The Single Source Regulations Office: Our personal information charter for staff and contractor data

This charter sets out what our staff and contractors working for the Single Source Regulations Office (the **SSRO**) can expect when we request or hold your personal data.

The SSRO is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this charter.

This charter applies to all employees, workers and contractors and covers the following categories of personal data:

- the SSRO’s employment records;
- the SSRO’s recruitment records;
- data collected by the SSRO in relation to providers of goods, works or services to the SSRO; and
- security footage of persons captured on CCTV within the SSRO’s premises.

This charter applies to current and former employees, workers and contractors and to the personal data we hold about you during and after your working relationship with us. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

What you can expect from us, and what we ask from you

We handle personal data about you so we can carry out our responsibilities as an employer or in respect of contracts for interim or other temporary assignments.

The SSRO’s high standards in handling personal data help us to maintain the confidence of everyone who deals with us. So, when we ask you for your personal data, we promise:

- to make sure you know why we need it;
- to ask only for what we need, and not to collect too much or irrelevant information;
- to protect it and make sure nobody has access to it who shouldn’t;
- to let you know if we share it with other organisations to give you better public services – and if you can say no;

- to make sure we don’t keep it longer than necessary; and
- to not make your personal data available for commercial use without your consent.

In dealing with your personal data, we will also:

- value the personal data entrusted to us and make sure we respect that trust;
- abide by the law when it comes to handling personal data;
- consider the privacy risks when we are planning to use or hold personal data in new ways, such as when introducing new systems; and
- provide training to staff who handle personal data and respond appropriately if personal data is not used or protected properly.

In return, we ask you to help us by:

- giving us accurate information;
- if we have asked for your consent, letting us know whether you consent to holding your information;
- telling us as soon as possible if there are any changes to your personal data, such as a new address;
- letting us know if your information is correct and up-to-date and that any consent you have given remains valid.

Our data protection policy

When we ask you for information we will keep to the law, including the General Data Protection Regulation (the **GDPR**) and the Data Protection Bill 2017-2019. Through appropriate management and strict controls, the SSRO will comply fully with the principles set out in Article 5 of the GDPR, which are that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- 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.

We will also ensure that:

- we have appointed a Data Protection Officer who has specific responsibility for data protection in the SSRO;
- the SSRO employees who manage and handle personal data understand that they are contractually responsible for following good data protection practice, and are appropriately trained and supervised;
- we deal with enquiries about how we handle personal data promptly and courteously;
- we will not generally rely on consent except where we need to, in which case we will seek informed consent; and
- we will explain how we handle personal data clearly, regularly review and audit how we manage personal data, and regularly assess and evaluate methods of handling personal data.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). In addition, there are “special categories” of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

(a) Your personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.

(b) Your date of birth.

(c) Your gender.

(d) Your marital status and dependants.

(e) Your next of kin and emergency contact information.

(f) Your National Insurance Number.

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

(h) Your salary, annual leave, pension and benefits.

(i) Your start date and date you stop working for us.

(j) Your location of employment or workplace.

(k) Your recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).

(l) Employment records (including your job titles, work history, working hours, training records and professional memberships).

(m) Your compensation history (including pay and expenses).

(n) Your performance information.

(o) Where relevant, your disciplinary and grievance information.

(p) CCTV footage and other information obtained through electronic means such as swipecard records.

(q) Information about your use of our information and communications systems.

(r) Photographs that may have been taken for official purposes with your consent.

Relevant information from the list above will be collected and held for agency workers and contractors on interim or temporary assignments to the SSRO. This will usually be limited to the personal information about you contained within your, or your agency's contract with us; information related to security and access to our premises; and information access to, and use of, our information and communications systems.

We may also collect, store and use the following "special categories" of more sensitive personal information about our direct employees:

(a) Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.

(b) Information about your health, including any medical condition, health and sickness records.

(c) Information about criminal convictions and offences (in highly limited circumstances as described below).

How is your personal information collected?

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers and credit reference agencies.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We need the personal information described above to allow us to carry out the following tasks to perform our contract with you:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.*
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.*
- Liaising with your pension provider.*
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.*
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.*
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.*
- Making decisions about your continued employment or engagement.*
- Making arrangements for the termination of our working relationship.*
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.*
- Ascertaining your fitness to work.*
- Managing sickness absence.*
- Complying with health and safety obligations.*
- Preventing fraud.*
- Monitoring your use of our information and communication systems to ensure compliance with our IT policies.
- Ensuring network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- Conducting data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.*

*These tasks will also need to be processed to enable us to comply with our legal obligations.

Please note that we may process your personal information without your knowledge or consent where required by law.

We may also use your personal information in the following situations, which are likely to be rare:

(a) Where we need to protect your life (or someone else's life).

(b) Where it is needed in the public interest or for the SSRO's official purposes.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you. For example, we may not be able to pay you or provide you with certain benefits. We may also be prevented from complying with our legal obligations, such as our obligation to ensure the health and safety of our workers.

Change of purpose

We will only use your personal information for the purposes for which we collect it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

(a) In limited circumstances, with your explicit written consent.

(b) Where we need to carry out our legal obligations, including in respect of your contract of employment (see below) or other contract covering working with us, and in line with our data protection policy.

(c) Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to pension schemes, and in line with our data protection policy.

(d) Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Our obligations as an employer

We will use your particularly sensitive ('special category') personal information in the following ways:

(a) We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.

(b) We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.

(c) We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting. At present, we limit such monitoring to executive roles.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law as set out above.

From time to time and in limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions only where we may be notified of such information directly by you in the course of you working for us. We do not receive or hold copies of any personal information relating to criminal

convictions or offences as part of the security clearance process. Such personal data will be provided by you directly to the relevant security clearance body. We will use information about criminal convictions and offences only to ascertain whether a criminal conviction or offence committed whilst working for us is of a nature that requires us to make a decision about your continued employment or engagement.

We are allowed to use your personal information in this way to carry out our obligations as an employer or as a party to a contract for labour services.

Please see our policy on handling special category data for more information.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We do not envisage that the SSRO will make any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

We would be allowed to use automated decision-making only in the following circumstances:

(a) Where we have notified you of the decision and given you 21 days to request a reconsideration.

(b) Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.

(c) In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we will put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Data sharing

We may have to share your data with third parties, including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law.

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

“Third parties” includes: tax authorities, those charged with Health & Safety legislation; and third-party service providers. The following third-party service providers process personal information about you for the following purposes:

- Ofgem: Payroll and payroll administration; Expenses payment and administration; HR services via iTrent;
- Scottish Widows: pension administration, benefits provision and administration
- MyCSP: pension administration, benefits provision and administration
- Littlefish: IT services
- E2E Assure: IT Services
- Government Actuaries Department: Building access security

All our third-party service providers are required through relevant, GDPR-compliant contract terms to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request from the SSRO Data Protection Manager (details below).

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the SSRO Data Protection Manager (details below).

We have put in place procedures to deal with any suspected data security breach and will notify you and the Information Commissioner of a suspected breach where we are legally required to do so.

Data retention

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention and disposal policy.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy.

Rights of access, correction, erasure, and restriction

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances, by law you have the right to:

(a) Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

(b) Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

(c) Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

(d) Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.

(e) Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

(f) Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact SSRO Data Protection Manager (details below) in writing.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the SSRO Data Protection Manager (details below). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data Protection Officer & Data Protection Manager

We have appointed a Data Protection Officer (DPO), Graham Payne, who is also Interim Director of Corporate Resources, and a Data Protection Manager, Ruaidhri Magee to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Data Protection Manager in the first instance (contact details below). You have the right to make a complaint at any time to the Information Commissioner’s Office, the UK supervisory authority for data protection issues.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact Ruaidhri Magee, Data Protection Manager, on 020 3771 4762, ruaidhri.magee@ssro.gov.uk.