mygovscot myaccount
Privacy Notice

Version 3.4

Contents

The myaccount Privacy Notice

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

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

About us

mygovscot myaccount services are provided by, and you are contracting with:

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.

This notice (together with our Terms & Conditions) applies to your use of myaccount.

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.

What is mygovscot myaccount?

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

Myaccount enables you to set up an online account, prove who you are and use that one account to access different online public services. We do this by transferring information about you to the organisation that is providing the service (Service Provider) when you log in. This tells Service Providers who you are. Service Providers uses that information to decide if you should be granted access to their service.

Some services will require you to have either a partially verified or verified account. We will always show you what personal information you are sharing with the Service Provider when you sign up for a service.

Our role in your privacy

Registration

We are the Data Controller for all account registrations.

Anyone in the world can register for a myaccount. Initially, your account is unverified, unless you register for a myaccount using Yoti. Verified data from your Yoti account will enable you to create a verified myaccount.

(Yoti is a global identity platform and free consumer app that enables you to put your ID on your 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 you provide them. When you share those attributes with myaccount, the Improvement Service becomes a data controller of those attributes.

Accessing Services from Service Providers

We become a joint data controller with a Service provider when you consent to share your data to access a service. We are joint Data Controllers for your account for the purposes of identity only.

This is because the Service Provider can update your details with your consent e.g. update your contact details.

Your responsibilities

- Read this policy
- Make sure your data is kept up to date
- Keep your myaccount credentials safe and do not share them

When and how we collect data

We collect information about you in several different ways:

1. When you register for an account;
2. When you raise a query with us;
3. When you verify your identity;
4. From data sources to help you prove who you are;
5. From a Service Provider who registers you for an account;
6. When you use myaccount to access a service;
7. From the device you use when you use our service.

1) When you register for myaccount

Some of the personal data you give us when you register for an account is mandatory as we need it to establish who you are and to help you manage your account.

We call this your core identity data and includes your:

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

We also ask you to set a password when you activate your account. We never share your password with Service Providers or anyone else.

You also have the option to register for a myaccount using your Yoti account. If chosen, you will be asked to consent to share your Yoti information (on the Yoti app) to create a myaccount.

The information includes your:

- 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 your Yoti to your myaccount. The Remember Me ID has no meaning outside the Yoti app).

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

Optional Information

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

This optional information includes:

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

2) Raising a query

If you want to contact us or report a problem, you can via the myaccount Helpdesk. You must supply a valid email address to enable the Helpdesk to reply to the query. You can also supply a contact telephone number if you would prefer that

If a query is about proving your identity, the Helpdesk may ask you 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.

3) Verifying your identity

myaccount has three verification levels:

- Unverified;
- Partially Verified; and
- Verified.

Some Service Providers need you to prove who you are. Therefore, you may need to supply supporting evidence before you can access a service. Some services may require you to have a partially verified or verified account. That's for the Service Provider to decide.

myaccount offers you the ability to partially verify or verify your account. If you have a partially verified or a verified myaccount, the Service Provider will have greater confidence you are who you are who you say you are.

A verified account means that you have gone through some checks to help prove who you claim to be. We will tell the Service Provider you have a verified account when you use myaccount to access their service.

We offer a range of options you can choose from to set up a verified account, including:

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

We will not ask you to do all the things in the list above. As we need to meet Government Identity Standards, we may ask you a range of different questions or ask you 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.

We look to provide you with multiple options. Some services however may require certain documents or checks to be conducted. For example, must verify using a passport or driving licence.

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

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

Details you supply to prove your 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, we may have to retain some information you supply for audit purposes. Access to audit information is strictly controlled. All access requests are logged and scrutinised periodically.

We may have to perform periodic checks on your identity while you hold a myaccount.
You may be asked to resubmit information so that it can be rechecked to maintain you verified status.

4) Data sources to help prove who you are

Attribute Service

To gain access to specific services, some Service Providers may require additional information (attributes) in addition to your myaccount data to be able to match you to their own back office systems or confirm your entitlement before providing access to a service.

Our Attribute Service helps Service Providers to do just that. We can look up data extracts (with explicit consent and under specific conditions) to confirm your details and provide an additional attribute to the service provider (if required).

Examples are noted below:

A local authority may request us to confirm your details against a limited extract of the National Health Service Central Register (NHSCR) to retrieve your UCRN (Unique Citizen Reference Number). The UCRN is unique to you and helps the Local Authority distinguish between you and other people who may have the same name. A Local Authority can use the UCRN to find/match your details in their back-office systems to provide you access to a service.

We will only look up your details against the NHSCR Extract with your consent user and your account is either partially verified or verified.

A health board may request us to confirm your details against a limited extract of the NHSCR to retrieve your CHI Number (Community Health Index Number). The CHI Number is unique to you and helps a Health Board distinguish between you and other people who may have the same name. A Health Board can use the CHI Number to find/match your details in their back-office systems to provide you access to a service.

We will only look up your details against the NHSCR Extract with your consent and your account is either partially verified or verified.

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

If you provide consent for us to check your details against the NHSCR Extract or **another data set (if available)** to retrieve an attribute, we do not store this attribute with your myaccount data. The data is stored separately. We get 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. We 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. We process 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 we look up your details in the NHSCR extract to get the UCRN or CHI number we must follow rules laid down (that are superimposed on the NHSCR Regulation) by NRS/the Registrar General and the NHS. These rules dictate that:

- We can only give the UCRN to Local Government;
- We 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 your identity via National Entitlement Card Extract

We may use a limited extract from the National Entitlement Card (NEC) system to help you partially verify or verify your account. The extract may also be used to confirm your eligibility to access a service from a Service Provider.

When we use the extract, we are acting as Data Processors under written instruction of the appropriate Data Controller.

Dundee City Council (acting as the National Entitlement Programme Office (NECPO)) operates the NEC scheme 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 Notice on its website.

When we check your information against the NEC extract, we must follow rules laid down by NECPO, acting as the Data Controller for all 32 Scottish Local Authorities.

We will only check your details against the NEC Extract if you provide consent.

The NEC extract is a list of everyone who has a National Entitlement Card. The extract contains basic information such as your name, address and 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.

5) Registration by an organisation

Some Service Providers can create a myaccount on your behalf with your consent. The Service Provider will collect the required information from you and use myaccount web services to register you for a myaccount.

The information we receive from Service Providers setting up your account is the same information you would enter when setting up an account yourself.

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

- Unverified;
- Partially Verified; or
- Verified.

We don't receive the proofs from Service Providers. We are just informed what was presented. For example, note that you verified your identity by presenting a passport, however no passport details would be passed to us. If a Service Provider creates accounts in this way, they must follow the standards and rules set by us.

6) Personal data we generate when you use the service:

The data helps Service Providers identify who you are.

Within the myaccount service, you can see the Service Provider you have consented to share data with. You can also check what specific data you have agreed to share. You can manage your consent from within your profile page and withdraw it if you wish.

When you sign-in to myaccount to access a service with a Service Provider, we generate a unique, anonymous identifier for you. The identifier is called a Secure Visitor Token (SVT) and is sent to a Service Provider along with the attribute's you agree to share.

The SVT is only shared between you and the Service Provider and is only used when you log in. It helps the Service Provider know that you are the same person that logged in previously.

If you enrol with more than one Service Provider then we generate additional SVTs, one for each service with which you enrol.

7) Personal data we collect from your device

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

The information collected includes:

- the type of device you use;
- the unique device identifier that the manufacturer embeds into the device (e.g. the IMEI number of a mobile phone);
- your operating system and browser versions; and
- the IP address used.

Every device that connects to the internet has an IP address and we use it to identify the geographic locations you access myaccount from. We store this information securely in logfiles on our servers.

We have an interest in understanding how people are using our service so that we can keep improving it. Another interest is ensuring that the service is protected from malicious use and protect you from potential identity theft or account compromise.

How and why we collect your data

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

Creating accounts and asserting your identity
We are funded to supply a digital identity services 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 you log-in to myaccount with consent.
Legal basis for this data usage: Consent

Customer Support
Notifying you 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, publish questionnaires, interact and review feedback, manage landing pages, heat mapping our site, traffic optimisation and data analysis and research.
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.

We will not sell your information or disclose it for direct marketing purposes.

Your Rights

Keeping you Informed

These documents inform you of your rights and how your data is used:

- Privacy Notice (This document)
- Terms and Conditions
- DPIA

These documents are available on the myaccount website. The privacy notice and terms and conditions are emailed to you when you activate your account.

Any changes to these documents are updated on the myaccount website. You will be 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.

Capturing you consent to share data

Consent is captured when you request to access a new service and is recorded in our database.

You can view who you have consented to share data with on the myaccount website. You can withdraw consent at any time via your 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.

Right to access data

You can log in to your profile page and see information we hold about you.

You can contact our Helpdesk to request information about your data. You can also request information in a machine-readable format.

You may be asked to prove who you are before information is provided.

Right to change and delete

You can log into your account and change your personal information. This may require you to re-verify their identity.

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

You can contact our Helpdesk and ask for your data to be updated, amended or account closed. If you are not logged in, you will be asked to prove who you are.

You can withdraw consent to share data with Service Providers. This will erase your SVT but will not delete the information held by Service Providers. You must contact Service Providers to request further action. We can provide you with a list of Service Providers you have consented to share data with.

If you have linked Yoti to myaccount, you have the option to 'delink" the accounts. This will prevent you logging into myaccount with Yoti. We will retain the Yoti Remember Me ID for fraud prevention reasons.

Right to object

You can raise a complaint with our Helpdesk if you feel your rights have been breached. Instructions are noted within the Privacy Notice and help section on the website.

How secure is the data we collect?

We work hard to protect your information and keep it safe from unauthorised disclosure, alteration or destruction. Some of the measures we use include:

- using a reputable, accredited data centre to store your data
- making sure our staff contractors are security-cleared and vetted
- encrypt our services and data
- review our processes and activities regularly
- restrict access only to authorised employees
- have our service checked regularly by an independent security company
- offering you and the Service Providers who use our services the use of two-factor or two-step verification to protect against compromised account reuse.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your personal data transmitted to myaccount. Any transmission is at your own risk.

Once we receive your data, we use strict procedures and security features as outlined above to try to prevent unauthorised access to your personal data.

As above, we cannot be held responsible for the security of your personal data held by a third party or Service Provider you consent to share data with. Such third parties shall have their own privacy notices.

Where do we store your data?

All personal data you provide to us is stored on secure servers in the UK. Your personal data will not be passed outside the EEA. Please note that we cannot be held responsible for the location of any personal data held by a third party or Service Provider if you consent to us sharing this personal data with such third party for the purposes set out in this notice e.g. to enrol with a service. Third parties have their own privacy notices and you should read them carefully.

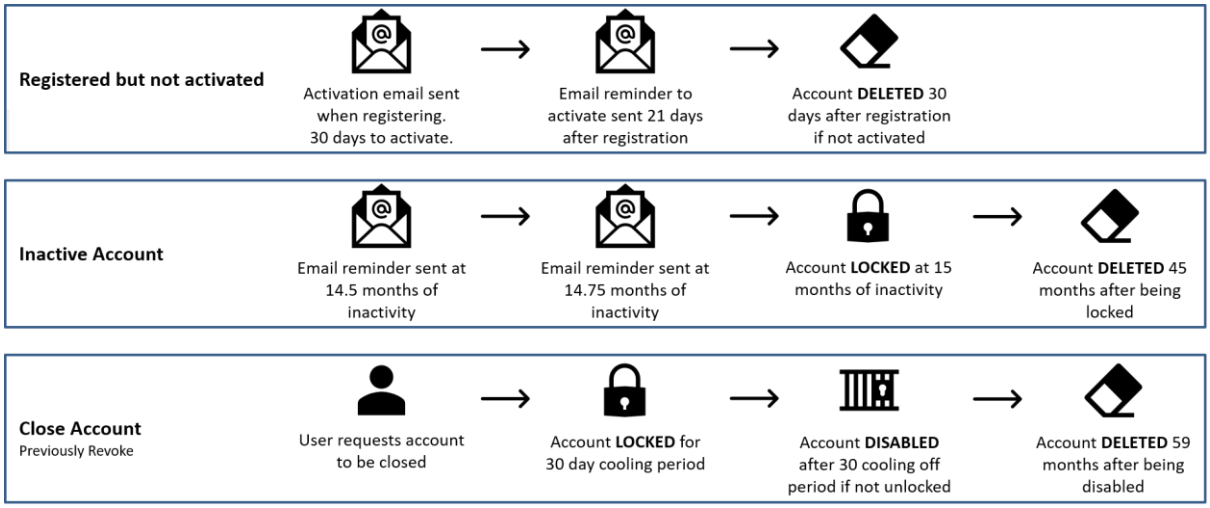
How long do we store your data?

We will keep your data for as long as you keep your myaccount active. Your myaccount will automatically be locked after 15 months of non-use. Your data will be held for a further 45 months before being deleted.

We keep a record of successful and unsuccessful logins for audit purposes. We retain this information for a period of two years.

If you decide to voluntarily close your account, you can do so by logging on to your account and choosing the close option. Your account will be locked for a 30 day "cooling off period", in case you change your mind. After the 30 days your account will be disabled. Your data held for 60 months before being deleted.

The image below summaries how long we will store your data for. It also states when we will contact you to advise you when we will lock or delete your account.



Third Parties

We will disclose data we process about you to the following third parties for the following purposes:

Category of Data	Recipient	Purpose
When you register for an account	Service Provider when you log in	To help the Service Provider give the service to the right person
When you raise a query about a service	Service Provider	To help with any queries in relation to the service
When you verify your identity	Agent in Local Authority or Health Board or external identity verification sources	To help you create a verified account
When you use the myaccount service	Service Provider when you log in	To help the Service Provider give you the correct service.
We collect about you from other sources	Any Service Provider you log in to	To verify who you are and help the Service Provider give you the correct service.

We may have a duty to disclose or share your data to comply with any legal or regulatory obligations or requests. They would be for the following reasons:

- To enforce or apply the Terms of Use, and other agreements you have agreed to with us.
- To investigate potential breaches.
- To protect the rights, property or safety of our you or others. Including exchanging information with other companies for fraud protection.

Third Party Links

Our website may contain links to third parties such as Local Authorities or Health Boards. These websites have their own privacy notices that we do not accept any responsibility or liability for, including any personal data collected through these websites or services. Please check these notices before you submit any personal data to these websites or use these services.

Cookies

The myaccount service uses cookies (small text files that we place on your device) to help provide our services to you and keep your account safe. For more information, please read our Cookie Policy.

reCAPTCHA

Our website uses reCAPTCHA. This service is provided by Google Inc. (Google). It helps protect our website from spam by using tools that can confirm you are a human rather than a machine.

Your entry in the reCAPTCHA field will be sent to Google in the USA and processed by Google for this purpose. The reCAPTCHA application will also send your IP address and other data to Google to enable it to provide the reCAPTCHA service. By using reCAPTCHA, you agree to Google processing your data for this purpose. The IP address provided as part of Google reCAPTCHA will not be merged with other Google data.

For more information about Google's Terms of Use and Privacy for reCAPTCHA here.

Updates

Version 3.4

Why did we change the Privacy Notice?
We're improving our Notices 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 Privacy Notice 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 Privacy Notice.
In this archive you can see versions of our Privacy Notices.

Version 3.3

Contact

Questions, comments and requests regarding this privacy notice are welcomed. For more information about how to contact myaccount please visit our website

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.