Privacy Notice for Employees and Contractors[1]

Foreword

RUSI is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you before, during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR) and the EU's GDPR. It applies to all employees, workers, and contractors.

RUSI[2] is a "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 privacy notice. This notice applies to current and former employees, workers, contractors, interns, dependents, beneficiaries, trustees and associate fellows.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using that information and what your rights are under the data protection legislation.

Data protection principles

We will comply with data protection law, which says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

[1] This policy does not form part of any employee's contract of employment, and it may be amended at any time.

[2] Means the Royal United Services Institute for Defence and Security Studies (registered charity no.210639, 61 Whitehall, London SW1A 2ET), and its subsidiaries and affiliated companies or organisations controlled by the Royal United Services Institute for Defence and Security Studies (collectively, "RUSI")

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 person's identity has been removed (anonymous data). There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health, sexual orientation, or criminal convictions.

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

- Personal contact details such as name, title, addresses, telephone numbers and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension, and benefits information.
- Start date and, if different, the date of your continuous employment.
- Leaving date and your reason for leaving.
- Location of employment or workplace.
- 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).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Photographs.
- Results of HMRC employment status check, details of your interest in and connection with the intermediary through which your services are supplied.

We may also collect, store, and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions.
- Information about your health, including any medical condition and sickness records, including:
    - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave;

- where you leave employment and the reason for leaving is related to your health, information about that condition needed for pension and life insurance purposes.

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.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us, or contracting to provide services to us, or you being a trustee or associate fellow of RUSI.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests.

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

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you [*] and to enable us to comply with legal obligations [**]. In some cases, we may use your personal information to pursue legitimate interests [***], provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below. We have indicated by asterisks the purpose or purposes for which we are processing or will process your personal information.

- Making a decision about your recruitment or appointment using your CV, interview feedback, references, etc. [*], [***]
- Determining the terms on which you work for us. [*], [***]
- Determining whether your engagement is deemed employment for the purposes of Chapter 10 of Part 2 of the Income Tax (Earnings and Pensions) Act 2003 (ITEPA 2003)

and providing you with a status determination statement in accordance with the applicable provisions of ITEPA 2003. [**]
- Checking you are legally entitled to work in the country in which you are applying for a position. [*], [***]
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).[*], [***]
- Providing employment benefits. [*]
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties. [*]
- Liaising with the trustees or managers of your pension provider and any other provider of employee benefits. [*], [***]
- 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. [*], [***]
- To prevent fraud. [*],[***]
- To monitor your use of our information and communication systems to ensure compliance with our Cyber Security and Data Protection Policies. [*], [***]
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution. [*], [**]
- To conduct data analytics studies to review and better understand employee retention and attrition rates. [***]
- Equal opportunities monitoring. [**],[***]

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

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 (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as 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 collected 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.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

Special categories of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation, or trade union membership, require higher levels of protection. We need to have further justification for collecting, storing, and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.
4. Where it is necessary to protect you or another person from harm.

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.

Situations in which we will use your sensitive personal information

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so. The situations in which we will process your particularly sensitive personal information are listed below.

- We will use information about your physical or mental health, or disability status, to:
    - ensure your health and safety in the workplace;
    - assess your fitness to work;
    - provide appropriate workplace adjustments;
    - monitor and manage sickness absence; and

- administer benefits including statutory maternity pay, statutory sick pay and pensions.

We need to process this information to exercise rights and perform obligations in connection with your employment.

- If we reasonably believe that you or another person are at risk of harm and the processing is necessary to protect you or them from physical, mental, or emotional harm or to protect physical, mental or emotional well-being.
- 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.

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. 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.

We do not need your consent where the purpose of the processing is to protect you or another person from harm or to protect your well-being and if we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you one month to request a reconsideration.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. 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 must also 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.

We do not envisage that any decisions will be taken about you using automated means. However, we will notify you in writing if this position changes.

Data sharing

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

We may transfer your personal information outside the UK or the EEA. If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

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.

Which third-party service providers process my personal information?

Third parties include third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, some IT services and life insurance.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required 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.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law. For example, this may include making returns to HMRC, reporting relevant information to the Charity Commission, or the trustees of RUSI, etc.

Transferring information outside the UK or the EEA

We may transfer the personal information we collect about you countries outside of the UK in order to perform our contract with you: Kenya and Belgium where RUSI has other offices. There is an adequacy decision in relation to Belgium, meaning no further measurements are required for the transfer of data between the London and Brussels offices.

On the contrary, there are no adequacy regulations in respect of Kenya. This means that Kenya is not deemed to provide an adequate level of protection for your personal information.

To ensure that your personal information does receive an adequate level of protection, we have put in place the following appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects UK law on data protection: an international data transfer agreement. Further information about this protective measures is available upon request to the Risk and Compliance Manager.

Data security

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. Employee records are stored separately to limit access to those with adequate credentials. Any necessary transfers of employee personal data will be marked as confidential and shared only when necessary. Files including employee data, particularly sensitive data will be encrypted and/or password protected. Additionally, 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.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so. For further information on the different security measures implemented by RUSI to keep your information safe, please refer to our Cyber Security and Data Protection Policies.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes for which we collected it, 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 Data Retention Policy which is available here: [insert link later]

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.

- The applicable legal requirements.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use that information without further notice to you. Once you are no longer an employee, worker, or contractor of RUSI, we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Rights of access, correction, erasure and restriction

Your duty to inform us of changes

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.

Your rights in connection with personal information

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

- **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.
- **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.
- **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).
- **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. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **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.
- **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 the Risk and Compliance Manager in writing.

No fee usually required

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 these circumstances.

What we may need from you

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 Risk and Compliance Manager. 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.

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 the Risk and Compliance Manager.