



Privacy & Cookie Policy

Version: 1.1.2

Last Updated: 19-Aug-2026

Information Classification: Public

Contents

1.	Definitions	3
2.	Introduction	3
3.	Who we are and who is responsible for Personal Data	3
4.	An introduction to UK data protection laws	4
5.	Special Category Data	4
6.	The legal basis for processing Personal Data	5
7.	What type of Personal Data do we collect	5
8.	Where do we collect Personal Data from	6
9.	How do we use Personal Data	7
10.	Marketing communications	8
11.	Automated decision-making.....	8
12.	Who do we share Personal Data with.....	8
13.	How long do we keep Personal Data.....	9
14.	How do we protect Personal Data	10
15.	Where do we store and process Personal Data	10
16.	Your legal rights	10
17.	Letting us know if your Personal Data is incorrect.....	11
18.	Links to third-party websites	11
19.	Children's Personal Data	12
20.	Cookie Policy	12
21.	Where to find further information on UK data protection laws	12
22.	Changes to this Privacy & Cookie Policy	13
23.	How to make a complaint.....	13
24.	How to contact us	13

1. Definitions

For the purposes of this Privacy & Cookie Policy the following definitions apply:

Expression	What it means
“Cyserri Cyber”, “Cyserri”, “we”, “us”, “our”	Cyserri Cyber Limited, registered in England and Wales with Company number 17392963 and with a registered office at 51 Lime St, London, EC3M 7DQ.
“Data Controller”	A data controller is an entity, such as a company or organisation, that determines what Personal Data to collect, how to collect it, the legal basis for collecting it, where to store it, and how to process it. They bear the ultimate responsibility for protecting the Personal Data they control and ensuring compliance with data protection laws.
“European Economic Area” or “EEA”	All of the countries that are part of the European Union and additionally Iceland, Liechtenstein and Norway.
“Personal Data”	Any information relating to an identifiable living person. This can include direct identifiers like a full name or passport number, or indirect identifiers such as physical location details, online identifiers (e.g. an IP address), or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity. If a piece of information allows you to directly or indirectly identify a living person, even if it needs to be combined with other information, it qualifies as personal data.
“Services”	Products and services we offer.
“Website”	www.cyserri.com and any sub-domains of this site. References to our Website include all the material it contains (e.g. text and images), even if that material is converted into a different format (e.g. printed).
“You”	The person accessing or using our Website or Services.

2. Introduction

Thank you for visiting the website of Cyserri Cyber Limited. We take your privacy very seriously and are committed to complying with all relevant UK data protection laws.

Please read our Privacy & Cookie Policy carefully. It is intended to help you understand who we are, what Personal Data we collect, how we collect it, what we use it for, how we protect it, who we share it with, and your rights under UK data protection laws.

By continuing to use our Website, you confirm that you have read, understood and agree to comply with this Privacy & Cookie Policy. If you do not agree to comply with this Privacy & Cookie Policy, you must stop using our Website.

If you have any questions about our Privacy & Cookie Policy, please contact us using one of the methods shown below in the “How to contact us” section.

3. Who we are and who is responsible for Personal Data

Cyserri Cyber is a limited company registered in England and Wales with Company number 17392963 and with its registered office at 51 Lime St, London, EC3M 7DQ. We are a London-based cyber security consultancy and service provider.

For the purposes of this Privacy & Cookie Policy, Cyserri Cyber is the Data Controller for the Personal Data that you share with us via our website, or that we collect in relation to the provision of our Services. This means that we are responsible for deciding how we use and protect this Personal Data.

We are registered with the Information Commissioner's Office (ICO) as a Data Controller under registration reference number ZC227569.

4. An introduction to UK data protection laws

UK data protection law is primarily governed by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), which together set out rules for how Personal Data can be collected and processed and how individual privacy rights must be protected. The Privacy and Electronic Communications Regulations 2003 (PECR) and the Data (Use and Access) Act 2025 (DUAA) also cover aspects of UK data protection law.

All UK businesses and organisations that use Personal Data have to comply with 'data protection principles' unless an exemption applies (see the ICO's website for further information on these exemptions).

These data protection principles are designed to ensure that Personal Data is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- only collected and processed where it is necessary
- accurate and, where necessary, kept up-to-date
- kept for no longer than is necessary
- handled in a way that ensures Personal Data is secure and protected against unlawful or unauthorised access, modification, processing, damage, destruction or disclosure.

5. Special Category Data

Some types of Personal Data have special status under UK data protection law and can only be collected and used in specific circumstances. These types of personal data are called "Special Category Data". Examples include information revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data when used to uniquely identify a person
- health data
- lifestyle information, including data related to sex life or sexual orientation
- criminal offences.

We will only collect, store and use Special Category Data if one of the following conditions is met:

- you have given us explicit consent
- where this could be established from information you provide to us
- where this is relevant to any service we offer
- where there is any other legal or regulatory justification
- for reasons of substantial public interest
- processing is necessary for the prevention or detection of crime, or acts of dishonesty, malpractice or other improper conduct
- to establish, exercise or defend legal claims.

Where appropriate, we may approach you for your approval to allow us to collect and / or process certain types of Special Category Data. If we do so, we will provide you with details of the information that we require and the reason why we require it. Without this approval, in some circumstances, we may not be able to provide some of our Services.

6. The legal basis for processing Personal Data

UK data protection laws state that when we collect and use Personal Data, we must have a legal basis (i.e. a valid legal reason) for these data processing activities. Examples of a legal basis in this context include:

- to fulfil our contract with you
- when it is in our legitimate interest (see below in this section)
- where you have given us your consent
- to comply with relevant laws and regulations
- when it is in the public interest
- in order to establish, exercise or defend our legal rights or for the purpose of legal proceedings.

The legal basis for processing your Personal Data may differ depending on the nature of our relationship with you.

A “legitimate interest” means that we have a valid business or commercial reason to use your information. Examples of a legitimate interest include:

- enabling us to deliver our Services
- allowing us to manage and administer our business
- managing our relationship with you including communication
- developing and improving our Services and Website
- maintaining compliance with internal policies and procedures
- delivering relevant advertisement content to you
- measuring or understanding the effectiveness of the advertising we use
- to comply with relevant laws and regulations.

When we rely on our legitimate interests for processing your Personal Data, the benefits of doing so must not outweigh your rights, freedoms or interests. You also have the right to object to and seek the restriction of this processing at any time. To learn more, please see the “Your legal rights” section below.

7. What type of Personal Data do we collect

In the course of providing our Website and Services we collect and process different types of Personal Data; this data can come from different sources. The type of Personal Data we collect about you will depend on the service we’re providing and the nature of our relationship with you.

The table below outlines the types of Personal Data that we could collect:

Type	Examples include
Identity Data	Full name, maiden name, gender, date of birth, marital status, title, passport number, driving license number, National Insurance number
Contact Data	Address, e-mail address, phone number, LinkedIn profile URL
Employment Data	Job title, role description, employer name, office location, employment start & end date
Education Data	Degree title, class of degree awarded, university name, details of other qualifications
Background Check Data	The results of a Disclosure and Barring Service (DBS) check, evidence of a person’s right to work in the UK, adverse media search results
Financial Data	Bankruptcy status, bank account sort code, bank account number, salary, tax code, National Insurance Contribution details

Contractual Data	Details about the services we provide to you or are looking to provide to you
Customer Relationship Data	Details of the enquiries raised
Communications Data	Details obtained during telephone, email, SMS, video conferencing, social media, letter or face-to-face communications
Health Data	Allergy information (e.g. if we were arranging a business lunch) and information relating to a disability, injury or ailment that could impact your ability to safely evacuate a building (e.g. if you were having a meeting at our office)
Open Data	Details about you that are in public records, and information about you that is freely accessible via the internet
Audio, Video & Photo Data	Voicemails, call recordings, CCTV footage, and photographs
Consent & Preference Data	Permissions, consents and preferences that you give us, for example, around marketing
Complaints Data	Details of any complaints that you have raised
Usage Data	Details of how you use our Website and Services (e.g. which pages you visit on our Website)
Technical Data	Details about the devices and technology you use, such as when accessing our Website (e.g. device IP address, device operating system, web browser version)

If you choose not to provide us with some types of Personal Data, it may prevent us from providing a service to you.

8. Where do we collect Personal Data from

We may collect Personal Data about you from any of these sources:

Source	Examples include
Data that you or your business / organisation provide to us	- when you communicate with us via email, phone call, voicemail, SMS, online meeting, social media, letter, or during face-to-face meetings or events - when you use our Website - when you use an online service that we are providing directly or via a third party - when you fill in a form - when you sign an agreement - your marketing communication preferences - as part of customer surveys
Data we collect when you use our Services	- as part of a training session, cyber security assessment or crisis simulation - as part of a dark web scan - as part of a penetration test
Data about your visits to our Website	- technical information about the device you use to access our Website, including its IP address, time zone setting, operating system and web browser version - information about how you use our Website, such as the webpages you viewed
Data from third-parties	- client / supplier due diligence services - credit reference agencies - fraud prevention agencies - recruitment agencies - universities and other educational bodies - government and law enforcement bodies - debt recovery services

	• industry and trade bodies • IT service providers • cyber security service providers
Data from publicly available sources	• Electoral Register • Companies House • online search engines • social media
Data from Cookies	• For further information on how we use cookies and similar technologies, please read our “Cookie Policy” section below

9. How do we use Personal Data

Set out below are examples of the ways we might use Personal Data:

Type	Examples include
To provide our services to you or your business / organisation	• to communicate with you • to register you as a new or potential client / supplier / other third party • to confirm your identity • to understand your requirements • to carry out our obligations arising from any contract or agreement we have entered into, or are about to enter into • to issue invoices • to process payments • to provide ongoing customer support
To provide updates about services you are using	• to notify you about changes to our services, including the terms and conditions by which they are offered • to notify you of an amendment to a Cyserrri policy
To market services	• to let you know about services and offers that may be of interest to you or your business / organisation • to let you know about online and face-to-face events that could be of interest to you or your business / organisation • we may also use your personal data for testimonials / case studies / marketing purposes. We will always obtain your prior written consent before publishing a testimonial or case study
To improve the services we offer	• to help us improve our Services or develop new Services • to request feedback on our Services and analyse the results
To maintain and improve customer experience	• to allow you to access and use the Services provided by us • for analytical and administrative purposes • for our internal purposes, such as research and analysis, reporting and quality control
To manage and administer the operation of our business	• to collect and recover money owed to us • to test our systems and processes • to mitigate IT risks including IT service interruptions • to mitigate cyber security risks including cyber attacks and data breaches
To comply with internal policies and procedures	• to maintain compliance with our internal policies and procedures • to conduct training
To resolve complaints	• to investigate and resolve complaints and disputes.

To prevent fraud	to help prevent fraud, money laundering and other crimes.
Pre-employment checks	to conduct pre-employment checks such as ID, right-to-work, and criminal record
To comply with laws	to comply with applicable laws and regulations
For Website maintenance and improvement	- to administer our Website, troubleshoot and resolve issues, and conduct data analysis, testing, and research (including via surveys) - to ensure content on our Website is displayed correctly - to evaluate the use of our Website
For copyright monitoring	to monitor the use of our intellectual property, copyrighted materials and trademarks
Legal rights	to exercise and defend our legal rights

We may rely upon more than one legal basis to lawfully process your Personal Data.

10. Marketing communications

We may use your Personal Data to provide you with information on Services and offers we think you may be interested in. We may contact you by phone, SMS, letter, email and / or other forms of electronic communication.

We will only use your Personal Data to communicate with you for marketing purposes if we have either your consent or there is a “legitimate interest”.

We may ask you to confirm or update your marketing preferences from time-to-time.

If you no longer wish to receive marketing communications from us, you are able to “opt out” of them at any time by simply emailing us (see the “How to contact us” section below) and stating “please cease all marketing communications to me” or something similar. We will reply once our records have been updated.

If you wish to amend your marketing preferences rather than fully opt out, simply send us an email at any time (see the ‘How to contact us’ section below) stating “please only send marketing communications to me via email” or something similar. We will reply once our records have been updated.

11. Automated decision-making

Automated decision-making takes place when an electronic system uses logic or algorithms to make a decision without human intervention. Some of the Services we provide, including those via our strategic partners, may use automated decision-making. We do not set or determine the logic or algorithm used in automated decision-making systems.

12. Who do we share Personal Data with

We will never sell or lease your Personal Data to any third-party.

We will only share your personal data with other businesses or organisations if they are affiliated to Cyserrri Cyber, they are one of our service providers or are affiliated to one of our service providers, or where our legal or regulatory obligations require us to share your Personal Data with another business or organisation.

Any third-party that we share your Personal Data with has an obligation to keep your Personal Data confidential, maintain adequate security safeguards and to comply with all applicable laws and regulations relating to protecting Personal Data. We only allow third-parties to process your Personal Data for specified purposes.

We may share your Personal Data with:

Third Party Type	Examples include
Affiliated Companies	- Companies that are affiliated with Cysserri - Companies that are affiliated with one of our service providers
Authorities, Regulators and other official bodies	- UK central and local government - HM Revenue & Customs (HMRC) - Financial Conduct Authority (FCA) - The Pensions Regulator (TPR) - Information Commissioner's Office (ICO) - National Cyber Security Centre (NCSC) - Law enforcement and fraud prevention agencies - Other third parties as required by and in accordance with applicable laws, regulations, or in the public interest
Individuals linked to you or your business	- a company director - a trustee or trustee board member
Service providers that need your Personal Data to provide a service	- providers of administrative support services - providers of IT and cyber security services - providers of cyber insurance and other related services - providers of cyber incident and data breach related services - providers of accountancy and bookkeeping services - providers of banking services - providers of consultancy services - providers of legal services - providers of credit reference and client / supplier due diligence services - providers of audit services - providers of marketing and market research services acting on our behalf - providers of search engines and analytics services
Business sale and restructuring	Companies involved in the restructure, reorganisation or sale of our business.
Other service providers	Other service providers that offer services that align with, or appear to align with, your requirements.

13. How long do we keep Personal Data

The length of time we retain Personal Data for will vary depending on the nature and sensitivity of the Personal Data, the purpose for which it is used, the legal basis for processing it, the nature and status of Cysserri's relationship with you and as required to comply with our legal and regulatory obligations.

Other factors that can impact the retention period of Personal Data include:

- where the "Right of erasure" has been exercised (see the "Your legal rights" section below)
- where your Personal Data relates to a complaint or dispute that has been lodged with us
- where we believe there is a prospect of litigation with you or your business or litigation has commenced
- where in limited cases, the law permits us to keep certain types of Personal Data indefinitely, provided we put appropriate protections in place.

14. How do we protect Personal Data

We take the protection of your Personal Data very seriously and have put in place appropriate security measures to prevent, or reduce the likelihood of, your Personal Data being unlawfully or inadvertently accessed, used, copied, modified, damaged, destroyed or disclosed.

In addition, we limit access to your Personal Data to only those employees, contractors and other third parties who need access to support us in providing services to you. They will only process your Personal Data on our instructions and are subject to a duty of confidentiality.

15. Where do we store and process Personal Data

Personal Data you provide to us may be transferred, stored, and processed outside of the UK and EEA. By way of example, this may happen if any of the servers of our third-party service providers are located in a country outside of the UK and EEA.

If we transfer your personal data outside of the UK and EEA in this way, we will take reasonable steps to ensure that appropriate security measures are in place with the aim of ensuring your privacy rights continue to be protected in accordance with applicable data protection laws.

If you use our services whilst you are outside of the UK and EEA, your information may be transferred, stored and processed outside of the UK and EEA in order to provide you with those services.

16. Your legal rights

You have a number of legal rights in relation to the Personal Data that we hold about you. Please be aware that your rights do not apply in all circumstances and are subject to exceptions.

Legal Right	Description
Right to be informed	You have the right to be informed about how your Personal Data is collected and used. We use this Privacy & Cookie Policy to inform you.
Right of access	You have the right to be provided with a copy of the Personal Data that you have shared with us. This right only applies to data that we still hold.
Right to rectification	You have the right to request that the Personal Data that we hold about you is corrected if it contains mistakes or added to if it contains omissions. If you seek to exercise this right, we may need to verify the accuracy of the new data you provide to us.
Right to erasure	You have the right to request that we delete your Personal Data in certain circumstances. This right is also known as the 'Right to be forgotten'. This right does not apply where processing your Personal Data is necessary in order to comply with a legal or regulatory obligation.
Right to object	You have the right to object to the processing of your Personal Data where we are relying on a legitimate interest as the legal basis for processing and you believe that the processing impacts on your rights and freedoms. You also have the right to object where we are processing your information for marketing purposes.

Right to restrict processing	You have the right to request that we restrict our processing of your Personal Data in certain circumstances. If you choose to exercise this right, we may not be able to provide you with our Services.
Right of data portability	You have the right to request the transfer of your Personal Data to you or to a third-party you have chosen, in a structured, commonly-used and machine-readable format. This right only applies to Personal Data which you have provided to us.
Right to withdraw consent	You have the right to withdraw your consent at any time where we are relying upon consent to process your Personal Data. If you choose to exercise this right, we may not be able to provide you with our Services.
Rights in Relation to Automated Decision-Making	You have the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects. If you choose to exercise this right, we may not be able to provide you with our Services.

Companies like Cyserri are required to respond to your request to exercise these rights within one calendar month of receiving your verified request, unless we determine that your request is manifestly excessive.

We will not charge you a fee to exercise the rights set out in this section, unless, that is, that we deem the effort to fulfil your request, or series of requests, is manifestly excessive. In such circumstances, we will inform you of the fee and explain why we are charging a fee; the fee will need to be paid in full prior to the required work being actioned.

You can exercise these rights by contacting us using the details set out below in the “How to contact us” section.

17. Letting us know if your Personal Data is incorrect

You are responsible for making sure that any Personal Data you have provided to us is accurate. Please contact us if your Personal Data changes during our relationship with you as this will help to ensure the data we hold remains accurate and allows us to contact you.

18. Links to third-party websites

Our Website may, from time-to-time, contain links to the websites of third-party businesses and organisations which are not owned, operated or controlled by Cyserri. We may also send emails or other communications with links to third-party websites. We provide such links solely for your convenience.

If you click a link to a third-party website, you will leave our Website. Clicking on such a link may allow third-parties to collect Personal Data about you. These third-party websites have their own privacy and cookie policies, and website terms and conditions of use. Please note that disclosure of Personal Data to third-party websites is at your own risk.

The inclusion of such links does not mean or imply that Cyserri recommends, endorses, guarantees or warrants the third-party websites, or the information that you may obtain from them. We have no control over the content provided on these websites, including malicious content introduced by threat actors.

Cyserri does not accept liability for any loss, damage, expense, cost or liability whatsoever incurred by you, your business / organisation, its affiliates, its service providers, its clients or any other stakeholder, in respect of these third-party websites, as a direct or indirect result of a link on our Website.

If you leave our Website using a third-party link (as opposed to, for example, simply closing the tab in your web browser), please ensure you read the privacy policy, cookie policy, website terms and conditions of use, and any other relevant policies and notices on the third-party website to ensure you understand their terms and conditions of use.

19. Children's Personal Data

None of the Services we provide, including our Website, are aimed at or designed to be used by children. We also do not knowingly collect Personal Data about children. If you have shared Personal Data about a child with us, please contact us as soon as possible using the details in the "How to contact us" section, so we can remove it.

20. Cookie Policy

Our Website uses cookies and other similar technologies. This policy explains what cookies are, how we use them and how you can manage your cookies preferences.

A cookie is a small text file which is stored on your device (e.g. laptop, tablet or smartphone) when you visit our Website.

Some cookies last for the length of your visit to our Website; these are known as session cookies. Other cookies remain on your device until they expire or until you delete them from your browser; these are known as persistent cookies.

The below table describes four types of cookie that may be used on our Website and what they could be used for:

Cookie Type	Description
Strictly Necessary Cookies	These cookies are required to make essential aspects of our Website operate as intended. Without strictly necessary cookies, parts of our Website will not work as intended. This type of cookie is therefore not designed to be disabled by the website visitor.
Functional cookies	Functional cookies allow us to present non-essential Website functionality to you, such as embedded videos. If you disable these cookies, certain functionality our Website uses may not be available to you.
Analytical cookies	These cookies help us to understand how people use our Website and how well our Website is working. Disabling these cookies means that we will be unable to establish certain information about the performance of our Website; this information is used to improve the online experience for visitors.
Advertising cookies	These cookies are used to capture information about your web browsing habits so that any displayed advertisements have a greater likelihood of being relevant to your interests.

Our Website may use cookie functionality from a number of third-parties. Further information about cookies can be found at www.allaboutcookies.org.

21. Where to find further information on UK data protection laws

If you wish to learn more about UK data protection laws, consider using one of the following sources:

- GOV.UK: <https://www.gov.uk/data-protection> -- Provides an overview of the UK's data protection legislation.
- ICO: <https://ico.org.uk/> -- The UK's independent authority that provides guidance and support on data protection laws as well as enforcement action.

22. Changes to this Privacy & Cookie Policy

The date when this Privacy & Cookie Policy was last updated is displayed on page 1 of this policy. We keep our Privacy & Cookie Policy under regular review and reserve the right to change it at any time and without notice.

If we update our Privacy & Cookie Policy we will replace the current version on our Website with the updated version. The updated version becomes effective immediately upon its publication on our Website.

Every time you wish to use our Website, you must check the date that this Privacy & Cookie Policy was last updated. If the last updated date has changed since you last read it, you should re-read it in full.

Your continued use of our Website and Services after the publication of a new version of this Privacy & Cookie Policy, means that you agree to comply with the new version.

23. How to make a complaint

We take data privacy very seriously. However, if you believe that our collection or use of your Personal Data, or the way we process requests to exercise your data privacy rights, do not comply with UK data protection laws and regulations, please contact us using one of the methods set out in the “How to Contact us” section below. We will then investigate your complaint.

We aim to complete complaint investigations within one calendar month. In some circumstances we would be permitted to take up to three calendar months to complete a complaint investigation, but this would usually only be the case if the complaint is very complex or manifestly onerous. If we deemed your complaint to be the latter, we would write to you within one calendar month to make you aware of the longer investigation period.

If having lodged a data-privacy related complaint with Cyserri using one of the methods outlined in the “How to Contact us” section below, you are still unhappy with our findings or resolution, you have the right to lodge a complaint with the Information Commissioner’s Office (ICO).

To lodge a data-privacy related complaint with the ICO, please contact the ICO using the methods found on the following webpage: <https://ico.org.uk/make-a-complaint/data-protection-complaints/> . This ICO webpage provides additional information on this topic which you may find helpful.

24. How to contact us

If you have any questions regarding our Privacy & Cookie Policy or how we collect and use your Personal Data, or if you wish to exercise any of your rights regarding your Personal Data, or for any other privacy related request, please contact us using one of the methods set out below in this section:

Email us: privacy@cyserri.com

Write to us: Cyserri Cyber Limited, 51 Lime St, London, EC3M 7DQ.

