Guide to pan-London DSA template

The Pan-London Data Sharing Agreement (DSA) Template is used as part of the Pan-London Data Sharing Project, when multiple London boroughs are sharing data among themselves or with other parties. The template is used often where London boroughs and the Metropolitan Police are sharing data.

If you want to use this template to document data sharing taking place with multiple London borough councils, speak to the Pan-London Information Governance Lead. They will explain the process and help you identify the engagement you need with the different parties.

If one of the parties to the DSA is the Metropolitan Police (MPS), then a lead officer from the police must speak to the MPS Office of the Data Protection Officer (OoDPO) before you begin work on drafting the DSA. The MPS lead must identify an MPS Senior Responsible Officer (SRO) for the DSA at Director or Commander level. The SRO must take responsibility for agreeing the DSA and associated risks.

A DSA can cover sharing across a wide subject area, such a child safeguarding or licensing. Where the content and context of the sharing is different in different circumstances, such as different types of meetings, description of the datasets should be provided within the appendices of the DSA (where appropriate), to specify the data that will be shared in agreed circumstances. The OoDPO will help you decide when this is necessary. This encourages the sharing of only what is necessary in each case. The DSA is agreed once by all parties, so these descriptions are expected to apply throughout the life of the DSA.

General

Text highlighted in yellow is either an instruction or is used to show where you need to add text. Delete the yellow prompts when the DSA is complete.The template cannot be changed outside of these highlighted sections, because it has been agreed by all parties.

If you have used the pan-London DPIA template, then much of the content can be copied from there into the DSA template. Check to ensure everything is correct.

Transparency

It is expected and encouraged that the DSA will be published by each party, as part of public sector transparency. In rare cases, some aspects of the DSA may be redacted. The parties should agree to this before the DSA is complete. If a copy is requested under FOI or business as usual, the final decision to disclose or not will lie with the receiving party as the legal duty lies with them. However, each party will seek advice/opinion from the other parties where there is concern about that information being released and any impact it is likely to have.

It is expected that data shared under this DSA would not be released under FOI as the personal data exemption will most likely apply.

Summary

This is an at-a-glance record of the DSA. If all the London boroughs are party to the agreement you do not need to list them individually. Instead say 'London boroughs'.
If you have many pieces of applicable legislation, please list the main ones. The detail is described in the appendices.

1.2 Parties to this agreement

Your DPO and/or the Information Governance officers on the working group developing the DSA, will help you establish the type of relationship between the parties.

Joint data controllership can only exist for Part 3 processing if all parties are processing for law enforcement purposes.

If there is a joint controller relationship, you must clearly define in each section of the DSA which controller is responsible for each controller obligation, such as system security.

2.1 Purpose

Describe the purposes for each party to share the personal data and explain where the purposes come from. This usually means naming the legislation and explaining what it means, explaining the statutory guidance, or describing the organisation's priorities. Insert a full description of the purposes for each party or type of party. Explain why you cannot achieve these aims without sharing the personal data. This section may expand to several pages, depending on the breadth and complexity of the data sharing.

2.1.1 Serious Violence Duty

This section will only be relevant where the Serious Violence Duty applies to at least some of the data sharing. This section will generally only be needed where a local authority's Community Safety Team and/or Youth Offending Team is involved. You can delete the section if this doesn't apply to the DSA.

2.2 Benefits

Describe the benefits for each of the three groups; individuals; parties and society. You may use bullet points or subheadings (especially if the benefits differ between parties), but you must clearly describe what benefits you expect to achieve from sharing the data. At what point are the benefits expected to be achieved? This section may expand to several pages, depending on the breadth and complexity of the data sharing.

2.3 DPIA

For a pan-London DSA, the working group completes a Data Protection Impact Assessment (DPIA) for the DSA. The parties to the DSA may use that DPIA in its entirety, adapt it to fit that party's template and risk tolerances, use their own process and template, or not undertake a DPIA. The responsibilities, drivers and circumstances of all the parties must be considered in the DPIA.

If the DSA involves the Metropolitan Police then the lead on the DSA for the police must also speak to the OoDPO to undertake a DPIA following the MPS process. There will be some duplication between the DPIA completed by the working group and the DPIA completed by the MPS, as both need to document the activities and responsibilities of all parties.

2.4.1 Part 2 processing

The most likely lawful basis conditions are listed in the template. Delete the unnecessary ones.

Consent is not generally the lawful basis that public sector organisations use for processing personal data. The parties will often work collaboratively with data subjects and aim for agreement with them on the actions to be taken. However, it is recognised that this is different to using consent (Article 6 (a)), explicit consent (Article 9 (a)), or consent for law enforcement processing (DPA 2018 Pt 3 Ch2 s35 2(a)) as the lawful basis conditions.

Speak to your Data Protection Officer and/or the Pan-London Information Governance Lead if you feel consent may be the lawful basis.

2.4.2 Part 3 processing

The police usually process personal data for law endorsement purposes, but local authorities do in some circumstances. Your DPO will provide advice on when this applies to your activities. If the DSA includes processing for law enforcement purposes then you must list the relevant parties and their purposes in the table.

There are additional safeguards required for 'sensitive processing'. It is expected that a pan-London DSA involving law enforcement processing will include sensitive processing. This is defined in Section 35(8) as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

One of either Section 35(4) or (5) must apply. Both require an appropriate policy document to be in place and your DPO will know about this.

Section 35(4) requires the consent of the data subject, which is not generally used by parties to pan-London DSAs, and 35(5) requires that the processing be 'strictly necessary' for the law enforcement purposes, and meets a condition in Schedule 8. The competent authorities that are party to this DSA consider the data sharing to be 'strictly necessary' and do not consider that there are less intrusive means of obtaining personal data held by partners.

If any of the parties are processing data for law enforcement purposes, then this should be noted in Appendix A.

2.4.3 Applicable legislation

You should know what legislation or statutory guidance applies to your work. The applicable legislation must be listed in the appendices, with details of how it applies to the sharing. You must provide the name of legislation and explain which sections apply and how. If you have used the DPIA template, then you can copy over the table from section 2.5.4 in the DPIA template.

2.5 Proportionality and necessity

You should only share the minimum amount of personal data necessary to achieve your purposes. You need to explain how you minimised the data needed

and any plan you have to anonymise or pseudonymise the data at any stage of its use.

Your sharing of the data should be proportionate, so that the necessity of processing and sharing the data balances against its sensitivity and the privacy rights of individuals. Describe why you consider the data sharing to be proportionate. This section may expand to several pages, depending on the breadth and complexity of the data sharing.

The DSA can cover sharing across a wide subject area, such a child safeguarding or licensing. Where the content and context of the sharing is different in different circumstances, such as different types of meetings, description of the datasets should be provided within the appendices of the DSA (where appropriate), to specify the data that will be shared in agreed circumstances. The OoDPO will help you decide when this is necessary. This encourages the sharing of only what is necessary in each case. The DSA is agreed once by all parties, so these descriptions are expected to apply throughout the life of the DSA.

2.6.1 Common law duty of confidence

The common law duty of confidence does not come from data protection legislation.

The word 'confidential' can mean different things to different people.

- Personal and special category data as defined by data protection legislation.
- Patient Identifiable Information (PII) or 'personal confidential information'; both terms most commonly used in health settings.
- Information which is not lawfully in the public domain or readily available from another public source.
- Where the person giving the information could reasonably expect that it would not be shared with others.

A duty of confidence arises where it is reasonable for a data subject to expect that the information will be kept confidential. As it is mostly public sector organisations that use this template, it is likely that a duty of confidence applies to at least some of the data shared under the DSA. The parties have already decided that there is a suitable override for the duty of confidence if they are creating a DSA. The appropriate override must be listed in the DSA.

Implied consent for overriding the duty of confidence is different to consent as a lawful basis for processing personal data.

Where a duty of confidence does not apply to the data shared under this DSA, this section can be deleted.

3.1 Data subject rights and complaints

The parties must describe how they meet their duties for individual rights, including where one or more parties is responsible for meeting a right on behalf of other parties, such as in a joint controller relationship. For example, one party may be solely responsible for responding to subject access requests for all parties, or ensuring suitable security for a shared system.

Privacy notice(s) can be provided through:

- Pages on a website
- Information leaflets or posters
- Letters, emails or texts
- Social media campaigns
- Verbal explanation
- Other

Describe these for each party in Appendix C and provide a link to a website notice or describe where it will be displayed and which party or parties is/are responsible for providing it.

The right to object only applies if the lawful basis is Article 6(e) public task or Article 6(f) legitimate interests. Mark that row as ‘does not apply’ if you are not using those lawful bases.

In some cases, it may not be appropriate to specifically inform a person that information about them is being processed and shared. Consideration should be given to whether notifying the individual may place someone at risk or prejudice a police or safeguarding investigation. In these circumstances, the parties need not inform individuals that the information is being processed/shared, but should record locally, their reasons for sharing information without making the individual aware.

The expectation of transparency when processing personal data under Part 2 of the Data Protection Act 2018 does not occur in the same way when processing under Part 3 for law enforcement purposes. You may not identify to a specific individual that you are processing their personal data, but you are still expected to explain in general terms, through privacy notices, why your organisation processes personal data.

3.2 Data subjects

Delete the options not applicable to the DSA. Add text to describe the data subjects more fully. For example, in the 'customers etc' field, state that they are adult social care clients.

4.2 The data to be shared

You can delete any data items that will not be shared under the DSA. You need to describe the specifics of the data that will be shared. This is particularly important where the police are a party to the sharing or where different parties access only some of the data items shared under the DSA.

Where the content and context of the sharing is different in different circumstances, such as different types of meetings, description of the datasets should be provided within the appendices of the DSA (where appropriate), to specify the data that will be shared in agreed circumstances. You may wish to develop operational documents that specify the data to be shared in select scenarios. For example, data shared between police and local authorities within a Multi-Agency Safeguarding Hub (MASH).

4.3 Storing and handling information securely

You need to describe the following, where relevant: data format; location of data; data flows (attach images if available); roles and access and access controls.

Describe the data security standards and which party has responsibility, whether for data they hold or data within a shared system or database - this should include reference to encryption, password protection, role based access controls (RBAC), restricted physical access, business continuity plans and security policies.

Describing the data flows, storage locations and role-based access controls fully is especially important for data shared for law enforcement purposes, to allow parties to demonstrate that the sharing is specific to the recipient and purpose, and necessary and proportionate for the stated law enforcement objective.

The following are standards for security of data.

Electronic records

All personal data held electronically will be stored in a secure area with password protected entry, audit records, and appropriate back-up functionality. All laptops, computers, and any other portable devices will be encrypted. Access will immediately be removed where an individual no longer needs it. Parties must ensure the chosen transfer method is suitably secure and that access is only provided to those who need it. Unencrypted email (i.e. sent in plain text over the public internet) must not be used to share information under this DSA. Sharing methods that may be appropriate include:

- Email encryption tools where the email and attachments are encrypted from named sender to named recipient.
- Encryption via Transport Layer Security (TLS) where the email and attachments are encrypted in transit over the internet. Both the sender and recipient email domains must have TLS enabled. This can be checked using https://www.checktls.com/
- Secure corporately managed data repository and sharing platforms (e.g. MS Teams; Google Docs)
- Secure group email services (eg CJSM: https://cjsm.justice.gov.uk/index.html)
- Secure File Transfer Protocols
- Virtual Private Networks

The above are examples, get advice from your organisation's information security or IT teams on secure methods of sharing available at your organisation and document these in the organisation's process documents.

Phone/virtual meetings/face-to-face meetings

Information may be shared over the phone, in a virtual meeting, or at face to face meetings. Meeting attendance and distribution of content, eg meeting minutes or recordings, must be limited to those with a need to know. Sharing by telephone should be avoided unless the requirement is urgent and email is not practicable.

Individuals should be aware of their surroundings and the presence of other individuals or voice recognition or 'Internet of Things' devices (eg virtual assistant apps like Alexa, Cortana, SIRI) to ensure they aren't overheard by those that should not have access to the information discussed.

Paper records

Paper records must be minimised and kept secure whether in the office, home or during transit. Organisations must adopt an appropriate policy for the use, transfer and disposal of paper records.

4.4 Outside UK processing

It is unlikely that any data shared under this agreement will be processed outside the UK, but each party must check, especially for locations of cloud storage or similar. Delete this section if not needed.

4.5 Data quality

You should describe the actions taken by each party to ensure adequate data quality and precision, including actions taken to ensure that any data matching is effective. You may wish to add bullets or sub-headings to identify the actions of each party.

4.6 Data breaches and incidents

You may draft specific action trees or processes for specific types of data or types of incident. For example, where police or social care is involved that could lead to the likelihood of severe harm.

4.7.1 Retention periods

You may simply list the standard organisational retention period for a type of data, such as 7 years for financial data, or you may need to describe specific periods relevant to the DSA.

4.7.2 When sharing ends

This may be that each controller continues to hold the data for the stated retention period(s), or there may be something specific for the DSA.

5.1 Appendix A: Parties to this agreement

Describe each party, its duties in the topic areas covered by this DSA, and whether they are acting as a competent authority to process data for law enforcement purposes.

Local Partners

As described in 1.2, local partners are not specifically named on the DSA when it is published. However, it may be accepted that a type of organisation will be a local partner. For example, multiple London Boroughs are expected to employ NHS Trusts to deliver substance misuse treatment services. Where this is expected, you should list in the table the type of organisation expected to be a local partner.

5.2 Appendix B: Applicable legislation

Describe each piece of legislation or statutory guidance, the party to which it applies, the main purpose of the legislation including section numbers etc to identify the specific duty, and how the legislation and duties applies to the data shared under this DSA.

5.3 Appendix C: Data subject rights

Describe how each party meets the data subject rights, including links to online privacy notices and any relevant processes.

5.3 Appendix D: Detailed guidance on appropriate data sets for MPS Officers

For a DSA with the Metropolitan Police as a party, it is expected that, where relevant, description of the datasets should be provided within this appendix. The OoDPO will help you decide when this is necessary. This encourages the sharing of only what is necessary in each case. The DSA is agreed once by all parties, so these descriptions are expected to apply throughout the life of the DSA.