Data Protection Policy[1]

Foreword

RUSI is committed to conducting its business according to all relevant laws and regulations. As part of its day-to-day activities, RUSI and its Staff may have to process and store Personal Data. Said processing and storage needs to comply with the United Kingdom's General Data Protection Regulation ("UK GDPR") as well as the Data Protection Act of 2018 ("DPA").

Application

This policy is mandatory for all of RUSI's employees, contractors and subcontractors (together "Staff") and should be abided by even if there are contractual obligations, policies or procedures which contradict the guidelines established herein. It applies to the Royal United Services Institute for Defence and Security Studies (registered charity no.210639, 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") and therefore all those employed or engaged by RUSI.

All Staff are required to read, understand, and comply with this Data Protection Policy when Processing Personal Data on RUSIs behalf and attend training on its requirements.

Definitions

For the purposes of this policy, the following definitions will apply:

Controller: The entity or individual who determines why Personal Data is processed and how. RUSI may act as Controller in relation to the Personal Data of its employees, Personal Data obtained while conducting research and Personal Data of its members, when it delegates its processing to another entity known as a Processor.

Consent: "Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her[2]."

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

[2] Article 4(11) of the UK GDPR: https://www.legislation.gov.uk/eur/2016/679/article/4

Data Subject: An identified or identifiable individual about whom RUSI holds Personal Data. Data Subjects have rights in relation to their information as established in Chapter III of the GDPR and articles 12-14 of the DPA.

ICO: Stands for Information Commissioner's Office which is the UK entity in charge of supervising compliance with data protection regulations, issuing guidance and sanctioning non-compliance.

Personal Data: Any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. All information which has been permanently anonymised, or which does not allow us to identify a Data Subject will be excluded from this policy.

Processing: Any activity that involves the use of Personal Data. RUSI will be considered a processor when handling Personal Data in relation to research and membership, or its employees.

Processor: The entity or individual who processes Personal Data on behalf of the Controller. RUSI may delegate Personal Data Processing to entities for different reasons. However, said delegation may only be done when there is a signed contract between RUSI and the Processor.

Special Categories of Personal Data: understood as Personal Data which, because of its nature, is subjected to a special protection by the GDPR. Special Categories of Personal Data include racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, as well as biometric or genetic data.

Principles

Lawfulness, fairness, and transparency:

All processing of Personal Data by RUSI will be lawful and justified in one of the lawful bases established in the UK GDPR. Staff must identify and document the legal ground being relied on for each processing activity. As an example, most Personal Data processed by RUSI will fall under one of the following lawful bases for processing:

- Consent/Explicit consent: A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are insufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters. A Data Subject must be easily able to 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 which was not disclosed when the Data Subject first consented. When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent. You will need to evidence Consent captured and keep records of all Consents so that RUSI can demonstrate compliance with Consent requirements.

Examples of consent include RUSI members who consent to having their Personal Data processed when signing up for our membership. This includes keeping a register of their contact information to keep them up to date with upcoming events and publications, as well as recording their payment information. RUSI employees will also consent to having their Personal Data processed so that RUSI can contact them, pay their salaries, etc.

- Contracts: RUSI will process Personal Data required to meet contractual obligations or to meet our legal compliance obligations. This will apply to the processing of information from subcontractors and service providers.
- Legitimate interest: exceptionally Personal Data may be processed without prior consent if there is a legitimate interest in said processing or to protect the Data Subject's vital interests. If any of RUSIs Staff wish to process Personal Data under the basis of legitimate interest, they will have to contact the Risk and Compliance Manager for guidance.
- The lawful basis for processing Personal Data will need to be determined before engaging in any new activity, project, or launching of a new product/service. Moreover, to protect the rights of individuals, any processing to be carried out by RUSI will be transparent, fair, and made clear to the Data Subjects before the processing begins.

For processing of Personal Data to be considered fair and transparent, detailed, and specific information needs to be given to each Data Subject. RUSI informs Data Subjects who visit our webpage on how and why their Personal Data will be processed through our Privacy Policy. In addition, if Staff are to have access to Personal Data collected by a third party, they must ensure that said data was collected in accordance with the UK GDPR and that Data Subjects are aware of their Data being processed by RUSI.

Purpose Limitation:

Personal Data held by RUSI may only be used for the specific and explicit purpose it was obtained for. Any new processing will need to be compatible with the original purpose for which the data was collected. New uses based on compatibility will have to be documented. Those which are incompatible will require a new lawful basis (new contract, fresh consent, or new legitimate purpose to be determined).

Data Minimisation:

Staff must ensure that only the Personal Data that is relevant and necessary to achieve a specific purpose will be processed and stored by RUSI. This means that no information aside from that which is strictly necessary to achieve a purpose will be requested from employees,

members or third parties. Once Personal Data is no longer needed, Staff must ensure it is adequately deleted or anonymized, depending on the circumstances.

Accuracy

Staff must ensure that the Personal Data they use, and hold is accurate, complete, kept up to date and relevant to the purpose for which it was collected. Staff must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Staff must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Some of the ways in which Staff can ensure compliance with the accuracy principle include:

- Employees will be required to inform HR if there are changes to relevant Personal Data. This includes informing any changes to their personal residence address, main phone number, emergency contact and on occasion, they will be required to report changes to special category data (i.e., acquired disabilities which require adjustments for the employee).
- Members will be required to confirm their Personal Data is up to date or report on any changes, at least once a year.
- Subcontractors and suppliers will be required to report any changes in their Personal Data which are relevant to fulfilling the obligations established in their contracts (i.e., main address and phone number, payment information, etc.)

Storage Limitation

No Personal Data must be kept for longer than it is needed to fulfil its purpose, and all retention periods will require adequate justification. Staff must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements. Staff must take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all RUSI's applicable records retention schedules and policies. Further information can be found in our retention policy. As an example, the following guidelines should be considered to comply with the storage limitation principle:

- If an existing member decides to cancel their membership, RUSI should erase all Personal Data linked to payment information and other contact details aside from name and email address. The latter may be kept for statistical/archiving purposes.

After an employee leaves RUSI, any Personal Data which is unlikely to be needed in the future (i.e., legal claims, pension arrangements, etc.) such as emergency contact details or previous addresses, will need to be erased.

Security, Integrity, and Confidentiality

Staff shall ensure that Personal Data is 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. Access is restricted to those who have been duly authorised. Staff must exercise particular care in protecting Special Categories of Personal Data from loss and unauthorised access, use or disclosure. Staff must follow all procedures and technologies RUSI puts in place to maintain the security

of all Personal Data from the point of collection to the point of destruction. Staff may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Although cybersecurity is a fundamental component of data protection confidentiality and integrity, these additional guidelines need to be observed by Staff as well:

- Any Personal Data should be safely stored in password protected devices. Staff should be aware that email is a favoured means of attack for the whole range of cyber threat actors. Although there are technical defences for malicious emails, they can only ever be partially successful: effective security requires the end user to be vigilant and to treat any suspicious emails with care. Whatever platform you choose to use for email services, you must ensure your email account is protected by multi factor authentication as described below.
- Passwords are also an important component of cyber security. It is important, when signing up for online services, that you have a unique password for each of them. Complex passwords are also better, but a unique password is a must and long passwords are always a good idea. By far the easiest way to manage your passwords is to use a piece of software called a password manager. These are an encrypted store of all your usernames and passwords, and even better, they will generate unique, strong passwords for you to use with each service. You must ensure you take care when choosing passwords:
    - Passwords must be unique. You must not reuse passwords on multiple systems or websites.
    - Do not choose passwords based on information that is easily guessable, or discoverable.
    - Do not include your name, place of work, date of birth etc. in passwords.
    - Do not use dictionary words, football teams, place names and other commonly use passwords.
    - Do not use common substitutions e.g., replace the letter 'o' with a zero.
    - Meeting these requirements across a range of websites is challenging, hence the recommendation that you use a password manager. However, you can also write down passwords, provided they are stored securely. If you choose to do this, you must ensure you never leave the notebook containing your passwords accessible and unattended. It must be stored in a locked cupboard or drawer that only you can access.
    - On no account must your password be disclosed to anyone else, not even to a trusted colleague.
- Multi factor authentication is a means of providing additional protection when logging into online services. Typically, you just have a username and password when authenticating to an online service, however if you have multi factor authentication enabled you need an additional step to successfully authenticate to an online service. This can be a hard device you plug into your computer, an app on a smartphone that generates a six-digit code, a notification you have to approve to continue with the login, or a text message. Most large online services, including all the main email providers, social media websites, and cloud storage companies, now support two-factor authentication in one, or more, of these forms. For any RUSI business, two-

factor authentication must be enabled, and where possible a hardware or software solution used, rather than a text message.

- The following security requirements must be met:
    - The device must be protected by PIN, passcode, or biometrics
    - The device must be encrypted
    - Laptops must have a software firewall enabled
    - Laptops must run some form of antivirus or antimalware software
    - The device must automatically lock if unattended or unused for a short period, and require a password to unlock
    - The device must support remote locking and wiping if lost.
    - All devices must be kept up to date. Updates, and security fixes to the device operating system must be applied when they are released. Devices that no longer receive security updates, or otherwise run out-dated operating systems, are not permitted. RUSI reserves the right the check device compliance where necessary.
- RUSI's required method for hosting and sharing files is SharePoint (part of the O365 application suite). In exceptional cases we may use Dropbox but only if the Dropbox is set up and administered by RUSI. Encryption tools should be used when transferring and storing Personal Data. Said encryption should ideally be end to end, covering data at rest as well as in transit.
- As most data breaches are sourced in human error, all employees should be suspicious of any requests of Personal Data from people outside the organisation. Requests of personal information via email or phone should be denied, unless there is a clear lawful basis for providing the information.
- If an employee thinks a data breach has occurred, they must report it to the Risk and Compliance Manager immediately. The Risk and Compliance Manager will then advise on whether the incident requires further reporting to the ICO and/or the National Crime Agency and the Chief Operating Officer/Senior Management Team will make the final reporting decision.

Accountability

RUSI acknowledges its responsibilities in relation to the Personal Data it processes. The guidelines included in this policy are some of the ways in which compliance with the UK GDPR is ensured. Additionally, Staff are required to do the following:

- Carry out a Data Protection Impact Assessment (DPIA) if processing activities considered as high-risk to the rights and freedoms of Data Subjects are to be undertaken. High risk processing includes profiling activities, systematic monitoring of individuals and/or large-scale processing of Special Category Data.
- Ensure an International Data Transfer Agreement is in place when transferring Personal Data outside of the UK.
- When processing Personal Data under the lawful basis of consent, Staff need to be aware that consent needs to be indicated clearly by the Data Subject either by a statement or affirmative action. In this sense, silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

- Perform and document a legitimate interest assessment prior to processing Personal Data under this lawful basis.
- Be aware that Personal Data must be collected only for specified, explicit and legitimate purposes. Any processing for a new purpose will require its independent lawful basis when incompatible with the original purpose. Any new uses based on compatibility need to be documented by Staff.
- Request prior consent from individuals and have a record of how and when consent was granted if this is the lawful basis which will justify a specific processing activity.
- Inform individuals of any changes to privacy policies and request their consent when their data is to be used for new purposes which are incompatible with existing ones.
- Complete all data protection training and be aware of the different rights Data Subjects have and how they may enforce those rights.
- Be aware that Personal Data cannot be shared with third parties unless certain safeguards and contractual arrangements exist. Staff may only share the Personal Data RUSI holds with other employees, agents or representatives of RUSI if the recipient has a job which entails access to Personal Data and the transfer complies with applicable cross-border transfer restrictions.
- Promptly inform the Risk and Compliance Manager of potential data breaches, requests and/or objections from Data Subjects.

Transfer Limitation

The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

Staff may only transfer Personal Data outside the UK if one of the following conditions applies:

a) The UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms.
b) Appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism.
c) The Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
d) The transfer is necessary for one of the other reasons set out in the UK GDPR including:
    i. the performance of a contract between us and the Data Subject.
    ii. reasons of public interest.
    iii. to establish, exercise or defend legal claims.
    iv. to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; and
    v. in some limited cases, for our legitimate interest.

In any case, to transfer Personal Data outside of the UK, a Data Transfer Agreement will be required.

Adequate use of Customer Relationship Management (CRM) Software

RUSI uses CRM Software to manage the information of different types of stakeholders such as members, event attendees, public figures, mailing lists, etc. As the current CRM manages personal data from many individuals, the following guidelines apply to its use. Failure to comply with adequate use of the CRM may result in withdrawal of access.

- **Only RUSI employees should be granted access to the CRM**.
- Employees inputting data into the CRM are in charge of ensuring the recorded information is accurate, complete and up to date, in line with the data protection principles described above. This means employees should verify that all information recorded in the CRM has no typos, is capitalized adequately, includes any relevant clarifications such as prefixes, rank, etc., and contains the most up to date information of an individual at the moment of recording.
- To comply with the data minimization principle, employees should avoid registering information which is not essential to reach the intended purpose for processing. In practice, this means RUSI must do as much as possible with as little data processing as possible.
- Employees should avoid recording special categories of personal data even if it's information they have been given access to. The latter as the UK GDPR prohibits the processing of special categories of personal data unless there is a condition which allows for said processing (e.g., explicit consent).
- Contact information included in the CRM should be used responsibly. This includes avoiding use of CRM information as a mailing list and/or including individuals in newsletters they haven't agreed to receive. Any new use of a data subject's information should be cleared with whoever recorded the personal data in the first place. This given that new or unexpected uses of personal data without prior identification of an adequate lawful basis may violate UK GDPR regulations.

International Data Transfer Agreements

If any Personal Data is to be transferred outside of the UK and/or the European Economic Zone ("EEA"), it is likely that an International Data Transfer Agreement will be required ("IDTA"). Staff that require the transfer of Personal Data outside the UK/EEA will need to contact the Risk and Compliance Manager for advice.

Rights of Data Subjects

All Data Subjects have rights in relation to their Personal Data, which include:

- Right to be informed
- Right of access

- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to restrict data portability
- Right to object
- Rights related to automated decision making, including profiling

Data Subjects may exercise these rights at any moment. The following are some guidelines which must be observed when Data Subjects contact RUSI in relation to their Personal Data:

- All requests made by a Data Subject in relation to their Personal Data must be forwarded immediately to the Risk and Compliance Manager. This is important because the date of the request must be logged.
- If a Data Subject objects to having their Personal Data processed by RUSI, all processing must stop until the Risk and Compliance Manager determines the following steps.
- If someone's Personal Data is being processed under the lawful basis of consent, said consent can be withdrawn at any moment. If consent is withdrawn, all processing must cease.
- Data Subjects can always object to having their Personal Data be processed for direct marketing purposes. If someone objects to receiving direct marketing emails or content, they must immediately be taken off the direct marketing list and their objection should be recorded to prevent contacting them in the future.
- Data Subjects may request access to their Personal Data and RUSI via the Risk and Compliance Manager, should disclose any information it holds on a Data Subject upon request.
- Data Subjects may request their Personal Data to be rectified, updated, or erased.

Any requests made by a Data Subject will be responded during the following month of their reception by the Risk and Compliance Manager. If the request is excessively burdensome, additional time may be required. However, the Data Subject needs to know their request is being processed and that it will take longer than a month to provide an answer.

To ensure compliance with the accountability principle, requests made by Data Subjects will be recorded, along with the outcome of each request by the [Risk and Compliance Manager]. If further action is required (i.e., erasure, rectification, etc.), this will be recorded as well once the task is completed.

Roles and Responsibilities

The Risk and Compliance Manager will be responsible for:

- Managing and requests from Data Subjects and replying in a timely manner.
- Liaising with other RUSI employees if additional information or access is required to reply to a Data Subject Request.
- Providing guidance in relation to the UK GDPR.
- Performing Data Protection Impact Assessments, Compatibility and Legitimate Interest tests when required.

- Implementing Data Transfer Agreements when required.
- Keeping record of any Data Subject requests, responses to requests, Data Protection Impact Assessments, Compatibility and Legitimate Interest Tests.

The Database and Membership Manager will be responsible for:

- Ensuring all Personal Data of members, donors and other individuals is correct and up to date.
- Deleting any Personal Data from members, donors and other individuals which is incorrect, out of date or unnecessary for RUSIs processing purposes.
- Limiting access to Members', Donors' and other individuals' Personal Data and ensure it is safely stored and adequately protected.
- Ensuring any companies hired to manage member/donor and other individuals Personal Data have adequate policies, procedures, and safety measures in place.
- Ensuring no direct marketing emails/content is sent to individuals who have objected or opted out to having their Personal Data processed by RUSI.

The lead researcher will be responsible for:

- Determining if a potential project will require processing and storing of Personal Data.
- If a project requires conducting interviews and/or processing of Special Categories of Personal Data, the lead researcher will be responsible for ensuring explicit consent is obtained from all interviewees and recorded for future reference.
- If a project may present a high risk for the rights and freedoms of Data Subjects, the lead researcher will have to report it to the Risk and Compliance Manager so that a Data Protection Impact Assessment can be concluded.

The Human Resources Director:

- Ensuring all employee data is accurate and up to date.
- Deleting any Personal Data from employees which is incorrect, out of date or unnecessary for RUSIs processing purposes.
- Limiting access to employee Personal Data and ensure it is safely stored and adequately protected.
- Ensuring any companies hired to manage employee Personal Data have adequate policies, procedures, and safety measures in place.
- Data Protection Breaches

In the event of a Data Protection breach, the incident must be reported immediately to the Risk and Compliance Manager who will set in motion the actions established in RUSI's Business Continuity Plan. The Risk and Compliance Manager, alongside the Chief Operating Officer will advise the Senior Management Team on whether reports need to be filed before the Information Commissioner's Office, the National Crime Agency and if Data Subjects need to be contacted in relation to their Personal Data being compromised.

Employees must however stick to the following guidelines if a Data Protection Breach has occurred:

- If the Data breach is a result of a cyber-attack, employees must take the compromised device offline **but should abstain** from turning the device off.

- Any threat or suspicion in relation to Personal Data being compromised must be promptly reported to both the Risk and Compliance Manager and the head of IT.
- Employees must be able to establish what kind of information can be considered as compromised and help assess the impact of the breach.

Version control

Author	First drafted	Approval date and approving body	Latest update
Andrea Plazas	05/03/2023	04/05/2023 – Approved by Senior Management	22/11/2023