

Privacy policy

Introduction

This policy applies across all websites that we own and operate and all services we provide, including our cloud-based applications, and any other apps or services we may offer (for example, events or training). For the purpose of this policy, we will just call them our “**Services**”.

When we say “**personal data**” we mean identifiable information about you, like your name, email, address, telephone number, bank account details, payment information, support queries, community comments and so on. If you can't be identified (for example, when personal data has been aggregated and anonymised) then this policy doesn't apply. Check out our [terms of business](#) for more information on how we treat your other data.

We may need to update this policy from time to time. Where a change is significant, we'll make sure we let you know – usually by sending you an email.

You can read the whole policy below, or if you haven't got much time, you can jump to the section you need using the navigation menu.

Last updated: 25 January 2024

Who are 'we'?

When we say “**Spktral**”, “**we**”, “**our**” or “**us**”, we're talking about Spktral Limited, a company registered in England and Wales with company number 12194589, whose registered office is situated at 20-22 Wenlock Road, London, N1 7GU (or any of our wholly owned subsidiaries).

We provide easy-to-use cloud-based applications that help organisations understand and address the complexities of diversity, inclusion and equality through the application of technology, data and measurement. If you want to find out more about what we do, see our website.

We'll only process your personal data in line with data protection laws, namely the EU law retained version of the General Data Protection Regulation ((EU) (2016/679) (“**UK GDPR**”) the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directives) Regulations 2023. If any of these laws are replaced or succeeded by another piece of law, we'll comply with those too.

We're registered with the Information Commissioner's Office (“**ICO**”), the UK regulator for data protection issues (www.ico.org.uk), and our registration number is **ZA571108**. If you ever have any concerns about how we handle your personal data, it's your right to complain to the ICO, but we'd ask for the heads up before you do so we can try and resolve your concerns first. You can reach us at privacy@spktral.com.

Are we a 'data controller' or a 'data processor'?

Let's talk about how we handle personal data. In the world of personal data, there are two key roles: data controllers and data processors. Think of Spktral as wearing two different hats, depending on the situation:

Data controller: When we're holding personal data about you, which we collect, such as key members of our clients' teams (i.e. names, roles, contact details), we're the data controller. This means we are responsible for collecting the personal data, deciding what personal data to collect, and for deciding how and why this personal data is used. An example is if you sign up to our newsletter – we decide that we need your name and email address, and so we collect this from you, and we then use this personal data to send you our newsletter. Of course, you can opt-out any time by clicking 'unsubscribe' within the newsletter.

Data processor: Other times, we're acting as data processors. Here, we receive personal data from our clients that they have collected and chosen to share with us, and we then use this personal data to provide our Services. In that scenario, our clients are the data controller, and we are the data processor because we're processing personal data in line with our clients' instructions.

Whether we're a data controller or a data processor, we will handling the personal data responsibly and transparently, and in line with this policy. If you have any questions about this, please drop us an email at privacy@spktral.com.

Our principles of data protection

Our approach to data protection is built around four key principles. They're at the heart of everything we do relating to personal data.

Transparency: We take a human approach to how we process personal data by being open, honest and transparent. We encourage you, as responsible individuals and organisations, to do the same.

Enablement: We enable connections and efficient use of personal data to empower productivity, growth and insight.

Security: We strive to implement industry leading approaches to securing the personal data entrusted to us.

Stewardship: We accept the responsibility that comes with processing personal data.

The data we collect

We might collect a variety of your personal data/information, and this means any information that might enable us to identify you (but it doesn't include anonymous data). We've grouped this personal data together as follows:

- **Identity Data** includes first name, maiden name, last name, marital status, title, data of birth, and gender.
- **Contact Data** includes address history, 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 goods and Services you have purchased from us.
- **Technical Data** includes 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 Services or 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 and our Services.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

At times we may collect aggregated data – think stats or demographics. This isn't considered personal data in law as this data will not directly or indirectly reveal your identity to us. It just helps us make your experience with our Services or website better.

We do collect special category data about the employees or contractors of the organisations that use our Services. The personal data that falls under this category includes details about ethnicity, disability and sexual orientation. We don't collect any information about criminal convictions and offences.

How we collect your data

When you visit our websites or use our Services, we collect personal data. The ways we collect it can be broadly categorised into the following:

Information you provide to us directly: When you visit or use some parts of our websites and/or Services we might ask you to provide personal data to us. For example, we ask for your contact information when you sign up for a free trial, request an industry update, participate in an online survey, join us on social media, take part in training and events, contact us with questions or request support. If you sign up to the newsletter on our website, we will collect your name and email address.

If you don't want to provide us with personal data, you don't have to, but it might mean you can't use some parts of our websites or Services.

Commented [LU1]: Anthony: This has been added so we can summarise the types of personal data that might be collected.

Commented [AJH2R1]: Ok

Commented [LU3]: Anthony: Could you advise if this is accurate?

Commented [AJH4R3]: No, because the introduction specifically states "our cloud-based applications" - in which we do collect Special category data.

Commented [LU5R3]: Thanks for this - I've relied on the feedback you kindly gave on the data processing addendum to update this list.

Information we collect automatically: We collect some information about you automatically when you visit our websites or use our Services, like your IP address and device type. We also collect information when you navigate through our websites and Services, including what pages you looked at and what links you clicked on. This information is useful for us as it helps us get a better understanding of how you're using our websites and Services so that we can continue to provide the best experience possible (e.g. by ensuring you have a smooth user experience as you navigate around).

Some of this information is collected using cookies and similar tracking technologies. If you want to find out more about the types of cookies we use, why, and how you can control them, take a look at our [cookie notice](#).

Information we get from third parties: The majority of information we collect, we collect directly from you. Sometimes we might collect personal data about you from other sources, such as publicly available materials (annual reports, Government Equalities Office Gender pay gap reports) or trusted third parties, like our marketing and research partners. We use this information to supplement the personal data we already hold about you, in order to better inform, personalise and improve our Services, and to validate the personal data you provide.

Where we collect personal data, we'll only process it:

- **Contract:** to perform a contract with you; or
- **Legitimate Interests:** where we have legitimate interests to process the personal data and they're not overridden by your rights; or
- **Legal Obligation:** in accordance with a legal obligation; or
- **Consent:** where we have your consent.

If we don't collect your personal data, we may be unable to provide you with our Services, and some functions and features on our websites may not be available to you.

If you're someone who doesn't have a relationship with us, but believe that a Spktral subscriber has entered your personal data into our websites or Services, you'll need to contact that Spktral subscriber for any questions you have about your personal data (including where you want to access, correct, amend, or request that the user delete, your personal data).

Commented [AJH6]: Does this apply to the data we receive from a controller? Surely they have to have explicit consent to obtain and use that - we can't obtain consent from the data subjects.

Commented [LU7R6]: You could rely on consent as of the legal bases where users sign up to receive newsletters, but legitimate consent is more appropriate, and you wouldn't solely rely on consent to process personal data.

Commented [A8R6]: I think there are two situations:
what we collect from website, newsletter, etc - which doesn't include special category data and
What we process on behalf of a controller which could possibly contain SCG. In this case, the only legal basis we have for processing is the controllers warrant that they have obtained and hold accurate explicit consent.

As long as this covers that then we're all good.

Personal data within organisations

If your organisation has signed up to our Services, we upload a data file provided by them which contains information about employees, workers and contractors. This data file doesn't contain any names of any person, just a unique identifier. However, the data file may contain the following items:

- date of birth
- start date
- leave date
- employee grade
- job family
- working pattern
- work location
- gender
- health information
- ethnicity
- sexual orientation

It is important to note that only invited users to our Services can access this data for analysis purposes and although these users can't see the raw data (like it would be displayed in the data file), they would be able to:

- view the adjusted hourly rate of pay of employees by unique identifier; and
- view, filter and group data by the demographic information listed above.

This means that a person could be identified, particularly in smaller organisations.

It is also important to note that we don't keep the raw data collected from your organisation – this remains under the control of your organisation.

If you contact us to ask to exercise your right to be forgotten, we will direct you back to your organisation, as they keep the raw data file that our Services process. It is your organisation's responsibility to delete your raw data, at which point we'll be notified that this has happened, and we will reload the data file with your personal data omitted.

How we use your data

First and foremost, we use your personal data to operate our websites and provide you with any Services you've requested, and to manage our relationship with you. We also use your personal data for other purposes, which may include the following:

To communicate with you: This may include:

- providing you with information you've requested from us (like training or education materials) or information we are required to send to you
- operational communications, like changes to our websites and Services, security updates, or assistance with using our websites and Services
- marketing communications (about Spktral or another product or service we think you might be interested in) in accordance with your marketing preferences
- asking you for feedback or to take part in any research we are conducting (which we may engage a third party to assist with)

To support you: This may include assisting with the resolution of technical support issues or other issues relating to the websites or Services, whether by email, in-app support or otherwise.

To enhance our websites and Services and develop new ones: For example, by tracking and monitoring your use of websites and Services so we can keep improving, or by carrying out technical analysis of our websites and Services so that we can optimise your user experience and provide you with more efficient tools.

To protect: So that we can detect and prevent any fraudulent or malicious activity, and make sure that everyone is using our websites and Services fairly and in accordance with our [terms of business](#).

To market to you: In addition to sending you marketing communications, we may also use your personal data to display targeted advertising to you online through our own websites and Services. If you contact us on LinkedIn, we create a contact card on our CRM system so that we can then reach out to you with a message, for which we rely on legitimate interests.

To analyse, aggregate and report: We may use the personal data we collect about you and other users of our websites and Services (whether obtained directly or from third parties) to produce aggregated and anonymised analytics and reports, which we may share publicly or with third parties.

We've summarised this in the table below. It shows the circumstances under which we collect personal data, what kind of personal data we collect and the lawful bases we rely on to do so:

Commented [LU9]: Anthony: I've added this table so it clearly summarises when you collect personal data and what your lawful basis is.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To enable you to submit an enquiry to us, whether via email, through our website or via social media, including but not limited to LinkedIn, Facebook and Instagram.	Identity Contact	Contract Legitimate Interests (to enable us to respond to your enquiry) Consent
To process and deliver our Services to you including: (a) Manage payments, fees, and charges (b) Collect and recover money owed to us	Identity Contact Financial Transaction Marketing Comms	Contract Legitimate Interests (to recover debts due to us)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy and cookie policies (b) Asking you to leave a review or take a survey	Identity Contact Profile Marketing Comms	Contract Legal Obligation Legitimate Interests (to keep our records updated and to study how customers use our Services)
To enable you to partake in a prize draw, competition or complete a survey	Identity Contact Profile Usage Marketing Comms	Contract Legitimate Interests (to study how customers use our Services, to develop them and grow our business) Consent
To enable you to register for our mailing list/email marketing	Identity Contact Marketing Comms	Contract Legitimate Interests (to enable us to provide you with the newsletter/email marketing and present you with information, or services we consider you will be interested in) Consent

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	Identity Contact Technical	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) Legal Obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	Identity Contact Profile Usage Marketing Comms Technical	Legitimate Interests (to study how customers 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	Technical Usage	Legitimate Interests (to define types of customers 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 goods or Services that may be of interest to you	Identity Contact Technical Usage Profile Marketing Comms	Legitimate Interests (to develop our products/Services and grow our business)

How we can share your data

There will be times when we need to share your personal data with third parties. We will only disclose your personal data to:

- other companies in the Spktral group of companies now and in the future
- third party service providers and partners who assist and enable us to use the personal data to, for example, support delivery of or provide functionality on the website or Services, or to market or promote our goods and Services to you. These third parties are known as sub-processors. Where we share your personal data with those sub-processors, they will be bound by confidentiality and data protection obligations. We do this to ensure that your personal data is kept safe and secure.
- regulators, law enforcement bodies, government agencies, courts or other third parties where we think it's necessary to comply with applicable laws or regulations, or to exercise, establish or defend our legal rights. Where possible and appropriate, we will notify you of this type of disclosure
- an actual or potential buyer (and its agents and advisers) in connection with an actual or proposed purchase, merger or acquisition of any part of our business
- other people where we have your consent.

Data storage and transfers

Your data is stored on servers within the UK's territorial waters. If we are planning to change the storage location at a future date, we will contact you well in advance to inform you of our plans and how we intend to maintain or even increase the security of the data we store and transmit.

We might need to transfer your personal data to countries outside of the UK or the European Economic Area (EEA) when we use third parties to help us provide our Services. This could happen, for example, when we need to receive Services or deal with payments. But don't worry. We make sure that your personal data is still protected by putting at least one of the following safeguards in place:

- we will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data
- where we use certain service providers, we may use specific contracts approved for use in the UK or the EEA which give personal data the same protection it has in the UK or in the EEA.

Just ask if you'd like more information on the specific mechanism we use when we transfer any personal data out of the UK or the EEA.

Commented [AJH10R9]: Looks good!

Commented [LU11]: Anthony: It is important to explain what happens if data is transferring outside the UK/EEA.

Commented [AJH12R11]: Ok thanks

Security

Security is a priority for us when it comes to your personal data – we want to build trust and a great measure of that is how we treat your most valuable commodity. We're committed to protecting your personal data and have appropriate technical and organisational measures in place to make sure that happens.

If there is an incident where we become aware that there has been a data breach, we will let you know without undue delay. We will then take all necessary steps, including informing the ICO, to limit the extent of the breach and to prevent a further reoccurrence.

Please keep in mind that while we do our best to protect your personal data, sharing information over the internet isn't 100% secure. So, any personal data you share with us online is done at your own risk.

Retention

The length of time we keep your personal data depends on what it is and whether we have an ongoing business need to retain it (for example, to provide you with a service you've requested or to comply with applicable legal, tax or accounting requirements).

We'll retain your personal data for as long as we have a relationship with you and for a period of time afterwards where we have an ongoing business need to retain it, in accordance with our data retention policies and practices. Following that period, we'll make sure it's deleted or anonymised.

Your rights

It's your personal data and you have certain rights relating to it. When it comes to marketing communications, you can ask us not to send you these at any time – just follow the unsubscribe instructions contained in the marketing communication or send your request to privacy@spktral.com.

You also have rights to:

- know what personal data we hold about you, and to make sure it's correct and up to date
- request a copy of your personal data, or ask us to restrict processing your personal data or delete it
- object to our continued processing of your personal data

You can exercise these rights at any time by sending an email to privacy@spktral.com.

We won't charge you to access your personal data or exercise your rights. However, we may charge a reasonable fee if your request is excessive or unfounded. In some cases, we may also refuse to fulfil your request.

To keep your personal data safe, we may ask for proof of identity and request additional information. We'll do our best to respond to all legitimate requests within one month, but sometimes it may take longer, especially if your request is complicated. If this happens, we'll keep you informed.

Third party links

Just so you know, this policy only applies to our website and Services. We have some links on our website that take you to other websites, like our social media accounts. Those websites are not under our control and they have their own privacy policies and terms and conditions. So, before you share any personal data with those websites, please make sure to check their privacy policies.

How to contact us

If you're curious about what personal data we hold about you or you have a question or feedback for us on this policy, our websites or Services, please get in touch.

As a technology company, we prefer to communicate with you by email – this ensures that you're put in contact with the right person, in the right location, and in accordance with any regulatory time frames.

Our email is: privacy@spktral.com.