**DPIA for Pan-London Data Sharing - Name of DSA**

| **Version** | **Reason** | **Date DPO Reviewed** | **DPO Name** | **Organisation** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

# Summary and parties

| **DSA Name** |  | **Anticipated Start Date** |
| --- | --- | --- |
|  |
| **Summary** |  | |

## **Screening**

|  | **Category** | **Screening question** | **Describe - or mark N/A** |
| --- | --- | --- | --- |
| 1.1.1 | Individuals | Will you process data concerning vulnerable data subjects, or where there is an imbalance of power eg children, older adults, domestic abuse victims or employees*?* |  |
| 1.1.2 | Individuals | Will you process personal data without providing a privacy notice directly to the individual eg investigations or covert surveillance? |  |
| 1.1.3 | Individuals | Will the processing prevent data subjects from exercising a right or using a service or contract? |  |
| 1.1.4 | Individuals | Will the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions? |  |
| 1.1.5 | Individuals | Will you process personal data that could result in a risk of physical harm to the data subject in the event of a security breach eg fraud investigations, domestic abuse, child exploitation, witness or complainant data? |  |
| 1.1.6 | Individuals | Will you track individuals’ online or offline locations or behaviour eg vehicle tracking, an appointment or activity tracking system, a lone worker system or monitoring an individual’s social media? |  |
| 1.1.7 | Data | Will you process special category data or criminal offence data on a large scale? |  |
| 1.1.8 | Data | Does the project involve new identifiers or re-use of existing identifiers eg NHS or NI number, council tax reference, passport number? Will you use intrusive identification or identity management processes? |  |
| 1.1.9 | Data | Will you process personal data for a different purpose than that it was originally collected or used? |  |
| 1.1.10 | Data | Does the project involve inter-linking, cross referencing or matching of personal data from multiple sources? |  |
| 1.1.11 | Data | Will you process biometric or genetic data eg fingerprints/facial recognition? |  |
| 1.1.12 | Data | Will personal data be processed out of the UK, and by whom? |  |
| 1.1.13 | Purpose | Will you be marketing/promoting paid for activities, commercial opportunities from other organisations, or charitable aims? |  |
| 1.1.14 | Purpose | Will the processing involve the 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 safety? |  |
| 1.1.15 | Technology | Does the processing use new or additional information technologies such as AI or smart tech? |  |
| 1.1.16 | Technology | Will decisions be made solely by automated processing, so that a person isn’t involved before a decision is made? |  |
| 1.1.17 | Technology | Will you use profiling to:   * collect and analyse personal data on a large scale, using algorithms, AI or machine-learning; * identify associations to build links between different behaviours and attributes; * create profiles that you apply to individuals; or * predict individuals’ behaviour based on their assigned profiles |  |
| 1.1.18 | Technology | Will you systematically monitor a publicly accessible place on a large scale eg CCTV? |  |
| 1.1.19 | Exemptions and Exceptions | Does the project relate to data processing which is in any way exempt from legislative privacy protections? |  |
| 1.1.20 | 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? |  |

## Parties

We need to be clear which organisations are involved and what relationships exist.

### Parties

Which parties will be involved in the data sharing?

| **Organisation name or type** | **Brief description of duties relevant to the data sharing** |
| --- | --- |
| Metropolitan Police | * The prevention and detection of crime * The maintenance of the King’s peace * Protection of the vulnerable |
| London Borough  (state all or name each borough involved) | * Co-ordinates, gathers, processes, risk assesses and shares information held about all the areas covered in the DSA in conjunction with information received from partner agencies, to enable the council to undertake its statutory duties in these areas * Makes decisions on whether to undertake enforcement or other appropriate actions under its powers in the legislation listed in this DSA * Allocates resources in accordance with priority of tasks and policies * Co-ordinates, gathers, processes, risk assesses and shares information covering all the areas under this DSA with partners to achieve common goals * Undertakes interventions as necessary to ensure the safeguarding of vulnerable people * Decides whether to undertake prosecutions when offences covered by the legislation in this DSA has been breached and it is within the council’s remit * Takes appropriate and proportionate steps to ensure the safety of employees and others |
|  |  |

### Relationships

What is the expected relationship between the parties? Are the parties individual controllers or joint controllers?

| **Describe the relationships** egController to Controller or Joint Controllers? | |
| --- | --- |
|  | |

### Data processors

Does the project involve employing contractors (data processors) who will have access to and process the personal data? Is there an existing contract or will one be created? Which party is responsible for the contract, due diligence and contract monitoring?

| **Describe** | |
| --- | --- |
|  | |

# Purpose and benefits

## Purpose and background

Why are you undertaking this work? What are the aims of the processing, are there drivers from legislation? How does the processing achieve your purpose? Describe the consultation or checks that have been carried out regarding this work.

| **Describe** | |
| --- | --- |
|  | |

## Proportionality and necessity

How have and how will you consider proportionality and necessity when sharing under this DSA? Why is it necessary for you to process the personal data to achieve your aim? Can data be anonymised or pseudonymised? How will you ensure you only use the minimum amount of data required to complete the aim(s)?

| **Describe** | |
| --- | --- |
|  | |

## Effects on individuals

What is the intended effect on individuals? Would individuals expect you to process their data in this way? Will your processing prevent individuals from exercising a right, or using a service or contract? eg will they gain or lose access to a benefit or service, be prosecuted or fined, receive support? Will individuals in society more broadly benefit, for example, from lower crime rates?

| **Describe** | |
| --- | --- |
|  | |

## Benefits

Describe who will benefit from the data sharing and how. It is expected that there are benefits for each of the sections below.

| **Individuals** |
| --- |
| [Suggestions to be expanded]   * receipt of better-tailored services * improved wellbeing * improved support to treat substance misuse |
| **Parties** (name the relevant party and the benefit) |
| [Suggestions to be expanded]   * more effective use of resources * ability to plan use of resources * ability to deliver statutory duties |
| **Society** |
| [Suggestions to be expanded]   * more effective use of resources * reduction in crime or fear of crime * reduced cost for treating substance misuse |

## Lawful basis

Speak to your Data Protection Officer or DP lead about completing this section.

### Part 2 processing

| **Article 6 lawful basis conditions** [delete unnecessary options] | **Applicable party** |
| --- | --- |
| c) legal obligation |  |
| e) performance of a task carried out in the public interest |  |
| f) purposes of the legitimate interests |  |

| **Article 9 lawful basis conditions** [delete unnecessary options] | **Applicable party** |
| --- | --- |
| f) necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity |  |
| g) substantial public interest |  |
| h) 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 |  |
| i) 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 |  |
| j) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes |  |

| **Article 9(2) (b) (h) (i) (j) - Sch 1 Pt 1** [delete unnecessary options] | **Applicable party** |
| --- | --- |
| Employment, social security and social protection |  |
| Health or social care |  |
| Public health |  |
| Research |  |

| **Article 9(2) (g) - Sch 1 Pt 2** [delete unnecessary options] | **Applicable party** |
| --- | --- |
| Statutory & government purposes |  |
| Equality of opportunity or treatment |  |
| Preventing or detecting unlawful acts |  |
| Regulatory for unlawful acts and dishonesty |  |
| Preventing fraud |  |
| Safeguarding of children and individuals at risk |  |
| Administration of justice |  |
| Racial/ethnic diversity at snr mgmt |  |
| Protecting the public against dishonesty |  |
| Terrorist financing or money laundering |  |
| Support for individuals with disability or medical condition |  |
| Safeguarding economic well-being |  |

### Criminal data

| **Criminal data - Sch 1 Pt 3** [delete unnecessary options or whole table if inapplicable] | **Applicable party** |
| --- | --- |
| Legal claims |  |
| Accounts for child indecency offences |  |
| Judicial acts |  |
| Extension of Sch 1 Pt 2 |  |

### Part 3 processing for law enforcement purposes [delete this section if inapplicable]

| **Name the parties that are competent authorities** |
| --- |
|  |

| **Sch 8 Law enforcement conditions** [delete unnecessary options or whole table if inapplicable] | **Applicable party** |
| --- | --- |
| Statutory purposes |  |
| Judicial acts |  |
| Legal claims |  |
| Archiving |  |
| Administration of justice |  |
| Safeguarding of children and individuals at risk |  |
| Preventing fraud |  |

### 

### Legislation

Describe what duties or allowances come from legislation and/or statutory guidance that applies to this data sharing. You may also refer to mission statements or terms of reference that influence why you wish to share personal data.

| **Legislation/Statutory guidance** | **Party to which it applies** | **Main purpose of Legislation** | **How it applies to this data sharing** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Proportionality and necessity

**Describe how proportionality and necessity have been and will be considered when sharing under this DSA. Can personal data be minimised?**

|  | |
| --- | --- |

### Duty of confidentiality [delete this section if inapplicable]

**Override for duty of confidentiality** [delete unnecessary options]

| Not applicable |
| --- |
| Implied consent |
| Explicit consent |
| Section 251 support (this means you have support from the Secretary of State for Health and Care or the Health Research Authority) |
| Legal requirement (law that requires data sharing. **State the legal requirement below.**) |
| Overriding public interest (eg to prevent or detect a serious crime or to prevent serious harm to another person, balanced against the public interest in maintaining public confidence in public sector organisations. **State the justification below.**) |
| Not applicable (the duty doesn’t apply or you are not proposing to use health and care data.) |

# 

# Individuals

## Data subject rights

How will you meet data subject rights?

| **Individual right** | **Party or type of party** | | **How the party complies** (or state not applicable if the right does not apply) |
| --- | --- | --- | --- |
| **The right to be informed** about the collection and use of personal data – privacy information. |  | |  |
| **The right of access** to details of data use and to receive a copy of their personal data, commonly called a subject access request. |  | |  |
| **The right to rectification** to have inaccurate personal data rectified or completed if it is incomplete. |  | |  |
| **The right to erasure**  (Does not apply when using the lawful basis conditions of Article 6: legal obligation, public task or legal claims, or Article 9: health and care services, public health or archiving, research or statistical purposes.) |  | |  |
| **The right to restrict processing**  and limit how their data is used. | Does not apply to this DSA. | | |
| **The right to data portability** to obtain and re-use their personal data. | Does not apply to this DSA. | | |
| **The right to object** to the use and sharing of personal data where the parties are using the public interest or legitimate interests conditions It is unlikely that an objection would be upheld but each request must be considered on a case-by-case basis. |  |  | |

## 

## Types of data subjects

**Whose data will be shared?** [delete unnecessary options]

| Customers, service users, clients or residents | Licence and permit holders |
| --- | --- |
| Service provider/contractor staff | Employees |
| Patients | Witnesses |
| Complainants and enquirers | Victim/complainant of crime |
| Carers/Guardians/Family/Support network/Next of Kin | Actual or suspected offenders or perpetrators |
| People in images in photographs, film, body worn/dashcam footage, CCTV, or audio recordings | Advisers, consultants and professional experts eg doctor, social worker, police officer, lawyer |
| Visitors | Volunteers |
| Traders or people subject to inspection | Councillors, MPs, elected officials |
| Students | Supporters or group members |

| **Describe (**explain the types of data subjects) | |
| --- | --- |
|  | |

# Data

## Data categories [Delete unnecessary options]

(include pseudonymised or anonymised if any part of the data or outputs will be non-identifiable.)

| **Part 2 processing** | **Part 3 processing** |
| --- | --- |
| Personal data | Personal data |
| Special category data | Sensitive data |
| Criminal data | Pseudonymised data |
| Pseudonymised data | Anonymised/Aggregate data |
| Anonymised/Aggregate data |  |

| **Describe any anonymisation or pseudonymisation of data or outputs** (for pseudonymised data include details of which organisation holds the key to re-identification) |
| --- |
|  |

## The data to be shared

### Personal data [Delete unnecessary options]

| Name | Social care information |
| --- | --- |
| Address | Human Resources information |
| Contact details (phone/email) | Employment |
| Postcode | Social media names and activity |
| Partial postcode | Education information |
| DOB | GP (or other medical professional) contact details |
| Age | Support network |
| Gender | Housing information |
| Financial information incl pension records | Legal or personal representative incl Power of Attorney |
| Property information / ownership | Images in photographs, film, body worn/dashcam footage, CCTV, or audio recordings |
| Family / relationship information incl next of kin | Referral / Assessment information |
| Location data eg GPS or IP address | Referees |
| NHS number | Copies of ID like passport or driving licence |
| Any unique reference number (describe below) | Physical description |
| Other (describe below) |  |

| **Describe the data** (are there datasets or named reports? Is there any data specifically excluded?) |
| --- |
|  |

### Special category data [Delete unnecessary options]

| **Type of data** | **Describe the data** - datasets, named reports, social care records, sickness forms. Is any data specifically excluded? |
| --- | --- |
| Information relating to an individual’s physical or mental health or condition |  |
| Biometric information to uniquely identify an individual eg fingerprint or facial recognition |  |
| Genetic data eg a DNA sample |  |
| Information relating to an individual’s sexual life or sexual orientation |  |
| Racial or ethnic origin |  |
| Political opinions |  |
| Religious or philosophical beliefs |  |
| Trade union membership |  |

| **Describe the data** (are there datasets or named reports? Is there any data specifically excluded?) |
| --- |
|  |

### Criminal data

| Y | N | Information relating to criminal or suspected criminal offences |
| --- | --- | --- |

| **Describe the data** (are there datasets or named reports? Is there any data specifically excluded?) |
| --- |
|  |

## 

## Storing and handling information securely

### Data format

| **Describe the data formats** (eg electronic, paper, visual or audio. ) | |
| --- | --- |
|  | |

### Location

| **Where will the data be stored? (**eg business system, shared database, cloud, office) | |
| --- | --- |
|  | |

### Data flows

| **Describe or attach images of data flows** | |
| --- | --- |
|  | |

### Roles and access

| **What roles will have access to the information? (**list individuals or staff groups) | |
| --- | --- |
|  | |

| **How will access to information be controlled?** | |
| --- | --- |
|  | |

| **What is in place to audit access to the data / system?** | |
| --- | --- |
|  | |

| **Are there planned reports or dashboard outputs? (**What roles will be able to run reports? What roles will receive the report or where will it be published? Will data be person-identifiable, pseudonymised or anonymised format?) | |
| --- | --- |
|  | |

### Business continuity

| **What Business Continuity Plans (BCP) and Disaster Recovery Plans for the proposed/existing system or process?** | |
| --- | --- |
|  | |

### Security

| **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.) | |
| --- | --- |
|  | |

## Data quality

| **Describe how data quality and accuracy will be checked and assured** (will you use standardised formats, how will you check the accuracy of data matching, which party is responsible?) | |
| --- | --- |
|  | |

## Data breaches/incidents

| **Describe how incidents will be handled** (which party is responsible for what? Is one party responsible for a system or database?) | |
| --- | --- |
|  | |

## Retention and disposal

| **Data/Organisation** | **Retention period** | **Automated or manual deletion? What processes ensure that disposal happens at the allotted time?** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### 

### When sharing ends

The parties must agree what happens to the shared data once the data sharing activity ends. If this is ongoing sharing, please specify.

| **Describe** | |
| --- | --- |
|  | |

# Risk

Risks here are risks of this sharing. Signatories should have DPIAs for their own individual systems and methods, covering their local risks.

|  | | **Likelihood of harm** | | | | |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **Very unlikely to occur** | **Unlikely** | **Likely** | **Highly** | **Certain** |
|  | | **Likely** |
| **Impact of harm** | | **1** | **2** | **3** | **4** | **5** |
| **No impact** | **1** | 1 | 2 | 3 | 4 | 5 |
| **Minor** | **2** | 2 | 4 | 6 | 8 | 10 |
| **Detrimental** | **3** | 3 | 6 | 9 | 12 | 15 |
| **Serious** | **4** | 4 | 8 | 12 | 16 | 20 |
| **Catastrophic** | **5** | 5 | 10 | 15 | 20 | 25 |

| **Describe source of risk and nature of potential impact on individuals.** | **Likelihood of harm** | **Severity of harm** | **Overall risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** |
| --- | --- | --- | --- | --- | --- | --- |
| 1-5 | 1-5 | 1-25 | Reduced  Tolerated | 1-25 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Outcomes

It remains the duty of any party to the pan-London DSA to ensure it has met its duties under data protection legislation.

This DPIA has been developed by those officers who are members of the working group for the pan-London DSA. A DPO from a London borough that is involved in the development of the pan-London DPIA and DSA will provide advice below that is applicable to the data sharing. Each party can then decide whether to:

* adopt and record this DPIA in it current format
* use this DPIA with a ‘top-up’ specific to them
* create or amend its own DPIA
* decide a DPIA isn’t necessary

| Name of DPO |  |
| --- | --- |
| DPO Organisation |  |
| Date of DPO Advice |  |
| DPO Advice | |
|  | |
| Actions required for the data sharing to occur | |
|  | |