

ACS-17 A03

DATA PROTECTION POLICY

WEBSITE AND ONLINE PLATFORMS

Academy Consulting (the 'Company') is committed to being transparent about how it collects and uses any personal data, and to meeting its data protection obligations. This policy sets out the Company's commitment to data protection, and individual rights and obligations in relation to personal data.

References in the text below to "you" mean the user of the website or associated online platforms

This policy applies to the collection of data from you via the Academy Consulting website (www.academy.eu.com) and online platforms.

The Company has appointed Managing Director as the person with overall responsibility for data protection compliance in relation to the personal data. For contact, questions should initially be directed to Quality and Accreditations Manager.

Data Controller: Academy Consulting Solutions, 71 London Road, Sevenoaks, Kent, TN13 1AX.

Definitions

"**Personal data**" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"**Sensitive Personal data**" includes information revealing racial or ethnic origin; political opinions, religious or philosophical beliefs, trade union membership, processing of genetic or biometric data, information concerning health, sexual orientation, or identifying statutory or financial information.

Data Collection

Registration is not required for the use of this website. If you are a visitor, we do not collect any personal information about you except through the use of cookies as described below.

Examples where data collection will occur are:

Email alerts; in order to sign up for email news we will ask for your email address and full name via the online form. We may also ask for other details such as job title, city, country and email preferences. You can unsubscribe at any time and we will keep your details only as long as you are subscribed.

Job applications: as applicable you will be able to register your interest in working for us. (There is an Applicant specific Data protection policy. For contact, questions should initially be directed to Quality and Accreditations Manager.)

Document No:	ACS-17 A03	Document Name:	GDPR – Data Protection Policy Website and Online Platforms
Revision No:	1	Date:	May 2022
Created By:	Andrew Jarrett	Approved By:	<i>Michael Bell</i>

Personal Data use

The data provided by signing up on our website and associated platforms will be used to: -

- To administer and improve the website
- To deal with any requests submitted to us by the contacts page
- To process any job application that you may have submitted via the website
- For statistical and research processes
- To personalise your experience at the website and associated platforms
- To contact you for marketing purposes where you have agreed to this
- To otherwise respond to any requests, queries or comments submitted to us by you

We may need to share your information with our service providers and agents for the above purposes.

Sensitive personal data

Other than for job application purposes we will not ask for or store sensitive personal data.

Disclosure

Academy, may disclose your personal information outside of the company in the following instances

- Where disclosure is necessary to fulfil your requests and involves third parties that Academy has relationship with
- Where explicitly requested by you the site visitor
- As a legal or regulatory requirement including a by a court order
- Where you interact with our social media channels using a publicly available feature

External providers may be asked to assist with IT and support services to operate our website and associated platforms.

Links to other websites

We may link to third party websites that are not governed by this privacy policy. We are not responsible for the content or privacy policies of these third-party websites and /or for third party advertisers and we are not agents for particular websites or advertisers and are not authorised to make representations on their behalf.

Document No:	ACS-17 A03	Document Name:	GDPR – Data Protection Policy Website and Online Platforms
Revision No:	1	Date:	May 2022
Created By:	Andrew Jarrett	Approved By:	<i>Michael Bell</i>

Use of Cookies

Cookies are small text files that are downloaded onto your computer or mobile device when you visit a site to optimise and tailor your site visit and track visitor trends.

The website will use: -

- session cookies that expire at the end of the session and will not have identifiable user information on them
- third party analytics cookies which are created by third parties and stored on a visitor's computer until deletion. They allow the actions of users across the website to be remembered and can be used by third parties to generate reports for example about number and type of visitors.

Changing your settings/disabling cookies

The browser settings can be adjusted to accept or decline cookies. (see www.allaboutcookies.org for more information)

Social media platforms

Academy Consulting has accounts on different social media sites.(ie facebook, Twitter, LinkedIn) In choosing to participate and interact with these accounts we may use the information you disclose in context of this privacy policy and for the same purposes to facilitate services and get in touch with you when you request this. We cannot be held responsible if you share personal information on social media that is subsequently used, misused or appropriated by another user.

Consent

By using the website, you consent to the processing of data about you by Academy, its subsidiaries and third parties.

Changes to the Privacy Statement

The Privacy Policy may change and therefore should be reviewed regularly.

Data protection principles

The Company processes the personal data of Industry Contacts in accordance with the following data protection principles:

- Processes personal data lawfully, fairly and in a transparent manner.
- Collects personal data only for specified, explicit and legitimate purposes.
- Processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

Document No:	ACS-17 A03	Document Name:	GDPR – Data Protection Policy Website and Online Platforms
Revision No:	1	Date:	May 2022
Created By:	Andrew Jarrett	Approved By:	<i>Michael Bell</i>

- Keeps personal data only for the period necessary for processing.
- Adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Company keeps a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Individual rights

As data subjects, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Company will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the Company has failed to comply with his/her data protection rights; and
- whether or not the Company carries out automated decision-making and the logic involved in any such decision-making.

The Company will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise. To make a subject access request, the individual should send the request to Quality and Accreditations Manager.

or use the Company's data subject access request form. In some cases, the Company may need to ask for proof of identification before the request can be processed. The Company will inform the individual if it needs to verify his/her identity and the documents it requires.

The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Company processes large amounts of the individual's data, it may respond within two months of the date the request is received. The Company will write to the individual within two weeks of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be

Document No:	ACS-17 A03	Document Name:	GDPR – Data Protection Policy Website and Online Platforms
Revision No:	1	Date:	May 2022
Created By:	Andrew Jarrett	Approved By:	<i>Michael Bell</i>

manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify him/her that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the Company to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Company's legitimate grounds for processing data.

To ask the Company to take any of these steps, the individual should send the request to the Data Controller and contact Quality and Accreditations Manager.

Data security

The website and associated platforms have security measures in place to protect against the loss, misuse and alteration of personal data under our control.

Where the Company engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

Where the Company considers that processing data in a way that may result in a high risk to individual's rights and freedoms, the Company will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

If the Company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Company will record all data breaches regardless of their effect.

Document No:	ACS-17 A03	Document Name:	GDPR – Data Protection Policy Website and Online Platforms
Revision No:	1	Date:	May 2022
Created By:	Andrew Jarrett	Approved By:	<i>Michael Bell</i>

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

The Company will not transfer personal data to countries outside the EEA.

Document No:	ACS-17 A03	Document Name:	GDPR – Data Protection Policy Website and Online Platforms
Revision No:	1	Date:	May 2022
Created By:	Andrew Jarrett	Approved By:	<i>Michael Bell</i>

GDPR – DATA PROTECTION POLICY

WEBSITE AND ONLINE PLATFORMS

ACS-17 A03

SCHEDULE OF REVISIONS

Revision Number	Date	Description of Change
1	May 2022	Amendment – updated first section Data Controller to from Tunbridge Wells to Sevenoaks address. Amended AJ
0	Aug 2019	New document

Document No:	ACS-17 A03	Document Name:	GDPR – Data Protection Policy Website and Online Platforms
Revision No:	1	Date:	May 2022
Created By:	Andrew Jarrett	Approved By:	<i>Michael Bell</i>