

AMICULUM – Privacy notice

Last updated: March 2022

Contents

1. Introduction
2. Who we are
3. Companies and websites within scope
4. The data we collect about you
5. Collection of personal data
6. Lawful basis for the processing of personal data
7. Disclosure of personal data
8. Storage of personal data
9. Security measures
10. Your rights as a data subject
11. Contact us
12. Complaints

1. Introduction

We appreciate the trust you place in us when sharing your personal data (that is, any information which identifies you, or is otherwise about you). The security of that data is very important to us. In this document, we will explain how we collect, use, and protect your personal data.

We will also explain what rights you have with regard to your personal data and how you can exercise those rights.

2. Who we are

AMICULUM Limited is the parent company for several companies, including Mudskipper Business Limited, Delta Kn Limited and 7.4 Limited. The full list can be found in Section 3 along with their associated websites.

AMICULUM Limited is the data controller for all its subsidiaries and is responsible for everything those companies do with your personal data. This means that AMICULUM Limited decides what data is collected by each company that it owns, how this data is going to be used, and how this data is protected.

Our registered office address is:

AMICULUM Limited

The Boathouse

Clarence Mill

Bollington

East Cheshire

SK10 5JZ

United Kingdom

If you have questions about this privacy notice or our data protection practices, please contact our data privacy team by email at privacy@amiculum.biz.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO). Please see Section 12 'Complaints' for more information.

3. Companies and websites within scope

The data processing activities of the following companies and websites are covered by this privacy notice:

AMICULUM Limited	www.amiculum.biz
AMICULUM Business Services Limited	careers.amiculum.biz
7.4 Limited	www.sevenpointfour.biz
Delta Kn Limited	www.delta-kn.biz
Mudskipper Business Limited	www.mudskipper.biz
As a trading division of AMICULUM Consulting Limited	
AMICULUM Digital	www.amiculum-digital.biz
Evida	www.evida.biz
Cence	www.cence.biz
Cogent	www.cogent.biz
Comradis	www.comradis.biz
Seques	www.seques.biz
AMICULUM Access	www.amiculum-access.biz
As a trading division of AMICULUM Business Services Limited	
Ambit	www.ambit.careers

We consider these websites to be UK-based websites; see Section 8 for more information on non-UK data processing. From time to time, personal data may also be shared with other group entities (including AMICULUM MENA DMCC, Mudskipper Business Consulting [Shanghai] Limited, and AMICULUM New Zealand [an overseas trading division of AMICULUM Consulting Limited]) as needed, and their processing of any such data will also be governed by this notice, as well as the prevailing laws in their own countries.

Our websites may include links to third-party websites, plug-ins, and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control those third-party websites and are not responsible for their privacy statements or practices. When you leave our website, we encourage you to read the privacy notice of every website you visit.

4. The data we collect about you

Personal data means any information about an individual from which that person can be identified, or any information about an identifiable individual. It does not include **anonymous data**, which are data that cannot be connected to an identifiable individual. It is important that the personal data we hold about you are accurate and current. Please keep us informed if the personal data we have collected about you changes during your relationship with us.

There are different types of personal data about you that we might collect, use, store, or transfer. We have grouped these together as follows, and provided some examples of the type of personal data that might fall into each grouping:

- **Identity Data** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth, and gender
- **Contact Data** includes billing address, delivery address, email address, and telephone numbers
- **Financial Data** includes bank account and payment card details
- **Transaction Data** includes details about payments to and from you and other details of products and services you have purchased from us
- **Technical Data** includes your device's 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 this website
- **Profile Data** includes your username and password, purchases or orders made by you, your interests, preferences, feedback, and survey responses
- **Usage Data** includes information about how you use our website, products, and services
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties, and your communication preferences

We may also collect, use, and share Aggregated Data, such as statistical or demographic data, for any purpose. Aggregated Data could be derived from your personal data but are not considered personal data in law as these 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 they can directly or indirectly identify you, we treat the combined data as Personal Data, which will be used in accordance with this privacy policy.

We do not generally collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data). Where we do collect

such data, it will only be processed with your consent or because we have some other proper legal basis for using it. We do not collect any information about criminal convictions and offences, unless required to do so in connection with our employees as a result of a customer requirement.

IF YOU FAIL TO PROVIDE PERSONAL DATA

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, this might mean that we will not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). If that happens, we might have to cancel a product or service you have with us, but we will notify you if this is the case at the time.

5. Collection of personal data

We collect personal data from you for one or more of the following purposes:

1. To provide you with information that you have requested or which we think may be relevant to a subject in which you have demonstrated an interest.
2. To initiate and complete commercial transactions with you, or the entity that you represent, for the purchase of products and/or services.
3. To fulfil a contract that we have entered into with you or with the entity that you represent.
4. If you have applied for a job with us, or in connection with a recruitment exercise.
5. To ensure the security and safe operation of our websites and underlying business infrastructure.
6. To manage any communication between you and us.

The table in Section 6 below provides more detail about the data that we collect for each of these purposes, the lawful basis for doing so, and the period for which we will retain each type of data.

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected them for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you. To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting, or other requirements.

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

- **Direct interactions.** You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
 - Apply for our products or services
 - Apply for a job with us, or are identified by us as a candidate for employment
 - Create an account on our website
 - Subscribe to our service or publications
 - Request marketing to be sent to you, or
 - Give us feedback or contact us
- **Automated technologies or interactions.** As you interact with our website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies (for more information please see below section headed “Technical information”). We may also receive Technical Data about you if you visit other websites employing our cookies. Please see our Cookie Policy (which can be viewed from the home page of each of our websites) for further details
- **Generated Data.** We may generate Transaction, Usage, Marketing and Communications Data about you, by way of records of the direct and automated interactions that you undertake with us or our website
- **Third parties.** We will receive personal data about you from various third parties and public sources as set out below:
 - Technical Data from the following parties:
 - a) Google as an analytics provider
 - b) LinkedIn as a provider of advertising and contact information.
 - Identity and Contact Data from publicly available sources, such as Companies House and the Electoral Register based inside the UK

Technical information

In addition, and in order to ensure that each visitor to any of our websites can use and navigate the site effectively, we collect the following:

- Technical information, including the Internet Protocol (IP) address used to connect your device to the Internet
- Your login information, browser type and version, time zone setting, browser plug-in types and versions
- Operating system and platform
- Information about your visit, including the Uniform Resource Locators (URL) clickstream to, through, and from our site

Our Cookie Policy, which can be viewed from the home page of each of our websites, describes in detail how we use cookies. You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly.

6. Lawful basis for the processing of personal data

The table below describes the various forms of personal data we collect and the lawful basis for processing these data and/or retaining these data, and we have identified our legitimate interests where appropriate. Our business architecture, accounting and systems infrastructure, and compliance organization mean that all personal data are processed on common platforms. We have processes in place to make sure that only those people in our organization who need to access your data can do so. A number of data elements are collected for multiple purposes, as the table below shows. Some data may be shared with third parties and, where this happens, this is also identified below.

When we process on the lawful basis of legitimate interest, we apply the following test to determine whether it is appropriate:

- **The purpose test** – is there a legitimate interest behind the processing?
- **Necessity test** – is the processing necessary for that purpose?
- **Balancing test** – is the legitimate interest overridden, or not, by the individual’s interests, rights, or freedoms?

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 there is more than one ground has been set out in the table below.

Purpose of collection	Information category	Data collected	Purpose for collection	Lawful basis for processing	Data shared with?	Retention period
1. To provide you with information	Subject matter information	Name, company name, geographic location, email address, business	To provide appropriate online or email information about products and services that you have requested	Contractual fulfilment	Internally only	Maximum of 8 years from the date the information is collected. 6 months if a marketing email

		sector	To provide further, related, online or email information and ongoing news updates in relation to the identified area of interest	Legitimate interest	Internally only	is left unopened
		Telephone number	Follow-up to ensure requested information meets needs and identify further requirements	Legitimate interest	Internally only	
		Personal contact information as provided through website forms or at trade shows or any other means	General mailing list subscription	Consent	Internally only	

Purpose of collection	Information category	Data collected	Purpose for collection	Lawful basis for processing	Data shared with?	Retention period
2. Transactional information	Transaction details	Name, physical address, email address, telephone number, bank account details (for credit accounts), other medium of content delivery	<p>To process purchase transactions for products and services with customers, and to ensure any transaction issues can be dealt with</p> <p>For accounting and taxation purposes</p> <p>Documentation should any contractual legal claim arise</p>	<p>Contractual performance</p> <p>Statutory obligation</p> <p>Legitimate Interest</p>	<p>Internally only</p> <p>Internally and professional advisers</p> <p>Internally and professional advisers</p>	<p>Maximum of 8 years from the date of the performance of the contract</p> <p>6 months from the date the data subject has input personal information but has not completed a transaction</p> <p>8 years for VAT records from the performance of the contract</p>

	Payment card data	Primary account number (PAN), cardholder name, service code, expiration date	To fulfil purchase requests using payment cards	Contractual performance	Payment card companies, all in line with the Payment Card Industry Data Security Standard (PCI DSS)	Only retained while authorization is pending
Purpose of collection	Information category	Data collected	Purpose for collection	Lawful basis for processing	Data shared with?	Retention period
3. Fulfilment information	Fulfilment data	Name, dietary requirements	Appropriate catering arrangements for training courses	Contractual performance	Internally and training venues	Maximum of 6 years from the date of the performance of the contract
		Name, contact and identification details	Access to training courses, attendance registers	Contractual performance	Internally and training venues	
		Name, contact and identification details	Exam attendance, exam results and certifications	Contractual performance	Internally and external examiners, proctors and certification bodies	
		Name, contact details	Licensing details necessary for allocation and maintenance of a licence purchased for use of software and related products, distance and e-learning	Contractual performance	Internally and any third parties whose products or services you may have purchased from us	
		Name, address(es), email address, contact details	Actual delivery of products or services, in physical or digital form, that you may have purchased from us	Contractual performance	Internally and any third-party logistics or supplier companies with whom we contract in order to fulfil these requirements	
4. Security	Security information	Technical information, as described above, plus any other information that may be required for	To protect our websites and infrastructure from cyber-attack or other threats, and to report and deal with any illegal acts	Legitimate interest	Internally, and forensic and other organizations with whom we might contract for this purpose	Relevant statutes of limitation

Purpose of collection	Information category	Data collected	Purpose for collection	Lawful basis for processing	Data shared with?	Retention period
5. Communications	Contact information	Names, contact details, identification details	To communicate with you about any issue that you raise with us, or which follows from an interaction between us	Legitimate interest	Internally and, as necessary, with professional advisers	Relevant statutes of limitation

7. Disclosure of personal data

We may share your personal data with a range of third parties for the purposes set out in the table above. If you require a list of these, please contact our data privacy team by email at privacy@amiculum.biz.

We may also share some limited personal data with 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 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.

We require all third parties to respect the security of your personal data and to treat them 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.

8. Storage of personal data

AMICULUM Limited is a UK-domiciled organization whose primary offices are in the UK. We have offices and staff based in Europe and share information between them and with our UK business under the reciprocal adequacy arrangements which exist between those states.

The majority of our websites and web applications are hosted within the European Economic Area (EEA) and are accessed only by our EEA-based staff. We shall keep developments in relation to the data sharing framework between the UK and Europe under review to ensure that there are no national or EU laws in

place in other member states that would affect the transfer of your personal data between the UK and any relevant member state.

Our customer relationship management, marketing, and accounting systems for all our businesses are either based in the UK or EEA; hosted by companies with operations in the UK or EEA; or supplied by providers based in the USA. Where we use providers based in the USA, we may transfer data to them provided that we adopt appropriate transfer safeguards in accordance with the requirements of the UK GDPR, EU GDPR or other applicable data protection legislation. Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

We use a wide range of Cloud Service Providers (CSPs) as part of our processing environment. Unless we specifically state otherwise:

- We are, in respect of all these CSPs, the data controller
- All the CSPs that we use either utilize data processing facilities located in the UK or the EEA or, where processing in another location is necessary, are subject to appropriate controls and safeguards as required by Chapter V of the UK or EU GDPR.

Our payment processors and banking arrangements are based in the UK or the EEA and, for our US payments, in the USA.

We ship and deliver physical products around the world; we therefore use logistics companies that are based outside the UK or the EEA and operate in other countries. We have appropriate legal and security relationships with those partners.

We operate a data retention policy in respect of all data, whether paper-based or digital, and those aspects of it that relate to personal data are contained in the table in Section 6, above.

9. Security measures

We have put in place appropriate security measures to protect personal data. In addition, we limit access to your personal data to those employees, agents, contractors, and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

We have also put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Risk assessment, including assessing risks to the rights and freedoms of data subjects, is at the heart of our information security management system. We do not, however, have any control over what happens between your device and the boundary of our information infrastructure. You should be aware of the many information security risks that exist and take appropriate steps to safeguard your own information. We accept no liability in respect of breaches that occur beyond our sphere of control.

10. Your rights as a data subject

As a data subject whose personal information we hold, you have certain rights. If you wish to exercise any of these rights, please email privacy@amiculum.biz or use the information supplied in the 'Contact us' section below. We try to respond fully to all legitimate requests within 1 month. Occasionally, it could take us longer than 1 month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated. You will not have to pay a fee for access to 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.

In order to process your request, we may ask you to provide up to two valid forms of identification for verification purposes. Your rights are as follows:

The right to be informed

As a data controller, we are obliged to provide clear and transparent information about our data processing activities. This is provided by this privacy notice and any related communications we may send you.

The right of access

You may request a copy of the personal data we hold about you free of charge. Once we have verified your identity and, if relevant, the authority of any third-party requestor, we will provide access to the personal data we hold about you as well as the following information:

- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has been disclosed
- The retention period or envisioned retention period for that personal data
- When personal data has been collected from a third party, the source of the personal data

If there are exceptional circumstances that mean we can refuse to provide the information, we will explain them. If requests are frivolous or vexatious, we reserve the right to refuse them. If answering requests is

likely to require additional time or occasions unreasonable expense (which you may have to meet), we will inform you.

The right to rectification

When you believe we hold inaccurate or incomplete personal information about you, you may exercise your right to correct or complete this data. This may be used with the right to restrict processing to make sure that incorrect/incomplete information is not processed until it is corrected.

The right to erasure (the 'right to be forgotten')

Where no overriding legal basis or legitimate reason continues to exist for processing your personal data, you may request that we delete that personal data. This includes personal data that may have been unlawfully processed. We will take all reasonable steps to ensure erasure, while reserving the right to retain copies of personal data that we are required to maintain by law, or for reasons of good and orderly business administration (for example, we will not delete information which might be required by relevant tax authorities, or information contained within our disaster recovery backups).

The right to restrict processing

You may ask us to stop processing your personal data. We will still hold the data but will not process it any further. This right is an alternative to the right to erasure. If one of the following conditions applies, you may exercise the right to restrict processing:

- a. The accuracy of the personal data is contested
- b. Processing of the personal data is unlawful
- c. We no longer need the personal data for processing, but the personal data is required for part of a legal process
- d. The right to object has been exercised and processing is restricted pending a decision on the status of the processing

The right to data portability

You may request your set of personal data be transferred to another controller or processor, provided in a commonly used and machine-readable format. This right is only available if the original processing was on the basis of consent, the processing is by automated means and if the processing is based on the fulfilment of a contractual obligation.

The right to object

You have the right to object to our processing of your data where:

- Processing is based on legitimate interest, and we have no over-riding interest for continuing to process it
- Processing is for the purpose of direct marketing

- Processing is for the purposes of scientific or historic research
- Processing involves automated decision-making and profiling

11. Contact us

Any comments, questions or suggestions about this privacy policy or our handling of your personal data should be emailed to privacy@amiculum.biz.

Alternatively, you can contact us at the following postal address:

Privacy Officer

AMICULUM Limited

The Boathouse

Clarence Mill

Bollington

East Cheshire

SK10 5JZ

United Kingdom

12. Complaints

Should you wish to discuss a complaint, please feel free to contact us using the details provided above. All complaints will be treated in a confidential manner.

Should you feel unsatisfied with our handling of your data, or about any complaint that you have made to us about our handling of your data, you are entitled to escalate your complaint to a supervisory authority within the UK or the EEA. For the UK, this is the Information Commissioner's Office (ICO), who is also our lead supervisory authority. Contact information can be found at ico.org.uk/global/contact-us.

