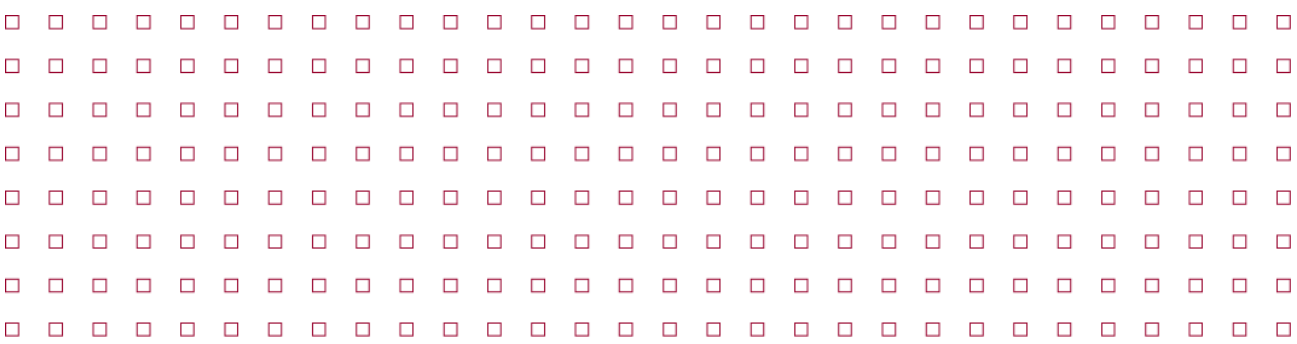
Ministry of Justice

Commissioning of a service provider to operate a national Homicide Service from 1 October 2014

Privacy Impact Assessment Report

January 2015



Ministry of Justice

Commissioning of a service provider to operate a national Homicide service from 1 October 2014

Privacy Impact Assessment Report

This information is also available on the GOV.UK website

Contents

.

Section 1 – Executive Summary

Background

The Ministry of Justice (MoJ) has undertaken a competitive process to award a grant for the provision of support services to those bereaved by homicide. This was to ensure that services would continue without any break following the end of the previous grant agreement with Victim Support (VS) on 30 September 2014. As identified in the screening process, a Small Scale Privacy Impact Assessment (PIA) was required for the Policy. This report is the PIA for the Policy.

Findings

There is little risk of an adverse privacy impact of the policy if the outcome of the competed grant award process is that the current supplier is successful in bidding for the future service. Even in this scenario work to improve the current data processes – which already meet legislative requirements – will nonetheless be helpful. Should a new provider be installed then there is greater risk – particularly when transitioning clients between providers – and work would have to be undertaken to ensure that processes were sufficiently secure. *Note: the report's details are based on the incumbent (VS) continuing as service provider as Ministers agreed that the new service should be operated by the incumbent.*

Recommendation

Requirement in grant agreement for new service provider to work with MoJ to mitigate any data protection issues.

Review Process

The data transfer processes and arrangements between the current service provider and police forces and the Foreign & Commonwealth Office (FCO) were mapped and these have informed the descriptive document for the new service. The grant agreement for the new service will also make it clear that compliance with data security requirements is essential.

Section 2 – Introduction

Background

A Privacy Impact Assessment (PIA) is a process that helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions. The primary purpose of a PIA is to visibly demonstrate that an organisation acts responsibly in relation to privacy. The deliverables and benefits of undertaking a PIA can be summarised as follows:

- The identification and management of risk;
- Avoidance of unnecessary costs;
- Prevention of inadequate solutions;
- Avoiding loss of trust and reputation;
- Informing citizens and partners of the organisation's communications strategy;
- Meeting and exceeding legal requirements.

Objective

The objective of conducting this PIA is to identify any data protection issues with the proposed commissioning of a national Homicide Service. It is important to remember that ultimately the focus of a PIA is compliance with the Data Protection Act (DPA).However, compliance with any other relevant legislation should also be considered.

Underlying principle

Data sharing and testing must be undertaken within a clear legal framework with any intrusion upon an individuals' privacy to be kept to a minimum. By undertaking a PIA we help to ensure this principle is met.

HMG requirement

The Data Handling Review, published in June 2008, states that all Departments will "introduce Privacy Impact Assessments, which ensure that privacy issues are factored into plans from the start, and those planning services are clear about their aims. Similarly, information risk management will be considered as part of the Government's "Gateway" reviews that monitor progress of the most important projects". The Data Handling Review has now been subsumed into HMG Information Assurance Standard No 6 – Protecting Personal Information and Managing Information Risk. Accordingly, PIAs are to be carried out on MoJ projects and policies that involve the processing of personal data.

PIA Process

The process for conducting a PIA is described by the ICO as follows:

1. Initial assessment (i.e. the Screening Process) – Examines the project at an early stage, makes an initial assessment of privacy risk and decides which level of assessment[1] is necessary. This has been undertaken and the subsequent report is referenced in this report.

2. Where necessary, conduct, either:

- Full-scale PIA – a more in-depth internal assessment of privacy risks and liabilities. It includes the need to identify stakeholders, analyse privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them; or
- Small-scale PIA – Similar to a full-scale PIA, but is less formalised. Requires less exhaustive information gathering and analysis. More likely to be used when focusing on specific aspects of a project.
- Review – Sets out a timetable for reviewing actions taken as the result of a PIA and examines their effectiveness. Looks at new aspects of the project and assesses whether they should result in an updated PIA.

This report deals with the PIA for the commissioning of a service provider to operate a national Homicide Service from 1 October 2014.

[1] Full Scale PIA, Small Scale PIA or no PIA.

Section 3 – Commissioning of a service provider to operate a national Homicide Service from 1 October 2014 – details

Commissioning of a service provider to operate a national Homicide Service from 1 October 2014 – Overview

1.	*[Project Name?]* The commissioning of a service provider to operate a national Homicide Service from 1 October 2014.
2.	*[What is the Project/Policy/Initiative?]* A competitive process to award a grant for the provision of support services to those bereaved by homicide post-2010. The MoJ will not have any control of the operator's data.
3.	*[What is the main function/purpose of the Project/Policy/Initiative?]* To ensure that services to those bereaved by homicide post 2010 continue without any break following the end of the previous grant agreement with Victim Support on 30 September 2014.
4.	*[Has a Screening Process been completed, provide a summary of the findings. Include: date of report, whether full scale or small scale PIA recommended?]* Screening process completed. Report dated 16 April 2014; small scale PIA recommended. Little change to current data management approach, but ongoing collection of data from new victims of homicide. Information to be made available to specialist support organisations.
5.	*[Has a PIA that related to this proposal already been conducted? If yes, please provide details e.g. date, whether full scale or small scale.]* No.
6.	*[Briefly, what are the main data that is to be processed as part of the Project/Policy/Initiative?]* Personal information relating to families bereaved through homicide. This may includes, addresses, nature of the homicide, victim details, bank, employment, health and other similar personal details.

System users

7.	*[Which user group(s) will have access to the data?]* Operator of the national Homicide Service. Any sub-contracted organisations as contracted by the service provider (with any necessary data agreements in place) providing specialist support to victims. Police and Foreign & Commonwealth Office. Potentially participating agencies in Multi Agency Risk Assessment Conferences (MARACs) where related to domestic violence homicide victims (appropriate information sharing protocols will be in place).
8.	*[Will contractors/service providers to MoJ have access to the data?]* Yes, as above.
9.	*[Is any remote support/maintenance by a 3rd party proposed? How will this access by 3rd parties be limited/managed/logged and audited?]* Yes, Claritas. Claritas***** is a police preferred supplier and all staff are SC cleared. ***** The company Claritas Solutions provides independent IT services and solutions across all industry sectors, specialising in ensuring clients avoid risks associated with using multiple vendors.

Business case

10.	*[What data is to be collected?]* Sensitive personal and support needs of the bereaved. These may include name, address, age, gender, financial, bank and employment details and other details as may be deemed necessary in order to enable the caseworker with the Homicide Service to conduct a needs assessment of the bereaved and therefore to supply the necessary support; also to monitor the progress of the support and adjust as appropriate. The statistical records will enable the Homicide Service operator to demonstrate to the MoJ that it is providing the service for which grant has been given and to demonstrate value for money in their use of public monies. This is important so that MoJ can monitor the grant agreement and respond to enquires about use of the grant from Ministers and Parliament.
11.	*[Briefly, what are the Personal Data elements used by the system/project? e.g. Surname, Forenames, Gender, Defendant number, DOB, Bail/Custody Status, Hearing/Trial/Conviction/Sentence Dates, Charges (inc addresses committed at), Sentence details, etc.]* See answer to Question 10.
12.	*[Please detail the data subjects from whom the Data is being collected?]* Families bereaved by homicide.

13.	*[How will the data collected from individuals or derived from the system be checked for accuracy?]* Homicide Service caseworkers will liaise with families, police and Foreign & Commonwealth Office (FCO). The Homicide Service will maintain internal checks to ensure accurate recording of all data. Personal and sensitive personal data will be provided to the Homicide Service by the police and the FCO with the consent of the data subject.
14.	*[Why is the Data being collected?]* To enable the Homicide Service to assess and record the support needs of bereaved individuals and to monitor the ongoing support identified.
15.	*[Will the project analyse the data to assist users in identifying previously unknown areas of note, concern, or pattern?]* No.
16.	*[How will the data collected from individuals or derived from the system be checked for accuracy?]* The Homicide Service will maintain internal checks to ensure accurate recording of all data. Data security managed via a Security Working Group which includes a CLAS (CESG***** Listed Advisors Scheme) consultant. Data management complies with appropriate System Security accredited by the Senior Police Systems Accreditor. ***** UK government's National Technical Authority for Information Assurance
17.	*[How is the Data collected?]* By Police Family Liaison Officers (FLOs), Homicide Service workers and FCO officials (can be face-to-face, telephone call or questionnaire.
18.	*[How is the data stored?]* On a case management system that is risk-assessed at appropriate Govt IS and IL level controls. Located in Police data centre, which complies with these standards and is accredited accordingly.
19.	*[Describe all the uses for the Personal Data (including for test purposes).]* To maintain records for use by homicide service caseworkers and sub-contracted organisations to support bereaved families; to enable statistical analysis, thereby enabling MoJ to monitor the effectiveness of the use of the award of grant in terms of numbers helped and satisfaction with the assistance supplied.
20.	*[How is the data going to be transferred?]* Via secure email system (accredited by CESG). Egress is a commercially available Data processing agreement in place between the service provider and with the Association of Chief Police Officers (ACPO). Data will be password protected.

21.	*[What quantity of data will be collected and stored (aggregated?), will the project store or transmit more that 250 Personal Data records?]* Likely to be data on over 1,000 individuals per annum.
22.	*[Will Sensitive Personal Data be processed, stored or transferred during this project? Sensitive Personal Data is Personal Data that consists of racial or ethnic origin, political opinions, religious beliefs, etc.]* Yes.
23.	*[What specific legal authorities/arrangements/ agreements define the collection of data?]* All relevant data protection legislation. Data is only shared with the consent of the data subject. Data sharing agreements or data processing agreements between provider and all relevant organisations.***** The Act allows for personal/sensitive personal data to be transferred with the informed consent of the data subject. Supporting this is the Victims' Code of Practice which requires the police to refer (with consent) the data to a victims' services agency. The incumbent (which is also the new service provider) has a data sharing agreement with ACPO. ***** A data sharing agreement is an agreement which allows an agency to share data with another agency with consent of the data subject or legal gateway. The receiving agency becomes the data controller. A data processing agreement is an agreement by which a data controller commissions (usually pays) an agency to deliver a function on its behalf. The sharing agency remains the data controller throughout and the receiving agency becomes the data processor.
24.	*[Was notice provided to the individual prior to collection of the data? If yes, please provide a copy of the notice as an appendix to this document (A notice may include a posted privacy policy or a privacy notice on forms). If notice was not provided, why not?]* Yes. This is done currently and will continue (Victims' Code of Practice now applies). Each police force area has its own notice. A typical example – from the Metropolitan Police Service – is appended.
25.	*[Do individuals have an opportunity and/or right to decline to provide data?]* Yes.
26.	*[(i) Are we processing the data for the original purpose for which it was collected? (ii) Do individuals have the right to consent to particular uses of the data, and if so, how does the individual exercise that right?]* (i) Yes. (ii) Yes, in accordance with relevant legislation. FLOs introduce the service to those bereaved and if they ask for assistance, their permission is obtained to pass their sensitive personal data to the Homicide Service.

27.	*[What are the procedures which allow individuals the right to gain access to their own data?]* In accordance with relevant Government legislation. Subject Access Requests should be made direct to the Homicide Service.
28.	*[What are the procedures for correcting erroneous data?]* By informing the Homicide Service.
29.	*[How are individuals notified of the procedures for correcting their data?]* The Homicide Service provide this information.
30.	*[If no redress is provided, are alternatives available?]* Not applicable.

Organisational relationships

31.	*[Is the data shared with internal organisations/departments? If yes, please list.]* It may be shared within appropriate internal teams where and if necessary.
32.	*[For each organisation/department, what data is shared and for what purpose?]* Data may be shared within relevant teams in order to ensure that the necessary support is provided to the bereaved families.
33.	*[How is the data transmitted or disclosed?]* Via secure email system accredited by CESG.
34.	*[Is data shared with external organisations/departments/non-Government organisations? If yes, which organisations/departments?]* Yes. Where appropriate and with families' consent, CJS agencies (HMCS, NOMS, CPS. Probation Service), the Police, FCO, MARACS, sub-contracted organisations supporting families bereaved by post-2010 homicide. All with necessary data agreements in place.
35.	*[Specify which, if any, of these organisations are outside of the European Economic Area, and specify how the DPA is being complied with?]* None. Nothing stored outside the UK.
36.	*[For each external organisation, what data is shared and for what purpose?]* To enable the support needs of the bereaved to be appropriately addressed. Data only shared with the informed consent of the data subject. To enable – where necessary – CJS depts / agencies to enable support of families through the CJS process. It is a

	Government aim to provide the best support possible to victims of crime. Statistical information for grant monitoring purposes, and to enable provision of advice to Ministers for policy / PQs etc. The statistical records will enable the Homicide Service operator to demonstrate to the MoJ that it is providing the service for which grant has been given and to demonstrate value for money in their use of public monies. This is important so that MoJ can monitor the grant agreement and respond to enquires about use of the grant from Ministers and Parliament. Personal data will only be shared with the consent of the data subject or other legal gateway (see question 23).
37.	*[How is the data transmitted or disclosed to all external organisations?* Via secure email. All secure email requires a password for access.
38.	*[How is the shared data secured by the recipient? How long will the data be retained for? How is the data going to be securely destroyed?]* All data is secured in accordance with requirements of legislation and only retained for as long as necessary. Data are retained for 6 years from the close of a case giving the service users this period to bring an action against the incumbent if the person considers that the service has been negligent. The incumbent has an appropriate data retention policy (which is copyrighted) in accordance with the requirements of the Data Protection Act.
39.	*[Is there a Memorandum of Understanding (MoU), contract, or any data sharing agreement in place with any external organisations with whom data is shared through the system, and does the agreement reflect the scope of the data to be shared?]* Yes. Agreement(s) will be compliant with data sharing requirements.
40.	*[What training is required for users from agencies outside MoJ prior to receiving access to the data and how is the training audited for compliance to current MoJ policy?]* The Homicide Service will provide for and monitor all appropriate training in order to comply with all relevant legislative requirements.

Technology employed

41.	*[Was the system built from the ground up ("bespoke"); or, was a COTS product purchased and installed?]* Built up. The service provider has conducted a Privacy Impact Assessment of the Case Management System. The Ministry of Justice is content that the provider has undertaken necessary work to ensure that it is, and will continue to be, compliant with the Data Protection Act.

42.	*[Describe how data integrity, privacy and security were analysed as part of the decisions made for your system (Security Working Group, User Requirements Document, Security Requirements Document)?]* See answer to Question 41.
43.	*[What design choices were made to enhance privacy?]* See answer to Question 41.
44.	*[Does the system use "roles" to assign privileges to users of the system?]* See answer to Question 41.
45.	*[What procedures are in place to determine which users may access the system and where are they documented?]* See answer to Question 41.
46.	*[How are the actual assignments of roles and rules verified according to established security and auditing procedures?]* See answer to Question 41.
47.	*[What auditing measures and technical safeguards are in place to prevent misuse of data?]* See answer to Question 41.
48.	*[Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system.]* See answer to Question 41.

Legislation and policies

49.	*[Privacy & Electronic Communications Regulations 2003* ***Technology*** *Does the project involve new or inherently privacy-invasive electronic communications technologies?* *For the avoidance of any doubt, 'communication' means any information exchanged or conveyed between finite parties by means of a public electronic communications service, but does not include information conveyed as part of a programme service, except to the extent that such information can be related to the identifiable subscriber or user receiving the information.']* No.
50.	*[Privacy & Electronic Communications Regulations 2003* ***Communication providers*** *Does the project involve new or existing communication providers?* *For the avoidance of doubt, 'communication providers' means a person or organisation that provides an electronic communications network or an electronic communications service.[2]]* Both.
51.	*[Privacy & Electronic Communications Regulations 2003* ***Communication subscribers / users*** *Does the project involve new or existing communication subscribers / users?* *For the avoidance of doubt, 'communication subscriber' means a person who is a party to a contract with a provider of public electronic communication services for the supply of such services. 'User' means an individual using a public electronic communications service.]* Both.

[2] Source – Communications Act 2003

52.	*[Human Rights Act 1998* ***Article 2: Right to Life*** *Does the project involve new or existing data processing that adversely impacts an individual's right to life, subject to any limitations as may be defined in Article 2(2)?* *For the avoidance of any doubt, the limited circumstances are that in peacetime, a public authority may not cause death unless the death results from force used as follows:* • *Self defence or defence of another person from unlawful violence;* • *Arresting of someone or the prevention of escape from lawful detention; and* • *A lawful act to quell a riot or insurrection.]* No.
53.	*[Human Rights Act 1998* ***Article 3: Prohibition of Torture*** *Does the project involve new or existing data processing that adversely impacts an individual's right to be not subjected to torture or inhuman or degrading treatment?* *For the avoidance of doubt, this is an absolute right.]* No.
54.	*[Human Rights Act 1998* ***Article 4: Prohibition of Slavery or Forced Labour*** *Does the project involve new or existing data processing that adversely impacts an individual's right to be not held in servitude or forced to perform compulsory labour?* *For the avoidance of doubt, this is an absolute right; the following are excluded from being defined as forced or compulsory labour:* • *Work done in ordinary course of a prison or community sentence;* • *Military service;* • *Community service in a public emergency; and Normal civic obligations.]* No.

55.	*[Human Rights Act 1998* ***Article 5: Right to Liberty and Security*** *Does the project involve new or existing data processing that adversely impacts an individual's right to be not deprived of their liberty subject to certain limitations?* *For the avoidance of doubt, the following limitations apply when a person is:* • *Held in lawful detention after conviction by a competent court;* • *Lawfully arrested or detained for non-compliance with a lawful court order or the fulfilment of any lawful obligation;* • *Lawfully arrested or detained to effect the appearance of the person before a competent legal authority;* • *Lawfully detained to prevent the spreading of infectious diseases;* • *Lawfully detained for personal safety (applies to persons of unsound mind, drug addicts etc.); and* • *Lawfully detained to prevent unlawful entry into the country or lawful deportation from the country.]* No.
56.	*[Human Rights Act 1998* ***Article 6: Right to a Fair Trial*** *Does the project involve new or existing data processing that adversely impacts an individual's right to have a public hearing within a reasonable time by an independent and impartial tribunal established by law?* *For the avoidance of doubt, the hearings included are both civil and criminal proceedings that are not specifically classified as hearings that must be heard 'in camera', i.e. closed to the public.]* No.
57.	*[Human Rights Act 1998* ***Article 7: Right to no Punishment without Law*** *Does the project involve new or existing data processing that adversely impacts an individual's right to not be prosecuted for a crime that was not, at the alleged time of commission, constitute a criminal offence under national or international law?* *For the avoidance of doubt, this is an absolute right.]* No.

58.	*[Human Rights Act 1998* ***Article 8: Right to Respect for Private and Family Life*** *Does the project involve new or existing data processing that adversely impacts an individual's right to respect for privacy in terms of their private and family life subject to certain qualifications?* *For the avoidance of doubt, the qualifications are:* • *Legal compliance;* • *National security;* • *Public safety;* • *National economy;* • *Prevention of crime and disorder;* • *Protection of public health and morals;* • *Protection of rights and freedom of others.]* No.
59.	*[Human Rights Act 1998* ***Article 9: Right to Freedom of Thought, Conscience & Religion*** *Does the project involve new or existing data processing that adversely impacts an individual's right to freedom of thought, conscience and religion subject to certain qualifications?* *For the avoidance of doubt, the qualifications are:* • *Unless prescribed by law;* • *In interest of public safety;* • *Protection of public order, rights or morals;* • *Protection of rights and freedoms of others.]* No.
60.	*[Human Rights Act 1998* ***Article 10: Right to Free Expression*** *Does the project involve new or existing data processing that adversely impacts an individual's right to hold opinions and express their views singly or in dialogue subject to certain qualifications?* *For the avoidance of doubt, the qualifications are as set out in Article 9 above.]* No.

61.	*[Human Rights Act 1998* ***Article 11: Right to Freedom of Assembly & Association*** *Does the project involve new or existing data processing that adversely impacts an individual's right to freedom of peaceful assembly and association with others subject to certain qualifications/* *For the avoidance of doubt, the qualifications are as set out in Article 9 above.]* No.
62.	*[Human Rights Act 1998* ***Article 12: Right to Marry*** *Does the project involve new or existing data processing that adversely impacts an individual's right to marry and found a family subject to certain restrictions?* *For the avoidance of doubt, the restrictions are regulated by law so long as they do not effectively take away the right, e.g. age restrictions apply.]* No.
63.	*[Human Rights Act 1998* ***Article 14: Right to Freedom from Discrimination*** *Does the project involve new or existing data processing that adversely impacts an individual's right to be treated in a manner that does not discriminate the individual from others subject to certain restrictions?* *The grounds for discrimination can be based on:* • *Sex* • *Race* • *Colour* • *Language* • *Religion* • *Political persuasion* • *Nationality or social origin* • *Birth* • *Other status.* No.

64.	*[Human Rights Act 1998* ***Articles: 16 / 17 / 18*** *Not relevant for the purpose of this questionnaire.]* As stated above – not applicable.
65.	*[Regulation of Investigatory Powers Act (RIPA) 2000* *Does the project involve new or inherently privacy invasive electronic technologies to intercept communications?* *For the avoidance of doubt, 'communications' is defined in RIPA Part V, section 81(1).]* No.
66.	*[Regulation of Investigatory Powers Act (RIPA) 2000* *Does the project involve new or inherently privacy invasive electronic technologies pertaining to the acquisition and disclosure of data relating to communications?]* No.
67.	*[Regulation of Investigatory Powers Act (RIPA) 2000* *Does the project involve new or inherently privacy invasive electronic technologies pertaining to the carrying out of surveillance?]* No.
68.	*[Regulation of Investigatory Powers Act (RIPA) 2000* *Does the project involve new or inherently privacy invasive electronic technologies pertaining to the provision of the means by which electronic data protected by encryption or passwords may be decrypted or accessed?]* No.
69.	*[Regulation of Investigatory Powers Act (RIPA) 2000* *Does the project undertake any of the functions of the Security Service, the Secret Intelligence Service or the Government Communications Headquarters?]* No.

Alternative solutions

No alternative technology solutions were considered.

Solution adopted

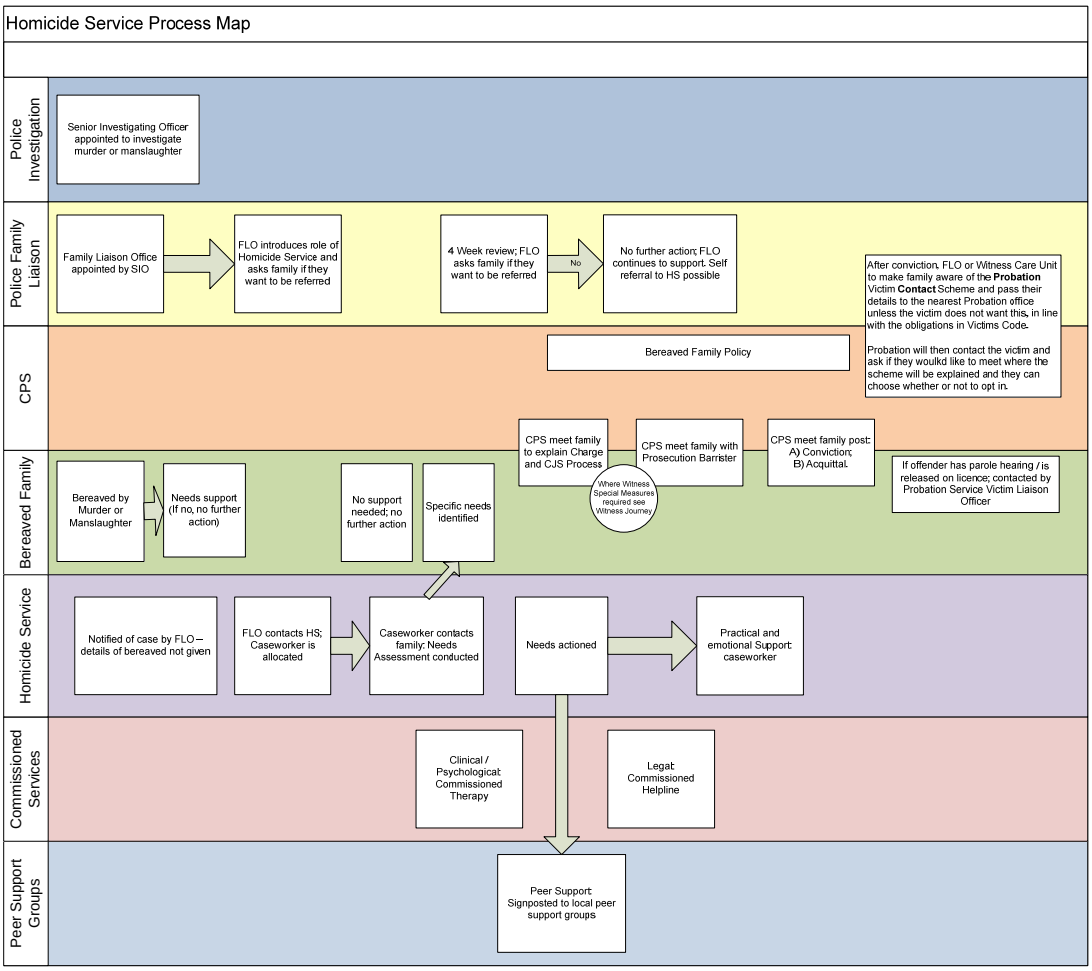
The new service provider has satisfied the grant award competition. Should any concerns arise in future, the MoJ will work with the provider to address them.

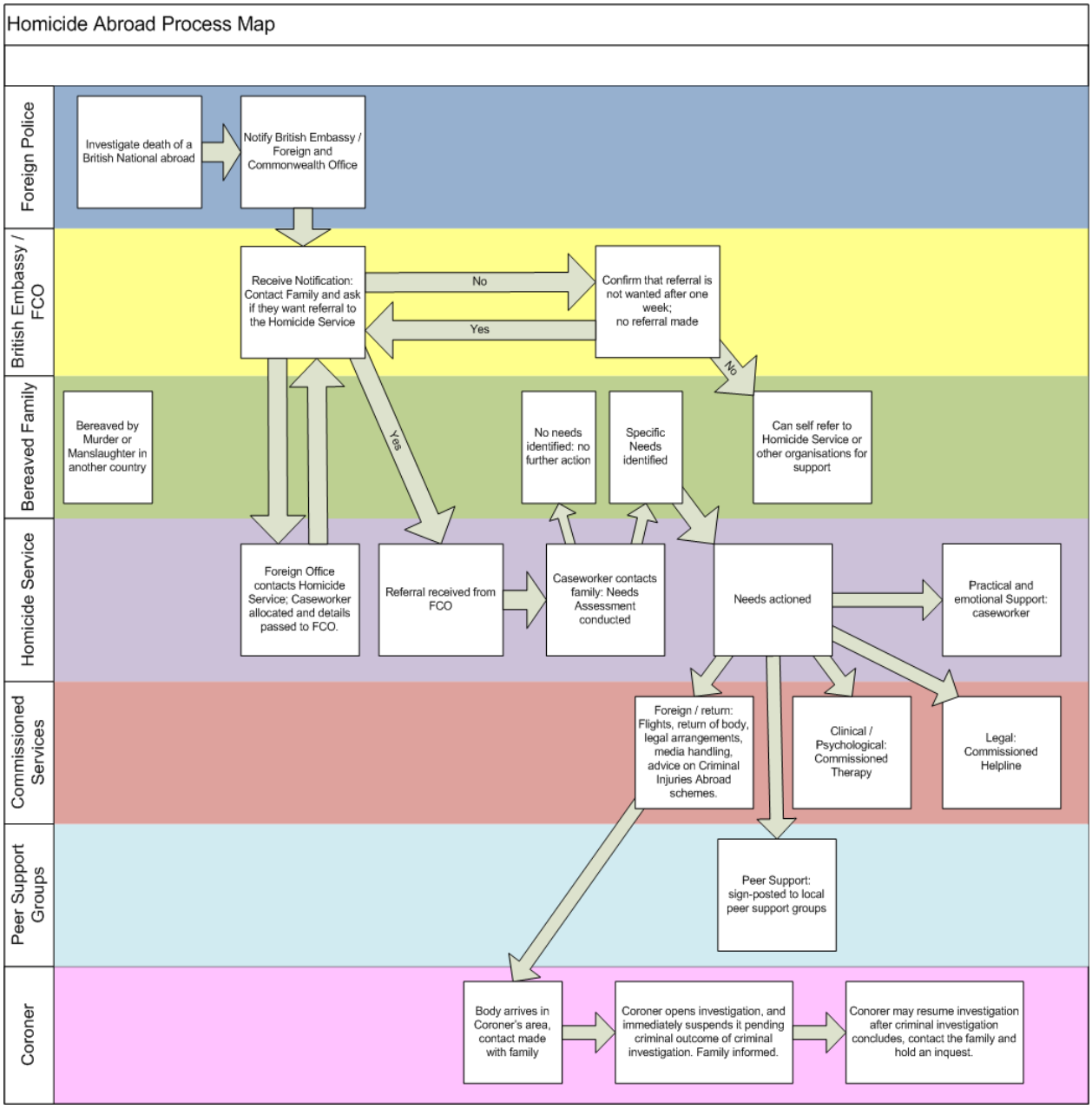
Data protection/risk reducing designs

Appropriate Government standard IS and IL level controls. All security based on the advice of a CLAS consultant.

Section 4 – Data flow analysis

Business data flow diagram and description





Data flow table

The above diagrams show the basic links in the process of supporting families bereaved by homicide. Where agencies link together they have secure email and data transfer agreements as necessary in order to comply with data protection legislation requirements.

Issues

None not covered by arrangements put in place to comply with necessary requirements to meet the grant competition award.

Section 5 – Data protection analysis and risk management plan

Stakeholders/participants

None involved in the screening process. Police, FCO, current service provider, CJS agencies and stakeholder support groups were involved in needs assessment process which underlies the Homicide Service commissioning process.

Analysis process

Screening process was a single process prepared by Procurement (NOMS).

Analysis summary

Only a short PIA needed. Data systems essentially as before, with some additionality / change in terms of organisations involved.

Risk management

Potential change of service provider might have impacted on data protection issues.

Note: Ministers have agreed that the new service should be operated by the incumbent. Data protection issues are not a risk.

Risk mitigation

Inclusion of a colleague from MoJ ICT data assurance at presentations by new service provider bidders enabled evaluation panel to assess data information proposals by bidders.

Summary

Risks minor if incumbent were to operate the new Homicide Service. Risks arising from a new service provider could be mitigated by working with same on data proposals

Note: Ministers have agreed that the new service should be operated by the incumbent. Data protection issues are not a risk.

Section 6 – Communication/publication strategy

Communications

Publication will be Full Disclosure.

Publication strategy

Published government commitment and a public grant award competition.

Commissioning of a service provider to operate a national Homicide Service form 1 October 2014 – summary publication

All sections of this report can be published.

Section 7 – Approval of report

Approval of:	**Commissioning of a service provider to operate a national Homicide Service from 1 October 2014.**
Policy lead/Business Sponsor/Project Manager	Nicola Hewer
Information Asset Owner	Victim Support
Date of approval	2nd December 2014

APPENDIX

ACPO – VICTIM SUPPORT VICTIM REFERRAL AGREEMENT (18 DEC 2003)

1. The *Victims of Crime* leaflet has a key role to play in these procedures. The leaflet is given to victims of crime by the police. It explains what happens when a crime is reported, what happens next, and what other help and advice is available. The leaflet explains that victims' details will be passed to Victim Support unless the victim expresses a contrary wish (except in cases of domestic violence or sexual crime or bereaved families of victims of homicide where express consent is always required).

2. This right is spelt out clearly on the front cover of the leaflet, where the fourth bullet point says that:
"The police will pass information about you to Victim Support so that they can offer help and support, unless you ask the police not to."

3. That message is reinforced in the 'Check List for Action' section of the leaflet and in the section headed 'Help From Victim Support Schemes'.

4. While the leaflet is one way of helping to ensure that victims are aware that they can opt out of having their details passed on to Victim Support, it should not be relied upon as the only way. It is important that officers should make it clear to victims that their details will normally be passed on to Victim Support unless the victim says they don't want this to happen. This requirement could be met by officers using a standard form of words when recording details of the crime from the victim, along th efolllowinh lines:

   "Victim Support is an independent charity which can offer you help. We recommend their services, and it is force policy to refer your details to them unless you ask us not to."

   If the victim then said that they did not want their details passed to Victim Support, the officer should/will record that fact as indicated by local force policy e.g. in his/her notebook, or on the computer system if recording the crime details over the phone, and ensure compliance. Unless a such a response was formally recorded, it could be assumed that the victim was content for their details to be passed on. The Information Commissioner believes that where information systems are used to record the reporting of a crime, then a mechanism for recording that the notification to the victim had taken place would also be valuable. If a victim were subsequently to complain to the Commissioner that their details had been passed on to Victim Support without their knowledge, then any Chief Officer having such a record available would be well placed to rebut such an assertion.

5. The force policy with regard to referral of victims' details to Victim Support should be emphasised in other ways, for example, on force websites, in force leaflets and on posters in police stations etc.

6. Express consent must still be sought from victims of domestic violence, sexual crime or the bereaved relatives of victims of homicide. Such victims, following a recommendation as to Victim Support services, should continue to be asked specifically if they want their details to be passed on to Victim Support, and onward referral should only be made if they positively opt in.

7. Where an FLO is involved, the availability of Victim Support services should be offered and recommended at the earliest appropriate moment and the consent sought.

8. Information to be routinely passed to Victim Support
    i. Name
    ii. Address
    iii. Contact telephone number
    iv. Gender
    v. Age
    vi. Brief crime details – including self-defined ethnicity (under the 16 + 1 system) where relevant to the offence. E.g. racially aggravated public order offences where the correct ethnicity of the victim may be at variance to that used by the perpetrators, or where the victim believes the crime to be racially motivated.

9. Other information may be passed on a case by case basis where the additional information will be required by Victim Support to assess the type and level of support required.

10. There are crimes, which due to their volume, cannot always be handled by Victim Support and the police may not routinely refer these offences unless there are aggravating factors involved. The offences this will relate to are:
    a. theft from motor vehicles
    b. tampering with motor vehicles
    c. minor criminal damage
    d. theft of motor vehicle

    However, aggravating factors such as repeat victimisation, victim request for contact, vulnerable victims or hate crime will ensure a referral to Victim Support.

11. The situations where a homicide or injury is a consequence of a road crash is currently being reviewed by a government working group, and each force should discuss with its Victim Support Area the level of support which they are currently able to provide.

12. Victim Support is also one of the listed agencies for engagement in response to emergenceis and disasters.

Agreed between ACPO and Victim Support – 18 December 2003

Alternative format versions of this report are available on request from:

Ministry of Justice, Victims, Witnesses and Criminal Justice Delivery, 4th Floor (Zone B), 102 Petty France, London, SW1H 9AJ

or from:

victimsandwitnesses@cjs.gsi.gov.uk