Service Police

Appropriate Policy Document for the Processing of Special Category and Criminal Personal Data for Law Enforcement Purposes under the Data Protection Act 2018

Introduction

1. This is the 'appropriate policy document' that sets out how the Service Police[1] will protect special category and criminal conviction personal data in compliance with the Data Protection Act 2018 (DPA 2018). Within this document special category personal data and criminal personal data will be referred to as either 'sensitive data' or 'sensitive processing'. This document will be reviewed not less than six months after its introduction and yearly thereafter.

2. Section 35(3) of the DPA 2018 (the first data protection principle: law enforcement processing) provides sensitive processing is permitted only in the two cases set out in sections 35(4) and (5). For the Service Police (noting that each Provost Marshal is a competent authority[2] and data controller[3]), this means either relying on the consent of the data subject to the processing for the law enforcement purpose[4], or the sensitive processing will only be permitted where:

   a. The processing is strictly necessary for any of the law enforcement purposes;

   b. The processing meets at least one of the conditions in Schedule 8 of the DPA 2018; and

   c. At the time, the processing is carried out the controller has an 'Appropriate Policy Document' in place. This is the 'appropriate policy document'.

Aim

2. The aim of this document is to explain:

   a. The Service Police procedures which are in place to secure compliance with the six data protection principles set out in Part 3 of the DPA 2018 when the processing is carried out by each force (in its capacity as controller) in reliance of one of the conditions set out in Schedule 8; and

[1] The Service Police consist of the Royal Naval Police, Royal Marines Police, Royal Military Police, and Royal Air Force Police.
[2] s.30(1) of the DPA 2018.
[3] s.32 of the DPA 2018.
[4] Consent is a lawful basis for sensitive processing under s.35(4) of the DPA 2018.

b. The Service Police policies about the retention and erasure of such personal data processed in reliance on a condition specified in Schedule 8 to the DPA 2018.

3. This 'appropriate policy document' reflects the requirements to have safeguards in place for sensitive processing carried out for a law enforcement purpose as set out in section 42 and Schedule 1 (Part 4) of the DPA 2018.

Compliance with data protection principles

4. **Lawfulness and fairness**. The lawfulness of the sensitive processing carried out by the Service Police is derived from its official functions as a discrete constituent parts of the Armed Forces, a public authority, and with express powers and responsibilities under primary[5], secondary[6] and subordinate legislation[7]. As permitted by Section 35 of the DPA 2018, the Service Police will carry out sensitive processing for:

a. The 'law enforcement purposes' (for the purposes of Part 3 of the DPA 2018 are defined in section 31 of the DPA 2018 as: 'The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'); and

b. In reliance on the following conditions set out in Schedule 8 to the DPA 2018:

i. Statutory purposes.
ii. Administration of Justice.
iii. Protecting individual's vital interests.
iv. Safeguarding of children and individuals at risk.
v. Legal claims.
vi. Judicial acts.
vii. Preventing fraud
viii. Archiving in the public interest, for scientific or historical research, or for statistical purposes.

5. Information about the sensitive data processing carried out by the Service Police is made available to data subjects via the MOD Privacy Notice.

Law Enforcement Purpose Limitation

6. The Service Police are authorised by law to carry out sensitive processing of personal data for any of the law enforcement purposes. Each force may process

[5] e.g. under the Armed Forces Act 2006.
[6] e.g. under the Armed Forces (Disposal of Property) Regulations 2009/1923.
[7] e.g. under The Queen's Regulations for the Army 1975 (as amended), paragraph J6.046.

sensitive data collected for one of these purposes (whether by the force or another controller), and further use it for any of our other law enforcement purposes, providing the processing is necessary and proportionate to that purpose.
The Service Police will only use sensitive data collected for a law enforcement purpose for purposes other than law enforcement, where it is 'authorised by law'.

Data minimisation

7. The Service Police only collects sensitive data that is necessary and proportionate to carry out the law enforcement purpose. It is processed in the context of carrying out processes which enable us to meet our stated law enforcement purposes for processing.

8. Additionally, the Service Police's internal guidance, training and policies require staff to use only the minimum amount of data required to enable specific tasks to be completed.

9. Where sensitive data processing is for research purposes, wherever possible this is done using anonymised or de-identified data sets.

Accuracy

10. Where key sensitive data is provided directly by individuals, its accuracy is checked where the expediency of the required police response does not prevent it. Data is kept up to date where new information is provided or obtained however it is also necessary to retain historic data for effective delivery of the law enforcement function.

11. Where possible the development and procurement of IT systems within the Service Police seeks to design in data validation and data quality tools to ensure accuracy of information.

12. The Service Police take reasonable steps to ensure that sensitive data which is inaccurate, incomplete or out of date is not transmitted. If it is discovered after transmission that the data was incorrect or should not have been transmitted, then we will tell the recipient as soon as possible. If an individual contacts the Service Police to question the accuracy of their data, we respond to the request in accordance with Section 46 of the DPA 2018. Where we decide not to erase or rectify the data, we will document our decision.

13. As far as possible, the Service Police distinguish between sensitive data based on facts and personal data based on personal assessments or opinions. This is often clear due to the source of the information or type of document. For example, personal information captured by a CCTV camera will be an obvious matter of fact whilst the views provided in a witness statement will clearly be a matter of the witness's opinion.

14. The key law enforcement systems used by the Service Police make it possible to distinguish between sensitive data relating to different categories of data subject, where it is relevant to do so, such as:

a. People suspected of committing an offence or being about to commit and offence;

b. People convicted of a criminal offence;

c. Known or suspected victims of a criminal offence; and

d. Witnesses or other people with information about offences.

Storage limitation

15. The Service Police will only retain 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. Defence records management policy and procedures JSP 441 is available online.

16. The College of Policing's Authorised Professional Practice on Information Management (Retention, Review and Disposal) is currently not applicable to the Service Police's retention of sensitive data processed for the law enforcement purpose, however where possible the Service Police complies with the direction provided. It can be accessed via the College of Policing website.

17. Where routine review and disposal is not feasible or cost-effective, safeguards will be put in place to minimise any detriment caused by continued retention of sensitive data and requests from individuals in regard to their rights to rectification and/or erasure will be dealt with by exception.

Integrity and confidentiality

18. The Service Police comply with the relevant parts of the legislation relating to security. Sensitive data will be stored within a secure government Information Technology system.

19. The Service Police ensure that appropriate security measures are in place to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed without lawful authority. In addition, access to sensitive data is limited to Service Police personnel, agents, contractors and other third parties (for example, the Service Prosecuting Authority, Military Court Service, Commanding Officers and their unit and formation discipline staff) who have a lawful purpose and need to know in the administration of the Service Justice System.

20. The Service Police seek to comply with both the College of Policing Information Assurance authorised practice, and relevant parts of the ISO27001 Information Security Standard.

20. The Service Police ensure that appropriate policy, training, technical and procedural measures are in place. These will include, but are not limited to, ensuring force buildings are secure and protected by adequate physical means. The areas restricted to Service Police officers and staff are only accessible by those holding the appropriate identification and having legitimate reasons for entry. Audits of our building security are carried out to ensure that they are secure.

21. The Service Police Single Service Technical Instructions, operating procedures and policies make clear what use may be made of any sensitive data contained within them.

22. All Service Police staff are subject to pre-employment vetting checks and periodical vetting checks once in post. All Service Police staff have to undergo mandatory data protection and security training.

23. Any security incidents involving sensitive data are fully and corporately recorded, investigated and assessed for whether they should be reported to the Information Commissioners Office.

Requirement to keep records

24. Where sensitive processing is carried out by the Service Police (as the data controller), the following information is recorded in its Record of Processing Activities:

a. Whether the sensitive processing is carried out in reliance on the consent of the data subject, or if not, which condition in Schedule 8 is relied on;

b. How the processing satisfies Section 35 (lawfulness of processing); and

c. Whether the sensitive data is retained and erased in accordance with the policies described in Paragraphs 14, 15 and 16, and, if it is not, the reasons for not following those policies.

Further information

25. Each of the Service Police Provost Marshals are, individually, competent authorities and controllers for the purposes of Part 3 of the DPA 2018. The function of Data Protection Officer is currently being carried out, for and on their behalf, by the MOD's Data Protection Officer until further notice. For further information about our compliance with data protection law or if you wish to contact our Data Protection Officer, please use contact details below:

a. **MOD Data Protection Officer**
Ground floor, zone D
Main Building
Whitehall
London SW1A 2HB

Email: cio-dpa@mod.gov.uk

b. **Service Police Data Protection Adviser:**
Service Police Crime Bureau
Bassett Wilson Building
MoD Southwick Park
Nr Fareham
Hampshire PO17 6EJ

Email: SpecOpsRMP-SPCB-DBS0Mailbox@mod.gov.uk