GDPR DATA POLICY

A. Introduction

This Policy sets out the obligations of STUDIO'CONNOR, a company registered in England and Wales with registered no. 07284783 and address, Bury Lodge, Bury Road, Stowmarket, Suffolk, England, IP14 1JA (the 'Company', 'we', 'us', 'our') regarding data protection and the rights of our customers, suppliers, business contacts and employees in respect of their Personal Data under EU Regulation 2016/679 General Data Protection Regulation ('GDPR').

The GDPR defines 'Personal Data' as any information relating to an identified or identifiable natural person (a 'Data Subject', 'you', 'your'); 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.

From the 25th May 2018, the GDPR (defined below), as amended or updated from time to time, is in force. We wish to ensure that we are compliant with our role as set out under the GDPR and as such this policy and the protocols it outlines are the principles which demonstrate our commitment regarding the collection, processing, transfer, storage, and disposal of your Personal Data. The protocols outlined here are followed at all times by the Company, its employees, agents, contractors, or other parties working on our behalf.

We are committed not only to the letter of the law, but also to the spirit of the law and we place a high importance on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy, and trust of all individuals with whom we deal.

The Company's nominated Data Protection Officer ('DPO') is Josef O'Connor who can be contacted by email at info@circa.art or in writing at the Company's office address above. The responsibilities of our DPO are outlined in section B9 below.

B. Data Protection

B1. Introduction

The GDPR sets out the following principles with which any party handling Personal Data must comply. All Personal Data must be:

- processed lawfully, fairly, and in a transparent manner in relation to the Data Subject;
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;
- kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed. Personal data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes,

or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the Data Subject; and
- processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

B2. Rights of the Data Subject

The GDPR also clarifies and enhances the rights of Data Subjects. As such, you have the right to:

- be informed that we hold your Personal Data (section B11 below);
- access the Personal Data we hold about you (section B12);
- rectify any data which is incorrect, inaccurate, incomplete or obsolete (B13);
- erasure of the data we hold about you (also known as the 'right to be forgotten') (B14);
- restrict how the data is processed and, in particular, how it is used (B15);
- obtain your Personal Data in a specific format (B16);
- object to your data being used in a specific way (B17); and
- determine use of your data in relation to automated decision-making and profiling (B18 and B19).

B3. Lawful, Fair, and Transparent Data Processing

The processing of your Personal Data is lawful if at least one of the following applies:

- You have given consent to the processing of your Personal Data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which you are a party, or in order to take steps prior to entering into a contract with us;
- The processing is necessary for compliance with a legal obligation to which we are subject;
- The processing is necessary to protect your vital interests or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us; or
- The processing is necessary for the purposes of our legitimate business interests, except where such interests are overridden by your fundamental rights and freedoms which require protection of Personal Data, in particular where the Data Subject is a child.

B4. Specified, Explicit, and Legitimate Purposes

We collect and process the Personal Data set out in section B20. This includes Personal data we have collected directly from you and Personal Data obtained from third parties. We only collect, process, and hold Personal Data for the specific purposes set out in section B20 or for other purposes expressly permitted by the GDPR. You have the right to be informed at all times of the purpose or purposes for which we use your Personal Data, as outlined in section B11.

B5. Adequate, Relevant, and Limited Data Processing

We only collect and process Personal Data for and to the extent necessary for the specific purpose or purposes about which you are informed (or will be informed) as per section B4, above, and as set out in section B20, below.

B6. Accuracy of Data and Keeping Data Up to Date

We ensure that all Personal Data collected, processed, and held by us is kept accurate and up to date. This includes, but is not limited to, the rectification of your Personal Data at your request, as set out in section B13, below. The accuracy of your Personal Data is checked when it is collected and at regular intervals thereafter. If any of your Personal Data is found to be inaccurate or out-of-date, we will take all reasonable steps without delay to amend or erase that data, as appropriate.

B7. Retaining Data

We will not keep Personal Data for any longer than is necessary in light of the purpose or purposes for which that Personal Data was originally collected, held, and processed. When Personal Data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

Full details of our approach to data retention, including retention periods for specific Personal Data types held by us, are outlined in our Data Retention Policy below.

B8. Secure Processing

We ensure that all Personal Data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which are taken are provided in sections B21 to B22.

B9. Accountability and Record-Keeping

Our Data Protection Officer ('DPO', named above) is responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy and with the GDPR and other applicable data protection legislation.

We keep written internal records of all Personal Data collection, holding, and processing, incorporating the following information:

- The name and details of the Company, its DPO, and any applicable third-party data processors;
- The purposes for which we collect, hold, and processes Personal Data;
- Details of the categories of Personal Data collected, held, and processed, and the categories of Data Subject to which that Personal Data relates;
- Details of any transfers of Personal Data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long Personal Data will be retained (see below); and
- Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of Personal Data.

B10. Data Protection Impact Assessments

For any and all new projects and/or uses of Personal Data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of Data Subjects under the GDPR, we will undertake Data Protection Impact Assessments. These assessments will be overseen by our DPO and will address the following:

- The type(s) of Personal Data that will be collected, held, and processed;
- The purpose(s) for which Personal Data is to be used;
- The Company's objectives;
- How Personal Data is to be used;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to Data Subjects;
- Risks posed both within and to the Company; and
- Proposed measures to minimise and handle identified risks.

B11. Keeping Data Subjects Informed

Where Personal Data is collected from you directly, you will be informed of its purpose at the time of collection. Where Personal Data is obtained from a third party, you will be informed of its purpose:

- if the Personal Data is used to communicate with you, when the first communication is made; or
- if the Personal Data is to be transferred to another party, before that transfer is made; or
- as soon as reasonably possible and in any event not more than one month after the Personal Data is obtained.

The following information shall be provided:

- Our details, including, but not limited to, the identity of our DPO;
- The purpose(s) for which the Personal Data is being collected and will be processed (as detailed in section B20) and the legal basis justifying that collection and processing;
- Where applicable, the legitimate interests upon which we are justifying our collection and processing of the Personal Data;
- Where the Personal Data is not obtained from you directly, the categories of Personal Data collected and processed;
- Where the Personal Data is to be transferred to one or more third parties, details of those parties;
- Where the Personal Data is to be transferred to a third party that is located outside of the European Economic Area (the 'EEA'), details of that transfer, including but not limited to the safeguards in place (see section B23);
- Details of data retention;
- Details of your rights under the GDPR;
- Details of your right to withdraw your consent to the Company's processing of your Personal Data at any time;
- Details of your right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of your Personal Data and details of any consequences of failing to provide it; and
- Details of any automated decision-making or profiling that will take place using the Personal Data, including information on how decisions will be made, the significance of those decisions, and any consequences.

B12. Data Subject Access

You may make Subject Access Requests ('SARs') at any time to find out more about the Personal Data which we hold about you, what we are doing with that Personal Data, and why.

If you wish to make a SAR, you should do using a Subject Access Request Form from us, returning the completed form to our Data Protection Officer at our office. Responses to SARs will normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, you will be informed.

All SARs received are handled by our DPO. We do not charge a fee for the handling of normal SARs. We do reserve the right to charge reasonable fees for additional copies of information that has already been supplied, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

B13. Rectification of Personal Data

You have the right to require us to rectify any of your Personal Data that is inaccurate or incomplete. We will rectify the Personal Data in question, and inform you of that rectification, within one month of you informing us of the issue. The period can be extended by up to two months in the case of complex requests, in which case you will be informed of the delay.

In the event that any affected Personal Data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that Personal Data.

B14. Erasure of Personal Data

You have "the right to be forgotten". This means you have the right to request that we erase the Personal Data we hold about you in the following circumstances:

- It is no longer necessary for us to hold that Personal Data with respect to the purpose(s) for which it was originally collected or processed;
- You wish to withdraw your consent to the Company holding and processing your Personal Data;
- You object to us holding and processing your Personal Data (and there is no overriding legitimate interest to allow us to continue doing so) (see section B17 for further details concerning the right to object);
- The Personal Data has been processed unlawfully;
- The Personal Data needs to be erased in order for the Company to comply with a particular legal obligation.

Unless we have reasonable grounds to refuse to erase Personal Data, all requests for erasure shall be complied with, and you will be informed of the erasure, within one month of receipt of

your request. The period can be extended by up to two months in the case of complex requests, and we will keep you informed.

In the event that any Personal Data that is to be erased in response to a Data Subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

B15. Restriction of Personal Data Processing

You may request that we cease processing the Personal Data we hold about you. If you make such a request, will retain only the amount of your Personal Data (if any) that is necessary to ensure that the Personal Data in question is not processed further.

In the event that any affected Personal Data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

B16. Data Portability

We may, in certain circumstances, process Personal Data using automated means. For example, individuals who provide their email address to one of our mailing lists will be recorded by our mailing system with no human intervention and our newsletters will be sent to you via an automated process.

Where you have given your consent to the Company to process your Personal Data in such a manner, such as subscribing to our newsletter above, or the processing is otherwise required for the performance of a contract between us, you have the right, under the GDPR, to receive a copy of your Personal Data and to use it for other purposes (namely transmitting it to other data controllers).

To facilitate the right of data portability, we shall make available all applicable Personal Data to you in the following format[s]:

- Electronic copies of commonly used file formats, such as PDF, DOCX, XLSX;
- Compressed folders, such as ZIP, where the data consists of more than one file.

Where technically feasible, if you request this specifically, your Personal Data can be sent directly to the required data controller.

All requests for copies of Personal Data shall be complied with within one month of your request. The period can be extended by up to two months in the case of complex or numerous requests and you shall be informed.

B17. Objections to Personal Data Processing

You have the right to object to us processing your Personal Data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes. If this is the case, we will cease such processing immediately, unless we can demonstrate that our legitimate grounds for such processing override your interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

We may use your Personal Data for direct marketing purposes, but if we do and you object, we will cease such processing immediately.

B18. Automated Decision-Making

The Company does not use Personal Data in automated decision-making processes.

B19. Profiling

The Company does not use Personal Data for profiling purposes.

B20. Personal Data Collected, Held, and Processed

The following Personal Data is collected, held, and processed by the Company:

Data	Type	Purpose
Employee/Worker Data	Personal data and information about our employees and workers.	Employment contract specific. (See section D below.)
Corporate Contacts	Contact details and records about clients, suppliers, etc.	Business interactions, contracts, invoices, etc.
Work-Related Contacts	Contract details and records for individuals who have worked with us on client projects and producing our work, such as photographers, models, etc.	Communication and interaction during the creation of our work.
Consumer Data	Email addresses for individuals on our circulation and mailing lists.	Communications, such as email newsletters, event invitations, etc.
Cookie Data	Anonymised browsing data.	See section E for our Cookie Policy, below.

B21. Data Security

Transferring Personal Data and Communications

We ensure that the following measures are taken with respect to all communications and other transfers involving Personal Data:

- All emails containing Personal Data must be encrypted, marked “confidential”;
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely, and the email itself should be deleted;
- Where Personal Data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where Personal Data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Registered Mail; and
- All Personal Data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

Storage

We ensure that the following measures are taken with respect to the storage of Personal Data:

- All electronic copies of Personal Data should be stored securely using passwords and, where appropriate, two-factor authentication;
- All hardcopies of Personal Data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- All Personal Data stored electronically should be backed up on a regular basis in line with our IT protocol, with backups stored securely both onsite and offsite;
- No Personal Data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of a Director and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- No Personal Data should be transferred to any device personally belonging to an employee and Personal Data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to us that all suitable technical and organisational measures have been taken).

Disposal

When any Personal Data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it will be securely deleted and disposed of. For further information on the deletion and disposal of Personal Data, please refer to our Data Retention Policy below.

Use of Personal Data

We ensure that the following measures are taken with respect to the use of Personal Data:

- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- If Personal Data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
- Where Personal Data is used for marketing purposes, it will be the responsibility of our DPO to ensure that the appropriate consent is obtained and that no Data Subjects have opted out, whether directly or via a third-party service such as the TPS.

IT Security

We ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect Personal Data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require such passwords;

- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on our behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- Where applicable, two-factor authentication is in place and must be used in connection with user passwords to access the system;
- All software (including, but not limited to, applications and operating systems) shall be kept up to date. Our IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
- No software may be installed on any Company-owned computer or device without the prior approval of the IT Department.

B22. Organisational Measures

We ensure that the following measures are taken with respect to the collection, holding, and processing of Personal Data:

- All employees, agents, contractors, or other parties working on our behalf shall be made fully aware of both their individual responsibilities and our responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, agents, sub-contractors, or other parties working on our behalf that need access to, and use of, Personal Data in order to carry out their assigned duties correctly shall have access to Personal Data held by us;
- All employees, agents, contractors, or other parties working on our behalf handling Personal Data will be appropriately trained to do so, will be appropriately supervised, and shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to Personal Data, whether in the workplace or otherwise. They will be bound to handle Personal Data in accordance with the principles of the GDPR and this Policy by contract, and their performance shall be regularly evaluated and reviewed;
- Methods of collecting, holding, and processing Personal Data shall be regularly evaluated and reviewed;
- All Personal Data held by us will be reviewed periodically, as set out in our Data Retention Policy below;
- All agents, contractors, or other parties working on our behalf handling Personal Data must ensure that any and all of their employees who are involved in the processing of Personal Data are held to the same conditions as our relevant employees arising out of this Policy and the GDPR; and
- Where any agent, contractor or other party working on our behalf handling Personal Data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

B23. Transferring Personal Data to a Country Outside the EEA

We may from time to time need to transfer some of your Personal Data to countries outside of the EEA (‘transfer’ includes making available remotely). The transfer of Personal Data to a country outside of the EEA shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for Personal Data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies;

binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (eg the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

- The transfer is made with your informed consent;
- The transfer is necessary for the performance of a contract between us (or for pre-contractual steps taken at your request);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of you or other individuals where you are physically or legally unable to give your consent; or
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

B24. Data Breach Notification

All Personal Data breaches must be reported immediately to our Data Protection Officer. If a Personal Data breach occurs and that breach is likely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the DPO must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a Personal Data breach is likely to result in a high risk to the rights and freedoms of Data Subjects, the DPO must ensure that all affected Data Subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of Data Subjects concerned;
- The categories and approximate number of Personal Data records concerned;
- The name and contact details of our DPO (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

C. Data Retention

The primary aim of this Policy is to set out limits for the retention of Personal Data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that we comply fully with our obligations and your rights under the GDPR.

In addition to safeguarding your rights under the GDPR, by ensuring that we don't retain excessive amounts of data, this Policy also aims to improve the speed and efficiency of managing data.

C1. Scope

This Policy applies to all Personal Data held us or third parties working on our behalf. Personal data, held by us is stored in the following ways and in the following locations:

1. Our computer servers, located at our London office;
2. Third-party servers, operated by our partners, service providers and contractors, such as payroll bureau;
3. Computers permanently located at our London office;
4. Laptop computers and other mobile devices provided by the Company to its employees;
5. Computers and mobile devices owned by employees, agents, and sub-contractors;
6. Physical records stored at our London office.

C2. Data Subject Rights and Data Integrity

All Personal Data held by us is held in accordance with the requirements of the GDPR and Data Subjects' rights thereunder, as set out above in our Data Protection Policy.

C3. Technical and Organisational Data Security Measures

Technical measures that are in place to protect the security of Personal Data are outlined in section B21 of our Data Protection Policy above. Organisational measures are outlined in section B22.

All employees and other parties working on our behalf are made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under our Data Protection Policy above.

C4. Data Disposal

Upon the expiry of the data retention periods set out below in section C5 of this Policy, or when a Data Subject exercises their right to have their Personal Data erased, Personal Data shall be deleted, destroyed, or otherwise disposed of as follows:

- Personal data stored electronically (including any and all backups thereof) shall be deleted;
- Personal data stored in hardcopy form shall be shredded and recycled;

C5. Data Retention Periods

As stated above, and as required by law, we will not retain any Personal Data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

Different types of Personal Data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.

When establishing and/or reviewing retention periods, the following shall be taken into account:

- Our objectives and requirements;
- The type of Personal Data in question;
- The purpose(s) for which the data in question is collected, held, and processed;
- Our legal basis for collecting, holding, and processing that data;
- The category or categories of Data Subject to whom the data relates.

If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

Notwithstanding the following defined retention periods, certain Personal Data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made by us to do so (whether in response to a request by a Data Subject or otherwise).

In limited circumstances, it may also be necessary to retain Personal Data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of Data Subjects, as required by the GDPR.

Data	Review Period	Retention Period of Criteria
Employee/Worker Data	Ongoing and continuous.	At least seven years after employment termination.
Corporate Contacts	Annually throughout the contract period.	At least seven years after the contract termination.
Work-Related Contacts	Annually.	Basic contact information is retained indefinitely for future project work.
Consumer Data	Annually.	Retained indefinitely for ongoing communications.
Cookie Data	See section E for our Cookie Policy, below.	

C6. Roles and Responsibilities

Our Data Protection Officer ('DPO', named above) is responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy and with the GDPR and other applicable data protection legislation.

Any questions regarding this Policy, the retention of Personal Data, or any other aspect of GDPR compliance should be referred to our DPO.

D. Employee Specific data protection

In addition to the Data Protection and Data Retention Policies outlined above, specific protocols exist in relation to the Personal Data we hold about our employees ("Employee Data").

D1. Lawful, fair and transparent data processing

Elements of the Personal Data we hold in relation to Employee Data are considered "special category data" or "sensitive personal data". Since that is the case, in addition to the lawful, fair and transparent data processing outlined in section B3 above, at least one of the following conditions must also be met:

- The Data Subject, in this case the employee, has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the Data Subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the Data Subject);
- The processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
- The processing relates to Personal Data which is clearly made public by the Data Subject;
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the Data Subject;
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
- The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject (in particular, professional secrecy); or
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

D2. Accountability and record keeping

Our Data Protection Officer ('DPO', named above) is responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy and with the GDPR and other applicable data protection legislation, as per section B9 of our Data Protection Policy above.

In the case of Employee Data, our DPO does not have access to the data in question. Access to this data is restricted to HR personnel only and certain senior managers and Directors of the Company.

D3. Personal Data
The Employee Data shall be collected, held, and processed in accordance with this Policy. This includes:

- Identification information relating to employees, including name and contact details;
- Equal opportunities monitoring information (such information shall be anonymised where possible), including age, gender, ethnicity, nationality, religion;

- Health records (see section D4 below), including details of sick leave, medical conditions, disabilities, prescribed medication;
- Employment records, such as interview notes, CVs, application forms, covering letters, performance reviews and similar documents, details of remuneration including salaries, pay increases, bonuses, commission, overtime, benefits, and expenses;
- Employee monitoring information (see section D6 below);
- Records of disciplinary matters including reports and warnings, both formal and informal;
- Details of grievances including documentary evidence, notes from interviews, procedures followed, and outcomes.

D4. Health Records

We hold health records on employee Data Subjects which are used to assess the health, wellbeing, and welfare of employees and to highlight any issues which may require further investigation. In particular, we place a high priority on maintaining health and safety in the workplace, on promoting equal opportunities, and on preventing discrimination on the grounds of disability or other medical conditions. In most cases, health data on employees falls within the GDPR's definition of special category data (see above). Any and all data relating to employee health, therefore, will be collected, held, and processed strictly in accordance with the conditions for processing special category personal data, as set out in section D1 of this Policy. No special category personal data will be collected, held, or processed without the relevant employee data subject's express consent.

Health records shall be accessible and used only by HR personnel and shall not be revealed to other employees, agents, contractors, or other parties working on our behalf without the express consent of the employee to whom such data relates, except in exceptional circumstances where the wellbeing of the employee to whom the data relates is at stake and such circumstances satisfy one or more of the conditions set out in section D2 above.

Health records will only be collected, held, and processed to the extent required to ensure that employees are able to perform their work correctly, legally, safely, and without unlawful or unfair impediments or discrimination.

Employees have the right to request that we do not keep health records about them. All such requests must be made in writing and addressed to the HR Department.

D5. Benefits

In cases where employees are enrolled in benefit schemes which are provided by the Company, it may be necessary from time to time for third party organisations to collect Employee Data from relevant employee Data Subjects.

Prior to the collection of such data, employee Data Subjects will be fully informed of the Employee Data that is to be collected, the reasons for its collection, and the way(s) in which it will be processed.

We shall not use any such Employee Data except insofar as is necessary in the administration of the relevant benefits schemes.

D6. Employee Monitoring

We may from time to time monitor the activities of employees. Such monitoring may include, but will not necessarily be limited to, internet and email monitoring. In the event that monitoring of any kind is to take place (unless exceptional circumstances, such as the investigation of criminal activity or a matter of equal severity, justify covert monitoring), employee Data Subjects will be informed of the exact nature of the monitoring in advance.

Monitoring should not (unless exceptional circumstances justify it, as above) interfere with an employee's normal duties.

Monitoring will only take place if we consider that it is necessary to achieve the benefit it is intended to achieve. Personal data collected during any such monitoring will only be collected, held, and processed for reasons directly related to (and necessary for) achieving the intended result and, at all times, in accordance with the employees' rights and our obligations under the GDPR.

We will ensure that there is no unnecessary intrusion upon employees' personal communications or activities, and under no circumstances will monitoring take place outside of an employee's normal place of work or work hours, unless the employee in question is using Company equipment or other facilities including, but not limited to, Company email, the Company intranet, or a virtual private network ('VPN') service provided by the Company for employee use.

D7. Data Security

As discussed in section D2 above, direct access to Employee Data is restricted to specific personnel, such as the HR Department and other senior members of our management team. The security measures outlined in section B21 of our Data Protection Policy above will be adhered to, with the additional technical instruments provided by our servers which restrict access to authorised personnel only.

E. Cookies

E.1 About This Cookie Policy

This cookie policy explains what cookies are and how we use them on our website. You should read this policy so you can understand what type of cookies we use, the information we collect using the cookies and how that information is used. By using our website you are agreeing that we can use cookies in accordance with this policy.

E2. What are cookies?

Cookies are files which contain a small amount of information. Cookies are stored on the browser or hard drive of your computer or device.

E3. How do we use cookies?

We use cookies to distinguish you from other users of our website and to provide a browsing experience that is unique to you. Cookies are used by us so that our website can remember what you have done whilst browsing, for instance, which pages you have visited.

E4. What type of cookies do we use?

Cookies can be in the form of session cookies or persistent cookies. Session cookies are deleted from your computer or device when you close your web-browser. Persistent cookies will remain stored on your computer or device until deleted or until they reach their expiry date.

We use the following cookies:

- Analytical/performance cookies. These cookies allow us to recognise and count the number of visitors to our website and to see how visitors move around when they are using it. This helps us to improve the way our website works, for example, by ensuring that users find what they are looking for easily.
- Functionality cookies. These cookies are used to recognise you when you return to our website. This enables us to personalise our content for you should we wish to do so, such as greeting you by name and remembering your preferences.
- Targeting cookies. These cookies record your visit to our website, the pages you have visited and the links you have followed. We can use this information to make our website and, where appropriate, any advertising displayed on it more relevant to your interests. We may also share this information with third parties for this purpose. These cookies allow you to share and send information to other websites.

E5. What kind of information do we collect by using cookies?

When you visit our website, we may automatically collect the following types of information from you: Your internet protocol (IP) address, time zone setting, operating system and platform, information about your visits including the URL you came from, your country, the search terms you used in our website, pages you viewed or searched, page response times, download errors, length of visits to certain pages, page interaction information, (such as scrolling, clicks, and mouse-overs) and the methods used to browse away from the page.

E6. How do you block cookies?

Most browsers allow you to refuse cookies. You may block our cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. You can find out more about cookies and how to delete and control them on www.aboutcookies.org or click help in your browser menu.

If you block our use of cookies, you may be unable to access certain areas of our website and certain functions and pages will not work in the usual way.

E7. How we can change the Cookie Policy

We may update this policy from time to time. Changes in technology, legislation and authorities' guidance may require us to inform you of the activities we undertake where it affects your privacy rights. The latest version of this policy will always be displayed on our website and you can check that page at any time to ensure you are familiar with any changes that have been made.

F. Implementation of Policy

This Data Policy and the individual policies and procedures outlined herein shall be deemed effective as of 1 July 2020. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Josef O’Connor, Data Protection Officer.