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.

1.2 We recognise that the correct and lawful processing of personal data will maintain confidence in the organisation, build trust with our customers and will provide for successful business operations.

1.3 Invest NI is committed to ensuring its personnel follow the requirements of Data Protection law as set out within the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

1.4 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. SCOPE

2.1 All Invest NI personnel are subject to this policy. It is the personal responsibility of each individual to comply with Data Protection law and this policy.

2.2 It is essential that all staff maintain awareness of the risks and responsibilities when handling personal data and to facilitate this, Invest NI has committed to annual Data Protection awareness training. All staff must complete this mandatory training within designated timescales each year.

2.3 Any breach of this policy may result in disciplinary action for employees or termination of contract for others.

3. PERSONAL DATA PROTECTION PRINCIPLES

3.1 Invest NI adheres 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 individuals 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 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 Personal data must be processed lawfully, fairly and in a transparent manner.

4.2 The GDPR sets out six lawful bases for processing, which are described below:

4.2.1 the processing is necessary 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.

4.2.2 the individual has given **Consent**;

4.2.3 the processing is necessary for the **performance of a contract with the individual**;

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

4.2.5 to protect the **vital interests** of (an) individuals;

4.2.6 to pursue our **legitimate interests** (or those of a third party) provided the fundamental rights of individuals 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.

4.3 None of the lawful bases are 'better' or more important than others. The lawful basis being relied on for each processing activity should be identified and documented within the relevant Personal Data Inventory (see 12.3 below).

4.4 CONSENT

4.5 Where consent is relied upon as a lawful basis for processing personal data, it must be freely given, specific, informed and unambiguous and Invest NI must effectively demonstrate that consent has been given.

4.6 Individuals must be able to easily 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 to that which was included in the Privacy Notice when the individual first consented.

4.7 You will need to keep records of all Consents so that the organisation can demonstrate evidence of compliance with Consent requirements.

4.8 TRANSPARENCY (Provision of a Privacy Notice)

4.9 The GDPR requires us to provide detailed, specific information to individuals about how their data is used. 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 an individual can easily understand.

4.10 The Invest NI organisational Privacy Notice can be found at investni.com/privacy. This provides all the information required by the GDPR including the identity of Invest NI as the Data Controller, how and why we will process (use, disclose, protect, retain and destroy) their personal data and the Data Protection Officer contact details.

4.11 Teams should review the Privacy Notice to ensure that all processing of personal data for their programmes / functions are captured within the Privacy Notice. Any required updates should be directed to privacy.officer@investni.com. For one-off specific projects it may be more appropriate to create a separate Privacy Notice.

4.12 Whenever we collect personal data directly from individuals, they must be directed to the Privacy Notice at the time of collection.

4.13 When personal data is collected indirectly (for example, from a third party or a publicly available source), you must provide the individual with a Privacy Notice within 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 is compatible with 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 those within the Privacy Notice when it was first obtained unless you have informed the individual of the new purposes and they have provided Consent where necessary.

6. DATA MINIMISATION

6.1 You may only process personal data when required for the delivery of Invest NI business functions. You cannot process personal data for any reason unrelated to identified organisational purposes.

6.2 You may only collect personal data that you require for specific business purposes: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

7. ACCURACY

7.1 You must ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to 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 when it is no longer needed 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 must take all reasonable steps to destroy or erase personal data that we no longer require in accordance with the Invest NI Records Management Policy and Records Retention and Disposal Schedule. This includes requiring third parties to delete such data where applicable.

9. SECURITY INTEGRITY AND CONFIDENTIALITY

9.1 Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

9.2 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 corporate information, including personal data.

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

9.3.1 Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

9.3.2 Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

9.3.3 Availability means that authorised users are able to access the personal data when they need it for authorised purposes (including Individuals when exercising their Rights under GDPR).

9.4 You are responsible for protecting the personal data we hold. You must comply with - and not attempt to circumvent - the policies, administrative procedures and physical and technical safeguards we implement to protect personal data. These are set out within the Invest NI **Information Security Handbook**.

9.5 REPORTING A PERSONAL DATA BREACH

9.6 The GDPR requires us to notify certain Personal Data Breaches to the Information Commissioner's Office and, in certain instances, to individuals impacted by a breach.

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

9.8 If you know or suspect that a Data Breach has occurred, follow the **Data Breach Management Policy**. Immediately advise your line manager and the privacy.officer@investni.com mailbox. You should preserve all evidence relating to the potential Data Breach.

10. ACCOUNTABILITY

10.1 The GDPR requires us to have appropriate measures and records in place to be able to demonstrate compliance with the data protection principles.

10.2 Invest NI must have adequate resources and controls in place to ensure and to document GDPR compliance including:

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

10.2.2 implementing Data Protection by Design and by Default when processing personal data including completing Data Protection Impact Assessments where required;

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

10.2.4 regularly training Invest NI personnel on Data Protection. All staff must complete the mandatory awareness training within the designated timescale each year. The organisation must maintain a record of this training; and

10.2.5 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.

10.3 RECORD OF PROCESSING ACTIVITIES

10.4 The GDPR requires us to keep full and accurate records of all our data processing activities. You must ensure that any processing you undertake is captured within a Personal Data Inventory (PDI).

10.5 Each division within Invest NI must maintain a PDI for each programme of support for which they are responsible and / or each function they perform which processes personal data.

10.6 Each Division must appoint a PDI Coordinator to liaise with the Information Governance Team to ensure that each of their PDIs are regularly reviewed and updated to reflect any changes in the processing of personal data.

10.7 DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

10.8 We are required to implement Data Protection 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 protection principles.

10.9 You must complete a DPIA screening questionnaire to establish whether a full DPIA will need to be completed for any processing you plan to undertake as part of an activity, project or procurement involving the processing of personal data.

10.10 A DPIA is a process to help you identify and minimise data protection risks. To meet its aims, it is essential that the DPIA is part of the decision making process and is started at the development stage of any new activity or project.

10.11 Further information on the DPIA process is provided in the **Invest NI DPIA Guidance and Procedure Manual**.

11. INTERNATIONAL TRANSFERS

11.1 The GDPR restricts data transfers to countries outside the European Economic Area (EEA) in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

11.2 An international transfer takes place when data is transmitted, sent, viewed or made accessible in a country outside the EEA and in such instances additional compliance requirements are needed.

11.3 The **Invest NI Procedure for International Transfers** sets out the procedures to be followed when transferring personal data internationally.

11.4 Under certain criteria the restrictions do not apply (unrestricted transfers). An Invest NI employee based within the EU can send personal data (necessary for the delivery of a service) to another Invest NI employee located in a satellite office that is located in a country outside the EEA without any considerations of additional compliance requirements. This will also apply to sending personal data to FCO seconded staff working at Invest NI international offices.

12. SHARING PERSONAL DATA

12.1 Generally we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

12.2 You may only share the personal data we hold with third parties, such as our service providers if:

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

12.2.2 sharing the personal data complies with the Privacy Notice provided to the Individual or, if required, the Individual's Consent has been obtained;

12.2.3 the third party has agreed to comply with the required data security standards and put adequate security measures in place;

12.2.4 a fully executed written contract that contains GDPR approved third party clauses has been obtained; and/or

12.2.5 a Data Sharing Agreement has been put in place.

13. INDIVIDUAL'S RIGHTS AND REQUESTS

13.1 Individuals have rights in relation to the personal data we hold on them. These include rights to:

13.1.1 receive certain information about the our processing activities (the Privacy Notice);

13.1.2 request access to their personal data that we hold (commonly known as a subject access request);

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

13.1.4 ask us to erase personal data if we have no lawful basis to process it;

13.1.5 restrict processing in specific circumstances;

13.1.6 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;

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

13.1.8 object to direct marketing and decisions based solely on Automated processing, including profiling.

13.2 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).

13.3 You must forward any request you receive from an individual exercising one of these Rights to the Information Governance team via dpo@investni.com and comply with the organisation's **Data Subject Rights process**.

14. CRIMINAL OFFENCES

14.1 The DPA creates a number of criminal offences, these are knowingly or recklessly:

14.1.1 Obtaining, retaining, disclosing or procuring the disclosure of personal data without the consent of the data controller.

14.1.2 Unlawful selling of, or offering for sale, personal data that was previously unlawfully obtained.

14.1.3 Altering, defacing, blocking or destroying records containing personal data, where the intention is to prevent the disclosure of that information in response to a request.

14.1.4 Re-identification of personal data that has been 'de-identified' (de-identification being a process - such as redactions or pseudonymisation - to remove/conceal personal data).

14.1.5 Processing of personal data that has been 'de-identified'.

14.1.6 Failure to comply with a warrant served by the Information Commissioner.

14.1.7 Knowingly or recklessly making a false statement in response to an Information Notice from the Information Commissioner.

14.1.8 Forcing another individual to provide relevant records regarding employment or contractual services (except as required by law).

14.2 Anyone found guilty of a criminal offence under the DPA, including individual members of staff, could face an unlimited fine and a criminal record.

14.3 The DPA imposes personal liability on Directors and Managers if an individual commits an offence attributable to their consent or neglect which may result in their prosecution.

15. FURTHER INFORMATION

15.1.1 Further detailed guidance on complying with Data Protection within Invest NI can be found on the Invest NI Data Protection intranet pages available via 'My Invest NI – Services' dropdown menu.

15.1.2 Specific queries regarding data protection matters should be referred to the Information Governance Team who can be contacted via privacy.officer@investni.com

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
7.0	Mark Hutchinson	Danny Smyth	01 July 2020	Scheduled review Added criminal offences section & general updates