Privacy Notice

Last updated: 31st August, 2022

1. It is all about data privacy

Your data belongs to you. We believe it is safer for people and better for businesses for you to control your data. Self enables you to allow others to use your personal data only for specific reasons and you remain in control of that.

Current Regulations, such as GDPR are a good start, but we think they don't go far enough. No company needs to keep your data, especially if they use Self. We believe in only holding data we have to hold*, and being clear as to the specific purpose of holding that data. Our privacy policy governs what personal information of yours we hold, why we hold it and how we use it.

**We would hold no personal data at all if we could get away with it.*

2. So, What is Self?

Self consists of the "App" (which you have just downloaded) and a "Network" across which "Members" (you and other users of the App) can share verified information securely. The App gives you access to the Network and lets you verify, share and control the use of the personal data "Facts" you store in it. The App lets you use Facts about yourself to make your everyday interactions with people and businesses you trust easier and safer.

As well as using Self to protect your data and your rights to privacy; you can use the App to replace logins, account numbers and other identifying information with third parties who support Self, including businesses and other organisations.

Your Membership is unique to you and the data you store in Self exists only on your phone under your control unless you choose to share it. It is never shared with or visible to us other than with your explicit consent and under your control as set out below. When you do share data, you determine who it is shared with.

Sharing data through Self is free to you as an individual user; we will however charge businesses and organisations for requesting data from you or for checking your Membership. In the future we may release new features, which may carry a charge, but these will always be optional. This privacy notice explains how your data is used inside the Self App and in the limited cases where it is used or stored by Self Group, how your data is used and protected.

3. Joining Self

Once you have installed the App it will take you through becoming a Self Member. You will be asked to provide some verifiable information like a phone number and taken through setting up backup and account recovery processes. These are crucial to your being able to use Self safely, without them you cannot recover an account.

The App lets you take advantage of the uniqueness of the things you do to secure your account. It is a tool that lets you check yourself, so the App needs access to things like your location and notifications to be sure that your account is safe. For the best experience, Please read the reasons for any permission requests the app makes in order to function.

4. Data Collection and Use

We enable you to verify personal information which you can then share from the Self App on your phone. To do this we have to collect some information which we store temporarily during verification and two pieces of information which we keep permanently (or until you replace them); your email and your mobile phone number. We do this for several reasons:

- To check if you already have an account.
- To create your account
- To verify that a document you add to your account is yours.
- To check you are the correct living, specific person.
- For authentication.
- To be able to contact you outside of Self in case of problems with Self or your account.

5. What Data Do We Collect?

A Photo of you. We capture an image of you during the registration process. This image is stored on your phone encrypted with keys only you hold.

- The image is taken from Video captured to confirm you are a real, live human. During the recording of the video you will be asked to perform various actions. Once the liveness check has been passed the image is captured and the video is deleted.
- The image we capture is encrypted and kept on your device in the App. When you need to biometrically verify yourself - for example during a login - the image is used to compare you with an image captured from your passport to verify you are both who you say you are and the person the account being accessed was given to. This comparison is done by sending the images to an external service where they are stored only while they are being processed and then deleted.
- The image is never shared with a third party except during the automated process of verification.
- The image is never linked to any other personal data.
- You keep this image on your phone until you delete your account.

Further photos of you. Every time you use the Self App to verify your identity you capture another photograph. These images are all stored in the app in encrypted form until your account is deleted. Apart from during the verification process for which they were created, they cannot be shared. Over time these images will be used to train an on-device model which can be used to recognise you. This will remove the need for sending images to an external service for comparison.

Your email address. We capture your email address, if you ask us to verify it, so that we have a means of communication with you outside of Self should it be necessary. This will only be used for support purposes where Self cannot be used. In hashed form your email address(es) are also used by you for discovery of other people who you know in Self. Existing Self users who hold each other's contact details in their device address books and who permit access to their contacts are able to see each other as Self users.

Your mobile phone number. Your phone number is used to check you do not already have an account as multiple accounts in Self are not allowed or necessary. The number is stored as a hash and cannot be used to contact you, nor can it be shared. In hashed form your phone number is also used by you for discovery of other people who you know in Self. Existing Self users who hold each other's contact details in their device address books and who permit access to their contacts are able to see each other as Self users.

6. Data Location and Security

The personal data we hold is stored securely in data centres in the UK. All data is encrypted. We hold no personal information other than that stated in Section 5.

7. Your Rights

Self holds only two pieces of personally identifiable data on any user. you have the right to correct, delete and restrict us from using the data we hold all of which you can do from within your Self App.

8. Using the Self App to store and verify Data

Once you have joined the Self Network and logged in to the App there will be a section marked Profile. This is for you to use to store Facts about yourself. Facts you added to Self during sign up will be displayed there and if they have been verified as being true by an authoritative third party they will be marked with a ticked shield.

The Facts only exist in your App (and in your encrypted device backup in iCloud or Google Cloud); they are verified bits of personal data which another Member has confirmed are true. You can add Facts to the App and ask Members you are connected to (both organisations and individuals) to verify those Facts are true. Organisations you are connected to can add custom fields to your profile to share relationship specific Facts to - like Account numbers and preferences.

You can add additional Facts about yourself and ask for them to be verified. This might include e-mail or physical addresses, your full name, details of your employer or the details from an official document like a passport or driving licence. Through the App you can share Facts about yourself with Members you are connected to. Even though you have chosen to be connected to another Member, you should be careful about the Facts that you share and the purpose that you are sharing them for. Your Facts are valuable and you should avoid giving them away without a good reason.

Requestors can ask to have access to a fact for a defined period of time if they are doing something that requires repeated access to the fact. This saves them storing your data while ensuring they have access to it if it is needed. You can revoke this access at any time.

The App contains a list of the Members you are connected to and the Facts you have shared with each one. The App also lets you check and manage all your sharing. We do not have access to any of the facts you store in your Self App other than those set out in Section 5.

9. App Recovery

As part of joining Self, we will provide you with a recovery key. You will need the recovery key if you ever lose access to the App for any reason (including if you lose the phone or other device containing your Self ID), so it is very important that you make a copy of this key and store it safely and securely and not on your phone.

10. Biometrics and PIN

You should only access the App using a device-based biometric check like a fingerprint or face scan. You will also be asked to create a 6 digit PIN for accessing the App in emergency, but it will only give you access to limited functionality. You must make sure no one else has access to your PIN, so it stays safe and private. The pin can be changed in settings, but you may be required to perform a biometric check to make the change. In addition to the Biometric checks done by the device, the App may use image capture and verification as set out in Section 5 to determine if the Member accessing the App is the correct Member.

11. Which Biometrics does the App Use?

- **Facial.** The images we capture of your face allow us to determine if the person using the App is the correct person. Some actions you want to take while using the app will require you to take a photo and liveness check to confirm you match the biometrics taken when you set up the account.
- **Liveness.** We use a range of technologies to check that the person claiming to be you is not an imposter, this could be using video, AI or other background information. These checks are done on the phone and are automated. Self Group has no access to the checks or their output, they are designed for you to use in your Self App to strengthen your ID security.

12. Encryption and Data Backup

All data stored in your App will be encrypted on your mobile in the App. Any data being shared is encrypted end-to-end. Backups of your data and membership details will be stored encrypted in the cloud drive nominated by you during the joining process. It is your responsibility to keep your phone, login details and recovery details safe, and to prevent others from having unauthorised access to your membership details.

13. Data that helps us fix problems you experience

We use Crashlytics which sends us information automatically if the app has problems or crashes. None of the information they gather allows us or anyone else to identify you. They delete all data after 90 days. If an issue is persistent we may ask you to share some information which will help us identify the specific session you are having difficulty with. This information will be requested through the support portal only and will only identify you by your Self user ID. Once the problems have been resolved the data will be deleted and you will be notified that it has been deleted.

14. If you no longer want a Self Membership

You can delete the App and your account at any time by choosing "delete account" from the Settings menu. Doing so will remove all your data from your phone and from backups. Once your App has been deleted, your Member details can be recovered, but your data will no longer be available.

15. General legal points

If you have a complaint regarding the service or you wish to exercise your privacy rights, please contact us by emailing our support team or through the support portal in the Self App. We will handle all complaints about data privacy within one month.

If you would like to contact the regulator local to you, you will find a list of them here https://globalprivacyassembly.org/participation-in-the-assembly/members-online/. As a UK Company, Self Group is registered with and regulated by the UK Information Commissioner's Office (ICO) https://ico.org.uk/global/contact-us/

The service is provided by Self Group Limited, a company registered in England with number 11855548 and whose address is at Harwood House, 43 Harwood Road, London

SW6 4QP UK. References to “we”, “us” and “our” in this notice shall be understood to be references to the company.