Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project.

Project / Work Stream Name	**Pan-London Data Sharing Agreement- People affected by an emergency**	
Project / Work Stream Lead	Name	[redacted] and [redacted]
	Designation	London Borough Of Barnet Deputy DPO/ London Borough of Camden Information Rights Team Leader, and LOTI Data Sharing Project Manager
	Email	[redacted]@barnet.gov.uk/[redacted]@camden.gov.uk
Overview: (Summary of the project/work stream)	This is a DPIA to cover a pan-London Data Sharing Agreement (DSA) between a number of agencies to cover sharing of personal data about people affected by an emergency with organisations that have a responsibility to undertake safeguarding actions and/or offer or provide support services to those people, such as humanitarian assistance.	
Implementation Date:	asap	
<u>Environmental Scan</u> Describe the consultation/checks that have been carried out regarding this initiative or, project of similar nature, whether conducted within your organisation or by other organisations.	This work is currently undertaken by the partners but without a comprehensive all party up to date DSA.	

Step 1: Complete the Screening Questions			
Q 1	**Category**	**Screening question**	**Yes/ No**
1.1	Technology	Does the project introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy?	No
1.2	Technology	Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?	No
1.3	Identity	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Local Gov. Identifier, Hospital ID no. or, will use intrusive identification or identity management processes or, electronic linkage of personal data?	Yes
1.4	Identity	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	No
1.5	Multiple organisations	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	Yes
1.6	Data	Does the project involve new process or significantly change the way in which personal data/special categories of personal data and/or business sensitive data is handled?	No
1.7	Data	Does the project involve new or significantly changed handling of a considerable amount of personal data/special categories of personal data and/or business sensitive data about each individual in a database?	No
1.8	Data	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	No
1.9	Data	Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special categories of personal data and/or business sensitive data from multiple sources?	Yes
1.10	Data	Will the personal data be processed out of the U.K?	No
1.11	Exemptions and Exceptions	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	Yes
1.12	Exemptions and Exceptions	Does the project's justification include significant contributions to public security and measures?	Yes
1.13	Exemptions and Exceptions	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	Possibly if terrorism related

The purpose of the screening questions is to confirm that the data protection laws are being complied with, or highlights problems that need to be addressed. It also aims to prevent problems arising at a later stage which might impede the progress or success of the project.

Answering "Yes" to any of the screening questions above represents a potential Information Governance (IG) risk factor, please proceed and complete the next section.

Step 2: Identify the need for a DPIA		
2.1	**Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared?**	New/Changed Changed

2.2 What data will be processed/shared/viewed?

Personal Data

Forename	Yes	Surname	Yes	Date of Birth	Yes	Age	Yes	Gender	Yes
Address	Yes	Postal address	Yes	Employment records	Yes	Email address	Yes	Postcode	Yes
Other unique identifier (*please specify*)	Yes*	Telephone number	Yes	Driving licence number		NHS No	Yes	Hospital ID no	Yes

Other data *(Please state):*	*potentially any reference number assigned by a partner Financial, property, employment data Images and footage including CCTV, dashcam and body worn footage (noting there is also a specific CCTV DSA) Information held in agencies' caution registers or similar which are a database of information about properties or individuals where a risk is posed to visitors due to the inhabitants or conditions in the property

Special Categories of Personal Data

Racial or ethnic origin	Yes	Political opinion		Religious or philosophical beliefs	Yes
Trade Union membership	Yes	Physical or mental health or condition			Yes
Sexual life or sexual orientation		Social service records	Yes	Child protection records	Yes

Sickness forms		Housing records	Yes	Tax, benefit or pension records		Adoption records	
DNA profile		Fingerprints		Biometrics		Genetic data	

Criminal allegation and prosecuting information	
Other data (Please state):	GP name and practice contact details Languages spoken

Will the dataset include clinical data? (please include)	Yes/No possibly
Will the dataset include financial data?	possibly

Description of other data processed/shared/viewed?

2.3	Business sensitive data			
	Financial		No	
	Local Contract conditions		No	
	Operational data		No	
	Notes associated with patentable inventions		No	
	procurement/ tendering information		No	
	Customer/ supplier information		No	
	Decisions impacting:	One or more business function		Yes/No
				No
		Across the organisation		No
	Description of other data processed/shared/viewed (if any).			
	N/A			

Step 3: Describe the sharing/processing			
3.1	**List of organisations/partners involved in sharing or processing personal/special categories personal data?** *If yes, list below*		Yes/No
			YES
	Name	Controller or Processor?	Completed and compliant with the IG Toolkit or Data Security and Protection (DSP) Toolkit
			Yes / No
	London Local Authorities	Controller	Yes
	Metropolitan Police Service, British Transport Police & City of London Police	Controller	Yes
	London Fire Brigade	Controller	TBC
	NHS England & NHS Improvement (London), NHS Acute Trusts, NHS MH Trusts, NHS Community Service Providers , London Ambulance Service NHS Trust	Controller	Yes
	UK Health Security Agency (HSA)	Controller	Yes
	Department for Work & Pensions (inc Job Centre Plus)	Controller	Yes
	Her Majesty's Coastguard	Controller	Yes
	Thames Water	Controller	Yes
	Transport for London	Controller	Yes
	British Red Cross	Controller	Yes
	Department for Levelling Up, Housing and Communities	Controller	Yes
	Victims of Terrorism Unit	Controller	Yes
3.2	**If you have answered 'yes' to 3.1 is there an existing ' Data Processing Contract' or 'Data Sharing Agreement' between the Controller and the Processor?**	Yes/No	
		Yes - A single DSA will be put in place to cover sharing with the listed adult safeguarding partners where they are Controllers. Each Local Authority will be responsible for ensuring that they have Data Processing Contracts in place with any local Processors.	
3.3.	**Has a data flow mapping exercise been undertaken?** **If yes, please provide a copy, if no, please undertake**	The flows will vary case by case according to specific circumstances and case requirements	
3.4	**Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?** If yes, provide a copy of the confidentiality agreement or contract?		Yes / No
			no
3.5	**Describe in as much detail why this information is being processed/shared/viewed?**		

information may be shared for the following resilience related reasons:

- warning and informing the public
- evacuation
- provision of rest centres, survivor reception centres, family and friends reception centres
- immediate medical treatment, health and social care
- longer-term health care (mental, physical and public health) and social care
- assistance with temporary accommodation
- financial and practical support
- bereavement support
- Casualty Bureau Receives information relating to persons who are believed to have been involved in an emergency

Data sharing is necessary for criminal and civil investigation purposes to:

- reduce immediate or short-term risk of continuation of the incident or a similar incident, where the incident is impacted by criminal activity.
- reduce potential fraud such as fraudulently seeking humanitarian or financial support.
- identify and interview victims and witnesses.

Outside of the immediate incident response, the sharing of information may be required to:

- support humanitarian assistance for a long period of time following an emergency. For example, long-term health care, support to people during inquests, memorials, and anniversaries.
- prepare for a potential emergency by identifying individuals likely to need support during an incident.
- help organisations identify individuals that may require wider future support e.g. ongoing social care and utility priority service registers.
- reduce the likelihood of a repeat or similar incident.
- plan for effective data sharing for future incidents e.g. agree definitions of vulnerability across organisations, or establish routes for data matching and ensuring suitable data quality.
- reduce likelihood of fraud, or future incidents impacted by criminal activity.

The sharing of information may also be required if an emergency is likely to occur (i.e. prior to an emergency). For example to identify and provide support to vulnerable persons who may be affected by a forecast flooding emergency and require additional support services.

Parties to this agreement have requirements under the Civil Contingencies Act 2004 to prepare for emergencies, which includes preparing to easily and quickly identify those individuals in need of support. This can be a 'List of Lists', which is non-personal data that details where information on vulnerable individuals can be found, or it can be personal data. If personal data, this may be drawn from within local authority safeguarding case files, or utility company Priority Service Registers for example. There are

	practices in place between some organisations to share or maintain lists of vulnerable persons regularly for emergency preparedness activity. The parties to this agreement recognise that this is encouraged by the Ofgem and Ofwat regulators. Data collected during an emergency response may allow organisations to identify or update their records of individuals needing support outside an emergency incident, whether utility company Priority Service Registers or local authority child and adult safeguarding casework. The parties recognise that this could be justified as part of the parties' public tasks, and substantially in the public interest (where using special category data). The necessity and benefits for sharing this data will change between types and severity of incident, and data sharing channels may be developed under this DSA to support this work. As part of work to reduce the likelihood of future incidents, the parties can consider sharing data to change processes or locations. Often non-personal or pseudonymised data could be used, and examples include use of footage and witness statements to change buildings and locations for better emergency evacuation, or install environmental remediations such as flood barriers.

Step 4: Assess necessity and proportionality	
4.1	**Lawfulness for Processing/sharing personal data/special categories of personal data?** ● **Article 6(1)(c) – legal obligation***:* processing is necessary for compliance with a **legal obligation** to which the controller is subject. Organisations may have a legal obligation to share data, especially in relation to children and safeguarding. ● **Article 6(1)(e) – public task:** (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. (Use of this article requires that the Data Protection Act section 8 be satisfied, the underlying task, function or power must have a clear basis in law, though that need not be statutory, it could be based on common law or part of a contractual obligation. The laws given in this DSA Appendix B – Applicable legislation provide for each party a legal basis under section 8 – the specifics are noted in the appendix). This is likely to be the most relevant lawful basis for sharing. ● It is highly likely that most data sharing under this DSA will fall within Article 6(1)(c) or (e) ● **Article 6(1)(d) – vital interests:** where processing is necessary to protect the data subject's life or the life of another person. This is unlikely to be a common basis. For more detail see the ICO's guidance on vital interest. ● **Outsourced or contracted services**. Where there is sharing by a contracted organisation, whether a company, public sector body, or voluntary organisation, where there is a formal relationship regulating the parties' relations and the contracted party is Data Processor of the public authority, the sharing by the Data Processor will be under the lawful basis of the Data Controller. **Article 9 (2) – Special Category Personal Data Processing** ● **Article 9(2)(c) processing is necessary to protect the vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. This will only be a relevant condition for sharing in life-or-death scenarios. There is also a higher bar to meet here than in the Article 6 lawful basis, in that persons in question must also be physically or legally incapable of giving their consent to their special category personal data being shared. If there is another lawful basis that applies, which is likely given the duties and powers of parties to this agreement from their specific legislation, then this should be used rather than vital interests. ● **Article 9(2)(g) substantial public interest** - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. This is likely to be the most relevant condition. One of the conditions in Part 2 of Schedule 1, Data Protection Act 2018 needs to be met. Likely conditions under Part 2, Schedule 1 are:

- para 6 Statutory etc and government purposes,
- para 10 Preventing or detecting unlawful acts, or
- para 18 Safeguarding of children and of individuals at risk.

The organisation must have an 'appropriate policy document' in place that explains the controller's procedures for securing compliance with the principles in Article 5 GDPR.

For some of the conditions in Schedule 1, there is a need to justify why obtaining explicit consent is not possible. Data subjects having their data processed for emergency resilience purposes are vulnerable and there is an imbalance of power between data subjects and data controllers. It is not considered that truly informed and freely given consent can be achieved, especially as consent could not be withdrawn for the processing undertaken under this DSA. It is also not considered practical to expect data controllers to seek consent for data processing during fast-moving emergency incidents.

- **Article 9(2)(h) provision of health or social care** - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

- **Article 9(2)(i) public health -** processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

  This is likely to be a suitable lawful basis for incidents involving disease spread such as influenza or Legionnaires'; for the spread and impact of radiation poisoning; or danger to health from sewage infiltrating water supplies.

Lawful Basis for Sharing Criminal Offence Data

Art. 10 GDPR: Processing of personal data relating to criminal convictions and offences states that processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 10 requires that an article 6 condition is met- this is likely to be the same as the article 6 basis for processing personal data. It also requires that a condition in Part 1 or 2 of Schedule 1 Data Protection Act 2018 is met. The most relevant conditions will be:

- Part 1 para 2 Health or social care purposes,
- Part 2 para 6 Statutory etc and government purposes
- Part 2 para 10 Preventing or detecting unlawful acts

	● Part 2 para 18 Safeguarding of children and of individuals at risk.		
4.2	**Will the information be processed/shared electronically, on paper or both?**	**Electronic**	Yes
		Paper	Yes
4.3	**How will you ensure data quality and data minimisation?**		
Each partner is responsible for ensuring the accuracy and relevance of the personal data that it processes and shares and must have clear processes in place for managing data quality. Any party learning of the inaccuracy of personal data is responsible for taking appropriate action to correct it and informing the parties with whom that data has been shared.			
4.4	**Have individuals been informed about the proposed use of their personal or special categories of personal data?** For example, do the organisations/partners listed in section 3.1 have updated Fair Processing Notice available to patients on their websites?		Not necessarily directly
	Privacy notices for all organisation note emergency related purposes. However, in some cases, data subjects may not be specifically notified about the use of their data where giving them this information would be impossible or involve disproportionate effort. It is noted that in many cases exemptions will apply.		
4.5	**How will you help to support the rights of individuals?**		
	Each controller remains responsible for complying with the applicable data subject rights.		
4.6	**Are arrangements in place for recognising and responding to Subject Access Requests (SARs)?**		
	Each controller remains responsible for their own data subject requests. Where a SAR covers data provided by another party, before responding to the SAR, the Controller will consult with the providing party regarding any disclosure concerns they may have.		
4.7	**Will the processing of data include automated individual decision-making, including profiling? If yes, please outline the profiling processes, the legal basis underpinning the process, and the rights of the data subject**		No
	N/A		
4.8	**Will individuals be asked for consent for their information to be processed/shared?** If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.		No
	As outlined above, consent is not the legal basis as other legal bases are utilised.		
4.9	**As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier?** If so please complete the embedded questionnaire.	Existing technologies are used, no new systems.	
4.10	**Where will the data be stored**		
	Provider systems are used. Paper storage is minimised; all storage is UK only.		
4.11	**Data Retention Period** *How long will the data be kept?*		
	Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared. This Record of Processing Activity (ROPA) must include the retention period for the data.		

	Information must not be retained for longer than necessary for the purpose for which it was obtained. Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.	
4.12	**Will this information be shared/processed outside the organisations listed above in question 3?** If yes, describe who and why:	Yes/No
	Due to the nature of the processing it is possible that this may be the case. It would not be possible to list organisations as these would vary depending on the emergency situation.	Possible

Step 5: Information Security Process

5.1	**Is there an ability to audit access to the information?**	Yes/No
	All DSPT certified provider systems have an audit built in. We cannot guarantee for the voluntary sector, however they will be supplying rather than receiving information in most cases.	Yes
5.2	**How will access to information be controlled?**	
	This varies between providers, but RBAC control is required with password access as minimum.	
5.3	**What roles will have access to the information?** (list individuals or staff groups)	
	This will vary by organisation but RBAC is in place	
5.4	**What security and audit measures have been implemented to secure access to and limit use of personal data/special categories of personal data and/or business sensitive data?**	

Username and password	yes	Smartcard	for some partners	key to locked filing cabinet/room	for some partners
Secure 1x Token Access	for some partners	Restricted access to Network Files			yes
Other: Provide a Description Below:					

5.5	**Is there a documented System Level Security Policy (SLSP) for this project? If yes, please embed a copy below:**	Yes/No
		Not required, no new system.

5.6	**Are there Business Continuity Plans (BCP) and Disaster Recovery Protocol for the proposed/existing system or process?**		Yes/No Yes
5.7	**Is there Mandatory Staff Training for information governance?**	Yes/No	Yes
5.8	**Are there any new or additional reporting requirements for this project?**	No	
	What roles will be able to run reports?		
	N/A		
	What roles will receive the report or where will it be published?		
	N/A		
	Will the reports be in person-identifiable, pseudonymised or anonymised format?		
	N/A		
	Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?		
	N/A		
5.9	**Have any Information Governance risks been identified relating to this project? (if Yes the final section will need to be completed)**		**Yes/No** Yes

Step 6: Identify and Assess Privacy Risks			
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Note: risks here are risks of this sharing ONLY. Signatories should have DPIAs for their own individual systems and methods, covering their local risks.			
Misuse of data: Personal data could be used by a recipient in a manner incompatible with the Data Sharing Agreement (Inappropriate secondary processing). Compliance risk: Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Possible	Moderate	Medium High
Inherent privacy intrusion from sharing information with a third party. Whilst much of the information to be shared will not be very intrusive, for some cases the information will be sensitive for example relating to vulnerabilities. Compliance risk: Personal data shall not be kept for longer than necessary. Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Possible	Moderate	Medium High
Inappropriate Further transfer of data: Risk to the safety of personal data if transferred elsewhere by a recipient. Concerns may be for sharing with 3rd parties such as insurance companies or the press. Compliance risk: Personal data shall be obtained for one or more specified and lawful purposes. Appropriate technical and organisational measures shall be taken. Personal data shall not be transferred outside the European Economic Area. Corporate risk: Reputational risk. Loss of trust	Possible	Major	Medium High
Loss of data in transfer. Personal data could be obtained and misused by third parties. Compliance risk: Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Unlikely	Major	Medium High
Disposal of data: If personal data is not disposed of in an appropriate manner by the party with whom it was shared, it may be possible for third parties to obtain the data. This is a risk when the urgency of sharing in emergencies may mean more reliance than usual on paper copies. Compliance risk: Personal data shall not be kept for longer than necessary. Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Possible	Major	Medium High

Step 7: Identify Measures to reduce privacy risk				
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 6				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Misuse of data	Organisations are bound by art 5 requirements and have policies and processes in place to guard against this as far as possible. Sharing will be by and to authorised officers only who are subjected to full employment checks. Access to council systems are fully RBAC and auditable. All organisations have full employee policies and codes of conduct. Beaches of those would be a disciplinary offence and may be a criminal act.	Reduced	Low	Yes
Inherent Privacy Intrusion	The DSA requires that sharing will only be of data necessary in each instance and will be the minimum needed to achieve the lawful purposes. A degree of privacy intrusion is unavoidable, otherwise the sharing could not be facilitated. Given the reasons for sharing the intrusion is considered to be proportionate to the risks	Reduced	Moderate	Yes
Inappropriate Further transfer of data	Each data controller has appropriate policies and security processes etc in place to rescue the risks as far as possible. Employees etc are subject to appropriate employment vetting and conditions. All parties have full policies and processes in place to ensure data is handled securely. Systems are auditable and RBAC is in force. It is noted that where one party receives data from another, the receiving party becomes a Data Controller and therefore takes the liability for the data from that point, and is bound by the requirements of data protection legislation. However it is noted that where a Data Controller handles data in a manner not expected this can lead to reputational damage for the supplying party, notwithstanding they have no legal	Reduced	Low	Yes

	liability data protection wise. For the data in this DSA it is considered these risks are low.			
Loss of data in transfer, either poor information security or malicious attempt.	Each data controller has appropriate policies and security processes etc in place to rescue the risks as far as possible The DSA specifies the appropriate technical measures in place to ensure the security of the data transfers. The organisations routinely share volumes of special category data and have well established protocols to do so safely.	Reduced	Low	Yes
Disposal of data:	It is noted that where one party receives data from another, the receiving party becomes a Data Controller and therefore takes the liability for the data from that point, and is bound by the requirements of data protection legislation. All parties have their own data retention policies which they will follow.	Reduced	Low	Yes

Residual Risk Level	**Medium**

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:		
Residual risks approved by:		
DPO advice provided:	[redacted] and [redacted]	London Borough of Camden Information Rights Team Leader, and LOTI Data Sharing Project Manager / London Borough Of Barnet Deputy DPO
Summary of DPO advice: **Note that local DPOs for each organisation need to either adopt this DPO, adopt it with additions (see the DSA FAQ) or undertake their own.** There are some residual risks to this sharing which are unavoidable due to the nature of the sharing and the cosuanrns under which it will take place. However these are considered acceptable and proportionate when taken in context with the reasons for which the sharing will be undertaken. None of the risks are considered to be high risk or of serious concern.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
This DPIA will kept under review by:	The DPIA will be reviewed by the respective DPOs of each organisation when required	The DPO should also review ongoing compliance with DPIA