AGILIO SOFTWARE LIMITED

Data Protection Handbook

(Comprising the Data Protection Policy and the Privacy Notice)

V1 January 2022

Data Protection Policy

1. Interpretation

1.1. Definitions:

1.2. **Automated Decision-Making (ADM)**: when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

1.3. **Automated Processing**: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

1.4. **Company name**: Agilio Software Limited and its subsidiary companies.

1.5. **Company Personnel**: all employees, workers, contractors, agency workers, consultants, directors, members and others.

1.6. **Consent**: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

1.7. **Controller**: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

1.8. **Criminal Convictions Data**: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

1.9. **Data Subject**: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

1.10. **Data Privacy Impact Assessment (DPIA)**: tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

1.11. **Data Protection Officer (DPO)**: the person required to be appointed in specific circumstances under the UK GDPR. Where a mandatory DPO has not been appointed, this term means a data privacy manager or other voluntary appointment of

a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

1.12. **Explicit Consent**: consent which requires a very clear and specific statement (that is, not just action).

1.13. **UK GDPR**: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the UK GDPR.

1.14. **Personal Data**: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

1.15. **Personal Data Breach**: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

1.16. **Privacy by Design**: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

1.17. **Privacy Guidelines**: the Company privacy and UK GDPR related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies, available here, on Myhrtoolkit or from the DPO.

1.18. **Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies**: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

1.19. **Processing or Process**: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

1.20. **Pseudonymisation or Pseudonymised**: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

1.21. **Related Policies**: the Company's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, available on the intranet: for example the IT and Communications Systems Policy and the Privacy Notice.

1.22. **Special Categories of Personal Data**: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

2. Introduction

2.1. This Data Protection Policy sets out how Agilio ("we", "our", "us", "the Company") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

2.2. This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

2.3. This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you for the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.

2.4. Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a DPIA as referenced in this Data Protection Policy or otherwise then you must comply with the Related Policies and Privacy Guidelines.

2.5. This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

3. Scope

3.1. We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to

£17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

3.2. All line managers, MD/CFDs, and directors are responsible for ensuring all Company Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

3.3. The DPO is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Chief Information Security Officer, and they can be reached at *privacy@agiliosoftware.com*.

3.4. Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

3.4.(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see paragraph 5.1);

3.4.(b) if you need to rely on Consent and/or need to capture Explicit Consent (see paragraph 6);

3.4.(c) if you need to draft Privacy Notices (see paragraph 7);

3.4.(d) if you are unsure about the retention period for the Personal Data being Processed (see paragraph 11);

3.4.(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see paragraph 0);

3.4.(f) if there has been a Personal Data Breach (paragraph 13);

3.4.(g) if you are unsure on what basis to transfer Personal Data outside the UK (see paragraph 14);

3.4.(h) if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 15);

3.4.(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 19) or plan to use Personal Data for purposes other than what it was collected for;

3.4.(j) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see paragraph 20);

3.4.(k) if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 21); or

3.4.(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see paragraph 22).

4. Personal data protection principles

4.1. We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

4.1.(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

4.1.(b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);

4.1.(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

4.1.(d) accurate and where necessary kept up to date (Accuracy);

4.1.(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

4.1.(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

4.1.(g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

4.1.(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

4.2. We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Lawfulness, fairness, transparency

5.1. Lawfulness and fairness

5.2. Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.3. You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.4. The UK GDPR allows Processing for specific purposes, some of which are set out below:

5.4.(a) the Data Subject has given his or her Consent;

5.4.(b) the Processing is necessary for the performance of a contract with the Data Subject;

5.4.(c) to meet our legal compliance obligations;

5.4.(d) to protect the Data Subject's vital interests; or

5.4.(e) to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

5.5. You must identify and document the legal basis being replied on for each Processing activity. Guidance on the appropriate Lawful Basis for Processing Personal Data is available from the DPO.

6. Consent

6.1. A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

6.2. A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.3. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.4. When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

6.5. You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines so that the Company can demonstrate compliance with Consent requirements.

7. Transparency (notifying Data Subjects)

7.1. The UK GDPR requires Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. The information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

7.2. Whenever we collect Personal Data directly from Data Subjects, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

7.3. When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

7.4. If you are collecting Personal Data from Data Subjects, directly or indirectly, then you must provide Data Subjects with a Privacy Notice in accordance with our Related Policies and Privacy Guidelines.

8. Purpose limitation

8.1. Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

8.2. You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

9. Data minimisation

9.1. Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

9.2. You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

9.3. You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

9.4. You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

10. Accuracy

10.1. Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

10.2. You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

11. Storage limitation

11.1. Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

11.2. The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time.

11.3. You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

11.4. You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

11.5. You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

12. Security integrity and confidentiality

Protecting Personal Data

12.1. Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

12.2. We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special

Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

12.3. You must follow all procedures and utilise the technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

12.4. You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

12.4.(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;

12.4.(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed; and

12.4.(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

12.5. You must comply with all applicable aspects of all group or divisional Information Security policies.

13. Reporting a Personal Data Breach

13.1. The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

13.2. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

13.3. If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches (the DPO on *privacy@agiliosoftware.com* and follow the Company's Breach Management and Notification Policy. You should preserve all evidence relating to the potential Personal Data Breach.

14. Transfer limitation

14.1. The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

14.2. You may only transfer Personal Data outside the UK if one of the following conditions applies:

14.2.(a) the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;

14.2.(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

14.2.(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

14.2.(d) the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

15. Data Subject's rights and requests

15.1. Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

15.1.(a) withdraw Consent to Processing at any time;

15.1.(b) receive certain information about the Controller's Processing activities;

15.1.(c) request access to their Personal Data that we hold;

15.1.(d) prevent our use of their Personal Data for direct marketing purposes;

15.1.(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

15.1.(f) restrict Processing in specific circumstances;

15.1.(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

15.1.(h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

15.1.(i) object to decisions based solely on Automated Processing, including profiling (ADM);

15.1.(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

15.1.(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

15.1.(l) make a complaint to the supervisory authority; and

15.1.(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

15.2. You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

15.3. You must immediately forward any Data Subject request you receive to the DPO.

16. Accountability

16.1. The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

16.2. The Company must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

16.2.(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

16.2.(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

16.2.(c) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines or Privacy Notices;

16.2.(d) regularly training Company Personnel on the UK GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

16.2.(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. Record keeping

17.1. The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

17.2. You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

17.3. These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject

types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

18. Training and audit

18.1. We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

18.2. You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training as required.

18.3. You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

19. Privacy by Design and Data Protection Impact Assessment (DPIA)

19.1. We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

19.2. You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

19.2.(a) the state of the art;

19.2.(b) the cost of implementation;

19.2.(c) the nature, scope, context and purposes of Processing; and

19.2.(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

19.3. Controllers must also conduct DPIAs in respect to high-risk Processing.

19.4. You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

19.4.(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

19.4.(b) Automated Processing including profiling and ADM;

19.4.(c) large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and

19.4.(d) large-scale, systematic monitoring of a publicly accessible area.

19.5. A DPIA must include:

19.5.(a) a description of the Processing, its purposes and the Controller's legitimate interests if appropriate;

19.5.(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

19.5.(c) an assessment of the risk to individuals; and

19.5.(d) the risk mitigation measures in place and demonstration of compliance.

19.6. You must comply with the Company's guidelines on DPIA and the principles of privacy by design.

20. Automated Processing (including profiling) and Automated Decision-Making

20.1. Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

20.1.(a) a Data Subject has Explicitly Consented;

20.1.(b) the Processing is authorised by law; or

20.1.(c) the Processing is necessary for the performance of or entering into a contract.

20.2. If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed but the Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

20.3. If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

20.4. We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

20.5. A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

21. Direct marketing

21.1. We are subject to certain rules and privacy laws when marketing to our customers.

21.2. For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

21.3. The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

21.4. A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

22. Sharing Personal Data

22.1. Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

22.2. You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

22.3. You may only share the Personal Data we hold with third parties, such as our service providers, if:

22.3.(a) they have a need to know the information for the purposes of providing the contracted services;

22.3.(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

22.3.(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

22.3.(d) the transfer complies with any applicable cross-border transfer restrictions; and

22.3.(e) a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

23. Changes to this Data Protection Policy

23.1. We keep this Data Protection Policy under regular review. This version was last updated in January 2022. Historic versions are available from the DPO.

23.2. This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates. Certain countries may have localised variances to this Data Protection Policy which are available on request to the DPO.

Staff and Candidate Privacy Notice

1. Introduction

1.1. This privacy notice tells you what to expect when Agilio collects personal information about you. It applies to all employees, ex-employees, agency staff, contractors, those who have been made a conditional or unconditional offer of employment, and non-executive directors. However, the information we will process about you will vary depending on your specific role and personal circumstances. Further information is provided towards the end of this notice on how Agilio process the data of candidates for job roles with Agilio.

1.2. Agilio is the controller for this information unless the notice specifically states otherwise. When appropriate we will provide a 'just in time' notice to cover any additional processing activities not mentioned in this document.

1.3. Agilio's nominated Data Protection Officer can be contacted by emailing *privacy@agiliosoftware.com*. Your information will be shared internally, including with senior executive staff and management, Human Resources staff and IT staff if access to the data is necessary for performance of their roles.

2. How do we get your information?

2.1. Agilio get information about you from the following places:

(a) Directly from you;

(b) From an employment agency;

(c) From referees, either external or internal;

(d) From Occupational Health and other health providers;

(e) From Pension administrators and other government departments, for example tax details from HMRC;

(f) From your Trade Union;

(g) From providers of staff benefits;

(h) CCTV images taken using our own CCTV systems; and

(i) From publicly available internet records, for example social media profiles.

3. What personal data we process and why

Specific details on the types of personal data Agilio process and reasons for processing are outlined below:

3.1. Your employment contract

(a) We use certain information to carry out the contract we have with you, provide you access to business services required for your role and manage our human resources processes. We rely on the lawful basis in Article 6(1)(b) of the UK GDPR which relates to processing necessary for the performance of a contract to process this information. This information includes:

(i) Personal contact details such as your name, address, contact telephone numbers (landline and mobile) and personal email addresses

(ii) Your date of birth, and NI number

(iii) A copy of your passport or similar photographic identification and / or proof of address documents

(iv) Next of kin, emergency contacts and their contact information

(v) Employment and education history including your qualifications, job application, employment references and right to work information

(vi) Location of employment (e.g., Holsworthy, Hove, Sheffield or at your own home)

(vii) Details of any secondary employment, political declarations, conflict of interest declarations or gift declarations

(viii) Your responses to staff surveys if this data is not anonymised

3.2. If you leave, or are thinking of leaving, we may be asked by your new or prospective employers to provide a reference. For example, we may be asked to confirm the dates of your employment or your job role.

3.3. Your salary, pension, and loans

(a) We process this information for the payment of your salary, pension and other employment related benefits. We also process it for the administration of statutory and contractual leave entitlements such as holiday or maternity leave. We rely on the lawful basis in Article 6(1)(b) of the UK GDPR which relates to processing necessary for the performance of a contract. This information includes:

(i) Information about your job role and your employment contract including:

(ii) your start and leave dates, salary (including grade and salary band)

(iii) any changes to your employment contract

(iv) working pattern (including any requests for flexible working)

(v) Details of your time spent working and any overtime, expenses or other payments claimed, including details of any loans such as for travel season tickets

(vi) Details of any leave including sick leave, holidays, special leave etc.

(vii) Pension details including membership of both state and occupational pension schemes (current and previous)

(viii) Your bank account details, payroll records and tax status information

(ix) Trade Union membership for the purpose of the deduction of subscriptions directly from salary

(x) Details relating to Maternity, Paternity, Shared Parental and Adoption leave and pay. This includes forms applying for the relevant leave, copies of MATB1 forms/matching certificates and any other relevant documentation relating to the nature of the leave you will be taking.

3.4. **Your performance and training**

(a) We use personal data to assess your performance, to conduct pay and grading reviews and to deal with any employer / employee related disputes. We also use it to meet the training and development needs required for your role. We rely on the lawful basis in Article 6(1)(b) of the UK GDPR which relates to processing necessary for the performance of a contract. This information includes:

(i) Information relating to your performance at work e.g., probation reviews, performance reviews, promotions

(ii) Grievance and dignity at work matters and investigations to which you may be a party or witness

(iii) Disciplinary records and documentation related to any investigations, hearings and warnings/penalties issued.

3.5. **Monitoring at work**

(a) We use information to assess your compliance with corporate policies and procedures and to ensure the security of our premises, IT systems and employees. We rely on the legitimate interest ground set out in Article 6(1)(f) of the UK GDPR to process personal data in this way. This information includes:

(i) Information derived from monitoring IT acceptable use standards

(ii) Photos and CCTV images

3.6. **Your health and wellbeing information and other special category data**

(a) We use this data to comply with our legal obligations and for equal opportunities monitoring. We also use it to ensure the health, safety and wellbeing of our employees. We rely on the lawful basis set out in Article 6(1)(c) of the UK GDPR which allows processing in order to comply with our legal obligations as a controller. This information includes:

(i) Health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires or fit notes i.e., Statement of Fitness for Work from your GP or hospital

(ii) Accident records if you have an accident at work

(iii) Details of any desk audits, access needs or reasonable adjustments

(iv) Information you have provided regarding Protected Characteristics as defined by the Equality Act 2010. This includes racial or ethnic origin, religious beliefs, disability status, and gender identification and may be extended to include other protected characteristics

(b) Where the information we process is special category data, for example your health data, the additional bases for processing that we rely on is set out in Article 9(2)(b) UK GDPR which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.

4. Lawful basis for processing your personal data

4.1. There may be further situations that arise during the course of employment which mean that we have to rely on lawful basis available to us under the UK GDPR for processing your data. Where reasonably practical and/or legally required, we will inform you in advance. These include:

(a) Article 6(1)(b) which relates to processing necessary for the performance of a contract

(b) Article 6(1)(c) so we can comply with our legal obligations as your employer

(c) Article 6(1)(d) in order to protect your vital interests or those of another person

(d) Article 6(1)(f) for the purposes of our legitimate interest

(e) Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights

(f) Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent

(g) Article 9(2)(f) for the establishment, exercise or defence of legal claims

(h) Article 9(2)(h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee

5. Retention of your personal data

5.1. We do not keep your data for longer than is necessary to fulfil the relevant purposes set out in this notice. We are also required to keep certain information to comply with our legal obligations, for example for our financial records. The exact period we hold your information for will depend on the type of information and your relationship with us. For example, if you are an employee, we will hold your data for longer than if you are an unsuccessful candidate.

5.2. We can provide you with further specific information regarding the periods we hold your data—please contact privacy@agiliosoftware.com.

6. Data Processors

6.1. Agilio use other organisations to carry out services on our behalf or provide services to you. This means that we sometimes share your information with these organisations. We still control your data and these organisations only have access to the data needed to perform their functions and cannot use it for any other reason—these organisations are known as “Data Processors”. We always ensure secure technical and legal safeguards are put in place to protect personal information we share with data processors. The categories of data processors we use are as follows:

(a) Information technology service providers to equip us with software, hardware, infrastructure, and digital storage needed to provide products and services to our customers

(b) Marketing software providers to enable us to communicate with customers and potential customers

(c) Payment processes to enable customers to make secure payments

(d) Credit check services

(e) Analytics services to help us better understand your interactions with our products and services

(f) Survey providers to get your feedback about our products and services

7. Data Sharing and Transfers outside the UK

7.1. In some circumstances, such as under a court order, we are legally obliged to share information. We may also share information about you with third parties including government agencies and external auditors. For example, we may share information about you with HMRC for the purpose of collecting tax and national insurance contributions.

7.2. Where an organisation we share information with processes personal information outside of the UK we ensure that either processing only occurs in countries that are deemed “adequate” by the UK or where there are standard contractual clauses and/or binding corporate rules in place.

7.3. Agilio’s customers are predominantly based in the UK, however, we do supply products and services with businesses and individuals based outside the UK (both EU and non-EU countries). In this case, transfer of data overseas is carried out to meet our contractual obligations with these customers, for example, sending a purchased goods to the buyer’s address. Transfers of this kind will only take place if the contract was entered into at the individual’s request or in their interests and was necessary.

8. Monitoring of staff

8.1. All our IT systems are auditable and can be monitored. Agilio does not undertake monitoring routinely and is committed to respecting individual users’ reasonable expectations of privacy concerning the use of our IT systems and equipment. However, we reserve the right to log and monitor such use in line with Agilio’s acceptable standards. Information acceptable standards that apply and further details on how Agilio may monitor your IT use can be found in HR policies relevant to IT use.

8.2. We operate CCTV inside both our Sheffield premises to monitor access to certain areas.

9. Further information for candidates

9.1. The following section applies to all candidates of job roles with Agilio. However, the information we will process about you will vary depending on your specific role you have applied for and your personal circumstances.

10. What information do we collect from candidates?

10.1. Agilio collect a range of information about you. We do not collect more information than we need to fulfil our stated purposes and will not keep it longer than necessary. The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for, but it may affect your application if you don't.

10.2. The type of information we collect includes:

(a) Your name, address and contact details, including email address and telephone number

(b) Details of your qualifications, skills, experience and employment history

(c) Information about personal interests and experience

(d) Information from interviews you may have

(e) Information about your current level of remuneration, including benefit entitlements

(f) Information about your entitlement to work in the UK

(g) Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or beliefs (This is not mandatory – if you don't provide it, it won't affect your application)

(h) Any feedback you provide about our recruitment process to develop and improve our future recruitment campaigns

11. How do we collect this information and who has access to it?

11.1. Agilio may collect this information in a variety of ways:

(a) Data might be collected from information provided by you, for example in completed application forms, CVs, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment

(b) Information may be provided to us by your named referees. This will include information including the dates of your previous employment and your performance during that time

(c) We may also collect publicly accessible information. For example, from social networking sites such as LinkedIn

Your information will be shared internally, including with senior executive staff and management. Human Resources staff and IT staff if access to the data is necessary for performance of their roles.

12. Purpose and basis for processing candidate's data

12.1. Our purpose for processing this information is to assess your suitability for a role you have applied for and to help us develop and improve our recruitment process.

12.2. The lawful basis we rely on for processing your personal data is article 6(1)(b) of the UK General Data Protection Regulation (UK GDPR), which relates to processing necessary to perform a contract or to take steps at your request, before entering a contract.

12.3. If you provide us with any information about reasonable adjustments you require under the Equality Act 2010 the lawful basis we rely on for processing this information is article 6(1)(c) to comply with our legal obligations under the Act.

12.4. The lawful basis we rely on to process any information you provide as part of your application which is special category data, such as health, religious or ethnicity information is article 9(2)(b) of the GDPR, which relates to our obligations in employment and the safeguarding of your fundamental rights. And Schedule 1 part 1(1) of the Data Protection Act 2018 which again relates to processing for employment purposes.

12.5. Agilio do not make recruitment determinations based on automated decision-making.

13. Your rights

13.1. As an individual you have certain rights regarding our processing of your personal data, including:

(a) You have the right to be informed - Individuals have the right to be informed about the collection and use of their personal data. This notice is a key part of Agilio ensuring that our customers have this information

(b) You have the right to access and receive a copy of your personal data, and other supplementary information

(c) You have the right to have inaccurate personal data rectified, or completed if it is incomplete

(d) You have a right to have your data erased in certain circumstances

(e) You have the right to request the restriction or suppression of your personal data

(f) You have the right to data portability which allows you to obtain and reuse your personal data for your own purposes across different services

(g) You have the right to object to the processing of your personal data in certain circumstances, including for direct marketing and the use of profiling

(h) A right to lodge a complaint with the Information Commissioner's Office (ICO) as the relevant supervisory authority

For more information on your personal data rights, you can access information and advice on the ***ICO's website***.

You may exercise any of your rights at any time by contacting ***privacy@agiliosoftware.com*** with your request.

Data Retention Policy

1. About this policy

1.1 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our business operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.

1.2 This Data Retention Policy explains our requirements to retain data and to dispose of data and provides guidance on appropriate data handling and disposal.

1.3 Failure to comply with this policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

1.4 This policy covers all employees, officers, consultants, contractors, interns, casual workers, agency workers and anyone who has access to our IT and communication systems.

1.5 All team members must comply with this policy at all times. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.6 This policy does not form part of any employee's contract of employment, and we may amend it at any time.

2. Scope of the policy

2.1 This policy covers all data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters, and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

2.2 This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by employees on personal devices in accordance with our Bring Your Own Device policy.

2.3 This policy defines Agilio's guiding principles in relation to Data Retention. Each division is responsible for managing and implementing its own specific Data Retention Policy.

3. Guiding principles

3.1 Agilio Software's overarching aim in relation to the principle of storage limitation is to build retention and deletion into our systems through a privacy-by-design approach.

3.2 Through this policy, and our data retention practices, we aim to meet the following commitments:

(a) We comply with legal and regulatory requirements to retain data.

(b) We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).

(c) We handle, store, and dispose of data responsibly and securely.

(d) We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.

(e) We allocate appropriate resources, roles and responsibilities to data retention.

(f) We regularly remind employees of their data retention responsibilities.

(g) We regularly monitor and audit compliance with this policy and update this policy when required.

4. Personnel responsible for the policy

4.1 The Chief Technology Officer has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for its operation to the Data Protection Officer. Responsibility for monitoring and reviewing the operation of this policy and making any recommendations for change to minimise risks to our operations also lies with the Data Protection Officer.

4.2 All Data Asset Owners have a specific responsibility to operate within the boundaries of this policy, ensure that all team members understand the standards of behaviour expected of them and to act when behaviour falls below its requirements.

5. Definitions

5.1 A Data Asset is any data or information that has a recognisable and manageable value, risk, content, and lifecycles.

5.2 A Data Asset Owner is a senior individual responsible for ensuring that specific Data Assets are managed appropriately to meet the requirements of the Company, and that risks and opportunities are monitored.

5.3 A Record of Processing Activities (ROPA) is a record of the Company's processing activities involving personal data in a written or electronic form.

6. Responsibilities

6.1 Each Data Asset Owner is responsible for implementing an appropriate procedure that ensures the retention rules set out in this policy, for the data they have responsibility over, are adhered to.

7. Retention Periods

7.1 Personal Data must not be retained for longer than the specified period. The Data Protection Officer must review the ROPA annually to ensure that the retention periods specified against a category of personal data meet the following criteria:

(a) No shorter than legal minimum periods (where applicable)

(b) At least the length of time equivalent to any relevant statutory limitation period for the purposes of litigation

(c) No longer than it is needed

(d) With consideration to specific industry sector rules or codes

7.2 The DPO must also ensure that:

(a) Each Data Asset has a Data Asset Owner specified in the ROPA. This owner must be an individual and not a department, however, they can be identified by reference to their position i.e., Head of Sales or Managing Director.

(b) The ROPA specifies whether archiving or deletion (or both in sequence) should be used.

8. Archiving and Deletion

8.1 The Data Asset Owner is responsible for creating, communicating, and implementing an appropriate procedure that ensures that data is deleted or archived at the point specified in the ROPA. Their responsibilities can be delegated; however, the Data Asset Owner remains responsible for adherence to this policy.

8.2 Implementing could be as simple as setting a flag on a third-party system to archive or delete a record at a specified point in time or in the case of paper files, may mean arranging the safe destruction of files.

8.3 The Data Asset Owner should be aware of the data assets, where they are stored and how to get access. The Data Asset Owner is responsible for ensuring that the data is stored in such a manner where its archiving or deletion date can be clearly identified.

8.4 It is important that the data assets are not deleted before the specified retention period and not kept unjustifiably longer than is necessary after this date. Most retention periods are listed in years, therefore, where deletion is not automatic, it would be appropriate for a procedure to categorise and file data by year and have one 'destruction point' each year. This may mean that some data is held for up to one year longer than is required, however, it would be a justifiable reason to hold data for longer than specified in the ROPA.

8.5 The Data Asset Owner must contact the DPO if they would like to delete data earlier than the period specified in the ROPA.

9. Oversight Role of the Data Protection Officer (DPO)

9.1 Agilio's DPO is responsible for assessing the effectiveness of the procedures adopted by the Data Asset Owner. At least annually, the DPO should undertake an audit of some or all Data Asset Owners as part of this assessment.

Breach management and notification policy

1. About this policy

1.1 This policy covers all employees, officers, consultants, contractors, interns, casual workers, agency workers and anyone who has access to our IT and communication systems.

1.2 All team members must comply with this policy at all times. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.3 This policy does not form part of any employee's contract of employment, and we may amend it at any time.

2. Personnel responsible for the policy

2.1 The Chief Technology Officer has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for its operation to the Divisional Managing Directors. Responsibility for monitoring and reviewing the operation of this policy and making any recommendations for change to minimise risks to our operations also lies with the Managing Directors.

2.2 All managers have a specific responsibility to operate within the boundaries of this policy, ensure that all team members understand the standards of behaviour expected of them and to act when behaviour falls below its requirements.

2.3 All team members are responsible for the success of this policy and should ensure that they take the time to read and understand it.

3. Definitions

3.1 In this policy “UK GDPR” shall mean the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR) as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

3.2 A “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than losing personal data. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted, or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and

this unavailability has a significant negative effect on individuals. Examples of personal data breaches:

(a) access by an unauthorised third party

(i) deliberate or accidental action (or inaction) by a controller or processor

(ii) sending personal data to an incorrect recipient

(iii) computing devices containing personal data being lost or stolen

(iv) alteration of personal data without permission

(v) loss of availability of personal data

4. Responsibility of all team members

4.1 Every individual working with personal data has a responsibility to report a personal data breach no matter how minor it may seem. This should be done by immediately alerting their line manager AND contacting Agilio Software's Data Protection Officer via privacy@agiliosoftware.com with details of the breach. Team Members should ensure that they continue to follow Agilio's data processing policies and procedures when communicating details of the breach.

5. Step 1: Investigation, Containment and Recovery

5.1 Agilio's Data Protection Officer is responsible for investigating the breach (Lead Investigator) unless they appoint a nominee to do so. In this case, the nominee is responsible. A nominee may be appointed where there is a clear and obvious conflict of interest in the DPO investigating the complaint.

5.2 On receipt of information about a data breach, the DPO must notify a senior member of management no lower than Chief Technology Officer. The Lead Investigator must be provided with appropriate resources and access to effectively investigate the breach.

5.3 The Lead Investigator must take appropriate steps to contain the breach, assess the ongoing risks, and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

5.4 Actions the Lead Investigator may take include:

(a) Interview staff and contractors as appropriate to get comprehensive details of the incident

(b) In the case of lost or stolen equipment, cross-reference lost equipment against asset records and undertake an audit of equipment to realise full extent of missing equipment if not obvious

(c) Obtain technical advice to determine the scope of data loss

5.5 The Lead Investigator should follow all current and relevant guidance on breach risk-assessment from the ICO by risk-assessing the likelihood and severity of a range of potential adverse effects on individuals, which include:

(a) Physical harm

(b) Financial loss

(c) Identity theft/fraud

(d) Psychological distress#

(e) Humiliation or reputational damage

5.6 All risk assessments and actions taken should be recorded in writing by the Lead Investigator.

5.7 As a processor, Agilio has a further responsibility under Article 33(2) of the UK GDPR to inform any controller(s) of data it processes which has been subject to a breach. This must be done without undue delay.

6. Step 2: Informing the individuals concerned of the breach

6.1 The Lead Investigator must assess whether the breach is likely to result in a "high-risk" to the rights and freedoms of individuals. If the breach does meet this threshold, they must inform those individuals concerned without undue delay particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach.

6.2 To determine whether the breach is "high-risk" the lead investigator will need to assess both the severity of the potential or actual impact on individuals because of the breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then the risk is also higher. The Lead Investigator should follow all current and relevant guidance from the ICO. Note that a 'high risk' means the requirement to inform individuals is higher than for notifying the ICO (see "Informing the ICO" below).

6.3 If a decision is taken to inform individuals, the Lead Investigator is responsible for ensuring that the following information is provided to the relevant individuals:

(a) the name and contact details of Agilio's DPO, or other contact point where more information can be obtained

(b) a description of the likely consequences of the personal data breach, and

(c) a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects

6.4 The Lead Investigator is responsible for ensuring that the relevant individuals are provided with specific and clear advice on the steps they can take to protect themselves, and what Agilio are willing to do to help them. Depending on the circumstances, this may include such things as:

(a) forcing a password reset

(b) advising individuals to use strong, unique passwords, and

(c) telling them to look out for phishing emails or fraudulent activity on their accounts

6.5 This information should be communicated in clear and plain language. A written record of actions taken and those contacted or decisions not to inform individuals should be recorded in writing.

7. Informing the ICO of the breach

7.1 When a personal data breach has occurred, the Lead Investigator will need to establish the likelihood of the risk to people's rights and freedoms. If a risk is likely, the ICO must be notified—this is known as a notifiable breach. If a risk is unlikely, the ICO do not need to be contacted. A written record of actions taken or not taken must be taken by the Lead Investigator.

7.2 A notifiable breach must be reported to the ICO without undue delay, but not later than 72 hours after the controller (Agilio in this case) becoming aware of it. When Agilio is considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

7.3 Breaches to the ICO are normally reported via telephone where a complete record of the breach can be obtained. Further details and contact information can be found on the ICO website.

8. Evaluation and Response

8.1 All breaches, regardless of whether or not they need to be reported to the ICO, should be recorded. Article 33(5) of the UK GDPR requires an organisation to document the facts regarding the breach, its effects and the remedial action taken.

8.2 Following the breach, the Lead Investigator should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented.

8.3 The Lead Investigator should recommend responses to a senior member of management no lower than Managing Director. Recommendations could include:

(a) Mandatory data protection refresher training

(b) Support and supervising until employees are proficient in their role

(c) Updating policies and procedures

(d) Working to a principle of “check twice, send once”

(e) Investigating the root causes of breaches and near misses; and

(f) Restricting access and auditing systems]

(g) Implementing technical and organisational measures, e.g., disabling autofill

8.4 Remedial action that is approved should be recorded by the Lead Investigator against the breach.