DATA PROTECTION POLICY

1. INTRODUCTION

1.1 This Policy sets out how Invest NI handles Personal Data processed within the Organisation and applies to all Personal Data we Process regardless of the media on which that data is held.

1.2 This Policy applies to all Invest NI Personnel. You must read, understand and comply with this Policy when Processing Personal Data on our behalf and undertake training on its requirements.

1.3 Related Policies are available to help you interpret and act in accordance with this Policy. You must also comply with all such Related Policies.

1.4 Your compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action and in serious cases, it could result in the termination of your employment.

1.5 A glossary of terms used within this policy can be found at Annex A.

2. SCOPE

2.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations.

2.2 Protecting the confidentiality, integrity and availability of Personal Data is a critical responsibility that we take seriously at all times. The Organisation is exposed to potential fines of up to €20 million (approximately £18 million) for failure to comply with the provisions of the GDPR.

2.3 The Board is ultimately responsible for ensuring that all Invest NI Personnel comply with this Policy and the need to implement appropriate practices, processes, controls and training to ensure such compliance.

2.4 The Data Protection Officer (DPO) is responsible for overseeing and advising Invest NI on, and administering compliance with, this Policy and the GDPR. That post is held by Danny Smyth, Information Governance & Data Protection Manager, telephone: 028 9069 8655, email: privacy.officer@investni.com / dop@investni.com

2.5 Please contact the DPO with any questions about how you should handle Personal Data, the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed.

3. PERSONAL DATA PROTECTION PRINCIPLES

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

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

3.1.2 Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

3.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

3.1.4 Accurate and where necessary kept up to date (Accuracy).

3.1.5 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).

3.1.6 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).

3.1.7 Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

3.1.8 Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

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

4. LAWFULNESS, FAIRNESS, TRANSPARENCY

4.1 LAWFULNESS AND FAIRNESS

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

4.3 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The 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.

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

4.4.1 in the exercise of official authority or to perform a specific task in the public interest that is set out in law. As a public sector body, the vast majority of personal data processed by Invest NI is done so in the exercise of the 'official authority' vested in Invest NI by virtue of the Industrial Development Act (Northern Ireland) 2002 and the Industrial Development (Northern Ireland) Order 1982. Broadly these allow Invest NI to process data for economic development purposes.

4.4.2 the Data Subject has given his or her Consent;

4.4.3 the Processing is necessary for the performance of a contract with the

Data Subject;

4.4.4 to meet our legal compliance obligations (e.g. health and safety or tax laws);

4.4.5 to protect the vital interests of Data Subjects;

4.4.6 to pursue our legitimate interests (or those of a third party) provided the fundamental rights of Data Subjects do not override our interests. We can only rely on legitimate interests if we are Processing for a legitimate reason other than performing our tasks as a public authority.

4.5 The legal ground being relied on for each Processing activity should be identified and documented. Within Invest NI this is done within the Personal Data Inventory (PDI) for each programme / function that the processing relates to. Each Division is responsible for maintenance of its own PDIs and ensuring these are kept up to date.

4.6 CONSENT

4.7 Where consent is relied upon, it must be free given, specific, informed and unambiguous and Invest NI must effectively demonstrate that consent has been given.

4.8 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.

4.9 You will need to evidence Consent captured and keep records of all Consents so that the Organisation can demonstrate compliance with Consent requirements.

4.10 TRANSPARENCY (NOTIFYING DATA SUBJECTS)

4.11 The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such 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.

4.12 The Invest NI organisational Privacy Notice can be found at investni.com/privacy. This will provide the Data Subject with all the information required by the GDPR including the identity of the Controller and DPO, how and why we will Process (use, disclose, protect, retain and destroy) their Personal Data.

4.13 Whenever we collect Personal Data directly from Data Subjects, they must be directed to the Privacy Notice at the time of collection.

4.14 When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR within at least one month of collecting/receiving the data. You must also check that the Personal Data was collected by the third

party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

5. PURPOSE LIMITATION

5.1 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.

5.2 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 provided Consent where necessary.

6. DATA MINIMISATION

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

6.2 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.

6.3 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.

7. ACCURACY

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

7.2 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 amend inaccurate Personal Data.

8. STORAGE LIMITATION

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

8.2 Invest NI maintains a records retention and disposal schedule to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

8.3 You will take all reasonable steps to destroy or erase all Personal Data that we no longer require in accordance with the Invest NI records retention and disposal schedule and Records Management Policy. This includes requiring third parties to delete such data where applicable.

8.4 Data Subjects must be informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

9. SECURITY INTEGRITY AND CONFIDENTIALITY

9.1 PROTECTING PERSONAL DATA

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

9.3 We regard the lawful and correct handling of personal data as essential to our successful operation. To this end Invest NI maintains an Information Security Management System certified to the international security standard ISO 27001 to protect the confidentiality, integrity and availability of corporate information, including personal data entrusted to us by our customers, employees and stakeholders.

9.4 The Invest NI Information Security Management System maintains data security by protecting the confidentiality, integrity and availability of tPersonal Data, defined as follows:

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

9.4.2 Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

9.4.3 Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes (including Data Subjects when exercising their Rights under GDPR).

9.5 You are responsible for protecting the Personal Data we hold. You must comply with and not attempt to circumvent the administrative procedures, physical and technical safeguards we implement and maintain in accordance with the GDPR and the ISO27001 standard to protect Personal Data. These are set out within the Invest NI Information Security Handbook.

9.6 REPORTING A PERSONAL DATA BREACH

9.7 The GDPR requires Controllers to notify certain Personal Data Breaches to the Information Commissioner's Office and, in certain instances, the Data Subject.

9.8 The Data Breach Management Policy sets out the procedures in place to deal with any suspected Personal Data Breach.

9.9 If you know or suspect that a Personal Data Breach has occurred, follow the Data Breach Management Policy. Immediately advise your line manager and contact the DPO. You should preserve all evidence relating to the potential Personal Data Breach.

10. TRANSFER LIMITATION

10.1 The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the 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.

10.2 You may only transfer Personal Data outside the EEA if one of the following conditions applies:

10.2.1 the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

10.2.2 appropriate safeguards are in place such as standard contractual clauses approved by the European Commission; or

10.2.3 the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of substantial 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.

11. DATA SUBJECT'S RIGHTS AND REQUESTS

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

11.1.1 receive certain information about the Data Controller's Processing activities (the Privacy Notice);

11.1.2 request access to their Personal Data that we hold (commonly known as a. subject access request);

11.1.3 ask us to rectify inaccurate data or to complete incomplete data;

11.1.4 ask us to erase Personal Data if we have no lawful basis to process it;

11.1.5 restrict Processing in specific circumstances;

11.1.6 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

11.1.7 challenge Processing which has been justified on the basis of our legitimate interests or in the exercise of our official authority; and

11.1.8 object to direct marketing and decisions based solely on Automated Processing, including profiling (ADM);

11.2 Where applicable 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).

11.3 You must immediately forward any Data Subject rights request you receive to the Information Governance team via dpo@investni.com and comply with the Organisation's Data Subject Rights process.

12. ACCOUNTABILITY, TRAINING AND AUDIT

12.1 The GDPR requires the Organisation to implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. Invest NI is responsible for, and must be able to demonstrate, compliance with the data protection principles.

12.2 The Organisation must have adequate resources and controls in place to ensure and to document GDPR compliance including:

12.2.1 The appointment of a suitably qualified DPO [Danny Smyth, the Information Governance & Data Protection Manager];

12.2.2 implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a risk to rights and freedoms of Data Subjects;

12.2.3 integrating data protection into internal policies and processes where relevant;

12.2.4 regularly training Invest NI Personnel on the GDPR. The Organisation must maintain a record of training attendance by Invest NI Personnel; and

12.2.5 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.

12.3 RECORD OF PROCESSING ACTIVITIES

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

12.5 You must keep and maintain accurate corporate records reflecting our Processing by ensuring that any processing you undertake is captured within a Personal Data Inventory (PDI). Each division within Invest NI will maintain a PDI for each programme of support for which they are responsible and / or each function they perform which processes personal data.

12.6 The PDI will include, 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 integrity measures in place.

12.7 Each Division should appoint a PDI Coordinator to liaise with the DPO to ensure that each of their PDIs are regularly reviewed and updated to reflect any changes in the processing of personal data.

12.8 Where applicable records of Data Subjects' Consents must be maintained.

12.9 PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

12.10 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.

12.11 You must complete a DPIA screening questionnaire to establish whether one will needed to be completed for any Processing you plan to undertake as part of a new project or procurement.

12.12 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:

12.12.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

12.12.2 Automated Processing including profiling and ADM;

12.12.3 large scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and

12.12.4 large scale, systematic monitoring of a publicly accessible area.

12.13 A DPIA must include:

12.13.1 a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

12.13.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

12.13.3 an assessment of the risk to individuals; and

12.13.4 the risk mitigation measures in place and demonstration of compliance.

12.14 SHARING PERSONAL DATA

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

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

12.16.1 they have a need to know the information for the purposes of providing the contracted services;

12.16.2 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;

12.16.3 the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

12.16.4 the transfer complies with any applicable cross border transfer restrictions; and

12.16.5 a fully executed written contract that contains GDPR approved third party clauses has been obtained.

ANNEX: GLOSSARY

DEFINITIONS:

"Automated Decision-Making (ADM)"	means when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.
"Automated Processing"	means 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.
"Invest NI"	means Invest Northern Ireland, a public body registered at Bedford Square, Bedford Street, Belfast, BT2 7ES.
"Invest NI Personnel"	means all employees, workers, contractors, agency workers, consultants, directors, interns, volunteers, members and others.
"Consent"	means 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, signifies agreement to the Processing of Personal Data relating to them.
"Controller"	means 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 GDPR. We are the Controller of all Personal Data relating to our Invest NI Personnel and Personal Data used in our business for our own commercial purposes.

"Criminal Convictions Data"	means personal data relating to criminal convictions and offences.
"Data Subject"	means 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.
"Data Privacy Impact Assessment (DPIA)"	means 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 programs involving the Processing of Personal Data.
"Data Protection Officer (DPO)"	means the person required to be appointed in specific circumstances under the GDPR.
"EEA"	means the 28 countries in the EU, and Iceland, Liechtenstein and Norway.
"Explicit Consent"	means consent which requires a very clear and specific statement (that is, not just action).
"General Data Protection Regulation (GDPR)"	means the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.
"Personal Data"	means 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.
"Personal Data Breach"	means 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.
"Privacy by Design"	means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

"Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies"	means separate notices setting out information that may be provided to Data Subjects when the Organisation 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) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.
"Processing or Process"	means 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.
"Pseudonymisation or Pseudonymised"	means 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.
"Related Policies"	means Invest NI policies, operating procedures or processes related to this Policy and designed to protect Personal Data available the intranet. These include the Information Security Handbook, the Data Breach Management Policy and the Data Subject Rights Policy.
"Special Categories of Personal Data"	means information revealing racial or ethnic origin, religious beliefs and political opinions, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, health and sickness records and information about criminal convictions and offences.

Version Control

Version	Reviewed by	Approved by	Review Date	Reason for change
6.0	Danny Smyth	Steve Chambers	25 May 2018	Revised to reflect GDPR