The Royal Artillery Centre for Personal Development

GDPR – Data Breach Policy

Policy Statement

1. The Royal Artillery Centre for Personal Development (RACPD) is committed to our obligations under the regulatory system and in accordance with the GDPR, and will maintain a robust and structured programme for compliance, adherence and monitoring. We carry out frequent risk assessments and gap analysis reports during Board Meetings to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, we recognise that breaches can occur, so this policy states our intent and objectives for dealing with such incidents.

2. Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data. The protection and security of the personal data that process is of paramount importance to us and we have developed data specific controls and protocols for any breaches relating to the GDPR and data protection laws.

Purpose

3. The purpose of this policy is to provide the RACPD's intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the GDPR, we also have a requirement to ensure that the correct procedures, controls and measures are in place and disseminated to all employees, ensuring that they are aware of what the protocols and reporting lines are for personal information breaches. This policy details our processes for reporting, communicating and investigating incidents.

Scope

4. This policy applies to all Trustees, employees, associate contractors and consultants who are working on behalf of RACPD in the UK and Germany. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

Data Security & Breach Requirements

5. The RACPD's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

6. Alongside our *'Privacy by Design'* approach to protecting data, we also have a legal, regulatory and business obligation to ensure that personal information is protected whilst being processed by the RACPD. Our technical and organisational measures are detailed in our Data Protection Policy & Procedures. We have certain objectives we wish to achieve:

   a. To adhere to the GDPR and UK Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches.

b. To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information.

c. To utilise information audits and risk assessments for mapping data and to reduce the risk of a breach.

d. To have adequate and effective risk management procedures for assessing any risks presented by processing personal information.

e. To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes as set out in their code of practice or handbooks.

f. To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring. To use the Data Breach spreadsheet for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected.

g. To protect learners and employees – including their data, information and identity.

h. To ensure that where applicable, the GDPR Lead is involved in and notified about all data breaches and risk issues.

i. To ensure that the Supervisory Authority is notified of the data breach (*where applicable*) with immediate effect and at the latest, within 72 hours after having become aware of the breach.

7. We carry out information audits to ensure that all personal data processed by us is accounted for and recorded, alongside risk assessments that assess the scope and impact of any potential data breach; both on the processing and on a data subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, including *(but not limited to*):

a. Encryption of personal data;

b. Restricted access;

c. Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

d. Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

e. Audit procedures on a regular basis to test, assess, review and evaluate the effectiveness of all measures and compliance with the data protection regulations and codes of conduct.

f. Employee assessments and testing to ensure a high level of competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information.

g. Recheck processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal, it is rechecked and authorised by the Data Owner.

Data Breach Procedures & Guidelines

8. The RACPD has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented breach incident form aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

Breach Monitoring & Reporting

9. All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, revision to any such process is recorded in the Change Management and Document Control records.

BREACH INCIDENT PROCEDURES

Identification of an Incident

10. As soon as a data breach has been identified, it is reported to the direct line manager and the GDPR Lead immediately so that breach procedures can be initiated and followed without delay.

11. Reporting incidents in full and with immediate effect is essential to the compliant functioning of the RACPD and is not about apportioning blame. These procedures are for the protection of its employees, learners and third parties and the company and are of the utmost importance for legal regulatory compliance.

12. As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organisation, system or data prior to investigation and reporting. The measures taken are noted on the incident record in all cases.

Breach Recording

13. The RACPD utilises a Breach Incident Form, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder on a secure area on the G Drive and reviewed against existing records to ascertain patterns or reoccurrences.

14. In cases of data breaches, the GDPR Lead is responsible for carrying out a full investigation, appointing the relevant employees to contain the breach, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

15. A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all employees, learners or third parties involved in the breach, in

addition to senior management. A copy of the completed incident form is filed for audit and record purposes.

16. The Supervisory Authority protocols are to be followed and their '***Security Breach Notification Form'*** should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

Breach Risk Assessment

Human Error

17. Where the data breach is the result of human error, an investigation into the root cause is to be conducted and an interview with the employee held.

18. A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with the RACPD's Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.

19. Resultant employee outcomes of such an investigation can include, but are not limited to:

a. Re-training in specific/all compliance areas.

b. Re-assessment of compliance knowledge and understanding.

c. Suspension from compliance related tasks.

d. Formal warning (in-line with the RACPD's disciplinary procedures).;

e. Possible Gross Misconduct proceedings.

System Error

20. Where the data breach is the result of a system error/failure, the IT Manager is to work in conjunction with the GDPR Lead to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.

21. Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident:

a. Attempting to recover any lost equipment or personal information.

b. Shutting down an IT system.

c. Removing an employee from their tasks.

d. The use of back-ups to restore lost, damaged or stolen information.

e. If the incident involves any entry codes or passwords, then these codes must be changed immediately and members of employees informed.

Assessment of Risk and Investigation

22. The GDPR Lead should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

23. The GDPR Lead should look at:

a. The type of information involved.

b. It's sensitivity or personal content.

c. What protections are in place (e*.g. encryption*)?

d. What happened to the information/Where is it now?

e. Whether there are any wider consequences/implications to the incident.

24. The GDPR Lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

Breach Notifications

25. The RACPD recognises our obligation and a duty to report data breaches in certain instances. All employees have been made aware of the RACPD's responsibilities and we have developed strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

Supervisory Authority (Information Commissioners Office, ICO) Notification

26. The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, it would lead to significant detrimental effects on the individual.

27. Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after us becoming aware of it and is kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

28. If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the GDPR Lead and deemed to be ***unlikely*** to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

29. The notification to the Supervisory Authority will contain:

a. A description of the nature of the personal data breach.

b. The categories and approximate number of data subjects affected.

c. The categories and approximate number of personal data records concerned.

d. The name and contact details of our GDPR Lead and/or any other relevant point of contact (*for obtaining further information).*

e. A description of the likely consequences of the personal data breach.

f. A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects).*

30. Where the RACPD acts in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obliged to notify us without undue delay after becoming aware of a personal data breach.

Data Subject Notification

31. When a personal data breach is likely to result in a high risk to the rights and freedoms of people, we will always communicate the personal data breach to the data subject without undue delay, in a written format and in a clear and legible format.

32. The notification to the Data Subject shall include:

a. The nature of the personal data breach.

b. The name and contact details of our GDPR Lead and/or any other relevant point of contact (*for obtaining further information).*

c. A description of the likely consequences of the personal data breach.

d. A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects).*

33. We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational protection measures which render the data unintelligible to any person who is not authorised to access it or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

34. If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

Record Keeping

35. All records and notes taken during the identification, assessment and investigation of the data breach are recorded and authorised by the GDPR Lead and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

Responsibilities

36. The RACPD will ensure that all employees are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

37. The GDPR Lead is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.