Heddlu Police
DYFED-POWYS

FOI Reference: 763/2020

Request:

I am currently researching what software solutions are used to manage covert investigations in Dyfed Powys Police and would be most grateful if you would provide me, under the Freedom of Information Act, details in respect to the contract below.

The details I require are:

1) What, if any, software is used for managing authorities for the acquisition of communications data under IPA 2016.

2) What, if any, software is used for managing authorities for use and conduct of informers 'CHIS' under RIPA 2000.

3) What, if any, software is used for managing authorities relating to directed and intrusive surveillance under RIPA 2000.

4) What, if any, software is used for managing Targeted equipment Interference authorities under IPA 2016.

5) In relation to the software used, what was the start date, duration and value of the contract ? please indicate a total and per category - communications data acquisition system - Informers 'CHIS' system and Surveillance system.

6) Is there an extension clause in the contract and, if so, the duration of the extension?

7) Has a decision been made yet on whether the contract is are being either extended or renewed?

8) Who is the senior person/s (outside of procurement) responsible for managing all covert data acquisition and covert policing investigation authorities ?

Response 1 – 7:

I can confirm that Dyfed-Powys Police does hold the information requested, however we are withholding the information by virtue of the following exemptions (please see the end of the document for an explanation of the applied exemptions).

- Section 24(1) – National Security
- Section 31(1)(a)(b) – Law Enforcement

Response 8:

I can confirm that Dyfed-Powys Police does hold the information requested, however we are withholding the information by virtue of the following exemptions (please see the end of the document for an explanation of the applied exemptions).

- Section 31(1)(a)(b) – Law Enforcement
- Section 40(2) – Personal Information

Explanation of the applied exemptions:

Section 1 of the Freedom of Information Act 2000 places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1) (a) is to confirm or deny whether the information specified in a request is held. The second duty at Section 1(1) (b) is to disclose information that has been confirmed as being held.

Where exemptions are relied upon section 17 of FOIA requires that we provide the applicant with a notice which:
a) States that fact
b) Specifies the exemption(s) in question and
c) State (if that would not otherwise be apparent) why the exemption applies

Section 24(1) - National Security
Section 31(1)(a)(b) - Law Enforcement
Section 40(2) - Personal Information

Section 24 and 31 are prejudice based qualified exemptions and as such there is a requirement to provide details of the harm as well as the public interest test. Section 40(2) is a class-based absolute exemption. This means that the legislators when writing the legislation considered that the release of such information under the Freedom of Information Act 2000 would cause harm to the public authority or individual concerned. There is therefore no requirement to carry out a HARM Test in respect of such information. There is also no requirement to carry out a Public Interest Test.

Overall Harm:

Modern day policing is intelligence led and law enforcement depends upon the development of intelligence and the gathering and security of evidence in order to disrupt criminal behaviour and bring offenders to justice. In this case the information relates to software which is used to store data about ongoing and live investigations, some of which potentially include covert activity. Revealing details of specific software will not only be revealing information which would undermine the process of preventing or detecting crime and the apprehension of prosecution of offenders but would also provide opportunities for criminals to carry out cyberattacks which would not only allow them to infiltrate policing systems thus accessing highly sensitive data, but also disrupt policing systems to such an extent as to render key law enforcement applications or even computer devices obsolete.

To provide information about these applications would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

Public Interest Considerations

Section 24(1) National Security

Factors favouring disclosure:

Disclosure would lead to a better informed public and the public are entitled to know how public funds are spent. The information simply relates to national security and disclosure would not actually harm it.

Factors favouring non-disclosure:

Operational systems and security measures are put in place to protect the community we serve. As evidenced within the harm disclosure of any such information in respect of investigative activity which may or may not be linked to terrorism would highlight to terrorists and individuals intent on carrying out criminal activity, vulnerabilities within Dyfed Powys Police force area.

Taking into account the current security climate within the United Kingdom, no information which may aid a terrorist should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that it will have an impact on a force's ability to monitor terrorist activity.

The cumulative effect of terrorists gathering information from various sources would be even more impactive when linked to other information gathered from various sources about terrorism. The more information disclosed over time will give a more detailed account of the infrastructure of not only a force area, but also the country as a whole.

Any incident that results from such a disclosure would, by default, affect National Security.

Section 31(1)(a)(b) Law Enforcement

Factors favouring disclosure:

Disclosing information relevant to this request would lead to a better informed public which may encourage individuals to provide intelligence in order to reduce the risk of police networks being hacked.

Factors favouring non-disclosure

Disclosing information in this case would suggest Dyfed Powys Police take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately.

Balancing Test

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive and relating to high profile as well as covert investigative activity. Weakening the mechanisms used to monitor any type of criminal activity, and specifically terrorist activity would place the security of the country at an increased level of danger. Therefore, in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

Section 40(2) Personal Information:

Section 40(2) applies to third party personal data and is exempt from disclosure under the Freedom of Information Act 2000 if disclosure, in relation to data subject to law enforcement processing, would breach any of the data protection principles contained within Part 3 -

Chapter 2 of the Data Protection Act 2018. Under Section 34 within Chapter 2 "The Controller in relation to personal data is responsible for and must be able to demonstrate, compliance with" Chapter 2. Such information would not be released under the Freedom of Information Act 2000 unless there is a strong public interest. One of the main differences between the Freedom of Information Act 2000 and the Data Protection Act 2018 is that any information released under FOI is released into the public domain, not just the individual requesting the information and disclosure under the Act must be made with that in mind. As such, any release that identifies an individual through releasing their personal data, even third party personal data is exempt.

Personal data is defined under Section 3 of the Data Protection Act 2018 as:

"(2) 'Personal data' means any information relating to an identified or identifiable living individual (subject to subsection (14)(c)).
(3) 'Identifiable living individual' means a living individual who can be identified, directly or indirectly, in particular by reference to—
(a) An identifier such as a name, an identification number, location data or an online identifier, or
(b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual."

All members of the public including those employed by the force have an intrinsic right to privacy and these rights are protected by virtue of the Human Rights Act, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) and a public authority must not interfere with that right. Any release of the information subject to the exemption is likely to compromise those rights.

Data Protection Act 2018
Part 3 – Law Enforcement – Chapter 2 Principles Section 35
The first data protection principle:

"(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair."

General Data Protection Regulation
Article 5 of the GDPR – 'Principles relating to processing of personal data' provides:

"1. 'Personal data' shall be

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency);
(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest…

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Dyfed-Powys Police would not want to disclose any information that could potentially identify an individual. In this particular case, to release the name of an individual alongside the nature of the role taking into account the topic of the request i.e. covert would not only be a direct breach of Data Protection legislation but would also present law enforcement issues. Therefore as a consequence I am satisfied that Section 40(2) Personal Information exemption is applicable to the release of the information.

The Section 40 exemption is in part qualified and in part absolute, in the present case it would be absolute as to release the information would breach Data Protection legislation and therefore there is no requirement to carry out a public interest test.

(This is a response under the Freedom of Information Act 2000 and disclosed on 19/01/21)