SAVVI - Information Governance Framework

revision	on	by	note
1	09/03/2021	Paul Davidson, SAVVI	1st draft
2	15/03/2021	Paul Davidson	Restructure

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)
[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

Principles

This SAVVI Information Governance Framework learns from the ICO's Data Sharing Code of Practice [1] where it says

- "Data protection law is an enabler for fair and proportionate data sharing, rather than a blocker."
- "The accountability principle means that you are responsible for your compliance, and you must be able to demonstrate that compliance."
- "You must share personal data fairly and transparently."
- "You must identify at least one lawful basis for sharing data before you start any sharing."
- "You must process personal data securely, with appropriate organisational and technical measures in place."

… and from ICO Guide to the UK General Data Protection Regulation (UK GDPR) [2] where it says

- You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear obligation or function set out in law.

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

topic	**requirement**	**input/output**	**references**
Data Controllers	The ICO describes a Data Controller as ... “A controller determines the purposes and means of processing personal data”.		[2]key-definitions
	This SAVVI Information Governance Framework considers each of the organisations in the SAVVI Process to be ‘Controllers’.		
Accountable Governance Group	Each Controller will have a Governance Group that is responsible and accountable for ‘Information Governance’, so that it can take decisions and adopt IG documents.	output:SAVVI Project Structure	[6]-effective governance and oversight mechanisms
Data Protection Officer		output:SAVVI Project Structure	
Project Team and Expert Input	List the members of the team and stakeholders Emphasising diversity and access to skills and expertise.	output:SAVVI Project Structure	[6]-diverse, multidisciplinary teams with wide ranging skill sets contributes 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

- 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

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 Define the purpose of the vulnerability initiative. Search the SAVVI Catalogue to see if an existing definition can be used. See examples.	Input: SAVVI Catalogue output: SAVVI Vulnerability Purpose	[3]-step2 [3]-step6 [3]-step7 [2]-Purpose-Limitation [6]-a clear articulation of its purpose.
	Demonstrate that the @LeadOrganisation has a duty to address the vulnerability.	output: SAVVI Vulnerability Purpose	
Rationale	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.
	Document the Benefits and Risks of sharing the data	output:SAVVI Data Ethics Assessment	[3]-step5
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. Document the rules that will be applied to determine a @RiskCategory.	output:SAVVI Risk Stratification Policy	
	Document the evidence that the	output:SAVVI Risk Stratification	

	selected Risk Model is successful in identifying people at risk	Policy	
	Statement that data has been minimised.	output:SAVVI Risk Stratification Policy	[3]-step12
Ethics	Assess the Ethics of the proposed data shares for • Transparency • Accountability • Fairness	output:SAVVI Data Ethics Assessment output:Equality Impact Assessment	[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. [6] Record your answers to create a data ethics assessment.
	In particular • **Would the proposed use of data be deemed inappropriate by those who provided the data** (individuals or organisations)? • 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? • How can you **explain** why you need to use this data **to members of the public?** • Does this use of data interfere with the rights of individuals? If yes, is there a less intrusive way of achieving the objective?	Input: User Research, Public Consultation output:SAVVI Data Ethics Assessment	[6]-Determining proportionality
Adopt	@LeadOrganisation An accountable governance group signs off the risk stratification policy.	Input : SAVVI Vulnerability Purpose Input: SAVVI Risk Stratification Policy Input SAVVI Ethics Assessment	[6]-effective governance and oversight mechanisms [6]-to eliminate your project's potential to have unintended

			discriminatory effects on individuals and social groups.
Publish	Publish the Vulnerability Initiative. Promotion such as press releases. Consider Feedback.	Input: SAVVI Vulnerability Purpose Input: SAVVI Risk Stratification Policy Input: SAVVI Ethics Assessment	[6]-made open to inspection by publishing information about the project in a complete, open, understandable, easily-accessible, and free format. [6]-Share your models

Propose a Lawful and Legal proposition for sharing

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 shared for this @Purpose, to find • GDPR article 6 and/or article 9 provisions • Legal Gateway Use the 'Proposition' as the starting point for an opinion from the @LeadOrganisation.	input:SAVVI Catalogue	
Lawful Basis	Select and justify one or more Lawful Basis Provision. The ICO provide a Lawful basis interactive guidance tool One or more of **(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose. **(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.	output:SAVVI Lawful and Legal basis	[1]-Lawful Basis [2]-Lawful Basis for Processing

	(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations). **(d) Vital interests:** the processing is necessary to protect someone's life. **(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. **(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party		
Special Category Data or Criminal Office Data	Determine if the @VulnerabiltyAttribute is • special category data • criminal offence data	output: SAVVI Lawful and Legal basis	[3]-step21 [2]-Lawful Basis for Processing [1]-Special Category Data [1]-Criminal Offence Data
If 'special category data'	find an Article 9 'condition for processing' one-off • (a) Explicit consent • (b) Employment, social security and social protection (if authorised by law) • (c) Vital interests • (d) Not-for-profit bodies • (e) Made public by the data subject • (f) Legal claims or judicial acts • (g) Reasons of substantial public interest (with a basis in law) • (h) Health or social care (with a basis in law) • (i) Public health (with a basis in law) • (j) Archiving, research	output: SAVVI Lawful and Legal basis	[3]-step22 [1]-Special Category Data

	and statistics (with a basis in law)		
	Check for further conditions required by the Article 9 condition	output: SAVVI Lawful and Legal basis	[1]-Special Category Data
If Criminal Offence Data	Check for further conditions required	output: SAVVI Lawful and Legal basis	[1]-Criminal Offence Data
Organisation Type	Consider if the source Organisation Type is • Public sector • Private Sector • Social Sector	output: SAVVI Lawful and Legal basis	[1]-Lawfulness
Legal Gateway	If the Source Organisation Type is 'public' ... Propose a Legal Gateway to share this @VulnerabilityAttribute for this @Purpose.	output: SAVVI Lawful and Legal basis	[3]-step14 [1]-Lawfulness
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 and Legal basis output: SAVVI IG QA Group review output: update to SAVVI Catalogue	
escalate	If a Legal Gateway cannot be found, make a proposal via the Digital Economy Act.	See - Making a Proposal via the Digital Economy Act	[1]-Data sharing across the public sector: the Digital Economy Act codes
Adopt	@Lead Organisation If a Legal Gateway has been found - an accountable governance group signs off the legal/lawful proposition, having sought internal legal opinion.	output: SAVVI Lawful and Legal basis	
Abort	If a Legal Gateway cannot be adopted, abort the intention to share the @Vulnerability Attribute for the @Purpose.		[3]-step25

	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 information about the datasets that it holds.	Input: Information Asset Register Input: Register of Processing Activities	
	Check that a @SourceOrganisation is a legal entity. Cannot share person identifiable data with organisations that are not legal entities.	???	[3]-step3
	Consider if the source organisation is • Public • Private • Social sector		[1]-Lawfulness
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 [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. [6]- Are all metadata and field names clearly understood?
Propose Legal/lawful data sharing in principle	Contact the @SourceOrganisation to establish agreement to the Legal and Lawful basis for data sharing.	Input: SAVVI Legal and Lawful basis output: SAVVI agreement on the Legal and Lawful basis to share data.	[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 Legal and Lawful - abort the intention to share the @VulnerabilityAttribute from the @SourceOrganisaitonfor the @Purpose. 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 • Controller • Joint Controller • Processor		[3]-step4
Privacy Statement	@SourceOrganisation and @LeadOrganisation prepare a joint Privacy Statement	output:SAVVI Privacy Statement	[3]-step18 [2] - ICO guidance on Privacy Notices
	Agree a communication plan to	output:SAVVI Comms	[3]-step19

	publicise the data sharing.	Plan	
Opt-Out	??		[3]-step20
DPIA	Complete an initial Data Protection Impact Assessment Check the SAVVI Catalogue to find DPIAs that other organisations have used when sharing this data for this purpose.	input :savvi catalogue output:dpia	[2]-DPIA Screen Checklist [2]-Data protection impact assessments [2]-ICO DPIA Template
	Consider Security risks and mitigations	output:dpia	
	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 Output:data sharing agreement	[1]-Data Sharing Agreement
Appropriate Policy Document	If processing ‘Special Category Data’ , or Criminal Office Data.	output: SAVVI Appropriate Policy Document	[2] - appropriate policy document

Agreement to Share

Adopt a Data sharing agreement / memorandum of understanding	@Lead Organisation @Source Organisation Publish	output:data sharing agreement	[3]-step31 [1]-Data Sharing Agreement
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	the right to be informed about how and why their data is used - and you must give them privacy information	input:SAVVI Privacy Statement	[2] - Right to be Informed.
	the right to access personal data held about them (the right of subject access);	output : Response to a Subject Access Request	[2] - Right of Access
Right to rectification erasure, restriction.	the rights to have their data rectified, erased or to have processing restricted;	Input: Response to Subject Access Request	[2] - Right to Rectification [2] - Right to Erasure [2] - Right to restrict processing
Right to Object:	the right to object; To be removed from current and future vulnerability initiatives.	input:SAVVI Privacy Statement	[2] - Right to Object
Right to Data Portability	???		[2] - Right to Data Portability
Automated Decision Making	the right not to be subject to a decision based solely on automated processing.		[2] - Rights related to automated decision making including profiling
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

Making a Proposal 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: ● if the information has already been lawfully placed into the public domain; ● 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

- Public service delivery - Assisting individuals or households who face **multiple disadvantages**

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 See the 'Information Sharing Agreements' tab. 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.	input:DEA Register of Data Shares. output:SAVVI Proposition for a New Data 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." The existing Objective that may be relevant to Vulnerability is 'Public service delivery - Assisting individuals or households who face multiple disadvantages' Check if the Purpose for the Vulnerability Initiative is in scope of 'multiple disadvantages'. 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"	Input: SAVVI opinion on how 'multiple-disadvantages' fits with vulnerability. Input: https://registers.culture.gov.uk	[5]
If there is no existing suitable objective	[5] says "If it doesn't you should 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]
If there is a suitable 'Objective' - make a proposal	Make an assessment as to why the proposed datashare fits with the Objective. Check that the parties to the Datashare are listed in Schedule 4	Input: [5]-Schedule 4 input:SAVVI	[5]

	Identify the policy objective and the data needed to support it. Assess the Ethics of the Data Share Data Protection Impact Assessment Business Case Security Plan	output:SAVVI Proposition for a New Data Share under the DEA.	
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.		[5]
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.		[5]

Complying with the DEA Code of Practice

The Digital Economy Act Code of Practice sets out a number of requirements on parties to 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 had to the Code should be included in any information sharing agreement produced for such sharing.		[5]
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 citizens 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, and where appropriate how long that data will be held for. Furthermore, under the data protection legislation, controllers 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.		
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).		
	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.		
Quality	You should check the accuracy of data prior to sharing		
	Organisations involved in an information sharing arrangement should also agree procedures and processes for: ● correcting inaccurate data and making sure all bodies that the data has been transferred to correct it too; ● recording and capturing corrections for auditing purposes; ● deleting data, where there is a right to erasure; ● contacting the data subject where appropriate; ● how information and access to data is to be provided to data subjects; ● how data subjects can exercise their rights to restrict and object to processing.		
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: ● 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; ● assurance that only people who have a genuine business need to see personal information will have access to it; ● who to notify in the event of a security breach; ● procedures to investigate the causes of any security breach.	output:SAVVI Security Plan	
	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	output:SAVVI Proposition for a New Data Share under the DEA.	

	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.		

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 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: • 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; • condition 2: the purpose is the improvement of the well-being of individuals or households; • 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. 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. 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? {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?	

	Supplier / System name	
Can data be extracted?	Formats? Can data be extracted to the SAVVI Logical Model?	
Identifiers	What References use use to identify • People • Properties • Households	
Data Quality	{List of data quality dimensions} - statement for each.	[4]

SAVVI - Legal and 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 Provision(s)	Check boxes for any of *(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;* *(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;* *(c) processing is necessary for compliance with a legal obligation to which the controller is subject;* *(d) processing is necessary in order to protect the vital interests of the data subject;* *(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;* *(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.*	[1]-Lawfulness
Special Category Data	Is the data? • special category data • criminal offence data This document should then cover information required for 'Appropriate Policy Document' See [2] What are the conditions for processing and Data Protection Act 2018 - Schedule 1 for Schedule 1 Conditions	[2]-Special Category Data [2]-Criminal Offence Data Data Protection Act 2018 - Schedule 1 [2] Template for Appropriate

		Policy Document
GDPR Article 9 Provision(s)	Checkboxes for (a) Explicit consent (b) Employment, social security and social protection (if authorised by law) (c) Vital interests (d) Not-for-profit bodies (e) Made public by the data subject (f) Legal claims or judicial acts (g) Reasons of substantial public interest (with a basis in law) (h) Health or social care (with a basis in law) (i) Public health (with a basis in law) (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 Legal and Lawful.	
Legal Opinion	The legal opinion from a representative of the @LeadOrganisation	
Compliance with the Human Rights Act	Statement form the @LeadOrganisation 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 Legal and 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 Legal and 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: ● the objective of the information sharing arrangement; ● an overview of the activity under the arrangement (and how the data will be used); ● the period of duration for the arrangement, when the data share will be live and how retention periods will be managed; and ● an outline of what types of data will be shared and the data security arrangements to be put in place. Persons included in the information share. This should include: ● 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. 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. A statement of adherence to the Code of Practice: ● 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 Legal and Lawful bases of the datashare
- Which Organisations have used this datashare
- About the datashare
    - Status
    - Who endorses it
    - Links
        - Plan