Data Protection Policy

1. Purpose

This policy sets out the Umbrella Paraplus approach to data protection in accordance with the Data Protection Act (DPA) 1998 and the updated requirements of the General Data Protection Regulations (GDPR) with effect from May 2018. Where other relevant legislation applies, this is referred to in the in the summary table (section 7).

2. Format of Policy

The narrative of the policy highlights the requirements on us as a business in relation to managing personal data and specifically in relation to the storage, retention and destruction of personal and other confidential data.

3. What the Law Says

For the purposes of data retention our approach is to comply with the requirements of the GDPR from the time of implementing this policy, which assumes compliance with the existing terms of the DPA 1998.

Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

4. **Our Privacy Principles**

We will:

- Process personal data lawfully, fairly and transparently
- Only collect personal data for specified, explicit and legitimate purposes
- Limit the collection and retention of personal data to what is adequate, relevant and necessary
- Ensure the data accurate and kept up to date where necessary
- Keep the data for no longer than is necessary where data subjects are identifiable
- Process it securely and protect against accidental loss, destruction or damage.

5. General Responsibilities

As a data controller, Umbrella Paraplus is committed to acting responsibly where there is a requirement to retain, share or destroy personal data and wherever possible, to only retaining data where there is a business need to do so. We have conducted an in-depth review of data types and current practices across the business as the starting point for this policy.

It is the responsibility of all Umbrella Paraplus managers, employees and contractors who access personal data to familiarise themselves with this policy and to adhere to its requirements.

Any queries in relation to data retention should be directed to our appointed Data Protection Officer.

6. Data Retention

The table below details the nature of data held and the rationale for holding the data, together with our retention period. Where the retention period is dictated by law, the relevant legislation is referenced. Where there is no associated legislation, the table details the rationale for the retention period identified. At the end of the retention period the electronic pack or paper record falling into the appropriate date range is marked for destruction on relevant date. Upon destruction date electronic file is deleted, paper record is shredded.

7. Data Retention Summary Table

Item	Details (including but not exhaustive)	Method of collection/retention	Legal requirement (or recommendation) for retention and destruction	Source
Candidate Registration Pack	CVs, application forms, right to work documentation, referee names and contact details, Marriage certificates, change of name deeds, Civil Partnership Certificate, National Insurance Number, Date of Birth, Address, Bank details, Mobile and home contact numbers, email address, mode of transport, place of work, job title, rate of pay. Shift type. Utility bills, DWP/JCP correspondence	Collected by Recruitment Agency. Received by email at Paraplus direct from Recruitment Agency or candidate. Stored by Paraplus electronically	To be kept for at least a year from their creation and at least 6 years from when services were last used.	Conduct of Employment Agencies and Employment Businesses Regulations 2003 Recommended based on statute of limitations on civil claims
Wage/Salary records	Overtime, bonus, expenses, statutory payments or deductions including Workplace	Electronic through payroll via etips, Able, Robot Paper* files held off site in storage facility Chaffinch	6 years	Taxes Management Act 1970

	Pension and attachment of earnings information Timesheets P45, P60, P11			
National Minimum Wage records	Individual pay records Timesheets Checking records	Electronic through payroll via etips, Able, Robot Paper* files held off site in storage facility Chaffinch	Must be kept for 3 years from the end of the tax year in which they apply.	National Minimum Wage Act 1998
Records relating to Working Time	Individual record of hours worked timesheets	Electronic through Paraplus Portal, CRM and payroll via etips, Able, Robot Paper* files held off site in storage facility Chaffinch	6 years	The Working Time Regulations 1998 (SI 1998/1833) Taxes Management Act 1970
Records relating to Notice served to terminate Employment Contract	Individual record of notice served and reason	Electronic copies of correspondence stored in Paraplus shared drive.	2 years after employment ceases	Conduct of Employment Agencies and Employment Businesses Regulations 2003 Recommended based on statute of limitations on civil claims
Employee details - Performance and Development data	Disciplinary, performance improvement, capability, promotion interviews Grievance records ACAS enquiries and correspondence Solicitor correspondence	Electronic through Paraplus CRM, email, server shared drive.	6 years after employment ceases	Recommended based on statute of limitations on civil claims

	Third Party Reference requests			
Training records	Record of courses and other training completed, exam results, certificates	Electronic through Paraplus CRM, email, server shared drive.	6 years after employment ceases	Recommended based on statute of limitations on civil claims
Sickness records	Doctors fit notes, occupational health reports, specialist reports, return to work forms, hospital/consultant correspondence/reports Death Certificate	Electronic through Paraplus CRM, email, server shared drive.	6 years after employment ceases	Recommended based on statute of limitations on civil claims
Medical records (dependent on relevant act)	Occupational health reports, specialist reports, GP reports Death certificates	Electronic through Paraplus CRM, email, server shared drive.	40 years from date of issue	COSHH Control of Lead at Work Control of Asbestos at Work
Accident Book and reports. RIDDOR reports	Record of work based accidents or incidents Police Report Death Certificate Witness Statements Solicitor letters	Electronic through Paraplus CRM, email, server shared drive.	3 years from entry date	(RIDDOR) (SI 1995/3163)
Statutory Maternity Pay records	MATB1 and other forms, planned leave and expected dates, appointment details, pregnancy related	Provision of medical practitioner/hospital forms, face to face, electronic through Paraplus CRM, email, server shared drive.	3 years from end of tax year in which pay was received	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960)

	sickness records, pay entitlements			
Statutory Sick Pay records	Name, pay rate, sick pay entitlement, amount of time off, nature of absence GP letter, hosp/consultant correspondence	Electronic through Paraplus CRM, email, server shared drive.	At least 3 months after sickness but 6 years recommended	CIPD

8. Data Destruction

Where we process or control personal data, we will retain it only for as long as it is required for the purposes agreed.

If a data subject requests the deletion or removal of personal data (the right to be forgotten) (other than in some specific circumstances), then the data relating to that individual will be destroyed.

In any event, if the data is no longer required, it will be securely destroyed in accordance with the retention periods set out in the table in section 7.

Individual departments have appropriate processes in place to ensure that they regularly review data they hold so that it is not held for longer than is required and is destroyed in a confidential, secure way when it is no longer required or when requested.

9. Data Breach Process

All potential personal data breaches MUST be reported IMMEDIATELY to the Data Protection Officer.

Umbrella Paraplus as Data Controller

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

The Data Protection Officer will review the potential breach and assess the likelihood and severity of the resulting risk to people's rights and freedoms.

If it is likely there is such a risk, the Data Protection Officer will notify the Information Commissioners Office (https://ico.org.uk/for-organisations/report-a-breach/) within 72 hours being notified of the breach.

If it is likely that there is a risk to a person's rights or freedoms, the Data Protection Officer will inform the individual.

The Data Protection Officer will lead any internal investigation required, supported by appropriate senior managers as required.

A central record of any potential breaches, the process followed and their outcome, including whether individuals and the ICO were informed, will be maintained.

10. Non-compliance with this policy

Breaches of the requirements for handling personal data can have serious ramifications for the business, including reputational damage and potentially significant financial cost.

As a result, failure to comply with the requirements is likely to be investigated and may result in disciplinary action being taken under the Company's Disciplinary Policy.

Employees who wish to raise a concern should do so initially with their line manager or the Data Protection Officer.

In the unlikely event that an employee does not wish to make their concern known through these channels, a complaint may be made through the Company's Whistleblowing Policy.

11. Useful Sources & Links

For further detail on the Data Protection Act 1998 and the General Data Protection Regulations 2018 visit The Information Commissioner's Office: https://ico.org.uk/

DOCUMENT CONTROL:

Policy/Procedure title:	*Data Protection Policy (Paraplus)*	**Date released:**	
Version number:	*V0.4*	**Replaces:**	
Policy owner:	*Data Protection Officer*	**Related documents:**	*Data Protection Policy (Employer)* *Data Protection Policy (e-tips)*