Fair Processing Notice

Multi-Agency Public Protection Arrangements (MAPPA) is a process by which agencies manage the risk of serious violent or sexual harm presented by certain individuals to the community, as defined by Part VII of The Criminal Justice (Sex Offenders and Miscellaneous Provisions) (Bailiwick of Guernsey) Law, 2013. This includes but is not limited to the management of the Notification Requirements prescribed by the same Law.

The processing of personal data carried out for the purposes of this fair processing notice is undertaken and co-ordinated by the MAPP Unit within the Guernsey Police. The data controller of these processing activities is the Responsible Authority ('the Controller'), comprised of representatives of the Guernsey Probation Service, Guernsey Police and Guernsey Prison.

1. The Data Protection Law

The controller acknowledges its obligations as per the Data Protection (Bailiwick of Guernsey) Law, 2017 ('the DP Law') which provides a number of requirements in terms of processing activities involving personal data. The controller further acknowledges the general principles of processing as well as the rights of a data subject and more information in relation to these provisions can be found on www.gov.gg/dp.

2. The Principles of Processing

a. Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner.

The Criminal Justice (Sex Offenders and Miscellaneous Provisions) (Bailiwick of Guernsey) Law, 2013 ('the Criminal Justice Law') provides the legal framework for Notification Requirements, dictating that certain categories of offenders must provide specific personal details to the Police Service.

Part VII of the Criminal Justice Law places a legal obligation on States Departments to work together to manage the risks posed by certain individuals. This is known as Multi-Agency Public Protection Arrangements (MAPPA); the Criminal Justice Law defines this co-operation as expressly including the exchange of information. Additionally, information will also be gathered from and/or shared with non-States bodies for the purpose of the management of serious risk under the auspices of MAPPA, as allowed by the Criminal Justice Law. The personal data processed by the controller for this purpose will be sought and obtained from

bodies within authorised jurisdictions and may, on occasion, also be requested from unauthorised jurisdictions.

The personal data which will be processed by the controller for this purpose will include, but is not limited to:

- Basic personal data
    - Name, address, date of birth, telephone number and email address (and any other data required for identification purposes, and/or defined within the Criminal Justice Law)
- Special category data
    - Criminal data required to inform risk assessments, support the management of serious harm presented by an individual and/or assist in the monitoring of those individuals for the purpose of risk management (i.e. criminal offences, information relating to relevant legal proceedings)

Section 37 of the Criminal Justice Law dictates that when an individual is at risk from a data subject managed under MAPPA, that individual may be informed of the serious risk presented to them. The controller will sanction the disclosure of personal data (including details of the risk, to whom this risk is presented and the context in which the individual presents a risk, which may require the provision of special category data) if such is necessary to comply with this statutory function.

The processing of personal data carried out by the controller for this purpose is carried out in accordance with Condition 2 of Schedule 2 of the Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018, which states:

"The processing is necessary for the controller to exercise any right or power, or perform or comply with any duty, conferred or imposed on the controller by an enactment or otherwise by Law."

Regular reviews are built into the MAPPA process to ensure that processing only continues in line with the statutory purpose of the management of risk of serious harm. Should an assessment carried out for this purpose indicate that the criteria for MAPPA registration is no longer met (e.g. risk of serious harm is no longer presented), the case will be de-registered from MAPPA processing.

The controller may also share personal data with other departments if required to do so by law, or for the purpose of facilitating the statutory duty of another public authority. Where the controller is required to share personal data for this purpose, they will ensure to restrict the personal data provided to only that which is absolutely necessary for this purpose to be undertaken.

The States of Guernsey have a professional relationship with a third-party supplier, Agilisys Guernsey Ltd., who provide support to and carry out maintenance on the IT infrastructure of the organisation. In order for Agilisys to carry out the function they are contracted to provide,

there will be instances where they may have sight of the personal data which is collected and processed by the controller. Furthermore, the controller will only provide Agilisys with access to personal data where there is a legitimate and lawful purpose for this access to be given in line with Schedule 2 of the DP Law and our internal policies and directives.

Personal data may also be shared with the Scrutiny Management Committee ('SMC') and also the Internal Audit function of the States of Guernsey as may be required for the completion of their relevant functions. Furthermore, any personal data shared with SMC and Internal Audit will be limited and processed in accordance with Conditions 5 and 13(b) of Schedule 2 of the DP Law.

b. Purpose limitation

Personal data must not be collected except for a specific, explicit and legitimate purpose and, once collected, must not be further processed in a manner incompatible with the purpose for which it was collected.

The controller acknowledges its responsibility with regards to this data protection principle and maintains that it will not further process that personal data in a way which is incompatible to its original reason for processing as specified in section 2a, unless required to do so by law.

Personal data will be transferred to a risk management body in an authorised or unauthorised jurisdiction (as per the definition within the DP Law), in the event that the controller has reason to believe the data subject has moved to that jurisdiction and/or that the data subject presents a risk of serious harm to individuals within that jurisdiction. This is in order for that jurisdiction to take any legal measures necessary to manage the risks presented by the data subject within that jurisdiction.

c. Minimisation

Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

The controller maintains that it will only process the personal data which is detailed in section 2a, and will not process any further personal data that is not necessary in relation to the original reason for processing personal data, unless required to do so by law.

d. Accuracy

Personal data processed must be accurate, kept up-to-date (where applicable) and reasonable steps must be taken to ensure that personal data that is inaccurate is erased or corrected without delay.

The controller will ensure that all personal data that it holds is accurate and kept up-to-date, and any personal data that is inaccurate will be erased or corrected without delay.

e. Storage limitation

Personal data must not be kept in a form that permits identification of a data subject for any longer than is necessary for the purpose for which it is processed.

Personal data will be kept for a period of 10 years following de-registration from MAPPA, at which point it will be reviewed and disposed of if no longer required for any statutory purpose. The 10-year period is necessary given that the original purpose for processing is the management of risk of serious harm, and disposal will occur once there has been a significant period of time to indicate that such risks are no longer presented.

f. Integrity and confidentiality

Personal data must be processed in a manner that ensures its appropriate security, including protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The controller maintains to process all personal data with appropriate levels of security. Personal data is held in electronic format, with some data kept in hard copy to enable certain working procedures to occur (attendance at meetings/interviews with data subjects, for example). Personal data is destroyed in hard copy once no longer required in that format and in order to minimise the potential for unauthorized access.

In order to prevent unauthorised or unlawful processing, the controller has put in place suitable physical, electronic and managerial procedures for both electronic and hard copy data to safeguard and secure the information that is collected and processed.

g. Accountability

The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

3. Contact Details

The contact details of the controller are as follows:

MAPPA Responsible Authority
C/o MAPP Unit
Police Headquarters
Hospital Lane
St Peter Port
Guernsey
GY1 2QN

Email: mapp@guernsey.pnn.police.uk

The contact details for the Data Protection Officer of the Committee *for* Home Affairs are as follows:

Data Protection Officer
The Committee *for* Home Affairs
Sir Charles Frossard House
La Charroterie
St Peter Port
Guernsey
GY1 1FH

Tel: 01481 220012

Email: data.protection@gov.gg