Data Protection Policy

TIRO

Table of Contents

Section 1 Introduction

1.1 Introduction

This Policy sets out the obligations of TIRO Ltd ("Tiro") regarding data protection and the rights of staff, customers, business contacts, suppliers, visitors etc., ("data subjects") in respect of their personal data under Data Protection Law. "Data Protection Law" means all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK 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, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.

This Policy sets Tiro's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be always followed by Tiro, its employees, agents, contractors, or other parties working on behalf of Tiro.

1.2 Definitions

"Consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them;
"Data controller"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, Tiro is the data controller of all personal data relating to staff, customers, visitors, suppliers, and business contacts used in our business for our commercial purposes;
"Data processor"	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
"Data subject"	means a living, identified, or identifiable natural person about whom Tiro holds personal data;

"EEA"	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
"Personal data"	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;
"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 transmitted, stored, or otherwise processed;
"Processing"	means any operation or set of operations performed on personal data or sets of personal data, whether 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;
"Pseudonymisation"	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
"Special category personal data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

1.3 Scope

Tiro is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

Tiro's Data Protection Lead is The Director of Quality and Compliance. The Data Protection Lead is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

All managers, department heads, and the senior leadership team are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of Tiro comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Lead. In particular, the Data Protection Lead should always be consulted in the following cases:

- if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed.
- if consent is being relied upon to collect, hold, and/or process personal data.
- if there is any uncertainty relating to the retention period for any type(s) of personal data.
- if any new or amended privacy notices or similar privacy-related documentation are required.
- if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests).
- if a personal data breach (suspected or actual) has occurred.
- if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data.
- if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors).
- if personal data is to be transferred outside of the UK and there are questions relating to the legal basis on which to do so.
- when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment.
- when personal data is to be used for purposes different to those for which it was originally collected.
- if any automated processing, including profiling or automated decision-making, is to be carried out; or
- if any assistance is required in complying with the law applicable to direct marketing.

1.4 The Principles of Data Protection

Data protection is about protecting people from misuse of their personal information This Policy aims to ensure compliance with Data Protection Law. The UK GDPR sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

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

in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR to safeguard the rights and freedoms of the data subject.

- processed in a manner that **ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

1.5 The Rights of Data Subjects

The UK GDPR sets out the following key rights applicable to data subjects:

- the right to be informed.
- the right of access.
- the right to rectification.
- the right to erasure (also known as the 'right to be forgotten').
- the right to restrict processing.
- the right to data portability.
- the right to object.
- rights with respect to automated decision-making and profiling.

Section 2
Our Procedures

2.1 Lawful, Fair and Transparent Data Processing

Tiro must establish a lawful basis for processing data. Employees must ensure that any data they are responsible for managing has a documented lawful basis approved by the Data Protection Lead in the information asset register. It is each employee's responsibility to check the lawful basis for any data they are working with and ensure all their actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

- **Consent**: We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
- **Contract:** The processing is necessary to fulfil or prepare a contract for the individual.
- **Legal obligation**: We have a legal obligation to process the data (excluding a contract).
- **Vital interests**: Processing the data is necessary to protect a person's life or in a medical situation.
- **Public task**: Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
- **Legitimate interest**: The processing is necessary for our legitimate interests and does not outweigh the individual's rights.

In certain circumstances, when processing information on employees Tiro may process 'special category of person data (also known as "sensitive personal data"), at least one of the following conditions must be met:

- the data subject has given their **explicit consent** to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so).
- the processing is necessary for the **purpose of carrying out the obligations and exercising specific rights of the data controller** or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides for appropriate safeguards for the fundamental rights and interests of the data subject).
- the processing is **necessary to protect the vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its **legitimate activities**, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects.
- the processing relates to personal data which is **manifestly made public by the data subject.**

- the processing is necessary for the **conduct of legal claims** or whenever courts are acting in their judicial capacity.
- the processing is **necessary for substantial public interest reasons**, based on law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.
- the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services based on law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR.
- the processing is **necessary for public interest reasons in the area of public health,** for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy).
- the **processing is necessary for archiving purposes in the public interest, scientific or historical research purposes**, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

2.1.1 Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

- Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.
- Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.
- Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.
- If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.
- If special category personal data is processed, Tiro shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice to capture their consent.

- In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained to ensure that Tiro can demonstrate its compliance with consent requirements.

2.1.2 Deciding which condition to rely on

2.1.2.1 When Tiro are assessing the lawful basis, we will first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. We cannot rely on a lawful basis if we can reasonably achieve the same purpose by some other means. Where more than one lawful basis applies, Tiro will rely on what will best fit the purpose, not what is easiest.

2.1.2.2 We will always consider the following factors and document the answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

2.1.2.3 Tiro's commitment to accountability and transparency requires that we document this process through privacy policies (candidate, staff, website) and annual/biannual audit and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

2.1.2.4 We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This will be achieved via a privacy information notice. This applies whether we have collected the data directly from the individual, or from another source.

2.1.2.5 Employees who are responsible for assessing the lawful basis and implementing the privacy notice for new processing activities must have them approved by the Data Protection Lead.

2.2 Specified, Explicit, and Legitimate Purposes

2.2.1 Tiro collects and processes the personal data either

- directly from data subjects (e.g., when a candidate applies for a job vacancy by submitting a CV, or when an apprentice applies, or when we pay a supplier's invoice).

- indirectly obtained from third parties (e.g., when we use data made available in the public domain for prospecting).

2.2.2 Tiro only collects, processes, and holds personal data for the specific purposes set out in our privacy policy or for other purposes expressly permitted by Data Protection Law.

2.2.3 Data subjects must be kept informed at all times of the purpose or purposes for which Tiro uses their personal data.

2.3 Adequate, Relevant, and Limited Data Processing

2.3.1 Tiro will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

2.3.2 Employees, agents, contractors, or other parties working on behalf of Tiro may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

2.3.3 Employees, agents, contractors, or other parties working on behalf of Tiro may process personal data only when the performance of their job duties requires it. Personal data held by Tiro cannot be processed for any unrelated reasons.

2.4 Accuracy of Data and Keeping Data Up to Date

2.4.1 Tiro shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out further on in this policy.

2.4.2 The accuracy of personal data shall be checked when it is collected and at a minimum on an annual basis. If any personal data is found to be inaccurate or out of date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

2.5 Data Retention

Under the Data Protection Legislation, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the Data Protection Legislation to protect that data).

Tiro shall not retain any personal data for any longer than is necessary considering the purpose(s) for which that data is collected, held, and processed. Different types of personal data, used for different purposes, will necessarily be retained for different periods **(**and its retention periodically reviewed), as set out in Appendix A: Statutory & Non Statutory Retention Periods.

When establishing and/or reviewing retention periods, the following shall be considered:

- The objectives and requirements of Tiro.
- The type of personal data in question.
- The purpose(s) for which the data in question is collected, held, and processed.
- Tiro's legal basis for collecting, holding, and processing that data.
- The category or categories of data subject to whom the data relates.

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

Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within Tiro to do so (whether in response to a request by a data subject or otherwise).

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

2.5.1 Data Disposal

2.5.1.1 A review of the Processing Activity will take place within 30 days after the expiry of the retention period. There will be a considered appraisal of the contents of the Processing Activity. The Data Protection Lead will undertake the review. The disposition decision must be reached having regard to:

- On-going business and accountability need(s) (including audit).
- Current applicable legislation.
- Whether the Information Asset has any long-term historical or research value.
- Best practice in the applicable professional field (for example human resources).
- Costs associated with continued storage versus costs of destruction.
- The legal, political, and reputational risks associated with keeping, destroying, or losing control over the Information Asset.

2.5.1.2 Decisions must not be made with the intent of denying access or destroying evidence. No destruction of an Information Asset will take place without assurance that:

- The Personal Data is no longer required by any part of Tiro.
- No work is outstanding by any part of Tiro
- No litigation or investigation is current or pending which affects the Information Asset.

- There are no current or pending Subject Access Requests which affect the Information Asset.

2.5.1.4 Upon the expiry of the data retention periods set out in Appendix A of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- **Destruction of Paper Records -** Destruction of paper records can be carried out in a variety of ways, including shredding, pulping, and burning. Paper records will be destroyed with the level of security required by the confidentiality of their contents. If paper records containing sensitive personal data have been shredded, the shredded paper will be handled securely. Paper records awaiting destruction will be stored securely.

  All outsourced shredding contractors will comply with BS 8470, the British Standard that specifies the disposal of confidential material, BS 7858, the British Standard that specifies a Code of Practice for security screening of individuals and third-party individuals and be members of the United Kingdom Security Shredding Association (UKSSA).

- **Destruction of Digital Records -** With digital records the deletion from a server or hard drive may not be sufficient. The digital records may no longer be visible, but they are not beyond any possibility of recovery. More extreme measures may be needed to achieve full destruction, e.g., overwriting with random digital code enough times to eliminate the data.

  If an external contractor is being used for destruction of the digital records, ensure the contract specifies clearly what is required, including transmission of Information Asset (e.g., hard drive or laptop) off-site and what constitutes destruction. The contractor will be required to supply a certificate of destruction and, for confidential Information Assets, a certificate of confidential destruction.

  Electronic media such as USB drives and digital files will be reformatted if the media type allows it or erased if formatting is not possible.

  The Information Commissioner's Office guidance on deletion clearly states (emphasis added):

  If you delete an item to you recycle bin, perform a 'quick format' of your hard drive or perform a factory reset of your device, you will be typically deleting data. However, data recovery experts can restore this data. ***Even with that said, data deletion is generally an adequate method of removing personal data from a device in most situations****.'*

  In short, therefore, selecting the data Tiro wishes to delete, deleting it, and emptying *Recycle Bins* or *Trash*, will generally be sufficient, particularly for Tiro handling comparatively low-risk personal data.

2.6 Secure Processing

Tiro shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

Data security must be always maintained by protecting the confidentiality, integrity, and availability of all personal data as follows:

- only those with a genuine need to access and use personal data and who are authorised to do so may access and use it.
- personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed.
- authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

2.6.1 Data Security - Transferring Personal Data and Communications

Tiro shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing special category or personal data must be encrypted.
- All emails containing personal data must be marked “confidential”.
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email, and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

2.6.2 Data Security - Storage

Tiro shall ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords.

- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.
- All personal data stored electronically should be backed up daily with backups stored offsite. All backups should be encrypted.
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Tiro or otherwise without the formal written approval of the Data Protection Lead and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is necessary.
- No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of Tiro and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Tiro where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the applicable Data Protection Law (which may include demonstrating to Tiro that all suitable technical and organisational measures have been taken).

2.6.3 Data Security - Use of Personal Data

Tiro shall ensure that the following measures are taken with respect to the use of personal data:

- No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of Tiro requires access to any personal data that they do not already have access to, such access should be formally requested the Data Protection Lead.
- No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of Tiro or not, without the authorisation of Data Protection Lead.
- Personal data must be always handled with care and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time.
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period, the user must lock the computer and screen before leaving it.
- Where personal data held by Tiro is used for marketing purposes, it shall be the responsibility of the Marketing Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

2.6.4 Data Security - IT Security

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

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and

lowercase letters, numbers, and symbols. All software used by Tiro is designed to require such passwords.

- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Tiro, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.
- All software (including, but not limited to, applications and operating systems) shall be kept up to date. Tiro's external IT support staff shall be responsible for installing all security-related updates as soon as reasonably and practically possible**.**
- No software may be installed on any Tiro-owned computer or device without the prior approval of the Data Protection Lead.

2.6.5 Organisational Measures

- Tiro shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:
- All employees, agents, contractors, or other parties working on behalf of Tiro shall be made fully aware of both their individual responsibilities and Tiro's responsibilities under Data Protection Law and under this Policy and shall be provided with a copy of this Policy.
- Only employees, agents, contractors, or other parties working on behalf of Tiro that need access to, and use of, personal data to carry out their assigned duties correctly shall have access to personal data held by Tiro.
- All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data.
- All employees, agents, contractors, or other parties working on behalf of Tiro handling personal data will be appropriately trained to do so.
- All employees, agents, contractors, or other parties working on behalf of Tiro handling personal data will be appropriately supervised.
- All employees, agents, contractors, or other parties working on behalf of Tiro handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise.
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.
- All personal data held by Tiro shall be reviewed periodically, as set out in the Retention Schedules in Appendix A.
- The performance of those employees, agents, contractors, or other parties working on behalf of Tiro handling personal data shall be regularly evaluated and reviewed.
- All employees, agents, contractors, or other parties working on behalf of Tiro handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract.

- All agents, contractors, or other parties working on behalf of Tiro handling personal data must ensure that all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Tiro arising out of this Policy and Data Protection Law.
- Where any agent, contractor or other party working on behalf of Tiro handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Tiro against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

2.7 Accountability and Record-Keeping

The Data Protection Lead is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

Tiro shall always follow a privacy by design approach when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects.

All employees, agents, contractors, or other parties working on behalf of Tiro shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Tiro policies.

Tiro's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

Tiro shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- the name and details of Tiro, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared).
- the purposes for which Tiro collects, holds, and processes personal data.
- Tiro's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data.
- details of the categories of personal data collected, held, and processed by Tiro, and the categories of data subject to which that personal data relates.
- details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards.
- details of how long personal data will be retained by Tiro (please refer to Tiro's Data Retention Policy).
- details of personal data storage, including location(s).
- detailed descriptions of all technical and organisational measures taken by Tiro to ensure the security of personal data.

2.7.1 Annual Data Protection Audits

2.7.1.1 On an annual basis the Data Protection Lead will conduct a Data Protection Audit to assess Tiro's current state of play. The Audit will determine the degree to which our current practices align with the

requirements set down in law and identifying areas for improvement. The audit reviews the following:

- Accountability and Governance.
- Register of Processing Activities (data mapping).
- Data Transfers Outside the UK.
- Privacy Policies.
- Training and Awareness.
- Policies and Procedures.
- Data Processor Due Diligence.
- Physical and Technical Security.

2.7.1.2 The Data Protection Lead will conduct interviews/meetings with heads of department, senior managers, and the executive team to discuss each of the above areas. Upon conclusion of the audit the Data Protection Lead will draft an action plan, allocating action owners and target completion dates.

2.7.2 Data Protection Impact Assessments and Privacy by Design

2.7.2.1 In accordance with the privacy by design principles, Tiro shall carry out Data Protection Impact Assessments for all new projects (e.g., when deciding to implement a new CRM, accounting system, and HR system) and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

The principles of privacy by design should be always followed when collecting, holding, and processing personal data. The following factors should be taken into consideration:

- the nature, scope, context, and purpose or purposes of the collection, holding, and processing.
- the state of the art of all relevant technical and organisational measures to be taken.
- the cost of implementing such measures; and
- the risks posed to data subjects and to Tiro, including their likelihood and severity.

2.7.2.2 Data Protection Impact Assessments shall be overseen by the Data Protection Lead and shall address the following:

- the type(s) of personal data that will be collected, held, and processed.
- the purpose(s) for which personal data is to be used.
- Tiro's objectives.
- how personal data is to be used.
- the parties (internal and/or external) who are to be consulted.
- the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.
- risks posed to data subjects.

- risks posed both within and to Tiro; and
- proposed measures to minimise and handle identified risks.

2.8 Transferring Personal Data to a Country Outside the UK

2.8.1 Tiro may, from time to time, transfer ('transfer' includes making available remotely) personal data to countries outside of the UK. The UK GDPR restricts such transfers to ensure that the level of protection given to data subjects is not compromised.

2.8.2 Personal data may only be transferred to a country outside the UK if one of the following applies:

- The UK has issued regulations confirming that the country in question ensures an adequate level of protection (referred to as 'adequacy decisions' or 'adequacy regulations'). From 1 January 2021, transfers of personal data from the UK to EEA countries will continue to be permitted.
- Transitional provisions are also in place to recognise pre-existing EU adequacy decisions in the UK.
- Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK (this includes those adopted by the European Commission prior to 1 January 2021), an approved code of conduct, or an approved certification mechanism.
- The transfer is made with the informed and explicit consent of the relevant data subject(s).
- The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the data subject and Tiro; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for Tiro's legitimate interests.

2.9 Managing Individual Rights

2.9.1 Keeping Data Subjects Informed (Privacy Notices)

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

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

2.9.1.1. The following information shall be provided in the form of a privacy notice:

- details of Tiro including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Lead.
- the purpose(s) for which the personal data is being collected and will be processed and the lawful basis justifying that collection and processing.
- where applicable, the legitimate interests upon which Tiro is justifying its collection and processing of the personal data.
- where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.
- where the personal data is to be transferred to one or more third parties, details of those parties.
- where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place.
- details of applicable data retention periods.
- details of the data subject's rights under the UK GDPR.
- details of the data subject's right to withdraw their consent to Tiro's processing of their personal data at any time.
- details of the data subject's right to complain to the Information Commissioner's Office.
- where the personal data is not obtained directly from the data subject, details about the source of that personal data.
- where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

2.9.2 Data Subject Access Requests

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which Tiro holds about them, what it is doing with that personal data, and why.

2.9.2.1 How to Recognise a Data Subject Access Request

- The Data Protection Legislation does not set out a particular format which a data subject access request "SAR") must follow. A SAR may be made orally or in writing, to any part of Tiro, and by any means of communication. A SAR does not need to use the words 'subject access request', 'data protection', 'personal data' or similar terms. This means that anyone in Tiro could receive a SAR and it may not be immediately obvious that a SAR has been received.

- SARs may use more general terminology, using terms such as 'information' rather than 'personal data'. For example, a message sent to Tiro via social media such as 'please provide details of all the information you have about me' will be a valid SAR and must be treated in the same

way as a more formal communication referring specifically to a 'subject access request' and data subjects' rights under the GDPR.

- Individuals may make SARs on their own behalf. It is also possible to make an SAR via a third party:

- This may be a solicitor making a request on behalf of a client, or it may be one private individual making the request on behalf of another. This is permissible, but you must be satisfied that the individual making the request has the authority to act on behalf of the data subject concerned.

- In certain limited cases, an individual may not have the mental capacity to manage their own affairs. In these cases, the Mental Capacity Act 2005 enables a third party to make a SAR on behalf of that individual.

- Adults, such as parents or guardians, may make SARs on behalf of children. The right of access itself, however, remains the child's right. When dealing with a SAR about a child it is important to consider whether that child is mature enough to understand their rights. If so, a response directly to the child should be considered. It may, however, be permissible to allow the adult to exercise the child's right on the child's behalf if the child has given their authorisation, or if it is evident that doing so is in the child's best interests.

- When a SAR is identified, or if a communication or request is received and you are in anyway unsure whether it is a SAR, it should be immediately forwarded to Tiro's Data Protection Lead.

2.9.2.2 What to do When a Subject Access Request is Received? Tiro has a limited timeframe within which to respond to a SAR, so it is important to act quickly.

Unless you are authorised to handle a SAR, it must be forwarded to the Data Protection Lead or to the relevant member of staff immediately. Please do not take any further action with respect to any SAR unless you are authorised to do so.

SARs may come in any form. This will determine how to forward the SAR to the appropriate member of staff:

- For SARs received by email or via social media, the message, or a link, if appropriate must be forwarded immediately to Tiro's Data Protection Lead.
- For SARs received by post or in any other hardcopy form, the SAR should first be scanned and emailed immediately to Tiro's Data Protection Lead and the original sent to the same recipient using the most direct and secure means possible (e.g., in person, by courier if available).
- For SARs made verbally, the name and contact details of the data subject should first be recorded before informing the data subject that the Tiro's Data Protection Lead will contact them for full details of their SAR. The data subject's details and any other information provided by the data subject should be emailed immediately Tiro's Data Protection Lead, including details of the time and date on which the SAR was made.

Tiro's Data Protection Lead should respond to you, confirming receipt of the SAR, within two business days of you sending it. If you do not receive a response within this period, you must contact them again to confirm receipt.

The Data Protection Lead must keep a record for management purposes and log any queries in the SAR log file. Create a file for each subject access request and keep in it:

- Copies of the correspondence between data protection lead and the data subject, and between data protection lead and any other parties.
- A record of any telephone conversations used to verify the identity of the data subject.
- A record of your decisions and how you came to those decisions.
- Copies of information sent to the data subject.
- The file should be kept for one year and then securely destroyed.

2.9.2.3 Identifying Data Subjects and Clarifying Requests

Before responding to a SAR, all reasonable steps must be taken to verify the identity of the individual making the request and, if Tiro is processing a large amount of personal data about them, to clarify their request (i.e., to specify the personal data or processing to which their SAR relates). Information requested for such purposes must be reasonable and proportionate. Individuals must not be asked to provide any more information than is reasonably necessary.

If additional information is required to confirm an individual's identity, the individual must be informed as soon as possible. If additional information is required, the time limit for responding to a SAR does not begin until that information is received.

If additional information is required to respond to the SAR, the individual must be informed as soon as possible. Note, however, that if additional information is required, the time limit for responding to a SAR is not affected and a response must still be given within one month of receipt of the SAR (subject to the possible extensions to the time limit explained below).

If a SAR is made by a third party on behalf of a data subject, the individual acting on behalf of the data subject must be required to provide sufficient evidence that they are authorised to act on the data subject's behalf.

Examples of information that may be requested to confirm an individual's identity include:

- A copy of the individual's passport.
- A copy of the individual's driving licence.

If, having requested additional information to verify an individual's identity, it is still not possible to do so (if, for example, the individual does not comply), Tiro may refuse to comply with a SAR, as set out below.

If, having requested additional information to clarify a SAR, the individual does not comply, Tiro must still endeavour to comply with the SAR by making reasonable searches for the personal data relating to the request.

2.9.2.4 Can we Charge a Fee?

Under normal circumstances, the Data Protection Legislation prohibits the charging of a fee for handling a SAR. Tiro does not normally charge for SARs.

In limited cases, it is permissible to charge a 'reasonable fee' to cover the administrative costs of complying with a SAR if that SAR is 'manifestly unfounded', 'excessive', or if a data subject requests further copies of their data following the SAR. In certain cases, it may also be permissible to refuse to comply with a SAR, as set out in the policy.

2.9.2.5 How Much Time Do We Have to Respond to the SAR?

Under normal circumstances, Tiro must respond to a SAR 'without undue delay' and, at the latest, within one month of receipt. The date of receipt of all SARs must be recorded, along with the due date for response. Under the Data Protection Legislation, the one-month period referred to above begins on the calendar day – not business day – that the request is received and ends on the corresponding calendar day in the following month (or, if the following month is shorter and does not have a corresponding day (e.g., January 31st to February 28th), the last day of that month).

Consequently, the time limit set by Tiro for responding to SARs is 28 calendar days. If the last day of the time limit falls on a weekend or bank holiday, the time limit is extended to the next business day.

If additional information is required from the individual making the SAR to confirm an individual's identity, as described in the section above, the time limit begins on the day that such information is received.

If the SAR is complex, or if the same data subject makes several SARs, it is permissible to extend the time limit by up to two months. If such an extension is necessary, the data subject must be informed, in writing, of the reason(s) for the extension within the original one-month time limit.

2.9.2.6 What Information Should We Provide?

Data subjects must be provided with the following information in response to a SAR:

a. the purposes for which Tiro collects, holds, and processes their personal data.

b. the categories of personal data involved.

c. the recipients or categories of recipient to whom Tiro discloses their personal data.

d. details of how long Tiro retains their personal data or, if there is no fixed period, our criteria for determining how long it will be retained.

e. details of the data subject's right to ask Tiro to rectify or erase their personal data, or to restrict or object to our processing of it.

f. details of the data subject's right to make a complaint to the ICO or to another supervisory authority.

g. if any of the personal data in question was not obtained from the data subject, details of the source of that data.

h. if Tiro carries out any automated decision-making (including profiling), details of that automated decision-making, including a meaningful

explanation of the logic involved and the significance and envisaged consequences for the data subject; and

i. if Tiro transfers their personal data to a third country (i.e., nonUK) or international organisation, details of the safeguards in place to protect that data.

In cases where a SAR relates to automated decision-making, the following shall apply:

a. Where a SAR relates to the logic underlying an automated decision that has been taken with respect to important matters relating to the data subject, the data subject must be provided with an explanation of the logic involved, subject to the following conditions:

b. the decision-making process in question must be solely automated (i.e., there must be no human involvement in the process); and

c. the information should be provided in such a way as to protect Tiro's intellectual property rights and trade secrets.

d. The data subject may also request information related to the automated decision itself, they may seek to exercise the right to human intervention (i.e., for Tiro to appoint a person to review the automated decision), to express their own point of view about the decision, and/or to contest it. If a data subject making a SAR seeks to exercise their rights with respect to automated decisions, Tiro's Data Protection Lead shall handle the same in accordance with the Data Protection Legislation.

The information set out above must be provided:

- in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.
- in writing; and
- if the data subject has made the SAR electronically, in a commonly used electronic format (unless the data subject requests otherwise); and • where possible, by using Tiro's secure online system, providing secure access for data subjects to their personal data.

It is important to note that data subjects are only entitled to access personal data that Tiro holds about them. If information located in the process of responding to a SAR does not meet the definition of "personal data", the Data Protection Legislation does not entitle the data subject to access it. In certain cases, it may be necessary to separate personal data from nonpersonal data when responding to a SAR.

2.9.2.7 How Can We Locate the Information?

Tiro holds personal data in various locations and in several systems. It is important to identify the type(s) of personal data to which a SAR relates to search in the correct place. Tiro's Register of Processing Activities sets out what personal data is processed, where it is stored and who is responsible for the system (in some instances, you may require support from a Third-Party supplier to extract the appropriate information.

2.9.2.8 Can We Refuse to Respond to a Subject Access Request?

In certain cases, it is permissible for Tiro to refuse to comply with a SAR:

- if it is not possible to identify the individual making the SAR after requesting additional verification; or
- if the request is 'manifestly unfounded' or 'excessive', considering whether the request is repetitive in nature. In such cases, it is also possible to request a 'reasonable fee' to handle it.

If either of the above grounds applies, Tiro's refusal to comply with the SAR must be justified and an explanation must be provided to the individual making the SAR within one calendar month after receiving the SAR. The individual must also be informed of their right to complain to the ICO or another supervisory authority and of possibility of seeking a judicial remedy.

Certain exemptions to the right of access are also included in the Data Protection Legislation.

2.9.2.9 Are there exemptions to the Right of Access?

The Data Protection Legislation provides several exemptions which apply to SARs and therefore justify Tiro refusing to comply with a SAR. Those most likely to be applicable within Tiro are situations in which the personal data in question is:

- subject to legal or litigation privilege; or
- purely personal or exists for a household activity; or
- a reference given (or to be given) in confidence for purposes of employment, training, or education; or
- is processed for management forecasting or management planning purposes in relation to a business or other activity (but only to the extent that complying with the SAR would prejudice the conduct of the business or activity); or
- consists of records of intentions with respect to negotiations between employer and employee (but only to the extent that complying with the SAR would prejudice such negotiations); or
- contains personal data concerning a third party; or
- is of a type likely to prejudice the prevention or detection of a crime, or the apprehension or prosecution of offenders if it is disclosed.

Additional exemptions relate to more specific (and generally public) matters such as national security. If any concerns or questions arise with respect to exemptions which may or may not apply during the process of handling a SAR (including, but not limited to those set out above), those questions should be referred to Tiro's Data Protection Lead and/or to the ICO.

2.9.3 Rectification of Personal Data

Data subjects have the right to require Tiro to rectify any of their personal data that is inaccurate or incomplete.

Tiro shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing Tiro of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

If any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

2.9.4 Erasure of Personal Data

Data subjects have the right to request that Tiro erases the personal data it holds about them in the following circumstances:

- it is no longer necessary for Tiro to hold that personal data with respect to the purpose(s) for which it was originally collected or processed.
- the data subject wishes to withdraw their consent to Tiro holding and processing their personal data.
- the data subject objects to Tiro holding and processing their personal data (and there is no overriding legitimate interest to allow Tiro to continue doing so) (see Part 21 of this Policy for further details concerning the right to object).
- the personal data has been processed unlawfully.
- the personal data needs to be erased in order for Tiro to comply with a particular legal obligation.

Unless Tiro has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

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

2.9.5 Restriction of Personal Data Processing

Data subjects may request that Tiro ceases processing the personal data it holds about them. If a data subject makes such a request, Tiro shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

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

2.9.6 Objections to Personal Data Processing

Data subjects have the right to object to Tiro processing their personal data based on legitimate interests, for direct marketing (including profiling).

Where a data subject objects to Tiro processing their personal data based on its legitimate interests, Tiro shall cease such processing immediately, unless it can be demonstrated that Tiro's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to Tiro processing their personal data for direct marketing purposes, Tiro shall cease such processing promptly.

Section 3
Data Breaches

3.1 Data Breaches

Any data breach of personal information must be recorded by Tiro. The GDPR sets out the requirements to respond to a personal data breach. Data controllers (Tiro) must report certain types of data breach to the supervisory authority (Information Commissioners Officer (ICO)) without undue delay and within 72 hours or becoming aware of data breach. Tiro will be required to notify individuals affected by the data breach in circumstances where it is likely to cause a high risk to their rights and freedoms.

A breach notification to the ICO should include:

1. The nature of the personal data breach including, where possible:
   - The categories and approximate number of individuals concerned.
   - Categories and approximate number of personal data records concerned.

2. The name and contact details of the Data Protection Lead.

3. A description of the likely consequences of the personal data breach.

4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measure taken to mitigate any possible adverse effects.

To effectively monitor data breaches, the Data Protection Lead will document each data breach in Tiro Data Breach Log file, including facts of the breach, the effects and action taken. The Data Protection Lead, with relevant support from staff in the organization, will assess the likely risk and impact on individuals affected by the breach immediately, and where necessary report to the ICO within 72 hours via the **ICO website.** Further details about the breach will be established using the data breach process.

3.1.1 Data Breach Process

To understand why a breach occurred and prevent further breaches, the Data Protection Lead will:

- Determine how the breach happened.
- Determine what, if anything, could have been done to prevent it.
- Understand what can be done to prevent future breaches.
- Determine how soon the changes can be implemented.
- Update and cascade training for employees as soon as possible
- Provide an update to individuals affected by the breach on the outcome of the investigation and what we are doing to prevent future breaches.

- Provide an update to the Partnership Board on the outcome of the investigation and what we are doing to prevent future breaches.
- Deal with any complaints
- Respond to any requests for further information from the Information Commissioner's Office (if relevant).
- implement and comply with recommendations from the Information Commissioner's Officer.

If an employee, agent, contractor, or other party working on behalf of Tiro becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Please complete the first section of the data breach report form (Appendix B) and send this to the Data Protection Lead immediately.

3.1.2 Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act 2018 allows personal data to be disclosed to law enforcement agencies without consent of the data subject.

Under these circumstances, Tiro will disclose requested data. However, the Data Protection Lead will ensure the request is legitimate, seeking assistance from the board and from the organisation's legal advisers where necessary.

Section 4 Policy Compliance

4.1 Policy Compliance

If any user is found to have breached this policy, they may be subject to Tiro's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Any unauthorised disclosure of personal data to a third party by an employee will be viewed seriously and may result in disciplinary proceedings.

The Board of Directors are accountable for compliance of this policy. A director could be personally liable for any penalty arising from a breach that they have made.

4.1.1 Review and revision

This policy must be reviewed every 12 months and, if appropriate, will be amended to maintain its relevance. Further reviews will be undertaken to reflect changes in legislation or standards. The Data Protection Lead will undertake policy review.

Appendix 1: Statutory & Non-Statutory Retention Periods

Tiro will only keep information for as long as it is needed to carry out its business objectives and to comply with any third-party obligations.

Type	Regulation\Best Practice	Retention Period
Accidents	The Reporting of Injuries, Disease and Dangerous Occurrences Regulation 1995	3 years after the last entry or end of investigation (if later)
Accounts (including income / monies received)	Companies Act 1985 section 221 as modified by the Companies Act 1989 and Companies Act 2006	6 years from the end of the financial year in which transaction was made.
Application forms (or CVs) and interview notes for unsuccessful candidates	Disability Discrimination Act 1995 and Race Relations Act 1976 recommend 6months. One year limitation for defamation actions under Limitations Act 1980	Six months to a year.
Contract with clients, suppliers, or agents, rental/hire purchase agreements	Limitations Act 1980	6 years after expiry or termination of the contract.
Employee / Personnel Records (including training records)	Limitations Act 1980	6 years after employment ceases. Note: Records for senior executives should be kept permanently for historical purposes.
Income Tax / National Insurance / Correspondence	The Income Tax (employments) Regulation 1993	Not less than 3 years after the end of the financial year to which they relate
Insurance Documents (including policies, claims, certificates and accident reports)	Data Protection Act, Employer's Liability Regulations 1998	3 years after policy lapses; 3 years after claim settled; 40 years EL certificate; 3 years after settlement (accident)
Payroll	Taxes Management Act 1970	6yrs Wage, Salary, Overtime, Bonuses, Expenses

Pensions (deductions and superannuation)	Pensions Act	6 years plus current year.
Purchase invoices and Supplier Documentation	Companies Act 1985	6 years from the end of the financial year in which the transaction was made.
Sick Pay / Calculations / Certificate / Self Certificates	The Statutory Maternity (General) and Statutory Sick Pay (General) Regulations 2005	3 years after tax year-end in with the period ends.
Direct Marketing data such a newsletter mailing lists	Based on the ICO's guidance on Consent	Delete immediately upon a 'right to be forgotten' request or 'unsubscribe' received. Review consent record every 2 years from the date consent granted.

Documents not included in this schedule do not have an agreed retention period or a legal requirement to retain. For these documents, such as internal emails, minutes of team meetings or work plans the following guidance should be followed.

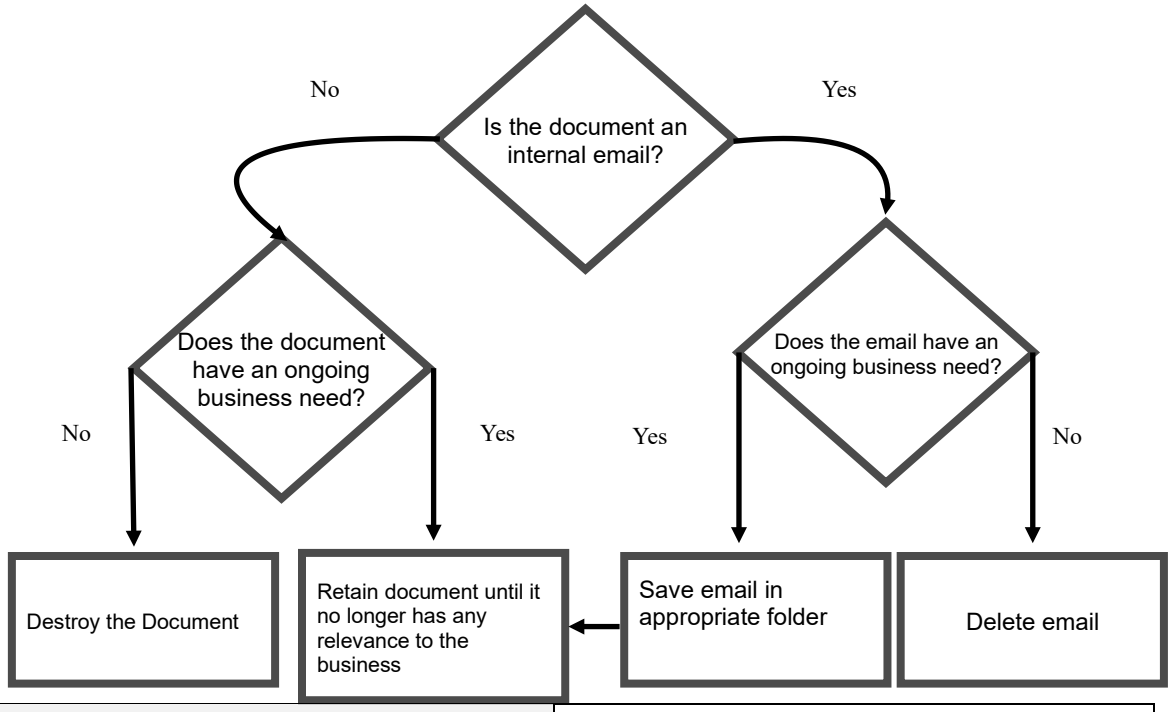
APPENDIX 2: DATA BREACH REPORTING FORMS

Please act promptly to report any data breaches. If you discover a data breach, please notify your Data Protection lead, complete Section 1 of this form and email it to

Section 1: Notification of Personal Data Breach

To be completed by the individual who identified the breach or is reporting the breach.

Date incident was discovered:	



Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection lead	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity

To be completed by the Data Protection Lead

Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of personal data loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for TIRO or third parties?	
How many data subjects are affected?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data **Special categories personal data** (as defined in the Data Protection Legislation) relating to a living, identifiable individual's: a) racial or ethnic origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health;	

Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	

Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action Taken To be completed by Data Protection Lead.

Incident number	
Report received by:	
On (date):	
Action taken by responsible lead	
Follow up action required/recommended:	
Reported to Data Protection Lead on (date):	
Reported to other internal stakeholders (details, dates):	

For use of Data Protection lead	
Notification to ICO	**YES/NO If YES, notified on: Details:**

Notification to data subjects	**YES/NO If YES, notified on: Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on: Details:**

Appendix A: Change Control Log

Version	Details of amendments/ change	Author	Formal approval required	Approved by	Date of approval	Date adopted by the Board
	N/A	Paul Irving, Operational	Y	Charlotte Blant, CEO	January, 2022	January, 2022
V1.1	Removed names, added Tiro throughout, added suggestions from Jan reviews	Paul Masterman, DPL	Y	Charlotte Blant, CEO	Oct 23	