# SAVVI - Information Governance Framework

| revision | on | by | note |
|---|---|---|---|
| 1 | 09/03/2021 | Paul Davidson, SAVVI | 1st draft |
| 2 | 15/03/2021 | Paul Davidson | Restructure |
| 3 | 04/07/2022 | Nailah Ukaidi ( Nyela IG Consultants ) | Review - Update to content |
| | | | |

# About

This document describes the SAVVI Information Governance Framework.

SAVVI is the '**S**calable **A**pproach to **V**ulnerability **v**ia **I**nteroperability'. SAVVI proposes

- a SAVVI Process - to find, assess, and support vulnerable people
- a SAVVI Data Standard - in which data can be shared across the Process
- a SAVVI Catalogue - listing good examples of how SAVVI has been used.

See the SAVVI website at http://www.savviuk.org

Personal data is re-used, shared, and analysed, to find potentially vulnerable people; and then new data is generated or created, and passed to a network of organisations to provide support.

This SAVVI IG Framework recommends the steps to take throughout the process so that information is handled legally and ethically.

# References

This framework makes reference to ...

| | |
|---|---|
| [1] | The ICO Data Sharing Code of Practice |
| [2] | ICO Guide to the UK General Data Protection Regulation (UK GDPR) including DPA 2018 |
| [3] | Data Sharing process proposed by Greater Manchester Health and Social Care Partnership |
| [4] | Government Data Quality Framework |
| [5] | Digital Economy Act 2017 - Code of Practice |
| [6] | GOV.UK Data Ethics Framework |
| [7] | Algorithmic Transparency Standard |
| | |

# Principles

This SAVVI Information Governance Framework speaks to the ICO's Data Sharing Code of Practice [1]:

- "Data protection law is an enabler for fair and proportionate data sharing, rather than a blocker."
- "The accountability principle means that Controllers / Processors are responsible for compliance, and must be able to demonstrate that compliance."
- "Controllers / Processors must share personal data fairly and transparently."
- "Controllers / Processor must identify at least one lawful basis for sharing data before they start any sharing."

- “Controllers must process personal data securely, with appropriate organisational and technical measures in place.”

# Compatible Purposes

SAVVI relies upon the re-use / repurposing of data already being used for a specific purpose. Controllers / Processors can only use the personal data for a new purpose if:

- the new purpose is not incompatible with the original purpose,
- Consent for the new purpose has been obtained, or
- there is a clear obligation or function set out in law.

To ascertain whether processing for another purpose is compatible (not incompatible) with the original purpose for which the personal data are initially collected, the Controller should take into account, inter alia:

- any link between the original purpose and the new purpose;
- the context in which the personal data was originally collected – in particular, the Controller(s)’ relationship with the individual(s) and what they would reasonably expect;
- the nature of the personal data – e.g. is it particularly sensitive;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards – e.g. encryption or pseudonymisation.

As a general rule, if the new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is likely to be incompatible with the original purpose.

Source: ICO Guide to the UK General Data Protection Regulation (UK GDPR) [2]:

# Roles

The SAVVI Process already defines the roles of the organisations involved in a Vulnerability Initiative. These definitions are found in the SAVVI Glossary.

| | |
|---|---|
| @LeadOrganisation | An organisation responsible for coordinating a vulnerability initiative. |
| @SourceOrganisation | An organisation that provides @Attribute data. |
| @ResponsibleOrganisation | An organisation which is made responsible for a @Case. |
| @DeliveryOrganisation | A service provider who delivers actions that respond to a @Need |

In summary

- A @LeadOrganisation will establish a vulnerability initiative, and will ask a number of @SourceOrganisations to share @Attribute data about people.
- A @LeadOrganisation will build a Risk-Index using @Attribute data, and apply a @RiskModel to place people into @RiskCategories.
- A @LeadOrganisation will pass responsibility for a person to a @ResponsibleOrganisation who can assess @Needs and raise a @Case.

- A @ResponsibleOrganisation directs various @DeliveryOrganisations to provide support services to address each @Need

# IG Specific Roles

The table below sets out a number of roles relevant to the governance of personal information. Organisations following SAVVI may need to deploy or exercise one or more of these roles to varying degrees at different stages of the process. Each organisation will need to ensure that they identity the appropriate roles that they need to deploy at each stage of the SAVVI process.

| topic | Requirement / description | input/output | references |
|---|---|---|---|
| Controller / Joint Controller | 'controller' means the….. public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data subject to DPA 2018 S.6<br><br>The Controller and Joint Controller relationship carry specific legal obligations | | [2 ]key-definitions<br>UK GDPR A.4(7)<br>DPA 2018 S.6 |
| Processor | 'processor' means …….public authority, agency or other body which processes personal data on behalf of the controller | | [2] UK GDPR A.4(8) |
| | This SAVVI Information Governance Framework considers each of the organisations in the SAVVI Process to be 'Controllers'.<br>However the @DeliveryOrganisation may also be a Processor | | [2] UK GDPR |
| Accountable Governance Group | Each Controller will have a Governance Group that is responsible and accountable for 'Information Governance', so that it can take decisions, adopt IG documents approve new processing activities. | output:SAVVI Project Structure | [6]-effective governance and oversight mechanisms |
| SIRO / Caldicott Guardian CG | Engage with Senior Information Risk Owner and / or Caldicott Guardian to ensure they are apprised of information risk. They should provide assurance that personal data ( health & social care only for CG) is used legally, ethically and appropriately, and that confidentiality is maintained. | | |
| Data Protection Officer | Possessing, expert knowledge of data protection law and practices | output:SAVVI Project Structure | UK GDPR A.37(5) |
| Project Team and Expert Input | List the members of the team and stakeholders | output:SAVVI Project Structure | [6]-diverse, multidisciplinary |

| | | | |
|---|---|---|---|
| | Emphasising diversity and access to skills and expertise. | | teams with wide ranging skill sets contribute to the success of any data or tech project. |

# Phases of data use in the SAVVI Process


This Information Governance Framework is a part of the ‘SAVVI Process’, and covers

- Considering the data provenance of existing personal data
- reusing existing personal data to build a risk-index
- capturing new data as needs are assessed
- sharing data to plan and monitor support
- improving a risk model by analysing data

## Data Provenance

Before using existing Personal Data sets consider tracing the data from its originating source to its current stage. This could include seeking to understand:

- Factors influencing data initiation / creation
- Data sources
- Input methods through which data entered the system

To ensure that there are adequate levels of data hygiene and data compliance and that this is maintained.

# Purpose - Reusing existing personal data to build a risk-index

## Defining Vulnerability and the Local Context

| topic | requirement | input/output | references |
|---|---|---|---|
| Define the **purpose** of the Vulnerability Initiative | @LeadOrganisation<br><br>Define the **purpose** of the vulnerability initiative.<br><br>Search the SAVVI Catalogue to see if an existing definition can be used. | Input: SAVVI Catalogue<br><br>output: SAVVI Vulnerability Purpose | [2]-Purpose-Limitation<br><br>[6]-a clear articulation of its purpose.<br><br>[3]-step2<br>[3]-step6<br>[3]-step7 |
| Basis for the **Purpose** | Demonstrate that the @LeadOrganisation has a duty to address the vulnerability. | output: SAVVI Vulnerability Purpose | |
| Rationale for the **Purpose** | Document the local context, consequences and objectives for the Vulnerability | output:SAVVI Data Ethics Assessment | [6]-clarity on what public benefit the project is trying to achieve and what are the needs of the people who will be using the service or will be most directly affected by it. |
| Consider presenting the outcome of Data Ethics Assessment for internal approval before proceeding | | | |
| **PURPOSE - ASSESSING THE RISK** | | | |
| Risk Stratification Policy | Search the SAVVI Catalogue for the selected vulnerability to find Risk Models that could be used as the basis for the selected Vulnerability. | Input: SAVVI Catalogue | |
| | Document the @VulnerabilityAttributes data that will be used in the Risk Model.<br><br>Document the rules that will be applied to determine a @RiskCategory. | output:SAVVI Risk Stratification Policy<br><br>output: SAVVI Data Flow Map | |
| Data Protection Impact Assessment | Document the Benefits and Risks to data subjects and organisations of sharing the data | Input:<br><br>output:SAVVI Data Ethics Assessment | UK GDPR A.30, A.35, A.32(1), A.39(2)<br>A.23. DPA 2018 Sch.2<br><br>[3]-step5 |
| | Document the evidence that the | output:SAVVI Risk Stratification | |

| | | | |
|---|---|---|---|
| | selected Risk Model is successful in identifying vulnerable individuals | Policy | |
| Data Protection Impact Assessment | Statement that data has been minimised. | output:SAVVI Risk Stratification Policy | UK GDPR A.5(1)c, A.35<br><br>[3]-step12 |
| Ethics | Assess the Ethics of the proposed data shares for<br>• Transparency<br>• Accountability<br>• Fairness | output: Data Ethics Assessment<br><br>output:Equality Impact Assessment<br><br>CDEI work on public consultation with BOLD | [5] The ethical issues around the use of data are factored into the decision-making process and any new data analysis techniques are assessed against the Data Ethics Framework.<br><br>[6] Record your answers to create a data ethics assessment. |
| Data Ethics Assessment / Data Protection Impact Assessment | Identifying and mitigating bias<br><br>Use of profiling, algorithms, etc Consideration of Data Ethics Assessment outcome | Input: Data Ethics Framework | [6]-Bias in Data<br><br>Data Ethics Assessment |
| Data Ethics Assessment / Data Protection Impact Assessment | In particular<br><br>• **Would the proposed use of data be deemed unfair / unlawful, intrusive or unexpected by those who provided the data** (individuals or organisations)?<br>• Would the proposed use of data for **secondary purposes** make it less likely that people would want to give that data again for the primary purpose it was collected for?<br>• How can you **explain** why you need to use this data **to members of the public?**<br>• Does this use of data interfere with the **rights of individuals?** If yes, is | Input: User Research, Public Consultation<br><br>output: Data Ethics Assessment Data Protection Impact Assessment | [6]-Determining proportionality<br><br>[6]-Bias in Data<br><br>[6]-data ethics assessment<br><br>[2] UK GDPR A.5(1)<br>A.35 DPIA |

| | | | |
|---|---|---|---|
| | there a less intrusive way of achieving the objective? | | |
| Adopt | @LeadOrganisation<br><br>An accountable governance group signs off the risk stratification policy. | Input : SAVVI Vulnerability Purpose<br><br>Input: SAVVI Risk Stratification Policy<br><br>Input Data Ethics Assessment / DPIA | [6]-effective governance and oversight mechanisms<br><br>[6]-to eliminate your project's potential to have unintended discriminatory effects on individuals and social groups. |
| Publish | Publish the Vulnerability Initiative.<br><br>Promotion such as press releases.<br><br>Consider Feedback. | Input: SAVVI Vulnerability Purpose<br><br>Input: SAVVI Risk Stratification Policy<br><br>Input: Data Ethics Assessment / DPIA | [6]-made open to inspection by publishing information about the project in a complete, open, understandable, easily-accessible, and free format.<br><br>[6]-Share your models |

## Propose a Lawful proposition for use

For each @Vulnerability Attribute

| **topic** | **requirement** | **input/output** | **references** |
|---|---|---|---|
| SAVVI Catalogue | Consult the SAVVI Catalogue to see if there is a proposition for the @VulnerabilityAttribute to be used for this @Purpose(s),<br><br>Use the 'Proposition' as the starting point for an opinion from the @LeadOrganisation. | input:SAVVI Catalogue | [6]-data ethics assessment |
| | Select and justify one or more Lawful Basis.<br>from<br>• GDPR Article 6<br><br>The ICO provide a Lawful basis interactive guidance tool | output:SAVVI Lawful basis | [1]-Lawful Basis<br><br>[2]-Lawful Basis for Processing |

| | | | |
|---|---|---|---|
| | One or more of<br><br>**(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.<br><br>This is the least likely option for SAVVI as individuals will not yet be known<br><br>**(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.<br><br>This is an unlikely option for SAVVI as individuals will not yet be known and or are unlikely to be contracting in for public services relating to a vulnerability.<br>**(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).<br><br>Many organisations will be able to rely on this basis as it applies to any legal obligation(s) they have in meeting the specified purpose(s).<br><br>**(d) Vital interests:** the processing is necessary to protect someone's life.<br><br>This basis will have limited application as the threshold of the processing being 'necessary to protect an interest which is essential for the life of the data subject or that of another natural person' is quite high when considering potential vulnerabilities.<br><br>**(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.<br><br>For many organisations embracing SAVVI this basis will be applicable in supporting the specified purpose(s). | | |

| | | | |
|---|---|---|---|
| | **(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party.*<br><br>Whilst this lawful basis has some flexibility, it will have limited use for public authorities, but may be more useful for other or organisations.<br>*Public authorities cannot, rely on legitimate interests for any processing performed as part of tasks as a public authority. | | |
| Special Category Data or Criminal Offence Data | Determine if the @VulnerabiltyAttribute is, includes or reveals:<br>• special category data<br>• criminal offence data | output: SAVVI Vulnerability Attribute definition | [3]-step 21<br><br>[2]-Lawful Basis for Processing<br><br>[1]-Special Category Data<br><br>[1]-Criminal Offence Data |
| If 'special category data' | find an Article 9 'condition for processing'<br><br>• (a) Explicit consent<br>• (b) Employment, social security and social protection (if authorised by law)<br>• (c) Vital interests<br>• (d) Not-for-profit bodies<br>• (e) Made public by the data subject<br>• (f) Legal claims or judicial acts<br>• (g) Reasons of substantial public interest (with a basis in law)<br>• (h) Health or social care (with a basis in law)<br>• (i) Public health (with a basis in law)<br>• (j) Archiving, research and statistics (with a basis in law) | output: SAVVI Conditions for processing Special Category data | [3]-step22<br><br>[1]-Special Category Data |
| | Check for further conditions required by the Article 9 condition<br><br>If relying on conditions (b), (h), (i) or (j), also need to meet the associated condition:Part 1 | output: SAVVI Conditions for processing Special Category data | [1]-Special Category Data<br><br>[2]Schedule 1 of the DPA 2018. |

| | | | |
|---|---|---|---|
| | of Schedule 1 of the DPA 2018. | | |
| | | | |
| If Criminal Offence Data | Check for further conditions required under Article 10 or Schedule 1 of the DPA 2018. | output: SAVVI Conditions for processing Criminal Offence data | [1]-Criminal Offence Data<br><br>[2]Schedule 1 of the DPA 2018. |
| | | | |
| Organisation Type | Consider if the source Organisation Type is<br>• Public sector<br>• Private Sector<br>• Social Sector | output: SAVVI Lawful basis and Conditions for processing | [1]-Lawfulness |
| | | | |
| | | | |
| Legal Gateway | If the Source Organisation Type is 'public' ...<br><br>Propose a Legal Gateway to share this @VulnerabilityAttribute for this @Purpose. | output: SAVVI Lawful basis and Conditions for processing | [3]-step14<br><br>[1]-Lawfulness \| ICO |
| | | | |
| Peer Group Review | If the selected legal gateway is not present on the SAVVI Catalogue for the @Purpose, ask for a review by the SAVVI IG QA group. | Input: SAVVI Lawful basis<br><br>output: SAVVI IG QA Group review<br><br>output: update to SAVVI Catalogue | |
| | | | |
| Escalate | If a Legal Gateway cannot be found, make a proposal via the Digital Economy Act. | See - Data Sharing via the Digital Economy Act | [1]-Data sharing across the public sector: the Digital Economy Act codes \| ICO<br><br>[5] Digital Economy Act 2017 - Code of Practice |
| Adopt | @Lead Organisation<br><br>If a Legal Gateway / Lawful basis has been found - an accountable governance group signs off the lawful proposition, having sought internal legal opinion. | output: SAVVI Lawful basis and Conditions for processing | |
| Abort | If a Legal Gateway cannot be | | [3]-step25 |

| | | | |
|---|---|---|---|
| | adopted, abort the intention to share the @Vulnerability Attribute for the @Purpose.<br><br>Return to defining the Risk Stratification Policy, so that the @VulnerabiltyAttribute is removed. | | |

## Agree in principle to share @VulnerabilityAttribute data

For each @Vulnerability Attribute

| **topic** | **requirement** | **input/output** | **references** |
|---|---|---|---|
| Identify Source Organisations | Consult the SAVVI Catalogue to see which 'organisation types' are typically controllers for a dataset that contains the selected @VulnerabiltyAttribute | input:SAVVI Catalogue | |
| | List the actual @SourceOrganisations that may be controllers for a dataset that contains the selected @VulnerabiltyAttribute | | |
| | Lookup an organisation's published / held information about the datasets that it holds. | Input: Information Asset Register<br><br>Input: Register of Processing Activities | |
| | Check that a @SourceOrganisation is a legal entity.<br><br>Cannot share person identifiable data with organisations that are not legal entities. | ??? | [3]-step3 |
| | Consider if the source organisation is<br>• Public<br>• Private<br>• Social sector | | [1]- Lawfulness \| ICO |
| Define the Dataset | Consult the SAVVI Catalogue to see if a named Organisation has already listed the @VulnerabilityAttribute as shareable for the Vulnerability Purpose. | Input: SAVVI Catalogue | |

| | | | |
|---|---|---|---|
| | Contact the @SourceOrganisation to ask about the availability and quality of data | output: SAVVI - initial risk data questionnaire | [3]-step11<br><br>[6]-You must ensure that the data for the project is accurate, representative, proportionally used, of good quality, and that you are able to explain its limitations.<br><br>[6]- Are all metadata and field names clearly understood? |
| Propose lawful data sharing in principle | Contact the @SourceOrganisation to establish agreement to the Lawful basis for data sharing. | Input: SAVVI Lawful basis and conditions for processing<br><br>output: SAVVI agreement on the Lawful basis to share data.<br><br>Output: @SourceOrganisation (s) Privacy Notice(s) | [2] - ICO Guide to the UK General Data Protection Regulation (UK GDPR)<br><br>[6]-Are individuals or organisations providing the data aware of how it will be used? |
| Abort | If the @SourceOrganisation does not agree that the proposed data share is Lawful - abort the intention to share the @VulnerabilityAttribute from the @SourceOrganisaitonfor the @Purpose.<br><br>Return to defining the Risk Stratification Policy, so that the @VulnerabiltyAttribute is removed. | | |

## Prepare Information Governance Documents

| topic | requirement | input/output | references |
|---|---|---|---|
| | | | |
| Establish the role of each Organisation in the data share. | Define as<br>• Controller<br>• Joint Controller<br>• Processor | | [3]-step4 |

| | | | |
|---|---|---|---|
| | | | |
| Privacy Statement | @SourceOrganisation and @LeadOrganisation prepare a joint Privacy Statement | output:SAVVI Privacy Statement<br><br>Incl. Algorithmic Transparency information if approriate | [3]-step18<br><br>[2] - ICO guidance on Privacy Notices<br><br>[7] Algorithmic Transparency Standard - GOV.UK (www.gov.uk) |
| | Agree a communication plan to publicise the data sharing and Privacy Statement | output:SAVVI Comms Plan | [3]-step19 |
| | | | |
| Opt-Out | | | [3]-step20 |
| | | | |
| DPIA | Complete an initial Data Protection Impact Assessment<br><br>Check the SAVVI Catalogue to find DPIAs that other organisations have used when sharing this data for this purpose. | input :SAVVI catalogue<br><br>output:DPIA | [2]-DPIA Screen Checklist<br><br>[2]-Data protection impact assessments<br><br>[2]-ICO DPIA Template |
| | Consider risks to organisations and individuals and mitigations | output:DPIA and risk assessment | |
| | Adopt the initial DPIA | output:DPIA | |
| | Make necessary arrangements to mitigate risks | | |
| | Complete and adopt final DPIA | output:DPIA | |
| | | | |
| Data Sharing Agreement | Create a Data Sharing Agreement | inputs<br><br>Output:data sharing agreement | [1]- Data sharing agreements \| ICO |
| | | | |
| Appropriate Policy Document | If processing ‘Special Category Data’ , or Criminal Office Data. | output: SAVVI Appropriate Policy Document | [2] - appropriate policy document<br>[2]Schedule 1 of the DPA 2018. |

## Agreement to Share

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

| | | | |
|---|---|---|---|
| Adopt a Data sharing agreement / memorandum of understanding | @Lead Organisation<br>@Source Organisation<br><br>Publish | output:data sharing agreement | [3]-step31<br><br>[1]- Data sharing agreements \| ICO |
| Update SAVVI Catalogue | Add a Data Sharing Agreement to the SAVVI Catalogue. | output:SAVVI Catalogue | |
| RoPA | @LeadOrganisation add an entry to the Record of Processing Activities. | output:RoPA | [2]-Record of Processing Activities |

## Set up procedures to support individuals' rights

| **topic** | **requirement** | **input/output** | **references** |
|---|---|---|---|
| Right to be informed | Facilitate the right to be informed about how and why individuals' data is used.<br><br>Relevant to source of the data | Input:SAVVI Privacy Statement<br>Output:<br>LeadOrganisation / @SourceOrganisation Privacy Notice(s) inclu. Algorithmic Transparency information if appropriate | [2] - Right to be Informed.<br><br>[7] Algorithmic Transparency Standard - GOV.UK (www.gov.uk) |
| Right of access | the right to access a copy of the personal data held to receive other supplementary information (the right of subject access)<br><br>Including if applicable: the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.<br><br>Where possible, the controller should be able to provide remote access to a secure system | Input: Data Ethics Assessment<br><br>output : Response to a Subject Access Request | [2] - Right of Access<br><br>[6] GOV.UK Data Ethics Framework - Data Ethics Assessment |

| | | | |
|---|---|---|---|
| | which would provide the data subject with direct access to his or her personal data. | | |
| Right to rectification erasure, restriction. | the rights to have data being used / processed rectified, erased or to have processing restricted; | Input: Response to Subject Access Request<br><br>Input: Data subject records<br><br>Output: Response to rectification, restriction or erasure request<br><br>Output: Notification statement to other recipients | [2] - Right to Rectification<br><br>[2] - Right to Erasure<br><br>[2] - Right to restrict processing |
| Right to Object: | the right to object to processing of personal data;e.g.<br><br>To be removed from / stop processing current and future vulnerability initiatives.<br><br>Not absolute right applicable in limited circumstances and subject to assessment of reasons for objection | Input:SAVVI Privacy Statement / Notice<br><br>Input:RoPA<br><br>Output: Response to right to object request | [2] - Right to Object |
| Right to Data Portability | Right to obtain and reuse their personal data for their own purposes across different services.<br><br>to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.<br><br>This right is unlikely to apply or have much relevance as only applicable where lawful basis is: Consent or Necessary for a contract with Data Subject | | [2] - Right to Data Portability |

| | | | |
|---|---|---|---|
| | | | |
| Automated Decision Making – Including profiling | the right not to be subject to a decision, including profiling, based solely on automated processing.<br><br>Consider ethical implications.<br><br>If you are a government or public sector employee using algorithmic tools to support decisions in your organisation, refer to CDDO/ CDEI guidance | Input:CDDO / CDEI Algorithmic Transparency Standard & Template<br><br>input : Data Ethics Assessment | [2] - Rights related to automated decision making including profiling<br><br>[6] GOV.UK Data Ethics Framework - Data Ethics Assessment |
| Handling Complaints | Publish data sharing so that ... Individual data subjects may have queries or complaints about the sharing of their personal data, particularly if they think the data is wrong or that the sharing is having an adverse effect on them. | Output: Complaint Handling Procedures | [2] - The rights of individuals<br><br>Transparency requirements |
| | | | |

## Data Sharing via the Digital Economy Act

If an existing legal gateway cannot be found, it may be possible to use the data sharing powers in the Digital Economy Act 2017.

### About the Digital Economy Act 2017

The Digital Economy Act 2017 - Code of Practice says ...

| |
|---|
| The Digital Economy Act 2017 creates a mechanism for **establishing clear and robust legal gateways** which will enable public authorities to share relevant information on the individuals and families they are working with in compliance with the data protection legislation. The primary purpose of this power is to support the well-being of individuals and households. |
| The 'public service delivery power' gives you the ability to gain access to the data you need to respond more efficiently and effectively to current and emerging social and economic problems. |
| Normally, information disclosed under these powers can **only be used for the purposes for which it was disclosed.** However there are very limited instances where information can be used **by a public authority for another purpose.** These circumstances vary between the powers but include:<br>• if the information has already been lawfully placed into the public domain;<br>• if the data subject has consented to the information being used for the other purpose; |

- for the prevention or detection of crime or the prevention of anti-social behaviour;
- for the purposes of a criminal investigation;
- for the purposes of legal proceedings;
- **for the purposes of safeguarding vulnerable adults or children**; or
- for the purposes of protecting national security.

### Health and social care

Health and adult social care bodies are **not included** in the list of specified persons permitted to use the new powers in England or for UK-wide activities.

### Defined 'Objectives'

Objectives are listed at https://registers.culture.gov.uk

When the Act was published, it contained a number of 'Objectives', including the following Public Service Delivery objectives:

| | |
|---|---|
| PSD - Multiple disadvantages | Public service delivery - Assisting individuals or households who face multiple disadvantages |
| PSD - Fuel poverty | Public service delivery - Assisting people living in fuel poverty |
| PSD - Water poverty | Public service delivery - Assisting people living in water poverty |
| PSD - TV retuning | Public service delivery - Providing targeted assistance in re-tuning televisions following spectrum changes |

That is "identifying individuals or households who face multiple disadvantages and enabling the improvement or targeting of public services to such individuals or households and providing for the monitoring and evaluation of programmes and initiatives"

Since the Act was published, further 'Objectives' have been added

- Civil registration: Allowing information on births, marriages, civil partnerships and deaths to be shared more widely to allow public authorities to deliver their functions more effectively
- Recovering debt owed to the public sector
- Combating fraud against the public sector

## Check existing Information Sharing Agreements

| topic | requirement | input/output | references |
|---|---|---|---|
| Check the Register | Information Sharing Agreements are listed at the Register of Information sharing agreements under chapters 1, 2, 3 and 4 of part 5 of the Digital Economy Act 2017<br><br>See the 'Information Sharing Agreements' tab. | input:DEA Register of Data Shares.<br><br>output:SAVVI Proposition for a New Data | |

| | | | |
|---|---|---|---|
| | If a suitable one is found, it can be used as the basis of a proposal for the same purpose/'disclosed information' with new controllers. | Share under the DEA. | |

## Using the Public Service Delivery - 'Multiple Disadvantages' Objective, or a future Objective.

| topic | requirement | input/output | references | |
|---|---|---|---|---|
| Check for an existing 'Objective' | [5] says "If your organisation has identified that the sharing of personal data is necessary to achieving a social or economic policy you should check whether the policy aims fall within one of the existing objectives set out in regulations."<br><br>The existing Objective that may be relevant to Vulnerability is 'Public service delivery - Assisting individuals or households who face multiple disadvantages'<br><br>Check if the Purpose for the Vulnerability Initiative is in scope of 'multiple disadvantages'.<br><br>that is "identifying individuals or households who face multiple disadvantages and enabling the improvement or targeting of public services to such individuals or households and providing for the monitoring and evaluation of programmes and initiatives" | Output: SAVVI opinion on how 'multiple-disadvantages' fits with vulnerability.<br><br>Input: https://registers.culture.gov.uk | [5] Code of Practice(Public Service Delivery, Debt and Fraud) Digital Economy Act 2017) | |
| If there is no existing suitable objective | [5] says "consider whether your purpose for information sharing falls within the criteria in section 35 and should be added as a new objective via regulations (see section 2.3)." | | [5] Code of Practice for public authorities (Public Service Delivery, Debt and Fraud) Digital Economy Act 2017 | |
| Once 'Objective' is identified- make a proposal | Make an assessment as to how and why the proposed datashare fits with the Objective.<br><br>Check that the parties to the Datashare are listed in Schedule 4<br><br>Identify the policy objective and the data needed to support it. | Input: [5]-Schedule 4<br><br>input:SAVVI<br><br>output:SAV | [5] Code of Practice for public authorities (Public Service Delivery, Debt and Fraud) Digital | |

| | | | | |
|---|---|---|---|---|
| | Assess the Ethics of the Data Share<br><br>Data Protection Impact Assessment/ Ethics Impact Assessment<br><br>Business Case<br><br>Security Plan | VI Proposition for a New Data Share under the DEA. | Economy Act 2017 | |
| Add to the Register | You should notify the secretariat for the Public Service Delivery review board in the Department for Digital, Culture, Media and Sport (DCMS) of your information sharing arrangement, to be maintained in a searchable electronic register available to the general public. | Output: DEA Register of Data Shares | [5] Code of Practice for public authorities (Public Service Delivery, Debt and Fraud) Digital Economy Act 2017 | |
| Draw up an appropriate data sharing agreement | Having established that there is a lawful basis to share data, draw up an appropriate data sharing agreement with the @SourceOrganisation and @LeadOrganisation | | [5] | |

## Complying with the DEA Code of Practice

The Digital Economy Act Code of Practice sets out a number of requirements on parties involved in data sharing. Here we have picked out some that are particularly relevant to SAVVI. All requirements of the code will need to be complied with.

| **topic** | **requirement** | **input/output** | **references** |
|---|---|---|---|
| Statements | A statement that due regard has been given to the Code should be included in any information sharing agreement produced for such sharing. | | [5] Code of Practice for public authorities (Public Service Delivery, Debt and Fraud) Digital Economy Act 2017 |
| DPIA | A Data Protection Impact Assessment will be conducted for all data sharing under the code. | | |
| Transparency | Data sharing under the code will be published | | |
| | It is important that individuals can understand what data is being shared, the specific purposes for which it is being shared, which bodies are disclosing and receiving that data, the potential benefits to be derived from the data sharing, their rights relating to the | | [2] - ICO Guide to the UK General Data Protection Regulation (UK GDPR) |

| | | | |
|---|---|---|---|
| | use of the data and where appropriate how long that data will be held for. Furthermore, under the data protection legislation, controllers and processors are required to keep records of their data processing activities. | | |
| Minimisation | You must only share the minimum data required to fulfil the stated purpose for sharing. | | [2] - ICO Guide to the UK General Data Protection Regulation (UK GDPR) |
| | | | |
| Agreements | Information sharing agreements must include details of retention and destruction policies that prevent the retention or use of data for longer than it is needed or its use for any purposes other than those for which it was disclosed/received (subject to limited exceptions provided for in law). | | [1] - Data sharing agreements \| ICO<br><br>[2] DPA 2018 Sch 2<br>[2] DPA 2018 Sch 3<br><br>[2] |
| | You should put procedures in place to ensure that data no longer required is destroyed promptly and securely and rendered irrecoverable. The same will apply to data derived or produced from the original data, (subject to the specific rules on data processed for research purposes). You should refer to the ICO guidance on Deleting Personal Data. | | [2] - ICO Guide to the UK General Data Protection Regulation (UK GDPR) - Principles |
| Quality | You should check the accuracy of data prior to sharing | | [2] The principles \| ICO |
| Data Protection Compliance | Organisations involved in an information sharing arrangement should also agree procedures and processes for:<br>● correcting inaccurate data and making sure all bodies that the data has been transferred to correct it too;<br>● recording and capturing corrections for auditing purposes;<br>● deleting data, where there is a right to erasure;<br>● contacting the data subject where appropriate;<br>● how information and access to data is to be provided to data subjects;<br>● how data subjects can exercise their rights to restrict and object to processing. | | [2] - ICO Guide to the UK General Data Protection Regulation (UK GDPR) |

| | | | |
|---|---|---|---|
| Security | You will need to agree a security plan as part of any formal information sharing agreement with public authorities and third parties who are party to the data share. Security plans should include:<br>● storage arrangements that make sure information is secured in a robust, proportional and rigorously tested manner, including how to comply with protective marking handling requirements where applicable;<br>● assurance that only people who have a genuine business 'need to know' personal information will have access to it;<br>● who to notify in the event of a security breach / personal data breach;<br>● procedures to investigate the causes of any security breach. | output:SAVVI Security Plan | [2] - ICO Guide to the UK General Data Protection Regulation (UK GDPR)<br><br>Personal data breaches \| ICO |
| | Non-public authorities can only participate in an information sharing arrangement once their sponsoring public authority has assessed their systems and procedures to be appropriate for secure data handling. | | |
| Conflict of Interest | Where an information sharing arrangement proposes that information be disclosed to or received from **a body which is not a public authority**,[footnote 9] the body should be asked to declare all potential conflicts of interest (see Annex A), for example from other work it does for public authorities or its own commercial interests. An assessment should be made of any conflicts of interest that the non-public authority may have, to identify whether there are any legal or reputational risks involved in sharing data with the organisation. | output:SAVVI Proposition for a New Data Share under the DEA.<br><br>Output: Conflict Risk Assessment | |
| | | | |

## Adding a new 'Objective'

it is possible to create a new 'objective' via regulations. To propose a new 'objective', you need to determine what types of data are required, which bodies hold the data and how the ability to share personal data will support the achievement of your policy objectives.

The DEA Code of Practice gives examples of potential new ‘Objectives’

- reducing the number of people sleeping on the street for more than one night;
- improving employment outcomes for ex-offenders;
- supporting gang members to safely exit gang culture.

| | | | |
|---|---|---|---|
| Consider if the purpose of the datashare is relevant to the Digital Economy Act | All objectives must meet all of the following conditions which are set out in section 35 of the Digital Economy Act 2017:<br>• condition 1: the purpose is the improvement or targeting of a public service provided to individuals or households, or the facilitation of the provision of a benefit (whether or not financial) to individuals or households;<br>• condition 2: the purpose is the improvement of the well-being of individuals or households;<br>• condition 3: the purpose is the supporting of the delivery of a specified person’s functions, or the administration, monitoring or enforcement of a specified person’s functions. | | [5] |
| Abort | If not relevant - abort the intention to share the @VulnerabilityAttribute from the @SourceOrganisaitonfor the @Purpose. | | [5] |
| Propose to DEA Review Board | All proposals for ‘objectives’ must be submitted to the review board. The review board will be supported by a secretariat based in the Government Digital Service and will sit on a quarterly basis. | | [5] |

# Templates

## General

Each document generated from these templates should have a cover sheet that includes

| | | |
|---|---|---|
| Version | | |
| Date | | |
| Adopted by | An accountable governance group in an organisation | |
| Adopted date | | |
| Contact Info | | |

## SAVVI - Vulnerability Purpose

| | | |
|---|---|---|
| @Lead Organisation | | |
| Vulnerability | A description of a vulnerability that could apply to a person or household.<br><br>At this stage, this should not include a local context or prioritisation, so that the definition can be shared and re-used. | |
| Duty | References to acts and regulations that give rise to a relevant duty.<br><br>Preferably, references to a URL from legislation.gov.uk | |

## SAVVI - initial risk data questionnaire

| | | |
|---|---|---|
| @Source Organisation | {defined by @Lead Organisation} | |
| @Vulnerability Attribute | {defined by @Lead Organisation} | |
| Dataset | Which dataset(s) is the @VulnerabilityAttribute contained in?<br><br>{could be pre-filled from the SAVVI Catalogue} | ?? |
| Purpose that it is held? | {could be pre-filled from the SAVVI Catalogue} | |
| Supplier / System | Is the dataset contained in a system?<br><br>Supplier / System name | |
| Can data be extracted? | Formats?<br><br>Can data be extracted to the SAVVI Logical Model? | |
| Identifiers | What References use use to identify<br>• People<br>• Properties<br>• Households | |
| Data Quality | {List of data quality dimensions} - statement for each. | [4] |

## SAVVI - Lawful Basis Proposition

Incorporate relevant parts of [1] the ICO data sharing checklist

| | | |
|---|---|---|
| Proposed by | @Lead Organisation | |
| Vulnerability | {as defined in the Risk Stratification Policy} | |
| Data Attribute | {defined by @Lead Organisation} | |
| GDPR Article 6 | Check boxes for any of | [1]-Lawfulness |

| | | |
|---|---|---|
| Provision(s) | (a) Consent;<br>(b) processing is necessary for the performance of a contract;<br>(c) processing is necessary for compliance with a legal obligation;<br>(d) processing is necessary in order to protect vital interests;<br>(e) processing is necessary for the performance of a public interest task or in the exercise of official authority vested in the controller;<br>(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. | |
| Special Category Data | Is the data?<br>● special category data<br>● criminal offence data<br><br>This document should then cover information required for 'Appropriate Policy Document'<br><br>See [2] What are the conditions for processing and Data Protection Act 2018 - Schedule 1 for Schedule 1 Conditions | [2]-Special Category Data<br><br>[2]-Criminal Offence Data<br><br>Data Protection Act 2018 - Schedule 1<br><br>[2] Template for Appropriate Policy Document |
| GDPR Article 9 Provision(s) | Checkboxes for<br><br>(a) Explicit consent<br>(b) Employment, social security and social protection (if authorised by law)<br>(c) Vital interests<br>(d) Not-for-profit bodies<br>(e) Made public by the data subject<br>(f) Legal claims or judicial acts<br>(g) Reasons of substantial public interest (with a basis in law)<br>(h) Health or social care (with a basis in law)<br>(i) Public health (with a basis in law)<br>(j) Archiving, research and statistics (with a basis in law) | [2] Rules for Special Category Data |
| Legal Gateway(s) | Referring to legislation.gov.uk | |
| Rationale | A narrative to explain why the proposition is Lawful. | |
| Legal Opinion | The legal opinion from a representative of the @LeadOrganisation | |
| Compliance with the Human Rights Act | Statement form the @LeadOrganisation<br><br>Particularly to Article 8 of the Convention, which gives everyone the right to respect for their private and family life, home and correspondence, is especially relevant to sharing personal data. | |

# SAVVI - Agreement on the Lawful Basis to share data

Incorporate relevant parts of [1] the ICO Data sharing request form template

| | | |
|---|---|---|
| Proposed by | @Lead Organisation | |
| Vulnerability | {as defined in the Risk Stratification Policy} | |
| Data Attribute | {defined by @Lead Organisation} | |
| GDPR Article 6 / Article 9 Provision(s) | | |
| Legal Gateway(s) | Referring to legislation.gov.uk | |
| Rationale | A narrative to explain why the proposition is Lawful. | |
| Legal Opinion | The legal opinion from a representative of the @LeadOrganisation | |

# SAVVI - Proposition for a new Data Share under the Digital Economy Act

The Digital Economy Act Code of Practice says

> you must develop and agree a business case with the other bodies participating in the data share. A single business case will need to be developed for each information sharing arrangement. An information sharing arrangement could cover multiple transactions, and may cover the exploration of the benefit of sharing a single data asset, through to the trialling of a complete business process (for example under the debt and fraud powers).

| | | |
|---|---|---|
| Business Case | An outline of the information share. This should include:<br>● the objective of the information sharing arrangement;<br>● an overview of the activity under the arrangement (and how the data will be used);<br>● the period of duration for the arrangement, when the data share will be live and how retention periods will be managed; and<br>● an outline of what types of data will be shared and the data security arrangements to be put in place.<br><br>Persons included in the information share. This should include:<br>● a list of all persons and bodies that will be involved in the share – specifying which would disclose or receive data: | |

| | | |
|---|---|---|
| | ○ to note - a business case provided under the fraud power need not go as far as detailing the counter fraud operation of partners.<br><br>How the benefits of the information share will be measured. This should include: + the potential benefits the information share could bring; + the success criteria for the data share and the methodology you will use to measure success.<br><br>A statement of adherence to the Code of Practice:<br>● for a debt data share, you should also include a statement explaining how you will comply with the Fairness Principles (in Part 3.4). | |

# SAVVI Catalogue

The SAVVI Catalogue is currently draft at http://52.56.166.229/html/datalicence

The SAVVI Catalogue will contain Information Governance scenarios that have been established with the SAVVI programme or contributed by organisations who have used the SAVVI Process.

This information can be a starting point when considering what data to use to find vulnerable people. However, organisations will need to take their own legal advice when deciding if data sharing is lawful.

The Catalogue will contain

- Purposes for data sharing
- Attribute(s) that have been used for a Purpose
- Datasets that typically contain Attributes
    - Type of Organisation that is the Controller
    - Dataset name
    - Original Purpose
    - Legal Basis for its original collection
- The Lawful bases of the datashare
- Which Organisations have used this datashare
- About the datashare
    - Status
    - Who endorses it
    - Links
        - Plan