Data Protection Policy

Introduction

1 The objective of this policy is to ensure that:

a Personal data (including special category data) is processed fairly and lawfully by the Undercover Policing Inquiry (the Inquiry), in compliance with the requirements of data protection legislation and other relevant information governance obligations;
b Undercover Policing Inquiry personnel are aware of their responsibilities when processing personal data on behalf of the Inquiry; and
c The Inquiry establishes and maintains a culture of data protection by design.
d Undercover Policing Inquiry personnel are aware of their responsibilities if a personal data breach occurs.

Scope

2 This policy applies to all Inquiry personnel and to all data/information processing activities.

Data Protection Legislation

3 Data Protection Legislation means the:
a General Data Protection Regulation (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;
b 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 General Data Protection Regulation 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).
c Other definitions in relation to data protection are at Annex A.

Policy Statement

4 The Inquiry will comply with data protection legislation, including integrating data protection by design and default, by:

a Ensuring all Inquiry staff handle personal data lawfully and correctly, adhering to the data protection principles[1]. This includes requiring all Inquiry personnel directly involved in the processing of personal data to complete appropriate training on a regular basis;

b 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;

c 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;

d Managing requests from data subjects to access their personal data in accordance with the *Information Commissioner's Subject Access Code of Practice*[2] 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;

e 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;

f 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 Information Commissioner's Officer;

g 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;

h 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;

i 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;

j 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;

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

l 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;

[1] Article 5 of the General Data Protection Regulation

[2] https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf

m 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;
n Maintaining accurate records on personal data processing.

Roles and Responsibilities

5 Inquiry Personnel

All Inquiry Personnel must:

a Actively comply with this policy;
b Only process personal data for lawful and legitimate purposes directly related to the performance of their duties;
c Report actual or suspected personal data breaches to the Information Manager/Data Protection Officer so that they can co-ordinate the Inquiry's response and help to implement any required remedial actions.

6 Information Asset Owners

Information Asset Owners must:

a Ensure that Inquiry personnel within their area of control are aware of this policy and are adequately trained in the handling of personal data;
b Assess and report data protection risk linked to the processing of personal data within their area of control;
c Ensure that Data Protection Impact Assessments are carried out as part of the development and implementation of any new business process including IT systems that are to be used to process personal data;
d Implement appropriate procedures to ensure compliance with data protection legislation and relevant restrictions to the processing of personal data within their area of control.

7 Data Protection Officer

Data Protection Officers and any Data Protection Practitioners must:

a Inform and advise the controller or the processor of their obligations pursuant to the data protection legislation;
b Maintain data protection compliance across the Inquiry and with those staff responsible for processing personal data;
c Provide advice and guidance to Inquiry staff about their obligations under data protection legislation, ensuring service delivery is balanced with compliance;
d Provide advice and guidance to colleagues on the implementation and interpretation of this policy;
e Monitor compliance with data protection legislation, including the assignment of responsibilities; and overseeing training for staff involved in processing operations;
f Design and implementing a programme of risk-based audits to test compliance;
g Provide advice on the mitigation of data protection risk, including those risks identified as a result of Data Protection Impact Assessments;
h Co-operate with the Information Commissioner's Office, acting as their main contact point on issues related to the processing of personal data;
i Providing advice and recommendations following both data processing audits and data breaches.

8 The Overview Board: Roles and Responsibilities

a Setting the policies that govern the organisation's overall adherence to the data protection legislation and its processing of personal data.

9 The Information Management and Security Board: Roles and Responsibilities

a Development of and advising the organisation on information management and security policies and procedures.

b Advising the Inquiry on the organisational measures and controls required to protect the security and integrity of personal data processed by the Inquiry;

10 Information Manager: Roles and Responsibilities

a Managing and resolving actual or suspected personal data breaches;

b Auditing the business processes, operating procedures and working practices of the Inquiry and its service providers including where appropriate, assessment of compliance with this policy;

c Sharing audit findings which identify instances of non-compliance with this policy and or data protection legislation with the Data Protection Officer;

d Notifying the Data Protection Officer of any personal data breach and keeping them fully informed.

Data Breaches

11 A personal data breach is:
"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted stored or otherwise processed"[3]

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just losing personal data"[4].

Examples of a personal data breach can include (but are not limited to):

a Access by an unauthorised third party ;

b Deliberate or accidental action (or inaction) by a controller or processor;

c Sending personal data to an incorrect recipient

d Computing devices containing personal data being lost or stolen;

e Alteration of personal data without permission; and

f Loss of availability of personal data.

12 All Inquiry personnel or processors discovering or responsible for any security incidents that may or may not lead to a personal data breach MUST report this as soon as possible to the Information Manager/Data Protection Officer.

13 In order to establish if a personal data breach has occurred, full details should be submitted to the Information Manager using the *Data Incident Report Form*.

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Article 4 (12))
[4] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

14 The Data Incident Report Form should be completed and returned to the Information Manager as quickly as possible, normally on the same day.

15 If a data breach has occurred, the **Data Protection Officer** will:

a Take prompt steps to mitigate the impact of the breach;

b Establish the likelihood and severity of the resulting risk to people's rights and freedoms. If 'high risk', promptly inform those affected and advise them of any immediate risk of damage and help them take steps to protect themselves from the effects of the breach. The following information should be provided:

i the name and contact details of the data protection officer or other contact point where more information can be obtained

ii a description of the likely consequences of the personal data breach; and

iii a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the steps taken to mitigate any possible adverse effects.

c Notify the Information Commissioner's Office, if required, as soon as possible but within 72 hours of becoming aware of the breach.

d Investigate the breach to ascertain if it was a result of human error, or a systemic issue and see how a recurrence can be prevented (for example, through better processes, further training or corrective steps.)

e Ensure all the facts relating to the breach, its effects and the remedial actions are documented.

f Notify the Home Office Corporate Security, (as accreditor of our information systems), as required under Home Office policy.

16 When reporting a breach to the Information Commissioner's Office the following information must be provided:

a A description of the nature of the personal data breach including where possible:

i The categories and approximate number of individuals concerned

ii The categories and approximate number of the personal data records concerned

b A description of the likely consequences of the personal data breach and

c A description of the measure taken or proposed to be taken to deal with the personal data breach, including, where appropriate the measures taken to mitigate any possible adverse effects.

Annex A: 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 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 Inquiry'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.

Inquiry Personnel: includes all Inquiry employees as well as all temporary staff, contractors, consultants and any third parties with whom special arrangements have been made, (such as processor, confidentiality or non-disclosure agreements).

Information Asset Owners: officials within the Inquiry, 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. The Information Commission enforces data protection legislation.

Personal data: information that 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 Inquiry. 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.