Privacy Statement

Introduction

Atlantic Data Ltd (“we”, “us” and “our”) refers to the owner of this mobile application, whose registered office is at Atlantic House, 7 Davy Avenue, Knowlhill, Milton Keynes, MK5 8HJ and whose registered company number is 04085856, ICO registration (Z5622273).

We are committed to protecting and respecting the privacy of our clients, mobile application visitors to Atlantic Data Digital ID and any sub-domains of these mobile applications (“the applications”), service users and applicants.

This Privacy Statement, together with our Cookies Policy and Mobile Application Terms of Use, explain how and why we collect personal information from you and what we do with it. By using the applications and services, you are agreeing to comply with and be bound by the terms of this Statement and our Mobile Application Terms of Use. If you disagree with any part of these terms, please do not use the applications and/or services.

We reserve the right to revise this Privacy Statement or any part of it from time to time. We will not process your data for any new purpose without first obtaining your consent.

Collection of personal information

We collect and process the following information:

- information provided by you when using Digital ID service using the applications
- information provided by you when reporting any fault with our services or mobile application, or complaints relating to our services or application
- information provided by you in any correspondence between you and us including by way of telephone
- information provided by you in response to any survey from us (although there is no obligation on you to complete any survey)
- information provided by you in order to allow us to provide the service which you have requested and for which you have agreed to our terms and conditions relating to such service.

Collection of information through the Mobile App

We may collect information about you whilst you use the applications, this includes whilst you and/or we:

- create your account and provide the products/services
- check you don't already have an account
- check the document you add is genuine and the photo matches your account set-up photo
- check you're a real live person
- verify your details
- check for identity fraud
- authenticate you when you make certain requests, such as to delete your account.

Information we collect

What we collect	Why
Mobile Number	We use your mobile telephone number to create your account in the applications. We will send a text message with a verification passcode to your telephone number. Access to the applications is exclusive to the registered phone.
Photo	We store your photograph against your profile for comparison against the documents you will be providing. This is to ensure that the documents belong to you.
3D Liveness Scan	We use 3D Liveness Scan to measure and make sure you are a real person when you set up your account. This also ensures that the account is not being created by an imposter. We will also use your face biometric scan when you want to share your information with your employer ensuring that only you are sharing your Digital Information. We also use a 3D Liveness Scan for restoring your account should you lose your mobile phone or need to reinstall the applications. This is to verify that you are the one re-installing the applications.
Personal Information	We collect your name, date of birth, photograph and address from the documents you provide.
Address	We use the services of Equifax to verify your address. This will leave a footprint on your credit file, but only as a 'soft' identity search, which will not affect your credit score.
Passport Information	We collect the information on your passport through OCR and NFC scanning of your passport and the biometric chip. We compare and cross check the information to ensure that the passport belongs to you and is a genuine passport issued by the government.
UK Driving Licence	We may collect your driving licence as an additional document if required (when the chip in your passport does not work). This is required in order to meet the confidence level in your identity by collecting additional information.
UK Visa/Work Permit	We may collect your UK visa/work permit as an additional document if required. This is required in order to meet the confidence level in your identity by collecting additional information.
PASS Proof of Age Card	We may collect your PASS Proof of Age Card as an additional

	document if required. This is required in order to meet the confidence level in your identity by collecting additional information.
Proof of Address Documentation	We may collect your proof of address documentation if required. This is required in order to meet the confidence level in your identity by collecting additional information.
Fraud checks	We check the information in your documents against the Fraud Prevention database. The results of this check, if positive will result in a failure to issue your Digital Identity.

Delete a Digital ID

If you want to delete your Digital ID this can be initiated from within the App. You will be able to select the ID you wish to delete and will then be prompted to enter your 4 digit pass code to confirm deletion.

For any document or device issues whilst using the App please refer to our Digital ID Support area at: https://www.addid.co.uk/index.php/support/

Sharing information with third parties

You sharing information

You will be able to share your Digital Identity information digitally with third parties using the Atlantic Data Digital ID app.

You are in control at all times and can decide whether you want to use the applications to share your information with a recruiting organisation. A request for Digital Identity information from a recruiting organisation will be in the form of a QR code which is necessary to share your information.

You will need to scan the QR code using the applications and will be asked to scan your face to ensure that it is you who is sharing the information.

Please note that you can only share information with recruiting organisations using the Atlantic Data Digital ID Service who will present you with a QR code.

Atlantic Data sharing information

We only share information with third parties when we are proving your identity. The complete list of information we share is provided below. We do not mine your data, we do not sell your data and we do not use your data for marketing purposes.

We use third party providers to carry out comprehensive background checks.

What we share	**With Whom**
Mobile Number	We share your mobile telephone number with: ▪ Equifax - a credit reference agency ▪ Synectics - National SIRA Fraud Prevention Service

	As part of verifying your identity information.
Photo	We will share your photo with your recruiting organisation if they have asked us to carry out a check using our Right to Work (RTW) service.
3D Liveness scan	We do not share your 3D Liveness scan with anyone.
Personal Information	We share your name, date of birth, and address with: ▪ Equifax - a credit reference agency ▪ Synectics - National SIRA Fraud Prevention Service As part of verifying your identity information. We also share your personal information this with your recruiting organisation when you share your Digital ID as part of a Disclosure Barring Service (DBS) and/or Right to Work (RTW) check.
Passport Information	We share your passport information with your recruiting organisation when you share your Digital ID as part of a DBS and/or RTW check.
UK Driving Licence	We share your UK Driving Licence information with your recruiting organisation when you share your Digital ID as part of a Disclosure Barring Service (DBS) check.

Sharing information about suspected or confirmed identity fraud

Typically, only you have right to choose when to and with whom to share your information. In the certain circumstances we must share your information with third parties:

Circumstances	**Who we share your data with**
In case of false document presented	We may pass a copy of your information or an image of the false document to the Fraud Prevention System. If, after investigation, we determine that there has been fraud that meets the criteria for reporting to the Fraud Prevention System, we will pass on the details to prevent further fraud and money laundering.

Sharing information in the event of technical issues or the need for troubleshooting.

In the certain circumstances we must share your information Internally:

Circumstances	**Who we share your data with**
Technical Support and Troubleshooting	In the event of technical issues or the need for troubleshooting, we may provide our development team with a copy of your information or an image to facilitate the assessment and resolution of the problem.

Fraud Prevention System

The personal information we have collected from you will be shared with fraud prevention agencies who will use it to prevent fraud and money laundering and to verify your identity. If fraud is detected, you could be refused certain services, finance, or employment.

Further details about how your information will be used by these fraud prevention agencies, and your data protection rights, can be found at: https://www.synectics-solutions.com/privacy-policy

Equifax

Equifax uses your personal data to provide services to Atlantic Data Ltd. for verifying the personal information that you have provided. To find out more about the Equifax privacy policy visit: https://www.equifax.co.uk/About-us/Privacy_policy.html

Synectics

Synectics uses your personal data to provide services to Atlantic Data. These services include identity verification services. To find out more about the Synectics privacy policy please visit: https://www.synectics-solutions.com/privacy-policy

Security during sharing

The information we collect from you is always encrypted in transit and stored separately and encrypted in secure locations. We continually test the applications to ensure that we are compliant and to ensure that we follow industry standards for information security.

External audits are carried out to check that our security controls are compliant. We follow internationally recognised standards for best practice in security such as ISO 27001: 2022 and BS25999.

We keep all the personal information you add to the applications in the UK in our highly secure data centre. All the information is held separately and encrypted.

How do we store your data?

We maintain a dedicated data centre on our premises. All systems are controlled, run and maintained in-house from a secure location.

We place great importance on the security of all information provided to us. We have security measures in place to protect against the loss, misuse and alteration of data under our control. For example, our security and privacy policies are periodically reviewed and enhanced as necessary and only limited, authorised personnel have access to personal information.

With regard to the applications, we use secure server software (SSL) to encrypt the information input by you before it reaches us. In addition, those authorised personnel who have access to your information are trained with regards to maintenance and security of this information. While we cannot guarantee that loss, misuse or alteration of data will not occur, we will always have strict measures in place to try to prevent this.

We are ISO 27001 certified and BS25999 compliant. We will always comply with our obligations in accordance with data protection legislation.

Biometrics

The applications include face biometric information to store and verify your identity. It works by

allowing you to set up a trusted, genuine and verified digital identity. The biometrics are a key part of making sure we keep out fake identities and documents. The biometrics also make sure that it really is you taking actions in the applications.

Essentially, our use of biometrics to identify or authenticate you is to prevent fraudulent use of the applications and to protect your data.

3D Liveness checks

When you take certain actions in the applications and if we need to check if it's really you. We will ask you to take a photo or take actions like moving closer to the camera. We also check that the image is of the real person.

Checking you're a real person

When your account is being setup, creating a Digital ID or taking certain other actions in the applications we need to make sure that it is you and not someone pretending to be you. We use technologies like 3D Liveness Scan for these checks.

How long do we retain your data for?

We do not keep your Digital ID information for any longer than necessary. Your account will be maintained whilst it is active. Once you decide to discontinue or delete your account on the Atlantic Data Digital ID app, your personal information including any photos, videos, ID documents and biometric information will be deleted from our systems.

The data relating transactions which have been carried out using the Atlantic Data Digital ID app will be retained for 1 year from the time of discontinuation.

Lawful basis for processing

Under the UK General Data Protection Regulation (UK GDPR), the lawful basis we rely on for processing this information is your consent. You can remove your consent at any time.

You can do this by contacting legal@atlanticdata.co.uk

Access to your information

Data protection legislation provides you with certain rights in relation to the information we process, in particular the right to access to a copy of the information we hold about you.

These rights are regarding the information we hold about you:

- your right of access - you have the right to ask us for copies of your personal information
- your right to rectification - you have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete
- your right to erasure - you have the right to ask us to erase your personal information in certain circumstances
- your right to restriction of processing - you have the right to ask us to restrict the processing of your personal information in certain circumstances
- your right to object to processing - you have the right to object to the processing of your personal information in certain circumstances
- you are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you

To request a copy of this information or for more information as to your rights, please address these to:

dpo@atlanticdata.co.uk with “**Subject Access Rights**” in the subject.

How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us at:

Data Protection Officer Atlantic House 7 Davy Avenue Knowlhill
Milton Keynes Buckinghamshire MK5 8HJ

Email Address: dpo@atlanticdata.co.uk

You can also complain to the ICO if you are unhappy with how we have used your data. The ICO's address:

Information Commissioner's Office Wycliffe House Water Lane
Wilmslow Cheshire SK9 5AF

Helpline number: 0303 123 1113 ICO website: https://www.ico.org.uk

Contact

Should you have any queries or comments relating to this Privacy Statement please address these to:

legal@atlanticdata.co.uk with “**Privacy Statement Enquiry**” in the subject.