National Security and Online Information Team

Data Protection and Compliance Policy

CONTENTS

Introduction

Audience & Aims

1.1 This Compliance Policy (**"Policy"**) is directed to officials working in the DSIT National Security and Online Information Team (**'NSOIT'**) (collectively referred to in this Policy as **"Analysts"**) and its purpose is to provide guidance to help ensure that the collection of open source information is necessary, proportionate and in line with applicable laws.

1.2 Failure to comply could result in enforcement action against DSIT by the Information Commissioner's Office or Investigatory Powers Commissioner's Office. Additionally, it could generate complaints or claims for compensation against DSIT from affected individuals which could result in negative reputational impacts.

1.3 Analysts should ensure that they carry out their activities in accordance with this Policy and use the Data Collection Checklist when undertaking new tasks in relation to mis/disinformation threats and online manipulation ("**Collection Activities"**).

NSOIT Overview

1.4 NSOIT sits within the Security and Online Harms Directorate in DSIT and works with cross-government partners and external organisations to build a picture of mis/disinformation threats, and lead on the day-to-day operational response to addressing disinformation online through our relationships with social media platforms.

1.5 NSOIT's remit is to focus on risks to national security and public safety broadly operates in two key areas:

[redacted] **Monitoring and analysis** – Analysts review Open Source Information (**"OSINF"**, i.e. data and information that resides in the public domain which is freely available) (**"OSINF Content"**) [redacted]

- [redacted]

b) **Operational response and Platform Engagement** – Evaluation of whether any OSINF Content may be in breach of the content moderation policies of the social media platforms from which the content derived. If OSINF Content is considered by NSOIT to be harmful and in violation of a provider's terms of service, or represents an emerging threat that platforms should be made aware of, then – subject to overall ministerial endorsement - NSOIT may share this with the relevant social media platform for appropriate action at their discretion. It is then for the platform to decide on the relevant course of action.

1.6 NSOIT respects freedom of expression, and does not seek to capture genuine political debate, nor does it share content with platforms from elected politicians, journalists or established news outlets to platforms.

1.7 For the purpose of paragraph 1.6 above, a journalist is someone whose content is published by an entity whose main purpose is the publication of news related material. That material should be produced by different people, subject to editorial control and be published in the course of a business. We would expect that the entity is subject to a standards code, which may have been put in place by an independent regulator, that it has clear complaints handling procedures and has a registered address or place of business within the UK.

2. Legal and regulatory framework

2.1 NSOIT must ensure that it operates in full compliance with all applicable legislation, including but not limited to:

a) **Human rights laws** such as the European Convention on Human Rights (ECHR) and the Human Rights Act 1998 (HRA) which protect Convention rights;

b) **Data Protection legislation**, including the UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018 (DPA); and

c) **Surveillance laws** such as the Regulation of Investigatory Powers Act 2000 ("**RIPA**").

2.2 Whilst the use of personal data is not necessary for NSOIT's activities, it is nevertheless likely to process personal data as part of the monitoring and analysis of OSINF Content, such as social media handles, usernames and any other personal data (including special category data) contained within collected social media posts. NSOIT recognises the importance of ensuring that interference with individuals' right to privacy is limited to what is strictly necessary in relation to its legitimate policy objectives and takes appropriate measures to safeguard personal data, as outlined in Schedule 2, Part A to this Policy. Schedule 2 Part B to this Policy describes how NSOIT ensures compliance with RIPA.

3. Monitoring & Analysis

Permitted data sources

3.1 Monitoring and analysis must be limited to overt capabilities, i.e. information sourced from monitoring/research that can be conducted across publicly accessible areas of the internet. **This is limited to traditional media reporting, curated databases, and social media platforms which are publicly accessible for the purpose of obtaining access to the platforms, HMG comms analysis and events monitoring**.

Permitted purposes

3.2 NSOIT may either itself commission particular tasks, provided that such tasks are within its remit or it may be tasked by central command structures, for example, Cabinet Office National Security Secretariat (NSS). In cases where NSOIT is setting up sustained monitoring for disinformation narratives (as the CDU did for Russia/Ukraine and Covid-19) , it must seek appropriate ministerial agreement, before undertaking those tasks.

3.3 Notwithstanding the way in which NSOIT is instructed to carry out a particular task, it is the responsibility of NSOIT's Analysis team to ensure that each Collection Activity undertaken by it:

a) meets an identifiable and legitimate policy objective of the government department, and is proportionate to that policy objective i.e. in line with NSOIT's lawful basis, it must be ensured that any collection activity is in line with NSOIT's remit as set out in 3.2 above and for example, the topic is within agreed expectations set at a policy level;
b) meets all applicable data protection requirements; and
c) does not amount to "**Directed Surveillance"**.

Engagement with external delivery partners

3.4 NSOIT may either carry out its own monitoring and analysis or engage external organisations to carry out such tasks.

3.5 When NSOIT appoints a third party to conduct social media monitoring and analysis (**"Delivery Partner"**), it must ensure that such partners operate strictly in accordance with NSOIT's instructions and with all applicable laws and policies. In particular:

a) Surveillance legislation: **NSOIT** bears overall responsibility in ensuring any work undertaken under its name remains outside the scope of RIPA for the duration of any project. The Home Office Revised Code of Practice on Covert Surveillance and Property Interference (**"CHIS guidance"**) makes clear that any private sector partner would be considered an agent of HMG;

b) Data protection legislation: DSIT assumes responsibility as controller under Data Protection Legislation to the extent that it is collecting and processing any personal data and accordingly third party providers must be appointed as processors in accordance with article 28 UK GDPR to ensure that they only operate on DSIT's documented instructions;

3.6 Accordingly, wherever a Delivery Partner is appointed, NSOIT must ensure:

a. All new Delivery Partners satisfy DSIT's standard **vendor onboarding processes** and DSIT Legal, DSIT Commercial and the DSIT Operational Data team are engaged.

b. **Contractual arrangements** reflect the Delivery Partner's obligations to operate within the boundaries of relevant legislation, including the UK GDPR and RIPA, and that they must provide this assurance to NSOIT.

c. **On a case by basis, clear methodologies** are agreed to ensure there is clarity as to how the Delivery Partner will carry out the activity, in particular regarding:

(i) The **data sources** it uses;

(ii) How it **conducts** the monitoring – i.e. the search terms it uses;

(iii) The scope of its **instructions** – i.e. the instructions given to it by NSOIT regarding the subject matter or purpose of the task;

(iv) How it **minimises** the collection of personal data, as described in Schedule 2 Part A below.

d) **Ongoing assurance** is carried out to periodically review and ensure Delivery Partners continue to meet these requirements.

Data collection assessment

3.7 Before commencing any new Collection Activity, NSOIT must ensure that it has considered the potential risks to operations, staff and any political sensitivities or reputational risks for the organisation, the checklist at Schedule 3 details where to record these. Activities should not risk the security of staff, NSOIT or DSIT, [redacted]

3.8 NSOIT must assess and be satisfied that all monitoring and analysis conducted by it or on its behalf:

a) meets the permitted purposes set out above;

b) is necessary and proportionate in line with applicable data protection laws; and

c) does not amount to Directed Surveillance.

The checklist provided in Schedule 3 will assist with this assessment.

Ongoing assurance

3.9 NSOIT must periodically review each ongoing Collection Activity to ensure it continues to meet the relevant policy objectives and is in line with the legal, regulatory and operational requirements of this Policy. [redacted]

Storage and Use of Data

3.10 The output provided by Delivery Partners (**"Monitoring Reports"**) must be saved in NSOIT's Teams folder [redacted] Access is only granted where relevant and necessary, and access permissions must be regularly reviewed and updated.

3.11 Analysts may review Monitoring Reports to perform aggregated analysis and draft internal HMG reports regarding mis/disinformation threats. Such reporting must only be shared with a distribution list of named HMG colleagues, who are tasked with working on counter disinformation policy or operations, on a need to know basis.

3.12 To minimise the processing of personal data, Analysts should ensure that analysis and reporting involves review of themes and narratives, rather than private individuals. Content may contain personal data of individuals (for example, social media handles, usernames, links to posts, to the extent that an individual is identified / identifiable from a particular social media post), but such personal data must be redacted wherever possible in reporting.

3.13 All OSINF Content, Monitoring Reports and any other reports produced by NSOIT must be retained in line with DSIT's Data Protection Policy and NSOIT's local policies. **DSIT's data retention period is up to two years, at which point the team will review whether retention of the personal data is still necessary.** Where raw data samples have been collected to generate narrative analysis, including where this is provided by a third party, it will typically be held for a period of up to 3 months, in line with NSOIT's local retention policies. Any retention of data beyond the time periods set out above must be authorised by the Head of NSOIT, in agreement with the DSIT Data Protection Officer, and only if they are satisfied that such retention is necessary and proportionate for the identified purposes of processing.

Data Breaches

3.14 [redacted]

[redacted]

4. Content Escalation

Flagging Process

4.1 The NSOIT's Ops and Analysis teams, or other similar teams across HMG, may identify content that it considers harmful – in line with its ministerially agreed remit – and which may breach platform terms of service.

4.2 It is NSOIT's responsibility to review the relevant content in accordance with agreed thresholds, [redacted] and escalate appropriately as follows:

[redacted]

b) NSOIT does not flag content originating from sensitive persons or organisations e.g. journalists, political parties Parliamentarians or elected officials.

c) Where content is authorised to be escalated as described above, NSOIT will share content with the social media providers to take appropriate action, at their discretion. In making such notifications, NSOIT must strictly limit the amount of information sent to social media providers, to be no more than is necessary for them to investigate the content.

Escalation

4.3 All content reviews should be [redacted] access permissions must be regularly reviewed and updated.

4.4 NSOIT analysts must take steps to minimise the collection of personal data when assessing if content needs to be shared with platforms. In particular:

A) Links

Links are essential to the assessment of content that is escalated to NSOIT for consideration, as well as for the analysis of content that has previously been flagged to social media companies. However, they represent a form of personal data as they can be used to identify the person that shared the content. As such, they should only be retained for as long as justifiable. An initial data retention period of a maximum of two years has been agreed, at which point the team will review whether continued retention of the personal data is still necessary. Analysis must be completed prior to expiry of the two year period.

It is the responsibility of each thematic lead to ensure links are removed from their respective escalations trackers on expiry of the retention period. This is outlined in the guidance section of each tracker, and leads must set diary reminders for 3 months prior to content reaching expiry or include these instructions in handover notes.

Thematic leads must record that this has been addressed once an operational response has been stood down in any summary notes.

B) Use of names

NSOIT should keep the use and recording of names to a minimum. Public figures should be referred to by name only when absolutely necessary. Any references to public figures should not include opinions. Members of the public should not be referred to by name/username.

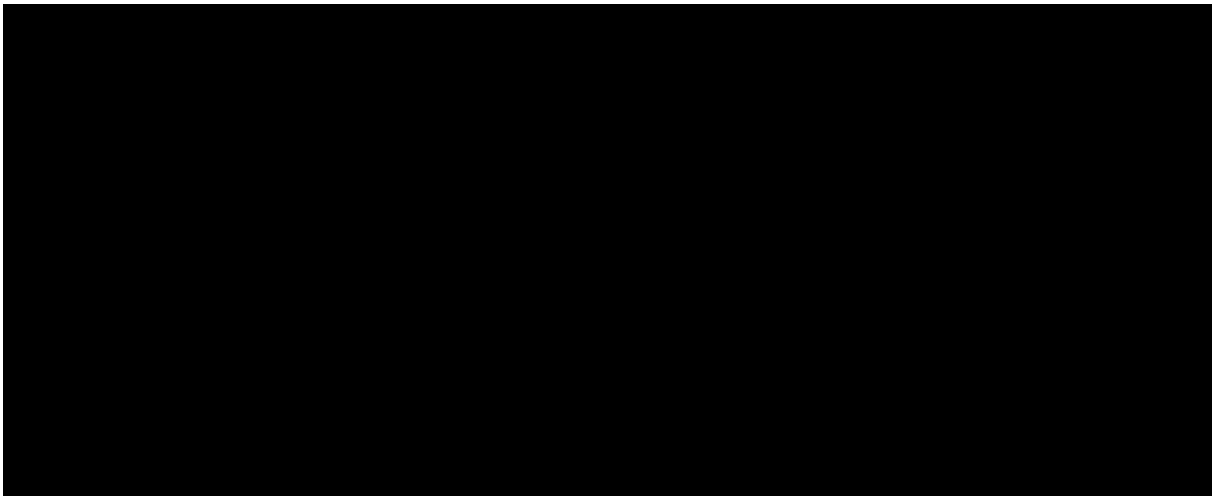
Analysts should be aware that freedom of information (FOIs) requests and subject access requests (SARs) could be made by members of the public to establish what personal information NSOIT holds and this would include any personal data collected as part of Content Escalation.

C) Content descriptions

It is possible that content wording could be used to identify an individual (e.g. through the inclusion of personal data such as usernames or political opinions), and therefore it should not be recorded in the assessment. Personal data (particularly names/usernames) should not be referenced. Instead, NSOIT should describe the content (claim made, descriptions of any photos/videos/links included). See below for an example of how this should be structured:

D) Assessment of content

To ensure that enough data is conducted for analysis, the assessment of content against social media platforms' Terms of Service should be structured based on NSOIT's thresholds and escalating principles.



SCHEDULE 1: NSOIT Monitoring & Analysis and Content Escalation Dos & Don'ts

- These Dos and Don'ts apply to NSOIT Analysts and should be communicated to Delivery Partners instructed by NSOIT / DSIT.

- **You must:**
- Before starting a new Collection Activity, [redacted]
- Ensure all Collection Activity meets an identifiable and legitimate policy objective of NSOIT or another HMG department.
- Remember to limit analysis to disinformation trends and narratives on an aggregated basis, rather than focusing specifically on actors.
- Limit the collection of personal data and redact personal data in reporting wherever possible (i.e. crop out, redact or do not include social media handles, usernames, links to posts, to the extent that an individual is identified / identifiable from a particular social media post)
- [redacted]
- **You must not:**
- Carry out any Collection Activity that risks the security of NSOIT staff, NSOIT itself or DSIT.
- Use individuals' names as search terms, nor seek to build up a picture about private individuals or groups by following their activity or instruct external delivery partners to do so;
- Analyse posts to make decisions about authors of specific posts;
- Share any content to other HMG departments without taking steps to redact personal data. Any information shared with social media providers should be strictly limited to sending links to content that may breach platforms' Terms of Service.
- Share content with social media providers posted by sensitive persons or organisations e.g. journalists, Parliamentarians, elected officials or established news outlets.
- Share any content or analysis with third parties except for in the course of your official duties and, as authorised depending on the relevant circumstances: (i) social media providers; (ii) other OGDs; or (iii) approved Delivery Partners;
- Use the tools made available to you by NSOIT for any purposes other than to carry out your official duties to understand the threat of disinformation on third party social media platforms.

SCHEDULE 2: Part A: **UK Data Protection Legislation** (UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA))

1 Introduction

1.1 Wherever personal data (including special categories of personal data) is being processed by NSOIT in the course of this work, including: monitoring of disinformation / misinformation trends and themes across social media; and reviewing content posted by individual users and storing links to these posts (some of which are provided as examples in external monitoring providers' reporting, or as part of content escalation work), this must be carried out in accordance with UK Data Protection Legislation.

1.2 UK Data Protection Legislation requires that DSIT, as Controller, complies with the data protection principles when processing personal data. This Schedule to the Policy sets out how NSOIT collects and processes personal data in accordance with such principles.

2. Data Protection Principles

Is Personal Data being processed?

2.1 HMG monitoring teams must determine whether the proposed Collection Activity amounts to the processing of personal data and consider ways in which this can be limited/excluded.

a. **"Personal data"** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. If information can be combined with other information we hold to enable identification of an individual, this would also amount to the processing of personal data.

b. Social media usernames and links to social media posts are likely to be considered personal data and social media posts themselves have the potential to contain identifiable information.

c. **"Special Category Data"** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data, data concerning health of a person's sex life or sexual orientation.

d. If there is any uncertainty as to the appropriate handling of personal data, or other compliance issues, DSIT legal advisers and/or Data Protection Officer should be consulted.

2.2 Is processing lawful, fair and transparent?

Lawful

a) In order for processing of personal data to be considered to be **lawful,** the processing must have a clear lawful basis under Article 6 of the UK GDPR and, if special categories of personal data are processed, also Article 9 of the UK GDPR.

b) It is considered that the applicable lawful basis for the processing activities covered by this Policy is:

- UK GDPR Art 6(1)(e) (processing necessary for the performance of a task in the public interest) as the lawful processing activity, on the grounds that any processing is *"necessary for the exercise of [its] function [as] a government department.*"

- (in the case of special categories of personal data) UK GDPR Art 9(2)(g) (processing necessary for reasons of substantial public interest), on the further grounds that the processing is *"necessary for the exercise of a function of the Crown, a Minister of the Crown, or a government department*".

c) To be able to rely on these lawful grounds, there must be a **clear basis in law** and the processing must be **necessary**. DSIT has overall lead within HMG for counter-disinformation policy and coordinating delivery of HMG's disinformation strategy. The monitoring of disinformation / misinformation trends and themes across social media is an integral and essential part of DSIT's mandate as lead on this policy area. Without having an in-depth understanding of the issues faced, it would not be possible for DSIT to carry out the functions with which it is specifically charged for the delivery of, such as setting the direction, focus and principles of domestic policy and leading our engagement with social media companies and the media. It is therefore considered that the activities are "*necessary for the exercise of a function of a government department*" within the meaning of DPA 2018.

Necessity & Proportionality

d) In reliance on these lawful bases, it must be demonstrated that the processing is necessary and proportionate – i.e. the processing is unlikely to be justified if there is another reasonable and less intrusive way to achieve the same result. A Data Protection Impact Assessment has been carried out to consider the impact of the team's activities overall on the processing of personal data. It is kept under regular review.

e) It is critical that NSOIT analysts are satisfied that each use case involving processing of personal data is both necessary and proportionate – *i.e.* ensuring that the activities undertaken are at all times strictly limited to tasks that are an integral and essential part of the analyst's policy work. The Data Collection Checklist in Schedule 4 will help make this assessment.

Fairness and Transparency

f) The principle of **fairness and transparency** requires that personal data should not be processed in a way that is unexpected, misleading or that has an unjustifiable adverse effect on data subjects.

g) Regarding **transparency**, where collection of OSINF Content amounts to the processing of personal data, the individual concerned must be provided with a "privacy information" notice, consistent with the requirements of articles 13 and 14 of UK GDPR (unless an exception applies). This should include information about why we are processing their data (i.e. for what legal purposes), whether it will be shared with others, how it is stored; for how long and how data subjects can exercise their rights in relation to the personal data.

h) In relation to Monitoring & Analytics and Content Escalation activities, DSIT has not obtained personal data directly from the data subject, and Article 14 UK GDPR recognises that it may not be feasible for the controller to issue a privacy notice to the data subject directly at the point of data collection. Instead, the controller must issue transparency information within a reasonable period and no later than one month from obtaining the data.

i) Accordingly, DSIT will soon publish an updated Privacy Notice for NSOIT's activities described in this Policy, which will be available on the public-facing gov.uk website. Analysts should ensure that all new and existing use cases fall within the reasonable expectations of data subjects, as described in the Privacy Notice.

2.3 Purpose Limitation

a) It is a key data privacy principle that personal data is collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Accordingly, analysts must ensure that any personal data collected for Monitoring & Analysis, operational response and platform engagement (specifically Content Escalation) purposes may not be used for any additional purposes, save to the extent that information collected for Monitoring & Analysis may be flagged to the Content Escalation team where appropriate.

2.4 Data Minimisation

a) Steps are taken to limit the collection, storage, processing and sharing of personal information as follows:

(i) Monitoring and Analysis:

A) Where content examples are shared with internal stakeholders in internal HMG reporting, analysts are responsible for ensuring any personal data is redacted.

B) External partners are instructed to minimise collection of personal data wherever possible and NSOIT must instruct them to base their searches on themes / narratives and not private individuals*;*

(ii) Content escalation:

A) Specific guidelines are in place in relation to the assessment and escalation of any content, which limit the collection of personal data as described in Section 4 above.

B) The processing of special categories of data is a likely by-product of collection of OSINF Content, for example, the nature of some disinformation themes could result in collection of, for example, political opinions. Whilst the assessment and escalation process is limited, it is possible, for example, that there will be some instances where a social media user will reference a special category of personal data in a post that is later assessed by the NSOIT for breaching platform terms of service relating to mis/disinformation. Analysts must take care to ensure that special categories of data are not disseminated further and access is strictly kept to a minimum.

2.5 Storage Limitation / Retention

[redacted]UK GDPR requires that personal data must not be stored for longer than necessary for the purposes for which it was collected. Where raw data samples have been collected to generate narrative analysis, including where this is provided by a third party, it will typically be held for a period of up to 3 months, in line with NSOIT's local retention policies. Any retention of data beyond the time periods set out above must be authorised by the Head of NSOIT, in agreement with the DSIT Data Protection Officer, and only if they are satisfied that such retention is necessary and proportionate for the identified purposes of processing. [redacted]

B) All information collected as part of these activities is recorded [redacted] in line with the DSIT's Data Protection Policy and the DSIT's Records Retention Policy.

[redacted]

2.6 Security / Integrity & Confidentiality

a) Access to stored data will be strictly limited to the monitoring team involved in the tasking and will only be made available to other HMG officials, where there is a compelling business case and such access is necessary for the performance of their functions.

B) Delivery Partners – must confirm personal data is encrypted both at rest and on transmission and data access is restricted only to key personnel working on specific projects.

2.7 Accountability

This Schedule 2, the DSIT Data Protection Impact Assessment and the Data Collection Checklist at Schedule 3 are designed to both ensure and demonstrate that the relevant data protection principles have been taken into account for relevant processing.

PART B: **Surveillance Laws:** Regulation of Investigatory Powers Act 2000 (RIPA)

1. Overview

1.1 Directed Surveillance is covert surveillance that is conducted as part of a specific investigation or specific operation in relation to an individual or group and is carried out in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation), and is otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought.

1.2 NSOIT does not conduct Directed Surveillance, or intentionally collect personal data for the purpose of storing or analysing information about private individuals.

1.3 Monitoring to gain an overall understanding of the disinformation threat landscape should not constitute Directed Surveillance, consistent with Home Office CHIS Code of Practice. However, analysts should take care to avoid analysis that may be used to support investigative activity or directed surveillance of private groups or associated individuals. Whether an activity constitutes Directed Surveillance will depend upon the nature and extent of the particular activity, and every Collection Activity should be considered on a case by case basis.

1.4 [redacted] Whilst it is acceptable to access publicly available sites in accordance with their different entry requirements, (such as Telegram which requires account login), analysts should never create fake personas for the purposes of NSOIT work.

1.5 DSIT does not hold a RIPA authorisation for carrying out Directed Surveillance, and so for each collection activity NSOIT must consider whether the collection activity could amount to Directed Surveillance. The checklist at Schedule 4 can help to record this.

1.6 If NSOIT or the Monitoring and Analysis team determines there is a risk that the Collection Activity will amount to Directed Surveillance, the Collection Activity shall not be authorised. If there is any uncertainty as to whether the Collection Activity would amount to Directed Surveillance, DSIT legal advisers should be consulted.

SCHEDULE 3: Data Collection Checklist

[redacted]

[redacted]

[redacted]