HR PPL

INDEPENDENT HR CONSULTANCY · HRPPL.CO.UK

Privacy Policy

Last updated: 29 October 2026

1. Who I am

I am Natasha Butler, founder of HR PPL, an independent HR consultancy. I am the data controller for the personal information described in this policy, unless section 6 says otherwise.

Contact details

- Name: Natasha Butler, Founder, HR PPL
- Email: natasha@hrppl.co.uk
- Phone: 07733 996 072
- Website: hrppl.co.uk
- Postal address: 16 Austendyke Road, Weston Hills, Spalding, PE12 6BX

If you have any question about how I handle your information, please contact me using any of the details above. I handle all data protection queries myself.

2. What this policy covers

This policy explains what personal information I collect, why I collect it, what I do with it, how long I keep it, and what rights you have over it. It applies to:

- visitors to hrppl.co.uk
- people who contact me to enquire about my services
- clients and prospective clients, and the individual contacts within those businesses
- people who complete my HR Health Check or download other resources from my website
- people who subscribe to my emails
- suppliers, associates and other business contacts

It does not cover the personal information I handle **on behalf of** my clients when I am delivering HR services to them. Section 6 explains how that works and where to find the relevant information.

I follow the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations 2003 (PECR) as amended by the Data (Use and Access) Act 2025.

3. What information I collect

3.1 Information you give me directly

When you enquire about my services, by form, email, phone, LinkedIn or in person: your name, your job title, the name of your business, your email address, your phone number, and whatever you choose to tell me about your situation.

When you complete the HR Health Check: your email address, your name and business name if you provide them, and your answers to the questions in the tool. Your answers describe your organisation's HR position rather than you personally, but because they are linked to your email address I treat the whole record as personal information.

When you become a client: everything above, plus your business address, your billing contact details, your VAT number if you have one, the contract we agree, and the correspondence we exchange during the engagement.

When you subscribe to my emails or download a resource: your name and email address, and a record of your consent (the date, and the form or page you used).

When you apply to work with me as an associate or supplier: your contact details, your CV or profile, your qualifications, your insurance and your right to work information where relevant.

3.2 Information I collect automatically

When you visit hrppl.co.uk, my website and its underlying services may collect:

- your IP address
- your browser type and version, device type and operating system
- the pages you visit, how long you stay, and the site or search that brought you here
- the date and time of your visit
- information from cookies and similar technologies (see section 10)

3.3 Information from other sources

I may collect information about you from:

- your colleagues, if someone in your organisation refers you to me
- publicly available sources such as your company website, Companies House, or your LinkedIn profile, where I am researching a prospective client
- referral partners, where you have agreed to be introduced to me

3.4 Information I do not want

Please do not send me detailed information about an individual employee's health, disciplinary history, grievance or personal circumstances in an initial enquiry, before we have an agreement in place. If you need to describe a situation, please keep it general at that stage. If you do send me sensitive detail before we have contracted, I will store it securely and delete it if the enquiry does not proceed.

4. Why I use your information, and my lawful basis

Under the UK GDPR I must have a lawful basis for every use of your personal information. Mine are set out below.

What I do	Information used	Lawful basis
Respond to your enquiry and discuss whether I can help	Contact details, enquiry content	Legitimate interests (responding to a request I have received), or taking steps at your request before entering a contract
Prepare proposals, quotes and contracts	Contact and business details, enquiry content	Steps prior to a contract, at your request
Deliver the services we have agreed	All client information	Performance of a contract
Send you the results of your HR Health Check	Email address, your answers	Consent
Send you marketing emails, updates and HR insight	Name, email address, engagement history	Consent, or legitimate interests where you are an existing client and the content is about similar services (the PECR soft opt-in)
Invoice you, take payment and chase non-payment	Billing contact and transaction details	Performance of a contract, and legitimate interests in recovering sums owed
Keep accounting and tax records	Transaction records, invoices	Legal obligation
Keep records to defend a potential legal claim or support an insurance claim	Engagement records and correspondence	Legitimate interests (establishing, exercising or defending legal claims)
Maintain and secure the website, prevent fraud and abuse	Technical data, IP address	Legitimate interests in running a secure, working website
Understand how the website is used and improve it	Analytics data	Consent, where analytics cookies are used
Manage relationships with associates and suppliers	Contact and professional details	Contract, or legitimate interests

Where I rely on legitimate interests, I have considered whether my interest is overridden by your rights and concluded that it is not. You can ask me to explain that assessment, and you can object (see section 11).

5. Special category and criminal offence data

HR work sometimes involves particularly sensitive information, including health and disability information, trade union membership, information revealing race, religion or sexual orientation, and information about criminal allegations or convictions.

Most of the time I encounter this information as a **processor** acting for a client, which is covered in section 6.

Where I hold such information as a controller in my own right, for example inside my engagement file or my correspondence with a client, I rely on:

- **Article 9(2)(b) UK GDPR** and Schedule 1, Part 1, paragraph 1 of the Data Protection Act 2018, for information processed in connection with employment law obligations, and
- **Article 9(2)(f) UK GDPR** and Schedule 1, Part 2, paragraph 33 of the Data Protection Act 2018, where the information is needed to establish, exercise or defend a legal claim.

I have an appropriate policy document in place covering this processing, as the Data Protection Act 2018 requires. You can ask me for a copy.

I collect no more of this information than the work needs, I keep it separately from routine correspondence where I can, and I delete it on the timescales in section 9.

6. When I am a controller, and when I am a processor

This distinction matters, so I want to be plain about it.

I am the controller for information about you as a business contact: your enquiry, our negotiations, our contract, my invoices to you, and my marketing to you. I decide why and how that information is used, and this policy governs it.

I am a processor for the personal information about your employees, workers, applicants and former staff that you give me, or that I access on your systems, so that I can deliver HR services to you. Examples include employee files I review during a casework matter, absence records I look at during an audit, and staff data inside a Breathe HR system I help you configure.

In that situation:

- **you** are the controller, not me
- I act only on your documented instructions
- what I may do with the information is governed by the data processing terms in our contract, made under Article 28 of the UK GDPR, not by this policy
- if you are an employee of one of my clients and you want to know how your information is handled, please ask your employer for their privacy notice, and direct any rights request to them in the first

instance. If you contact me instead, I will pass your request to them promptly and tell you that I have done so.

7. Who I share your information with

I do not sell your personal information, and I do not share it for anyone else's marketing.

I share it with the following categories of recipient, only as far as each of them needs it:

Service providers who process information on my behalf

Provider	What they do	Where
Hostinger	Website hosting for hrppl.co.uk	United Kingdom
Brevo (Sendinblue)	Email marketing, HR Health Check results delivery, contact management	European Union (France)
Microsoft 365	Business email, file storage, calendar	United Kingdom
Breathe HR	HR software, where I help a client set it up or administer it	United Kingdom
Xero	Invoicing and accounts	United States, with some processing in New Zealand, under the safeguards in section 8
Google	Website analytics through Google Analytics, spam protection on my contact form through reCAPTCHA, and the typefaces my website is designed in through Google Fonts	United States, under the safeguards in section 8
Really Simple Plugins (Complianz)	Manages cookie consent on my website and generates my Cookie Policy. Receives my domain name and a list of the plugins my website uses	Netherlands
SEO Platform	Runs a script on my website in support of search engine optimisation	See section 8

Each of these is bound by a contract requiring them to keep your information secure and to use it only for the purpose I have set.

Professional advisers: my accountant, my insurers and insurance brokers, and my legal advisers, where there is a proper need.

Associates: if I bring in another HR professional to support a piece of work, they will see only what that work requires, and they are bound by confidentiality and data protection obligations.

Authorities and regulators: where I am required by law to disclose information, for example to HMRC, a court, the police, or the ICO.

A buyer: if I ever sell or transfer the business, your information may transfer with it, subject to the same protections.

8. Where your information is held

I aim to keep personal information within the UK and the European Economic Area.

Some of my suppliers may process information outside those areas. Where they do, I make sure a lawful safeguard is in place, which will normally be the UK International Data Transfer Agreement, or the EU Standard Contractual Clauses with the UK Addendum, or a UK adequacy regulation covering the destination country.

You can ask me for details of the safeguards that apply to a particular transfer.

9. How long I keep your information

Information	Retention period
Enquiries that do not become work	12 months from our last contact, then deleted
Client engagement records and correspondence	6 years from the end of the engagement, reflecting the limitation period for a contract claim
Employee data held on behalf of a client (processor role)	Returned or securely deleted within 30 days of the engagement ending, or as our contract specifies
Invoices, receipts and accounting records	6 complete financial years plus the current year, as HMRC requires
Marketing contacts and consent records	Until you unsubscribe or ask me to stop, and I review the list every 24 months and remove contacts who have not engaged
HR Health Check submissions	24 months, unless you become a client, in which case it joins the engagement record
Website analytics data	Event data is retained for 2 months and user data for 14 months, after which it is deleted. Aggregate reports remain available
Unsuccessful associate or supplier applications	6 months

When a retention period ends I delete the information securely, or anonymise it so it can no longer identify you.

10. Cookies and similar technologies

My website uses cookies and similar technologies, including browser local storage. A cookie is a small text file stored on your device.

Strictly necessary cookies keep the site working. They support security, page caching, load balancing and remembering the cookie choice you made. These do not need your consent and cannot be switched off.

Everything else is blocked until you agree to it. When you first visit, a banner asks you to accept or decline, and both options are equally available. If you decline, or if you ignore the banner, no analytics cookies are set. If your browser sends a Global Privacy Control or Do Not Track signal, I treat that as a decline and the banner does not appear.

You can change or withdraw your choice at any time using the **Cookie settings** link at the foot of every page, or by clearing cookies in your browser.

I use Google Analytics to understand how my website is used. It runs in Google Consent Mode, so until you accept, Google receives no cookies and no identifiers from your visit.

My **Cookie Policy**, linked at the foot of every page, lists every cookie my website sets, what each one does, who provides it and how long it lasts. It is kept current by an automated monthly scan of the live site.

Some pages load services supplied by Google. reCAPTCHA protects my contact form from automated abuse and is used only on that page. Google Fonts supplies the typefaces my website is designed in. My website also loads a script from SEO Platform, which supports search engine optimisation.

Most browsers let you block cookies entirely. If you block strictly necessary cookies, parts of the site may not work properly.

11. Your rights

Under the UK GDPR you have the right to:

- **be informed** about how your information is used, which is what this policy is for
- **access** a copy of the personal information I hold about you
- **rectification** of information that is inaccurate or incomplete
- **erasure** of your information, in certain circumstances
- **restrict processing** of your information, in certain circumstances
- **data portability**, meaning a copy of information you gave me in a common machine-readable format, where the processing is based on consent or contract and is automated
- **object to processing** based on legitimate interests. Where you object to direct marketing, I will stop, without exception and without needing a reason
- **withdraw consent** at any time, where I relied on consent. Withdrawing consent does not affect anything done before you withdrew it

- **not be subject to a decision based solely on automated processing** that produces a legal or similarly significant effect

To exercise any of these, contact me at natasha@hrppl.co.uk. I will respond within one month. If your request is complex I may extend that by up to two further months, and I will tell you if I do, and why. There is no charge, unless a request is manifestly unfounded or excessive.

I may ask you to confirm your identity before I act, so that I do not disclose your information to someone else.

If your request concerns information I hold as a processor for a client, section 6 explains what I will do.

12. Automated decision making

The HR Health Check produces an indicative score and a set of suggestions based on the answers you give. It is an informational tool, not a decision about you, and it has no legal or similarly significant effect. It does not determine whether I will work with you, and it is not a substitute for advice on your specific circumstances.

I do not carry out any other automated decision making or profiling.

13. Marketing

If you have consented, or if you are an existing client and the content concerns similar services, I may email you with HR updates, resources and information about what I offer.

Every marketing email includes an unsubscribe link, and you can also just reply and ask me to stop, or email natasha@hrppl.co.uk. I will action it promptly. I will keep a minimal record of your request so that I do not add you back by mistake.

14. Security

I take the security of your information seriously. The measures I use include encrypted connections to my website and email, access controls and strong authentication on the systems I use, encrypted storage on my devices, regular software updates, secure backups, and suppliers chosen partly on their security posture.

No system is completely secure, and I cannot guarantee the security of information sent to me over the internet. If a personal data breach happens and it is likely to risk your rights and freedoms, I will report it to the ICO within 72 hours of becoming aware of it, and I will tell you directly if the risk to you is high.

15. Children

My services are aimed at businesses, and my website is not directed at children. I do not knowingly collect information about anyone under 18 through this website. If you believe a child has given me their information, please contact me and I will delete it.

16. Links to other sites

My website may link to other websites, including LinkedIn, Facebook and Breathe HR. I am not responsible for the privacy practices of those sites, and this policy does not apply to them. Please read their own privacy notices before giving them your information.

17. Changes to this policy

I may update this policy from time to time, for example if I change the systems I use or the services I offer. The date at the top shows when I last changed it. If a change materially affects how I use your information, I will tell you directly where I can, and I will place a notice on my website.

18. How to complain

If you are unhappy with how I have handled your personal information, please tell me first at natasha@hrppl.co.uk, so that I have the chance to put it right.

You also have the right to complain to the Information Commissioner's Office at any time:

Information Commissioner's Office
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Helpline: 0303 123 1113
Website: ico.org.uk/make-a-complaint