for any longer than necessary. The appropriate retention period will depend on the circumstances, including the reasons why the personal information was obtained and any legal, regulatory or contractual requirements. Staff must follow the Company's Retention and Erasure Policy, which sets out relevant retention periods or the criteria used to determine them. Where there is any uncertainty, staff should consult the DPO/M.

14.3 Personal information that is no longer required will be deleted or anonymised in our systems and any hard copies will be destroyed securely, subject to any legal or regulatory requirements to retain specific records for defined periods.

---

15. Data Breaches

15.1 A data breach may take many forms, including but not limited to:

- (a) Loss or theft of data or equipment on which personal information is stored.
- (b) Unauthorised access to or use of personal information by a member of staff or a third party.
- (c) Loss of personal data resulting from an equipment, system or software failure.
- (d) Human error, such as accidental deletion or alteration of data or sending data to the wrong recipient.
- (e) Unforeseen circumstances such as a fire or flood.
- (f) Deliberate attacks on IT systems, such as hacking, malware, ransomware or phishing.
- (g) Social engineering or “blagging” offences, where information is obtained by deceiving the organisation that holds it.

15.2 The Company will maintain internal procedures and forms to support the timely reporting, investigation and remediation of data breaches. All staff must promptly report suspected or actual breaches in accordance with those procedures.

15.3 The Company will assess all incidents to determine whether they constitute a personal data breach and, if so, whether notification to a supervisory authority and/or data subjects is required. Where a reportable breach occurs under UK-GDPR or EU-GDPR, the Company will:

- (a) Make the required report to the relevant supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of the breach.
- (b) Notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms and notification is required by law.
- (c) Maintain records of all breaches, whether or not they are notifiable, including their causes, effects and remedial actions taken.

15.4 Where the Company acts as a processor and a data breach affects client data, the Company will notify the relevant client(s) without undue delay in accordance with the DPA and will cooperate with the client in relation to any regulatory or data subject notifications.

---

16. International Transfers

16.1 The Company may transfer personal information to countries outside the UK and/or the EEA in the course of providing its services, for example where sub-processors or infrastructure providers are located in third countries or where clients access the platform from outside these regions.

16.2 The Company will only transfer personal information outside the UK in accordance with UK-GDPR and the Data Protection Act 2018, and only transfer personal information outside the EEA in accordance with EU-GDPR (where applicable). In particular, the Company will ensure that one of the following conditions applies:

- (a) The transfer is to a country, territory or international organisation which has been formally recognised as providing an adequate level of protection for personal data under UK or EU law (as relevant).
- (b) Appropriate safeguards are in place, such as the UK International Data Transfer Agreement ("IDTA"), the UK Addendum to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses ("SCCs"), binding corporate rules or an approved code of conduct or certification mechanism.
- (c) A specific derogation applies, such as explicit consent from the data subject, the necessity of the transfer for the performance of a contract with the data subject, or other limited circumstances permitted by law.

16.3 Where the Company relies on appropriate safeguards under paragraph 16.2(b), it will assess the laws and practices of the destination country and implement any supplementary measures required to ensure that data subjects are afforded a level of protection essentially equivalent to that in the UK or EEA, as applicable.

16.4 The Company will maintain a record of international transfers and the applicable safeguards as part of its RoPA and will provide additional information to clients on request, including information on sub-processor locations. Where the Company acts as a processor, it will only make international transfers in accordance with the client's instructions and the relevant DPA.

16.5 The Company aims to provide a high and consistent level of protection for personal information regardless of where it is processed and will take steps to ensure that this policy and supporting information security measures are applied across its operations and suppliers.

---

17. Training

17.1 The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Data protection and information security training will be

provided as part of induction for all new staff who have access to personal information and will be refreshed at appropriate intervals (for example, annually).

17.2 Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to data subject requests or incidents (for example, HR, client support, product, engineering and operations staff), will receive additional role-specific training to help them understand their duties and how to comply with them.

17.3 The Company will maintain records of training completion and may require periodic assessments to ensure that staff understand key concepts and responsibilities.

---

18. UK-GDPR and EU-GDPR Compliance Failures

18.1 The Company takes compliance with this policy and with applicable data protection law very seriously. Failure to comply:

- (a) Puts at risk the individuals whose personal information is being processed.
- (b) Exposes the Company and, where applicable, clients to the risk of significant civil and criminal sanctions, regulatory investigation and reputational damage.
- (c) May, in some circumstances, amount to a criminal offence by the individual responsible.

18.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, up to and including dismissal for gross misconduct. If a non-employee (such as a contractor or supplier) breaches this policy, their contract may be terminated with immediate effect and other appropriate remedies may be pursued.

---

19. Appendices

19.1 The following appendices are maintained by the Company and are considered part of the data protection framework. They may be updated more frequently than this policy and are available internally on request:

- Appendix 1: Data Protection Impact Assessment Template.
- Appendix 2: Legitimate Interests Assessment Template.
- Appendix 3: Data Subject Access Request Form and Process.
- Appendix 4: Breach Notification and Incident Reporting Form.

- Appendix 5: Breach Investigation and Root Cause Analysis Process.