Privacy Policy for Professional Passport Fortis

Last Updated: 17/09/25

1. Introduction

Professional Passport Shield Ltd ("we", "us", "our") is committed to protecting and respecting your privacy. This Privacy Policy explains how we collect, use, disclose, and protect the personal data of:

· Our clients (the businesses that use our payroll services);

· Our clients' employees whose data we process to provide the payroll service; and

· Visitors to our website, htps://fortis.professionalpassport.com.

We are registered in England and Wales under company number 16656701 and our registered office is at 8 The Manor, Shinfield, Reading, England, RG2 9DP

This policy sets out the basis on which any personal data we process is handled. Please read it carefully.

2. Data Controller and Data Processor

Understanding our role is crucial under UK data protection law:

· For our Client's employees: When we process employee data (e.g., names, salaries, bank details) to run payroll on our Client's behalf, the Client is the Data Controller. They determine the "why" and "how" of the processing. We are the Data Processor, acting on their documented instructions. This relationship is governed by our Data Processing Addendum (DPA), which forms part of our Terms and Conditions.

· For our Client data and website visitors: For the personal data of our clients (business contacts) and visitors to our website, we are the Data Controller.

3. Information We Collect and How We Use It

Data Category What we collect Lawful Basis for Processing Purpose of Processing

Client Employee Data (Processed as a Processor) Name, address, date of birth, NI number, salary, bank details, tax code, pension contributions, leave, sickness. Necessary for the performance of a contract (between us and our Client) and to comply with legal obligations (e.g., HMRC reporting). To calculate pay, deductions, and taxes; to generate payslips; to submit RTI filings to HMRC; to administer pension contributions.

Client Business Data (Controller) Business name, business address, client contact name, email, phone number, financial information for billing. Performance of a contract (to provide our services to you) and legitimate interests (for account management and service updates). To set up your account, provide customer support, invoice for services, and manage our relationship.

Website Visitor Data (Controller) IP address, browser type, device information, pages visited (via cookies). See our Cookie Policy. Consent (for non-essential cookies) and legitimate interests (for essential website operation and security). To improve our website experience, analyse traffic, and ensure network and information security.

Marketing Data (Controller) Name, business email address, company name. Consent (for direct marketing emails) or legitimate interests (for sending relevant business-to-business marketing). To send you marketing communications about our services, events, and industry news. You can opt-out at any time.

4. How We Share Your Personal Data

We may share personal data with the following third parties:

· HMRC: We are legally obligated to submit payroll data to HMRC under the Real Time Information (RTI) regime.

· Pension Providers: To facilitate auto-enrolment pension contributions, as instructed by you.

· Sub-processors: We use trusted third-party service providers who help us deliver our services (e.g., cloud hosting providers, email communication services, support ticketing systems). These sub-processors are subject to strict data processing agreements and cannot use your data for their own purposes.

· Professional Advisers: Such as accountants, lawyers, and consultants where necessary.

· Law Enforcement or Regulatory Bodies: Where we are required to do so by law.

We will never sell your personal data.

5. International Transfers

We primarily store and process data within the UK and European Economic Area (EEA). If we ever need to transfer personal data outside the UK/EEA (e.g., if a sub-processor uses servers in the USA), we will ensure a valid transfer mechanism is in place as required by UK law, such as:

· The UK International Data Transfer Agreement (IDTA) or Addendum.

· Transfers to countries deemed by the UK to provide an adequate level of data protection.

6. Data Security

We have implemented robust technical and organisational measures to protect your personal data from accidental loss, unauthorised access, use, alteration, or disclosure. These include encryption, secure access controls, and regular security testing.

7. Data Retention

· Client Employee Data: We will retain this data only for as long as necessary to provide the payroll services and to fulfil our legal and regulatory obligations (HMRC requires payroll records to be kept for a minimum of 3 years from the end of the tax year they relate to, but often 6+ years is recommended). Upon termination of our contract with a Client, we will delete or return all data in accordance with our DPA and our data retention schedule.

· Client Data: We will retain this for as long as you have an account with us and for a period afterwards to comply with legal obligations (e.g., financial records) and for legitimate business purposes (e.g., resolving disputes).

8. Your Data Protection Rights

Under UK data protection law, you have rights, including:

· The right to access – You have the right to request copies of your personal data.

· The right to rectification – You have the right to request correction of inaccurate information.

· The right to erasure – You have the right to request that we erase your personal data, under certain conditions.

· The right to restrict processing – You have the right to request the restriction of processing your personal data, under certain conditions.

· The right to data portability – You have the right to request the transfer of your data to another organisation, or to you, under certain conditions.

· The right to object to processing – You have the right to object to our processing of your personal data, under certain conditions.

· Rights in relation to automated decision making and profiling.

How to exercise your rights:

· If you are a Client or Website Visitor: Please contact us using the details in Section 10.

· If you are an Employee of a Client: You should first contact your employer (the Data Controller). They are responsible for responding to your requests. We will support our Clients as the Data Processor in fulfilling these obligations.

We will respond to any valid request within one month.

9. How to Complain

If you have any concerns about our use of your personal data, please contact us first so we can try to resolve the issue.

You also have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO.

10. Contact Us

To exercise your rights, ask questions, or raise concerns about this policy, contact our Data Protection Officer (DPO) or designated privacy manager at:

Email:support@yprofessionalpassport.com] Post: The Data Protection Officer, 8 The Manor, Shinfield, Reading, England, RG2 9DP

11. Changes to this Privacy Policy

We may update this policy from time to time. The latest version will always be posted on our website. We will notify our Clients of any material changes that affect how we process data.