Privacy and Data Protection Policy

For Home Office Expert Panels

(i) Expert Panel to consider applications for special licences to prescribe cannabis based medicinal products

26th June 2018

Version 1.0

Version Control

This guide is managed by the Home Office Science Secretariat. Any suggestions for improvements or comments should be directed to Joanne.Wallace@homeoffice.gsi.gov.uk

Version 1.0	**Effective Date**	26/06/2018
	Last Revision Date	26/06/2018
	Approved by	Mark Greenhorn
	Next Revision Date	26/06/2020
	Audience	All members and staff of, and supporting: • Expert Panel

Contents

1.0 Overview

1.1 Purpose

1.1.1 The objective of this policy is to ensure that:

- Personal Data (including Special Category Data) is processed fairly and lawfully by the Expert Panel in compliance with the requirements of Data Protection Legislation and other relevant information governance obligations;
- The Expert Panel, as well as the Home Office officials within the Secretariat are aware of their responsibilities when processing Personal Data on behalf of the Expert Panel; and
- The Expert Panel establishes and maintains a culture of data protection by design.

1.2 Scope

1.2.1 This policy applies to all members of the Expert Panel, as well as Home Office officials supporting the Panel, and to all processing activities, including those associated with law enforcement functions.

1.3 Approval

1. 3.1 This policy was approved by the relevant bodies as follows

- Expert Panel (TBC)

1.4 Review and consultation

1.4.1 This policy will be subject to periodic review as considered appropriate by the Panel and supported by officials within the Home Office Science Secretariat.

2.0 Policy statement

2.1 The Expert Panel will comply with Data Protection legislation, including integrating data protection by design and default, by:

I. Ensuring all staff within each body and officials supporting each body within the Home Office handle Personal Data lawfully and correctly, adhering to the Data Protection Principles. This includes requiring all personnel directly involved in the processing of Personal Data to complete appropriate training on a regular basis;

II. Always requiring a legitimate and proportionate reason for the processing of Personal Data, ensuring that only the minimum necessary for a specified purpose(s) is processed;

III. Being open and transparent, so far as operational and security constraints allow, about how it processes Personal Data and for what purposes. This includes providing appropriate fair processing information when Personal Data is collected or obtained for the first time or is processed for a new purpose;

IV. Managing requests from Data Subjects to access their Personal Data in accordance with the Information Commissioner's Subject Access Code of Practice and providing mechanisms which allow Data Subjects to exercise their rights, including to amend, update, delete, or restrict the processing of Personal Data where appropriate;

V. Implementing processes and procedures designed to ensure the accuracy and quality of Personal Data at the point it is collected or obtained and throughout its lifecycle;

VI. Undertaking a Data Protection Impact Assessment and consulting with the Data Protection Officer before new Personal Data processing is deployed that is likely to significantly affect individuals. This includes profiling, large scale processing and sharing of Personal Data. Where processing is high risk and those risks cannot be sufficiently addressed the Data Protection Officer will consult with the ICO;

VII. Managing the lifecycle of the Personal Data including securely destroying Personal Data once the purpose(s) for its processing have come to an end, provided that there is no other specified legal requirement or valid business/operational reason for its continued retention;

VIII. Ensuring that its procurement processes and contractual arrangements with external service providers (or any other third party) processing Personal Data on its behalf, include adequate measures to ensure compliance with Data Protection Legislation and any associated requirements outlined in this policy;

IX. Notifying the Data Protection Officer (in advance where possible) of implementing or agreeing any proposed transfer arrangements of Personal Data to countries or territories outside the European Economic Area;

X. Complying with all other relevant legal requirements which apply to its processing of Personal Data, including relevant information sharing gateways and common law powers to disclose data;

XI. Adhering to other relevant legal requirements, policies or guidance which apply to its processing of personal;

XII. Ensuring that any complaint about the processing of Personal Data or non-compliance with this policy will be dealt with promptly and in accordance with the relevant procedure. The Data Protection Officer will be notified of any such complaints;

XIII. Approaching the identification, control and mitigation of Data Protection risks in the same way as other risks and reflecting them in corporate and local risk registers;

XIV. Maintaining accurate records on Personal Data processing.

3.0 Related legislation, policies, standards and guidance

3.1 Legislation

3.1.1 Data Protection Legislation means the:

- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)), and;

- Data Protection Act 2018, regulations made under the Act, and regulations made under section 2(2) of the European Communities Act 1972 which relate to the GDPR or the Law Enforcement Directive (Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA).

3.2 Other relevant policies and guidance

- HMG Security Policy Framework

- HMG Data Sharing Framework (currently being drafted by DCMS)

3.3 Supporting standards and guidance

3.3.1 This policy will be supported by standards, guidance and Privacy Impact Notice published on the Expert Panel website.

3.4 Data use and protection

3.4.1 See associated Privacy Impact Notice published on the Expert Panel website.

Annex 1: Definitions

Controller: the organisation (alone, jointly or in common with other organisations) which determines the manner and purposes for which Personal Data is to be processed.

Processor: processes data on behalf of the Controller (other than an employee).

Data Protection Impact Assessment: a methodology to identify the most effective way to comply with Data Protection Legislation and meet individuals' expectations of privacy. It allows organisations to identify and mitigate Data Protection Risk.

Data Protection Legislation: the General Data Protection Regulation together with the Data Protection Act 2018 (DPA) and all secondary legislation made under it. These laws govern the way in which Controllers can process an individual's Personal Data and provide individuals rights in relation to the processing of, and access to, their personal data.

Data Protection Principles: a set of overarching requirements defined in Data Protection Legislation.

Data Protection Risk: that part of the Department's overall risk portfolio which relates to the, integrity, availability and confidentiality of Personal Data.

Data Subject: an individual who is the subject of Personal Data.

European Economic Area: the member states of the European Union plus Norway, Iceland and Lichtenstein.

Home Office: the Secretary of State for the Home Department and the Home Office.

Personnel: includes the Forensic Science Regulator, Surveillance Camera Commissioner, the members of the ACMD, ASC and BFEG and Home Office officials supporting directly these five Arms Length Bodies within the Home Office Science Secretariat, Pathology, Regulation and Services team as well as all temporary staff, contractors, consultants and any third parties with whom special arrangements (such as Processor, confidentiality or non-disclosure agreements) have been made.

Information Asset Owners: officials within each ALB, who are responsible for the processing of Personal Data within their assigned area of control.

Information Commissioner: the regulator appointed by the Crown to promote public access to official information and protection of personal information. Compliance with the Data Protection Legislation is enforced by the Information Commissioner.

Personal Data: information which relates to a living individual who can be directly identified from either the information itself, or by combining the information with other data available to the Home Office. Personal Data includes expressions of opinion and indications of intention, as well as factual information. Where referenced in this document the term Personal Data includes Special Category Data.

Personal Data Breach: the loss, theft, inappropriate use or unauthorised disclosure of Personal Data.

Process/Processed/Processing: includes collecting, recording, storing, retrieving, transmitting, amending or altering, disclosing, deleting, archiving and destroying Personal Data.

Restrictions: limitations which apply to the processing of personal data in specific circumstances as expressed within legislation.

Special Category Data: Personal Data that is particularly sensitive because it could create more significant risks to a Data Subject's fundamental rights and freedoms if compromised or processed inappropriately. It includes information about: race; ethnic origin; political views; religion; trade union membership; genetics; biometrics (where used to verify identity); health; sex life; and sexual orientation.

Annex 2: Roles and responsibilities

A2.1 ALB plus Home Office Secretariat Personnel

All members of the five Arms Length bodies and Home Office officials within the HO Science Secretariat, Pathology, Regulation and Services Unit are responsible for:

- Actively supporting compliance with this policy and should only process Personal Data for lawful and legitimate purposes directly related to the performance of their duties;
- Reporting actual or suspected Personal Data Breaches to HO Security so that they can co-ordinate the Department's response and help to implement any required remedial actions.

A2.2 Information Asset Owners

Information Asset Owners are responsible for:

- Ensuring that Home Office Personnel within their area of control are aware of this policy and are adequately trained in the handling of Personal Data;
- The assessment and reporting of Data Protection Risk linked to the Processing of Personal Data within their area of control;
- Ensuring that Data Protection Impact Assessments are carried out as part of the development and implementation of any new business process including IT system which is to be used to Process Personal Data;
- Implementing appropriate procedures to ensure compliance with data protection legislation and any relevant restrictions on the Processing of Personal Data within their area of control.

A2.3 Data Protection Practitioners

Within the HO Science Secretariat, Pathology, Regulation and Services Unit we have appointed a number of Data Protection Practitioners. These staff will provide first line support to the staff supporting each body on Data Protection issues, in particular by providing practical support, data sharing advice and guidance, answering data protection related questions, monitoring compliance with the regulation on data protection related matters, including but not limited to:

- Who can data be shared with

- What data can be shared
- What data can be requested from third parties
- What is the legal basis for sharing/requesting data
- What is large scale/bulk data sharing
- Support/advise/review Data Protection Impact Assessments (DPIA)
- How long data can be kept for

Data Protection Practitioners are responsible for:

- Providing advice and guidance to colleagues within their designated business area(s) on the implementation and interpretation of this Policy and/or Data Protection Legislation;
- Supporting the assessment and reporting of Data Protection Risk linked to the Processing of Personal Data within their designated business area;
- Promoting and monitoring compliance with this Policy, Data Protection Legislation and other related statutory, common law or regulatory requirements which apply to the Home Office.

A2.4 Data Protection Officer

The Data Protection Officer is responsible for:

- Raising the profile of data protection compliance across the Expert Panel and with those staff responsible for the processing of Personal Data;
- Providing advice and guidance to Home Office staff within the unit about their obligations under Data Protection Legislation, ensuring service delivery is balanced with compliance;
- Monitoring compliance with Data Protection Legislation, including the assignment of responsibilities; and overseeing training for staff involved in Processing operations;
- Designing and implementing a programme of risk-based audits to test compliance;
- Providing advice on the mitigation of Data Protection Risk, including those risks identified as a result of Data Protection Impact Assessments;

- Co-operating with the Information Commissioner's Office, acting as their main contact point on issues related to the Processing of Personal Data;
- Providing advice and recommendations following both data processing audits and data breaches.

A2.5 Home Office Science Secretariat, Pathology, Regulation and Services Unit

The Home Office Science Secretariat, Pathology, Regulation and Services Unit is responsible for liaison with the Home Office Sponsorship Unit and other relevant Home Office bodies to enable:

- The setting the policies that govern the business' overall adherence to the data protection legislation, and its processing of personal data.
- The setting and advising the business on Knowledge and Information Management policies and procedures.
- Advising the business on the organisational measures and controls required to protect the security and integrity of Personal Data Processed by the Home Office, Managing and resolving actual or suspected Personal Data Breaches and notifying the Data Protection Officer of any Personal Data Breach and keeping them fully informed during its management and resolution. These activities will be undertaken in consultation with Home Office Security officials.

A2.7 The Home Office Internal Audit Unit

The Home Office Internal Audit Unit is responsible for:

- Auditing the business processes, operating procedures and working practices of the Home Office and its service providers including, where appropriate, assessment of compliance with this policy;
- Sharing audit findings which identify instances of non-compliance with this policy and/or Data Protection Legislation with the Data Protection Officer.