CSO ALLIANCE LIMITED

PERSONAL DATA PROTECTION COMPLIANCE MANUAL

HENRY & CO.

CONTENTS

SCHEDULE

Schedule 1 Introduction

1. INTRODUCTION

1.1 CSO Alliance Limited (**CSO Alliance**) is a company registered in England and Wales under company number 08319882 whose registered office is at The Mill, Quainton Road, Waddeson, Aylesbury, Buckinghamshire, England HP18 0LP.

1.2 CSO Alliance is required under EU law, to comply with, *inter alia*, the General Data Protection Regulation 2016/679 (the **Regulation**) and the ePrivacy Directive 2002/58 as amended in 2009 (the ***e*PD**).

1.3 This Personal Data Compliance Manual (the **DPM**) sets out the main policies and procedures that govern CSO Alliance 's processing of personal data under the general law, and by particular reference to the Regulation and the *e*PD.

1.4 Article 25 of the Regulation requires companies to introduce privacy by design and default. Directors and trustees of CSO Alliance should have the requisite degree of knowledge of the application of privacy by design and default.

1.5 Employees of CSO Alliance should be familiar with the Regulation and the ePD, to the extent it applies to them.

1.6 Any questions you may have with regard to its contents or what you have to do to comply with it should be referred to your line manager or, where the business has one, CSO Alliance 's data protection officer (**DPO**).

1.7 The policies and procedures set out in this DPM apply to all staff unless otherwise indicated.

2. RESPONSIBILITY FOR THE PERSONAL DATA COMPLIANCE MANUAL

2.1 The Managing Director of CSO Alliance has overall responsibility for this DPM and for ensuring that its policies and procedures comply with CSO Alliance 's legal obligations.

2.2 The DPM is reviewed regularly to ensure that its provisions continue to meet CSO Alliance's legal obligations and reflect best practice.

2.3 Everyone should ensure that they take the time to read and understand the content of this manual and act in accordance with its aims and objectives.

2.4 Managers must ensure all staff understand the standards of behaviour expected of them and to take action when behaviour falls below those requirements.

3. CONTACT

Where you have any questions or concerns regarding compliance with this manual and with data protection laws in general, please contact your line manager in first instance.

Schedule 2 Communications Procedure

COMMUNICATIONS PROCEDURE

CSO ALLIANCE LIMITED

1. SCOPE

1.1 CSO Alliance Limited (**CSO Alliance**) will identify the GDPR Owner. The GDPR Owner is responsible for GDPR compliance matters, with the close attention of the directors of CSO Alliance.

1.2 All internal and external communications related to personal data, data breaches, GDPR compliance or any other topic related to data protection by CSO Alliance is within the scope of this procedure.

1.3 Where relevant, CSO Alliance 's policies, procedures and work instructions may determine the requirements for specific internal or external communications. Where this is the case, those documents supersede the procedure below.

2. RESPONSIBILITIES

2.1 The GDPR Owner is responsible for:

2.1.1 identifying any necessary internal/external communications relating to GDPR compliance including when internal or external communication are necessary;

2.1.2 identifying requirements for internal and external communications and scheduling any necessary regular internal communications relevant to the GDPR; and

2.1.3 determining requirements for external communications and approving external communications.

3. INTERNAL COMMUNICATIONS

3.1 The GDPR Owner will identify the necessity for internal communication based on ongoing compliance requirements.

3.2 The directors and trustees will identify the appropriate audience for the communication according to the following conditions:

3.2.1 classification of the information being communicated;

3.2.2 need-to-know;

3.2.3 the medium of communication; and

3.2.4 any other matter consistent with GDPR compliance.

3.3 The relevant director will draft the communication as appropriate.

4. EXTERNAL COMMUNICATIONS

4.1 The GDPR Owner will identify the necessity for external communication based on the ongoing compliance requirements of CSO Alliance.

4.2 The GDPR Owner will establish the content of the communication according to the following conditions:

4.2.1 cause for the communication;

4.2.2 classification of the information being communicated;

4.2.3 classification of related information; and

4.2.4 additional matters as necessary.

4.3 The GDPR Owner will identify the appropriate audience for the communication according to the following conditions:

4.3.1 cause for the communication;

4.3.2 classification of the information being communicated;
4.3.3 contractual, statutory or regulatory obligations;
4.3.4 the medium of communication (e.g. email, staff room notice, mandatory signed notification, etc.); and
4.3.5 additional matters as necessary.

4.4 The GDPR Owner will compose the communication as appropriate, in accordance with CSO Alliance 's style guide for external communications.
4.5 The communication is subject to review and approval by the directors and trustees of CSO Alliance, and as necessary, subject to legal advice.

5 DOCUMENT CONTROL

The responsibility for the content of this document is with the directors and trustees of CSO Alliance.

Schedule 3 Personal Data Breach Notification Procedure

PERSONAL DATA BREACH NOTIFICATION PROCEDURE

CSO ALLIANCE LIMITED

1. SCOPE

1.1 This procedure applies in the event of a personal data breach described in Article 33 of GDPR: *Notification of a personal data breach to the supervisory authority*; and Article 34: *Communication of a personal data breach to the data subject*.

1.2 The GDPR draws a distinction between a 'data controller' and a 'data processor' to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility.

1.3 To comply with its obligations below, each organisation should establish whether it is data controller or a data processor for the same data processing activity; or whether it is a joint controller.

1.4 The CSO Alliance GDPR Owner is responsible for GDPR compliance matters, with the close attention of the directors and trustees of CSO Alliance.

2. RESPONSIBILITY

2.1 All users (whether trustees, directors, employees, contractors or temporary workers and third-party users) and shareholders of CSO Alliance are required to be aware of and follow this procedure in the event of a personal data breach.

2.2 All CSO Alliance employees, contractors or temporary personnel are responsible for reporting any personal data breach to the GDPR Owner.

3. PROCEDURE – BREACH NOTIFICATION DATA PROCESSOR TO DATA CONTROLLER

3.1 As a data processor, CSO Alliance, acting through the GDPR Owner, will report any personal data breach or security incident to the data controller *without undue delay* and provide the controller with all of the details of the breach.

3.2 The breach notification should be acknowledged by the data controller, provided by email and as necessary, in writing.

4. PROCEDURE – BREACH NOTIFICATION DATA CONTROLLER TO SUPERVISORY AUTHORITY

4.1 CSO Alliance will assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.

4.2 As a result of its evaluation, CSO Alliance will determine if the supervisory authority needs to be notified.

4.3 Acting through the GDPR Owner, CSO Alliance will report the personal data breach to the supervisory authority without undue delay and not later than 72 hours after it becomes aware of the breach.

4.4 If the data breach notification to the supervisory authority is not made within 72 hours, CSO Alliance will submit it electronically with a justification for the delay.

4.5 If it is not possible to provide the necessary information at the same time CSO Alliance will provide the information in phases without undue further delay.

4.6 The following information needs to be provided to the supervisory authority:

- 4.6.1 a description of the nature of the breach;
- 4.6.2 the categories of personal data affected;
- 4.6.3 approximate number of data subjects affected;
- 4.6.4 approximate number of personal data records affected;

4.6.5 name and contact details of the director with responsibility;
4.6.6 consequences of the breach;
4.6.7 any measures taken to address the breach; and
4.6.8 any information relating to the data breach.

4.7 The GDPR Owner will undertake the breach notification by suitable media, including email and telephone; and ensure that receipt is provided by email and as necessary, in writing.

5. PROCEDURE – BREACH NOTIFICATION DATA CONTROLLER TO DATA SUBJECT

5.1 If the personal data breach is likely to result in *high risk* to the rights and freedoms of the data subject, CSO Alliance will notify those/the data subjects affected immediately.
5.2 The notification to the data subject describes the breach in clear and plain language.
5.3 CSO Alliance takes measures to render the personal data unusable to any person who is not authorised to access it.
5.4 The data controller will take subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are managed and reduced.
5.5 If the breach affects a high volume of data subjects and personal data records, CSO Alliance will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder CSO Alliance 's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner.
5.6 If CSO Alliance has not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, CSO Alliance will communicate the data breach to the data subject.
5.7 CSO Alliance will document any personal data breaches, incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

6. DOCUMENT CONTROL

6.1 The responsibility for the content of this document is with the GDPR Owner.

Schedule 4 Data Protection and Privacy Policy

DATA PROTECTION AND PRIVACY POLICY

CSO ALLIANCE LIMITED

1. INTRODUCTION

1.1 The General Personal Data Protection Regulation 2016 (the **Regulation**) replaces the EU Personal Data Protection Directive of 1995. It supersedes the laws of individual Member States developed in compliance with the Personal Data Protection Directive 95/46/EC.

1.2 Defined terms used in this Policy Statement are set out in the Appendix.

2. POLICY STATEMENT

2.1 The Directors, trustees and management of CSO Alliance are committed to compliance with all relevant EU and Member State laws in respect of Personal Data, and the protection of the "rights and freedoms" of individuals whose information CSO Alliance collects and processes in accordance with Regulation.

2.2 Compliance with the Regulation is described by this policy and other relevant policies such as CSO Alliance 's information security policy along with connected processes and procedures.

2.3 The Regulation and this policy apply to all CSO Alliance's Personal 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 The GDPR Owner is responsible for reviewing the Processing register annually to evaluate any changes to CSO Alliance 's activities (as determined by changes to the Personal Data inventory register and the management review.

2.5 This register will be available on the supervisory authority's request.

2.6 This policy applies to all Employees of CSO Alliance and may apply to others. Any breach of the Regulation should be dealt with under CSO Alliance 's disciplinary policy.

2.7 No Third Party may access Personal Data held by CSO Alliance without having first entered into a confidentiality agreement which imposes on the Third Party, obligations no less onerous than those to which CSO Alliance is committed, and which gives CSO Alliance the right to audit compliance with the agreement.

3. RESPONSIBILITIES AND ROLES

3.1 The CSO Alliance is a Data Controller and a Personal Data Processor under the Regulation.

3.2 All of those in managerial or supervisory roles throughout CSO Alliance are responsible for good information handling practices within CSO Alliance.

3.3 The GDPR Owner is a member of the management team and is accountable for the management of Personal Data within CSO Alliance and for ensuring that compliance with Personal Data protection legislation and good practice can be demonstrated. This accountability includes:

- 3.3.1 development and implementation of the Regulation as required by this policy; and
- 3.3.2 security and risk management in relation to compliance with the policy.

3.4 The GDPR Owner has been appointed to take responsibility for CSO Alliance 's compliance with this policy on a day-to-day basis and has direct responsibility for ensuring that CSO Alliance complies with the Regulation.

3.5 The GDPR Owner has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees/Staff seeking clarification on any aspect of Personal Data protection compliance.

3.6 Compliance with Personal Data protection legislation is the responsibility of all Employees/Staff of CSO Alliance who process Personal Data.

3.7 CSO Alliance 's Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of CSO Alliance generally.

3.8 Employees/Staff of CSO Alliance are responsible for ensuring that any Personal Data about them and supplied by them to CSO Alliance is accurate and up-to-date.

4. DATA PROTECTION PRINCIPLES

4.1 All Processing of Personal Data must be conducted in accordance with the Personal Data protection principles as set out in Article 5 of the Regulation. The CSO Alliance 's policies and procedures are designed to ensure compliance with the principles, which are described below:

4.2 **Personal Data must be processed lawfully, fairly and transparently**

Lawful – identify a lawful basis before you can process Personal Data. These are often referred to as the "conditions for Processing".

Fairly – for Processing to be fair, the Data Controller has to make certain information available to the Data Subjects as practicable. This applies whether the Personal Data was obtained directly from the Data Subjects or from other sources.

Transparently – the Regulation includes rules on giving privacy information to Data Subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the Data Subject in an intelligible form using clear and plain language.

4.3 The specific information that must be provided to the Data Subject must, as a minimum, include:

4.3.1 the identity and the contact details of the Data Controller and, if any, of the Data Controller's representative;

4.3.2 the contact details of the Data Protection Officer (if there is one);

4.3.3 the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;

4.3.4 the period for which the Personal Data will be stored;

4.3.5 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;

4.3.6 the categories of Personal Data concerned;

4.3.7 the recipients or categories of recipients of the Personal Data, where applicable;

4.3.8 where applicable, that the Data Controller intends to transfer Personal Data to a recipient in a third country and the level of protection afforded to the Personal Data; and

4.3.9 any further information necessary to guarantee fair Processing.

4.4 **Personal Data can only be collected for specific, explicit and legitimate purposes**

Personal Data obtained for specified purposes must not be used for a purpose that differs from those purposes.

4.5 **Personal Data must be adequate, relevant and limited to what is necessary for Processing**

4.5.1 The GDPR Owner is responsible for ensuring that CSO Alliance does not collect information that is not strictly necessary for the purpose for which it is obtained.

4.5.2 All Personal Data collection forms (electronic or paper-based), including Personal Data collection requirements in new information systems, must be include a fair Processing statement or link to privacy statement and approved by the GDPR Owner.

4.5.3 The GDPR Owner will ensure that, on an annual basis all Personal Data collection methods are reviewed by an internal auditor to ensure that collected Personal Data continues to be adequate, relevant and not excessive.

4.6 **Personal Data must be accurate and kept up to date**

4.6.1 Personal Data that is stored by the Data Controller must be reviewed and updated as necessary. No Personal Data should be kept unless it is reasonable to assume that it is accurate.

4.6.2 The GDPR Owner is responsible for ensuring that all staff are trained in the importance of collecting accurate Personal Data and maintaining it.

4.6.3 It is also the responsibility of the Data Subject to ensure that Personal Data held by CSO Alliance is accurate and up to date. Completion of a registration or application form by a Data Subject will include a statement that the Personal Data contained therein is accurate at the date of submission.

4.6.4 Employees are required to notify CSO Alliance of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of CSO Alliance to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.6.5 The GDPR Owner 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 Personal Data collected, the speed with which it might change and any other relevant factors.

4.6.6 On at least an annual basis, the GDPR Owner will review the retention dates of all the Personal Data processed by CSO Alliance, by reference to the Personal Data inventory, and will identify any Personal Data that is no longer required in the context of the registered purpose.

4.6.7 The GDPR Owner is responsible for responding to requests for rectification from Data Subjects within one month (commonly known as a Subject Access Request or SAR). This can be extended to a further two months for complex requests.

4.6.8 If CSO Alliance decides not to comply with the request, GDPR Owner 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.

4.6.9 The GDPR Owner is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date Personal Data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the Personal Data to the Third Party where this is required.

4.7 **Personal Data must be kept in a form such that the Data Subject can be identified only as long as is necessary for Processing.**

4.7.1 Personal Data will be retained in line with the Retention of Records Procedure and once its retention date is passed, it must be securely destroyed as set out in this procedure.

4.7.2 The GDPR Owner must specifically approve any Personal Data retention that exceeds the retention periods defined in Retention of Records Procedure and

must ensure that the justification is clearly identified and in line with the requirements of the Personal Data protection legislation. This approval must be written.

4.8 **Personal Data must be processed in a manner that ensures appropriate security**

4.8.1 The GDPR Owner will carry out a risk assessment taking into account all the circumstances of CSO Alliance 's controlling or Processing operations.

4.8.2 In determining appropriateness, the GDPR Owner 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 CSO Alliance itself, and any likely reputational damage including the possible loss of customer trust.

4.8.3 When assessing appropriate technical measures, the GDPR Owner may 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; and
- Identifying appropriate international security standards relevant to CSO Alliance.

4.9 When assessing appropriate organisational measures, the GDPR Owner will consider the following:

4.9.1 The appropriate training levels throughout CSO Alliance;
4.9.2 Measures that consider the reliability of employees (references for example);
4.9.3 The inclusion of Personal Data protection in employment contracts;
4.9.4 Identification of disciplinary action measures for Personal Data breaches;
4.9.5 Monitoring of staff for compliance with relevant security standards;
4.9.6 Physical access controls to electronic and paper-based records;
4.9.7 Adoption of a clear desk policy;
4.9.8 Storing of paper based Personal Data in lockable fire-proof cabinets;
4.9.9 Restricting the use of portable electronic devices outside of the workplace;
4.9.10 Restricting the use of employee's own personal devices being used in the workplace;
4.9.11 Adopting clear rules about passwords;
4.9.12 Making regular backups of Personal Data and storing the media off-site; and
4.9.13 The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring Personal Data outside the EEA.

These controls have been selected on the basis of identified risks to Personal Data, and the potential for damage or distress to individuals whose Personal Data is being processed.

4.10 **The Data Controller must be able to demonstrate compliance with the Regulation's other principles (accountability)**

4.10.1 The Regulation includes provisions that promote accountability and governance. These complement the Regulation's transparency requirements. The accountability principle in Article 5(2) requires CSO Alliance to demonstrate that it complies with the principles and states explicitly that this is CSO Alliance 's responsibility.

4.10.2 The CSO Alliance will demonstrate compliance with the Personal Data protection principles by implementing Personal Data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as Personal Data protection by design, DPIAs, breach notification procedures and incident response plans.

5. DATA SUBJECTS' RIGHTS

5.1 Data subjects have the following rights regarding Personal Data Processing, and the Personal Data that is recorded about them:

5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed;
5.1.2 To prevent Processing likely to cause damage or distress;
5.1.3 To prevent Processing for purposes of direct marketing;
5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them;
5.1.5 To not have significant decisions that will affect them taken solely by automated process;
5.1.6 To sue for compensation if they suffer damage by any contravention of the Regulation;
5.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate Personal Data;
5.1.8 To request the supervisory authority to assess whether any provision of the Regulation has been contravened;
5.1.9 To have Personal Data provided to them in a structured, commonly used and machine-readable format, and the right to have that Personal Data transmitted to another Data Controller; and
5.1.10 To object to any automated Profiling that is occurring without consent.

5.2 The CSO Alliance ensures that Data Subjects may exercise these rights:

5.2.1 Data Subjects may make Personal Data access requests as described in Subject Access Request Procedure; this procedure also describes how CSO Alliance will ensure that its response to the Personal Data access request complies with the requirements of the Regulation; and
5.2.2 Data Subjects have the right to complain to CSO Alliance related to the Processing of their Personal Data, the 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.

6. CONSENT

6.1 The CSO Alliance 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.

6.2 The CSO Alliance 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.

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

6.4 For Sensitive Personal Data, explicit written consent must be obtained unless an alternative legitimate basis for Processing exists.

6.5 Where CSO Alliance provides online services to a Child, parental or custodial authorisation must be obtained.

7. SECURITY OF DATA

7.1 All Employees are responsible for ensuring that any Personal Data that CSO Alliance 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 CSO Alliance to receive that information and subject to a confidentiality undertaking.

7.2 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees of CSO Alliance. All Employees 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.

7.3 Personal Data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste.'

8. DISCLOSURE OF DATA

8.1 The CSO Alliance 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.

8.2 All Employees/Staff should exercise caution when asked to disclose Personal Data held on another individual to a Third Party.

8.3 All requests to provide Personal Data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the GDPR Owner.

9. RETENTION AND DISPOSAL OF DATA

9.1 The CSO Alliance will not keep Personal Data in a form that permits identification of Data Subjects for longer a period than is necessary, in relation to the purpose(s) for which the Personal Data was originally collected.

9.2 The CSO Alliance may store Personal 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.

9.3 The retention period for each category of Personal Data will be set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations CSO Alliance has to retain the Personal Data.

9.4 The CSO Alliance 's Personal Data retention and Personal Data disposal procedures will apply in all cases.

9.5 Personal Data must be disposed of securely in accordance with the sixth principle of the Regulation i.e. processed in an appropriate manner to maintain security, thereby

protecting the "rights and freedoms" of Data Subjects. Any disposal of Personal Data will be done in accordance with the secure disposal procedure.

10. DATA TRANSFERS

10.1 All exports of Personal Data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the Regulation as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the Data Subjects".

10.2 The transfer of Personal Data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

10.2.1 *An adequacy decision*: The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required. Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision. A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union: http://ec.europa.eu/justice/PersonalData-protection/international-transfers/adequacy/index_en.htm

10.2.2 *Privacy Shield*: If CSO Alliance wishes to transfer Personal Data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the Personal Data according to a strong set of Personal Data protection rules and safeguards. The protection given to the Personal Data applies regardless of whether the Personal Data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use Personal Data from the EU under that framework.

10.2.3 *Assessment of adequacy by the Data Controller:* In making an assessment of adequacy, the UK based exporting Data Controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the Personal Data in the overseas location.

10.3 *Binding corporate rules*: The CSO Alliance may adopt approved binding corporate rules for the transfer of Personal Data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that CSO Alliance is seeking to rely upon.

10.4 *Model contract clauses*: CSO Alliance may adopt approved model contract clauses for the transfer of Personal Data outside of the EEA. If CSO Alliance adopts the model

contract clauses approved by the relevant supervisory authority there is an automatic recognition of adequacy.

10.5 *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 will only take place on one of the following conditions:

10.5.1 the Data Subject 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;

10.5.2 the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken at the Data Subject's request;

10.5.3 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and another natural or legal person;

10.5.4 the transfer is necessary for important reasons of public interest;

10.5.5 the transfer is necessary for the establishment, exercise or defence of legal claims; and/or

10.5.6 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.

11. INFORMATION ASSET REGISTER/DATA INVENTORY

11.1 CSO Alliance has established a Personal Data inventory and Personal Data flow process as part of its approach to address risks and opportunities throughout its Regulation compliance project.

11.2 CSO Alliance's Personal Data inventory and Personal Data flow determines:

11.2.1 business processes that use Personal Data;

11.2.2 source of Personal Data;

11.2.3 volume of Data Subjects;

11.2.4 description of each item of Personal Data;

11.2.5 Processing activity;

11.2.6 maintains the inventory of Personal Data categories of Personal Data processed;

11.2.7 documents the purpose(s) for which each category of Personal Data is used;

11.2.8 recipients, and potential recipients, of the Personal Data;

11.2.9 the role of CSO Alliance throughout the Personal Data flow;

11.2.10 key systems and repositories;

11.2.11 any Personal Data transfers; and

11.2.12 all retention and disposal requirements.

11.3 CSO Alliance is aware of any risks associated with the Processing of particular types of Personal Data:

11.3.1 CSO Alliance assesses the level of risk to individuals associated with the Processing of their Personal Data. Personal Data protection impact assessments (DPIAs) are carried out in relation to the Processing of Personal Data by CSO Alliance , and in relation to Processing undertaken by other organisations on behalf of CSO Alliance.

11.3.2 CSO Alliance will manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

11.3.3 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, CSO Alliance will, 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.

11.3.4 Where, as a result of a DPIA it is clear that CSO Alliance is about to commence Processing of Personal Data that could cause damage and/or distress to the Data Subjects, the decision as to whether or not CSO Alliance may proceed must be escalated for review to the GDPR Owner.

11.3.5 The GDPR Owner will, if there are significant concerns, either as to the potential damage or distress, or the quantity of Personal Data concerned, escalate the matter to the supervisory authority.

11.3.6 Appropriate controls will be selected a suitable security standard and applied to reduce the level of risk associated with Processing Personal Data to an acceptable level, by reference to CSO Alliance ’s risk acceptance criteria and the requirements of the Regulation.

12. DOCUMENT CONTROL

The responsibility for the content of this document is with the GDPR Owner.

APPENDIX

DEFINED TERMS OR SUMMARY EXPLANATIONS USED IN THIS POLICY

Child: the Regulation defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The Processing of Personal Data of a child is only lawful if parental or custodian consent has been obtained. The Data Controller will make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.
CSO Alliance: CSO Alliance Limited, a company registered in England and Wales under company number 08319882 whose registered office is at The Mill, Quainton Road, Waddeson, Aylesbury, Buckinghamshire, England HP18 0LP.
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; where the purposes and means of such Processing are determined by Union or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Processor: a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.
Data Protection Officer: the person or persons appointed by CSO Alliance in a formal capacity to ensure compliance with the Regulation.
Data Subject: any living individual who is the subject of Personal Data held by an organisation.
Data Subject Consent: 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.
Establishment: the main establishment of the Data Controller in the EU will be the place in which the Data Controller makes the main decisions as to the purpose and means of its Personal Data Processing activities. The main establishment of a processor in the EU will be its administrative centre. If a Data Controller or Data Processor is based outside the EU, it will have to appoint a representative in the jurisdiction in which the Data Controller or Data Processor operates to act on behalf of the Data Controller and deal with supervisory authorities.
Filing system: any structured set of Personal Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
GDPR Owner: the Data Protection Officer or in the absence of a Data Protection Officer the person or persons responsible for compliance with Regulation.
Material Scope (Article 2): the Regulation applies to the Processing of Personal Data wholly or partly by automated means (i.e. by computer) and to the Processing other than by automated means of Personal Data (i.e. paper records) that form part of a Filing System or are intended to form part of a Filing System.
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 Personal 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.
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. There is an obligation on the Data Controller to report Personal Data breaches to the supervisory authority and where the breach is likely to adversely affect the Personal Data or privacy of the Data Subject.
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.

Profiling: is any form of automated Processing of Personal Data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the Data Subject to object to Profiling and a right to be informed about the existence of Profiling, of measures based on Profiling and the envisaged effects of Profiling on the individual.

Sensitive Personal Data: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the Processing of genetic Personal Data, biometric Personal Data for the purpose of uniquely identifying a natural person, Personal Data concerning health or Personal Data concerning a natural person's sex life or sexual orientation.

Territorial Scope (Article 3): the Regulation will apply to all Data Controllers that are established in the EU (European Union) who process the Personal Data of Data Subjects, in the context of that Establishment. It will also apply to Data Controllers outside of the EU that process Personal Data in order to offer goods and services or monitor the behaviour of Data Subjects who are resident in the EU.

Third Party: a natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, processor and persons who, under the direct authority of the Data Controller or processor, are authorised to process Personal Data.

Schedule 5 Training Policy

TRAINING POLICY

CSO ALLIANCE LIMITED

1. SCOPE

1.1 This policy applies to the training and awareness programme of CSO Alliance and where relevant to the GDPR, compliance with the GDPR and other matters relating to data protection and privacy.

1.2 CSO Alliance will identify the GDPR Owner; who will be responsible for GDPR compliance matters, with the close attention of the directors of CSO Alliance or organisation.

2. TRAINING POLICY

2.1 CSO Alliance assigns data protection responsibilities to its employees in relation to CSO Alliance 's policies and procedures on personal data management.

2.2 The GDPR Owner will ensure that all employees with day-to-day responsibilities involving personal data and processing operations, and those with permanent/regular access to personal data, demonstrate compliance with the GDPR.

2.3 Employees of CSO Alliance will be able to demonstrate competence in their understanding of the GDPR, how this is practised and implemented throughout CSO Alliance.

2.4 The GDPR Owner will ensure that employees are kept up to date and informed of any issues related to personal data.

2.5 The GDPR Owner will promote training and awareness programmes, and CSO Alliance will make resources available to raise awareness. The GDPR Owner will demonstrate and communicate to employees the importance of data protection in their role and ensure that they understand how and why personal data is processed in accordance with CSO Alliance 's policies and procedures.

2.6 The GDPR Owner will ensure that all security requirements related to data protection are demonstrated and communicated to employees to the same affect.

2.7 Employees will be provided with specific training on processing personal data relevant to their individual day-to-day roles and responsibilities, and in accordance with CSO Alliance 's policies and procedures.

2.8 Employees will be provided with specific training on any information security requirements and procedures applicable to data protection and the data processing within their individual day-to-day roles and responsibilities, including reporting personal data breaches.

2.9 Employees will be provided with training on dealing with complaints relating to data protection and processing personal data.

2.10 The CSO Alliance will retain records of the relevant training undertaken by each person who has this level of responsibility.

2.11 The GDPR Owner will assess its personal data management system and its capability to demonstrate compliance to the GDPR.

2.12 The GDPR Owner is responsible for organising relevant training for all responsible individuals and employees generally, and for maintaining records of the attendance of staff at relevant training at appropriate times across CSO Alliance 's business cycle.

3. DOCUMENT OWNER AND APPROVAL

3.1 The GDPR Owner is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

Schedule 6 External Privacy Notice

CSO ALLIANCE LIMITED: PRIVACY NOTICE

This is the privacy notice for CSO Alliance Limited (and the Maritime Cyber Alliance). This privacy notice sets out the basis on which any personal data We collect from you, or that you provide to us, directly or indirectly will be processed by us. Please read the following carefully to understand our views and practices regarding personal data and how We treat it.

CSO Alliance Limited is a company registered in England and Wales under company number 08319882 whose registered office is at The Mill, Quainton Road, Waddeson, Aylesbury, Buckinghamshire, England HP18 0LP.

For the purpose of the General Data Protection Regulation 16/679 the data controller is CSO Alliance Limited. We can be contacted at the registered office address or info@csoalliance.com

WHO WE ARE

CSO Alliance is a community of company security officers tasked with defending over 50,000 merchant marine assets with over 1.2 million crew, from criminality. CSO Alliance collects and aggregates data isolating criminal activity and trends to ensure that all chief security officers who are members (hereafter referred to as 'Clients') can fully brief their captains and crew as to the risks they face, wherever they sail.

OUR STATUS UNDER GDPR

Depending on the nature of the interaction, we act as a processor in that we are acting upon instructions from our Clients when we provide our services to them; and when we control the purposes and means of the processing of personal data, such as processing our employee's personal data, we are a controller, as defined under the Regulation.

THE PERSONAL DATA WE COLLECT ABOUT YOU

We collect personal data for a number of purposes in order to undertake our business model. This includes the collection of personal data which identifies you when you sign up to our mailing list, become a member or communicate with us. If you make a purchase or sign up for an event we maintain a record of your history. If you share any access requirements or other special requirements with us we will note this in your record on our contact management system, Capsule CRM. We keep a record of the emails we send you, and we may track whether you receive or open them so we can make sure we are sending you the most relevant information. When we collect personal data from you we store it under a strict safeguarding and confidentiality regime.

THE REASON WE USE PERSONAL DATA

CSO Alliance will collect data from you to process payments, our member experience and provide you with information or services you have requested, to meet contractual requirements and comply with our administrative duties, sectoral regulations and the general law. Personal data collected this way will only be used to provide you with information that you would reasonably expect or have agreed to. When we run activities in partnership with other organisations we will only share your personal data with them if your consent is required, and you have given us consent to do so. We do not share or sell your personal data with other organisations to use for their own purposes without your agreement. We may pass your personal data on to third-party service providers contracted to us. In these circumstances, the third party

will be obliged to keep your details securely, and to use them only to fulfil their contractual obligations to us. When they no longer need your personal data to fulfil this service, they will dispose of the details in line with our data retention policy.

Personal data, including in your capacity as a member of CSO Alliance, will be held on a customer relationship management system which holds contact details and a record of your interactions with us. Where possible we aim to keep a single record for each member. Where you apply for employment at CSO Alliance and are unsuccessful, we delete your records in line with our data retention policy.

SHARING INFORMATION

As set out above, we may share information with third parties so that they can assist us in providing our services; selected third parties could include:

- Clients, suppliers and sub-contractors for the performance of any contract we enter into with them. For example, so that our platform can work effectively, we may engage with contractors to carry out part of our services.
- Analytics and search engine providers that assist us in the improvement and optimisation of our site.

We will disclose your personal information to third parties:

- If CSO Alliance or substantially all of its assets are acquired by a third party, in which case personal data held by it about its Clients will be one of the transferred assets.
- If we are under a duty to disclose or share personal data to comply with any legal obligation, or in order to enforce or apply our terms and other agreements; or to protect the rights, property, or safety of CSO Alliance, our Clients, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

THE LEGAL BASIS UPON WHICH WE ACT

We only process personal information where we have a lawful basis for doing so. These are:

Consent
Where We process personal data as a result of your consent, We ensure that consent is freely given, specific and informed, and established by a clear affirmative act. Where you wish to withdraw your consent, we have set out (below) how you may do this.

Contract Performance
Where We enter into a contract with third parties, processing of personal data may, as a matter of course, be necessary to execute such contract or take pre-contract preparation steps. This can include obligations under our terms and conditions with our members.

Legal Obligations
Where We have legal obligations, processing of personal data may be required by law. This may include contact with our regulators or public institutions.

Legitimate Interest
Where We process personal data as it is necessary for the purpose of our legitimate interests, We do so on the basis of a balanced evaluation of our interests and yours. We may therefore contact you about things which we feel are of interest to you or which, based on what we know about you, are in the interests of our charitable objectives to let you know. This will from time

to time include marketing and raising awareness, but at any stage you can tell us that you do not want to receive such information and we will stop contacting you with it.

WITHDRAWAL OF CONSENT

Consent should be as easy to withdraw as it is to give and you may ask that we do not process your personal data at any time. You may contact us to withdraw your consent using the contact details at the end of this privacy statement. Equally, where we process personal data based on our legitimate interest, you have a right to request that we stop processing personal data for our legitimate interests and withdraw your consent.

HOW WE PROTECT YOUR PERSONAL INFORMATION

We take appropriate physical, electronic and managerial measures to ensure that we keep your information secure, accurate and up to date, and that we only keep it as long as is reasonable and necessary. Any external providers we use to process your data (for instance the operators of our contact management system) must meet our security policies and comply with all relevant legislation about how they store and process your personal data. We may also receive information about you from third parties but will only contact you if we have your express permission.

YOUR RIGHTS TO FURTHER INFORMATION

At your request we will confirm the information We hold about you and how it is processed. You can request the following information:

- Identity and the contact details of the person or organisation that has determined how and why to process your data.
- The purpose of the processing as well as the legal basis for processing.
- If the processing is based on the legitimate interests, information about those interests.
- The categories of personal data collected, stored and processed.
- Recipient(s) or categories of recipients that the data is/will be disclosed to.
- If we intend to transfer the personal data to a third country or international organisation, information about how We ensure this is done securely.
- How long the data will be stored.
- Details of your rights to correct, erase, restrict or object to such processing.
- Information about your right to withdraw consent at any time.
- The source of personal data if it wasn't collected directly from you.
- Any details and information of automated decision making, such as profiling, and any meaningful information about the logic involved, as well as the significance and expected consequences of such processing.

What forms of ID will I need to provide in order to access this?

We accept the following forms of ID when information on your personal data is requested: passport, driving licence, birth certificate, utility bill from the previous 3 months.

SENSITIVE PERSONAL DATA

Where CSO Alliance processes sensitive personal data, we do so on the basis that the Client has established a lawful exception to the prohibition on processing sensitive personal data under Article 9 of the Regulation; and where CSO Alliance is processing sensitive personal data of employees, it does so pursuant to its employment relationship with its personnel and so uses the exception set out in paragraph 2(b) of Article 9 of GDPR.

TRANSFERRING OUT OF THE EEA

Storing: We use cloud providers to store our personal data. Personal data may be transferred to and stored at a destination outside of the European Economic Area (EEA).
Processing: We may use third parties to help us deliver our services and they may be based outside the EEA. Where data is transferred outside the EEA, We adhere to compliance mechanisms that are identified by the European Commission, for example, the use of EU model contract clauses or conformity to US Privacy Shield.
Where we are the processor: in general, personal data is stored in the locations required by our Clients. Periodically, our Clients may agree specific terms as to where customer data, venue employee data and head office employee data is stored by us. At all times, We act in accordance with the Regulation.

DATA RETENTION PERIODS

CSO Alliance has a data retention policy which sets out how long it will store personal data, which is consistent with Article 5 of the Regulation. CSO Alliance only keeps personal data for as long as is necessary. For example, CSO Alliance is required to retain certain information in accordance with the general law, where information needed for income tax and audit purposes. How long certain kinds of personal data should be kept may also be governed by specific business-sector requirements and agreed practices. Personal data may be held in addition to these periods depending on CSO Alliance's business needs, which are balanced against the requirements of GDPR and the rights of the individual.

Where we are the controller
We will retain personal data for as long as necessary. As described above, in some cases, we will have a legal or statutory obligation to retain information for a set period, such as the limitation period.

Where we are the processor
Data is stored as instructed by our Clients in accordance with their approach to retention of personal data provided that this is within GDPR. We recommend you view their Terms of Use and Privacy Policy for more information.

SUMMARY OF DATA PROCESSORS

In order to provide our services to our Clients and their customers, CSO Alliance defines the different categories of personal data and works with carefully selected third parties. Some of our selected third parties are required to process personal data on our behalf, in compliance with our role as both a controller and processor. Our suppliers include Mailchimp, Capsule CRM, Sage, Kashflow, HSBC and Wididi.

CONTACTING YOU

The personal data We process is subject to rigorous measures and procedures to minimize the risk of unauthorized access or disclosure. We will get in touch with the supervisory authority (which in CSO Alliance's case is the Information Commissioner on the United Kingdom) and with affected data subjects where this is required under GDPR.

LINKS TO OTHER WEBSITES

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which

you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

COOKIES

We use cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and allows us to improve our site. By continuing to browse the site, you are agreeing to our use of cookies. A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer if you agree. Cookies contain information that is transferred to your computer's hard drive. We use the following cookies:

Strictly necessary cookies

These are cookies that are required for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website.

Analytical/performance cookies

They allow us to recognize and count the number of visitors and to see how visitors move around our website when they are using it. This helps us to improve the way our website works, for example, by ensuring that users are finding what they are looking for easily

Functionality cookies

These are used to recognize you when you return to our website. This enables us to personalise our content for you, greet you by name and remember your preferences (for example, your choice of language or region)

Targeting cookies

These cookies record your visit to our website, the pages you have visited and the links you have followed. We will use this information to make our website more relevant to your interests.

FIRST PARTY COOKIES

How do I block first party cookies?

You block first party cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our site.

THIRD PARTY COOKIES

We may use Google Analytics cookies to track anonymous usage statistics but we do not collect any personal information that can be used to identify you. This data helps us analyze web page usage and improve our website to tailor it to our audience needs.

Google Analytics stores information about what pages you visit, how long you are on the site, how you got there and what you clicked on.

These are cookies served by a third-party service provider and are usually used to identify your computer when it visits another website, for example, when you log in to a social media site to share an article.

How do I block third party cookies?

You block third party cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our site.

FURTHER INFORMATION

For more information on cookies, go to www.aboutcookies.org

YOUR RIGHT TO COMPLAIN

If you have a complaint about the way we process your personal data, you can register your concern by contacting the Information Commissioner and following the instructions set out at www.ico.org.uk

CONTACT DETAILS

CSO Alliance Limited	
Address:	The Mill, Quainton Road, Waddesdon, Aylesbury, Buckinghamshire, England HP18 0LP FAO Data Protection Owner.
Email:	info@csoalliance.com

Schedule 7 Cookies and Tracking Policies

COOKIES AND TRACKING POLICY

This is the cookies and tracking policy for CSO Alliance Limited (CSO Alliance or We). CSO Alliance Limited.

OUR USE OF COOKIES.

We use cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and allows us to improve our site.

By continuing to browse the site, you are agreeing to our use of cookies. A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer if you agree. Cookies contain information that is transferred to your computer's hard drive. We use the following cookies:

- **strictly necessary cookies**

These are cookies that are required for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website

- **analytical/performance cookies**

These allow us to recognise and count the number of visitors and to see how visitors move around our website when they are using it. This helps us to improve the way our website works, for example, by ensuring that users are finding what they are looking for easily

- **functionality cookies**

These are used to recognise you when you return to our website. This enables us to personalise our content for you, greet you by name and remember your preferences (for example, your choice of language or region)

- **targeting cookies**

These cookies record your visit to our website, the pages you have visited and the links you have followed. We will use this information to make our website more relevant to your interests.

To give you a better experience, we use first-party cookies and third-party cookies. A first party cookie is a cookie that we set when you directly visit our site. A third-party cookie is one that is placed on your device by a site from an address other than directly from us.

FIRST PARTY COOKIES

How do I block first party cookies?

You block first party cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies and following the instructions provided. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our site

THIRD PARTY COOKIES

How do I block third party cookies?

You block third party cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our site.

COOKIES: FURTHER INFORMATION

Learn more about cookies

More information about cookies can be found at: http://www.allaboutcookies.org
Internet Advertising Bureau: Guide to online advertising and privacy
International Chamber of Commerce United Kingdom: ICC UK cookie guide

Changes to cookies policy

Any changes we make to our cookies policy in the future will be posted on this page. Please check back frequently to see any updates or changes to our cookies policy.

Last updated: May 2018

Schedule 8 Internal Privacy Notice

INTERNAL PRIVACY NOTICE

CSO ALLIANCE LIMITED

1. SCOPE

All data subjects whose personal data is collected, in line with the requirements of the GDPR.

2. RESPONSIBILITIES

2.1 The GDPR Owner is responsible for ensuring that this notice is made available to data subjects prior to CSO Alliance collecting/processing their personal data.

2.2 All employees of CSO Alliance who interact with data subjects are responsible for ensuring that this notice is drawn to the data subject's attention and their consent to the processing of their data is secured.

3. PRIVACY NOTICE

3.1 Who are we?

CSO Alliance Limited is a business which facilitates the exchange of travel-critical information between Chief Security Officers in the maritime sector.

3.2 Contact

Our GDPR Owner can be contacted directly here:

CSO Alliance Limited	
Contact Name:	Jo Chuter
Address:	The Mill, Quainton Road, Waddeson, Aylesbury, Buckinghamshire, England HP18 0LP
Email:	info@csoalliance.com

The personal data we would like to process is:

Personal data type:	**Source** (where CSO Alliance obtained the personal data from if it has not been collected directly from you, the data subject. Note if the personal data has been accessed from publicly accessible sources):
Name; address	First party
Tax identification numbers and national insurance number	First party/Third Party
References	Third Party
Any other personal data which is necessary for the performance of your duties	First party/third party

3.3 The Purpose of Collecting Personal Data

The personal data we collect will be used for the following purposes:

1. to establish the suitability of you as an employee of or contractor to the Company
2. to facilitate the payment to you of salary or contractor payments
3. to ensure that tax is deducted at source

3.4 Recipients of the Personal Data We Collect

Personal data will be shared with third party service providers for the purposes of secure retention of personal data under the terms of a data processing agreement in addition to third parties where We are obliged to do so under our general legal obligations (such as the provision of data relating to your tax status in order to deduct income tax from your salary).

3.5 The Legal Basis Under Which We collect Personal Data

The two lawful reasons We use to process personal data are set out in Article 6 of the Regulation. Processing will only be lawful if and to the extent that at least one of the following applies:

1. processing in necessary for compliance with a legal obligation to which the controller is subject (**Compliance**)
2. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (Article 6 (1) (f) (**Legitimate Interest**)

Compliance

We may process personal data where this is necessary for compliance with a legal obligation we are subject to, such as the legal requirement to deduct certain income taxes and national insurance obligations, at source.

Legitimate Interest

Where We process personal data as it is necessary for the purpose of our legitimate interests, We do so on the basis of a balanced evaluation of our interests and the rights and freedoms of the data subject which require protection. Presently, We have concluded that the way We manage the processing of personal data results in a cumulation of data subject protections which show that the balance is in favour of CSO Alliance being able to rely on Article 6.1(f) of the Regulation as a lawful reason to process personal data.

Our Legitimate Interests

It is in our legitimate interests to process your personal data to, amongst other things, facilitate the provision of goods and services to our customers and clients (as the case may be).

Sensitive Personal Data

Where you provide us with sensitive personal data, we may only process this under an exception to the general prohibition set out in Article 9 of GDPR.

1.1 Disclosure

CSO Alliance will periodically disclose your personal data to third parties. The recipients of your personal data are as follows:

1. HMRC; and equivalent state organisations which the Company is legally obligated to engage with
2. Data storage businesses, with whom we have entered into data processing agreements pursuant to the terms of Article 28 GDPR
3. Businesses and organisations which provide email and business efficiency tools, such as Google, with whom we have entered into data processing agreements pursuant to Article 28 GDPR
4. Occasional access, which is limited to the specific needs of the Company, subject at all times to the provisions of Article 5 GDPR

1.2 **Retention period**

The Company will process personal data in accordance with the principles set out in Article 5 GDPR, namely that personal data will only be stored for as long as necessary. Where personal data is not required, it is deleted; where it is not required but may be subject to legal proceedings in the future, personal data is kept pursuant to the appropriate limitation period, namely 6 years. Tax-related data is kept for 7 years. In each case, such personal data will be archived with restricted access.

1.3 **Transfers of Personal Data**

Where CSO Alliance is required to send personal data outside of the European Economic Area, in some cases to jurisdictions which the EU has not deemed to be 'adequate' for the purposes of the Regulation, CSO Alliance will ensure that such transfers are undertaken in a manner consistent with the requirements of the Regulation.

1.4 **Your rights as a data subject**

At any point while we are in possession of or processing your personal data, you, the data subject, have the following rights:

1. Right of access: you have the right to request a copy of the information that we hold about you.
2. Right of rectification: you have a right to correct data that we hold about you that is inaccurate or incomplete.
3. Right to be forgotten: in certain circumstances you can ask for the data we hold about you to be erased from our records.
4. Right to restriction of processing – where certain conditions apply to have a right to restrict the processing.
5. Right of portability: you have the right to have the data we hold about you transferred to another organisation.
6. Right to object: you have the right to object to certain types of processing such as direct marketing.
7. Right to object to automated processing, including profiling: you also have the right to be subject to the legal effects of automated processing or profiling.
8. Right to judicial review: in the event that CSO Alliance refuses your request under rights of access, we will provide you with a reason as to why. You have the right to complain.

All of the above requests will be forwarded on should there be a third party involved in the processing of your personal data.

1.5 **Complaints**

In the event that you wish to make a complaint about how your personal data is being processed by CSO Alliance, or how your complaint has been handled, you have the right to lodge a complaint directly with the supervisory authority and CSO Alliance's data protection representatives GDPR Owner.

The details for each of these contacts are:

	Supervisory authority contact details	**GDPR Owner contact details**
Contact Name:	Information Commissioner	Director, CSO Alliance Limited
Address:	Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number Fax: 01625 524 510	The Mill, Quainton Road Waddeson Aylesbury Buckinghamshire England HP18 0LP

Document Owner and Approval

THE GDPR Owner is the owner of this document.

Schedule 9 Information Security Policy

INFORMATION SECURITY POLICY

CSO ALLIANCE LIMITED

1. SCOPE

1.1. CSO Alliance ensures the security of its information processing facilities and information assets in relation to external parties. All external parties who need to access any organisational information assets are subject to this procedure.

1.2. CSO Alliance has (or may have) external party agreements with the following categories of organisations, all of whom are covered by this procedure. Risks may be assessed for external parties as individual organisations or as categories, depending on the level of risk involved:

- Service providers
- Managed security services
- Customers
- Outsourcing suppliers (facilities, operations, IT systems, data collection, call centres, others)
- Consultants and auditors
- Developers and suppliers of IT systems and services
- Cleaning, catering and other outsourced support services
- Temporary personnel, placement and other (casual) short-term appointments

2. RESPONSIBILITIES

2.1. The GDPR Owner is responsible for services in any of the above categories that include personal data; required to ensure that external parties have entered into a formal external party agreement under this procedure; and will ensure that transfers (of information, information processing facilities, and any other information assets or personnel) are planned and executed without a reduction in the level of security that existed prior to commencement of the transition.

2.2. The GDPR Owner is responsible for ensuring that the security controls, service definitions and delivery levels included in external party agreements are implemented, maintained and operated by the external party.

2.3. The GDPR Owner is responsible for carrying out risk assessments where required by this procedure.

3. PROCEDURE

3.1. Where there is a business need for working with external parties, CSO Alliance will ensure that its information security is not reduced and access to organizational assets is not granted until a risk assessment has been completed, appropriate controls identified and implemented.

4. RISK IDENTIFICATION

4.1. CSO Alliance will carry out a risk assessment to identify risks related to external party access and the possible need to complete a data protection impact assessment.

4.2. The risk assessment identifies and documents, for each external party:

4.2.1. the information processing facilities and information assets the external party will access;

4.2.2. the type of access the third party will have such as physical access and/or logical access (identifying the assets that will be accessed), whether the access is taking place on site or off site and the exact location from which access will be made;

4.2.3. the value and classification of the information that will be accessed;

4.2.4. the information assets that the external party are not intended to access and which may require additional controls to secure;
4.2.5. the external party's personnel, including their contractors and partners, who will or might be involved;
4.2.6. how external party personnel are to be authenticated;
4.2.7. how the external party will process, communicate and store information;
4.2.8. the impact to the external party of access not being available when required, or of inaccurate or misleading information being entered, received or shared;
4.2.9. how CSO Alliance's information security incident management will be extended to incorporate information security incidents involving the external party;
4.2.10. any legal, regulatory or other contractual issues that should be taken into account with respect to the external party; and
4.2.11. how the interests of other stakeholders might be affected by any decisions.

4.3. Controls will be selected in line with the requirements of GDPR.
4.4. CSO Alliance will implement those controls that are within its own power and in line with the requirements of the GDPR.
4.5. Where appropriate, CSO Alliance will agree with the external party those controls that the external party is required to implement and document them in an agreement that the third-party signs. The obligations on the external party include ensuring that all its personnel are aware of their obligations.

5. MANAGING CHANGES TO THIRD-PARTY SERVICES

5.1. CSO Alliance may need to agree changes to external party contracts and agreements to take account of changes that it makes to, or as a result of:

5.1.1. the services it currently offers to its clients and subscribers;
5.1.2. new applications and systems it has developed or acquired;
5.1.3. modifications, changes or updates to its own policies and procedures; and
5.1.4. new or amended controls arising from new risk assessments or information security incidents.

5.2. The external party may need to request changes to the contract to implement:

5.2.1. changes or improvements to their networks or other infrastructure;
5.2.2. new or improved technologies, new products or new releases of current products;
5.2.3. new development tools, methodologies and environments;
5.2.4. new physical locations or physical services; and
5.2.5. new vendors or other suppliers of hardware, software or services.

5.3. Any changes that may be required are subject to a new risk assessment (taking into account the criticality of the business systems involved) and review of the selected controls.

5.4. New controls, or changes to existing controls are identified, authorised, agreed with the third party, and made the subject of an agreed variation to the existing contract.

5.5. The GDPR Owner is responsible for ensuring that the revised controls are implemented and incorporated into the existing review and monitoring arrangements.

6. DOCUMENT CONTROL

The responsibility for the content of this document is with the GDPR Owner.

Schedule 10 Risk Assessment Procedure

RISK ASSESSMENT PROCEDURE

CSO ALLIANCE LIMITED

1. SCOPE

1.1 An assessment of risks relating to CSO Alliance (including information security risks) may be required periodically.
1.2 The method of risk assessment set out below will be applied (as necessary) throughout CSO Alliance in respect of all information risks.
1.3 Compliance is managed by the GDPR Owner.

2. RESPONSIBILITIES

2.1 The GDPR Owner is responsible for carrying out risk assessments wherever they are required by the GDPR.

3. IDENTIFY THE RISKS

3.1 The risks to CSO Alliance 's information are identified by the GDPR Owner under the headings of risks to availability, confidentiality and integrity.

4. ASSESS THE RISKS

4.1 The impact that might result from the loss of availability, confidentiality or integrity for each relevant risk is assessed by the GDPR Owner.
4.2 The realistic likelihood that each of these risks might occur is assessed by the GDPR Owner.
4.3 The risk levels are assessed by the GDPR Owner.
4.4 A decision will be made for each of the risks as to whether it is acceptable or if it must be controlled in line with criteria established by the GDPR Owner.

5. IDENTIFY AND EVALUATE OPTIONS FOR THE TREATMENT OF RISKS

5.1 For each of the risks, identify the possible options for treating it in line with the decision made in paragraph 4.4 above.
5.2 For each of the risks, document which treatment action (accept, reject, transfer or control) is going to be taken and the reasons for each choice.

6. CONTROL OBJECTIVES THE TREATMENT OF RISKS

6.1 Appropriate control objectives will be selected or designed by the GDPR Owner according to the specific needs of the risk and CSO Alliance and controls to achieve those objectives are selected from a variety of sources.
6.2 The final selection of controls and control objectives and the reasons for the selections (whether inclusion or exclusion) will be documented.
6.3 These control objectives and controls are then summarized in a Statement of Applicability.

Document Control

The responsibility for the content of this document is with the GDPR Owner.

Schedule 11 Consent Procedure

CONSENT PROCEDURE

CSO ALLIANCE LIMITED

1. **SCOPE**

1.1 The consent of the data subject is one of the conditions for the processing of his or her personal data.

1.2 Consent of the data subject is defined by the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

1.3 Explicit consent is required for the processing of Sensitive Personal Data.

1.4 Specific conditions apply to the validity of consent given by children in relation to information society services, with requirements to obtain and verify parental consent below certain age limits.

2. **RESPONSIBILITIES**

2.1 CSO Alliance is responsible under the GDPR for obtaining consent from the data subject under advisement from GDPR Owner.

3. **Consent procedure**

3.1 CSO Alliance will provide a clear privacy notice wherever personal data is collected to ensure that consent is informed, and that the data subject is informed of their rights in relation to their personal data.

3.2 CSO Alliance will demonstrate the following:

- 3.2.1 data subject(s) consent to the processing of his or her personal data or explicit consent for Sensitive Personal Data;
- 3.2.2 the data subject(s) consent to the processing of his or her personal data for one or more specific purposes;
- 3.2.3 that the data subject(s) consent is clearly distinguishable from any other matter relating to the data subject;
- 3.2.4 that the data subject(s) consent is intelligible and accessible using clear and plain language;
- 3.2.5 that the data subject(s) are informed of their right to withdraw consent before giving consent; and
- 3.2.6 the processing of data is limited to that stated in the contract, bound by the explicit consent given by the data subject.

4. **CHILD CONSENT PROCEDURE**

4.1 Where processing relates to a child under 16 years old, CSO Alliance will demonstrate that consent has been provided by the person who is the holder of parental responsibility over the child in instances where CSO Alliance offers services online targeting children.

4.2 CSO Alliance will demonstrate reasonable efforts have been made to verify the age of the child and establish the authenticity of the parental responsibility taking into consideration available technology.

5. **DOCUMENT CONTROL**

The responsibility for the content of this document is with the GDPR Owner.

Schedule 12 Data Subject Consent Form

DATA SUBJECT CONSENT FORM

CSO ALLIANCE LIMITED

GDPR CONSENT STATEMENT

I, *[data subject name]*, hereby grant CSO Alliance Limited and *[third-party processor]* authority to process my personal data for the purpose of *[specify in explicit terms, the reason for processing the personal data]*, which is attached to this declaration.

I am aware that I may withdraw my consent at any time.

Signed by data subject:

Date:

Request actioned:

GDPR Owner

Date:

This work instruction was approved by the GDPR Owner on *[date]* and is issued on a version-controlled basis under his/her signature

Signature: Date:

Schedule 13 Withdrawal of Data Subject Consent Form

WITHDRAWAL OF DATA SUBJECT CONSENT FORM

CSO ALLIANCE LIMITED

WITHDRAWAL OF CONSENT

I, *[data subject name]*, withdraw my consent to process my personal data from CSO Alliance Limited.

CSO Alliance Limited no longer has my consent to process my personal data for the purpose of *[specify legitimate reason of processing personal data]*, which was previously granted.

Signed by data subject:

Date:

Request actioned:

GDPR Owner

Date:

This work instruction was approved by the GDPR Owner on [date] and is issued on a version-controlled basis under his/her signature

Signature: Date:

Schedule 14 Subject Access Request Procedure

SUBJECT ACCESS REQUEST PROCEDURE

CSO ALLIANCE LIMITED

1. SCOPE

1.1 All personal data processed by CSO Alliance is within the scope of this procedure.

1.2 Data subjects are entitled to obtain:

- 1.2.1 confirmation as to whether CSO Alliance is processing any personal data about that individual;
- 1.2.2 access to their personal data; and
- 1.2.3 any related information including matters related to automated information.

1.3 For the purposes of this procedure, CSO Alliance will identify the GDPR Owner who will be responsible for GDPR compliance matters LONG with the close attention of the trustees, directors of CSO Alliance or organisation.

2. RESPONSIBILITIES

2.1 The GDPR Owner is responsible for the application and effective working of this procedure.

2.2 The GDPR Owner is responsible for handling all SARs.

3. Procedure

3.1 Subject Access Requests are made using the Subject Access Request Record.

3.2 The data subject should provide CSO Alliance with evidence of their identity in the form of current passport or driving licence and the signature on the identity must be cross-checked to that on the application form.

3.3 The data subject may identify the specific data held by CSO Alliance on their subject access request (SAR). The data subject can request all data held on them.

3.4 CSO Alliance will record the date that the identification checks were conducted and the specified data sought.

3.5 CSO Alliance will provide the requested information to the data subject within 1 month from this recorded date.

3.6 Once received, the subject access request (**SAR**) application will be immediately forwarded to the GDPR Owner who will ensure that the requested data is collected within the time frame specified above.

3.7 Collection entails:

- 3.7.1 collecting the data specified by the data subject, or
- 3.7.2 searching all databases and all relevant filing systems (manual files) in CSO Alliance , including all back up and archived files (computerised or manual) and all email folders and archives. The GDPR Owner maintains a data map that identifies where all data in CSO Alliance is stored.

3.8 The GDPR Owner will maintain a record of requests for data and of its receipt, including dates.

3.9 The GDPR Owner will review subject access requests from a child. Before responding to a SAR of the child data subject, the GDPR Owner considers their ability to making the request by, amongst other things, explaining any implications of sharing their personal data.

3.10 The GDPR Owner will review all documents that have been provided to identify whether any third parties are present in it, and either remove the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed.

3.11 If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:

- National security
- Crime and taxation
- Health
- Education
- Social Work
- Regulatory activity
- Journalism, literature and art
- Research history, and statistics
- Publicly available information
- Corporate finance
- Examination marks
- Examinations scripts
- Domestic processing
- Confidential references
- Judicial appointments, honours and dignities
- Crown of ministerial appointments
- Management forecasts
- Negotiations
- Legal advice and proceedings
- Self-incrimination
- Human fertilization and embryology
- Adoption records
- Special educational needs
- Parental records and reports

3.12 If a data subject requests CSO Alliance to provide them with the personal data stored by the controller/processor, then CSO Alliance will provide the data subject with the requested information in electronic format, unless otherwise specified.

3.13 If a data subject requests what personal data is being processed, then CSO Alliance provides the data subject with the following information:

3.13.1 purpose of the processing;
3.13.2 categories of personal data;
3.13.3 recipient(s) of the information, including recipients in third countries or international organisations;
3.13.4 how long the personal data will be stored;
3.13.5 the data subject's right to request rectification or erasure, restriction or objection, relative to their personal data being processed;
3.13.6 inform the data subject of their right to lodge a complaint with the supervisory authority and a method to do so;
3.13.7 information on the source of the personal data if it hasn't been collected from the data subject;
3.13.8 inform the data subject of any automated decision-making; and
3.13.9 if and where personal data has been transferred and information on any safeguards in place.

4. Document Control

The responsibility for the content of this document is with the GDPR Owner.

Schedule 15 Subject Access Request Recommended Form

SUBJECT ACCESS REQUEST

RECOMMENDED FORM

CSO ALLIANCE LIMITED

1. DATA SUBJECT DETAILS:

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Home					
Work					
Mobile					
Email address					
Date of birth					
Details of identification provided to confirm name of data subject (We will need two copies of forms of identification, which can be: • Passport • Driving licence • Birth certificate • Utility bill (from last 3 months) • Current vehicle registration document • Bank statement (from last 3 months) • Rent book (from last 3 months).					
Details of data requested:					

2. DETAILS OF PERSON REQUESTING THE INFORMATION (if not the data subject):

Are you acting on behalf of the data subject with their written or other legal authority?	Yes ☐ No ☐
If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor)	
Please enclose proof that you are legally authorised to obtain this information.	

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Home					
Work					
Mobile					
Email address					

3. DECLARATION

I, ……, the undersigned and the person identified in (1) above, hereby request that CSO Alliance Limited provide me with the data about me identified above.

Signature: Date:

SAR form completed by (employee name):

I, ……, the undersigned and the person identified above, hereby request that CSO Alliance Limited provide me with the data about the data subject identified above.

Signature: Date:

SAR form completed by (employee name):

This form must immediately be forwarded to the GDPR Owner.

Schedule 16 Complaints Procedure

COMPLAINTS PROCEDURE

CSO ALLIANCE LIMITED

1. SCOPE

1.1 This procedure addresses complaints from data subject(s) related to the processing of their personal data, CSO Alliance 's handling of requests from data subjects and appeals from data subjects on how complaints have been handled.

1.2 For the purposes of this procedure, CSO Alliance will identify the GDPR Owner who will be responsible for GDPR compliance matters, with the close attention of the trustees, directors of CSO Alliance or organisation.

2. RESPONSIBILITIES

2.1 All employees are responsible for ensuring any complaints made in relation to the scope of this procedure are reported to GDPR Owner

2.2 The GDPR Owner is responsible for dealing with all complaints in line with this procedure.

3. PROCEDURE

3.1 CSO Alliance has published the contact details of the GDPR Owner published on its website.

3.2 CSO Alliance has clear guidelines on this that enable the data subject to lodge a complaint. This is accompanied by a form in order to do so.

3.3 Data subjects are able to complain to CSO Alliance about:

- 3.3.1 how their personal data has been processed;
- 3.3.2 how their request for access to data has been handled;
- 3.3.3 how their complaint has been handled; and
- 3.3.4 appeal against any decision made following a complaint.

3.4 Data subject(s) lodging a complaint with the GDPR Owner are able to do so by the contact form published on CSO Alliance website, and/or via email direct to the GDPR Owner published on CSO Alliance website:

- 3.4.1 Complaints received via the contact form are directed to the GDPR Owner for resolution;
- 3.4.2 Complaints are to be resolved within as short a timeframe as possible and within the requirements of GDPR; and
- 3.4.3 Appeals on the handling of complaints are to be resolved within as short a timeframe as possible and within the requirements of GDPR.

3.5 If CSO Alliance fails to act on a data subject's access request within 1 month or refuses the request, it shall set out in clear and plain language the reasons it took no action/refusal.

3.6 CSO Alliance will also inform the data subject(s) of their right to complain directly to the supervisory authority. In doing so, CSO Alliance provides the data subject(s) with the contact details of the supervisory authority and informs them of their right to seek judicial remedy.

4. DOCUMENT CONTROL

4.1 The responsibility for the content of this document is with the GDPR Owner.

Schedule 17 Managing Sub-Processing

MANAGING SUB-PROCESSING

CSO ALLIANCE LIMITED

1. SCOPE

1.1 All external suppliers that process personal data on behalf of CSO Alliance are within the scope of this procedure.

1. RESPONSIBILITIES

2.1 The GDPR Owner is responsible for approving the selection of all sub-contracted processors of personal data in line with the requirements of this procedure.
2.2 The owners of third-party relationships are responsible for ensuring that all external data processing is contracted out in line with this procedure.
2.3 The GDPR Owner is responsible for ensuring that adequate technical and other resources that might be required are made available to support the relationship owner in the monitoring and management of the relationship.
2.4 The GDPR Owner is responsible for carrying out regular audits of third-party compliance.

2. PROCEDURE

3.1 CSO Alliance selects only suppliers that can provide technical, physical and organisational security that meet CSO Alliance 's requirements in terms of all the personal data they will process on CSO Alliance 's behalf.
3.2 CSO Alliance has in place appropriate checks that ensure all contracts are reviewed to see if personal data is processed. These checks are carried out even if data processing activities are not the primary reason for the contract.
3.3 CSO Alliance will ensure that the all security arrangements are outlined in the contract with the external processor.
3.4 Suppliers from outside the EU will only be selected under the following conditions, in addition to the conditions noted elsewhere in this procedure:

- 3.4.1 if the supplier or the state in which it resides has been positively identified in an adequacy decision by the EU Commission; or
- 3.4.2 where there are legally binding corporate rules, and organisational and technical safeguards, established between CSO Alliance and the supplier to secure the rights and freedoms of data subjects at least equal to those afforded within the EU; or
- 3.4.3 where the arrangement has been approved by the supervisory authority.

3.5 If the GDPR Owner considers it necessary because of the nature of the personal data to be processed or because of the particular circumstances of the processing, an audit of the supplier's security arrangements may be conducted before entering into the contract.
3.6 CSO Alliance requires a written agreement to provide the service as specified and requires the supplier to provide appropriate security for the personal data it will process.
3.7 All data processing contracts will allow CSO Alliance to conduct regular audits of the supplier's security arrangements during the period in which the supplier has access to the personal data.
3.8 All data processing contracts forbid suppliers from using further subcontractors without CSO Alliance 's written authorisation for the processing of personal data.
3.9 Where CSO Alliance permits a supplier to subcontract processing of personal data, the immediate supplier must prohibit the second-level contractor (or further down the chain) from subcontracting these processing operations without CSO Alliance 's written authorisation.
3.10 Contracts with second-level subcontractors will only be approved if they require the subcontractors to comply with at least the same security and other provisions as the primary subcontracting organisation (the supplier) if they specify that, when the contract

is terminated, related personal data will either be destroyed or returned to CSO Alliance and so on down the chain of sub-contracting.

Document Owner and Approval

THE GDPR Owner is the owner of this document.

Schedule 18 Pro Forma Data Processing Agreement

DATA PROCESSING AGREEMENT

between

[PARTY]

and

CSO ALLIANCE LIMITED

THIS AGREEMENT is dated

PARTIES

1. [INSERT DETAILS] (**Data Processor**); and
2. CSO Alliance Limited (CSO Alliance or We) a company registered in England and Wales under company number 08319882 whose registered office is at The Mill, Quainton Road, Waddeson, Aylesbury, Buckinghamshire, England HP18 0LP (**Data Controller**).

BACKGROUND

A. The Data Controller has a requirement for the processing of Personal Data (as defined below).
B. The Supplier has agreed to provide the requested processing of such Personal Data under the terms set out in this Agreement.

1. DEFINITIONS

1.1 In this Agreement, the following terms will have the meanings set out below and cognate terms will be construed accordingly:

Effective Date has the meaning given to it in section 2.
Applicable Laws means (a) European Union or Member State laws with respect to the Personal Data; and (b) any other applicable law with respect to the Personal Data.
Contract for Services: the agreement entered into by the Data Controller and Data Processor under which the Data Processor (as Supplier) will provide the Services specified therein.
Data Processor Affiliate means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with the Data Processor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
Data Protection Laws will mean Directive 95/46/EC and Directive 2002/58/EC, in each case as transposed into domestic legislation of each Member State of the European Economic Area and in each case as amended, replaced or superseded from time to time, including without limitation by the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("**GDPR**") and/or other applicable data protection or national/federal or state/provincial/emirate privacy legislation in force, including where applicable, statues, decisions, guidelines, guidance notes and codes of practice issued from time to time by courts, any Supervisory Authority and other applicable authorities.
Data Controller, Data Processor, Data Subject, Process/Processing and Special Categories of Personal Data will have the same meaning as described in the Data Protection Laws;
Delete means the removal or obliteration of Personal Data such that it cannot be recovered or reconstructed.
Group will mean, in relation to a company, that company, any subsidiary or any holding CSO Alliance from time to time of that company, and any subsidiary from time to time of a holding company of that company. Each company in a Group is a member of the Group. A reference to a holding company or a subsidiary means a holding company or a subsidiary (as the case may be) as defined in section 1159 of the Companies Act 2006.
Personal Data means the personal data (as defined in the Data Protection Laws) set out in Annex 1 to this Agreement and any other personal data, as defined in the Data Protection Laws, Processed by the Data Processor on behalf of the Data Controller pursuant to or in connection with the Contract for Services.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data transmitted, stored or otherwise Processed.
Relevant Date means the date falling on the earlier of (i) the cessation of Processing of the Personal Data by the Data Processor; or (ii) termination of the Contract for Services.
Restricted Transfer means:

(i) a transfer of the Personal Data from any Data Controller to a Data Processor or Subprocessor; or

(ii) an onward transfer of the Personal Data from a Data Processor or Subprocessor to (or between two establishments of) a Data Processor or Subprocessor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws).

Subprocessor means any Data Processor (including any third party) appointed by the Data Processor to Process Personal Data on behalf of the Data Controller.
Supervisory Authority means (a) an independent public authority which is established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws.

1.2 The terms used in this Agreement will have the meanings set forth in this Agreement. Capitalized terms not otherwise defined herein will have the meaning given to them in the Contract for Services. Except as modified below, the terms of the Contract for Services will remain in full force and effect.

1.3 The parties hereby agree that the terms and conditions set out below will be added as an Agreement to the Contract for Services.

2. FORMATION OF THIS AGREEMENT

2.1 This Agreement comes into effect on the Effective Date, which will be the earlier of:

(a) the date on which this Agreement is signed by the Data Processor;

(b) the date which is thirty (30) calendar days after the date on which this Agreement is sent by the Data Controller to the Data Processor,

except where the Data Processor objects to the terms of this Agreement in accordance with section 2.2 below.

2.2 If, following receipt of this Agreement, the Data Processor objects to its terms it will notify the Data Controller in writing of its objection within thirty (30) calendar days after the date on which the Agreement is sent by the Data Controller to the Data Processor. The Parties will then work together promptly and in good faith to resolve the Data Processor's objections and to agree upon a mutually satisfactory form of this Agreement, whereupon the Agreement Effective Date will be the date on which the agreed form of the Agreement is signed by the parties.

3. DATA PROCESSING TERMS

3.1 In the course of providing the Services to the Data Controller pursuant to the Contract for Services, the Data Processor may Process Personal Data on behalf of the Data Controller as per the terms of this Agreement. The Data Processor agrees to comply with the following provisions with respect to the Personal Data submitted by or for the Data Controller to the Data Processor or otherwise collected and Processed by or for the Data Controller by the Data Processor.

3.2 Processing of Personal Data

3.3 The Data Controller hereby appoints the Data Processor in relation to the Processing of Personal Data and the parties agree to act in accordance with their respective obligations under this Agreement.

3.4 The parties will at all times comply with applicable Data Protection Laws.

3.5 The Data Processor will not Process the Personal Data other than on the Data Controller's documented instructions (whether in the Contract for Services or otherwise) unless Processing is required by Applicable Laws to which the Data Processor is subject, in which case the Data Processor will to the extent permitted by Applicable Laws inform the Data Controller of that legal requirement before the relevant Processing of that Personal Data.

3.6 The Data Controller:

(a) instructs the Data Processor (and authorises the Data Processor to instruct each Subprocessor) to:

(b) Process the Personal Data; and

(c) subject to sections 8 (Subprocessors) and any relevant restrictions, transfer the Personal Data to any country or territory,

(d) as reasonably necessary to the provision of the Services and consistent with the Contract for Services.

3.7 Annex 1 to this Agreement sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject as required by Article 28(3) of the GDPR or equivalent provisions of any Data Protection Law. The Data Controller may make reasonable amendments to Annex 1 by written notice to the Data Processor from time to time as the Data Controller reasonably considers necessary to meet those requirements. As between the parties, nothing in Annex 1 (including as amended pursuant to this section 3.7) confers any right or imposes any obligation on either party.

1. DATA PROCESSOR PERSONNEL

The Data Processor will take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Personal Data, as strictly necessary for the purposes set out in section 4.3 above in the context of that individual's duties to the Data Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

2. SECURITY

2.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate including inter alia as appropriate: (a) the pseudonymisation and encryption of the Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

2.2 In assessing the appropriate level of security, the Data Processor will take account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

3. PERSONAL DATA BREACH

3.1 The Data Processor will notify the Data Controller without undue delay and in any case within twenty-four (24) hours, upon becoming aware of or reasonably suspecting a Personal Data Breach, with sufficient information which allows the Data Controller to meet any obligations to report a Personal Data Breach under the Data Protection Laws. Such notification will as a minimum:

3.1.1 describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

3.1.2 communicate the name and contact details of the Data Processor's data protection officer or other relevant contact from whom more information may be obtained;

3.1.3 describe the likely consequences of the Personal Data Breach; and

3.1.4 describe the measures taken or proposed to be taken to address the Personal Data Breach.

3.2 The Data Processor will co-operate with the Data Controller and take such reasonable commercial steps as are directed by the Data Controller to assist in the investigation, mitigation and remediation of each Personal Data Breach.

3.3 In the event of a Personal Data Breach, the Data Processor will not inform any third party without first obtaining the Data Controller's prior written consent, unless notification is required by EU or Member State law to which the Data Processor is subject, in which case the Data Processor will to the extent permitted by such law inform the Data Controller of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Data Controller before notifying the Personal Data Breach.

4. DATA SUBJECT RIGHTS

4.1 Taking into account the nature of the Processing, Data Processor will assist the Data Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising Data Subject rights laid down in the GDPR or equivalent provision of any Data Protection Laws.

4.2 The Data Processor will promptly notify the Data Controller (and in any case within 3 business days) if it receives a request from a Data Subject under any Data Protection Laws in respect of the Personal Data.

5. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

5.1 The Data Processor will provide reasonable assistance to the Data Controller with any data protection impact assessments which are required under Article 35 GDPR and with any prior consultations to any supervisory authority of the Data Controller which are required under Article 36 GDPR, in each case solely in relation to Processing of Personal Data by the Data Processor on behalf of the Data Controller under the Contract for Services and this Agreement, and taking into account the nature of the Processing and information available to the Data Processor.

6. RESTRICTED TRANSFERS

6.1 In the event that that the Data Processor (whether it is required to by the Data Controller or otherwise) undertakes the transfer of Personal Data to a jurisdiction outside the EEA which has not been assigned 'adequate' status by the European Commission, the parties agree that any such transfer will conform to the provisions of Chapter V GDPR in particular (but not limited to) the provisions of Article 46 (Transfers Subject to Appropriate Safeguards). The provisions of this clause apply to any Subprocessor appointed by the Data Processor pursuant to the terms of this Agreement.

7. AUDIT RIGHTS

7.1 In addition to any audit rights granted pursuant to the Contract for Services, the Data Processor will make available to the Data Controller on request all information necessary to demonstrate compliance with this Agreement and allow for and contribute to audits, including inspections, by the Data Controller or an auditor mandated by the Data Controller. The Data Processor will immediately inform the Data Controller if, in its opinion, an instruction pursuant to this section 10 (Audit Rights) infringes the GDPR or other EU or Member State data protection provisions.

8. SUB-PROCESSING

8.1 The Data Controller authorises the Data Processor to appoint (and permit each Subprocessor appointed in accordance with this section 8 to appoint) Subprocessors in accordance with this section 8 and any restrictions in the Contract for Services.

8.2 The Data Processor may continue to use those Subprocessors already engaged by the Data Processor as at the date of this Agreement, subject to the Data Processor in each case as soon as practicable meeting the obligations set out in section 8.4.

8.3 The Data Processor will give the Data Controller prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 30 (thirty) calendar days of receipt of that notice, the Data Controller notifies the Data Processor in writing of any objections (on reasonable grounds) to the proposed appointment:

(a) the Data Processor will work with the Data Controller in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and

(b) where such a change cannot be made within 30 (thirty) calendar days from the Data Processor's receipt of the Data Controller's notice (or such longer period as the parties may agree in writing), notwithstanding anything in the Contract for Services, the Data Controller may by written notice to the Data Processor with immediate effect terminate the Contract for Services to the extent that it relates to the Services which require the use of the proposed Subprocessor.

8.4 With respect to each Subprocessor, the Data Processor will:

(a) carry out adequate due diligence on each Subprocessor to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Agreement including without limitation sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of GDPR or equivalent provisions of any Data Protection Law and this Agreement;

(b) include terms in the contract between the Data Processor and each Subprocessor which offer at least the same level of protection for the Personal Data as those set out in this Agreement Upon request, the Data Processor will provide a copy of its agreements with Subprocessors to the Data Controller (which may be redacted to remove confidential commercial information not relevant to the requirements of this Agreement); and

(c) remain fully liable to the Data Controller for any failure by each Subprocessor to fulfil its obligations in relation to the Processing of the Personal Data.

9. DELETION OR RETURN OF PERSONAL DATA

9.1 Subject to sections 9.2 and 9.3 the Data Processor will promptly and in any event within 28 (twenty-eight) calendar days of the Relevant Date, Delete and procure the Deletion of all copies of Personal Data Processed by the Data Processor or any Subprocessor.

9.2 Subject to section 9.3, the Data Controller may in its absolute discretion notify the Data Processor in writing within 15 (fifteen) days of the Relevant Date to require the Data

Processor to: (a) return a complete copy of all Personal Data to the Data Controller by secure file transfer in such format as notified by the Data Controller to the Data Processor; and (b) Delete and procure the Deletion of all other copies of Personal Data Processed by the Data Processor or any Subprocessor. The Data Processor will comply with any such written request within 28 days of the Relevant Date.

9.3 The Data Processor may retain Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that the Data Processor will ensure the confidentiality of all such Personal Data and will ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.4 The Data Processor will provide written certification to the Data Controller that it has fully complied with this section 9 within 28 (twenty-eight) days of the Relevant Date.

10. LIABILITY AND INDEMNITY

10.1 Notwithstanding anything to the contrary in the Principle Agreement, The Data Processor 's liability for any breach of this Agreement will be unlimited.

10.2 The Data Processor will indemnify and hold harmless the Data Controller against all losses, fines and sanctions arising from any claim by a third party or Supervisory Authority arising from any breach of this Agreement.

11. GENERAL TERMS

11.1 The parties agree that this Agreement will terminate automatically upon: (i) termination of the Contract for Services; or (ii) expiry or termination of all service contracts, statements of work, work orders or similar contract documents entered into by the Data Processor with the Data Controller pursuant to the Contract for Services, whichever is later.

11.2 Any obligation imposed on the Data Processor under this Agreement in relation to the Processing of Personal Data will survive any termination or expiration of this Agreement.

12. GOVERNING LAW OF THIS AGREEMENT

12.1 To the extent that EU Data Protection Laws apply to the Processing of the Personal Data this Agreement will be governed by:

(a) the governing law of the Contract for Services for so long as that governing law is the law of a Member State of the European Union; or

(b) where section 12.1(a) does not apply, the laws of England.

12.2 To the extent that EU Data Protection Laws do not apply to the Processing of the Personal Data, this Agreement will be governed by the governing law of the Contract for Services.

12.3 Notwithstanding the general choice of law above, any questions of contract formation pertaining to this Agreement will be governed by English law.

13. CHOICE OF JURISDICTION

13.1 Notwithstanding the choice of law above, the parties to this Agreement hereby submit to the choice of jurisdiction stipulated in the Contract for Services with respect to any disputes or claims howsoever arising under this Agreement.

14. CROSS-DEFAULT

14.1 Any breach of this Agreement will constitute a material breach of the Contract for Services.

14.2 With regard to the subject matter of this Agreement, in the event of inconsistencies between the provisions of this Agreement and any other agreements between the parties, including but not limited to the Contract for Services, the provisions of this Agreement will prevail with regard to the parties' data protection obligations for Personal Data of a Data Subject from either a Member State of the European Union or from the UK (following the UK's exit from the European Union).

14.3 Compliance by the Data Processor with the provisions of this Agreement will be at no additional cost to the Data Controller.

14.4 A person who is not a party to this Agreement will have no right to enforce any term of this Agreement.

14.5 The rights of the parties to rescind or vary this Agreement are not subject to the consent of any other person.

14.6 The Data Controller may notify the Data Processor in writing from time to time of any variations to this Agreement which are required as a result of a change in Data Protection Laws including without limitation to the generality of the foregoing, any variations which are required as a result of any changes to UK Data Protection Laws following any exit of the UK from the European Union. Any such variations will take effect on the date falling 30 (thirty) calendar days after the date such written notice is sent by the Data Controller to the Data Processor will procure that where necessary the terms in each contract between the Data Processor and each Subprocessor are amended to incorporate such variations within the same time period.

14.7 Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement will remain valid and in force. The invalid or unenforceable provision will be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Agreement is entered into and becomes a binding part of the Contract for Services with effect from the Agreement Effective Date first set out above.

DATA CONTROLLER:	DATA PROCESSOR:
CSO ALLIANCE LIMITED	[IDENTIFY]
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

ANNEX 1

PERSONAL INFORMATION

[INSERT THE RELEVANT DETAIL]

(a) This Annex 1 includes certain details of the Processing of the Personal Data as required by Article 28(3) GDPR.

(b) Subject matter and duration of the Processing of the Personal Data

(c) The subject matter and duration of the Processing of the Personal Data are set out in the Contract for Services and this Agreement.

(d) The nature and purpose of the Processing of the Personal Data

(e) As described in the SOW attached to the Contract for Services

(f) The types of the Personal Data to be Processed

(g) [Include list of data types here]

(h) The categories of Data Subject to whom the Personal Data relates

(i) [Include categories of data subjects here]

(j) The obligations and rights of the Data Controller

(k) The obligations and rights of the Data Controller are set out in the Contract for Services and this Agreement.

Schedule 19 Managing International Data Transfers

MANAGING INTERNATIONAL DATA TRANSFERS

CSO ALLIANCE LIMITED

1. SCOPE

1.1 This procedure applies where, in accordance with the GDPR, CSO Alliance wishes to transfer personal data to third countries or international organisations outside of the EU for processing. This includes the onward transfer of personal data from a third country, or an international organisation to another third country, as well as to another international organisation within the scope of this procedure.

2. RESPONSIBILITIES

2.1 It is the responsibility of CSO Alliance to ensure that the appropriate level of protection of personal data of natural persons guaranteed by the GDPR to EU residents is not undermined.

3. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS PROCEDURE

3.1 When transferring personal data to third countries or international organisations outside of the EU, CSO Alliance will check that there is an adequate level of protection established by one of the following:

3.1.1 the country, or industry sector within that country, of the recipient is on the EU approved list of countries as set out in the Official Journal of the European Union;

3.1.2 the country of the recipient has adequate data protection controls established by legal or self-regulatory regime;

3.1.3 CSO Alliance has a contract in place that uses existing or approved data protection clauses to ensure adequate protection;

3.1.4 CSO Alliance is making the transfer under approved binding corporate rules;

3.1.5 CSO Alliance is relying on approved codes of conduct or certification mechanisms, together with binding and enforceable commitments in the third country or international organisation to apply the appropriate safeguards in relation to data subject rights.

3.1.6 Provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

3.1.7 Where there is no adequacy decision or appropriate safeguards in place, CSO Alliance can rely on an exemption on data transfers; in the absence of all of the above, if the processing is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual) a one-off transfer is possible under restricted conditions if the data controller informs the relevant supervisory authority of the transfer and provides additional information to individuals.

4. Document Owner and Approval

THE GDPR Owner is the owner of this document.

Schedule 20 Data Retention Policy

DATA RETENTION POLICY

CSO ALLIANCE LIMITED

1. **SCOPE**

1.1 All CSO Alliance's records, whether analogue or digital, are subject to the retention requirements of this procedure.

2. **RESPONSIBILITIES**

2.1 The following roles are responsible for retention of these records because they are the information asset owners.
2.2 Asset owners within CSO Alliance are/responsible for ensuring that all personal data is collected, retained and destroyed in line with the requirements of the GDPR.
2.3 The GDPR Owner is responsible for:

2.3.1 the retention of financial and related records;
2.3.2 the retention of all HR records;
2.3.3 health and safety records; and
2.3.4 all other statutory and regulatory records.

2.4 The GDPR Owner is responsible for storage of data in line with this procedure.
2.5 The GDPR Owner is responsible for ensuring that retained records are included in business continuity and disaster recovery plans.

3. **PROCEDURE**

3.1 The required retention periods, by record type, are recorded in under the following categories:

3.1.1 record type;
3.1.2 retention period;
3.1.3 retention period to start from (at creation, submission, payment, etc.);
3.1.4 retention justification;
3.1.5 record medium; and
3.1.6 disposal method.

3.2 Cryptographic keys are retained.
3.3 For all storage media (electronic and hard copy records), CSO Alliance retains the means to access that data.
3.4 The GDPR Owner is responsible for destroying data once it has reached the end of the retention period.
3.5 Destruction must be completed within 30 days of the end of the planned retention period.

4. ***Document Owner and Approval***

This procedure was approved by the GDPR Owner.

Personal Data Retention Policy: Retention Periods			
Record Type	Period Retained	Commencement Date	Reason for Retention Period	Media	Disposal Approach
Internal Personal Data					
Corporate governance: shareholder agreements, option agreements, investment agreements; records of shareholders meetings and board minutes; submissions to Companies House, company books and shareholders' register	Retain until earlier of cessation of organisation or obsolete; archive under password	On agreement or formal approval	Legal risk: managing data in the event of a dispute	Digital; Paper	Shredding; deletion
Employment contracts including Directors Services Agreement, also including contractor and consultancy agreements with third parties	Retain for 6 years; archive after 1 year under password	Keep until cessation; time runs from cessation of relationship	Legal risk: managing data in the event of a dispute	Digital; Paper	Shredding; deletion
Human Resources records; notes relating to performance and disciplinary matters over the course of employment	Retain for 6 years; archive after 1 year under password	Time runs from cessation of relationship	Legal risk: managing data in the event of a dispute (evidence and detail of interaction)	Digital; Paper	Shredding; deletion
Governance Records: Tax and Accounting Matters; Financial Records relating to staff and contracted third parties	7 years; archive under password within 6 months of use	Time runs from cessation of relationship	Compliance risk	Digital; Paper	Shredding; deletion
Emails; intra-company correspondence	2 years on specified dates;			Digital; Paper	Shredding; deletion

	staff to purge all non-commercial emails and correspondence; anything left to be archived	2 years after initial specified date (25th May 2018)	Legal risk: managing data in the event of a dispute (evidence and detail of interaction)		
Miscellany which contains personal data: details of phone calls; expenses	3 years on specified dates; staff to purge all non-commercial emails and correspondence; anything left to be archived	3 years after initial specified date (25th May 2018)	Legal risk: managing data in the event of a dispute (evidence and detail of interaction)	Digital; Paper	Shredding; deletion
Specific derogations: (list exceptional matters where the general rules set out above do not apply)					
Contracts; third party agreements with clients/customers					
Contracts for the provision of goods and services; services; goods which disclose personal data: can include non-disclosure agreements, memorandum of understanding, partnering agreements, joint venture agreements, master services agreements, membership agreements and any other commercial agreement where product or services are being	Retain for 6 years after cessation of agreement	Keep until cessation; time runs from termination of contract/agreement	Legal risk: managing data in the event of a dispute (evidence and detail of interaction)	Digital; Paper	Shredding; deletion

developed for commercial purposes					
Specific derogations: (list exceptional matters where the general rules set out above do not apply)					
Contracts; third party agreements with Suppliers					
Include all contracts with suppliers where personal data is being processed: accountants, legal services, consultancy agreements, lease or licenses of premises, payment agreements (PayPal, Stripe), server agreements, CRM and ERP management services, finance agreements with third parties (loan agreements for example)	Retain for 6 years after cessation of agreement	Time runs from termination of contract/agreement	Legal risk: managing data in the event of a dispute (evidence and detail of interaction)	Digital; Paper	Shredding; deletion
Specific derogations: (list exceptional matters where the general rules set out above do not apply)					
Marketing Lists					
				Digital	Deletion

Summary lists of recipients of marketing information who have opted in (Soft opt-in or hard opt-in) under the ePrivacy Directive	Retain as a live interaction until the earlier of the cessation of the organisation, a valid opt-out or other information meaning that the interaction is no longer consistent with GDPR	Keep opt-out data to ensure that the data subject is not approached again; archive after 3 years; delete after 6 years	To ensure that future interactions do not mean breach of consent rules		
Prospect personal data	Long enough to establish if development objective achieved	Keep opt-out data to ensure that the data subject is not approached again; archive after 3 years; delete after 6 years	To ensure that future interactions do not mean breach of consent rules	Digital	Deletion
Specific derogations: (list exceptional matters where the general rules set out above do not apply)					