**DATA PROTECTION**

**APPROPRIATE POLICY DOCUMENT**

**CONTENTS**

Introduction

Scope

Details of special categories of personal data and criminal offence data we process

Purposes for processing special categories of personal data and criminal offence data

Compliance with data protection principles

Retention and erasure of personal data

Related legislation

Review

1. INTRODUCTION

In order to meet Scottish Enterprise's statutory functions and, as part of our corporate functions, we process (meaning any activity that involves the use of personal data, including collecting, using and storing) special categories of personal data and criminal offence data in accordance with the requirements of Articles 9 and 10 to **UK GDPR** (the retained-EU version of the General Data Protection Regulation ((EU) 2016/679)) and Schedule 1 to the Data Protection Act 2018 (**DPA 2018**).

Some of the Schedule 1 conditions for processing special categories of personal data and criminal offence data require us to have an appropriate policy document in place, setting out fair procedures for ensuring we meet our obligations under the UK GDPR and DPA 2018 to protect such data.

1. SCOPE

This document explains our processing, and meets the requirement of the DPA 2018 that an appropriate policy document be in place where processing special categories of personal data and criminal offence data in certain circumstances. It applies to all **data subjects** (a living, identified or identifiable individual about whom we hold personal data) about whom such categories of personal data are processed by Scottish Enterprise. The information contained in this appropriate policy supplements our privacy notices.

1. DETAILS OF SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL OFFENCE DATA WE PROCESS
* We process information revealing the following special categories of personal data:-
* racial or ethnic origin,
* political opinions,
* religious or similar beliefs,
* trade union membership,
* physical or mental health conditions,
* sexual life,
* sexual orientation,
* biometric or genetic data

We also process criminal offence data, which is personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

1. PURPOSES FOR PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL OFFENCE DATA

We process special categories of personal data and criminal offence data for the purposes below, under the following UK GDPR articles and schedule 1 to the DPA 2018.

* 1. To fulfil our obligations as an employer

This includes information about our employees’ health and well-being, ethnicity, sexual orientation and trade union membership, and where applicable, about criminal offences for the purposes of:-

* assessing an employee’s fitness to work
* complying with health and safety obligations
* complying with the Equality Act 2010, including the requirements to make reasonable adjustments
* Checking applicants’ and employees’ right to work in the UK
* Undertaking pre-employment checks to verify candidates are suitable for employment or continued employment
* responding to medical emergency involving a member of staff
* relating to an employment tribunal or legal claim
	+ 1. Special categories of personal data for these purposes are processed under:-
* UK GDPR
* Article 9(2)(a) - where we have obtained the explicit consent of the employee.
* Article 9(2)(b) -processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or confirmed by law on Scottish Enterprise or the data subject in connection with employment, Social Security or social protection.
* Article 9(2)(c) - Where processing is necessary to take the vital interests of the data subject or of another natural person.
* Article 9(2)(f) - for the establishment, exercise or defence of legal claims
* Schedule 1 to the DPA 2018

Part 1 - Paragraph 1(1) employment, Social Security and social protection

* Part 2 - Paragraph 8(1) equality of opportunity or treatment
* Part 2 - Paragraph 10(1) preventing or detecting unlawful acts
* Part 2- Paragraph 11(1) and (2) - protecting the public against dishonesty
* Part 2- Paragraph 12(1) and (2) - regulatory requirements relating to unlawful acts and dishonesty
	+ 1. Criminal offence data is processed under:-
* UK GDPR –
* Article 6(1)(f) - where processing is necessary for our legitimate interests; and
* Article 10
* Schedule 1 to the DPA 2018
* Part 1 - Paragraph 1(1) employment, Social Security and social protection
* Part 2 - Paragraph 10 necessary for the prevention or detection of an unlawful act
	1. To fill our statutory obligations, particularly for investment activities.

This includes information about health and well-being, sexual orientation, ethnicity and criminal offences, for the purposes of:-

* undertaking pre-investment due diligence;
* undertaking human rights due diligence prior to investment or award of grant;
* appointing or considering for appointment of non-executive directors to boards of companies in which we invest; and
* Equality monitoring under the equality Act 2010
	+ 1. Special categories of personal data for these purposes are processed under:-
* UK GDPR
* Article 9(2)(a) - where we have obtained the explicit consent of the employee.
* Article 9(2)(g) - reasons of substantial public interest.
	+ 1. Criminal offence data is processed under:-
* UK GDPR -
* Article 6(1)(a) consent has been given by the data subject;
* Article 6(1)(e) performance of a task in the public interest; and
* Article 10
* Schedule 1 to the DPA 2018
* Part 2 - Paragraph 6(1) statutory etc purposes; and
* Part 2 - Paragraph 12(1) regulatory requirements relating to unlawful acts and dishonesty etc; and
* Part 3 – Paragraph 29 consent

Scottish Enterprise is the national economic development agency for Scotland, formed under the Enterprise and New Towns (Scotland) Act 1990 (**the 1990 Act**). Special categories of personal data and, in certain circumstances, criminal offence data are processed for the purposes of fulfilling our statutory functions under Sections 1 and 4 of the 1990 Act, which require Scottish Enterprise to develop Scotland’s economy by providing funding, support and investment. There is substantial public interest in SE being able to make investments which are commercially sound and viable, and which do not expose us to unlawful activity, particularly given our use of public funds.

1. COMPLIANCE WITH DATA PROTECTION PRINCIPLES
	1. Accountability principle

Scottish Enterprise has put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:-

* providing a privacy notice to data subjects setting out how their personal data will be handled, when we first obtain their personal data. This includes the period for which the personal data will be stored.
* Maintaining a record of all our processing activities;
* appointment of a data protection and information governance officer who reports directly to our highest management level;
* carrying out data protection impact assessments for high risk processing to understand how processing may affect data subjects and consult with the Information Commissioner if appropriate;
* adopting and implementing a data protection policy and related information handling and security policies;
* ensuring we have written in contract written contracts in place with our data processors and come away to applicable, data sharing arrangements in place with third parties with whom we share data centre:
* implementing appropriate technical and organisational security measures in relation to the personal data we process
	1. Lawfulness, fairness and transparency

Processing is only lawful where the explicit consent of the data subject is given or we rely on at least one of the conditions set out in Schedule 1 to the DPA 2018. These are as outlined above.

Scottish Enterprise provides clear and transparent information on the lawful basis relied upon when processing personal data in our privacy notices and this policy document. Our processing for the purpose of substantial public interest is necessary to:-

* execute our functions under the 1990 Act;
* for the purposes of complying with the requirement forming principles of good practise for a body investing public funds; and
* for taking steps to establish whether another person has committed an unlawful act, or being involved in dishonesty, malpractice or other serious improper conduct.
	1. Purpose limitation

Personal data collected by us is for specified purposes. We inform data subjects what those purposes are in our published privacy notices. Personal data is not used by us for new, different or incompatible purposes from those disclosed when it was first obtained, unless we have informed the data subject of the new purposes and, where necessary, they have consented.

* 1. Data minimisation

Only the minimum personal data necessary is collected and/or disclosed for the relevant purpose and we ensure that this is not excessive. We ensure that the personal data collected is adequate and relevant for the intended purposes. Where data provided to or obtained by us is irrelevant or exceeds the purpose, it is deleted.

* 1. Accuracy

The personal data we hold and use is accurate, complete, kept up to date and relevant to the purpose for which it is collected by us. We take steps to ensure the accuracy of data at the point of collection. Our employees can check the accuracy of their own data through a self-service portal. All reasonable steps are taken by us to destroy or amend inaccurate or out-of-date Personal Data.

* 1. Storage limitation

We maintain a Retention Policy and related procedures to ensure personal data is deleted or anonymised after a reasonable time has elapsed after it has fulfilled the purposes for which it was being held. This is unless we are legally required to retain that data for longer.

We ensure Data Subjects are informed of the period for which data is stored and how that period is determined in our Privacy Notices.

* 1. Security, integrity, confidentiality

Reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of or damage to personal data have been implemented and are maintained by us. We also ensure that all staff are appropriately trained on data protection and information security.

1. RETENTION AND ERASURE OF PERSONAL DATA

We take the security of special categories of personal data and criminal offence data very seriously. We have administrative, physical and technical safeguards in place to protect personal data against unlawful or unauthorised processing, or accidental loss or damage. We will ensure, where special categories of personal data or criminal offence data are processed that:

* the processing is recorded, and the record sets out, where possible, a suitable time period for the safe and permanent erasure of the different categories of data in accordance with our Retention Policy;
* where we no longer require special categories of personal data or criminal offence data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible; and
* where records are destroyed, we will ensure that they are safely and permanently disposed of.
1. RELATED LEGISLATION
* Data Protection Act 2018
* UK GDPR
1. REVIEW

This policy on processing special categories of personal data and criminal offence data:-

* + - is reviewed annually,
		- will be retained where we process special categories of personal data and criminal offence data and for a period of at least six months after we stop carrying out such processing; and.
		- will be provided to the Information Commissioner's Office on request and free of charge.

For further information about our compliance with data protection law, please contact our Data Protection and Information Governance Officer.