



DIGITAL FUTURES – PRIVACY POLICY

CONTENTS

1. Introduction
2. About Digital Futures and this Privacy Policy
3. The Data we collect about you
4. Consequences of an Omission to provide Personal Data
5. Methods of Data Collection
6. Usage of your Personal Data
7. Purposes for Data Usage
8. The Athena Platform
9. Marketing
10. Mobile Communications
11. Cookies
12. Change of Purpose
13. Disclosures
14. International Transfers
15. Your Legal Rights
16. Fees
17. Identity Confirmation for Data Access
18. Policy Review
19. Glossary

1. Introduction

1.1 Digital Futures Group Limited respects your privacy and is committed to protecting your personal data. This Privacy Policy contains information pertaining to the way in which your personal data is processed and taken care of when you visit our website (regardless of your access location), when you use our Athena AI skills assessment platform, and pertaining to your privacy rights under the law.

1.2 For a smooth consultation of this policy, you can click through to the specific areas set out above or, alternatively, you can request a PDF version. Please note that the meaning of some of the terms used in this Privacy Policy is defined within the Glossary.

2. About Digital Futures and this Privacy Policy

2.1 Purpose

The purpose of this Privacy Policy is to provide you with information on how Digital Futures Group Limited collects and processes your personal data through your use of this website and our Athena platform. This website is not intended for access by children and we do not knowingly collect data relating to children.

We recommend that you read this Privacy Policy together with any other privacy policy or fair processing policy we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This Privacy Policy supplements other notices and privacy policies and is not intended to override them.

2.2 Controller

Digital Futures Group Limited is the controller and responsible for your personal data (collectively referred to as "we", "us" or "our" in this Privacy Policy). Where we provide the Athena platform to a client organisation on your behalf, we act as Data Processor and the client organisation is the Data Controller. Please see Section 8 for further details.

2.3 Data Privacy Officer

We have appointed a Data Privacy Officer (DPO) who is responsible for overseeing the way in which data is processed and who will be the person you may need to contact should you have any questions, including any requests to exercise your legal rights, according to this Privacy Policy.

DPO's contact details are as follows:

Full name: Matt Hayday

Email address: dpo@digitalfutures.com

Postal address: Worship Square, 65 Clifton Street, London, EC2A 4JE

ICO Registration Number: ZB792993

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

2.4 Variation procedure

This Privacy Policy is kept under regular review and, in order to ensure that your personal data currently processed by us is accurate and up to date, please keep us informed in a timely manner of any personal data changes during your relationship with us.

2.5 Third-party links

This website may include links to third-party websites, plug-ins and applications that may allow third parties to collect or share data about you.

We encourage you, after clicking on those links, to read the privacy policy of every website you visit as we do not control these third-party websites and we are not responsible for their privacy statements.

3. The Data we collect about you

3.1 Personal data means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

3.2 We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

3.2.1 Identity Data may include first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.

3.2.2 Contact Data may include postal address, email address, billing address, delivery address and telephone numbers.

3.2.3 Financial Data may include bank account details, payment cards and/or other payment methods details.

3.2.4 Transaction Data may include details about payments to and from you and other details of services rendered or products offered by us to you or vice versa.

3.2.5 Technical Data may include internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access our website.

3.2.6 Profile Data may include your username and password, your interests, preferences, feedback and survey responses.

3.2.7 Usage Data may include information about the way in which you use our website, products and services.

3.2.8 Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.

3.2.9 Aggregated Data means and may include statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Privacy Policy.

3.2.10 Athena Platform Data may include, where you access Athena through your employer, your company role, seniority level, team, department, employee start date, learning pathway assignment, and skills assessment results. Please see Section 8 for full details of personal data processed through the Athena platform.

4. Consequences of an Omission to provide Personal Data

We may need to collect your personal data by law, or under the terms of a contract we have with you, and in this case, should you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you. As a consequence, we may have to suspend or cancel the contract you have with us, but we will use our best endeavours to provide you with a timely notification if this is the case at the time.

5. Methods of Data Collection

5.1 We use different methods to collect data from and about you, including through:

5.1.1 Direct interactions: filling your data in forms, corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- (a) request or apply for our services;
- (b) create an account on our website;
- (c) subscribe to any of our services;
- (d) request marketing to be sent to you;
- (e) give us feedback or contact us.

5.1.2 Automated technologies or interactions: automatic collection of Technical Data about your equipment, browsing actions and patterns. Please note that this personal data is processed by using cookies and other similar technologies and that we may also receive Technical Data about you if you visit other websites employing our cookies. Please see our Cookie Policy (<https://digitalfutures.com/cookie-policy/>) for further details.

5.1.3 Third parties or publicly available sources: we may receive personal data about you from various third parties and public sources including analytics providers (such as Google Analytics), advertising networks, and search information providers.

5.1.4 Client organisations: where you are an employee of an organisation that engages Digital Futures to provide the Athena platform, we may receive personal data about you from your employer. Please see Section 8 for further details.

6. Usage of your Personal Data

6.1 We will only use your personal data according to the law. Most commonly, we will use your personal data in the following circumstances:

6.1.1 where we need to perform the contract we are about to enter into or have entered into with you;

6.1.2 where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests; and

6.1.3 where we need to comply with a legal obligation.

6.2 Generally, we do not rely on consent as a legal basis for processing your personal data through our website, although we will get your consent before sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us. Please request a copy of our Data Protection Policy for further details on how we use your personal data.

7. Purposes for Data Usage

7.1 The following table provides a description of the ways in which we will most commonly use your personal data, together with each of the legal bases we rely on to do so, identifying the nature of our legitimate interests where appropriate.

7.2 Please note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

| Purpose/Activity | Type of data | Lawful basis for processing including basis of legitimate interest |
|--|--|--|
| To register you as a new client or service provider | (a) Identity (b) Contact | Performance of a contract with you |
| To manage our contractual relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey | (a) Identity (b) Contact (c) Profile (d) Marketing and Communications | (a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to verify how customers use our products or services) |
| To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data) | (a) Identity (b) Contact (c) Technical | (a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) |

| | | |
|--|--|---|
| | | (b) Necessary to comply with a legal obligation |
| To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you | (a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical | Necessary for our legitimate interests (to study how clients use our services, to develop them, to grow our business and to inform our marketing strategy) |
| To use data analytics to improve our website, services, marketing, customer relationships and experiences | (a) Technical (b) Usage | Necessary for our legitimate interests (to define types of clients for our services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy) |
| To make suggestions and recommendations to you about our services | (a) Identity (b) Contact (c) Technical (d) Usage (e) Profile (f) Marketing and Communications | Necessary for our legitimate interests (to develop our services and grow our business) |
| To provide the Athena AI skills assessment and personalised learning pathway platform on behalf of your employer | (a) Identity (b) Athena Platform Data (c) Usage | (a) Performance of a contract (between Digital Futures and your employer) (b) Necessary for our legitimate interests (to generate workforce skills insights for your employer's managers) Note: Digital Futures acts as Data Processor for this activity. Your employer is the Data Controller. Please see Section 8. |

8. The Athena Platform

This section applies specifically to individuals whose personal data is processed through the Athena AI skills assessment and learning platform as part of a corporate engagement facilitated by your employer.

8.1 Athena is an AI-powered skills assessment and personalised learning pathway platform provided by Digital Futures to corporate clients ('Client organisations') to support AI literacy and workforce insights.

8.2 Our Role as Data Processor

8.2.1 Where you access Athena through your employer, your employer is the Data Controller and Digital Futures acts as the Data Processor. This means:

- (a) Your employer determines the purposes and means by which your personal data is processed;
- (b) We process your personal data only on documented instructions from your employer;
- (c) Your employer is responsible for providing you with information about their lawful basis for processing your data; and
- (d) To exercise your data protection rights in relation to Athena data, you should contact your employer's HR or data protection representative in the first instance, or alternatively contact our DPO at dpo@digitalfutures.com.

8.3 Personal Data Collected Through Athena

8.3.1 We process the following personal data provided by your employer for the purpose of delivering Athena services:

| Data Field | Description |
|-----------------------------|--|
| Full Name | Employee's complete legal name |
| Company Email Address | Corporate email address (work email only) |
| Company Role | Job title within the employer organisation |
| Seniority Level | Career level (e.g. Junior, Mid-level, Senior, Lead, Director, Executive) |
| Team Assignment | Direct team within the organisation |
| Department | Organisational department |
| Employee Start Date | Date the employee joined their employer |
| Athena Role | Access level within the Platform (e.g. Admin, Standard User) |
| Learning Pathway Assignment | Assigned personas for pathway specific materials |
| Skill Manager | Name of assigned manager within Athena |

8.3.2 We do not process special category data (as defined in Article 9 UK GDPR) through the Athena platform.

8.4 Purposes of Athena Data Processing

8.4.1 We process Athena personal data for the following purposes:

- (a) AI-powered skills assessment: to evaluate each user's current AI skills and competencies through interactive assessments;
- (b) Personalised learning pathway generation: to create tailored learning journeys based on assessment results and the user's assigned persona;
- (c) Platform access administration: to provide and manage user access to the Athena platform; and
- (d) Workforce skills insights: to generate individual employee and aggregated analytics and insights for the employer regarding skills and development needs.

8.5 Lawful Basis for Athena Processing

8.5.1 Digital Futures processes Athena personal data on the following lawful bases:

- (a) Performance of Contract: processing is necessary for the performance of the contract between Digital Futures and your employer for the delivery of Athena services; and
- (b) Legitimate Interests: we have a legitimate interest in generating workforce skills insights and analytics for your employer, provided this does not override your fundamental rights and freedoms.

8.6 Athena Sub-Processors

8.6.1 We engage the following sub-processors to provide Athena services. All sub-processors operate exclusively within the United Kingdom:

| Sub-Processor | Location | Processing Activity |
|-----------------------------|----------------|---|
| Amazon Web Services (AWS) | United Kingdom | Cloud infrastructure hosting and data storage (UK region only) AI model processing for assessment analysis and insight generation (AWS Bedrock, UK region) |
| Google Cloud Platform (GCP) | United Kingdom | Cloud infrastructure hosting including backups |

| | | |
|---------------|----------------|---|
| Auth0 (Auth0) | United Kingdom | Authentication and access management services |
|---------------|----------------|---|

8.6.2 We remain responsible to the Client Organisation for the performance of our sub-processors in relation to the processing of personal data. We maintain written agreements with all sub-processors that require them to process personal data only in accordance with our documented instructions and in compliance with UK GDPR, and that provide us with appropriate rights of redress where a sub-processor causes or contributes to a breach of this Agreement or applicable data protection law.

8.7 Athena Data Residency

8.7.1 All personal data processed through Athena is stored and processed exclusively within the United Kingdom. Digital Futures shall not transfer Athena personal data outside the UK without prior written consent from the relevant Client organisation and the implementation of appropriate safeguards.

8.8 Athena Data Retention and Deletion

8.8.1 Personal data processed through Athena is retained only for as long as necessary for the purposes for which it was collected, including the provision of services to the Client Organisation and any related legitimate business purposes. In any event, personal data will not be retained for more than seven (7) years after the end of the relevant engagement, unless a longer period is required by applicable law, after which it will be securely deleted.

8.8.2 Upon the Client Organisation's written request, we will securely delete personal data processed through Athena within 90 days of that request, except where we are required or permitted by law, or have ongoing legitimate business needs, to retain certain records for longer.

8.9 Data Sharing with Your Employer

8.9.1 We share your Athena assessment results, learning pathway assignments, and aggregated workforce insights with your employer (the Data Controller). Your employer determines how such data is used within your organisation. For further information about how your employer uses this data, please contact your employer's HR or data protection representative.

9. Marketing

9.1 We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which services and offers may be relevant for you (marketing).

9.2 Marketing communications will be sent to you only if requested and provided you have not opted out of receiving such communications.

9.3 We will not share your personal data with any third party for marketing purposes unless we get your express opt-in consent in advance.

9.4 You can ask us or third parties to stop sending you marketing messages at any time by logging into the website and using the relevant boxes to adjust your marketing preferences or by contacting us at any time.

9.5 Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of training attended, services rendered, warranty registration, service experience or other transactions.

10. Mobile Communications

10.1 By providing your mobile number and expressly opting in, you consent to receiving text message communications from us.

10.2 Your mobile numbers will not be shared with third parties or processed by third parties, unless in accordance with this policy.

10.3 Text message frequency may vary based on the nature of information that is sent to you.

10.4 Standard rates and charges may apply when you receive text messages from us (rates are determined by your service provider) and we shall not be responsible for such rates and charges incurred by you as a result of receiving our text messages.

10.5 You can contact our DPO for any help or to opt out of receiving text message communications from us.

11. Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. Please note that, if you disable or refuse cookies, this website may become inaccessible or not function properly. For more information about this, please refer to our Cookie Policy (<https://digitalfutures.com/cookie-policy/>).

12. Change of Purpose

12.1 We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

12.2 If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

12.3 Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

13. Disclosures

13.1 We may share your personal data with the parties set out above for the purposes set out in the table at Clause 7 as follows:

13.1.1 internal Third Parties as set out in the Glossary;

13.1.2 external Third Parties as set out in the Glossary; or

13.1.3 third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If such a change happens to our business, then the new owners may use your personal data in the same way as set out in this Privacy Policy.

13.2 We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your

personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

14. International Transfers

14.1 We will share your personal data within the Digital Futures Group. We may also share your personal data with employees, contractors and other third parties on a business need to know basis. This may involve transferring your personal data outside the UK.

14.2 Please note that personal data processed through the Athena platform is stored and processed exclusively within the United Kingdom and is not subject to international transfer.

14.3 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

14.4 Your personal data may be transferred outside the UK only if one of the following conditions applies and the corresponding safeguard is implemented:

14.4.1 the UK has issued regulations confirming that the country to which the data is transferred ensures an adequate level of protection for your data rights and freedoms;

14.4.2 appropriate safeguards are in place such as binding corporate rules or standard contractual clauses approved for use in the UK;

14.4.3 the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between you and us and reasons of public interest.

14.5 Please request a copy of our Data Protection Policy for further details on international data transfer.

15. Your Legal Rights

15.1 Under certain circumstances, you have rights under data protection laws in relation to your personal data. Below is an illustrative list of your rights, and if you need more information please contact our DPO:

15.1.1 Request access to your personal data: this enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

15.1.2 Request correction of your personal data: this enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

15.1.3 Request erasure of your personal data: this enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

15.1.4 Object to processing of your personal data: where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may

demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

15.1.5 Request restriction of processing your personal data: this enables you to ask us to suspend the processing of your personal data in the following scenarios:

- (a) if you want us to establish the data's accuracy;
- (b) where our use of the data is unlawful, but you do not want us to erase it;
- (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
- (d) you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.

15.1.6 Request transfer of your personal data to you or to a third party: we will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

15.1.7 Right to withdraw consent: please note that, where we are relying on consent to process your personal data, this right will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain services to you. We will advise you if this is the case at the time you withdraw your consent.

15.2 If you wish to exercise any of the rights set out above, please contact us.

16. Fees

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

17. Identity Confirmation for Data Access

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

18. Policy Review

We will annually review this policy and its procedures to ensure we are in compliance with relevant new or amended laws, regulations or guidance. Additionally, we will regularly monitor compliance with this policy, including by carrying out audits.

19. Glossary

19.1 Lawful basis

19.1.1 Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service and the best and most secure experience. We make sure we consider and balance any potential impact on you (both

positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

19.1.2 Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request or in any other case with your consent before entering into such a contract.

19.1.3 Comply with a legal obligation means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.

19.1.4 Data Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller. Where Digital Futures provides Athena to a client organisation, it acts as Data Processor and the client organisation is the Data Controller.

19.2 Third Parties

19.2.1 Internal Third Parties means other companies in the Digital Futures Group Limited acting as joint controllers or processors and who are based in the UK.

19.2.2 External Third Parties means:

Service providers acting as processors based in the UK who provide IT and system administration services.

Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers based in the UK who provide consultancy, banking, legal, insurance and accounting services.

HM Revenue & Customs, regulators and other authorities acting as processors or joint controllers based in the UK who require reporting of processing activities in certain circumstances.

Athena sub-processors (Amazon Web Services, Google Cloud Platform and Auth0), all based in the United Kingdom and engaged exclusively for the provision of Athena platform services.

Digital Futures Group Limited | Worship Square, 65 Clifton Street, London, EC2A 4JE | dpo@digitalfutures.com | www.digitalfutures.com

This Privacy Policy is governed by the laws of England and Wales and complies with the UK GDPR and Data Protection Act 2018.