Office of Criminal Prosecutions and Litigation policy on sensitive processing for law enforcement purposes

Introduction

The Office of Criminal Prosecutions & Litigation ("OCPL") is a competent authority for the purpose of Part 3 of the Data Protection Act 2004 (DPA 2004, section 39 and Schedule 7(16)) which applies to the processing of personal data by such authorities for law enforcement purposes.

These purposes are set out at section 40 of the DPA 2004 and include 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.

Appropriate Policy Document

This policy document outlines our Sensitive Processing for law enforcement purposes and explains:

1. Our procedures for securing compliance with the law enforcement data protection principles.

2. Our policies as regards the retention and erasure of personal data, giving an indication of how long the personal data is likely to be retained.

Description of data processed

As part of our responsibilities the OCPL will carry out Sensitive Processing for law enforcement purposes in one area, namely the prosecution of criminal offences.

We may, on occasion, need to share information with law enforcement for the purposes of the prosecution of criminal offences who also have responsibilities under data protection law.

In addition, information will be provided to the Gibraltar Court Services and lawyers representing individuals who have been charged with a criminal offence. This is done so that we may proceed with our public service duty to prosecute criminal offenders and also for the greater benefit of the administration of justice.

The OCPL will no longer be responsible for processing the data that has been securely and appropriately transferred to such an organisation.

On occasions we carry out sensitive processing of some of the categories of data defined in Part 3, section 44(5).

Consent or schedule 8 conditions for processing

We carry out Sensitive Processing under section 44(3) DPA 2004 only in reliance on the consent of the data subject or where it is strictly necessary for the law enforcement purposes and it meets one of the conditions in schedule 8 of the DPA 2004.

The relevant conditions in schedule 8 of the DPA 2004 are as follows:

1. Statutory purposes
2. The Administration of Justice
3. Personal data already in the public domain
4. Legal claims
5. Judicial acts
6. Preventing fraud
7. Archiving

Processed lawfully and fairly (lawfulness and fairness)

The principles set out in Part 3 of the DPA require personal data to be:

1. Processed lawfully and fairly.

2. Collected for specified, explicit and legitimate law enforcement purposes, and not further processed in a way which is incompatible with those purposes (purpose limitation).

3. Adequate, relevant and not excessive in relation to the purposes for which it is processed (data minimisation).

4. Accurate and where necessary kept up to date (accuracy).

5. Kept for no longer than is necessary for the purposes for which it is processed (storage limitation).

6. Processed in a way that ensures appropriate security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality).

Principle one: Lawfulness and Fairness

Processing for law enforcement must be lawful and fair. Sensitive Processing is only permissible if it is:

- based on the consent of the data subject - section 44(3) (a) or

- is strictly necessary for the law enforcement purpose; satisfies at least one of the conditions in Schedule 8; and there is a policy in place at the time the sensitive data is processed (this policy) - section 44(3) (b) DPA 2004.

The OCPL works to ensure the lawful processing of information is of substantial public interest. Our processing of sensitive data for law enforcement purposes satisfies the second schedule 8 condition. It is necessary for the exercise of the function conferred on the OCPL as the government department responsible for prosecuting criminal offences and is for the administration of justice. We are a competent authority and have responsibility to prosecute offences committed in Gibraltar.

In circumstances where we seek consent, we make sure:

- the consent is unambiguous
- the consent is given by an affirmative action
- the consent is recorded as the condition for processing

Principle two: Purpose

The OCPL primarily processes personal data for the purpose of prosecuting criminal offences committed in Gibraltar, which is listed at section 40 of the DPA 2004.

The OCPL is authorised by law to carry out Sensitive Processing for this purpose. The OCPL may process personal data collected for this purpose (whether by us or another controller), provided the processing is necessary and proportionate to that purpose.

The OCPL will only use data collected for a law enforcement purpose for purposes other than law enforcement where we are authorised by law to do so.

Principle Three: Data Minimisation

The OCPL collects personal data necessary for the relevant purpose and ensures it is not excessive. The information we process is necessary for and proportionate to our purpose. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Principle four: Accuracy

Where the OCPL becomes aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, OCPL will take every reasonable

step to ensure that data is erased or rectified without delay. If OCPL decides not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision.

Principle five: Storage Limitation

The OCPL will retain information processed for the purpose of law enforcement for the periods set out in our Data Retention Schedule. We have given careful consideration to the documents that we retain and the purposes that they fulfil. As such we have applied retention periods to each category of case that we process as per the Data Retention Schedule.

Principle six: Security

We have analysed the risks presented by our processing activities and implemented appropriate levels of security based on those risks. Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures.

Where applicable, our electronic systems and physical storage have appropriate access controls applied, including user credentials and audit trails. We operate on a strict need to know basis, which means that only those officers that need to access information for their work role will have such access.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

Retention and erasure policies

There may be cases where personal data collected from the prosecution is further processed in a future prosecution. The OCPL intends to hold the personal information for the periods set out in our Data Retention Schedule, to ensure that it can use that personal information lawfully and in line with the applicable data protection legislation in order to carry out its public task obligations.

The data would be stored on secure government systems. Processes will be implemented to ensure the data is purged or archived as required. All Right of Erasure requests will be processed in accordance with OCPL's statutory obligations under the Gibraltar GDPR and DPA 2004.

Review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed annually or revised more frequently if necessary.