

SERVICE POLICE LEGACY INVESTIGATIONS PRIVACY NOTICE

Content

Introduction	1
What constitutes personal data?	2
The identity and contact details of Ministry of Defence (MOD) Data Controller and Data Protection Officer	2
Data Protection Principles	2
Our legal basis for processing your personal data	2
How we collect your Data?	3
Why we are collecting or processing your data?	4
Can SPLI process my personal data without my consent?	4
With whom we will be sharing your personal data?	4
How we will Process your Personal Data?	4
How we store your data	4
How long will we keep the personal data, or criteria used to determine the retention period	5
Automated decision making	5
Your rights	5
Why some rights are not applicable?	6
Costings	6
What we need from you	6
Right to complain	6

Introduction

1. The following document is to explain your rights and to provide you with information you are entitled to under the Data Protection (DP) legislation.
2. This notice applies to all persons external to Service Police Legacy Investigations (SPLI) of whose personal data SPLI processes in the investigation of the allegations made by Iraqi civilians of serious criminal behaviour by UK Armed Forces in

OFFICIAL

Iraq from 2003-2009. Personal data can be processed in relation to Iraqi nationals and both current and former British Service personnel.

What constitutes personal data?

3. Personal data is information that relates to an identified or identifiable individual. What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier.

The identity and contact details of Ministry of Defence (MOD) Data Controller and Data Protection Officer

4. The Ministry of Defence (MOD) is the Data Controller. The contact details are; MOD Main Building, Whitehall, London SW1A 2HB

5. The Data Protection Officer can be contacted at;

MOD Data Protection Officer

Ground floor, zone D
Main Building
Whitehall
London
SW1A 2HB

Email

cio-dpa@mod.gov.uk

Data Protection Principles

6. SPLI will comply with the data protection principles under the DP legislation. This says that personal information which we hold about you must be:

- a. Used lawfully, fairly and in a transparent way.
- b. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- c. Relevant to the purposes we have told you about and limited only to those purposes.
- d. Accurate and kept up-to-date.
- e. Kept for only as long as necessary for the purposes we have told you about.
- f. Kept securely.

Our legal basis for processing your personal data

7. We will only process your personal data when the law allows us to. The Data Protection Act 2018 states that, as a government department, SPLI may process

OFFICIAL

personal data for law enforcement purpose if it is necessary for the effective prevention or detection of unlawful acts.

8. SPLI have been directed by the Secretary of State to carry out investigations into alleged criminal behaviour by UK Armed Forces during 2003-2009 in Iraq. SPLI is meeting the government's legal duty to investigate the remaining allegations. SPLI ensures that all investigations are conducted both legally and in accordance with the statutory framework of the Armed Forces Act 2006 as amended.

9. We may also process your personal data for non-law enforcement purposes. You can read the [MOD privacy Notice](#) for further information on general personal data processing within the MOD.

How we collect your Data?

10. SPLI collects personal information through various support agencies in the course of investigative processes as listed below;

- a. Permanent Joint Headquarters (PJHQ)
- b. Royal Military Police (RMP)
- c. Royal Air Force (RAF)
- d. Army
- e. Royal Navy (RN)
- f. Army Historic Branch
- g. Intelligence service
- h. Legal organisations

11. The personal data that SPLI may collect relates to individual suspects or offenders, dependants, victims, and witnesses or information providers of the alleged offences. We collect, store and use the following categories of personal information about you:

- a. Personal contact details for example name, address title, personal email addresses
- b. Date of birth
- c. Gender
- d. Marital status
- e. Copy of identification documents
- f. Service records
- g. Performance information
- h. Financial details

12. We may collect, store and use the following sensitive personal information:

- a. Medical records
- b. Genetic information and biometric including fingerprints and other scanning data
- c. Information about criminal convictions/ allegations and offences

OFFICIAL

- d. Race, ethnic origin
- e. Sex life or sexual orientation
- f. Religious or philosophical belief

13. This list is by no means comprehensive and further personal data may be collected to facilitate the investigative process.

Why we are collecting or processing your data?

14. The situation in which we will process your personal information is listed below:

- a. If you are a victim
- b. If you are a complainant
- c. If you are a witness or information provider
- d. If you are a suspect
- e. Requests for assistance

Can SPLI process my personal data without my consent?

15. SPLI, as a competent authority, can process your personal data without your consent if it is necessary for the performance of a task carried out for the purpose of prevention, investigation, detection or prosecution of an offence.

With whom we will be sharing your personal data?

16. SPLI are obliged to share your data with the following organisations:

- a. Directorate of Judicial Engagement Policy (DJEP)
- b. Service Prosecuting Authority (SPA)
- c. Courts – if under instruction to do so (Exemption)¹

How we will Process your Personal Data?

17. Data is processed via the Forensic Data Handling Capability (FDHC) System. This is a standalone, air gapped and fully accredited system. Accreditation is provided by Army HQ Cyber-Sec and STRAPSO. Data is used to facilitate criminal investigations.

How we store your data

18. Your personal data is stored in secure government information technology systems, this includes FDHC. We have put in place all appropriate measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered, or disclosed. In addition, we limit access to your personal information only to MOD personnel, agents, contractors and other third parties who

¹ Legal advice and proceedings - section 31(2)

OFFICIAL

have a business need to know. They will only process your personal information on our instructions. Details of these measures are available on request only.

How long will we keep the personal data, or criteria used to determine the retention period

19. We only retain your personal information for as long as necessary to fulfil the purposes we have collected it for, including for the purposes of satisfying any legal requirements. Our Defence records management policy and procedures JSP 441 is available online.

20. After the retention period, has elapsed all data will be destroyed securely in line with MOD data destruction policy. To determine the appropriate retention period for your personal data, we consider the amount, nature, and sensitivity of the personal data, the protentional risk of harm from unauthorised use or disclosure of your personal data and the applicable legal requirements to retain personal data.

Automated decision making

21. Your personal data will not be used for any automated decision making.

Your rights

22. Under Data Protection legislation you have the following individual rights with regards to your personal data:

23. **The right of access** to your personal data and supplementary information (commonly known as a Subject Access Request (SAR)) enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

24. If you want to find out if SPLI, or any of our partners, hold personal information about you or want to make any correction you can make a “SAR” request under the Data Protection Legislation. If we hold information about you, we will:

- a. Give you a description of it
- b. Tell you why we are holding it
- c. Tell you to whom it has been disclosed
- d. Let you have a copy of the information in a form that is clear and as understandable as possible

25. Please be as specific as possible about the information that you require.

26. Each request is assessed on a case by case basis, and where it is identified, due to legal reasons, that information cannot be disclosed, you will be provided with an explanation as to why your request has been refused.

OFFICIAL

27. **The right to correction.** This allows you to have any inaccurate personal data rectified, corrected or completed if it is incomplete.

28. **The right to data portability.** This allows you to obtain and re-use your personal data for your own purposes across different services.

29. If you wish to have your data rectified, to submit a SAR or request your information to be transferred to another party, please make a request in writing to the following address; SPLI, Building 396C, Trenchard lines, Upavon, SN9 6BE.

Why some rights are not applicable?

30. Due to the nature of SPLI work, some rights such as the right to erasure, the right to object to processing and the restrictions of processing does not apply. The Data Protection Act 2018 states that SPLI, as a law enforcement agency, can withdraw individual rights for the purposes of 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.

Costings

31. You will not have to pay a cost to access your personal information (or to exercise any of the other rights). However, we may be lawfully allowed to charge a fee if your request is clearly unfounded or excessive. Alternatively, we can refuse to comply with the request in such circumstances.

What we need from you

32. To comply with your request, we may sometimes 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 an appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to complain

33. If you are unhappy with how any aspect of this privacy notice, or how your personal information is being processed, please contact:

MOD Data Protection Officer

Ground floor, zone D
Main Building
Whitehall
London SW1A 2HB

Email: cio-dpa@mod.gov.uk

SERVICE POLICE LEGACY INVESTIGATIONS

OFFICIAL

34. We will acknowledge your complaint within 5 working days and send you a full response within 20 working days. If we can't respond fully in this time, we will write and let you know why and tell you when you should get a full response.

35. If you are still not happy, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Email: casework@ico.org.uk or via their website; <https://ico.org.uk/global/contact-us/>

Further information can be found at; <http://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

Changes to this privacy notice

36. SPLI reserve the right to update this privacy notice at any time, and we will provide a new privacy notice when any substantial updates are made.

37. If you have any questions about this privacy notice, please contact the DPA officer at the following address. SPLI, Building 396C, Trenchard Lines, Upavon, SN9 6AE.