The Single Source Regulations Office: Our personal information charter

This charter sets out what you can expect from the Single Source Regulations Office (the **SSRO**) when we request or hold your personal information (**personal data**).

The SSRO was established by the Defence Reform Act 2014 (**the Act**) and plays a key role in the regulation of the Ministry of Defence (**MOD**) single source defence contracts, by issuing statutory guidance, assessing compliance and determining how the regime applies to individual contracts.

Our principal statutory aims are to ensure that good value for money is obtained for the UK taxpayer in expenditure on qualifying defence contracts, and that single source suppliers are paid a fair and reasonable price under those contracts.

This charter covers the following categories of personal data:

- data held in the SSRO's Defence Contracts Analysis and Reporting System (**DefCARS**);
- communications outside of DefCARS in connection with the discharge of the SSRO's functions;
- data held for the purposes of our stakeholder engagement and public consultation;
- our employment records;
- our recruitment records;
- our records of dealings such as enquiries and complaints and other dealings in the public interest;
- data in relation to the providers of goods, works or services to us; and
- security footage of persons captured on CCTV within our premises.

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

We handle personal data about you so we can carry out our statutory functions. When we ask you for information we will keep to the law, including the General Data Protection Regulation (the **GDPR**) and the Data Protection Act 2018.

Our 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; and
- 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

Through appropriate management and controls, we 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 our organisation;
- our 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.

Lawful basis for processing personal data

The GDPR and the Data Protection Act 2018 specify the lawful basis for the retaining and processing personal data. We collect and process personal data lawfully as follows:

For the purpose of undertaking the SSRO's statutory functions

DefCARS

Data which is provided in standard reports relating to qualifying contracts that is held in DefCARS is processed in accordance with our obligations under the Act and the Single Source Contract Regulations 2014 (**the Regulations**). This processing is necessary for the performance of our tasks carried out in the public interest or in the exercise of official authority vested in us (GDPR Article 6(1)(e)).

This type of data will be retained permanently to enable us to carry out our statutory functions.

Referrals

Data provided to the SSRO during a referral for an opinion or a determination is processed in accordance with our obligations under the Act and the Regulations. The processing is necessary for the performance of the SSRO's tasks carried out in the public interest or in the exercise of official authority vested in the SSRO (GDPR Article 6(1)(e)).

Data provided to the SSRO as evidence for and in communications relating to a referral will be kept for a period of one year and three months after receipt of the final referral decision by the parties, following which the information will be reviewed to determine whether the data is still required; if not, it will be deleted or destroyed.

Reports and consultations

Data which is connected with the discharge of the SSRO's function to receive and review reports (ie communications in connection with statutory reports), and data collected during public consultations, is processed in accordance with our obligations under the Act and the Regulations. This processing is necessary for the performance of the SSRO's tasks carried out in the public interest or in the exercise of official authority vested in the SSRO (GDPR Article 6(1)(e)).

This type of data will be retained for a period of ten years, following which time the data will be reviewed to determine whether the data is still required to enable us to carry out our statutory functions; if not, it will be deleted or destroyed.

For stakeholder engagement

The personal data of our stakeholders will be collected to create and maintain stakeholder contact lists for the purposes of our stakeholder engagement functions. Information in respect of those individuals with a direct interest in the operation of the single source regime (government, Ministry of Defence, industry etc) that is collected as part of the SSRO's operations determination is processed in accordance with our obligations under the Act and the Regulations. The processing is necessary for the performance of the SSRO's tasks carried out in the public interest or in the exercise of official authority vested in the SSRO (GDPR Article 6(1)(e)).

We will only process the personal data of other stakeholders if the data subject has given consent to the processing of his or her personal data (GDPR Article 6(1)(a)).

Each year, we will write to all individuals whose details are held on our stakeholder contact databases, and from whom consent is required, to confirm the personal data we hold about you and to confirm that you still give your consent to us retaining and using it. We will provide a copy of the contact information we hold and provide the opportunity for you to:

- ask us to update or correct the personal data we hold about you;
- withdraw your consent and ask us to delete the personal data we hold about you; or
- object to us using your personal data in a particular way.

If you do not respond to our request, we will delete your personal data within six months.

We will retain stakeholder data only for as long as you provide your consent to hold it. If you withdraw your consent, we will immediately delete your personal data.

You do not have to wait for this annual exercise and you can update your personal data or withdraw your consent at any time.

We may commission a third-party organisation to undertake a stakeholder engagement survey on our behalf. Any such third-party will be required, through contractual safeguards, to take appropriate security measures to protect your personal information in line with GDPR and our policies. We do not allow third-party organisations to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and strictly in accordance with our instructions.

Employee/contractor data

We will process the financial details (tax, bank, pension, payment history details) of our employees and contractors for the purposes of payroll. We will also process the personal data of our employees and contractors (employment history, disciplinary history, qualifications) for the purposes of its personnel records. The lawful basis for processing this data is that the processing is necessary for the performance of the employment contract to which the employees and contractors are party (GDPR Article 6(1)(b)).

We will also process special category data in relation to our employees, including gender, ethnicity, nationality, disability, sickness record and marital status. For senior staff, we will also process data in relation to gender identity, sexual orientation, faith or belief and political activity. This special category data is also processed as far as it is necessary for the purposes of carrying out our obligations and exercising the rights of the employee in the fields of employment, social security and social protection law in the UK (GDPR Article 9 2(b)).

Certain personal data held in our manual records systems relating to appointments, removals, pay, discipline, superannuation or other personnel matters are exempted by section 24(3)(b) of the Data Protection Act 2018.

We will delete or destroy the employee/contractor's sensitive personal data, next of kin and emergency contact data and bank details within six months of the employee/contractor's last day of employment.

Otherwise, the retention period for other employee/contractor personal data is a period of seven years from the last day of employment or the last date of payment, whichever is the later. For further information for employees and contractors who work for us, please refer to our employee data protection policy.

Recruitment data

We will process personal data provided by applicants for employment during the course of recruitment exercises. The lawful basis for processing this data is that the processing is necessary to take steps at the request of the individual prior to entering into a contract ((GDPR Article 6(1)(b))).

For candidates applying for senior roles, the special category data described above under ‘employee data’ (gender, ethnicity, nationality etc, with the exception of sickness records) will also be processed under this lawful basis.

The retention period for this type of personal data is a period of up to one year following the particular recruitment campaign in which the job candidate participated. After the expiry of this time period, we will destroy the personal data we hold in relation to the recruitment candidate.

Records of dealings such as enquiries, complaints and public interest

Data collected in working documents related to enquiries, complaints and the public interest is processed in accordance with our obligations under the Act and the Regulations. This processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us (GDPR Article 6(1)(e)).

This type of data will be retained for a period of seven years, following which the data will be reviewed and stored for archival purposes or deleted.

Data collected in relation to providers of goods, works or services

We will process personal data provided by certain providers of goods, works or services to us. The lawful basis for processing this data is that the processing is necessary for the performance of a contract to which we are a party ((GDPR Article 6(1)(b))).

This type of data will be retained for a period of seven years, following which time the information will be reviewed to determine whether the data is still required for legal reasons; otherwise, it will be deleted or destroyed.

CCTV data

For our employees and visitors to our premises, we will process data captured by CCTV cameras inside Finlaison House for the physical security of the SSRO. The lawful basis for processing this data is that the processing is necessary for the purposes of our legitimate interests (GDPR Article 6(1)(f)). This data may be shared with police, when appropriate.

CCTV images will be retained for a period of up to three months from the date of filming, following which the data will be deleted. The reason for this retention period is that it is anticipated that any security incidents may be identified within this timeframe and the police may require the CCTV footage for evidentiary purposes.

Our retention policy

For additional information about the period for which your personal data will be stored and how we have determined the retention period, please refer to our data retention policy.

Your rights as a data subject

Data subject access requests

Under the GDPR and the Data Protection Act 2018, an individual may make a data subject access request, which is a request for details of the personal data that an organisation holds about them. You can make this request electronically or physically. Our response will provide the following information:

- confirmation of whether, and where, we are processing your personal data;
- information about the purposes of the processing;
- information about the categories of data being processed;
- information about the types of people or organisations with whom we may share your data;
- information about the period for which the data will be stored (or how we will determine that period);
- where the data were not collected from you, the source of the data;

To make a subject access request, you can write to:

Data Protection Manager
The Single Source Regulations Office
G51/G52 100 Parliament Street
London
SW1A 2BQ

You can also write to us by email at: ruaidhri.magee@ssro.gov.uk

We will respond to your subject access request within one month. We will not charge a fee for responding to your request.

Your right to be forgotten

Under the GDPR, as a data subject, you have the right to be forgotten (also known as the right to erasure), if:

- your personal data is no longer needed for its original lawful basis (and we have no new purpose for holding it);
- the lawful basis for the processing is your consent, you withdraw that consent, and we have no other purpose for processing the information;
- you exercise your right to object, and we have no overriding grounds for continuing the processing; or
- the data has been processed unlawfully.

To exercise this right, please write to the Data Protection Manager at the address above (see data subject access requests).

Your right to object

Under the GDPR, you also have the right to object to the processing of personal data where it is being processed on the ground of public interest, and we will cease such processing unless we can demonstrate that we have compelling legitimate grounds for processing or that we require the data to establish, exercise or defend our legal rights.

To exercise this right, please write to the Data Protection Manager at the address above (see data subject access requests).

Your right to data portability

Under the GDPR, you also have the right to ‘data portability’, which allows you to obtain and reuse your personal data for your own purposes across different services.

It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

You have the right to data portability:

- in relation to personal data you have provided to the SSRO;
- where the processing is based on your consent or for the performance of a contract; and
- when processing is carried out by automated means (ie by computer).

Upon request, we will provide your personal data to you in a structured, commonly used and electronic form.

To exercise this right, please write to the Data Protection Manager at the address above (see data subject access requests).

Your right to rectification

Under the GDPR, you also have the right to rectification of inaccurate personal data. If we receive a request for rectification, we will take reasonable steps to satisfy ourselves that the data is accurate and to rectify the data if necessary.

To exercise this right, please write to the Data Protection Manager at the address above (see data subject access requests).

Making a complaint and further information

To make a complaint about our use of your personal data or to get independent advice about data protection, privacy and data-sharing issues, you can contact:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Telephone: 01625 545 745 or 0303 123 1113
Fax: 01625 524 510

Website: www.ico.gov.uk