Information Sharing Arrangement for Jersey

Multi Agency Safeguarding Hub (MASH)

Sharing of information between the police and agencies and departments of the States of Jersey, to assist in identifying and assessing risks to children's welfare.

Contents

Section 1.
Purpose of the Agreement

1. This agreement has been developed to:

   - Define the specific purposes for which the signatory public authorities have agreed to share information.
   - Describe the roles and structures that the MASH will use to control the exchange of information between signatories.
   - Summarise the legal controls on information sharing in this context
   - Describe the type of information that may be shared.
   - Set out how the signatories will share information about children who have come to their attention in a way that ensures compliance with the legal controls and that the information is managed in a secure way
   - Describe how this arrangement will be monitored and reviewed by the signatories from time to time

2. The signatories to this MASH agreement are:

   - The Children's Service;
   - The States of Jersey Police;
   - Family Nursing and Home Care;
   - The Department of Education Sport and Culture
   - Health and Social Services
   - Virtual partners include Probation and Housing.

Comment [redacted]: It isn't clear from the agreement what this phrase means, is it worth explaining somewhere or is it a term that you think all those involved in the agreement will understand?

Section 2.
Purpose of the MASH

3. Research and experience both in the UK and in Jersey has demonstrated the importance of information sharing across professional boundaries to ensuring that, as far as is possible, the welfare of children is safeguarded. Particularly in the UK, some serious case reviews (including in the [redacted] case) have highlighted deficiencies in relation to the sharing of information and communication as contributing to the subsequent death of a child.

4. In order to deliver the best safeguarding decisions which ensure timely, necessary and proportionate interventions, decision makers need the full picture concerning a child and their circumstances to be available to them. Information viewed alone or in silos may not give the full picture or identify the true risk. As such all the information from various agencies needs to be available and accessible in one place.

    - A Multi Agency Safeguarding Hub (MASH) helps ensure this and aids communication between all safeguarding partners[1].

    - By ensuring all partners have the ability to share information, it will help to identify those who are subject to, or likely to be subject to, harm in a timely manner, which will keep individuals safe from harm.

    - This will in turn also assist signatories to this agreement in planning or delivering their services or in making interventions, to do so in a co-ordinated way.

5. The Children's Service is leading work to establish a MASH arrangement in Jersey. A stand alone system named, 'MASH IT' has been created by the Police IT department and has been agreed by partner agencies, for sole use within the MASH.

[1] The MASH model was highlighted in the UK's Munro Report into Child Protection: http://www.education.gov.uk/childrenandyoungpeople/safeguardingchildren/protection where it was cited as an example of good practice in multi-agency partnership working because of how it improved information sharing between participating agencies.

Section 3.
Legal controls on information sharing

6. This section of the agreement summarises the legal issues arising from the sharing of personal information by the public authorities participating in the MASH and by the MASH itself. It is intended to assist signatories by helping them to understand the main legal principles applicable to the exchange of information between public bodies wishing to participate in the MASH. It is not intended as a substitute for legal advice and where there are doubts as to the propriety of sharing information in any specific case then further advice should be sought from the Law Officers' Department.

7. In Jersey, the legal framework relating to the protection of personal information is set out in:

   a. The Human Rights (Jersey) Law 2000 ("HRL 2000"), which incorporates the European Convention on Human Rights ("ECHR") into Jersey law, including the Article 8 right to a private and family life;
   b. The customary law duty of confidentiality; and
   c. The Data Protection (Jersey) Law 2005 ("the DPL 2005")

   This framework is similar to that found in the UK where MASH arrangements have already been widely introduced and is explained below.

   As public authorities, the signatories to this agreement also need to satisfy themselves that they have the authority to share data under this agreement in each case. In the UK, legal powers and functions have been placed on public authorities that authorise them to co-operate with one another for child protection purposes, including by means of data sharing. Not all of these powers appear in statute in Jersey and so it is important that public authorities are able to identify a power or function that information sharing serves and is proportionate to. Authority to share information may derive from powers

   a. explicitly to share data (i.e. an express statutory information sharing power); or

   b. to do things to which the sharing of data is necessarily ancillary (i.e. an implied power to share data).

8. In the UK, in running MASH arrangements, local authorities have tended to rely on a mixture of express and implied powers to share information. In respect of Jersey, Annex B to this memorandum contains a brief summary of the powers that have, so far, been identified as being relevant to the work

of the MASH. That Annex is not exhaustive and further powers and the signatories might identify additional powers that are relevant to the operation of the MASH.

The HRL 2000

9. The HRL 2000 incorporates the European Convention on Human Rights ("the ECHR") into Jersey's domestic law. Article 7 of the HRL 2000 requires that public authorities act compatibly with the ECHR. With regard to the disclosure of personal information for the purposes of the MASH, the right that needs to be taken most earnestly into account by public authorities is Article 8 of the ECHR. Article 8(1) ECHR recognises that everyone has the right to respect for his private and family life, his home and his correspondence. However, Article 8(2) then qualifies this right by providing that:

> *"There shall be no interference by a public authority with exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of crime or disorder, protection of health and morals or for the protection of rights and freedoms of others.*

10. Sharing personal and confidential information held about a person may interfere with a person's rights under Article 8(1). Therefore, those public authorities sharing information with the MASH and responsible for running the MASH hub itself, should satisfy themselves, in each case, that sharing personal information is a justified interference with the right to private life for the purpose of Article 8(2). Where information sharing takes place in accordance with the informed and explicit consent of the subject of the information, the risk of an unjustified interference with the right in Article 8(1) ECHR will be very low. However, it will also sometimes be necessary to share information under the MASH arrangements without consent. Where that is the case it will be important to ensure that any interference with the Article 8(1) ECHR right is "*in accordance with the law*". It must also be "*necessary in a democratic society*" and in pursuit of one of the legitimate aims set out in Article 8(2) ECHR. Where a child or young person is at risk of significant harm or sharing information is necessary to prevent crime or disorder, interference with the individual's rights may be justified under Article 8(2) ECHR, provided that the amount of information shared is proportionate to the purpose and that sharing takes place in accordance with the law.

Duty of confidence

11. In Jersey a duty of confidence will arise where a person receives information that has the necessary quality of confidence about it in circumstances that expressly or impliedly give rise to an expectation that the information will be kept confidential. Much of the information that will be shared with or held in the MASH will be subject to a duty of confidence owed to the subjects of that information.

12. Where a duty of confidence arises it will usually be unlawful to disclose the information subject to that duty to a third party. However, the existence of a duty of confidence is not an absolute bar on the disclosure. Confidential information can be lawfully disclosed where the person to whom the duty is owed has given their explicit consent. Further, even where it is not possible or appropriate to obtain consent to disclose, it may still be possible to share the information lawfully where there is either an overriding public interest in disclosure or sharing is required by a court order or other legal obligation.

The DPL 2005

13. The DPL 2005 regulates the "*processing*" of "*personal data*". Personal data is data which relates to a living person, including the expression of any opinion or indication about the intentions in respect of the individual[2]. Processing of personal data includes anything which may be done to personal data, such as obtaining, holding, using, disclosing or destroying it. Therefore, the requirements of the DPL 2005 are almost certain to apply to the sharing of information with or by the MASH[3].

14. Under the DPL 2005 a person or organisation that (either alone, or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed is a "data controller"[4] and must comply with the eight data protection principles set out in Schedule 1 to the DPL 2005. The data controller will also be responsible for handing request for access to personal data from the data subjects[5].

15. In relation to the MASH, the signatories to this agreement supplying personal data to the MASH and receiving personal data from the MASH will be data controllers in relation to that data. As the Children's Service will be solely responsible for determining the purposes and the manner in

[2] Article 1(1) of the DPL 2005
[3] The definition of "data" for the purposes of the DPL 2005 excludes some information that is held only as part of manual paper files.
[4] Article 1(1) of the DPL 2005
[5] The right afforded by Article 7 of the DPL 2005.

which personal data are processed within the MASH, the Children's Service will be the data controller for that personal data, even though the information may be processed electronically on the MASH IT system.

16. With regard to the substantive requirements of the DPL 2005, all eight of the data protection principles must usually be complied with by the data controller[6]. Annex A to this memo briefly describes the requirements of the most relevant data protection principles for these purposes[7].

Section 4.
Description of procedures

17. As outlined above, to enable the MASH to operate lawfully, the signatories should ensure that in practice data sharing takes place with lawful authority and in a manner that is compatible with the legal framework for the sharing of personal information. While the law is complicated, there are some essential practices that, if they adhered to by the signatories and those administering the MASH, will help to ensure that data sharing takes place in a lawful manner. These essential practices are:

    a. **Openness:** wherever possible those participating in the MASH arrangements should be open with the person(s) whose information they wish to share about their intention to share information with the MASH. They should explain the reasons for wanting to share information with the MASH, who the information will be shared with and how it will be used. Where possible, this information must be given in writing to the person(s) whose information will be shared either before or soon after any sharing takes place.

    b. **Consent**: explicit consent to disclosure of personal information to the MASH must be sought except where that would be contrary to the public interest, for example because it would put someone at risk of harm.

    c. **Reasoning:** information may only be shared without consent where those participating in the MASH have reason to consider, in the specific circumstances, that sharing is necessary in the public interest and for the performance of a public function. The reasons for that view should be recorded at the time wherever possible and reference should be made to the relevant statutory powers and functions of those sharing information.

[6] There are some potentially relevant exceptions from the application of these principles, but these do not need to be set out in detail for the purposes of this advice.
[7] The sixth and the eight principles would apply but are not referred to specifically in this advice.

d. **Proportionality:** the information shared with and by the MASH should not be more than is necessary for the specific purposes for which it is shared and it should only be shared with those persons who need to have it.

e. **Accuracy:** So far as practical, all those participating in the MASH and those responsible for information held by the MASH itself should ensure, so far as is practical, that the personal information shared is accurate and is stored for no longer than necessary.

f. **Security:** All personal information shared with or by the MASH and stored by the MASH must be kept securely.

18. These points are reflected in the more detailed procedures described below.

Information entering the MASH:

19. Where it has come to the police's attention that a child is in circumstances that are adversely impacting upon their welfare or safety, a Child Protection Notification ("CPN") will be placed by the reporting police officer onto the SoJP network.

20. The Police Sergeant based in the MASH will review these CPNs to see if there is a need to inform Children's Services that the child has come to police attention.

21. [The Police Sergeant based in the MASH will check] to see if there is an open case about the child on the Children's Services database. Where there is, they will forward the CPN directly to the MASH referral co-ordinator who will send it onto the responsible social worker.

22. Where there is no open case the Police Sergeant will send the CPN to the MASH Decision Maker for assessment.

23. Information from non-Police sources will be processed initially by the MASH referral co-ordinator. Similar to the Police process, they will check to see whether there is an open case and if so, forward that information onto the relevant social worker. Where there is not an open case, they will create a new case record.

Information sharing by the MASH:

24. If a MASH assessment is required, consideration will be given to which other agencies (both present and virtual) should be approached for relevant

Comment [redacted]: Who will carry out these checks is it the Sergeant

Comment [redacted]: Who is this, does this need to be specified in the agreement?

Comment [redacted]: Will a new case record be required in every case in which information is received from non-police sources?

Comment [redacted]: How will it be determined whether a MASH assessment is required - what is involved in a MASH assessment - is this the process of considering which other agencies should be involved?

information taking into account the framework for the protection of personal information and in particular the need to ensure that any information sharing is proportionate in light of the purpose it may serve. The agencies approached will then be asked to provide relevant information to the MASH, for further assessment by the MASH Decision Maker, to ensure a prompt, proportionate and appropriate response to safeguarding measures.

25. Based on an assessment of all the information gathered, the Decision Maker will then decide what the most suitable course of action will be; to include social work assessment or early intervention via universal services. Having taken account of the framework for the protection of personal information, The Decision Maker will the supply such information as is appropriate and relevant to agencies who 'need-to-know' that information when interacting with that child.

……..

26. Where appropriate, at the earliest opportunity, the Decision Maker will consult with the Police Sergeant within the MASH, to see if a crime has been committed. If so this will be recorded by the Sergeant and an investigation started. Progression of the MASH assessment should not be delayed by the time taken for the police investigation to conclude. It should be run in parallel, unless there are exceptional circumstances.

Section 5.
Security matters

27. All partners to this agreement will provide a list of contacts to deal with queries and requests for information under this agreement. The organisations will also nominate persons to act as the contact to ensure continuity in the absence of the original points of contact. Email is the preferred method of enquiry submission. All information will be recorded centrally in the MASH in accordance with arrangements to be determined by the Children's Service These arrangement will take full account of the Children's Services responsibilities as data controller under the DPL 2005. Other agencies may also keep records of information shared and agree to do so in accordance with their responsibilities as data controllers for the information process for their purposes.

28. The information to be shared under this agreement is to be treated as [confidential / restricted]. Staff working with MASH information must be vetted to [CTC / CRB level]. Staff should treat the information on a strict 'need-to know' basis. Signatories to this agreement agree to seek the permission of the originating public authority if they wish to disseminate shared information outside of the MASH arrangement for any purpose. Such permission will only be granted where proposed sharing is within the agreed principles: i.e. for policing purposes, safeguarding and supporting the wellbeing of children.

29. All signatories to this agreement accept responsibility for ensuring that all appropriate security arrangements are complied with. Information will be stored in secured premises and so that it can only be accessed with the use of a username and password. Where it must be sent or received, that should be by way of secure, appropriate and approved methods. The sharing of any information electronically must be done via secure email, meaning only email addresses [specify]. Once information contained within emails is transferred to partner's electronic systems, the emails will be deleted. Information provided as part of this agreement will be subject to periodic [specify] review by signatories and will be destroyed in accordance with each signatories usual practices for handling information in accordance with the 2005 Law.

30. Any unauthorised release of information or breach of conditions contained within this agreement will be dealt with through the internal discipline procedures of the individual partner, but may be reported to the police. Any issues concerning compliance with security measures will form part of the annual review of this agreement.

Section 6.
Other matters

31. All partners will hold a copy of this agreement. It is the responsibility of each partner to ensure that all individuals likely to come in contact with the data shared under this agreement are trained in the terms of this agreement and their own responsibilities.

32. All parties are aware that in extreme circumstances, non-compliance with the terms of this agreement may result in the agreement being suspended or terminated.

33. The arrangements set out in this document will be reviewed in one year's time

34. This document may be published or disclosed in response to a request under the Code on Access to Information or the Freedom of Information (Jersey) Law 2011, once that law comes into force.

35. However, any requests for information that relate to the operation of this agreement should, be dealt with following consultation with those who are likely to be affected by the disclosure (or non-disclosure) of the information requested.

36. As acknowledged above, the Children's Service is responsible for fulfilling the role of data controller with regard to the information processed by the MASH hub, but Partner Organisations will remain responsible for compliance with their responsibilities as data controller in relation to information that they have shared and with compliance with Article 7 of the Data Protection (Jersey) Law 2005.

Section 7.
Agreement to abide by this arrangement

37. The representatives signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between the public bodies concerned in a manner compliant with their statutory and professional responsibilities.

38. As such they undertake to:

- implement and adhere to the procedures and structures set out in this agreement;
- ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement;
- engage in a review of this agreement with partners annually.

39. We the undersigned agree that each agency/organisation that we represent will adopt and adhere to this information sharing agreement:

Agency	Post Held	Name	Signature	Date
The Children's Service				
Police				
Family Nursing and Home Care				
Health and Social Services				
Education, Sport and Culture				

Annex A

Requirements contained in the data protection principles contained in the DPL 2005

1. The first principle requires that personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless— (a) at least one of the conditions in Schedule 2 to the DPL 2005 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. The 'fairness' requirement is an objective standard that must be applied on a case by case basis taking into account the method by and purposes for which the information was obtained[8]. Part 2 of Schedule 1 to the DPL 2005 sets out in further detail what is required if processing is to be 'fair'[9]. In particular, it states that personal data are not to be regarded as being processed fairly unless the data subjects are provided with (or have ready access to) certain pieces of information, either prior to, or at the time that the processing first takes place, or very soon afterwards. This information includes the identity of the data controller or any nominated representative; the purposes for which the data are intended to be processed; and any further information that is necessary in order for the processing to be regarded as fair in the circumstances. Usually this requirement is complied with through the provision of a fair processing notice, which is drawn to the data subject's attention when they supply the personal data to the data controller. I note that the draft procedure document attached to your e-mail makes reference to the provision of a fair processing notice whenever consent is sought to the making of a MASH enquiry.

3. The 'lawfulness' requirement means that all relevant legal obligations, both statutory and under customary law, must be complied with (as to which see the rest of this note). In particular, the DPL 2005 cannot render lawful any processing which would otherwise be unlawful. This means, in particular, that any public authority supplying information to the MASH and the data controller for the MASH hub must have power to carry out the processing and ensure that the processing does not amount to an unjustified breach of an ECHR right or unlawful breach of a duty of confidence.

4. The first principle also requires that as a requisite of fair and lawful processing, personal data shall not be processed unless at least one of the conditions in Schedule 2 to the DPL 2005 is met and, in the case of processing

[8] So, for example, if a public authority obtains personal data in a statistical survey, but then, without informing the subject of the information sells it for the purpose of direct marketing that is unlikely to be fair.
[9] Paragraphs 1 and 2 of Part 2 of Schedule 1 to the DPL 2005.

Comment [redacted] All reference to the actual procedures to be applied when in contact with service users and seeking consent to disclosure isn't found in this agreement now. This will need to come out unless further information is added above.

sensitive personal data at least one of the conditions in Schedule 3 to the DPL 2005 is also met. The Schedule 2 conditions include, inter alia:

a. the data subject has given consent to the data processing;

b. the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;

c. the processing is necessary to protect the data subject's vital interests;

d. the processing is necessary for the administration of justice, for the exercise of any functions conferred on any person by or under any enactment, for the exercise of any functions of the Crown, the States or any public authority, for the exercise of any other public functions exercised in the public interest by any person; or

e. the processing is necessary for the purposes of legitimate interests of the data controller, or of the third party or parties to whom the data is disclosed, except where the processing is unwarranted by reason of the rights and freedoms or interests of the data subject.

5. The Schedule 3 conditions, inter alia, include:

a. the data subject has given explicit consent to the processing;

b. the processing is necessary to protect the vital interests of the data subject or someone else, in a case where the data subject cannot give consent or consent cannot reasonably be obtained, or, in order to protect another person's vital interests, the data subject is unreasonably withholding consent;

c. the information has been made public as a result of steps taken by the data subject;

d. the processing is necessary for the purposes of, or in connection with any legal proceedings, obtaining legal advice or to establish, exercise or defend legal rights;

e. the processing is necessary for the administration of justice, for the exercise of any functions conferred on any person by or under any enactment, or for the exercise of any functions of the Crown, the States, any administration of the States or any public authority; or

f. the processing is necessary for medical purposes and is undertaken by a health professional.

6. The second data protection principle is that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed further in any manner incompatible with that purpose or those purposes. Simply processing information for a different purpose from that for which it was originally collected will not necessarily infringe this principle. Processing will only breach this principle where the purposes for which the data were obtained and are subsequently processed are *incompatible*. Where information is obtained for a purpose related to promoting the welfare of a child or young person then processing that information for another purpose also related to their welfare is unlikely to infringe this principle.

7. The third principle is that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed. The fourth principle is that personal data shall be accurate and, where necessary, kept up to date. Compliance with these principles will be judged taking into account the purposes for which the data was obtained and whether the data controller has taken reasonable steps manage their data responsibly. In relation to the MASH, the data controller will need to consider what the appropriate method of managing information will be to ensure that, so far as is reasonable, only relevant and accurate information are processed by the MASH.

8. The fifth principle is that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. There are no actual timescales imposed so the data controller for the MASH will need to consider, taking into account the nature and purpose of the records kept by the MASH, what the retention period should be.

9. The seventh principle is that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Again the data controller for the MASH will be responsible for ensuring that appropriate training is given to those participating in the MASH and that suitable security precautions are taken to ensure the data is properly protected against loss or theft. It is essential that such measures are as robust as possible to avoid the regulatory and reputational risks that might arise from a loss or theft of information.

Annex B

Brief summary of express and implied powers to share data that are relevant for the purpose of operating a MASH in Jersey

The Children (Jersey) Law 2002

1. An express power to share information arises from Article 42 of the 2002 Law, which creates an obligation for the Minister to make enquires where he or she is informed that a child is the subject of an emergency protection order or is in police protection, or where the Minister has reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm. In such circumstances the Minister is required to make or cause to be made, such enquiries as the Minister considers necessary to enable the Minister to decide whether he or she should take any action to safeguard or promote the child's welfare. Where the Minister is conducting enquiries under this Article, it is the duty of any administration of the States to assist the Minister with his or her enquiries (in particular by providing relevant information and advice) if called upon by the Minister to do so, unless it would be unreasonable to do so in all the circumstances of the case.

2. Implied powers for the Minister (and their officials) to share information may arise from several functions under this Law, particularly those functions in Part 3, which contain provisions concerning Ministerial support for children and families. For example, Article 17 of the Law contains obligations for the Minister to provide accommodation to any child in need who appears to the Minister to require accommodation. Article 24 of the Law makes provision for the Minister to apply for a care order or supervision order where he or she is satisfied of certain matters. I expect that it can properly be said that information sharing is necessary in order for the Minister to fulfill these duties and functions.

3. Express and Implied powers for the police to share information arise from Article 41 of this law which empower a police officer, who has reasonable cause to believe that a child would otherwise be likely to suffer significant harm, to take the child into police protection.

The Adoption (Jersey) Law 1961

4. Powers to share information for the purposes of the MASH potentially arise under the 1961 Law. For example, at a general level, Article 3 places a duty on the Court and the Minister when making adoption decisions to have regard

to all the circumstances, first consideration being given to the need to safeguard and promote the welfare of the infant throughout the infant's childhood. Some information sharing by and with the Minister or their officials might be expected if that duty is to be fulfilled.

The Education (Jersey) Law 1999

5. Article 14 makes provision for the Minister to apply for an education supervision order, in specified circumstances, placing a child under the supervision of an officer in an administration of the States. Under Schedule 3 of that Law, where a supervision order is in force, the supervisor may give directions to the child and the parents of the child and, where any directions he gives to the child or parent are not complied with, the supervisor may consider what further steps to take. It might be implied from these powers that the Minister and the supervisor have the power to collect and share personal information to fulfil these responsibilities.

Police Force (Jersey) Law 1974

6. The police have many express and implied powers to share information. In general though, Article 2 of the 1974 Law places a general duty on a police officer to the best of his or her power to cause the peace to be kept, prevent all offences and to take all such lawful measures as may be necessary for the purposes of bringing offenders with all due speed to justice. Again, some proportionate information sharing will necessarily be ancillary to the performance of this duty.

Mental Health (Jersey) Law 1969

7. At a general level, Article 3 of the 1969 Law gives the Minister the power to make arrangements for the purpose of the care of persons suffering from mental disorder or addiction or for the after-care of persons who have been so suffering, and for persons requiring special care. A power to share information where necessary for the purposes of fulfilling this function can be implied.

Sex Offenders (Jersey) Law 2010

8. Among other things, Article 28 of the 2010 Law requires that arrangements be put in place between Ministers and the police for the assessment and management of persons who pose a risk of sexual harm. Article 28(8) of the 2010 Law makes it clear that the co-operation that is required to fulfill these arrangements may in practice include the exchange of information.

The States of Jersey Law 2005

9. Article 26 of the 2005 Law provides that each Minister shall be a corporation sole with the power to enter into agreements, acquire, hold and dispose of movable property, do any other thing which the Minister can do by virtue of his or her office, and do anything "*reasonably necessary or expedient for or incidental to*" any of those matters. The power to do anything necessary, expedient or incidental to any other thing the Minister can do in my view ensures that where the sharing of personal information is necessary to fulfill an identifiable statutory function there will be a power to do so. Further, by virtue of Article 28 the Minister can delegate powers conferred upon or vested in them by or under the 2005 Law or any other enactment to an officer, subject to some restrictions. This could include powers to do things that are necessary, expedient or incidental to the Ministers other functions such as sharing personal information.