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.

Version Control

Version	Reason	Date	Author(s)
0.1	Draft - initial draft	March 2022	Sarah Laws
0.2	Comments	March 2022	Andrew Bessant
0.3	Comments	March 2022	Andrew Bessant and Sarah Laws

Project / Work Stream Name	**Environmental Crime Data Sharing Agreement**
Overview: (Summary of the project/work stream)	This DPIA covers the data sharing agreement [DSA] for the sharing of information by and between local authorities in London for the purpose of preventing, deterring, investigating and prosecuting environmental crimes. It is noted that there is an overlap between the responsibilities of the Environment Agency and local councils, and that information sharing between those is covered in a different DSA and outwith the scope of this DSA. The scope of environmental crime covers a wide range of activities from littering and dog fouling, to fly tipping which can include bulk disposal of contaminated materials, and illegal scrap metal activities. It also covers areas such as graffiti and similar defacements, abandoned vehicles, highways obstructions, unauthorised road side sales, pest control, and stray dogs. It is noted that bulk disposal of contaminated materials, and illegal scrap metal activities may be linked to Organised Criminal Gang activities. Road side sales (such as flower sellers, “squeegee wielders” and so on) may be linked to modern slavery and the road side sales can cause danger to the sellers as well as harrassment to motorists. Whilst the other areas covered by this DSA may not be considered to be serious offences, they are ones that can cause anxiety to residents and lead to detrimental environmental effects for residents. Councils receive many complaints about graffiti, abandoned vehicles, and dog fouling and these, and the other areas covered in this DSA are ones that frequently negatively affect local residents. Sharing information allows councils and agencies to take joined-up action and ensure the most appropriate course of action can be taken in respect of both individual cases and wider problems. Targeted actions can be coordinated, offenders located and prosecuted, and information shared to ensure that proportionate outcomes are pursued.

Implementation Date:	1/4/22
Environmental Scan 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.	Some sharing is likely to be taking place currently under local agreements or as DPA 18 disclosure requests. There are no known DSAs in place for this work. There is currently a draft (anticipated go-live Spring 2022) DSA between the Environment Agency and London councils to cover the EA's work **and this DSA has been written to exclude that scope.** Some sharing may involve CCTV footage which would be partly covered by the CCTV DSA. Some sharing, such as links to safeguarding issues, such as Prevention of Damage by Pest Act where there are vermin issues, may be linked to adult safeguarding concerns which would be covered by the Adult Safeguarding DSA. Similarly, roadside sales where there were OCG/modern slavery issues would have coverage of the safeguarding aspects under Adult Safeguarding or the MAS DSAs. This DSA covers the environmental aspects only and does not cover the safeguarding or CCTV aspects.

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?	No
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?	No
1.12	Exemptions and Exceptions	Does the project's justification include significant contributions to public security and measures?	No
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?	No

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 Depends on the council, for some it will be new.

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	possibly	Email address	yes	Postcode	yes
Other unique identifier (*please specify*)	yes*	Telephone number	yes	Driving licence number		NHS No		Hospital ID no	

Other data *(Please state):*

*reference numbers in relevant council databases or case management systems

Other data as necessary in appropriate cases:

- housing information
- financial information for example to show that waste was carried as a business activity
- images / video footage in Body Worn Video, photographs, film or CCTV, although note that this is fully covered in the CCTV DSA
- employment information
- any known risk the data subject may pose to council or Partner staff or others
- Vehicle details (inc VRN, make, model, registered keeper details)

		• information held in licence registers and provided as part of licensing applications whether successful or not • details of previous visits and inspections undertaken by the Party • details of complaints held by the Party where relevant to enforcement action being taken • information that would assist the Party in locating or identifying a suspected perpetrator or witness to a matter covered in this DSA • Information that would assist the Party in establishing that an offence has or has not been committed

Special Categories of Personal Data

Racial or ethnic origin	Yes in some cases where relevant	Political opinion		Religious or philosophical beliefs	
Trade Union membership		Physical or mental health or condition			
Sexual life or sexual orientation		Social service records		Child protection records	
Sickness forms		Housing records	Yes in some cases where relevant	Tax, benefit or pension records		Adoption records	
DNA profile		Fingerprints		Biometrics		Genetic data	
Proceedings for any offence committed or alleged, or criminal offence record *only where relevant to enviro crime or Partner officer safety					YES*
Other data *(Please state):*					

Will the dataset include clinical data? (please include)	**Yes/No** NO
Will the dataset include financial data?	YES in some cases

	Where relevant to the offence such as where a POCA application may be made, or where the provision of services such as illegal waste transportation is for cost is an aggravating factor, or where it may change the assessment of whether a prosecution is in the public interest or not.
	description of other data processed/shared/viewed? N/A

2.3	**<u>Business sensitive data</u>**			
	Financial		Yes	in some cases see 2.2 above
	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			

<table>
<tr><th colspan="4">Step 3: Describe the sharing/processing</th></tr>
<tr><td rowspan="4">3.1</td><td colspan="2" rowspan="2">List of organisations/partners involved in sharing or processing personal/special categories personal data? If yes, list below</td><td>Yes/No</td></tr>
<tr><td></td></tr>
<tr><td>Name</td><td>Controller or Processor?</td><td>Completed and compliant with the Data Security and Protection (DSP) Toolkit
Yes / No</td></tr>
<tr><td>London Local Authorities</td><td>Controller</td><td>Yes</td></tr>
<tr><td>3.2</td><td>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?</td><td colspan="2">Yes/No
Yes - A single DSA which is the subject of this DPIA will be put in place to cover sharing. Some councils may have outsourced some/all of their environmental functions and there will be Data Processing Contracts in place with any local Processors, with the council being the Data Controller for purposes of this DSA</td></tr>
<tr><td>3.3.</td><td>Has a data flow mapping exercise been undertaken?
If yes, please provide a copy, if no, please undertake</td><td colspan="2">The flows will vary case by case according to specific circumstances and case requirements</td></tr>
<tr><td rowspan="2">3.4</td><td colspan="2" rowspan="2">Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?</td><td>Yes / No</td></tr>
<tr><td>No, these are covered by existing arrangements and are not required for this DSA</td></tr>
<tr><td rowspan="2">3.5</td><td colspan="3">Describe in as much detail why this information is being processed/shared/viewed?</td></tr>
<tr><td colspan="3">This agreement covers the sharing of information by and between the listed agencies for the purpose of preventing, deterring, investigating and prosecuting environmental crimes. It is noted that there is an overlap between the responsibilities of the Environment Agency and local councils, and that information sharing between those is covered in a different DSA and outwith the scope of this DSA.

The scope of environmental crime covers a wide range of activities from littering and dog fouling, to fly tipping which can include bulk disposal of contaminated materials, and illegal scrap metal activities. It also covers areas such as graffiti and similar defacements, abandoned vehicles, highways obstructions, unauthorised road side sales, pest control, and stray dogs.

It is noted that bulk disposal of contaminated materials, and illegal scrap metal activities may be linked to Organised Criminal Gang activities. Road side sales (such as flower sellers, “squeegee wielders” and so on) may be linked to modern slavery and the road side sales can cause danger to the sellers as well as harrassment to motorists. Whilst the other areas covered by this DSA may not be considered to be serious offences, they are ones that can cause anxiety to residents and lead to detrimental environmental effects for residents. Councils receive many complaints</td></tr>
</table>

	about graffiti, abandoned vehicles, and dog fouling and these, and the other areas covered in this DSA are ones that frequently negatively affect local residents. Sharing information allows councils and agencies to take joined-up action and ensure the most appropriate course of action can be taken in respect of both individual cases and wider problems. Targeted actions can be coordinated, offenders located and prosecuted, and information shared to ensure that proportionate outcomes are pursued. The sharing will allow both partners to better deliver their statutory series and will allow more effective use of resources, giving more joined-up working which increases efficiency. The public will benefit from this approach, as services will be delivered in a more streamlined way that utilises the information shared to provide better tailored and appropriate services. The benefits of this DSA are to: • Cover the sharing of information for the prevention, detection, and prosecution of environmental crimes • Remove barriers to effective information sharing. • Sets parameters for sharing personal data and clearly identifies the responsibilities of organisations. • Identify the correct lawful basis to share personal information. • Ensure information is shared whenever there is a requirement to do so. • Enables authorities to share data on performance, quality assurance, learning and impact analysis. • Raises awareness amongst all agencies of the key issues relating to information sharing and gives confidence in the process of sharing information with others. • Allow agencies to deal more effectively with environmental crimes that cross agency boundaries • Allow agencies to have a fuller picture of environmental crimes that affect more than one borough, to allow appropriate action to be determined

Step 4: Assess necessity and proportionality	
4.1	**Lawfulness for Processing/sharing personal data/special categories of personal data?** **Part 2 Processing:** **It is likely that processing of personal data by the sharing party, and some processing by the receiving party will fall under Part 2 DPA18.** **Personal Data:** Article 6 1(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. The applicable laws are : Environmental Protection Act 1990 Clean Neighbourhoods and Environment Act 2005 Control of Pollution Act 1974 and Control of Pollution (Amendment) Act 1989 Refuse Disposal (Amenity) Act 1978 and Removal and Disposal of Vehicles Regulations 1986 Noise Act 1996 Town and Country Planning Act 1990 The Local Government (Miscellaneous Provisions) Act 1976 Highways Act 1980 Prevention of Damage by Pests Act 1949 Human Rights Act 1998 **Special Category Data** Article 9 2(g) **substantial public interest** - processing is necessary for reasons of substantial public interest, on the basis of 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 Use of Article 9 2(g) requires that the Data Protection Act Section 10(3) be satisfied. This requires that a condition within Schedule 1, Part 2 (substantial public interest conditions) is met. For this agreement these are: ● *Statutory etc., and government purposes under Para 6(1)(2)* ● *Preventing and detecting unlawful acts under Para 10(1)(2)(3)* **Criminal Offence data sharing** Article 10 processing is necessary to exercise official authority or as authorised by UK law. The processing shall be authorised by UK law under Article 10 where a condition within Schedule 1, Parts 1, 2 or 3 is met. For this agreement these are: the Substantial Public Interest conditions set out in Schedule 1, Part 2: ● *Statutory etc., and government purposes under Para 6(1)(2)* ● *Preventing and detecting unlawful acts under Para 10(1)(2)(3)* **It is likely that processing of the shared personal data by the receiving party will fall at least partly under Part 3 DPA18**

	The "competent authorities" are defined in Section 30 of the DPA which refers to Schedule 7. The competent authorities under this agreement are councils when acting under Part 3 and not Part 2. **Personal data lawful basis**: The "law enforcement" purposes are defined in Section 31 of the DPA as "*prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".* This applies to many of the offences under this DSA. **Sensitive data:** Where the information is Sensitive as defined in section 35(8) is processed then a DPA18 schedule 8 condition must be met. The sensitive data under this DSA would be data revealing racial or ethnic origin, or processing of data concerning health, where relevant in specific cases, although processing is expected to be minimal. The relevant conditions in Schedule 8 would be: ● Statutory etc. purposes Para 1(a)(b); ● Administration of justice Para 2 The processing must also be strictly necessary (relates to a pressing social need which cannot reasonably be achieved through less intrusive means).		
4.2	**Will the information be processed/shared electronically, on paper or both?**	Electronic	Yes
		Paper	No
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?**		
	Privacy notices for all organisations note law enforcement related sharing. 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, involve disproportionate effort, or would be exempt under the crime prevention exemptions.		Yes
4.5	**How will you help to support the rights of individuals?**		
	Each controller remains responsible for complying with the applicable data subject rights. Each council has established policies and procedures in place for 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?**		No
	N/A		
4.8	**Will individuals be asked for consent for their information to be processed/shared?**		No

	If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.	
	Consent is not the lawful basis for processing.	
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?**	
	Each authority has their own case management solution. Paper storage is minimised; all storage is UK only.	
4.11	**Data Retention Period** *How long will the data be kept?*	
	Each council will comply with their own data retention policies which may vary according to local requirements. .	
4.12	**Will this information be shared/processed outside the organisations listed above in question 3?** *If yes, describe who and why:*	Yes/No
	Some councils may have outsourced some or all of their environmental functions, others may have shared service arrangements. Outsourcing arrangements will have the providers as data processors of the council; shared services are likely to be joint data controllers. Information relevant to a prosecution may be shared further such as instructed external lawyers or counsel, the courts and defence lawyers.	Possibly
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.	Yes
5.2	**How will access to information be controlled?**	
	This varies 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)	
	Environmental officers which may have various job titles, lawyers and related professionals	
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	y	Smartcard		key to locked filing cabinet/room	
	Secure 1x Token Access		Restricted access to Network Files			y
	Other: *Provide a Description Below*:					

5.5	**Is there a documented System Level Security Policy (SLSP) (as named differently for different councils) for this project?** SLSP is required for new systems.	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 Mandatory Staff Training in place for the following?**	Yes/No	
	● Data Collection:	Yes	
	● Use of the System or Service:	Yes	
	● Information Governance:	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 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. Compliance risk: Appropriate technical and organisational measures shall be taken. Corporate risk: Reputational risk. Loss of trust. Legal implications.	Medium	High	Medium

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.	Medium	High	Medium/high
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	Medium	High	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. 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.	Medium	High	Medium/high
Inherent privacy intrusion: sharing of personal data is inherently privacy intrusive, especially for offences which are not particularly serious Compliance risk: dasta minimization, privacy intrusion Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications	High	High	High

Step 7: Identify Measures to reduce 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: .	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. Breaches of those would be a disciplinary offence and may be a criminal act.	Reduced	Low	Yes
Loss of data in transfer.	The DSA specifies the appropriate technical measures in place to ensure the security of the data transfers. Organisations have full policies and procedures in place for the safe transfer of data. Councils routinely share volumes of special category data and have well established protocols to do so safely.	Reduced	Low	Yes
Further transfer 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 full policies and processes in place to ensure data is handled securely. Systems are auditable and RBAC is in force. Employees are subject to robust employment checks. 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 liability data protection wise. For the data in this DSA it is considered these risks are low.	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
Inherent privacy intrusion	The risk is the sharing with and by councils **not** the existing processing for enviro crime which are covered by other DPIAs. A degree of privacy intrusion is unavoidable, otherwise the sharing could not be facilitated. Where the offences are more serious then intrusion is more proportionate. However it is noted that even minor offences such as graffiti can have negative consequences on many people in a locality and these are often matters of general public concern. 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.	Reduced	Medium	Yes

Residual Risk Level	**Medium**

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:	Sarah Laws Andrew Bessant	Note that each Data Controller's IAO needs to ensure they accept these
Residual risks approved by:	Sarah Laws Andrew Bessant	Note that each Data Controller's IAO needs to ensure they accept these
DPO advice provided:	Sarah Laws Andrew Bessant	Data Protection Manager, LB Camden Information Governance Manager, LB Richmond and Wandsworth
Summary of DPO advice: *Please see the FAQs on how councils should adopt/adapt this DPIA or undertake their own.* This is assessed as medium risk although it is noted only one residual risk scores medium. The inherent privacy intrusions are considered proportionate to the aims of the processing and bearing in mind the procedures and processes in place to ensure data minimisation and proportionality.		
Comments: Accepted by Andrew Maughan Data Protection officer March 2022		
This DPIA will kept under review by: [redacted]	The DPIA will be reviewed by the respective DPOs of each organisation when required	The DPO should also review ongoing compliance with DPIA