mygovscot myaccount

The secure and easy way to access public services online

Data Privacy Impact Assessment

V2.0

March 2019 Update

www.improvementservice.org.uk
signin.mygovscot.org

Operated by The Improvement Service
Scottish Government funded

improvement service

Document Control

Document Title	**DPIA - myaccount**		
Issue Status	V2.0	Issue Date	11/03/2019
Author	Business Owner	Title	
Tel:		E-Mail	
Security Classification	Public	Retention Period	Per policy
Review Period	Annual		

Version No	Date	Summary of changes
1.0 FINAL	15/08/2018	Released
2.0 FINAL	11/03/2019	Update following changes to myaccount functionality

Authorisation

Document Approvals

Document Authorisation	Title/Organisation	Date
	Director Customer First	11/03/2019

Contents

The Need For a DPIA 5

The Processing 5

Nature of the Processing 5

Data processing lifecycle 5

Processing responsibilities 5

Scope of the Processing 6

Account Registration 6

Raising a Query 7

Verifying Identity 7

Registration by an Organisation 8

Personal data we generate when the service is used 8

Personal data we collect from other sources 8

Personal data we collect when someone uses the service 8

Data Retention 9

Context of the Processing 10

Purposes of Processing 11

Consultation 11

Proportionality and Necessity 11

Legal bases for processing 11

Standards applicable to the processing 11

Data minimisation 12

Keeping data accurate and up to date 12

Supporting the Personal Rights of Data Subjects 12

Keeping Data Subjects Informed 12

If applicable, how is the consent of data subjects obtained? 13

Rights of Access and Data Portability 13

Rights to Rectification and Erasure 13

Rights to Restriction and to Object 13

Processor Obligations 14

International Transfers 14
Risks 15
Confidentiality 15
Integrity 16
Availability 17
Existing and Planned Measures 18
Sign-Off and Record Outcomes 20
Action plan 20
Sign-Off 21

The Need For a DPIA

This DPIA has been created in line with guidance released by the Information Commissioner's Office (ICO) in May 2018 at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/. The guidance lists categories that trigger a mandatory DPIA. The triggers for myaccount are:

- New technologies: the service is introducing machine learning/AI for security monitoring purposes and real-time alerting to potentially fraudulent activity
- New technologies: the service is looking at how the innovative use of new technologies could make the online identity proofing process easier for individuals
- Combine, compare or match data from multiple sources: the service will use several different identity validation and verification sources to establish that account holders are who they claim to be

The ICO has also identified that services such as federated identity assurance services, of which myaccount is one, would attract a mandatory DPIA.

Regardless of the ICO guidance, Improvement Service policy dictates that major systems that process personal data will always be subject to a DPIA either before implementation or following a significant change.

The Processing

Nature of the Processing

Myaccount is an identity verification and sign-in service designed to help public sector organisations deliver services to the correct individual. It consists of several services including account registration, identity validation and verification, data correction, authentication and sign-in, service enrolment with Service Providers, notification of changes of circumstances and a helpdesk/support system.

Data processing lifecycle

See the Information Flow Architecture Document for detailed information.

Processing responsibilities

The Improvement Service, a company limited by guarantee and registered in Scotland (Company No. SC287978) and operating from iHub, Quarrywood Court, Livingston, EH54 6AX is the operator of myaccount.

The Improvement Service is the Data Controller for all account registrations. Anyone in the world can register for a myaccount and initially all accounts are unverified unless the user registers for a myaccount using Yoti where 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 are a Data Controller of the attributes that users provide them. At the point attributes are shared with myaccount by a user The Improvement Service becomes a Data Controller of those Attributes in their own right.

When an account holder goes on to enrol with a Service Provider, the Service Provider becomes joint Data Controller with the Improvement Service for that account. This is because the Service Provider can make decisions on the data held in the myaccount service e.g. manage level of assurance, change contact details.

Account holders can validate and verify their personal details in different ways and may be asked to provide supplementary proof to support this. Proofs may be presented in person or electronically. They are checked for authenticity and applicability to the account holder.

Checking of proofs may be carried out automatically by checking against electronic data sources or manually by inspection by authorised agents. Agents will normally be Local Authority or Health Board staff authorised to carry out this task.

An exception to the above is verification of identity by checking against the extract of the National Health Service Central Register (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 holds a limited extract of the register to help us verify that account holders are who they claim to be. The Improvement Service looks up this list automatically whenever someone resident in Scotland registers for an account.

Another exception to the above is verification of identity where users provide verified data from their Yoti account. Registering using Yoti allows the myaccount applicant to achieve a higher level of trust within the service (verified status) as proofs of identity and residence have already been checked as part of the Yoti application process. Registration using a Yoti is entirely voluntary.

The Improvement Service has contracts with a managed service company (TCS) and a hosting company (brightsolid UK). Both companies are Data Processors for the Improvement Service. The contracts with these companies relating to the service have been updated to reflect the GDPR obligations of both the Improvement Service and the contractors.

Scope of the Processing

Basic personal information is collected from anyone in the world who wants to set up an account. Account holders can gain verified status by providing proofs of identity that can be checked against trusted identity stores. No special categories of data are processed.

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

- directly from someone registering for an account
- directly from someone raising a query
- directly from someone verifying identity
- from an organisation when that organisation registers someone for an account
- generated when someone enrols with a Service Provider
- from other sources to help prove that someone is who he or she claims to be
- from the devices used to access the service

Account Registration

Information That Must Be Provided to Get an Account

Some of the personal data is mandatory as it is required to establish identity (core identity data) and to manage the account. This includes name, gender, address, date of birth, e-mail address and user name (if different from email address).

Users also have the option to register for a myaccount using their Yoti account.
When selecting this option, users will be prompted to consent to share their Yoti information on the Yoti app to create a myaccount; this includes: full name, given names, family name, email address, date of birth, gender address (Structured) and Yoti Remember Me ID. Only Yoti accounts where both the name and address has been verified will be allowed to register for a myaccount.

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

Optional Information That May Be Helpful

We also allow account holders to provide additional, optional information that may be helpful to Service Providers in allowing them to personalise the services they provide or contact users if there is a problem. This optional information includes mobile telephone number, landline telephone number, preferred first name and preferred last name.

If account holders live in Scotland and cannot be found automatically in the NHSCR (or multiple matches are returned from the details entered), mother's birth surname and place of birth will be asked for. We pass these two pieces of information along with the claimant's forename, surname, gender and Date of Birth to NRS to see if they can find the correct details. Provision of these two pieces of information is optional.

Raising a Query

We offer a support request system that can be used by anyone. To allow us to contact request originators and keep them up to date with progress we require a valid email address. Requestors can also supply a contact telephone number but it is entirely optional.

In some instances, a requestor will raise a query that relates to the Service Provider rather than the myaccount service. We forward this request to an authorised Agent within the Service Provider organisation for action. Once the request has been closed by the Agent, we sanitise the data by removing the body of the request leaving only a reference number, a requestor ID and the date and an audit trail of how the request has been handled. This prevents us from inadvertently storing information that has been entered by the requestor in a free text field that may be sensitive in nature. Retaining the handling history allows us to route the request back to the Service Provider if the original requestor raises the same request a second time.

Verifying Identity

Some services require assurance that Service Consumers are who they claim to be so they may need to supply supporting evidence before being granted access to a service. We may ask for identity information (Passport, Driving Licence, utility bill details and so on) that we can check with other trusted sources. When we check with other trusted sources we will send them the information submitted and ask them to verify that they can match those details in their own systems by returning an answer of either 'yes' or 'no'. We offer a range of options and choices that allow Service Consumers to do this, including:

- verify identity using a verified Yoti
- scanning and uploading different forms of identity evidence
- submitting electronically a photograph or video of self and/or identity documents ('selfie')
- submitting details electronically about services the consumer may already have used, for example a Council Tax Reference number or other identifier
- sharing social media profile details
- answering questions about services consumers may have used in the past and to which only they are likely to know the answer
- checking bank or financial details
- having an authorised person vouch for the consumer
- visiting an authorised office in person to prove identity to an Agent

These options are provided to ensure that the widest possible range of technologies, supporting evidence and personal choice can be accommodated but some services may ask for specific checks, like a passport for example, for legal or regulatory reasons.

Details that are supplied specifically to prove identity will be deleted once they have been checked and verified either automatically against a trusted electronic source or in person by an authorised agent (Agent). An Agent will normally be an authorised employee within a Local Authority or Health Board.

Note that we will have to perform periodic identity checks on account holders and we may, from time to time, ask for information to be resubmitted so that we can check it is still valid.

Registration by an Organisation

Some Service Providers use myaccount by collecting personal data themselves and using electronic tools (web services) to create an account on the claimant's behalf and in doing so pass personal data to us.

The information we receive from such Service Providers setting up an account is the same as the information that the claimant would have entered personally. They pass this information to us so that we may verify an identity.

Some Service Providers may establish identity before setting up an account on the account holder's behalf. In this case, they may also pass us information that relates to what verification process was carried out. This would include:

- Verification Levels – either unverified, partially verified or verified. (Previously named Scottish Levels of Assurance 0, 1 & 2).
- An indication of what identity evidence was presented. We don't get the proofs, just a note of what was presented (for example we might be told that a passport was presented but we wouldn't get the passport number or any of the passport details)

Personal data we generate when the service is used

When someone creates an account with us and uses it to access a service with a Service Provider, we generate a unique anonymous identifier for that account holder (a Secure Visitor Token or SVT) and pass it to the Service Provider along with the other identity attributes in scope. The SVT is shared only between the account holder and the Service Provider and is only used at log in. It helps the Service Provider know that this is the same person that logged in last time. If the account holder enrols with more than one Service Provider then we generate additional SVTs, one for each service.

Personal data we collect from other sources

When we verify identity, we check details against the extract of the NHSCR that we hold and if there is a match, record the UCRN. We will also look up the extract of the NHSCR to find a CHI number if the account holder is accessing a health-related service. We are legally allowed to hold and process the data in the NHSCR limited extract by the LEARS (Scotland) 2006 Act.

Personal data we collect when someone uses the service

We collect data that helps us understand how people are using the service so that we can improve it over time. The information we collect includes the type of device, the unique device identifier that the manufacturer embeds into the device (e.g. the IMEI number of a mobile phone), operating system and browser versions and the IP address from which the service is being accessed. Every device that connects to the internet has an IP address and we use it to identify the geographic locations from which people access the myaccount service. We store this information securely in logfiles on our servers.

We also use this information to protect account holders and us from potentially malicious or fraudulent use. For example, if the service is accessed using a device we have not seen before, we may ask the account holder to authorise that device before continuing to use the service.

Data Retention

myaccount data is stored in line with the myaccount Data Retention Policy. The following table refers:

Entity	Type	State	Retention Period	Data Deleted
Account	Service Consumer	Inactivity (not logged in)	450 days then deleted after further 30 days	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	Revoked	Deleted after 30 days	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	750 days	All log data
Authentication Log	Unsuccessful	Unknown user	750 days	All log data
FTP files			Retained for 15 days then deleted after further 7 days	File

Context of the Processing

Many online public services require surety of identity on the part of the person requesting the service. Trying to ensure that someone is who he or she claims to be in an online context is fraught with difficulty.

The myaccount system is designed to enable identity proofing across a range of service requirements ranging from anonymous transactions - where no proof of identity is required - to more trusted transactions i.e. where proof of identity is required to ensure protection of the public purse or the avoidance of fraud or identity theft.

The process to validate and verify trusted account holders should ideally meet the following criteria:

- a single, unique trusted identity should exist within the context of the population of users that myaccount serves
- all supplied evidence should be correct and genuine (i.e. not counterfeit or misappropriated)
- the claimed identity should exist in the real world
- the claimed identity should be successfully associated with the real person supplying the identity evidence

The proofing processes in the myaccount service are designed to meet these aims. The outcome of the proofing process is a Verification Level that reflects the type of evidence produced, how robustly it has been checked and how trustworthy the evidence is viewed.

This is a common model for federated identity assurance.

The mandatory information asked of applicants supports this process.

The myaccount service asserts identity only. When an account holder successfully logs in and requests a service that requires authentication, identity attributes relating to that user are passed securely to the provider of the service who will use those attributes to make an authorisation decision. The myaccount service has no knowledge of the Service Consumer's interaction with the service itself, other than the fact that the Consumer has logged in.

On registration, Service Consumers can provide additional optional information that may be useful to both them and Service Providers. This does not relate solely to identity but relates to the service and includes elements such as contact details which are useful to follow up service requests or personalise the service.

Within the myaccount service, the Service Consumer must consent to this optional information being passed to Service Providers. Core identity information, the mandatory information supplied as part of account registration, will be passed at login as this is a condition of using the service.

Within the myaccount service, each Service Consumer can see the services with which they have enrolled and what optional information they have agreed to share. They can also manage their consent from within their profile page and revoke it if they wish.

The myaccount service uses open standards for identity federation that are commonly used for such services e.g. SAML and OpenID Connect. The service is accredited by National Records of Scotland (NRS) using UK Government standards. Accreditation is managed and monitored through an independent oversight group comprised of senior Information Assurance professionals from across the public sector and a representative of the supervisory authority (Information Commissioner's Office).

Purposes of Processing

Personal data is collected and processed for the following purposes:

- to allow an individual to set up an account and access a range of public services
- to notify online public Service Providers of a change to personal data
- to determine that an applicant for myaccount is real and genuine
- to help account holders with any queries they may have in relation to the service
- to help develop and improve the services that myaccount offers
- to protect individuals and the service from fraudulent or malicious use

Consultation

This DPIA is a refinement of the revised August 2018 DPIA (to align with GDPR requirements) to incorporate changes and new functionally that have been made to the myaccount service.

The myaccount service is due to be continually refreshed throughout 2019 with new features and upgrades and ongoing consultations will be carried out for those developments; including further and ongoing consultation with the Open Rights Group and its wider network. myaccount User Groups and key stakeholders will also be invited to participate in ongoing consultations.

Proportionality and Necessity

Legal bases for processing

The legal basis for account creation and assertion of identity is in the legitimate interest of the Improvement Service to supply a digital identity to Service Consumers and maximise account adoption. This demonstrates value for money for the public purse as the Improvement Service is funded by Scottish Government. A legitimate interest assessment has been carried out and recorded.

Where optional information may be passed at logon, the legal basis for processing is consent of the individual account holder.

The legal basis for looking up Scottish residents in the NHSCR is the LEARS (Scotland) Act 2006.

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

Standards applicable to the processing

The Improvement Service has standards for identity proofing i.e. for what identity evidence must be presented to prove that someone is who he or she claims to be and how that evidence is checked. A differentiation is made between data collected only for identity purposes (core identity) and other optional information that may be of use to Service Providers to deliver services. In general, the optional information consists of contact details so that any requested service can be followed up or the service personalised to the requesting individual.

For sign-in, 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 Data Sharing Agreement between the Improvement Service and individual Service Providers. The Data Sharing Agreements are approved and managed through a formal change management process by the Improvement Service Change Board which meets fortnightly. The Change Board assesses all changes for 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

An account applicant must provide the minimum amount of information to allow an identity to be checked as part of registering for the myaccount service. This minimum amount of information is set as:

- name
- address
- date of birth
- gender
- a unique persistent identifier that helps differentiate between cases where duplicates might exist within the myaccount service user population

These data elements are in line with agreed standards on identity set out in 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.

Other optional information processed relates to what might be deemed reasonable for someone to access an online service. This is either to have the system personalised in some way or to provide contact details so that the Service Consumer can be informed of progress or any issues with the requested service.

Keeping data accurate and up to date

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

Service Providers may also submit changes to personal data to the myaccount service. In such instances, a notification by email is sent to the account holder and the change only applied if the account holder confirms.

The core NHSCR data is maintained by the NHSCR team in NRS. Changes are received periodically by the Improvement Service and any impacts on existing holders e.g. notification of a death are assessed and implemented.

Supporting the Personal Rights of Data Subjects

Keeping Data Subjects Informed

Data Subjects are informed via a privacy notice displayed on the myaccount website. A Data Privacy Impact Assessment (this document) and Information Architecture documentation including flow diagrams have also been published.

The privacy notice and any other terms and conditions relating to the service are displayed at account registration and are sent to the account holder's registered email address on successful account activation.

Any change to the terms and conditions or privacy notice are communicated to account holders on the website. A confirmation notice asking users to accept the changes is displayed at the next login. Acceptance of changes is written to an audit file along with the specific versions that were accepted. Failure to accept the conditions means that the service is no longer accessible. In this instance, the account is permanently deleted.

If applicable, how is the consent of data subjects obtained?

Consent to pass optional attributes to a Service Provider is captured at service enrolment and recorded in the myaccount database.

Via the myaccount profile page, account holders can see and manage the organisations with which they have consented to share optional information.

Via the myaccount profile page, account holders can withdraw their consent to pass optional information to Service Providers.

Any withdrawal or provision of consent is written to a date and time stamped audit trail.

Service Providers are informed of any changes to consent via routine service reporting so that they may take the appropriate action.

Rights of Access and Data Portability

Data subjects can log in and navigate to their profile page and see information held about them in the myaccount system.

Data subjects can also contact the Improvement Service by raising a support request in the myaccount system to ask for any additional information or for their data to be presented to them in a machine-readable format.

If the request is made by a user who has not logged in then an identity verification process is required before the request will be approved.

Rights to Rectification and Erasure

Data subjects can log into their account and change their personal information. Doing so may trigger a requirement to re-prove identity in some instances

Data subjects can log in and revoke their accounts. The accounts will then be permanently deleted after 30 days.

Data subjects can contact the Improvement Service using the support request system and ask for their data to be updated, amended or erased. If the request is made by a user who has not logged in then an identity verification process is required before the request will be approved.

Data Subjects can 'unenroll' from services with Service Providers. This will erase their SVT but will not delete the information held by Service Providers. Data Subjects must contact individual Service Providers to request further action. The Improvement Service can provide Data Subjects with a list of Service Providers with which they have enrolled.

Where Data Subjects have linked their myaccount to their Yoti, they have the option to ‘delink” the accounts; preventing the user from being able to login to myaccount using Yoti in the future. myaccount will still retain the Yoti Remember Me ID for fraud prevention reasons.

Rights to Restriction and to Object

Data subjects can contact the Improvement Service by raising a support request. If the request is made by a user who has not logged in then an identity verification process may be required before the request can be actioned.

Instructions are included within the Privacy Notice on the website and sent to account holders at registration on how to lodge a complaint with the supervisory authority if they feel their rights have been infringed.

Processor Obligations

The Improvement Service has contracts in place with TCS and brightsolid that have explicit GDPR-compliant schedules.

International Transfers

No data is transferred outside the EEA/European Union

Risks
Confidentiality

Source and nature of potential impact on individuals	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 We are still currently using only username and password so there is a possibility of account compromise due to users who might use the same credentials on other sites and those sites were somehow compromised. But Service Providers also carry out a degree of assurance before any transaction is carried out or finalised.	Distress or inconvenience to an individual; potential for minor financial loss. While most of the services currently being used require low levels of assurance, the system itself may suffer reputational damage if its overall trust was compromised. There are also some services that require higher levels of assurance - such as benefits claims - so an individual could undergo distress or financial inconvenience if the account was compromised.	Digital certificates for encryption and client signing, logical and physical controls, network security, continuous network monitor. Service Providers also 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 although reporting is not yet in near real time.	medium

Action plan / corrective actions

2FA would provide some protection against account compromise due to data breaches elsewhere (users are prone to using the same credentials on multiple sites). This is currently on the roadmap for implementation by the middle of 2019.

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. Many breaches or data losses often go undetected for many months or even years after a breach occurs.

Integrity

Source and nature of potential impact on individuals	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 individuals.	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

Consideration could be given to encryption of 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 needs proper impact assessment on both Service Providers and Consumers.

Availability

Source and nature of potential impact on individuals	Likelihood	Severity or Harm	Mitigating controls	Overall Risk
Nature of Impact: data breach, ransomware, DDoS, other cyber incident. Source: internal or external human sources, non-human sources.	Likely	Minor inconvenience to many individuals. The service is used by many Local Authorities and there is likely to be an increasing reliance on this channel. This in turn could cause inconvenience to individuals although other channels for service delivery (face to face, telephone) are generally made available 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

The myaccount service has been independently accredited by NRS with the accreditation overseen by a cross public sector management forum that includes senior Information Assurance representatives including a representative from the supervisory authority. Accreditation is based on UK Government IS1/IS2 risk assessment using iso27001 baseline control set. Accreditation includes a range of technical, administrative and physical controls. The scope of the accreditation includes the Improvement Service and all its sub-contractors/processors/sub-processors.

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 polices 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).

Organisation

IASMF - cross sectoral body of senior IA professionals oversee myaccount accreditation. Meets regularly. Includes representative from supervisory authority.

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. IS currently working towards CyberEssentials+.

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

Implement utility within the account to allow a logged in user to download data in a machine-readable format.
Expected date of implementation: 31/12/2019

2FA would provide some protection against account compromise due to data breaches elsewhere (users are prone to using the same credentials on multiple sites).
Expected date of implementation: Mid 2019

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. Many breaches or data losses often go undetected for many months or even years after a breach occurs.
Expected date of implementation: Ongoing

Consideration could be given to encryption of 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 needs proper impact assessment on both Service Providers and Consumers.
Expected date of implementation: to be assessed as in late 2019

Sign-Off

Item	Name/date	Notes
Measures approved by:		
Residual risks approved by:	Director	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Role Date	
Summary of DPO advice: As this is an update in format no further actions required apart from those identified in the Action Plan		
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:		