

SMART MANUFACTURING TECHNOLOGY

PRIVACY NOTICE

(INTERNAL)

Published 17th October 2025

CONTACT DETAILS

Contact: Privacy Team

Address: 1 Clifton Lane, Wilford, Nottingham, NG11 7AT

E-mail: privacy@smartmt.com

Website: smartmt.com

INTRODUCTION

We are Smart Manufacturing Technology (SMT), a global engineering solutions and services provider dedicated to providing leading engineers with the expertise and tools to deliver innovative powertrain technology. Our Head Office is in Nottingham, UK. SMT maintain registration with the Information Commissioners Office (ICO).

This notice explains how we collect and use personal data during the employment and engagement lifecycle (recruitment and assessment, onboarding, employment or contracting, benefits and payroll, learning and development, IT security operations, premises security including CCTV) for employees, contractors, and candidates. It does not cover customers, prospects, website visitors or suppliers, see our External Privacy Notice for those audiences.

Your privacy, and the security of your information is a responsibility that SMT takes seriously. We understand our responsibility to ensure that any personal data that we collect, store, use or otherwise handle, is processed in accordance with applicable data protection legislation.

THE TYPE OF PERSONAL DATA WE COLLECT

At SMT we only collect the personal data necessary to provide our services, protect and enforce our intellectual property rights, and to undertake necessary internal business functions such as recruitment or human resources management.

We need to keep records of engagements with our business and website, as well as basic contact details to inform our interactions with customers, candidates, and service partners.

The personal data that we collect includes

(Note this list is non-exhaustive and is provided only for example)

- **Identifiers & contact information:** names (including usernames/hostnames), addresses (home and email), phone numbers, date of birth, signatures, as well as personal identifiers such as location and network data associated with the use of corporate devices.
- **Employment & background:** CV, education and work history, references, right-to-work and ID documents, professional memberships.
- **Payroll & benefits:** bank details and other payroll information, pension and benefits selections.
- **Security & premises:** photography and CCTV footage.
- **Travel & driving:** driving licence and eligibility, visa and vaccination status required for business travel.
- **Special category data** (where relevant and permitted): health data (e.g.: sick notes), and equality monitoring data (e.g.: gender, race, religion) collected for statutory reporting or inclusivity initiatives.

This list is non-exhaustive, and we may, where deemed necessary and appropriate to our relationship, collect further personal data from you, people you know, or third parties that you identify to us.

HOW WE GET THE PERSONAL DATA AND WHY WE HAVE IT

Most of the personal data that we process is provided to us directly by you during recruitment, onboarding and throughout your engagement.

We also receive personal data indirectly from third parties including:

Recruitment agencies – relating to employment opportunities.

Universities – relating to employment opportunities and research projects.

Referring partners – where you partner with companies to refer your details to us for services, employment, or other business or research opportunities.

Your employer(s) – in the case of references, or service introductions and referrals.

Education providers, accreditation, and qualification bodies – in the case of references, training and development opportunities and applications for funding relating to training and development opportunities.

We use this data for the following purposes:

Recruitment & onboarding: assessing suitability, verifying identity and right-to-work, processing offers and contracts.

Employment/contractor administration: payroll, pensions, benefits, performance and progression, learning & development, Health & Safety, and internal record-keeping.

IT & security operations: identity and access management, device and network administration, safeguarding of systems and data, and premises security.

Legal & regulatory obligations: tax, employment and workplace legislation, and responding to lawful requests.

THE LAWFUL BASES WE RELY ON FOR PROCESSING PERSONAL DATA ARE:

We rely on one or more of the following lawful bases, as appropriate to each activity:

(a) Your consent.

Only where requested for optional processing, you can remove your consent at any time by contacting privacy@smartmt.com

(b) We have a contractual obligation.

To enter into or perform your employment or engagement

(c) We have a legal obligation.

E.g.: tax, employment, health & safety

(d) We have a legitimate interest.

E.g.: IT and information security, internal record-keeping, proportionate monitoring of systems and premises

(e) We have a vital interest.

It is unlikely that SMT will rely on the lawful basis relating to vital interests to process your personal data. SMT only relies on vital interest as a lawful basis where the sharing of information is necessary to protect someone's life, or to avoid significant harm to life, in an emergency.

Public tasks: SMT does not rely on the lawful basis relating to public tasks as we do not process personal data in the exercise of official authority or to perform public interest tasks set out in law.

Special category data: we rely on one or more additional conditions under UK GDPR Article 9 and the Data Protection Act 2018, such as employment, social security and social protection law, occupational health, equality of opportunity monitoring, or establishment, exercise or defence of legal claims. For such we limit access and apply additional safeguards.

WHERE NECESSARY AND APPROPRIATE, WE MAY SHARE THIS INFORMATION WITH:

We share data only where necessary and with appropriate safeguards. Typical recipients include:

- **HR/people services:** banks, accountants, outsourced payroll, pension and employee-benefits providers, HRIS provider, outsourced Health & Safety consultancy, outsourced staffing recruitment providers, and quality management consultancy.
- **IT and information security providers:** e.g., Microsoft and outsourced IT and Security solutions partners, including CCTV monitoring providers.
- **Professional/insurance services:** consultants and advisors, auditors, certification bodies, and insurers.
- **Legal and regulatory authorities:** law enforcement, tax authorities, courts and regulators when required by law.

- **Corporate transactions:** prospective buyers and their agents in the context of a business sale or reorganisation.

When sharing your personal data, we may have need to transfer it outside of the country of collection, this may mean transferring the information outside of the UK, or outside of the EEA, this may be to third countries, or to countries with no adequacy agreement in place.

Where a service provider stores or processes data outside the UK or EEA, we ensure appropriate safeguards (e.g., ICO-approved Standard Contractual Clauses/International Data Transfer Agreement and risk assessments) to afford an adequate level of protection.

HOW WE STORE YOUR PERSONAL DATA

We apply technical and organisational measures, including strong encryption and secure disposal of data storage media (to recognised industry standards) prior to reuse or recycling. Physical records are securely destroyed.

Physical and electronic records shall be retained for the following periods at the end of which they are securely disposed of, or put beyond use:

- **All HR records (candidates, employees & contractors)** – Held in line with the statutory and non-statutory retention periods published by the CIPD. <https://www.cipd.org/uk/knowledge/factsheets/keeping-records-factsheet>.
- **Financial documents, Timesheets, and attendance records** – 6 years from the end of the current financial year in line with the HMRC records retention guidance.
- **Insurance records** – 40 years from the date the document or electronic record was created.
- **Photographs and filmed footage, including CCTV footage** - kept for 30 days unless they are required for a criminal investigation as outlined in the retention schedule
- All physical records containing personal data are disposed of by secure information disposal methods in line with applicable standards and regulations.
- All data storage media (hard drives / USB drives / disks etc.) are wiped, and factory reset prior to internal reuse of any associated device and are wiped to recognised industry standards, or permanently destroyed, prior to external recycling or sale of any associated device.
- Archived records clearly display the scheduled destruction date.

DATA SUBJECT RIGHTS

Under data protection law, data subjects have rights including:

Your right of access – You have the right to ask us for copies of your personal data.

Your right to rectification – You have the right to ask us to rectify personal data you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure – You have the right to ask us to erase your personal data in certain circumstances.

Your right to restriction of processing – You have the right to ask us to restrict the processing of your personal data in certain circumstances.

Your right to object to processing – You have the right to object to the processing of your personal data in certain circumstances.

Your right to data portability – You have the right to ask that we transfer the personal data you gave us to another organisation, or to you, in certain circumstances.

Please note that the rights available to you are subject to the lawful basis for processing your data, for example if you have provided your consent, you cannot object to that consent, however, you do have a right to withdraw consent.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you. Please contact us at privacy@smartmt.com if you wish to exercise your data subject rights.

CHANGES TO THIS NOTICE

We may update this notice from time to time and will make the most recent version available on our website.

HOW TO COMPLAIN

If you have any concerns about our use of your personal data, you can make a complaint to us at:

Privacy Team, Smart Manufacturing Technology Ltd

1 Clifton Lane, Wilford

Nottingham, NG11 7AT

Email: privacy@smartmt.com

SMT take your privacy seriously and invite you to raise any concerns to us directly in the first instance, to allow us the opportunity to advise, and where necessary, perform any relevant investigations.

You have the right to complain directly to the ICO if you have concerns with how we are processing your personal data.

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Helpline number: 0303 123 1113

ICO website: <https://www.ico.org.uk>