Government Digital Service

GOV.UK Verify

Data Protection Impact Assessment

Published 18th May 2016

DOCUMENT CONTROL

Owner	Orvokki Lohikoski, Privacy Officer
Author	Toby Stevens, Independent Privacy Advisor
Version	1.0
Date	18th May 2016
Version History	
V0.1	27th January 2015
V0.2	15th February 2015
V0.3	31st March 2016
V0.4	13th May 2016
V0.5	16th May 2016
V1.0	18th May 2016

Table of Contents

1. Executive Summary

1.1 Background

The Government Digital Service (GDS) has created a cross-government identity assurance platform, GOV.UK Verify, which provides an identity service for secure online transactions between individuals and Government Services. GOV.UK Verify service brings together certified private-sector companies to act as identity providers on behalf of individuals when they assert their identity to Government Services, and is structured around a partial-anonymisation and matching hub service operated by GDS.

GDS maintains a Data Protection Impact Assessment (DPIA) of the GOV.UK Verify service to ensure that it reflects service user expectations and legal/regulatory requirements for the handling of personal information. The DPIA is complementary to the various security and legal reviews prepared for GOV.UK Verify.

An initial DPIA based on Cabinet Office guidelines was prepared as part of the project approval for GOV.UK Verify. This DPIA, which was initially prepared in February 2015, replaced the earlier DPIA, and has been updated to reflect the project since then. The DPIA does not consider the requirements of the EU General Data Protection Regulation (GDPR), since the final text was only published in May 2016. GDPR compliance is part of a separate check that will be completed in 2016.

1.2 Recommendations

The DPIA has found no critical privacy issues with GOV.UK Verify's service delivery, but includes recommendations to ensure the ongoing management of personal data across the system continues to reflect service user expectations, and follows best practice in privacy management. These recommendations include:

- GDS should continue to prepare appropriate internal privacy policies and processes to apply across the GOV.UK Verify programme and ensure that every member of staff is aware of the policies and their duties to follow them.
- GDS should ensure that it has prepared and tested incident response plans to work with stakeholders should a loss, modification or misuse of the Matching Data Set occur.
- GDS should continue to support the development of Transaction Monitoring controls to prevent session hijack.
- GDS should establish procedures to create and maintain a comprehensive record of use of personal data across the GOV.UK Verify ecosystem. The record should include details of processing carried out on GDS' behalf. This record should be checked regularly.
- GDS should establish protocols to ensure the regular review of retention periods for personal data.
- GDS should mandate that Certified Companies are not permitted to solicit, infer or otherwise obtain information about the Service User's interactions with Government Services (including knowing the identity of those Government Services).
- GDS should ensure that Certified Companies and Government Services do not charge Service Users for access to their personal data (Subject Access). This will be an enforced legal requirement under the EU GDPR from May 2018.
- GDS should ensure that by May 2018 Certified Companies allow Service Users to obtain their personal data and transfer it to other Certified Companies should they wish to do so.
- GDS regularly reviews the requirement for the IDA Supervisor function, which is currently served by the User Support team, and should expand the function should that be necessary.
- GDS should ensure that it maintains a coherent policy approach to exemptions to the Principles, and that protection of the Principles remains a policy (and if necessary, legislative) priority.

There are no privacy recommendations that prevent GOV.UK Verify proceeding to live service delivery, although the recommendations provided here, which are now in progress, should be addressed by the Privacy Officer as a matter of priority.

This DPIA should be maintained and revised by the Privacy Officer to incorporate an assessment of the requirements of the EU General Data Protection Regulation.

2. Introduction

2.1 Introduction

The Government Digital Service (GDS) has created a cross-government identity assurance platform, GOV.UK Verify, which provides an identity service for secure online transactions between individuals and Government Services. The service brings together private-sector Certified Companies to act on behalf of individuals when they assert their identity to Government Services, and is structured around a partial-anonymisation and matching Federation Hub service operated by GDS.

Given the importance and value of this service, GDS recognises the need not only to comply with relevant privacy legislation and regulations, but also to deliver 'best of breed' privacy controls to protect consumer data, and to have confidence that these are embedded in the design, technologies, processes and operation of the system. GDS has prepared a Data Protection Impact Assessment (DPIA) of the GOV.UK Verify service to provide assurance that the service can, or will in future, deliver against these requirements. The DPIA is complementary to previous DPIAs and the various security and legal reviews prepared for GOV.UK Verify.

2.2 History and Context

Cabinet Office has a Knowledge & Information Management team that is responsible for privacy issues across the department. An initial DPIA and data protection compliance check based on Cabinet Office guidelines were prepared in September 2014 as part of the project approval for GOV.UK Verify.

Since then, GDS appointed first an Independent Privacy Advisor, and then a permanent Privacy Officer. This DPIA, which was initially prepared in February 2015, replaced the earlier DPIA, and has been updated to reflect the project since then. The DPIA method is both broader in scale and deeper in its investigation of privacy issues than the original checks.

The document was originally referred to as a Privacy Impact Assessment, but has been updated to a Data Protection Impact Assessment to reflect the terminology of the new EU General Data Protection Regulation.

2.3 What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (DPIA) is an analysis of a system and/or process from the perspective of the data subject (i.e. an individual whose personal data might be processed by the system) to understand what the privacy-related needs – and associated protections – are from the data subject's point of view.

The DPIA is a complementary process to a security risk assessment, which generally considers risks from the perspective of the data controller (e.g. the owner of the system). The DPIA does not form part of the formal security accreditation process, but can inform it and support broader security outcomes.

At the end of the DPIA process, the organisation should have a firm understanding of privacy-related risks, and whether existing and planned controls are suitable to mitigate those risks to acceptable levels. Remediation plans can be prepared and measured against recommendations.

2.4 Approach

This DPIA uses a methodology based upon the Information Commissioner's Privacy Impact Assessment Code of Practice, but which has been modified to take into account other specific requirements for the GOV.UK Verify environment, most notably the Identity Assurance Principles published by the Cabinet Office Privacy and Consumer Advisory Group (PCAG).

The DPIA approach comprises the following stages:

- ***Preparation:*** Gather details of the project and confirm understanding with the project team;
- ***Analysis:*** Analyse the information to identify the key privacy issues and develop appropriate recommendations. This includes describing the programme's overall privacy risk profile, and examining privacy delivery to confirm areas where privacy-related risks may have a potential impact on stakeholders;
- ***Documentation and Review:*** Circulate the findings within GDS to confirm correctness and ensure that recommendations are practical;
- ***Maintain and Update:*** Revise the document to reflect significant project changes, and consult the DPIA to inform project decisions which may impact privacy and data protection outcomes.

The approach aligns with, but is not intended to replace, the requirements of ISO27001 and related information security standards by providing a risk-based approach, which identifies assets, risks, impacts and associated control areas.

2.5 Scope of Work

The DPIA forms part of the on-going GDS delivery of GOV.UK Verify, and as such there has been no opportunity for a 'big bang' review of all stakeholders, systems and services in a single phase of work. The scope therefore focuses upon a review of the GOV.UK Verify service under Procurement 2, covering those aspects of external stakeholders (e.g. Certified Companies, Government Services) over which GDS has influence as defined in the framework agreement. The scope includes the generic functions of Certified Companies (identity providers) and Government Services, as described in the relevant contracts, service standards and good practice guides, without reference to provider-specific implementations. The review includes subcontractors operating on behalf of GDS, for example for hosting services.

The review includes the use of the Document Checking Service (DCS) in the context of its interface with GOV.UK Verify, but does not look at the internal operation of that service.

The DPIA does not include inspection (audit) of the Federation Hub, Certified Companies (these are inspected as part of the tScheme certification approach) or Government Services. The DPIA does not consider the requirements of the EU General Data Protection Regulation (GDPR), since the final text was only approved in May 2016. GDPR compliance is part of a separate check that will be completed in 2016.

2.6 What this document contains

This document contains the following sections:

- ***Part 1:*** Executive summary: A summary of the key findings and recommendations;
- ***Part 2:*** Introduction: An overview of the review;
- ***Part 3:*** Service description: A brief overview of the GOV.UK Verify programme;
- ***Part 4:*** Privacy screening process: Detailed responses to questions that determine the need for a Small-Scale or Full-Scale DPIA;
- ***Part 5:*** Data Protection Impact Assessment: Consideration of the key issues of the DPIA with associated recommendations;
- ***Part 6:*** Data Protection Compliance Check: Assessment of GOV.UK Verify against the requirements of the Data Protection Act (1998);
- ***Part 7:*** Identity Assurance Principles Compliance Check: Assessment of GOV.UK Verify against the requirements of the Identity Assurance Principles;
- ***Part 8:*** Summary of recommendations.

Where a recommendation has been made in the body text, it is denoted with a shaded reference as shown here.

2.7 About this document

This is an active project document which has been prepared for the purpose of assessing and managing privacy risks in GOV.UK Verify, and has not necessarily been subject to the levels of scrutiny of a formal government publication. Whilst efforts have been made to ensure accuracy, the conclusions and recommendations may be subjective in nature, reflecting the author's experience and opinions.

As an internal project document the DPIA is not necessarily intended to be read by individuals unfamiliar with privacy or identity assurance, and there may be concepts and terms that are not familiar to some readers which are not explained in detail in the document.

The DPIA is revised regularly to reflect the changing GOV.UK Verify project environment, but nevertheless may include inaccuracies where services have developed without time to update the DPIA, or information has not been available to the privacy team at GDS. Note that this document is not intended to provide a qualified legal opinion.

3. Service Description

3.1 Introduction

This section describes, at a high level, the operation of GOV.UK Verify and some of the key privacy aspects of the service. As an internal project document, it is not intended to provide a comprehensive or in-depth guide to all privacy aspects of GOV.UK Verify.

3.2 Stakeholders

The key stakeholders associated with the GOV.UK Verify system include:

- **Service Users:** individuals seeking access to online public services;
- **Certified Companies:** private-sector companies that have been certified to verify users' identities (identity providers);
- **Government Services:** government functions that can consume identities (i.e. relying parties);
- **GDS:** Government Digital Service, which operates the Federation Hub and the Document Checking Service (DCS).

3.3 Service overview

The basic operation of the GOV.UK Verify service is as follows:

- A Service User approaches a Government Service and requests a service for which verification of identity is required;
- The Government Service refers the Service User to the Federation Hub, with an associated request for authentication to a defined level of assurance;
- The Service User selects a Certified Company from the Federation Hub, and is referred to the Certified Company together with the associated request for authentication to a defined level of assurance;
- If the Service User already has an account with the Certified Company, then the Service User authenticates and is referred back to the Federation Hub with the associated assertion of level of assurance;
- If the Service User does not have an account with the Certified Company, then the Certified Company verifies the user against a user-asserted identity, using a combination of external data sources, which which may include the Document Checking Service, which can validate user-asserted document data for passports and driving licences.
- Once the Service User has been verified to the required level of assurance, they are returned to the Federation Hub with a Matching Data Set (MDS) comprising name, address, date of birth, (optionally) gender, history of attributes, and the associated assertion of level of assurance. In some cases, if the Service User cannot verify to the required level of assurance then they may be returned with a lower level of assurance if that is acceptable to the Government Service.
- The Federation Hub returns the Service User to the Government Service together with the associated assertion of level of assurance, and drops out of the session, which continues between the Service User and Government Service.

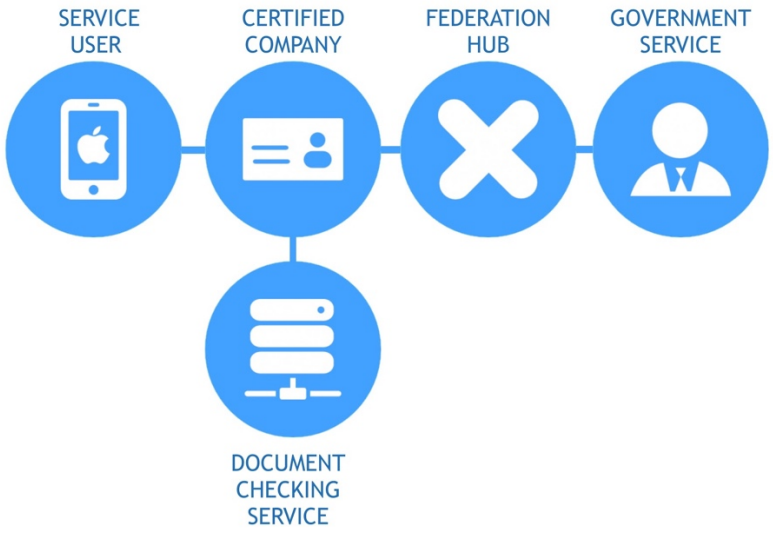

Figure 1: Service overview

The identity assurance data flows are described in detail in the relevant specification[1].

3.4 Privacy overview of the GOV.UK Verify system

GOV.UK Verify has been designed to meet the requirements of the Data Protection Act (1998) and associated privacy-related legislation.

3.4.1 Controller/processor relationships

GDS, the Certified Companies and Government Services are data controllers for their roles within the system. There are no data processors within these roles (although individual data controllers may have appointed their own data processors subject to the contractual constraints of the framework agreement).

3.4.2 Registration

GOV.UK Verify is delivered by the Government Digital Service, which is part of the Cabinet Office that is a registered data controller number Z7414053.

3.4.3 Consent

GOV.UK Verify uses consent to enable processing, and processing is also enabled by Data Protection Act Schedule 2 Part 5 (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, and (d) for the exercise of any other functions of a public nature exercised in the public interest by any person), comprising:

- The Federation Hub does not store personal data (some data is gathered to assist Service Users in selecting a Certified Company, but this does not include any personal details, is not linked to any record of the Service User and is dropped at the end of the session), so does not obtain or require consent to data collection.
- The Certified Company obtains consent to operate an account for the Service User, and to collect, share and maintain the personal information in order to verify and maintain the service user's identity. The Certified Company obtains consent from the Service User to release matching data to the Federation Hub and on to the Government Service, at the request of the Service User.

[1] http://alphagov.github.io/rp-onboarding-tech-docs/pages/saml/samlWorks.html#samlflow-diagram

- The Government Service is bound by a memorandum of understanding that the matching data from the Certified Company may only be used to match the Service User to its own records; any onward use of that data requires further consent from the Service User. The Government Service operates its own privacy notice and consent mechanisms for its ongoing interactions with the service user.

Each Certified Company's privacy notice has been reviewed by the GDS team to ensure that they align with service expectations and that they satisfy the requirements of the framework agreement.

3.4.4 Responsibilities

The Cabinet Office has a Knowledge & Information Management team that has responsibility for data protection and freedom of information issues across the department. The GOV.UK Verify Programme Director has the executive accountability for data protection issues, and a Privacy Officer has been appointed with responsibility for day-to-day management of personal data across GOV.UK Verify.

3.4.5 Privacy Notices

GDS is subject to Cabinet Office policies for personal data management. These are defined in the *Data Protection Act and Copyright Guidance* issued by the Knowledge & Information Management team. A privacy notice and cookie notice specific to GOV.UK Verify are provided on the Federation Hub landing page. The GOV.UK Verify Privacy Officer is developing policies specific to the programme for internal use.

GDS should continue to prepare appropriate internal privacy policies and processes to apply across the GOV.UK Verify programme and ensure that every member of staff is aware of the policies and their duties to follow them.

4. Privacy screening process

4.1 Introduction

As part of the Data Protection Impact Assessment (DPIA) approach, a short assessment - or 'screening process' - can provide an overview of the key privacy issues, and an insight into where further effort should be focussed. This section details the results of the DPIA Screening Process.

4.2 The screening process

The Screening Process comprises a series of questions to be asked of a project at inception. If a few responses are affirmative, then there may be no need for further work; if there are many positive responses then a more detailed review is appropriate. For each question, a response is provided based upon a subjective analysis of the issue. The results are shown in ***Table 1***.

Question	Y/N	Response
Data handling		
Does the project involve the collection and processing of personal information? If so, what types of personal information are involved?	Y	Service Users register by providing a Matching Data Set (MDS) comprising present (and previous) name, address, date of birth and gender. Service Users then go on to provide document details (passport, driving licence) for validation, and answer a series of questions based upon personal information drawn from public-domain sources, e.g. credit records. Personal information (the Matching Data Set only) transits the Federation Hub. The User Support team may process personal information if the Service User provides contact information or transaction data when contacting User Support.
Are individuals easily identifiable from the personal information?	Y	The purpose of GOV.UK Verify is to enable Service Users to assert their identities online. GDS could in theory access the Matching Data Set as it transits the Federation Hub (but this is cryptographically protected), but does not have access to transactional data, since that is handled directly between the Service User and Government Service. GDS' User Support can identify a Service User if the Service User provides contact information, but do not have access to information held in the Certified Company or Government Service.
Does this information include sensitive personal information? If so, what types of sensitive personal information are involved?	N	Personal information which transits the hub does not include sensitive personal information. It is possible that in certain contexts, the Matching Data Set might be considered to be sensitive (e.g. persons at risk), but for such individuals the risk is mitigated by existing protocols to amend or remove identities at Government Services, document issuers and attribute providers (e.g. credit reference agencies). GDS would not be in a position to know that such information is sensitive.

GOV.UK VERIFY DATA PROTECTION IMPACT ASSESSMENT

Question	Y/N	Response
Is any personal information collected relating to an individual of 13 years of age or younger?	N	The service does not knowingly process information relating to individuals of 13 years of age or younger, since there are no Government Services available for that age group at this time, and verification data is not available for users of that age.
Purpose		
Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?	N	The project applies a significant change to the authentication mechanism for Service Users who might previously have used Government Gateway or service-specific authentication, but the MDS should not be particular concern to service users since this is available in the public domain.
Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the system?	N	The project does not handle a considerable amount of personal information about each individual; indeed, one of the purposes of identity assurance is to reduce the amount of information processed by Government Services for the purpose of authentication.
Does the project involve new or significantly changed handling of personal data about a large number of individuals?	Y	The project is intended to provide the default mechanism for individuals to authenticate with Government Services.
Aggregation		
Does the project involve the merging or joining of personal information from several different sources?	Y	The project draws upon information from the Service User, the Document Checking Service and third-party sources (e.g. credit reference agencies and mobile operators), to validate an identity during the registration process. This validation is performed by the Certified Company, and GDS does not see this information. The GDS User Support team can use session ID data and feedback form data to resolve Service User enquiries.
Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?	Y	The project draws upon information from the Service User, the Document Checking Service and third-party sources e.g. credit reference agencies and mobile operators, to validate an identity during the registration process. These are matched by the Federation Hub against the Government Service's record, and the results of this matching are passed to the Certified Company to facilitate a session for the Service User.
Multiple Organisations		
Does personal information flow between multiple organisations (e.g. suppliers/partners)? If so, for what purpose?	Y	GOV.UK Verify enables the flow of information between Service User and Government Service, with the support of the Certified Company, for the purpose of mutual authentication between Service User and Government Service.

Question	Y/N	Response
Do suppliers/partners have the right to use the personal information collected or shared under the service for their own purposes?	N	Certified Companies do not have the right to use the personal information collected or shared under the service for their own purposes (this is an obligation under the framework agreement), although they may seek a separate consent to use personal information as part of other relationships with the Service User. Government Services may use information for their own purposes, but will have to disclose purposes and details of information required to the service user on a per-transaction basis, and seek appropriate consent.
Does the service allow marketing materials to be sent to service users by suppliers/partners?	N	Certified Companies are not permitted to use identity assurance data for other purposes without the Service User's informed consent and contractual permission from GDS.
Can the supplier/partner subcontract all or part of the services?	Y	Certified Companies and Government Services can subcontract some or all of the service delivery, although there are contractual restrictions under the framework agreement on the nature and diversity of subcontracted suppliers, and the locations in which personal data may be processed.
Does the project involve multiple organisations, whether they are government agencies (e.g. in 'joined-up government' initiatives) or private sector organisations (e.g. as outsourced service providers or as 'business partners')?	Y	An underlying principle of identity assurance is to spread service delivery and operation across multiple private sector Certified Companies, in order to provide identity assurance for multiple Government Services.
Does the contract involve the transfer of large volumes of personal information?	Y	In accumulation, large volumes of personal information will be transferred between Certified Companies and Government Services via the Federation Hub (although this will be limited to data in the Matching Data Set for each user).
Overseas transfers		
Is the personal information transferred beyond the country in which the data subject is located? If so, what countries?	Y	Suppliers may operate from offshore locations, but are contractually bound by privacy rules and are not permitted to process data outside of the EEA without suitable controls and specific permission from GDS. GDS may use subcontractors but these need to be contractually bound by privacy rules and may not process data outside of the EEA without suitable controls.
If based in the US is the supplier/partner subject to appropriate legal controls (e.g. model clauses, binding corporate rules)?	Y	Suppliers or their subcontractors wishing to operate from the US are obliged to establish binding corporate rules or equivalent contractual safeguards over privacy practices, and these are checked as part of the onboarding process.
Identity		

Question	Y/N	Response
Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?	N	GOV.UK Verify is designed to minimise data required for registration and authentication compared with current processes.
Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?	Y	GOV.UK Verify reuses new/existing identifiers from the Certified Companies engaged within the scheme.
Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	N	In most cases, GOV.UK Verify reduces the amount of personal information required for a transaction, particularly by facilitating variable levels of assurance proportionate to the use case. GOV.UK Verify facilitates a degree of anonymity and pseudonymity by enabling service users to have multiple identities across multiple Certified Companies, with the Certified Company and Government Service not knowing each other's identities.
If anonymised, can the data and information be converted or interpreted by some means to identify an individual?	N/A	The services processes personal information which is not anonymised. Partial pseudonymisation is provided by the separation of Certified Company and Government Service.
Exemptions and Exceptions		
Does the project relate to data processing which is in any way exempt from legislative privacy protections?	N	GOV.UK Verify is subject to the requirements of the Data Protection Act (1998), Privacy and Electronic Communications Regulations, and other relevant legislation.
Does the project's justification include significant contributions to public security (i.e. crime/counter-terror) measures?	Y	GOV.UK Verify is intended to counter fraud and crime by establishing more robust authentication mechanisms between government and individuals.
Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	N	Certified Companies and Government Services will be subject to strict legislative, regulatory and contractual privacy controls.

Table 1: Privacy Screening Process

4.3 Summary

Of the 24 questions, 13 returned a positive response. The Screening Process demonstrates that whilst there are various privacy controls embedded into the GOV.UK Verify platform, there is nevertheless a need for a detailed review of controls to ensure that these are appropriate for the potential privacy risks associated with its operation.

5. Data Protection Impact Assessment

5.1 Introduction

The Data Protection Impact Assessment identifies stakeholders, assets, threats and potential impacts associated with a system, and recommends mitigating actions to control identified risks. This ensures that stakeholder needs are properly considered in the system delivery.

5.2 Stakeholders

The stakeholder analysis, which identifies key stakeholder groups whose privacy interests may have an influence on, or be influenced by, the personal data processed by the system, is based upon the GOV.UK Verify platform as delivered by Procurement 2 and does not consider possible future stakeholders that might be associated with the system.

The list of stakeholders is shown in ***Table 2***. For each stakeholder, they are marked to indicate their interest in GOV.UK Verify, as:

- **Data Subject:** An individual whose personal data is associated with the project;
- **Data Controller:** An organisation that collects, processes or stores personal data;
- **Data Processor:** An organisation that collects, processes or stores personal data on behalf of a data controller.

Each stakeholder may perform certain actions on personal data, including:

- **Collect:** Collects personal data as part of the service delivery;
- **Process:** Processes or creates/derives personal data as part of the service delivery;
- **Store:** Retains personal data for operational or audit purposes as part of the service delivery;
- **Share:** Shares personal data with third parties within or outside of the GOV.UK Verify ecosystem.

Stakeholder	Description	Subject	Controller	Processor	Collect	Process	Store	Share
Service User	Individual service user	✔						✔
Delegated Service User	Individual service user acting on behalf of another legal person (e.g. individual, company) in a delegated authority role	✔						✔
Certified Company	Private sector organisation issuing credentials on behalf of service users		✔		✔	✔	✔	✔
Certified Company Sub- contractor	Private sector organisation acting on behalf of a Certified Company		✔	✔	✔	✔	✔	✔
Document Checking Service (DCS)	Service offering verification of asserted documents against trusted source (e.g. HM Passport Office, DVLA)		✔		✔	✔	✔	✔
Data Aggregator	Service offering verification of asserted data against trusted source (e.g. credit reference agency)		✔		✔	✔	✔	✔
Federation Hub	Federation Hub operated by GDS providing anonymisation and matching services		✔		✔	✔	✔	✔
GDS User Support	User helpdesk service operated by GDS		✔		✔	✔	✔	✔
Service Provider (SP)	Relying party (e.g. DEFRA, DVLA, HMRC)		✔		✔	✔	✔	
GDS Sub-contractors	Subcontractors offering services to GDS, e.g. hosting, helpdesk platform			✔	✔	✔	✔	✔
Attribute Provider	Organisation offering information to relying parties (e.g. local authority, credit reference agency)		✔		✔	✔	✔	✔
Trust Scheme	Organisation to normalise and manage relationships between providers (e.g. tScheme)							
Regulators	e.g. Information Commissioner's Office							
Industry bodies	e.g. OIX, GSMA							
Media	Print/broadcast/social media							
Privacy advocates	Privacy advocates and pressure groups							
Law enforcement	Police, security services		✔		✔	✔	✔	✔

Table 2: Stakeholder Analysis (continued)

The stakeholder analysis indicates that the key stakeholders to be considered within the Data Protection Impact Assessment are:

- **Data Subjects:** Service Users;
- **Data Controllers:** Certified Companies, Data Aggregators, Document Checking Service, Hub Service, Service Provider, Law Enforcement Agencies.

5.3 Information assets

Prior to the main Data Protection Impact Assessment, a simple stakeholder impact analysis has been prepared to identify the sensitivity of information processed from the perspective of the service users. The personal information assets are shown in ***Table 3***.

Each personal information asset has been assigned a sensitivity where:

- **High:** Personal information that an individual would not choose to reveal without good reason, e.g. financial records, and sensitive personal information including healthcare, sexual history, political beliefs, trades union membership;
- **Medium:** Personal information that would not be found in the public domain;
- **Low:** Personal information likely to be found in the public domain.

Data Asset	Description	Location	Sensitivity
Matching Data Set	Name (& history), address (& history), date of birth, gender	Service User, Certified Company, Federation Hub, Government Service	L
Citizen Verification Data	Passport number and details, driving licence number and details	Service User, Certified Company, Hub, Document Checking Service	M
Money Verification Data	Consented bank records, long-term loans, credit cards, credit history	Service User, Certified Company, Federation Hub	M
Living Verification Data	E.g. Utility records, mobile phone accounts, insurance	Service User, Certified Company, Federation Hub	M
Authentication Credentials	User name, password, mobile device	Service User, Certified Company	H
Transactional Data	User transaction with government department (e.g. tax credit notification)	Service User, Government Service	H
Audit Data	Activity records	Certified Company, Hub, Government Service, Document Checking Service	M
User Support Data	Queries, complaints, User Support information	Certified Company, Government Service, GDS	L
Operational Data	Audit records, statistical analysis	Certified Company, Government Service, GDS	M

Table 3: Personal information assets

The most sensitive information processed are the Service User's authentication credentials and the transactional data between Service User and the Government Service, which sits outside of the GOV.UK Verify domain.

5.4 Data protection Impact

By assessing the likely impact of risk groups on each identified asset, and then considering the severity of the impact for each stakeholder group, the overall data protection impact can be considered, and mitigating controls proposed.

The review considers risks in the context of Confidentiality, Integrity, Availability and Authorisation, which are defined as:

- **Confidentiality:** Accidental or deliberate exposure of personal information (including derived information) within or outside of the GOV.UK Verify environment;
- **Integrity:** Accidental or deliberate modification of personal information;
- **Availability:** Temporary or permanent inability to access some or all of a personal information record;
- **Authorisation:** Accidental or deliberate misuse of personal information.

Table 4 shows the perceived severity of impact levels of each of the data assets when a risk is realised, where severity is considered as:

- **High:** a risk that could cause direct or indirect damages for the Service User, and result in a disruption to the broader GOV.UK Verify service, have legal consequences for GDS, Certified Companies or Government Services, or result in adverse publicity in mainstream media channels;
- **Medium:** a risk that could cause distress or loss of service for a significant number of Service Users, and result in significant efforts by GDS, Certified Companies or Government Services to remedy the problem or handle formal complaints;
- **Low:** a risk that could cause inconvenience for the individual or require action by GDS, Certified Companies or Government Services to remedy the problem.

The assessment is from the perspective of the data subject rather than the data controller, and for this reason some ratings may differ from those that might be assigned in a security assessment. For example, the loss of confidentiality, integrity or availability of the Matching Data Set is considered to be a relatively low risk compared with other data, since this information is likely to be already in the public domain.

Asset	Confidentiality	Integrity	Availability	Authorisation
Matching Data Set	L	L	L	M
Citizen Verification Data	H	H	L	H
Money Verification Data	M	M	L	M
Living Verification Data	M	M	L	M
Authentication Credentials	H	M	L	H
Transactional Data	H	H	L	H
Audit Data	H	H	L	H
User Support Data	L	L	L	L
Operational Data	M	M	L	M

Table 4: Impact severity

The analysis indicates the particular sensitivity of:

- **Citizen verification data:** Information about or from passports and driving licences is commonly used to obtain other forms of ID, and as such is more sensitive than other attribute data;
- **Authentication credentials:** The Service User's credentials to access the service are considered in detail by GOV.UK Verify's security reviews, but should also be treated as sensitive personal information;

- **Transactional data:** The transactions between individuals and government departments are confidential, and even if GOV.UK Verify is not the source of a breach of that confidentiality, an associated incident would erode consumer privacy in the system;
- **Audit data:** A loss of confidence in audit data could reveal information about users and transactions, and undermine confidence in the system.

It should be noted that Money and Living data are generally considered to be of a lower sensitivity than Citizen data since they are used widely for proof of identity/circumstance purposes, and as such are already available to a limited domain of stakeholders. Availability is not considered to be a major risk in this context, since GOV.UK Verify is currently one of a number of ways to access government services: if GOV.UK Verify becomes the only means of access then these levels will need to be revised.

The next stage is to consider data protection impacts upon the Service User, GOV.UK Verify and Regulatory outcome. These are distinct from impacts that might be considered in Impact Level Tables in the formal accreditation process, and are based upon likely outcomes from the identified privacy risks and impacts. The impacts are shown in ***Table 5***.

Asset	Service User Impact	GOV.UK Verify Impact	Regulatory Impact
Matching Data Set	Minimal, data already likely to be in public domain	Loss of trust with service users, adverse publicity	Potential ICO reprimand for failure to protect data
Matching Data Set (for politically exposed persons)	Possible threats to safety of individuals	Loss of confidence from service users, adverse publicity, potential suspension of service	Likely ICO fine for failure to protect data
Citizen Verification Data	Possible loss of service, highly vulnerable to identity theft	Loss of confidence from service users, adverse publicity, potential suspension of service	Potential ICO fine for failure to protect data
Money Verification Data	Possible loss of service, vulnerable to identity theft	Loss of trust with service users, adverse publicity	Potential ICO reprimand for failure to protect data
Living Verification Data	Possible loss of service, vulnerable to identity theft	Loss of trust with service users, adverse publicity	Potential ICO reprimand for failure to protect data
Authentication Credentials	Loss of service, financial damages, potential identity theft	Loss of confidence from service users, potential suspension of service	Unlikely further action unless credentials are misused
Transactional Data	Loss of service, financial damages, potential identity theft	Loss of confidence from service users, potential suspension of service	Likely ICO fine against SP for failure to protect data
Audit Data	Possible disclosure of usage of GOV.UK Verify leading to loss of confidence and vulnerability to identity theft	Loss of confidence from service users, potential suspension of service	Potential ICO fine for failure to protect data
User Support Data	Degraded service for user, risk of identity theft if transaction data included	Loss of trust with service users, adverse publicity	Potential ICO fine for failure to protect data

Table 5: Data protection impacts

The impact analysis indicates the significant responsibilities of the Government Services for protecting authentication, transactional and audit data, and that helpdesk data should be handled with appropriate security controls which are often overlooked in otherwise secure systems.

5.5 Mitigating actions

The final step in the DPIA process is to propose mitigating actions that will control the risks identified previously. For each, the risk should be eliminated, reduced, or accepted. The recommended mitigating actions are shown in ***Table 6***.

Risk	Mitigating Action	Recommendation
Loss, modification or misuse of Matching Data Set	Certified Companies are subject to strict security controls, and the Federation Hub and Document Checking Service have received pan-government accreditation.	GDS should ensure that it has prepared and tested incident response plans to work with stakeholders should a loss, modification or misuse of the Matching Data Set occur.
Loss, modification or misuse of matching data set relating to politically exposed persons	Since politically exposed persons cannot be distinguished from ordinary Service Users by any of the stakeholders, it is not possible to implement special controls.	No recommendation
Loss, modification or misuse of Service User data (e.g. driving licence / passport details), financial data (e.g. credit details) or utility data (e.g. phone account).	The Federation Hub and Document Checking Service have received pan-government accreditation. Certified Companies are subject to contractual obligations for security management and are obliged to report incidents to GDS under the framework agreement.	No recommendation
Disclosure of transactional services between user and service provider	GDS is establishing Transaction Monitoring controls to detect and prevent session hijack.	GDS should continue to support the development of Transaction Monitoring controls to prevent session hijack.
Loss, modification or misuse of audit data	The Federation Hub and Document Checking Service have received pan-government accreditation. Certified Companies are subject to strict security controls.	No recommendation

Table 6: Recommended mitigating actions

5.6 Summary of recommendations and integration into plan

The Data Protection Impact Assessment has identified two recommendations, namely:

- GDS should ensure that it has prepared and tested incident response plans to work with stakeholders should a loss, modification or misuse of the Matching Data Set occur.

- GDS should continue to support the development of Transaction Monitoring controls to prevent session hijack.

5.7 Next steps

The recommendations have been integrated into the GOV.UK Verify project plans, and are subject to regular review (both periodic and in response to significant project changes) by the Privacy Officer.

6. Data Protection Compliance Check

6.1 Introduction

In order to confirm the findings of the DPIA, and ensure completeness of the review, a Data Protection Compliance Check[2] has been conducted, and the results are provided in the section. The process applied in this instance is derived from the UK Information Commissioner's Data Protection Compliance Check.

6.2 Scope of the Data Protection Compliance Check

This Data Protection Compliance Check applies to the GOV.UK Verify service, and specifically those aspects of the service which are within the control of the Government Digital Service, including the Federation Hub and Document Checking Service. Interfaces with Certified Companies are considered, but the operations of the Certified Companies are outside of the scope of the review since they are covered by separate contractual and legal obligations.

6.3 Data Protection Compliance Check

Item	Question	Response	Recommendation
PRINCIPLE 1: FAIR AND LAWFUL PROCESSING Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: • at least one of the conditions in Schedule 2[3] is met, and; • in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.			
1.1	**Preliminary**		
1.1.1	What type of personal data are you processing?	GOV.UK Verify processes a Matching Data Set (MDS) comprising the Service User's name, date of birth, address, gender, and a history of these fields where needed, for the purpose of matching the Service User to a record in the Government Service. The Federation Hub will also have visibility of the Service User's Certified Company, and the Government Service with which they are transacting. The Certified Company may require access to other information from the Service User, their own records, and third-party sources, in order to register, verify and maintain Service User identities, e.g. document checking service, credit reference data, and evidence of other activities including utility records.	No recommendation

[2] http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/3-app2.html

[3] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

Item	Question	Response	Recommendation
		The analytics system may also record the Service User's IP address, browser used, OS version, and whether javascript is enabled. When users contact the User Support team, they can give their name and email address in addition to the description of their problem.	
1.1.2	Are sensitive personal data being differentiated from other forms of personal data?	GOV.UK Verify does not knowingly process sensitive personal data. In certain contexts, Matching Data Set data might be considered sensitive (e.g. home address of politically exposed persons, stated gender of a transgendered person), and that the data collected and held by Government Services for the purposes of registering, verifying and maintaining identities could, in certain cases, be sensitive.	No recommendation
1.2	**Schedule 2 - Grounds for Legitimate Processing of Any Personal Data**		
1.2.1	Have you identified all the categories of personal data that you will be processing and how?	Yes. Personal data handled by the Federation Hub is limited to the Matching Data Set (name, DoB, address, gender, and history of these where needed). Personal data handled by Certified Companies will vary according to the nature of their solution, but is subject to the definitions in *GPG45 Identity Proofing and Verification of an Individual Using Public Services*[4], the IPV Operations Manual as well as the *Identity Assurance Principles* issued by the Privacy and Consumer Advisory Group[5]. The User Support service processes the minimum data that is needed to resolve queries raised by Service Users. If a Service User provides more information than is needed to resolve a query, then it is immediately deleted.	No recommendation
1.2.2	Have you identified the purposes for which you will be	Yes. GDS will process personal data for the purpose of matching Service Users to Government Service records. Purposes for	N/A

[4] https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

[5] https://identityassurance.blog.gov.uk/2015/09/11/gov-uk-verify-identity-assurance-principles/

Item	Question	Response	Recommendation
	processing personal data and how?	Certified Companies processing personal data are defined within the procurement documentation, and Certified Companies are obliged to clearly state purposes in their privacy notices. The User Support team processes Service User data to resolve Service User enquiries.	
1.2.3	Have you identified which of the grounds in Schedule 2[6] you will be relying on as providing a legitimate basis for processing personal data?	Yes. The processing is necessary under Schedule 2 Part 5 (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, and (d) for the exercise of any other functions of a public nature exercised in the public interest by any person. Certified Companies are obliged by the framework agreement to obtain consent for processing and sharing information with Government Services.	N/A
1.2.4	Are you relying on different grounds for different categories of personal data?	No. All personal data is processed under the same grounds.	N/A
1.3	**Schedule 3 - Grounds for Legitimate Processing of Sensitive Personal Data**		
1.3.1	Have you identified the categories of sensitive personal data that you will be processing?	There is no expectation that sensitive personal data will be processed knowingly by the Federation Hub or Certified Companies for the delivery of GOV.UK Verify. Government Services may process sensitive personal data, but this will be outside of the scope of the GOV.UK Verify system.	No recommendation
1.3.2	Have you identified the purposes for which you will be processing sensitive personal data?	There is no intention knowingly to process sensitive personal data. If such data were unknowingly processed in a given context (e.g. politically exposed persons) then it would be for the same purposes as identified in 1.2.2.	No recommendation
1.3.3	Have you identified which of the grounds in	There is no intention to knowingly process sensitive personal data.	No recommendation

[6] http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_10

Item	Question	Response	Recommendation
	Schedule 3[7] you will be relying on as providing a legitimate basis for processing sensitive personal data?		
1.3.4	Are you relying on different grounds for different categories of sensitive personal data?	There is no intention to knowingly process sensitive personal data.	No recommendation
1.4	**Obtaining consent**		
1.4.1	Are you relying on the individual to provide consent to the processing as grounds for satisfying Schedule 2?	Yes. GOV.UK Verify relies on Schedule 2 Part 5 (c) and Part 5 (d) to provide a legitimate basis for processing, but also asks the Service User to provide consent to the processing as further grounds for satisfying Schedule 2. Consent is obtained from the Service User by the Certified Company at time of registration. Personal data collected or processed by the Government Service is subject to a separate consent arrangement between the Service User and the Government Service, which sits outside of the scope of GOV.UK Verify.	No recommendation
1.4.2	For the processing of sensitive personal data, are you relying on explicit consent as specified in Schedule 3, s1 of the Data Protection Act?	GDS will not knowingly process sensitive personal data. Where a Certified Company may need to process sensitive personal data for purposes unrelated to GOV.UK Verify, this will rely on explicit consent from the service user.	No recommendation
1.5	**Lawful processing**		
1.5.1	Does your processing of personal data fall within your statutory powers?	The processing of personal data by GDS is not subject to statutory powers. For some Government Services, processing may fall under statutory powers, but this falls	No recommendation

[7] http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_10

Item	Question	Response	Recommendation
		outside of the scope of GOV.UK Verify.	
1.5.2	How is compliance with the UK Human Rights Act (1998) being assessed?	Compliance with the UK Human Rights Act (1998) is subject to scrutiny by GDS' legal advisors, and is not within the scope of this review.	No recommendation
1.5.3	Are you assessing whether any of the personal data being processed is held under a duty of confidentiality (e.g. doctor/patient or lawyer/client privilege)?	The personal data being processed is not subject to a duty of confidentiality.	No recommendation
1.5.4	How is that confidentiality maintained? (e.g. instructions on disclosure or shredding)	The personal data being processed is not subject to a duty of confidentiality. GDS, Government Services and Certified Companies are subject to specific controls over data destruction.	No recommendation
1.5.5	Are you assessing whether your processing is subject to any other legal or regulatory duties?	Yes. Compliance with other legal or regulatory duties (e.g. Privacy and Electronic Communications Regulations) is the responsibility of the Cabinet Office Knowledge & Information Management team.	No recommendation
1.5.6	How are you ensuring that those legal duties are being complied with?	Compliance with other legal or regulatory duties (e.g. Privacy and Electronic Communications Regulations) is the responsibility of the Cabinet Office Knowledge & Information Management team.	No recommendation
1.6	**Fair processing**		
1.6.1	Are individuals being made aware of the identity of your organisation as the data controller?	Yes. GDS is a data controller for its role in GOV.UK Verify delivery, as are the Certified Companies. GDS' notification as a data controller is covered in the broader Cabinet Office notification handled by the Knowledge & Information Management team. Certified Companies are obliged to confirm their notification as a mandatory requirement under the framework agreement.	No recommendation

Item	Question	Response	Recommendation
1.6.2	How are individuals being made aware of how their personal data is being used?	Privacy notices are managed by individual Certified Companies and Government Services. Government Services will have to ensure that their privacy notices comply with the Identity Assurance Principles defined by the Privacy & Consumer Advisory Group (PCAG), and the procurement process has been subject to review against those requirements. Consent is obtained as part of the transaction with the Service User.	No recommendation
1.6.3	How are individuals offered the opportunity to restrict processing for other purposes? When is that opportunity offered?	GDS contractually prevents Certified Companies from using personal data collected for the use of the GOV.UK Verify for other purposes without first obtaining informed consent from the Service User and permission from GDS. Data derived from the Document Checking Service may not be used for other purposes.	No recommendation
1.6.4	Do you receive information about individuals from third parties?	Yes. GOV.UK Verify creates a federation of data sources to verify the identity of Service Users. Data is only received as a result of the service user applying for the service, and providing consent to sharing information with GOV.UK Verify. Sources, data types and processing purposes are identified within the privacy notice.	No recommendation
1.6.5	How are individuals informed that the data controller is holding personal data about them? When are individuals informed?	Service Users are informed about the processing at the start of their registration process. Certified Companies obtain consent for sharing as part of the transaction, and are obliged to publish privacy notices.	No recommendation
1.7	**Exemptions from the First Data Protection Principle**		
The UK Data Protection Act requires[8] that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:- 1. the identity of the data controller; 2. the identify of any nominated data protection representative, where one has been appointed; 3. the purpose(s) for which the data are intended to be processed;			

[8] http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9#sch1-pt2

Item	Question	Response	Recommendation
4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.			
1.7.1	Do you provide individuals with all of the information in the box above? If no, which exemption to these provisions is being relied upon?	Yes. The Federation Hub links to GDS' privacy notice[9] which provides Service Users with the information required. Certified Companies are obliged by the framework agreement to publish privacy notices.	No recommendation
PRINCIPLE 2: PURPOSE LIMITATION Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.[10]			
2.1	**Preliminary**		
2.1.1	Are procedures in place for maintaining a comprehensive and up-to-date record of use of personal data?	No. Whilst there are strict controls over data use defined in the framework agreement, GDS has yet to establish procedures to maintain a comprehensive and up-to-date record of use of personal data.	GDS should establish procedures to create and maintain a comprehensive record of use of personal data across the GOV.UK Verify ecosystem. The record should include details of processing carried out on GDS' behalf. This record should be checked regularly.
2.1.2	How often is this record checked?	GDS has yet to establish procedures to maintain a comprehensive and up-to-date record of use of personal data.	See 2.1.1
2.1.3	Does the record cover processing carried out on your behalf (e.g. by a subcontractor)?	GDS has yet to establish procedures to maintain a comprehensive and up-to-date record of use of personal data.	See 2.1.1
2.1.4	What is the procedure for notifying (where necessary) the data subject of the purpose for processing their personal data?	GDS notifies data subjects of the purpose for processing their personal data in the privacy notice which is accessible from the Federation Hub. Certified Companies are obliged by the framework agreement to provide similar notifications.	No recommendation
2.2	**Use of Existing Personal Data for New Purposes**		

[9] https://www.signin.service.gov.uk/privacy-notice

[10] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

Item	Question	Response	Recommendation
2.2.1	Does the project involve the use of existing personal data for new purposes?	Yes. The project uses existing personal data from sources such as identity documents and credit reference files, for new purposes including the provision of online identity assurance services.	No recommendation
2.2.2	How is the use of existing personal data for new purposes being communicated to:- (a) the data subject; (b) the person responsible for Notification within the organisation; (c) the Information Commissioner?	Certified Companies are obliged to inform Service Users of the purposes for processing, and the data that may be processed, at the point the Service User accesses the Government Service through the Certified Company. Certified Companies must obtain permission from GDS to use personal data for new purposes, and are responsible for notifying the Information Commissioner of the use of personal data for new purposes if that happens.	No recommendation
2.2.3	What checks are being made to ensure that further processing is not incompatible with its original purpose?	Certified Companies are contractually prohibited from further processing beyond the original purpose without explicit consent from the Service User. Certified Companies are contractually prohibited from reusing information derived from the Document Checking Service (this being a Y/N response to a check on information provided by the Service User).	No recommendation
2.3	**Disclosures of Data**		
2.3.1	Do you have a policy on disclosures of personal data within your organisation / to third parties? Is it documented?	Yes. GDS is subject to Cabinet Office data protection policies. It is not possible for GDS staff to access personal data as it transits the Federation Hub.	No recommendation
2.3.2	How are staff made aware of this policy / instructed to make disclosures?	GDS is subject to Cabinet Office data protection policies that include the disclosure of personal data.	No recommendation
2.3.3	How are individuals / data subjects made aware of	GDS is subject to Cabinet Office data protection policies that include the disclosure of personal data.	No recommendation

Item	Question	Response	Recommendation
	disclosures of their personal data?		
2.3.4	Do you assess the compatibility of a 3rd party's use of the personal data to be disclosed?	GDS is subject to Cabinet Office data protection policies that include the disclosure of personal data.	No recommendation
PRINCIPLE 3: ADEQUATE, RELEVANT AND NOT EXCESSIVE Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.[11]			
3.1	**Preliminary**		
3.1.1	How is the adequacy of personal data for each purpose determined?	GOV.UK Verify is designed around a principle of data minimisation; and the programme should enable a radical reduction in the amount of personal data held by government. GDS has exhaustively reviewed the adequacy of personal data for use in the Matching Data Set (MDS), and Certified Companies' use of personal data is strictly defined by the Good Practice Guides. The onward use of personal data by Government Services is not within the scope of GOV.UK Verify.	No recommendation
3.1.2	How is an assessment made as to the relevance (i.e. no more than the minimum required) of personal data for the purpose for which it is collected?	The relevance of data collected has been defined in the Matching Data Set (MDS), and has been subject to lengthy consultation with Government Services to understand the minimum data that is needed to reliably match an individual within a dataset. Certified Companies are obliged by regulations to retain an audit trail of registration data for the purposes of fraud prevention and criminal investigation.	No recommendation
3.1.3	What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in	GOV.UK Verify does not collect personal data. The User Support team may record data as part of the support process, and they work under defined processes to ensure that they retain no more information than necessary to assist the Service Users. Certified Companies are obliged to prepare and maintain	No recommendation

[11] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

Item	Question	Response	Recommendation
	relation to the purpose for which data are being processed? How often will these procedures be reviewed?	collection and retention policies to ensure that data collection procedures remain adequate, relevant and not excessive in relation to the purpose of collection.	
3.1.4	Are there procedures for assessing the amount and type of personal data collected for a particular purpose?	Yes. See 3.1.3	No recommendation
3.1.5	Are items of personal data held in every case which are only relevant to a subset of those cases?	No. The Matching Data Set has been minimised to a point where data is not held in every case even when it is relevant only to a subset of those cases.	No recommendation
PRINCIPLE 4: ACCURATE AND UP TO DATE Personal data shall be accurate and, where necessary, kept up to date.[12]			
4.1	**Preliminary**		
4.1.1	Are personal data evaluated to establish the degree of damage to both the data subject / data controller that could be caused through inaccuracy?	Yes. Personal data is effectively evaluated by the Service User: the consequence of inaccurate personal data in the Certified Company or Government Service would be a failure to match the Service User with their record, thereby requiring the Service User to notify the Certified Company or Government Service, so that the record is updated and service restored.	No recommendation
4.1.2	How, and how often, are personal data checked for accuracy? Please give examples.	Personal data is checked as part of its use in each transaction by the Service User, and is verified for accuracy at least annually by the Certified Company.	No recommendation
4.1.3	In what circumstances is the accuracy of the personal data	Personal data is checked for accuracy at the time of use by the matching process instigated at the Service User's authentication.	No recommendation

[12] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

Item	Question	Response	Recommendation
	being checked with the data subject?		
4.1.4	Are the sources of personal data (i.e. data subject, data user, or third party) identified in the record? If so, how? Please give examples:	Personal data sources are recorded by the Certified Company at time of registration and reverification in accordance with the requirements of GPG45 and the IPV Operations Manual.	No recommendation
4.1.5	Is there any facility to record notifications received from the data subject if they believe their data to be inaccurate? If no, please indicate why not.	Yes. There is no requirement for Certified Companies to record notifications from the Service User if they believe their data to be inaccurate, since the Service User can immediately update that data to rectify the inaccuracy. Inaccuracies reported to the Government Service should be updated immediately by the Government Service, although this is outside of the scope of GOV.UK Verify.	No recommendation
4.2	**Keeping personal data up to date**		
4.2.1	Are there procedures to determine when and how often personal data requires updating?	Yes. Personal data is updated at least annually by the Certified Company as part of the reverification process mandated in GPG45 and the IPV Operations Manual; or on an *ad hoc* basis by the Service User when they use the system.	No recommendation
4.2.2	Are personal data evaluated to establish the degree of damage to: (a) the data subject, or (b) the data controller that could be caused through being out of date? Please specify whether to data subject or data controller:	No. There is no requirement to assess personal data to establish the degree of damage that might be caused by data being out of date, since out of date data would result solely in the Service User being unable to match when trying to access a Government Service, and then updating their personal data and thereby remedying the problem. Should a Service User experience problems arising from inaccuracies in third-party data sources (e.g. credit reference data) then the User Support function can assist and advise as appropriate. User accounts expire after one year if they are not reverified.	No recommendation
4.2.3	Are there procedures to	Yes. GOV.UK Verify does not collect free text information or other	No recommendation

Item	Question	Response	Recommendation
	monitor the factual relevance, accuracy and timeliness of free text options or other comments about individuals?	options about individuals. User Support may collect minimal amounts of data to resolve Service User enquiries, but is subject to procedures to monitor the factual relevance, accuracy and timeliness of free text options or other comments about individuals.	
PRINCIPLE 5: NO LONGER THAN NECESSARY Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.[13]			
5.1	**Preliminary**		
5.1.1	What are the criteria for determining retention periods of personal data? How often are these criteria reviewed?	Retention periods of personal data are defined by the Service Standards, which mandate that Certified Companies must maintain a records relating to an identity for 12 months after its' last use, after which it becomes obsolete and is deleted. Audit records are retained for seven years in keeping with HMRC requirements, since the transaction records may have a tax implication, but Certified Companies will not be able to distinguish which records are relevant since they do not know which Government Services have consumed the data.	GDS should establish protocols to ensure the regular review of retention periods for personal data.
5.1.2	Does the project(s) include the facility to set retention periods?	Yes. The Federation Hub and Certified Companies will retain audit records for seven years in keeping with HMRC anti-fraud requirements.	No recommendation
5.1.3	Is the project subject to any statutory / sectoral requirements on retention? If yes, please state relevant requirements:	The project is not subject to statutory/sectoral requirements on retention (although some Certified Companies may be subject to their own industry requirements, e.g. FCA for banks). However there are recommended retention periods in the IPV Operations Manual.	No recommendation
5.2	**Review and deletion of personal data**		
5.2.1	Is there a review policy? Is it documented?	No. GOV.UK Verify does not retain personal data in the Federation Hub, and very limited personal data in the User Support service. Certified Companies' retention	See 5.1.1

[13] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

Item	Question	Response	Recommendation
		periods and deletion policies are mandated under the framework agreement.	
5.2.2	When data is no longer necessary for the purposes for which it was collected: (a) How is a review made to determine whether the data should be deleted? (b) How often is the review conducted? (c) Who is responsible for determining the review? (d) If the data is held on a computer, does the application include a facility to flag records for review / deletion?	GDS does not retain personal data in the Federation Hub (except for audit purposes). User Support may retain some personal data, which is subject to a specific policy for their collection, use and deletion of personal data.	No recommendation
5.2.3	Are there any exceptional circumstances for retaining certain data for longer than the normal period? If yes, please give justification:	No. There are no exceptional circumstances for the Certified Company or GDS retaining certain data for longer than the normal period. However, retention could be mandated by law enforcement authorities under a warrant for the purpose of investigating criminal activity.	No recommendation
5.2.4	Is there any guidance on deletion / destruction of personal data? If no, please indicate why not.	Yes. Certified Companies are bound by deletion/destruction requirements defined in the framework agreement. GDS has prepared guidance on deletion/destruction of personal data in the User Support service.	No recommendation
PRINCIPLE 6: DATA SUBJECT ACCESS Personal data shall be processed in accordance with the rights of data subjects under this Act.[14]			

[14] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

Item	Question	Response	Recommendation
6.1.1	Are procedures in place to provide access to records under this Principle? If yes, please specify proposed procedures. If no, please indicate why not.	Yes. GDS is subject to Cabinet Office policies and procedures for subject access requests. GDS mandates that Certified Companies must provide subject access for Service Users, and the framework agreement mandates that Certified Companies must inform Service Users how to access their information, and to report on subject access request volumes and outcomes.	No recommendation
6.1.2	How do you locate all personal data relevant to a request (including any appropriate 'accessible' records)?	As a privacy protection, if the unique identifier of one 'end' of a transaction is known then the Federation Hub service can only release the unique identifier of the other 'end'. To obtain information relating to an end-to-end transaction, the Certified Company and the Government Service (as separate data controllers) would need to provide the Service User's information to GDS. In practice, the Service User would need to contact the Certified Company and Government Service separately to obtain their personal data.	No recommendation
6.1.3	Do you provide an explanation of any codes or other information likely to be unintelligible to a data subject? If yes, how? If no, please indicate why not.	GDS is subject to Cabinet Office policies and procedures for subject access requests. GDS does not specifically mandate subject access procedures for Certified Companies, but an explanation of codes or other information is a legal requirement for them to deliver a compliant solution, and failure to do so would be an effective breach of the framework agreement.	No recommendation
6.1.4	Are procedures in place to manage personal data relating to third parties?	GDS is subject to Cabinet Office policies and procedures for subject access requests.	No recommendation
6.1.5	How is data relating to third parties managed?	GDS is subject to Cabinet Office policies and procedures for subject access requests.	No recommendation
6.2	**Withholding of personal data in response to a subject access request**		
6.2.1	Are there any circumstances where you would	Yes. GDS is subject to Cabinet Office policies and procedures for subject access requests. Data	No recommendation

Item	Question	Response	Recommendation
	withhold personal data from a subject access request? If no, go to section 6.3. If yes, on what grounds?	might be withheld from a subject access request if GDS or a Certified Company are subject to legal obligations to withhold (e.g. Service User is subject to an ongoing criminal investigation); or if there are concerns that the application has not been authenticated in accordance with the sensitivity of data held.	
6.2.2	How are the grounds for doing so identified?	GDS is subject to Cabinet Office procedures for determining whether to withhold personal data from a subject access request.	No recommendation
6.2.3	Are there circumstances under which data subjects might be coerced into submitting an 'enforced subject access' request (e.g. to obtain a copy of their criminal record for employment purposes)?	There is a low level of likelihood that Service Users would be coerced into a committing an enforced subject access request, given that the information about them would be available in credit reference agencies, mobile network operators and other primary sources. The framework agreement mandates that Certified Companies must monitor and report on potential enforced subject access requests.	No recommendation
6.3	**Processing that may cause damage or distress**		
6.3.1	Do you assess how to avoid causing unwarranted or substantial damage or unwarranted and substantial distress to an individual?	The potential for unwarranted or substantial damage or unwarranted and substantial distress to an individual is anticipated to be very low, given that individuals are not obliged to use GOV.UK Verify, and that possible service outcomes are success or failure to verify with a Government Service. Where a Service User fails to verify, the Government Service is obliged to provide alternative mechanisms. Nevertheless, GDS has delivered a Data Protection Impact Assessment, covering all aspects of the GOV.UK Verify service, to check that processing does not cause unwarranted or substantial damage or distress to an individual.	No recommendation
6.3.2	Do you take into account the possibility that such damage or distress to the	Yes. The possibility of compensation claims arising from damage or distress to the individual is considered in the scope of the	No recommendation

Item	Question	Response	Recommendation
	individual could leave your organisation vulnerable to a compensation claim in a civil court?	Data Protection Impact Assessment.	
6.4	**Right to object**		
6.4.1	Is there a procedure for complying with an individual's request to prevent processing for the purposes of direct marketing?	No. GDS does not retain data that could be used for the purpose of direct marketing. GDS does not engage in direct marketing. Certified Companies are contractually obliged not to use GOV.UK Verify data for the purposes of direct marketing (although they may have such a relationship with the Service User as part of unrelated services and consent notices).	No recommendation
6.5	**Automated decision-taking**		
6.5.1	Are any decisions affecting individuals made solely on processing by automatic means?	Yes. The ability of a Service User to authenticate with a Government Service depends upon processing of their information by the Certified Company. The nature of the decision-taking is defined in the GPGs and each Certified Company's implementation is assessed as part of their onboarding process. In the event that automated decision-taking causes Service User problems which cannot be resolved through the Certified Company, the Service User may escalate their problem to GDS User Support.	No recommendation
6.6	**Rectification, Blocking, Erasure and Destruction**		
6.6.1	What is the procedure for responding to data subject's notice (in respect of accessible records) or a court order requiring: (a) rectification; (b) blocking; (c) erasure or;	GDS is subject to Cabinet Office procedures for responding to individuals' notice or a court order requiring rectification, blocking, erasure or destruction of personal data. Certified Companies and Government Services are responsible for establishing their own procedures, and as data controllers, will have primary responsibility for handling such requests (with GDS then servicing	GDS should establish User Support procedures for reviewing and responding to Service User's notice or a court order for rectification, blocking, erasure or destruction of personal data.

Item	Question	Response	Recommendation
	(d) destruction of personal data?	these on their behalf if required to do so).	
PRINCIPLE 7: DATA SECURITY Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.[15]			
7.1	**Security policy**		
7.1.1	Is there a Data Security Policy? If no, please indicate why not and then go to 7.1, question 5.	Yes. Certified Companies are responsible for drafting and enforcing their own data security policies, as mandated in the framework agreement, and are expected to demonstrate compliance with ISO27001 and equivalents in order to join tScheme. The Federation Hub service (excluding Certified Companies) has been subject to pan-government accreditation, with security policies which have been derived using the requirements of HMG IS1 and RSDOPS (GPG43). Government Services are responsible for their own security controls in accordance with the same government policy requirements.	No recommendation
7.1.2	If yes, who / which department(s) are responsible for drafting and enforcing the Data Security Policy within the organisation?	Certified Companies are responsible for drafting and enforcing their own data security policies, as mandated in the framework agreement. GDS' own security policies are drafted by the IA National Technical Authority (CESG).	No recommendation
7.1.3	Does the Data Security Policy specifically address data protection issues?	Yes. The accreditation process requires legal compliance with the Data Protection Act (1998), and covers managing risks associated with personal data handling. Certified Companies are obliged to comply with ISO27001 which mandates the need for data protection compliance.	No recommendation
7.1.4	What are the procedures for monitoring	The service is maintained within GDS to ensure that it remains compliant with the conditions of	No recommendation

[15] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

Item	Question	Response	Recommendation
	compliance with the Data Security Policy within the organisation?	accreditation (RMADS). There are regular accreditation reviews, and ad hoc reviews would be conducted in response to specific changes of circumstances. Certified Companies are obliged to comply with ISO27001 which mandates the need for monitoring compliance with the information security policy, and must maintain that status as part of their contract.	
7.1.5	Does the level of security that has been set take into account the state of technological development in security products and the cost of deploying or updating these?	Yes. The risk assessment process that generates and maintains the RMADS takes into account the state of technological advancements in threats and controls. The formal accreditation of the hub service includes annual review and continuous upgrade and improvement. The identity assurance system incorporates innovative security intelligence and fraud detection mechanisms. Individual Certified Companies are expected to comply with ISO27001 but are not mandated to adopt specific technologies; but nevertheless have to demonstrate that their technology controls are appropriate to the risk levels and the broader environment.	No recommendation
7.1.6	Is the level of security appropriate for the type of personal data processed?	Yes. The Federation Hub has been subject to formal security accreditation with security levels that exceed those required for the type of personal data processed. Mandated compliance with ISO 27001 for Certified Companies reflects industry good practice for security.	No recommendation
7.1.7	How does the level of security compare to industry standards, if any?	Government security requirements provide parity with the requirements of ISO27001, and reflect good practice in information security management.	No recommendation
7.2	**Unauthorised or unlawful processing of data**		
7.2.1	Describe security measures that are in place to prevent any unauthorised or	Certified Companies are obliged to comply with the requirements of ISO 27001 and ISO 15489-1, which include requirements for the prevention of unauthorised or	No recommendation

Item	Question	Response	Recommendation
	unlawful processing of: (a) Data held in an automated format (e.g. password controlled access to PCs) (b) Data held in a manual record (e.g. locked filing cabinets)?	unlawful processing of automated and manual data.	
7.2.2	Is there a higher degree of security to protect sensitive personal data from unauthorised or unlawful processing? If yes, please describe the planned procedures. If no, please indicate why not.	No. GDS does not knowingly collect or process sensitive personal data. Certified Companies may, on occasion, unknowingly process sensitive personal data as part of their verification of Service Users (e.g. where the Service User is a politically exposed person). GDS does not impose specific obligations upon Certified Companies for how they handle that data, since they would have no way of identifying it as sensitive.	No recommendation
7.2.3	Describe the procedures in place to detect breaches of security (remote, physical or logical)?	GDS' accreditation takes into account the physical and logical environment for the service delivery. GDS operates protective monitoring controls for the hub service, and is establishing a Transaction Monitoring service to consider vulnerabilities and protections in end-to-end security. The framework agreement does not stipulate specific controls for Certified Companies for detecting security breaches (although this would be covered by their ISO27001 compliance), but it does mandate breach reporting.	No recommendation
7.3	**Destruction of personal data**		
7.3.1	Describe the procedures in place to ensure the destruction of personal data no longer necessary?	GDS is subject to the Security Policy Framework and associated government policies for the destruction of personal data. GDS does not stipulate specific controls for the destruction of data. Certified Companies are obliged to comply with the requirements of ISO 27001 and ISO 15489-1, which require	No recommendation

Item	Question	Response	Recommendation
		organisations to provide suitable data destruction controls.	
7.3.2	Are there different procedures for destroying sensitive personal data?	No. GDS is subject to the Security Policy Framework and associated government policies for the destruction of personal data. GDS does not stipulate specific controls for the destruction of data. Certified Companies are obliged to comply with the requirements of ISO 27001 and ISO 15489-1, which require organisations to provide suitable data destruction controls.	No recommendation
7.4	**Contingency Planning - Accidental loss, destruction, damage to personal data**		
7.4.1	Is there a contingency plan to manage the effect(s) of an unforeseen event?	Yes. GDS has contingency plans for a failure of the Federation Hub and Document Checking Service. Certified Companies are obliged to comply with the requirements of ISO 27001 and ISO 15489-1, and the effect of an event would put them in breach of their key performance indicators under individual call-offs.	No recommendation
7.4.2	Describe risk management procedures to recover data (both automated and manual) which may be damaged/lost through: human error; computer virus; network failure; theft; fire; flood; other disaster.	The RMADS defines protocols for responding to data loss incidents and recovering data/services. Certified Companies are obliged to comply with the requirements of ISO 27001 and ISO 15489-1, which include requirements for risk management during serious incidents. Failure to offer continuity of service would be a breach of performance levels prescribed in each contractual call-off.	No recommendation
PRINCIPLE 8: OVERSEAS TRANSFER Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.[16]			
8.1	**Data transfers**		

[16] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

Item	Question	Response	Recommendation
8.1.1	Are you transferring personal data to a country or territory outside of the EEA?	GDS does not transfer personal data to a country or territory outside of the EEA. Where Certified Companies might transfer data outside of the EEA (for example, use of cloud hosting to deliver their services) they are legally and contractually obliged to have adequate legal safeguards in place, and these are assessed as part of the onboarding process.	No recommendation
8.1.2	What types of data are transferred? (e.g. contact details, employee records)	See 8.1.1	No recommendation
8.1.3	Are sensitive personal data transferred abroad?	See 8.1.1	No recommendation
8.1.4	What are the main risks involved in the transfer of personal data to countries outside the EEA?	If a Certified Company were to transfer personal data to countries outside the EEA, then that might be intercepted by third parties. GDS assesses the adequacy of safeguards over Certified Companies' transfers of personal data and these are not permitted unless suitable safeguards are in place.	No recommendation
8.1.5	Are measures in place to ensure an adequate level of security when the data are transferred to another country or territory?	Yes. Certified Companies are obliged to apply suitable controls if they wish to transfer data to another country or territory, and these are assessed as part of the onboarding process.	No recommendation
8.1.6	Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?	Yes. GDS assesses the adequacy of safeguards over Certified Companies' transfers of personal data and this is not permitted unless suitable safeguards are in place.	No recommendation
8.2	**Exempt Transfers**		

Item	Question	Response	Recommendation
8.2.1	Is your organisation carrying out any transfers of data where it has been decided that the Eighth Principle does not apply?	No. There are no transfers where the Eighth Principle does not apply.	No recommendation
8.2.2	To which country/territory are these transfers made?	See 8.2.1	No recommendation
8.2.3	What are the criteria set by your organisation, which must be satisfied before a decision is made about whether the transfer is exempt from the Eighth Principle?	See 8.2.1	No recommendation
8.3	**Monitoring**		
8.3.1	What reasonable steps did you take to ensure that the Data Processor complies with data protection requirements?	Cabinet Office is a data controller under the GOV.UK Verify contracts, with Certified Companies and Government Services also acting as data controllers. All parties are contractually obliged to comply with data protection requirements, and to obtain trust scheme accreditation. GDS' subcontractors are obliged to comply with appropriate government policies for the destruction of personal data.	No recommendation
8.3.2	How did you assess their data security measures?	Certified Companies are required to obtain certification from an approved trust body, including certification of their security measures. They are also required to comply with ISO 27001 and ISO 15489-1.	No recommendation
8.3.3	How do you ensure that the Data Processor complies with these measures?	Compliance with security requirements is assessed through binding declarations by Certified Companies in their contracts with GDS. Failure to provide adequate security is treated as a breach of contract.	No recommendation

Item	Question	Response	Recommendation
8.3.4	Is there an on-going procedure for monitoring their data security measures?	Yes. Compliance with trust scheme certification and security standards must be maintained for Certified Companies to continue to remain under contract. Failure to maintain compliance would be treated as a breach of contract.	No recommendation

7. Identity Assurance Principles Compliance Check

7.1 The Identity Assurance Principles

The Privacy and Consumer Advisory Group (PCAG)[17] is an independent body comprising representatives from privacy campaign groups, civil society and acknowledged experts on the subject. It was established to help GDS develop an approach to identity assurance that, amongst other things, ensures users are in control of their information, that information is not centralised and that users have a choice of who provides services on their behalf.

In June 2013, PCAG released a set of Identity Assurance Principles which set out, in detail, how GOV.UK Verify could be configured to meet the privacy and consumer expectations of its users. A second version of the document was released in September 2014 to incorporate feedback received during a consultation on the draft version published in June 2013. This was the second round of consultation, following an earlier draft published in April 2012.

The principles have been accepted by GDS, and are subject to ongoing review by PCAG. The Identity Assurance Principles are as follow:

1. **User Control:** I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them.
2. **Transparency:** Identity assurance can only take place in ways I understand and when I am fully informed.
3. **Multiplicity:** I can use and choose as many different identifiers or identity providers as I want to.
4. **Data Minimisation:** My interactions only use the minimum data necessary to meet my needs.
5. **Data Quality:** I choose when to update my records.
6. **Service User Access and Portability:** I have to be provided with copies of all of my data on request; I can move / remove my data whenever I want.
7. **Certification:** I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements.
8. **Dispute Resolution:** If I have a dispute, I can go to an independent Third Party for a resolution.
9. **Exceptional Circumstances:** I know that any exception has to be approved by Parliament and is subject to independent scrutiny.

7.2 Review of Compliance with the PCAG Identity Assurance Principles

In *Part 17.1 Privacy* of the Procurement 2 Framework Agreement, Identity Providers are obliged to offer "a privacy policy (the "Provider Privacy Policy") which is clear and easily comprehensible, and which outlines (i) the steps the Provider, its Affiliates and Provider Personnel have taken to comply with the provisions in the Identity Assurance Principles which are applicable to such parties; and (ii) any measures they plan to implement in future."

The Identity Assurance Principles are not, however, one of the mandatory compliance requirements defined in *Part 8.3 Provision of Services*. To address this, we have reviewed the procurement documents to ensure that all aspects of the Identity Assurance Principles are mandated therein, and to recommend those areas where changes might be desirable to ensure that the Principles are protected within the provider contracts.

[17] https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group

The detailed results are shown in the associated spreadsheet. For each principle, the appropriate reference in the procurement document is provided; where there is a possible need for remediating actions, then this is shown.

7.3 Identity Assurance Principles Compliance Check

The following table provides the Identity Assurance Principles Compliance Check. For each line item in the Identity Assurance Principles, the table shows the controlling policy in the framework agreement that ensures the requirement is adhered to. Where there is a need for further controls to guarantee the principle is followed, a recommendation has been made.

It should be noted that the Identity Assurance Principles and the framework agreement refer to "Identity Provider" (IdP) in place of "Certified Company", and in some cases to "IdA" (Identity Assurance) in place of "GOV.UK Verify."

Item	Requirement	Controlling Policy	Recommendation
1: User Control: I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them.			
4.1.1	An Identity Provider or Service Provider must ensure any collection, use or disclosure of IdA data in, or from, an Identity Assurance Service is approved by each particular Service User who is connected with the IdA data.	**Framework Agreement 17.4.a, Schedule 4 Provider Ts & Cs 2.1:** The Provider shall ensure that the User's consent to such Processing: (a) is given actively (and not deemed to have been given through silence, failure to object or other inaction); (b) follows a full, specific and detailed explanation of: (i) all the actions to which consent is sought; and (ii) all the consequences which are reasonably likely to result from such actions.	No recommendation
4.1.2	There should be no compulsion to use the Identity Assurance Service and Service Providers should offer alternative mechanisms to access their services. Failing to do so would undermine the consensual nature of the service.	**No policy** This is a policy requirement for individual Government Services and is not within GDS' remit.	No recommendation
2: Transparency: Identity assurance can only take place in ways I understand and when I am fully informed.			

Item	Requirement	Controlling Policy	Recommendation
4.2.1	Each Identity Provider or Service Provider must be able to justify to Service Users why their IdA data are processed. Ensuring transparency of activity and effective oversight through auditing and other activities inspires public trust and confidence in how their details are used.	**Framework Agreement 17.4.a, Schedule 4 Provider Ts & Cs 2.1** The Provider shall ensure that the User's consent to such Processing: (a) is given actively (and not deemed to have been given through silence, failure to object or other inaction); (b) follows a full, specific and detailed explanation of: (i) all the actions to which consent is sought; and (ii) all the consequences which are reasonably likely to result from such actions.	No recommendation
4.2.2	Each Service User must be offered a clear description about the processing of IdA data in advance of any processing. Identity Providers must be transparent with users about their particular models for service provision.	**Framework Agreement Pt 17.1 Privacy** The Provider shall publish and make readily available to Users on or through any Provider Public Facing Services and Marketing a privacy policy (the "Provider Privacy Policy") which is clear and easily comprehensible.	No recommendation

Item	Requirement	Controlling Policy	Recommendation
4.2.3	The information provided includes a clear explanation of why any specific information has to be provided by the Service User (e.g. in order that a particular level of identity assurance can be obtained) and identifies any obligation on the part of the Service User (e.g. in relation to the User's role in securing his / her own identity information).	**Framework Agreement 17.4.a, Schedule 4 Provider Ts & Cs 2.1** The Provider shall ensure that the User's consent to such Processing: (a) is given actively (and not deemed to have been given through silence, failure to object or other inaction); (b) follows a full, specific and detailed explanation of: (i) all the actions to which consent is sought; and (ii) all the consequences which are reasonably likely to result from such actions.	No recommendation
4.2.4	The Service User will be able to identify which Service Provider they are using at any given time.	**No policy** Certified Companies apply their own branding to their services, thereby ensuring that they are clearly distinguishable.	No recommendation
4.2.5	Any subsequent and significant change to the processing arrangements that have been previously described to a Service User requires the prior consent or approval of that Service User before it comes into effect.	**Framework Agreement Pt 17.2 Privacy** The Provider should disclose to Users on a timely basis any changes to its Provider Privacy Policy or how it is implemented and enforced.	No recommendation

Item	Requirement	Controlling Policy	Recommendation
4.2.6	All procedures, including those involved with security, should be should be made publicly available at the appropriate time, unless such transparency presents a security or privacy risk. For example, the standards of encryption can be identified without jeopardy to the encryption keys being used.	**Attachment 2 Selection Questionnaire SQD14, Framework Agreement 8.10.g Provider Undertakings, Framework Agreement 24.1 Protection Provisions, etc.** The Provider shall at all times a) take all steps reasonably required to protect the Authority System, the HMG Service Provider Systems, the IT Environment, the Services and Users' data from security breach or other unauthorised access or acts, in accordance with the Industry Documents, Good Industry Practice and such other guidance as may be issued by the Authority to the Provider in writing from time to time, including (without limitation) all measures reasonably required to prevent, detect, mitigate and respond to third party attack, including (without limitation) protective monitoring and transaction monitoring. Compliance with ISO27001 is a mandatory requirement for Provider selection, and one of the Conditions Precedent for the contract to be enacted.	No recommendation
3: Multiplicity: I can use and choose as many different identifiers or identity providers as I want to.			
4.3.1	A Service User is free to use any number of identifiers that each uniquely identifies the individual or business concerned.	**No policy** The underlying infrastructure contains no mechanism to evaluate or restrict whether a Service User has multiple identifiers.	No recommendation
4.3.2	A Service User can use any of his identities established with an Identity Provider with any Service Provider.	**No policy** The underlying infrastructure contains no mechanism to restrict with which Relying Parties a User can assert an Identity, beyond ensuring that the Identity has been verified to the Level of Assurance requested by the Government Service.	No recommendation

Item	Requirement	Controlling Policy	Recommendation
4.3.3	A Service User shall not be obliged to use any Identity Provider or Service Provider not chosen by that Service User; however, a Service Provider can require the Service User to provide a specific level of Identity Assurance, appropriate to the Service User's request to a Service Provider.	**No policy** The underlying infrastructure contains no mechanism to restrict with which Government Services a User can assert an Identity, beyond ensuring that the Identity has been verified to the Level of Assurance requested by the Government Service.	No recommendation
4.3.4	A Service User can choose any number of Identity Providers and where possible can choose between Service Providers in order to meet his or her diverse needs. Where a Service User chooses to register with more than one Identity Provider, Identity Providers and Service Providers must not link the Service User's different accounts or gain information about their use of other Providers.	**No policy** The underlying infrastructure contains no mechanism to allow Providers to interrogate with which Relying Parties a User interacts.	GDS should mandate that Certified Companies are not permitted to solicit, infer or otherwise obtain information about the Service User's interactions with Government Services (including knowing the identity of those Government Services).
4.3.5	A Service User can terminate, suspend or change Identity Provider and where possible can choose between Service Providers at any time.	**Framework Agreement 17.4.f Data Protection** Ensure that it has the capability...to provide or correct or delete at the request of a User all the Personal Data relating to that User that the Provider holds.	No recommendation

Item	Requirement	Controlling Policy	Recommendation
4.3.6.a	A Service Provider does not know the identity of the Identity Provider used by a Service User to verify an identity in relation to a specific service.	**No policy** The underlying infrastructure contains no mechanism to allow Providers to interrogate with which Relying Parties a User interacts.	See 4.3.4
4.3.6.b	The Service Provider knows that the Identity Provider can be trusted because the Identity Provider has been certified, as set out in GPG43 – Requirements for Secure Delivery of Online Public Services (RSDOPS).	**Attachment 2 Selection Questionnaire SQD14, Framework Agreement 8.10.g Provider Undertakings, Framework Agreement 24.1 Protection Provisions, etc.** The Provider shall at all times a) take all steps reasonably required to protect the Authority System, the HMG Service Provider Systems, the IT Environment, the Services and Users' data from security breach or other unauthorised access or acts, in accordance with the Industry Documents, Good Industry Practice and such other guidance as may be issued by the Authority to the Provider in writing from time to time, including (without limitation) all measures reasonably required to prevent, detect, mitigate and respond to third party attack, including (without limitation) protective monitoring and transaction monitoring. Compliance with ISO27001 is a mandatory requirement for Provider selection, and one of the Conditions Precedent for the contract to be enacted.	No recommendation
4: Data Minimisation: My interactions only use the minimum data necessary to meet my needs.			
4.4.1	Identity Assurance should only be used where a need has been established and only to the appropriate minimum level of assurance.	**No policy** Certified Companies are not responsible for determining the Services that will be supported by GOV.UK Verify. GDS issues procedures to ensure that Government Services only use GOV.UK Verify where a need has been established and only to the appropriate minimum level of assurance.	No recommendation

Item	Requirement	Controlling Policy	Recommendation
4.4.2	Identity Assurance data processed by an Identity Provider or a Service Provider to facilitate a request of a Service User must be the minimum necessary in order to fulfil that request in a secure and auditable manner.	**Framework Agreement 17.4.c Data Protection** ...request from the User only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information for the purposes of Clause 25 (Confidentiality).	No recommendation
4.4.3	When a Service User stops using a particular Identity Provider, their data should be deleted. Data should be retained only where required for specific targeted fraud, security or other criminal investigation purposes.	**Framework Agreement 17.4.f Data Protection, Service Delivery Requirements v3 Audit Storage - Security and Retention Requirements** Ensure that it has the capability...to provide or correct or delete at the request of a User all the Personal Data relating to that User that the Provider holds. C2.0.1 Records should be kept for the period that a User is registered with the Provider and for a further period of 7 years after that point subject always to its obligations to comply with the DPA. C2.0.2 All records must be kept secure, in line with the DPA and ISO 15489-1 Records Management	No recommendation
5: Data Quality: I choose when to update my records.			
4.5.1	Service Providers should enable Service Users (or authorised persons, such as the holder of a Power of Attorney) to be able to update their own personal data, at a time at their choosing, free of charge and in a simple and easy manner.	**No recommendation** The Identity Provider service includes the ability for Service Users to update their own personal data (indeed, it can only function correctly if they can do so). The MDS data passed to Service Providers can be reused for updating records so long as the Service User provides consent.	No recommendation

Item	Requirement	Controlling Policy	Recommendation
4.5.2	Identity Providers and Service Providers must take account of the appropriate level of identity assurance required before allowing any updating of personal data.	**IPV Operations Manual v2.3.1 Part 19 Updating verified data** The IdP shall enable the Customer to update their records to reflect a change in the Customer's circumstances after successful proofing. The IdP shall take appropriate measures to ensure that when this occurs it is being done by the legitimate owner of the account. The measures may vary depending on the strength of the Credential used to authenticate the Customer to the service that allows the Customer to change their details and other risk factors (e.g. detection of malware).	No recommendation
6: Service User Access and Portability: I have to be provided with copies of all of my data on request; I can move / remove my data whenever I want.			
4.6.1	Each Identity Provider or Service Provider must allow, promptly, on request and free of charge, each Service User access to any IdA data that relates to that Service User.	**Framework Agreement 17.4.f Data Protection** Ensure that it has the capability...to provide or correct or delete at the request of a User all the Personal Data relating to that User that the Provider holds.	GDS should ensure that Certified Companies and Government Services do not charge Service Users for access to their personal data (Subject Access). This will be an enforced legal requirement under the EU GDPR from May 2018.
4.6.2	It shall be unlawful to make it a condition of doing anything in relation to a Service User to request or require that Service User to request IdA data.	**Service Delivery Requirements v3 C1.6 Compliance auditing & reporting** C1.6.1.1 The Provider is required to record Subject Access Requests and report unusual patterns of behaviour to the Authority.	No recommendation

Item	Requirement	Controlling Policy	Recommendation
4.6.3	The Service User must be able to require an Identity Provider to transfer his personal data, to a second Identity Provider in a standard electronic format, free of charge and without impediment or delay.	**Framework Agreement 17.4.f Data Protection** Ensure that it has the capability...to provide or correct or delete at the request of a User all the Personal Data relating to that User that the Provider holds. (The Framework Agreement does not mandate an automated mechanism to ensure that the Service User can obtain timely access to all information relating to their account, although in practice it would be impracticable to offer a Provider service without such capabilities.)	GDS should ensure that by May 2018 Certified Companies allow Service Users to obtain their personal data and transfer it to other Certified Companies should they wish to do so.
7: Certification: I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements.			
4.7.1	As a baseline control, all Identity Providers and Service Providers will be certified against a shared standard. This is one important way of building trust and confidence in the service.	**Framework Agreement 8.10.f Provider Undertakings** …do all things necessary to maintain its certification as a Provider of trust services by the applicable Certification Body.	No recommendation
4.7.2.a	As part of the certification process, Identity Providers and Service Providers are obliged to co-operate with the independent Third Party and accept their impartial determination and to ensure that contractual arrangements:	**Framework Agreement 12.1 Complaints** The Authority may appoint a third person (in the form of an ombudsman or otherwise) to perform a supervisor role in respect of the Complaints Procedure (IDA Supervisor).	No recommendation
4.7.2.b	reinforce the application of the Identity Assurance Principles	**Framework Agreement 17.1 Privacy** The Provider shall publish… a privacy policy… which outlines (i) the steps the Provider, its Affiliates and Provider Personnel have taken to comply with the provisions in the Identity Assurance Principles…	No recommendation

Item	Requirement	Controlling Policy	Recommendation
4.7.2.c	contain a reference to the independent Third Party as a mechanism for dispute resolution	**Framework Agreement 12.1 Complaints** The Authority may appoint a third person (in the form of an ombudsman or otherwise) to perform a supervisor role in respect of the Complaints Procedure (IDA Supervisor).	No recommendation
4.7.3	There will be a certification procedure subject to an effective independent audit regime that ensures all relevant, recognised identity assurance and technical standards, data protection or other legal requirements, are maintained by Identity Providers and Service Providers.	**Specification for Organisations Providing Proofing and Authentication of Digital Identities - Criteria 9** Organisations shall demonstrate that they are able to meet the requirements of this specification through the achievement of certification by a Certification Body in accordance with the certification specification.	No recommendation

Item	Requirement	Controlling Policy	Recommendation
4.7.4	In the context of personal data, certification procedures include the use of Data Protection Impact Assessments, Security Risk Assessments, Privacy by Design concepts and, in the context of information security, a commitment to using appropriate technical measures (e.g. encryption) and ever improving security management. Wherever possible, such certification processes and security procedures reliant on technical devices should be made publicly available at the appropriate time.	**Schedule 5 Conditions Precedent 2.d Operational conditions precedent** ...the delivery to the Authority of evidence reasonably satisfactory to the Authority that the Provider has made all notifications that it is required to have made to the Information Commissioner under Data Protection Law and has carried out a Data Protection Impact Assessment in respect of the performance of its obligations under this Agreement;	No recommendation

Item	Requirement	Controlling Policy	Recommendation
4.7.5	All Identity Providers and Service Providers will take all reasonable steps to ensure that a Third Party cannot capture IdA data that confirms (or infers) the existence of relationship between any Participant. No relationships between parties or records should be established without the consent of the Service User.	**No policy**	GDS should mandate that Certified Companies are not permitted to solicit, infer or otherwise obtain information about the Service User's interactions with Government Services (including the identity of those Government Services).
4.7.6	Certification can be revoked if there is significant non-compliance with any Identity Assurance Principle.	**Framework Agreement 35.2 Termination by the Authority** The Authority may terminate the Framework Agreement and/or any Call-Off by issuing a Termination Notice to the Provider either: (a) pursuant to the terms of the following provisions: (i) Clause 17.8 (Breach of privacy and data protection provisions);	No recommendation
8: Dispute Resolution: If I have a dispute, I can go to an independent Third Party for a resolution.			

Item	Requirement	Controlling Policy	Recommendation
4.8.1	A Service User who, after a reasonable time, cannot, or is unable, to resolve a complaint or problem directly with an Identity Provider or Service Provider can call upon an independent Third Party to seek resolution of the issue. This could happen for example where there is a disagreement between the Service User and the Identity Provider about the accuracy of data.	**Framework Agreement 12.1 Complaints** The Authority may appoint a third person (in the form of an ombudsman or otherwise) to perform a supervisor role in respect of the Complaints Procedure (IDA Supervisor).	GDS regularly reviews the requirement for the IDA Supervisor function, which is currently served by the User Support team, and should expand the function should that be necessary.
4.8.2	The independent Third Party can resolve the same or similar complaints affecting a group of Service Users.	**Framework Agreement 12.1 Complaints** The Authority may appoint a third person (in the form of an ombudsman or otherwise) to perform a supervisor role in respect of the Complaints Procedure (IDA Supervisor).	See 4.8.1
4.8.3	The independent Third Party can co-operate with other regulators in order to resolve problems and can raise relevant issues of importance concerning the Identity Assurance Service.	**No policy**	See 4.8.1

Item	Requirement	Controlling Policy	Recommendation
4.8.4	An adjudication / recommendation of the independent Third Party should be published. The independent Third Party must operate transparently, but detailed case histories should only be published subject to appropriate review and consent.	**No policy**	See 4.8.1
4.8.5	There can be more than one independent Third Party.	**No policy**	See 4.8.1
4.8.6	The independent Third Party can recommend changes to standards or certification procedures or that an Identity Provider or Service Provider should lose their certification.	**Framework Agreement 12.1 Complaints** The Authority may appoint a third person (in the form of an ombudsman or otherwise) to perform a supervisor role in respect of the Complaints Procedure (IDA Supervisor).	See 4.8.1
9: Exceptional Circumstances: I know that any exception has to be approved by Parliament and is subject to independent scrutiny.			

Item	Requirement	Controlling Policy	Recommendation
4.9.1	Any exemption from the application of any of the above Principles to IdA data shall only be lawful if it is linked to a statutory framework that legitimises all Identity Assurance Services, or an Identity Assurance Service in the context of a specific service. In the absence of such a legal framework then alternative measures must be taken to ensure, transparency, scrutiny and accountability for any exceptions.	**No policy**	GDS should ensure that it maintains a coherent policy approach to exemptions to the Principles, and that protection of the Principles remains a policy (and if necessary, legislative) priority.

Item	Requirement	Controlling Policy	Recommendation
4.9.2	Any exemption from the application of any of the above Principles that relates to the processing of personal data must also be necessary and justifiable in terms of one of the criteria in Article 8(2) of the European Convention of Human Rights: namely in the interests of national security; public safety or the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals, or for the protection of the rights and freedoms of others.	**No policy**	See 4.9.1
4.9.3	Any subsequent processing of personal data by any Third Party who has obtained such data in exceptional circumstances (as identified by Article 8(2) above) must be the minimum necessary to achieve that (or another) exceptional circumstance.	No policy	See 4.9.1

Item	Requirement	Controlling Policy	Recommendation
4.9.4	Any exceptional circumstance involving the processing of personal data must be subject to a Privacy Impact Assessment by all relevant “data controllers” (where “data controller” takes its meaning from the Data Protection Act).	No policy	See 4.9.1
4.9.5	Any exemption from the application of any of the above Principles in relation to IdA data shall remain subject to the Dispute Resolution Principle.	**No policy**	See 4.9.1

8. Summary of Recommendations

8.1 Introduction

The review has identified potential areas for improvement to ensure that GOV.UK Verify effectively manages the risks to both GDS and Service Users arising from the handling of personal data. The recommendations are summarised in the table below, and each has been assigned a priority and costs where the priority is defined as:

- **High Priority:** Actions that should be completed before GOV.UK Verify go-live;
- **Medium Priority:** Actions that should be completed as a matter of priority, and by the end of 2016 as a minimum;
- **Low Priority:** Actions that should be completed by May 2018 at the very latest.

Cost is defined as:

- **High Cost:** Actions that may require significant amounts of GDS team time, or specific procurement of software or services;
- **Medium Cost:** Actions that may require sufficient time or resources to merit a specific budget or procurement;
- **Low Cost:** Actions that are unlikely to require a specific budget or procurement and can be absorbed into 'business as usual' within the GDS team.

Recommendation	Priority	Cost	Status
GDS should continue to prepare appropriate internal privacy policies and processes to apply across the GOV.UK Verify programme and ensure that every member of staff is aware of the policies and their duties to follow them.	M	L	Assigned to Privacy Officer, in progress
GDS should ensure that it has prepared and tested incident response plans to work with stakeholders should a loss, modification or misuse of the Matching Data Set occur.	M	L	Assigned to Operations Team, in progress
GDS should continue to support the development of Transaction Monitoring controls to prevent session hijack.	L	L	Assigned to Privacy Officer, in progress
GDS should establish procedures to create and maintain a comprehensive record of use of personal data across the GOV.UK Verify ecosystem. The record should include details of processing carried out on GDS' behalf. This record should be checked regularly.	M	L	Assigned to Privacy Officer, in progress
GDS should establish protocols to ensure the regular review of retention periods for personal data.	M	L	Assigned to Privacy Officer, in progress
GDS should mandate that Certified Companies are not permitted to solicit, infer or otherwise obtain information about the Service User's interactions with Government Services (including knowing the identity of those Government Services).	M	L	Assigned to Privacy Officer, to be mandated in next framework agreement
GDS should ensure that Certified Companies and Government Services do not charge Service Users	L	L	Assigned to Privacy Officer, to be mandated

Recommendation	Priority	Cost	Status
for access to their personal data (Subject Access). This will be an enforced legal requirement under the EU GDPR from May 2018.			in next framework agreement
GDS should ensure that by May 2018 Certified Companies allow Service Users to obtain their personal data and transfer it to other Certified Companies should they wish to do so.	L	L	Assigned to Privacy Officer, to be mandated in next framework agreement
GDS regularly reviews the requirement for the IDA Supervisor function, which is currently served by the User Support team, and should expand the function should that be necessary.	L	L	Assigned to User Support team, ongoing
GDS should ensure that it maintains a coherent policy approach to exemptions to the Principles, and that protection of the Principles remains a policy (and if necessary, legislative) priority.	L	L	Assigned to GDS Executive team, ongoing

8.2 Next Steps

There are no privacy recommendations that prevent GOV.UK Verify proceeding to live service delivery, although the recommendations provided here, which are now in progress, should be addressed by the Privacy Officer as a matter of priority.

This DPIA should be maintained and revised by the Privacy Officer to incorporate an assessment of the requirements of the EU General Data Protection Regulation.