

## **1. Introduction & Identity**

**M.D. ADVISORY SERVICES LTD** (“we”, “us”, “our”) is committed to protecting the privacy and security of your personal data. This Privacy Notice explains how we collect, use, share, and retain your personal data when you interact with us through this website or otherwise.

This notice is provided in accordance with data protection law in the United Kingdom, including the **UK GDPR** and the **Data Protection Act 2018**.

**Controller:**

**M.D. ADVISORY SERVICES LTD**

26 Mosley Street, Newcastle Upon Tyne, England, NE1 1DF

**Email:**

(for both Heads HR and Sapphire HR) [info@sapphire-hr.co.uk](mailto:info@sapphire-hr.co.uk)

**Phone:** 0330 124 3732

## **2. What Personal Data We Collect and How We Use It.**

We may collect and process personal data about you, as either a Data Controller or Data Processor.

Where we act as a Data Processor on behalf of a Data Controller we;

- Process data **only on documented instructions** from the client (the controller)
- Implement **appropriate technical and organisational security measures**
- Assist the controller with **data subject rights**, DPIAs, and breach management
- Ensure **confidentiality**, staff training, and sub-processor controls
- Delete or return personal data as appropriate and in accordance with data protection law at the end of the contract

We may process the following data on behalf of the Controller as a Data Processor;

### **Employee identification & contact data**

Processed to administer HR services on behalf of the client.

- Name (including previous names)
- Date of birth
- Home address
- Personal and work email addresses
- Telephone numbers
- Employee ID numbers
- National Insurance number
- Right-to-work documentation

### **Employment & contractual information**

Used to support HR administration and employment lifecycle management.

- Job title, role, department
- Start date, end date, probation information
- Employment contracts and amendments
- Working hours and patterns
- Salary, pay reviews, bonuses (where applicable)
- Notice periods

### **Payroll & financial data**

Processed only where payroll or pay-related support is provided.

- Bank account details
- Salary and payment records
- Tax codes and PAYE information
- Pension contributions and auto-enrolment data
- Expenses and benefits information

**Special category data (where necessary)**

Handled with enhanced safeguards and only where lawful.

- Health information (e.g. sickness absence, fit notes, occupational health reports)
- Disability and reasonable adjustment information
- Maternity, paternity, adoption and parental leave data
- Trade union membership (where relevant)
- Equality, diversity and inclusion data (e.g. ethnicity, gender identity, sexual orientation)

**Performance & conduct information**

Used to support HR advice and employee relations processes.

- Appraisals and performance reviews
- Disciplinary and grievance records
- Investigation notes and outcomes
- Capability and absence management records

**Recruitment & onboarding data**

Processed when supporting hiring on behalf of clients.

- CVs and application forms
- Interview notes and assessments
- References
- Right-to-work checks
- Pre-employment screening results (e.g. DBS checks where applicable)

**Training & development records**

Used to support workforce development.

- Training attendance and completion records
- Professional qualifications and certifications
- Continuing professional development (CPD) records

**System & technical data**

Generated when providing HR systems or platforms.

- User account details and login credentials
- Audit logs and system activity records
- Access permissions and role-based controls
- IP addresses and device identifiers (where applicable)

**Communications data**

Processed when handling HR-related correspondence.

- Emails and written correspondence
- Call recordings or meeting notes (where used)
- Internal HR case notes

**Data relating to other individuals**

Occasionally processed in the context of HR matters.

- Emergency contact details
- Next of kin information
- Witness statements
- Referee details

Where we act as a Data Controller, we process your personal data for the following purposes:

- To respond to enquiries you submit to us
- To provide services you request
- To improve our website and services
- To send you marketing communications where you have consented
- For compliance with legal obligations, fraud prevention and to protect our rights.

### 3. Lawful Bases for Processing

We rely on one or more of the following lawful bases:

- Your **consent** (e.g., for marketing and cookies)
- **Contract performance** (to fulfil your request)
- **Legal obligation** (e.g., compliance with statutory requirements)
- Our **legitimate interests** (e.g., improving services, analytics), provided such interests do not override your rights.

### 4. Sharing Your Data

We may share your personal data with:

- Service providers acting on our behalf (e.g., IT, analytics, email systems)
- Legal and regulatory authorities where required by law
- In accordance with instructions from the Data Controller.

### 5. International Transfers

Where we transfer personal data outside the UK, we ensure appropriate safeguards are in place in line with UK GDPR requirements.

### 8. Data Retention

We retain personal data only for as long as necessary for the purposes for which it was collected, in line with our retention schedules and legal obligations. Please see our retention schedule below;

Purpose	Data category	Examples	Retention period	Lawful basis	Disposal method
Client relationship & business administration (Controller role)	Client contact details	Names, job titles, work emails, phone numbers	Contract duration + 6 years	Contract, legitimate interests	Secure deletion
Client relationship & business administration (Controller role)	Contracts & DPAs	Service agreements, DPAs	6 years from contract end	Legal obligation	Secure deletion
Client relationship & business administration (Controller role)	Invoices & financial records	Billing records, payment history	6 years	Legal obligation (HMRC)	Secure deletion
HR advice line & case management records (Processor role)	HR advice case files	Call notes, emails, summaries	6 years from case closure (unless client instructs otherwise)	Contract	Secure deletion
HR advice line & case management records (Processor role)	Investigation records	Disciplinary/grievance reports	As instructed by client	Contract	Secure deletion
HR advice line & case management records (Processor role)	Outcome summaries	Recommendations, reports	As instructed by client	Contract	Secure deletion
Purpose	Data category	Examples	Retention period	Lawful basis	Disposal method
Employee personal data (processed on behalf of clients)	Core employment data	Contracts, job roles, dates	As instructed by client	Contract	Secure deletion
Employee personal data (processed on behalf of clients)	Payroll-related data	Salary details, bank info	As instructed by client	Contract	Secure deletion
Employee personal data (processed on behalf of clients)	Absence records	Sickness, maternity, leave	As instructed by client	Contract	Secure deletion
Employee personal data (processed on behalf of clients)	Performance records	Appraisals, reviews	As instructed by client	Contract	Secure deletion
Special category data (Processor role)	Health data	Fit notes, OH reports	As instructed by client	Contract	Secure deletion
Special category data (Processor role)	Equality data	Ethnicity, gender	As instructed by client	Contract	Secure deletion
Special category data (Processor role)	Trade union data	Membership info	As instructed by client	Contract	Secure deletion
Recruitment support data (Processor role)	Unsuccessful candidates	CVs, interview notes	Up to 12 months unless client instructs otherwise	Contract	Secure deletion
Recruitment support data (Processor role)	Successful candidates	Recruitment records	As instructed by client	Contract	Secure deletion
Recruitment support data (Processor role)	Right-to-work checks	ID documents	As instructed by client	Contract	Secure deletion
Website enquiries & marketing data (Controller role)	Website enquiries	Contact forms, emails	12 months	Legitimate interests	Secure deletion
Website enquiries & marketing data (Controller role)	Marketing contacts	Mailing lists	Until consent withdrawn or 24 months inactivity	Consent	Secure deletion
Website enquiries & marketing data (Controller role)	Analytics data	IP addresses, usage data	14-26 months	Legitimate interests	Automatic deletion
IT systems, logs & security data	System access logs	Login records, audit logs	12 months	Legitimate interests	Automatic deletion
IT systems, logs & security data	Backups	Encrypted backups	Rolling 30-90 days	Legitimate interests	Automatic overwrite
IT systems, logs & security data	Incident records	Security/data incidents	6 years	Legitimate interests	Secure deletion
End of client contract	Client personal data	Return or delete	Within 30-90 days	Contract	Secure deletion
End of client contract	Backup data	Removed via backup rotation	Within 90 days	Contract	Secure deletion
End of client contract	Confirmation	Deletion confirmation provided on request	N/A	N/A	N/A

### 9. Your Rights

Under UK data protection law, you have the following rights:

- The right to access personal data held about them (the right of subject access);
- The right to be informed about how and why their data is
- The rights to have their data rectified, erased or restricted;
- The right to object;
- The right to portability of their data; and
- The right not to be subject to a decision based solely on automated processing.
- The right to complain

To exercise these rights, for both Heads HR and Sapphire HR, please contact us at [info@sapphire-hr.co.uk](mailto:info@sapphire-hr.co.uk). For more information about your rights, you can also visit <https://ico.org.uk/for-the-public/>

### 10. Security

We implement appropriate technical and organisational measures to safeguard your personal data against unauthorised access, loss, or alteration.

### 11. Complaints

If you have concerns about how your data is being used, you can contact us in the first instance, and we will respond in line with our process for data privacy complaints. If you remain unsatisfied you can contact the ICO.

<https://ico.org.uk/for-the-public/how-to-make-a-data-protection-complaint/>

### 12. Changes to This Notice

We may update this Privacy Notice from time to time. Updated versions will be published on our website. Last updated on 22/06/26