improvement service Digital Public Services

mygovscot myaccount

Data Privacy Impact Assessment

Version 3.4

improvement service

Contents

Mygovscot myaccount Data Privacy Impact Assessment (DPIA) 4
The Need for a DPIA 4
The Processing 5
What is myaccount used for 5
Context of the Processing 6
Processing Responsibilities 7
Purposes of Processing 8
Scope of the Processing 9
Account Registration 10
Raising a Query 11
Verifying Identity 12
Data source to help prove who you are 14
Attribute Service 14
Registration by an Organisation 16
Personal Data generated when a user uses the service 17
Personal Data we collect from your device 18
Data Retention 19
Proportionality and Necessity 20
Legal Bases for Processing 20
Standards Applicable to the Processing 21
Data Minimisation 22
Keeping Data Accurate and up to Date 22
Supporting the Personal Rights of Data Subjects 23
Keeping Data Subjects Informed 23
If Applicable, how is the Consent of Data Subjects Obtained? 23
Rights of Access and Data Portability 23
Rights to Rectification and Deregistration 23
Rights to Restriction and to Object 24
Processor Obligations 24
International Transfers 24
Consultation 25
Risks 26
Confidentiality 26
Integrity 27
Availability 28
Existing and Planned Measures 29

Sign-Off and Record Outcomes 31
Action plan 31
Sign-Off 32
Updates 33
Version 3.4 33
Previous Versions 33
Definitions 34

Mygovscot myaccount Data Privacy Impact Assessment (DPIA)

Effective 1st June 2020. **Download PDF**

We've updated our DPIA on 1st June 2020. For more detail we have provided a summary of the key changes. If you have any questions about the DPIA, please contact the Improvement Service.

The Need for a DPIA

mygovscot myaccount (myaccount for short) is an identity verification and single sign-in service. myaccount is designed to help Scottish public sector organisations such as Local Authorities and Health Boards deliver services to the right person.

myaccount provides a broad range of services under the myaccount name that are made available to citizens and service providers, including:

- **An online account –** to use to sign into multiple service providers and access their services
- **Identity verification –** a service that enables citizens to prove who they are
- **Authentication –** different options to sign into myaccount
- **Helpdesk –** an online helpdesk to help citizens resolve any queries which they may have

This DPIA has been created in line with the Information Commissioner's Office (ICO) guidelines. Guidelines can be found at the ICO's website.

A DPIA is necessary as the myaccount service:

- Combines, compares or matches data from multiple sources, to establish that users are who they say there are;
- Processes personal data that could result in a risk of physical harm in the event of a security breach;
- Uses new technologies to make online identity proofing easier for citizens;
- Uses technology for security monitoring purposes and real-time alerting of potentially fraudulent activity.

Improvement Service policy, (the company who operate myaccount), also dictates that major systems that process personal data will always be subject to a DPIA before implementation or following a significant change.

The Processing

What is myaccount used for

Myaccount allows a user to set up an online account, prove who they are and use that single account to access different online public services.

Myaccount transfers information about a user to the organisation that provides the service (Service Provider) when they log in. The information tells Service Providers who a user is. Service Providers uses that information to decide if a user should be granted access to their service.

Some services will require a user to have either a partially verified or verified account. Myaccount will always show a user what personal information they are sharing with the Service Provider when the user signs up for a service with them.

Context of the Processing

Many online public services require a user to prove who they claim to be before a service can be provided. Proving a user is who they claim to be online is challenging.

The myaccount system is designed to be flexible. It enables users to access services that are accessible to unverified accounts. Myaccount also has tools to help a user prove who they claim to be. This is called a verified myaccount. Verified accounts are needed to access some services to protect from fraud or identity theft.

The process to validate and verify accounts should meet the following criteria:

- an identity should be unique;
- all supplied evidence should be correct and genuine (i.e. not counterfeit or misappropriated);
- the claimed identity should exist in the real world; and
- the claimed identity should be successfully associated with the real person supplying the identity evidence.

The proofing processes in myaccount service are designed to meet these aims. The outcome of the proofing process is a Verification Level. That level reflects:

- the type of evidence produced;
- how strongly it has been checked; and
- how trustworthy is the evidence?

This model is in line with Government Standards to verify identities of users accessing online services.

The myaccount service uses open standard protocols for identity federation that are commonly used e.g. SAML and OpenID Connect. myaccount is run in line with best practice and is currently seeking formal external accreditation for ISO27001.

Processing Responsibilities

mygovscot myaccount services are provided by:

The Improvement Service
A company limited by guarantee and registered in Scotland (Company No. SC287978)

iHub
Quarrywood Court
Livingston
EH54 6AX

You can read more about the Improvement Service and what we do on our website.

Any reference to Data Protection Law we make in this document refers to the EU General Data Protection Regulation ((EU) 2016/679) and the UK Data Protection Bill 2018, which came into effect in the UK on 25th May 2018.

Registration
The Improvement Service is the Data Controller for all account registrations.

Anyone in the world can register for a myaccount. Initially, all accounts are unverified, unless the user registers for a myaccount using Yoti. Verified data from the users Yoti account will enable the user to create a verified myaccount.

(Yoti is a global identity platform and free consumer app that enables user to put their ID on their phone. It's a simple, safe, a fast way to prove your identity online and in person. Further information about Yoti can be found at www.yoti.com.)

Yoti is the Data Controller of the attributes that users provide them. When a user shares those attributes with myaccount, The Improvement Service becomes a data controller of those attributes.

Accessing Services from Services Providers
The Improvement Service becomes a Joint Data Controller with a Service Provider when a user consents to share their data to access a service, for the purposes of identity only.

The Service Provider can update the myaccount data with the users consent e.g. change contact details. Users can request services from multiple Service Providers. Multiple Service Providers could be joint Data Controllers at the same time with the Improvement Service.

Data Processors
The Improvement Service has contracts with a managed service company (Tata Consultancy Services) and a hosting company (brightsolid UK). Both companies are Data Processors for the Improvement Service. The contracts with these companies reflect the GDPR obligations of both the Improvement Service and the contractors.

Purposes of Processing

Myaccount processes a user’s personal data for the following purposes:

- To allow users to register for myaccount.
- To allow users to use their single myaccount to access multiple online public services.
- To allow users to update their details.
- To allow users to confirm who they claim to be. Users may have to provide information that myaccount can be checked against other sources to prove their identity.
- To provide Service Providers with information to decide whether a user should be granted access to a service.
- To notify Service Providers of any change to a user’s personal data that may be relevant to their records.
- To enable the myaccount Helpdesk resolve any queries raised by a user.
- To develop and improve the myaccount service.
- To protect both users and the myaccount service from possible fraudulent or malicious use.

Scope of the Processing

Basic personal information is collected from anyone who wants to set up an account. Users can verify their account by providing additional information that can be checked to prove who they claim to be. Some information or documents may be checked against trusted identity stores if required. No special categories of data are processed.

Information is collected in one of more of the following ways:

- directly from user registering for an account
- directly from user raising a query
- directly from user verifying identity
- from data sources to help prove that someone is who they claim to be
- from a Service Provider when they register users for an account
- generated when a user uses the service
- from the devices used to access myaccount

Account Registration

Information That Must Be Provided to Get an Account

Some of the personal data a user supplies when they register for an account is mandatory. myaccount needs the data to establish who the user is and to help them manage their account.

This data is called, core identity data and includes:

- First Name;
- Surname;
- Gender (Male, Female, Prefer Not to Say or Prefer to Self-Disclose);
- Address;
- Date of Birth;
- E-mail Address; and
- Username (if different from your email address).

Myaccount will ask users to set a password when creating an account. Myaccount will never share the password with Service Providers or anyone else.

Users have the option to register for a myaccount using their Yoti account. If chosen, users will be asked to consent to share their Yoti information (on the Yoti app) to create a myaccount. The information includes:

- Full name;
- Given names;
- Family name;
- Email address;
- Date of birth;
- Gender;
- Address; and
- Yoti Remember Me ID.

(The Yoti Remember Me ID is only used to link a user's Yoti to their myaccount. The Remember Me ID has no meaning outside the Yoti app).

Only Yoti accounts where both the name and address has been verified will be allowed to register for a myaccount.

Optional Information That May Be Helpful

Myaccount provides users the option to add optional information to their account profile. The information may be helpful to Service Providers to personalise their services e.g. call a user by a preferred name or contact a user if there is a problem.

Optional information includes:

- Mobile telephone number;
- Landline telephone number;
- Preferred First Name; and
- Preferred Surname.

Raising a Query

If a user wants to contact us or report a problem, they can do so via the myaccount Helpdesk. Both registered and unregistered users can contact the Helpdesk. A user must supply a valid email address to enable the Helpdesk to reply to the query. A user can also supply a contact telephone number if they would prefer this.

If a query relates to a user proving their identity, the Helpdesk may ask the user to provide more information to help resolve the query.

If is query is about a service provided by a Service Provider, the Helpdesk will forward the query to that Service Provider.

Verifying Identity

myaccount has three verification levels:

- Unverified;
- Partially Verified; and
- Verified.

Some Service Providers need to know that a user is who they claim to be. Therefore, the user may need to supply supporting evidence before they can access a service. Some services may require a user to have a partially verified or verified account. That's for the Service Provider to decide.

myaccount offers users the opportunity of setting up a partially verified or a verified account. If a user has a partially verified or a verified myaccount, the Service Provider will have greater confidence in who the user claims to be.

A verified account means that a user has gone through some checks to help prove who they are. Myaccount will tell the Service Provider that the user has a verified account when they login with their myaccount and ask for a service.

Myaccount offers a range of options a user can choose from to set up a verified account, including:

- verifying their identity using a smartphone and the Yoti app (linking Yoti to their myaccount);
- scanning and uploading different forms of identity evidence; or
- attending an authorised office to verify and present evidence in person.

Myaccount will not ask a user to do all the things in the list above. As myaccount needs to meet Government Identity Standards it may ask the user a range of different questions or ask them to submit more than one piece of evidence.

The requested identity evidence may include one or a combination of the following documents:

- Passport;
- Driving Licence;
- PASS Accredited identity document
- Utility bill;
- Bank statement or similar financial document.

Other documents may be requested or could be added to the list.

Myaccount looks to provide users with multiple options. Some services however may require certain documents or checks to be conducted. For example, that they must verify using a passport or driving licence.

myaccount may need to verify documents or a user's personal data against trusted sources. Checks are only carried out with the consent of the user. When myaccount checks with other trusted sources, myaccount will only ask them to verify that they can match a user's details in their own systems. Trusted sources will confirm a match by returning an answer of either 'yes' or 'no'. Myaccount does not ask for any other information to be returned. Myaccount will record that these sources have been looked up with the user's consent. Myaccount does this for audit purposes.

If a user does not consent to their data being checked against a trusted source, myaccount may not be able to offer them a verified account. The Service Provider may ask the user to provide additional information if the account is unverified. In some cases, Service Providers may deny the user access.

Details supplied by a user to prove their identity will normally be deleted once they have been checked and verified, either electronically or by an authorised agent. An Agent will normally be an authorised employee within a Local Authority or Health Board. In some cases, myaccount may have to retain some information users supply for audit purposes. Access to audit information is strictly controlled. All access requests are logged and scrutinised periodically.

myaccount may have to perform periodic checks on a user's identity while they hold a myaccount. A user may be asked to resubmit information so that it can be rechecked to maintain their verified status.

Data source to help prove who you are

Attribute Service

To grant access to specific services, some Service Providers may require more information (attributes) in addition to the myaccount data to be able to match a user to their own back office systems or confirm a user's entitlement to grant access to service.

The myaccount Attribute Service helps Service Providers to do just that. myaccount can look up data extracts (with explicit consent and under specific conditions) to confirm a user's details and provide an additional attribute to the service provider (if required).

Examples are noted below:
A local authority may request myaccount to confirm a user's details against a limited extract of the National Health Service Central Register (NHSCR) to retrieve their UCRN (Unique Citizen Reference Number). The UCRN is unique to a user and helps the Local Authority distinguish between a user and other people who may have the same name. A Local Authority can use the UCRN to find/match a user's details in their back-office systems to provide a user access to a service.
Myaccount will only look up a user's details against the NHSCR Extract with consent from the user and the user's account is either partially verified or verified.

A health board may request myaccount to confirm a user's details against a limited extract of the NHSCR to retrieve their CHI Number (Community Health Index Number). The CHI Number is unique to a user and helps a Health Board distinguish between a user and other people who may have the same name. A Health Board can use the CHI Number to find/match a user's details in their back-office systems to provide a user access to a service.
Myaccount will only look up a user's details against the NHSCR Extract with consent from the user and the user's account is either partially verified or verified.

When myaccount uses these limited extracts, The Improvement Service are acting as Data Processors under written instruction of the appropriate Data Controller. These systems have strict controls on what processing is allowed.

If a user provides consent for myaccount to check their details against the NHSCR Extract or **another data set (if available)** to retrieve an attribute, myaccount does not store this attribute with their myaccount data. The data is stored separately. Myaccount gets these attributes in real time, when required, before passing them to the Service Provider.

More information about the NHSCR

The NHSCR is a list of everyone who was born or who has died in Scotland along with everyone who has registered with a GP or hospital. The Improvement Service hold a limited extract of the register containing basic details as below:

- Forename;
- Surname;
- Date of Birth;
- Gender (currently limited to M or F);
- Date of Death (if applicable);
- UCRN - Unique Citizen Reference Number (see below);
- CHI – Community Health Index number (see below).

The NHSCR is operated by National Records of Scotland (NRS). NRS is the Data Controller for the NHSCR extract. The Improvement Service processes the NHSCR extract on behalf of Local

Government, the NHS and the Registrar General. Processing of the extract is in line with instructions it receives from NRS, the Data Controller. Use of the NHSCR is governed by the Local Electoral Administration and Registration Services (Scotland) Act 2006.

When myaccount looks up a user's details in the NHSCR extract to get the UCRN or CHI number myaccount must follow rules laid down (that are superimposed on the NHSCR Regulation) by NRS/the Registrar General and the NHS. These rules dictate that:

- Myaccount can only give the UCRN to Local Government;
- Myaccount can only give the CHI number to the NHS; and
    - The CHI Number can only be released for specific purposes following formal agreement with the relevant NHS Information Governance bodies.

Verify Identity via National Entitlement Card Extract

Myaccount may use a limited extract from the National Entitlement Card (NEC) system to help users partially verify or verify their account. The extract may also be used to confirm a user's eligibility to access a service from a Service Provider.

When myaccount use the extract, The Improvement Service are acting as Data Processors under written instruction of the appropriate Data Controller.

The NEC scheme is operated by Dundee City Council (acting as the National Entitlement Programme Office (NECPO)) on behalf of all Scottish Local Authorities. NECPO is the Data Controller for the National Entitlement Card data extract. More information about the National Entitlement Card and its Privacy Policy can be found at: https.//www.entitlementcard.org.uk/privacy-policy

When myaccount checks a user's information against the NEC extract, it must follow rules laid down by NECPO, acting as the Data Controller for all 32 Scottish Local Authorities.

Myaccount will only check a user's details against the NEC Extract if they provide consent.

The NEC extract is a list of everyone who has a National Entitlement Card. The extract contains basic information such as a user's name, address and their card number. The extract does not contain any transactional information. It contains the following information only:

- Forename;
- Surname;
- Date of Birth;
- Address; and
- NEC Number.

Registration by an Organisation

Some Service Providers can create a myaccount on behalf of a user with a user’s consent. The Service Provider will collect the required information from the user and use myaccount web services to register them for a myaccount.

The information myaccount receives from Service Providers setting up an account on a user’s behalf is the same information users enter themselves when setting up an account.

Some Service Providers may establish a user’s identity before setting up a myaccount for them. In this case, it may also pass myaccount information confirming the verification process was used. This would include a user’s account verification level; either:

- Unverified;
- Partially Verified; or
- Verified.

Myaccount doesn’t receive the proofs from Service Providers. Myaccount is just informed what was presented. For example, note that the user verified their identity by presenting a passport, however no passport details would be passed to myaccount. If a Service Provider creates accounts in this way, they must follow the standards and rules set by the myaccount service.

Personal Data generated when a user uses the service

The data helps Service Providers identify individual users.

Within the myaccount service, each user can see the Service Provider they have agreed to share data with. They can also check what specific data they have agreed to share. Users can manage their consent from within their profile page and revoke it if they wish.

When a user signs-in to myaccount to access a service with a Service Provider, myaccount generates a unique, anonymous identifier for that user. The identifier is called a Secure Visitor Token (SVT) and is sent to a Service Provider along with the attribute's a user has agreed to share.

The SVT is only shared between a user and the Service Provider and is only used when a user logs in. It helps the Service Provider know that the user is the same person that logged in previously.

If users enrol with more than one Service Provider then myaccount generates additional SVTs, one for each service with which they enrol.

Personal Data we collect from your device

The data helps understand how myaccount is used. This helps provide information to keep improving myaccount.

The information collected includes:

- the type of device being used by a user;
- the unique device identifier that the manufacturer embeds into the device (e.g. the IMEI number of a mobile phone);
- a user's operating system and browser versions; and
- the IP address used.

Every device that connects to the internet has an IP address and myaccount uses it to identify the geographic locations people access myaccount from. myaccount stores this information securely in what are called logfiles on its servers.

The Improvement Service has an interest in understanding how people are using the myaccount service so that myaccount can keep improving. Another interest is ensuring that the myaccount service is protected from malicious use and protect users from potential identity theft or account compromise.

Data Retention

The myaccount Data Retention Policy is in line with the GOV.UK Verify: IPV Operations Manual. The manual is a set of instructions for identity providers on how to provide identity proofing services in line with Good Practice Guides (GPGs 44 and 45).

The table below notes the data retention rules:

Entity	Type	State	Retention Period	Data Deleted
Account	Service Consumer	Inactivity (not logged in)	After 15 months accounts are locked, then deleted after further 45 months.	Account Data, Account History, Support Requests, Authentication Logs, Credentials
Account	Service Consumer	Never activated	Deleted after 30 days.	Account Data, Account History, Support Requests, Authentication Logs, Credentials
Account	Service Consumer	Close	Account locked for 30 days, before being disabled. Data deleted after 59 months.	Account Data, Account History, Support Requests, Authentication Logs, Credentials
Account	Service Consumer	Marked deceased	Indefinitely (used for anti-fraud check).	
Account	Agent	Inactivity (not logged in)	45 days.	Account Data, Account History, Support Requests, Authentication Logs, Credentials
Account	Agent	Never activated	45 days.	Account Data, Account History, Support Requests, Authentication Logs, Credentials
Account	Agent	Disabled	450 days.	Account Data, Account History, Support Requests, Authentication Logs, Credentials
Support Request	Myaccount	Closed	450 days then deleted after further 30 days.	Support request and audit trail
Support Request	Service Provider	closed	450 days then deleted after further 30 days. Sanitised after 30 days (see Support Request section below)	Support request and audit trail
Authentication Log	successful	Known user	5 years.	All log data
Authentication Log	Unsuccessful	Unknown user	5 years.	All log data
FTP files			Retained for 15 days then deleted after 7 days.	File

Proportionality and Necessity

Legal Bases for Processing

Data protection law means that we can only use data for certain reasons and where we have a legal basis to do so. Here are the reasons for which we process data:

Creating accounts and asserting the identity of a user

The Improvement Service are funded to supply a digital identity service to users and Service Providers. By maximising account adoption across Scotland, further demonstrates value for money for the public purse.

Legal basis for this data usage: Legitimate interest

Pass additional information to Service Providers

Optional information can be passed to Service Provider when a user logs-in to myaccount with consent from the user.

Legal basis for this data usage: Consent

Customer Support

Notifying users of any changes to our service, solving issues via our Helpdesk, phone or email including any bug fixing.

Legal basis for this data usage: Legitimate interest

Improve myaccount

Test features, interact and review feedback, manage landing pages, heat mapping our site, traffic optimisation and data analysis and research, including profiling and the use of machine learning and other techniques over your data and in some cases using third parties to do this.

Legal basis for this data usage: Legitimate interest

Asserting the identity of a user

Look up Scottish users in the NHSCR.

Legal basis for this data usage: Consent and Legal (The Local Electoral Administration and Registration Services (Scotland) Act 2006)

Look up Scottish users in the NEC Extract.

Legal basis for this data usage: Consent

Where Legitimate Interest has been sighted, a Legitimate Interest Assessment is conducted.

The legal basis for using a myaccount to access services lies with individual Service Providers and is outside the scope of this DPIA.

Further explanations of legal basis for processing can be found on the Information Commissioners Office’s website.

Standards Applicable to the Processing

The Improvement Service follows several standards to operate the myaccount service.

The myaccount service follows standards and guidelines for identity proofing set by Government including; GOV:UK Verify IPV Operations Manual, GPG 44 and GPG 45.

For authentication, SAML and OpenID Connect network federation standards are used. The OpenID Connect solution has self-certification through the OpenID website.

An Information Exchange Protocol outlines the agreed technical controls for securing data in transit between the myaccount service and Service Providers.

The Information Exchange Protocol is part of a wider Framework Services Agreement between the Improvement Service and individual Service Providers.

The Improvement Service has internal governance to assesses changes, risk, impact, supportability, privacy and alignment with architecture principles, standards, relevant legislation and Scottish Government policy guidance.

Authentication traffic is signed and encrypted using strong cipher suites and uses either SAML or OpenID Connect protocols. Strong digital certificates against fully qualified domain names are used to encrypt and sign all web services traffic including authentication.

Signature of encrypted traffic is required by both the sender and the receiver.

Any bulk traffic is transmitted using secure file transfer to named users and whitelisted IP addresses.

Data Minimisation

myaccount is built with data minimisation principles. myaccount only asks a user for the minimum amount of data they require. The minimum data required to register for a myaccount is:

- Name
- Address
- Date of birth
- Gender
- Email Address

This is a user's core identity data. Users can add optional data to their myaccount profile and consent to share that data with a Service Provider.

A Secure Visitor Token (SVT) is shared with the data a user consents to share. The SVT is an anonymous unique persistent identifier. The SVT that helps Service Providers identify a unique user.

Myaccount aligns its data policy with agreed standards set out by Government. These standards include the GOV.UK Verify: IPV Operations Manual which provides instructions for identity providers on how to provide identity proofing services in line with Good Practice Guides (GPGs) 44 and 45.

Keeping Data Accurate and up to Date

All users can keep their own details up to date via self-service on their account

Service Providers can update a user's personal data on their behalf. In such instances, a notification email is sent to the user to inform them of the change. The user can reverse the change if required.

Supporting the Personal Rights of Data Subjects

Keeping Data Subjects Informed

Many documents are made available to users to inform them of their rights and how data is used.

These documents include:
Privacy Notice
Terms and Conditions
DPIA (this document)

These documents are available on the myaccount website. The privacy notice and terms and conditions are emailed to a user when the activate their myaccount.

Any changes to these documents are communicated with users on the myaccount website. Users are prompted to read and accept the changes on screen. Acceptance of changes is logged in audit files.

Refusal to accept terms and conditions will result in in the service being withdrawn.

If Applicable, how is the Consent of Data Subjects Obtained?

Consent is captured at service enrolment and recorded in the myaccount database.

Users can view who they have consented to share data with on the myaccount website. Users can withdraw their consent at any time via their myaccount profile. Any withdrawal or consent is logged for an audit trail.

Service Providers are informed of any consent changes so that they may take the appropriate action.

Rights of Access and Data Portability

Users can log in to their profile page and see information myaccount holds about them.

Users can contact the myaccount Helpdesk to request information about their data. User can also request information in a machine-readable format.

Users may be asked to prove who they are before information is provided.

Rights to Rectification and Deregistration

Users can log into their account and change their personal information. This may require users to re-verify their identity.

Users can log in and close their account. The account will be locked for a 30 day “cooling off period”, in case the person changes their mind. The account will then be disabled. Data will be permanently deleted in line with the Data Retention Policy.

Users can contact the myaccount Helpdesk and ask for their data to be updated, amended or account closed. If the request is made by a user who has not logged in, they will be asked to prove who they are.

Users can withdraw consent to share data with Service Providers. This will erase their SVT but will not delete the information held by Service Providers. Users must contact Service Providers to request further action. Myaccount can provide users with a list of Service Providers they have consented to share data with.

Users who have linked Yoti to their myaccount have the option to ‘delink” the accounts. This will prevent the user logging into myaccount with their Yoti. myaccount will retain the Yoti Remember Me ID for fraud prevention reasons.

Rights to Restriction and to Object

Users can raise a complaint with the myaccount Helpdesk if they feel their rights have been breached. Instructions are noted within the Privacy Notice and help section on the website.

Processor Obligations

The Improvement Service has contracts with TCS and Brightsolid. They have explicit GDPR-compliant schedules. Both companies are Data Processors for the Improvement Service.

International Transfers

No data is transferred outside the EEA/European Union

Consultation

This DPIA is an update to the March 2019 DPIA. The DPIA has been updated to incorporate changes and new functionally.

Changes to the myaccount data model (which are reflected in this DPIA) were carried out in consultation with many stakeholders including:

- Scottish Local Authorities
- Scottish Health Boards,
- National Records of Scotland,
- Young Scot,
- The Open Rights Group, and
- Scottish Government.

myaccount is due to be updated throughout 2020/2021 with new features and functionality to meet customer requirements. Consultations will be carried out for new developments where required. Invitations to participate in future consultations will include the organisations listed above. Further consultation will be carried out with myaccount User Groups and other key stakeholders.

Risks

Confidentiality

Source and nature of potential impact on users	Likelihood	Severity or Harm	Mitigating controls	Overall Risk
Nature of Impact: Identity theft due to: • Spoofing, • Impersonation, • Human error. Source: • External, or • Internal human sources.	Possible Username and password are used to access most accounts. Accounts could be compromised if there is a data breach on a different site a user uses the same credentials on. Service Providers also carry out a degree of assurance before any transaction is carried out or finalised.	Distress or inconvenience to user. Potential for minor financial loss. Reputation damage to the system and service provider.	• Digital certificates for encryption and client signing, • Logical and physical controls, • Network security, and • Continuous network monitoring. Service Providers carry out additional checks before any transaction is carried out or finalised. We have controls within the data centres to monitor for potential data loss and anomalous behaviour.	Medium

Action plan / corrective actions

Two-Factor-Authentication would provide protection against account compromise due to data breaches elsewhere. The myaccount Authenticator App is available for users to voluntarily download.

Emails are sent to users to notify them if their myaccount has been accessed from a new device and at what time to make sure it is them who are accessing their account and not someone who should not be.

Continue to develop network monitoring so that a more active approach to looking for threats can be developed. Alerts need to be real time or near real time.

Integrity

Source and nature of potential impact on users	Likelihood	Severity or Harm	Mitigating controls	Overall Risk
Nature of Impact: • Human error, • Misconfiguration. Source: • Internal or • External human sources.	Possible	Minor inconvenience to one or more users.	Network security, continuous network monitoring including file integrity monitoring. Data at rest is protected by defence in depth infrastructure and a range of technical and procedural controls. Data in transit is encrypted using strong encryption and requires digital signature by both the sender and receiver before transmission.	Low

Action plan / corrective actions

Encrypt all data items within the system so that no meaningful access to personal data could be possible without the relevant keys. This would require a significant redesign and requires an impact assessment.

Availability

Source and nature of potential impact on users	Likelihood	Severity or Harm	Mitigating controls	Overall Risk
Nature of Impact: • Data breach, • Ransomware, • DDoS, • Another cyber incident. Source: • Internal or • External human sources, • Non-human sources.	Likely	Minor inconvenience to many users. myaccount is used by many Local Authorities with usage increasing. Lack of service could cause inconvenience to users. Other channels (face to face, telephone) are generally still offered by Service Providers.	• DDoS protection in data centres, • Failover to warm standby site, • Contract/SLA with supplier.	Medium

Action plan / corrective actions

Consider enhancement to DDoS service if cost effective,

Existing and Planned Measures

Accreditation

Myaccount is operated in line with security best practice. Accreditation to ISO27001 is currently being sought.

Encryption

All authentication transactions are signed and encrypted using strong digital certificates and delivered over TLS. Transactions must be signed by valid digital certificates by both sender and receiver. All bulk data transfer uses secure file transfer over TLS with IP whitelisting.

Logical access control

VLANs are used to separate different environments. IP whitelisting and shared metadata in conjunction with digital certificates ensure that partner organisations are trusted.

Strong password controls in password policy.

No generic accounts are permitted so that all actions within the system are traceable to an individual. This is monitored and reported on as part of routine service management.

Use of captcha and failed login account lockout is used to mitigate brute force attacks.

Remote access for support personnel is via VPN and 2FA to named users only.

All privileges and access are reviewed monthly. Any elevation of privileges is monitored and reviewed.

Operating security

Comprehensive System Security Policy covering all elements of operational security. Adopted/signed by all contractors and sub-contractors.

Website security

Real time monitoring from industry-leading specialist products includes both external and internal anomalies. Annual IT Health Check is carried out by an accredited security company. Formal change and release management policies require vulnerability assessment prior to any upgrade or deployment.

Monitoring network activity

GPG13 compliant network monitoring including anomaly detection, malware and virus scanning.

Protecting against non-human sources of risks

Secure resilient UK data centres (primary data centre with warm standby failover to secondary).

Policy

Security policy framework includes a range of procedural controls including extensive system security policy adopted by contractors and sub-contractors.

Managing privacy risks

Fortnightly risk and change boards within Improvement Service look at all risks to the services with clear escalation paths to senior stakeholders. SIRO signs off residual risk.

Integrating privacy protection in projects

Threat modelling as standard in new developments. DPIA screening using ICO guidance. Staff awareness sessions and supporting documentation.

Traceability (logging)

Audit logs are stored and encrypted to prevent tampering. Logs are aggregated into SIEM. Logs are analysed for near real-time threats and longer-term trends analysis.

Clamping down on malicious software

Up to date anti-virus/anti-malware on all connected system machines. Anti-virus/anti-malware scanning on network boundary for all inbound and outbound traffic.

Maintenance

Routine patching policy with machines updates every 6 months or immediately if emergency arises. Industry-leading specialist software used to block any unpatched vulnerabilities through routine application of IDS rules. This gives breathing space to manage patching.

Physical access control

Data Centres are ISO27001 accredited. Strong perimeter controls, mantraps, turnstiles. Visitors escorted on premises, wearing of visible badges is mandatory. IS premises protected by electronic door entry.

Hardware security

All builds created from golden images, cabinets locked, storage deletion using CESG-approved software accredited up to OFFICIAL. Controls over management ports, firewall rules tested and reviewed regularly by independent security company.

Processing contracts

Contracts include specific instructions on what data to be processed, and how, in line with GDPR et al requirements. Solution design signed off by security architect prior to go live.

Network security

Host based firewalls with deny all by default and specific entries to limit traffic only to what is required between machines. IDS/IPS monitoring. Regular internal scans using industry-leading specialist software. Solution being extended in 2018-19 to include user behaviour analytics.

DDoS Protection

Data Centre provides DDoS protection service that can be switched on if a spike in traffic is detected. Possibility of having DDoS protection switched on permanently under investigation.

Sign-Off and Record Outcomes

Action plan

Launch Two Factor Authentication to increase account security.
Expected date of implementation:
Android App launched in July 2019. IOS version launched in April 2020.

Continue to develop network monitoring so that a more active approach to threat hunting can be developed. Alerts need to be real time or near real time.
Expected date of implementation: Ongoing

Encrypt all data items within the system so that no meaningful access to personal data could be possible without the relevant keys. This would require a significant redesign though and an impact assessment
Expected date of implementation: to be assessed in 2020.

Sign-Off

Item	Name/date	Notes
Measures approved by:		
Residual risks approved by:	SIRO	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Chief Security Officer 30/08/2019	
Summary of DPO advice: Suggest with the addition of the attribute service that consideration is given to how these attributes are stored and released with the user's consent. Avoidance of large-scale data stores is preferable but may be the only solution so strict controls are required – this should be reflected in risk assessments or threat modelling. It may be pertinent to examine the concept of personal data stores and/or DLT with appropriate encryption and signing.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

Updates

Version 3.4

Why did we change the DPIA?

We're improving our DPIA and making them easier for you to understand. These changes reflect an evolving regulatory environment and our ongoing efforts to simplify how we communicate with users.

What are the main changes?

At a glance, here's what this update means for you:

- **Improved readability**: We've done our best to make the DPIA easier to understand which includes adding links to useful information and providing definitions.

Previous Versions

We want to be as transparent as possible about the changes we make to our DPIA.
In this archive you can see versions of our DPIA.

Version 3.3

Definitions

Authentication

This is the process you go through to sign-in to myaccount.

CAPTCHA

CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. In other words, CAPTCHA determines whether the user is real or a spam robot. CAPTCHAs stretch or manipulate letters and numbers and rely on human ability to determine which symbols they are.

Data

This is information about you that you give us like your name or email address,
or
information we collect while you use our service, like what type of device you are using or browser.
Our Privacy Notice explains more about how your information (data) is used.

Federated Identity Assurance Services

A federated identity in information technology is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.

Identity

Any reference to identity in myaccount refers to the identity of the user, which is you. You have an identity and at times, you may be asked to verify your identity to prove who you are. This enables service providers to provide you with the correct service and prevent people from fraudulently gaining access to a service.

IDP

An identity provider (abbreviated IdP or IDP) is a system entity that creates, maintains, and manages identity information for principals while providing authentication services to relying applications within a federation or distributed network. Identity providers offer user authentication as a service.

ISO 27001

ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

Log Files

A log file is a file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software.

Open Standard Protocols

Open standard protocols for identity federation define how service providers (SPs) and identity providers (IdPs) exchange identity information. Open standards are critical to enable secure interoperability between unique identity systems, web resources, organisations and vendors.

Service Provider

Is an organisation that uses myaccount to allow people to login to access their services online. Like a council offering people the service to view their council tax bill online.

Single Sign On (SSO)
Single sign-on is an authentication process that allows a user to access multiple applications with one set of login credentials.

Two Factor Authentication (2FA)
Two-factor authentication (2FA), sometimes referred to as two-step verification or dual-factor authentication*,* is a security process in which users provide two different authentication factors to verify themselves.

Example: a user can sign-in to an account using a username and password (something they know) and an authentication code is sent to their mobile phone (something they have).
If a user could sign in without the code, there's a risk that someone else could guess or steal their password to access their account. Using an authentication code as another authenticator means that, even with the password, a fraudster would still not be able to access the account.

Users
This is you and other people who use our services.

Verified
This means you have gone through a process to prove you are who you claim to be. You have verified your identity.

VLANS
A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs). A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area.

Yoti
Yoti is a company which the Improvement Service contracts with to provide us with services. Their services enable you to register, sign-in and verify a myaccount. More info can be found on their website.