Data Privacy Notice

What is this and why should I read it?

Bibra is committed to protecting the privacy and security of your Personal Data, and we want to ensure you understand your rights and our responsibilities when it comes to your Personal Data.
This data privacy notice describes how we handle your Personal Data throughout our relationship, whether you are a client or prospect, a potential business partner, or just a member of the public hoping to get to know us better or access educational content by exploring our website or getting in touch.

If you are an employee, consultant, agency worker or candidate, please refer our Data Privacy Notice for Employees, Consultants, and Workers (available upon request to the Privacy Lead). This website and our services are not intended for children and we do not knowingly collect data relating to children.

What if I have any questions or concerns?

Our Privacy Lead is responsible for overseeing our privacy program. If you ever have any questions or concerns about how we handle your Personal Data, please contact:

Ashleigh Ace Barrett, Commercial Director
Bibra toxicology advice & consulting
BTS House
69-73 Manor Road
Wallington
Surrey SM6 0DD
UK

Tel: +44 (0)20 8619 0770
E-mail: info@bibra.co.uk (FAO Ashleigh Ace Barrett)

Our commitment to your privacy (Personal Data Protection Principles)

Regardless of where, why or how we obtain or Process your Personal Data, we comply with Data Protection Law (DP Law). DP Law protects 'data subjects' in the UK and EU (that's you) by imposing stricter obligations on 'data controllers' (that's us) and 'data processors' (those that help us) when we 'process' 'personal data'. Click here to see our glossary below under 'Personal Data', 'Processing', 'Controller', 'Processor'.

In a nutshell, DP Law applies to any data that might identify you, wherever or however we got it, whatever we do with it and wherever we Process it, even if someone else Processes it on our behalf, and even if we send it outside the EEA.

This means that whenever we Process your Personal Data we do so:

- **Lawfully**: Only if we can justify it on one of the following Lawful Bases:
    - Consent – this means you have given us permission, which you can withdraw at any time. We need your **explicit consent** to process sensitive data like health-related data (Special Data) or to transfer your Personal Data outside the EEA where we don't have another basis for doing so
    - Legitimate Interest – to help fulfil a legitimate business objective (see the 'Why' column of our At-a-Glance table) after confirming we've only used what's reasonably necessary and proportionate to meet that objective and struck the right balance between our interests and yours (Legitimate Interests Assessment (LIA)). Generally speaking, we need this it to operate our business, generate leads and sales, make sure our relationship with you runs smoothly, and protect the Personal Data and commercial data we hold by securing our network and information systems
    - Contractual necessity – to enter into or fulfil our contract, including to generate a quote
    - Legal obligation – to comply with the law (e.g. tax reporting, Anti-Corruption)
    - Vital interests – in rare instances where one of the others don't apply but we need your Personal Data to protect your vital interests or those of another person
- **Fairly** and **transparently**: we strike the right balance between our interests and yours and we tell you what we do with your Personal Data

- For a **specific purpose**: we won't use your Personal Data for another incompatible purpose unless the law permits or requires us to
- Using the **least amount** reasonably necessary
- Ensuring it is accurate, **complete** and **up-to-date**
- For a **limited time**: Only for as long as reasonably necessary, and then we either destroy it or de-identify it so it can't be linked back to you
- **Securely**: managing our people and designing our processes and technology to ensure end-to-end **confidentiality, integrity** and **availability**
- **Within the UK/EEA**: we don't transfer your Personal Data outside the EEA except as permitted under DP Law. We use appropriate safeguards for consistent protection and ensure third parties we rely on do so as well
- With **your rights** in mind: We make it easy for you to exercise your rights (see Your Rights)

The types of Personal Data we Process about you are grouped under the following categories:

- **Identity Data**: first name, last name, company name, title
- **Contact Data**: billing address, trading/physical address (if different from billing address), email address and telephone numbers, contact name(s)
- **Financial Data**: bank details (if you are a supplier of ours), invoices we send (if you are a client of ours)
- **Transaction Data**: details about payments to and from you and other details of products and services you have purchased from us (e.g. Membership, TRN subscription) or for which you have sought a quote or additional information through our Contact Us form or via email
- **Profile Data**: purchases or orders made by you, your company 'category'/SIC code, preferences, feedback on work
- Marketing and Communications Data: your preferences in receiving marketing and newsletters from us – including do-not-call and unsubscribe requests (suppression lists), cookie preferences, and your preferred communication methods
- **Client Data** refers to Personal Data we receive or generate in connection with matters for which you've sought our expertise: director or employee names or details, emails, text messages, internal or external documents you've shared

At-a-glance Table

Why	What	From whom?	Lawful basis	With whom?
To register you as a new member, subscriber or customer	Identity Contact Marketing and Communications	You	Contract Legitimate Interests (Direct marketing)	Commercial Team and Managing Director
To respond to an enquiry, process your order, finalise a transaction	Identity Contact Financial Transaction Technical Information about matters for which you require our assistance	You Commercial Team and Toxicologists (who correspond with you and manage the customer relationship)	Contractual Necessity (deliver a newsletter, connect to guest WIFI) Legitimate Interests (recover payments; protect our business; meet client needs)	Commercial Team Xero (accounts package) Stripe (if payment is made via credit card) IT service provider (Solar Systems IT) on a need-to-know basis ('Help desk')

bibra toxicology advice & consulting

Why	What	From whom?	Lawful basis	With whom?
To manage our relationship with you and deliver what we promised	Identity Contact Profile Usage Marketing and Communications Client Data	You	Contractual Necessity (fulfil our contract with you) Legal obligation (notify you of privacy updates) Legitimate Interests (feedback; QA; reputation management)	Commercial team Toxicologists
To manage our finances, generate and manage invoices, produce accounting, audit and sales reports, and manage credit	Financial Data Transaction Data	You Us (internal reports, spreadsheets, software, email)	Contractual Necessity (to ensure we get paid) Legitimate Interests (to optimise our finances, set the right price, forecast)	Commercial Team External professionals (accountants, auditors, lawyers) Insurers
To generate leads and get/keep in touch	Identity Contact Marketing and Communications	You (business card, email) Your contacts (referrals, intros) Conference attendee lists	Legitimate Interests (to grow our business)	Commercial Team Managing Director
To comply with marketing and cookie rules	Identity Contact Marketing and Communications	You (your preferences) Cookie Dashboard provider (CookieBot)	Legal Obligation (PECR rules on direct marketing and cookies)	Commercial Team Managing Director Cookie Dashboard provider (CookieBot)
To improve our services and products	Identity Profile Usage	You (feedback, surveys) Commercial Team, your Toxicologist (notes, emails)	Legitimate Interests (define customer segments for our products and services, keep our website and communications updated and relevant, develop our business and inform our market strategy)	Customer Service Personnel Marketing and sales consultants Product Development Personnel

Why	What	From whom?	Lawful basis	With whom?
To administer and protect our business and the security of our Network and Information Systems (NIS), including this website	Identity Contact Technical Usage	You Technical data from your use of our NIS (to monitor activity not people and only consider individual activity if further action / investigation required) Alerts from third-party tools to out of policy or suspicious activity	Legitimate Interests (establish baseline or 'normal' activity patterns; identify abnormal activity (downloads, spikes in prints or transfers, visits to prohibited websites, etc.)	Commercial Director IT service provider (Solar Systems IT) Vendors who support, optimise and help secure our Website (Cloudflare, WP Engine) or other parts of our NIS (Sophos)
Rarely: To investigate criminal wrongdoing or assist law enforcement	Any of the categories of information we already have about you Publicly available information Court-ordered or regulator-ordered disclosure	You Publicly available information Third parties permitted by law to share the information, e.g. in response to a subpoena	Legal Obligation Legitimate Interests	Strictly need-to-know personnel and the third parties involved in disclosure (law enforcement, external legal counsel, forensics experts, auditors, external investigators)

How do you strike the right balance when you rely on Legitimate Interests?

We conduct Legitimate Interests Assessments (LIA's) whenever we rely on Legitimate Interests and, where appropriate, Data Protection Impact Assessments (DPIAs). You can find more detailed information by contacting our Privacy Lead.

For example, we do some limited profiling based on your past purchasing behaviours or requests, to target products, services, educational content, and conferences to you that we're quite confident you'll like, and avoid bombarding you with those you won't. To do this, we need to learn more about you and your preferences, but we ensure we have appropriate safeguards to prevent this information from being misused and ensure we strike the right balance:

- **Only what we need**: Our Commercial Team, Managing Director and the Toxicologists you work with do things the old-fashioned way. They get to really know their clients and their interests, and they stay up-to-date on industry developments and advances in research so they can alert you to changes that might impact your business and require attention. They know your business and what your concerns are because they've worked closely with you in the past. This personal touch, and the relationship they maintain with you, helps them tailor their communications to you.
- **When we need it, and only by those who need it**:
    - Our Commercial Team and Toxicologists. Only our Commercial Director can view your account history information, and we have implemented additional safeguards
    - We never let third parties use your information for their own purposes, and we prevent this by giving them only what they need and as little Personal Data as possible, for example by pseudonymising our project numbers (for project monitoring) to protect your company name and contact information, securely transmitting it to protect your identity

    - We don't disclose identifiable information about your company or individuals within it. Even when we describe our achievements, we take care to sanitise the information to avoid revealing who our customers are (see our Recent Projects for an example of this), unless you expressly choose to provide a testimonial
- **We've struck the right balance**: we've conducted Legitimate Interest Assessments (LIA) where appropriate, to confirm our use of any Personal Data you provide is fair
- **Even so…it's optional**: You can object to this activity by opting out at any time. Simply contact our Privacy Lead (Ashleigh Ace Barrett) or disable our marketing cookies on your cookie dashboard

What happens if you can't get this personal data?

If we can't process this Personal Data, or if it's inaccurate, we may not be able to perform the contract we have entered into with you (e.g. provide you with the TRN subscription you've requested and paid for), or we may be prevented from complying with our legal obligations (e.g. doing our due diligence under Anti-Money Laundering rules) or Legitimate Interests (managing credit risk by vetting prospects). If we aren't able to get profile, technical, usage and marketing and communications data (e.g. ad clicks, customer feedback, page visits) it will be difficult for us to optimise our services or website or meet consumer demands and serve up content we think you'll like, which means you might either receive communications that aren't suited to you, or you may miss out ones tailored to you, like alerts for certain educational content or regarding major regulatory developments.

What about sensitive Personal Data (Special Data) and Criminal Records Data?

Special Data requires higher levels of protection. We don't collect Special Data or Criminal Records Data related to our customers or prospects.

What about third-party links, plug-ins, content or cookies on your website?

If you click on a link to third-party content, like an ad, this will either take you to those third-party sites or applications or send your Personal Data to that third party related to your click. We have no control over their use of your Personal Data in this regard. We encourage you to read the Data Privacy Notice of websites you visit. Where there are Third Party Cookies and trackers on our website, our Cookie Notice provides links.

Who else can see my Personal Data?

Need-to-know is the default…

- Within the company: only those individuals within our company or the third parties listed under the 'With Whom' column of the At-a-Glance table can see or access your Personal Data, and they only Process the specific data they need to fulfil their tasks. We have implemented internal measures to enforce this need-to-know access and to ensure those who do Process it do so on our instructions and under a duty of confidentiality
- With our service providers and vendors: we do not allow our third-party service providers to use your Personal Data for their own purposes. We only permit Processors to Process your Personal Data for specified purposes and in accordance with our instructions. We minimise how much of your Personal Data needs to be transferred to ensure this objective is met

Wherever we Process your Personal Data jointly with another Controller (Joint Controller), we establish clear lines of accountability to ensure your rights are respected and our obligations are met, and we adhere to the principles and approach we mentioned earlier to minimise how much Personal Data we use.

In all cases, we require third parties to respect the security of your Personal Data and to treat it in accordance with DP Law through binding contracts.

Do you share my Personal Data with other third parties?

We also share your Personal Data with other third parties in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your Personal Data with the other parties if and to the extent required under the terms of the transaction and on the basis of Legitimate Interests. This ensures

seamless service for you, regardless of who owns the business. Still, we will notify you if this is the case and you will have the right to object to this transfer.

We may also need to share your Personal Data with a regulator or to otherwise comply with the law. This may include making returns to HMRC, disclosures to financial services regulators and disclosures to shareholders such as directors' remuneration reporting requirements.

Do you transfer my Personal Data outside the EEA?

We primarily Process your Personal Data – including back-ups and archives – in the EEA and in countries the European Commission has recognised as providing adequate levels of protection (Adequate countries): (full list tbc) Certain systems or databases we use are partially or entirely hosted outside the EEA in third countries that haven't been listed as Adequate (our accounting system; Xero). However, we have put in place the following appropriate measures to ensure that it is treated by those third parties in a way that is consistent with and which respects the EU and UK Data Protection Laws: (e.g. standard contractual clauses with Cloudflare, our website hosts). Contact our Privacy Lead to find out more.

Is my Personal Data secure?

We've implemented measures to prevent your Personal Data from accidental loss, unauthorised use, access, alteration or disclosure. We've implemented procedures and safeguards to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where legally required to do so. Details of these measures are available upon request.

How long will you use my Personal Data?

We will only retain your Personal Data for as long as necessary to fulfil the purposes we mentioned in our At-a-Glance table, including to satisfy any legal, accounting, or reporting requirements. This will vary according to the Personal Data involved and the purpose.

We consider the amount, nature, and sensitivity of the Personal Data, the potential risk of harm from unauthorised use or disclosure, the purposes for which we use it, whether we can achieve those purposes through other means, and the applicable legal requirements. To illustrate:

- We generally hold onto Financial Data for 7 years to satisfy tax and corporate reporting requirements
- We hold onto identifiable Marketing Data for 1 year post-campaign
- We retain our suppression lists (do-not-call/unsubscribe) because we have an ongoing legal obligation under Direct Marketing rules

In some circumstances we may aggregate or anonymise your Personal Data so that it can no longer be associated with you, in which case we may use it without further notice to you. We do this for purchasing statistics, historical operations data, or to analyse sales and marketing trends.

What rights do I have over my Personal Data?

You have various rights with respect to your Personal Data:

Right	What this means
Access	Receive a copy of the Personal Data we hold about you and confirm we're lawfully Processing it by making a Data Subject Access Request (DSAR). It's free of charge unless your request is clearly unfounded or excessive.
Rectification	Ask us to update, complete or correct your Personal Data at any time if you detect an inaccuracy. In fact, we encourage you to do so.
Portability	Get any Personal Data you've given us in electronic form on the basis of Consent or Contractual Necessity in a common machine-readable format. We can also transfer it to a third party if you ask

Right	What this means
Erasure	Ask us to delete or remove Personal Data where there is no good reason or Lawful Basis for us continuing to process it. You also have the right to ask us to delete or remove your Personal Data where you have exercised your right to Objection. We are allowed to refuse in certain circumstances. Find out more, at https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/
Objection	Object to any Processing we do based on Legitimate Interests. You also have the right to object where we are processing your Personal Data for direct marketing purposes
Automated processing	Not to be subject to automated decision-making without human intervention that has significant legal or other affects
Restriction	Suspend the Processing of some of your Personal Data, for example if you want us to establish its accuracy or the reason for processing it
Withdrawal of consent	Withdraw consent at any time and we will stop Processing it unless we have another legitimate basis for doing so in law. Where we rely on your consent we also explain how you can easily withdraw it

We will need to confirm your identity to confirm your right to access the information or exercise any of your other rights. This is to prevent Personal Data being disclosed to anyone who has no right to receive it.
You can find out more about your rights by visiting the Information Commissioner's Office website.

How can I make a complaint?

If you are unhappy with the way we handle your personal data, we encourage you to contact our Privacy Lead first so we can try to address your concerns. You may complain to the Information Commissioner's Office. You can find details here.

Glossary

Term	What is means
Data Subject	A living individual. We'll just say 'you', 'your' or 'individuals' in this Notice
Data Controller	The person or entity that decides what, how and why to Process Personal Data. We'll use 'we' 'our' and 'us,' since we're the Data Controller
Data Processor	The person or entity that Processes Personal Data on behalf of a Data Controller according to their instructions
Data Protection Law (DP Law)	The General Data Protection Regulation (GDPR), the UK Data Protection Act 2018 (DPA 2018), the Privacy and Electronic Communications Regulation 2003 (UK PECR), and other data protection legislation, as amended from time to time
Joint Controller	A person or entity that decides what, how and why to Process Personal Data jointly with another Data Controller
Process or Processing	Anything we do to Personal Data throughout its lifecycle: generating, scraping, collecting, sharing, storing, accessing, deleting, recording, organising – whether manually or using automation
Personal Data	Any information relating to an identifiable individual, even if we don't know their name. That means that any data that, alone or with other information, can be used to figure out who an individual is or to target or impact an individual – like location, IP address, ID number, image or voice, or identifiable cookies – is likely to be Personal Data. Even Personal Data that's been

Term	What is means
	'pseudonymised' (i.e. identifiers have been stripped away but the pseudonym could be reverse-engineered or linked back to the individual) is Personal Data. Unless data is truly anonymous, assume it's Personal Data
Special Data	Special categories of more sensitive Personal Data that requires a higher level of protection, such as information about a person's health or sexual orientation. Special Data is subject to more stringent safeguards, and we're only allowed to Process it in certain cases