

Legal entity	Thistle Design (MMC) Limited
Registered / business address	40 Dryden Road, Bilston Glen, Loanhead, Midlothian EH20 9LZ, United Kingdom
Privacy contact	sales@thistleprecision.com
Website	https://www.thistleprecision.com/

Last updated: 8 September 2026

I. Overview

This Privacy Policy explains how Thistle Design (MMC) Limited ("Company," "we," "us," or "our") collects, uses, discloses, retains, and protects Personal Data when you visit our website, communicate with us, purchase or inquire about our products or services, attend an event, apply for employment, or otherwise interact with us.

This Policy is designed as a UK-established, global privacy notice and is intended to address the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (as amended), including amendments in force under the Data (Use and Access) Act 2025, and the Privacy and Electronic Communications Regulations 2003 (PECR). It also addresses the EU General Data Protection Regulation (EU GDPR) where the EU GDPR applies to our processing.

Our customers and business contacts are predominantly in the United Kingdom, European Union/European Economic Area (EU/EEA), and United States, with additional global customers. We primarily provide products and services to businesses rather than to individuals acting in a personal capacity. The law applicable to a particular processing activity depends on the nature of the processing, the location of the individual, and the territorial scope of the applicable law.

II. Who We Are and Scope

Controller: Thistle Design (MMC) Limited

Address: 40 Dryden Road, Bilston Glen, Loanhead, Midlothian EH20 9LZ, United Kingdom

Privacy contact: sales@thistleprecision.com

Website: <https://www.thistleprecision.com/>

Where an affiliate operates a separate website, service, or activity and acts as an independent controller, that affiliate may provide its own privacy notice. Where an affiliate processes Personal Data on our behalf, the affiliate or other provider will act as a processor subject to appropriate contractual, confidentiality, privacy, and security requirements.

III. UK and EU Territorial Scope

UK GDPR applies to processing carried out by the Company as a controller or processor where UK data-protection law applies, including processing connected with the Company's UK establishment. EU GDPR may also apply where its territorial scope is met, including where a non-EU-established organisation intentionally offers goods or services to individuals in the EU/EEA or monitors their behaviour there.

Where EU GDPR applies, the Company will comply with the requirements applicable to that processing, including transparency, lawful bases, data-subject rights, security, records, processor, personal-data breach, international-transfer, and supervisory-authority requirements.

The Company primarily operates on a B2B basis. EU GDPR Article 3(2) will nevertheless be assessed whenever processing is intentionally directed to individuals in the EU/EEA through an offer of goods or services or through monitoring of behaviour. The existence of EU/EEA business customers alone does not automatically determine the Article 3(2) outcome.

EU representative status: No EU representative is currently designated based on the Company's present documented processing profile. This status will be reassessed whenever an activity may trigger EU GDPR Article 3(2). If Article 27 applies, the representative will be designated and the applicable privacy information will be updated.

Trigger Conditions

The following triggers determine when the principal UK/EU privacy requirements described in this Policy apply. The Company will assess the trigger when a new website, service, customer activity, processing activity, technology, marketing campaign, transfer, or other material change is introduced.

- **UK GDPR** - Triggered because the Company is established and operates in the United Kingdom. UK GDPR applies to processing connected with the activities of the Company's UK establishment, including processing carried out outside the UK where it is linked to that UK establishment.
- **EU GDPR - Offer of goods/services:** Triggered for processing related to an intentional offer of goods or services to individuals who are in the EU/EEA. The mere fact that a customer or business partner is incorporated or located in the EU/EEA, or that the Company's website is accessible there, does not by itself establish an Article 3(2) offer; the Company must consider whether the activity is intentionally directed to individuals in the EU/EEA.
- **EU GDPR - Monitoring:** Triggered for processing related to monitoring the behaviour of individuals while they are in the EU/EEA. Examples may include systematic tracking, profiling, or behavioural monitoring through cookies, analytics, advertising technologies, or similar tools where the monitoring is directed to individuals in the EU/EEA.
- **EU GDPR Article 27 representative:** Triggered when EU GDPR Article 3(2) applies and the Company does not qualify for the Article 27(2) exemption. The exemption must be supported by a documented assessment that the processing is occasional, does not involve large-scale special-category or criminal-offence data, and is unlikely to result in a risk to individuals' rights and freedoms. Because regular customer or business operations may be recurring, this assessment will be made for the actual processing activity rather than assumed from the Company's B2B model.
- **UK PECR - Cookies and similar technologies:** Triggered when the Company stores information on, or gains access to information already stored on, a user's device in the UK. Consent is required unless a specific PECR exception applies, including the limited exception for technologies that are strictly necessary to provide a service requested by the user or another applicable statutory exception. Where Personal Data is processed, the applicable UK GDPR requirements also apply.
- **EU/EEA e-privacy rules - Cookies and electronic marketing:** Triggered when cookies, similar technologies, or electronic direct marketing are directed to users or recipients in an EU/EEA Member State. The Company will assess the applicable Member State e-privacy rules before deploying non-essential tracking, behavioural advertising, or electronic marketing to EU/EEA recipients. EU GDPR requirements may also apply where the underlying processing falls within EU GDPR territorial scope.
- **International transfer:** Triggered when Personal Data subject to UK GDPR or EU GDPR is transferred, disclosed, or made available to a separate recipient in another country, including where remote access or other arrangements constitute a restricted transfer under the applicable regime. Before the transfer occurs, the Company will identify the applicable transfer rules and implement the required adequacy decision, contractual safeguard, or other lawful mechanism.
- **Data protection impact assessment (DPIA):** Triggered when a planned processing activity is likely to result in a high risk to individuals' rights and freedoms, including qualifying profiling, systematic monitoring, large-scale processing of sensitive data, or other processing identified by applicable law or regulatory guidance as requiring a DPIA. The Company will assess the activity before processing begins.
- **Personal Data breach:** Triggered when a security incident results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. The Company will assess the incident promptly and make notifications required by applicable UK or EU law, including applicable supervisory-authority deadlines.
- **Individual rights request:** Triggered when an individual exercises a privacy right under applicable UK or EU law. The Company will identify the applicable regime, verify identity where reasonably necessary, apply any lawful exemption or restriction, and respond within the applicable statutory timeframe.
- **Direct marketing:** Triggered when the Company communicates advertising or promotional material to particular individuals, including by email, text, direct messaging, or telephone where covered by applicable law. The Company will determine whether UK PECR and/or applicable EU/EEA e-privacy rules apply before the campaign begins and will maintain required consent, objection, suppression, and opt-out controls.

IV. Definitions

Interpretation. The words of which the initial letter is capitalized have meanings defined under the following conditions. The definitions have the same meaning whether they appear in singular or plural.

Definitions. For purposes of this Privacy Policy:

Account means a unique account created for You to access our Service or parts of our Service.

Company (referred to as either "Company", "We", "Us" or "Our") refers to Thistle Design (MMC) Limited, operating at 40 Dryden Road, Bilston Glen, Loanhead, Midlothian EH20 9LZ, United Kingdom. Where our affiliate operates a specific website or service, that affiliate may act as a separate controller and will provide notice where required.

Cookies are small files or similar technologies placed on or accessed from Your computer, mobile device, or other device by a website or service for functionality, preferences, analytics, security, or other purposes.

Country refers to the United Kingdom.

Controller means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

Device means any device that can access the Service such as a computer, a cellphone, a tablet, or similar device.

EEA means the European Economic Area, comprising the EU Member States together with Iceland, Liechtenstein, and Norway.

EU GDPR means Regulation (EU) 2016/679 (General Data Protection Regulation), to the extent it applies to the Company or particular processing activities.

ICO means the Information Commissioner's Office, the independent supervisory authority responsible for enforcing UK data-protection law.

Personal Data means information relating to an identified or identifiable natural person, as defined under applicable UK GDPR and, where applicable, EU GDPR.

Processing means any operation or set of operations performed on Personal Data, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transfer, dissemination, restriction, erasure, or destruction.

Processor means a natural or legal person which processes Personal Data on behalf of the Controller.

Privacy Officer means the individual or function designated by the Company to oversee privacy compliance and receive privacy inquiries, rights requests, and complaints.

PECR means the Privacy and Electronic Communications (EC Directive) Regulations 2003, as amended, and related UK rules governing certain electronic communications, direct marketing, cookies, and similar technologies.

Service or Services means our websites and other online or offline services that link to or otherwise provide this Privacy Policy, including forms, event-registration pages, marketing pages, customer portals, and related services.

Service Provider means a third party that provides services to or on behalf of the Company and may process, store, host, access, or otherwise handle Personal Data under contractual or other lawful arrangements.

Special Category Data means Personal Data falling within the special categories identified by Article 9 of the UK GDPR or EU GDPR, including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data used for unique identification, and data concerning health or sex life or sexual orientation.

UK GDPR means the retained EU General Data Protection Regulation as incorporated into UK law, as amended and supplemented by the Data Protection Act 2018, the Data (Use and Access) Act 2025, and other applicable UK legislation.

Usage Data refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself, such as duration of a page visit and technical information regarding access and use.

Website refers to the Company, accessible from <https://www.thistleprecision.com/>, and any other websites maintained by the Company or an associated business unit that link to this Privacy Policy.

You means the individual accessing or using the Service, or the company or other legal entity on behalf of which such individual is accessing or using the Service, as applicable. Under applicable data-protection law, You may be referred to as the data subject.

Data Protection Act 2018 means the UK Data Protection Act 2018, as amended, which supplements the UK GDPR and establishes additional UK requirements for certain processing activities.

Data (Use and Access) Act 2025 means the UK legislation amending aspects of UK data-protection, digital-information, and related rules, to the extent applicable to the Company and the relevant processing activity.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

Term	Meaning
Personal Data	Information relating to an identified or identifiable individual.
Processing	Any operation performed on Personal Data, including collection, recording, storage, access, use, disclosure, transfer, or deletion.
Controller	The entity that determines the purposes and means of processing Personal Data.
Processor	A person or organisation that processes Personal Data on behalf of a controller.
Service	Our websites, online forms, portals, services, communications, and other business interactions covered by this policy.
UK GDPR	The retained EU General Data Protection Regulation as it forms part of UK law, together with relevant provisions of the Data Protection Act 2018, as amended.
EU GDPR	Regulation (EU) 2016/679, where applicable to our processing.

V. Personal Data We Collect

Depending on the nature of our relationship with you, we may collect:

- Identity and professional contact information, such as name, business address, email address, telephone number, employer, job title, and professional contact details.
- Account and authentication information, such as usernames, account identifiers, preferences, and security information.
- Commercial and transaction information, such as quotations, orders, purchase history, billing and shipping details, and business correspondence.
- Technical and usage information, such as IP address, browser/device information, log data, website interactions, cookie information, and security/audit information.
- Employment-related information where you apply for or hold a role with us, as applicable.
- Information you provide through correspondence, surveys, events, support requests, forms, or other interactions.
- Information received from third parties, such as business partners, customers, suppliers, event organisers, professional networking platforms, publicly available sources, and service providers.
- Special category data only where legally permitted and necessary for a specific purpose, subject to the additional conditions required by applicable law. We do not intentionally seek to collect special category data through our ordinary customer-facing services.

VI. How We Collect Personal Data

- Directly from you, including when you complete forms, contact us, request information, create an account, place an order, or communicate with us.

- Automatically through our websites and systems, including technical logs, cookies, and similar technologies, subject to applicable cookie, consent, and privacy requirements.
- From third parties, including customers, suppliers, service providers, event organisers, professional networking platforms, and other lawful sources.
- From publicly available sources where permitted by applicable law.

VII. Purposes and Lawful Bases

- Performance of a contract: processing is necessary to enter into or perform a contract with You.
- Legal obligation: processing is necessary to comply with a legal obligation applicable to the Company.
- Legitimate interests: processing is necessary for the Company's legitimate interests or those of a third party, except where those interests are overridden by Your interests or fundamental rights and freedoms.
- Consent: You have given valid consent for one or more specific purposes where consent is required or appropriate.
- Vital interests: processing is necessary to protect the vital interests of You or another individual, where applicable.
- Public task/official authority: processing is necessary for a task carried out in the public interest or in the exercise of official authority, where applicable.

We process Personal Data only where permitted by applicable law. Depending on the activity, our lawful bases may include:

Processing purpose	Typical lawful basis
Providing products and services; processing orders and contracts	Performance of a contract; steps at your request before entering a contract
Responding to enquiries and providing customer/supplier support	Performance of a contract or legitimate interests, as applicable
Managing business relationships, quotations, procurement, and account administration	Performance of a contract; legitimate interests
Legal, regulatory, tax, accounting, export-control, sanctions, and compliance obligations	Compliance with a legal obligation; legitimate interests
Security, fraud prevention, investigations, and protection of systems/property	Legitimate interests; legal obligation where applicable
Recruitment and workforce administration	Steps before entering a contract; performance of a contract; legal obligation; legitimate interests, as applicable
Marketing communications where permitted	Consent where required; legitimate interests where permitted and appropriate; PECR requirements also apply
Website analytics and non-essential cookies	Consent where required by applicable cookie law/PECR and data-protection law
Other specifically identified purposes	Consent or another lawful basis permitted by applicable law

Where we rely on legitimate interests, we assess and document the relevant interests and consider whether those interests are overridden by your rights and freedoms. Where consent is required, we obtain it through an appropriate affirmative mechanism and provide a practical means to withdraw it. We do not condition a contract on consent where consent is not necessary for the contract.

VIII. Special Category and Sensitive Data

We seek to avoid collecting special category data unless it is necessary and lawful. Where we process special category data, we rely on an applicable condition under Article 9 of the UK GDPR and/or EU GDPR, together with any additional condition required by the Data Protection Act 2018 or other applicable law. Where criminal-offence data is processed, additional legal conditions also apply.

IX. Sharing and Recipients

We may disclose Personal Data, as appropriate and lawful, to:

- Affiliates and group companies that support our business operations, subject to appropriate governance and data-protection requirements.
- Service providers and processors supporting IT, hosting, cybersecurity, communications, CRM, ERP, HR, finance, shipping, compliance, document management, analytics, and other business functions.
- Professional advisers, auditors, insurers, banks, legal counsel, and other professional service providers.

- Government authorities, regulators, courts, law-enforcement agencies, customs authorities, and other public bodies where required or permitted by law.
- Transaction counterparties and advisers in connection with mergers, acquisitions, reorganisations, financing, or sale/transfer of assets, subject to applicable law.
- Other recipients when you direct us to disclose information or when disclosure is otherwise permitted by law.

We do not disclose Personal Data to third parties for their independent marketing purposes unless permitted by law and, where required, with your consent.

X. International Transfers

Because we operate in an international business environment, Personal Data may be accessed from or transferred to countries outside the United Kingdom or European Economic Area (EEA). The international-transfer requirements are triggered when a transfer or other disclosure/making-available arrangement falls within the applicable UK or EU restricted-transfer rules. We will make such transfers only where permitted by the applicable data-protection regime.

- For UK restricted transfers, we may rely on UK adequacy regulations, an appropriate safeguard such as the UK International Data Transfer Agreement (IDTA) or UK Addendum to the EU Standard Contractual Clauses, or a permitted statutory exception, as appropriate.
- For EU GDPR restricted transfers, we may rely on an EU adequacy decision, EU Standard Contractual Clauses (SCCs), binding corporate rules, or another lawful transfer mechanism available under EU GDPR.
- Where required, we will assess the transfer and implement appropriate safeguards and supplementary measures based on the applicable legal requirements and the circumstances of the transfer.
- Where required, we will make information about the applicable transfer safeguards available to individuals.

Personal Data may be transferred from the EEA to the UK where the relevant UK adequacy decision applies. Transfers from the UK to other countries remain subject to the UK GDPR international-transfer rules.

XI. Retention

We retain Personal Data only for as long as reasonably necessary for the purposes described in this Policy, including to provide services, maintain business records, comply with legal and regulatory requirements, resolve disputes, enforce agreements, and protect our systems and rights. Retention periods are determined using documented criteria such as legal requirements, contractual requirements, business needs, security logging, and regulatory obligations.

When Personal Data is no longer required, we will securely delete, destroy, anonymise, or otherwise dispose of it in accordance with our retention and security procedures, subject to lawful exceptions.

XII. Security

We use appropriate technical and organisational measures designed to protect Personal Data against unauthorised access, alteration, disclosure, loss, or destruction. These measures may include access controls, authentication, encryption, network and endpoint security, logging, monitoring, secure backups, physical controls, supplier due diligence, incident response, and workforce training.

No method of transmission or storage can be guaranteed to be completely secure. We maintain incident-management processes for suspected Personal Data breaches and will make notifications required by applicable law.

XIII. Cookies and Similar Technologies

Our websites may use cookies, tracking pixels, local storage, scripts, tags, or similar technologies. The trigger for UK PECR is the storing of or accessing information on a user's device in the UK. For EU/EEA users, the Company will also assess the applicable Member State e-privacy rules and, where relevant, EU GDPR territorial scope.

- Strictly necessary technologies used to provide a service requested by you, or falling within another applicable PECR exception, may be used without consent where the exception applies.
- Non-essential analytics, advertising, behavioural tracking, or similar technologies will be controlled through an appropriate consent mechanism where required by applicable law.

- Cookie choices will be presented clearly, and users will be given an appropriate means to change or withdraw consent where consent is required.
- Our websites may use third-party technologies; those providers may process technical or Personal Data subject to their own contractual and privacy requirements.

Our cookie notice or preference centre will provide more specific information about the technologies used on the applicable website.

XIV. Direct Marketing and Electronic Communications

Where we send direct marketing by email, text, direct messaging, telephone, or other electronic means, we will first determine whether the recipient and communication trigger UK PECR, applicable EU/EEA e-privacy requirements, or both. We will maintain appropriate records of consent, objections, suppression requests, and lawful exceptions where required and provide a practical means to opt out of marketing communications.

XV. Your Privacy Rights

Depending on the applicable law and circumstances, you may have the right to:

- Be informed about how your Personal Data is processed.
- Request access to Personal Data we hold about you.
- Request correction of inaccurate or incomplete Personal Data.
- Request deletion/erasure of Personal Data, subject to applicable exceptions.
- Request restriction of processing in circumstances permitted by law.
- Object to processing based on legitimate interests or for direct marketing, subject to applicable law.
- Request data portability where the legal conditions for portability are met.
- Withdraw consent where processing is based on consent, without affecting the lawfulness of processing before withdrawal.
- Challenge certain solely automated decisions or profiling where applicable legal conditions are met.
- Exercise additional rights available under applicable UK or EU law.

The scope and availability of these rights differ depending on the applicable law, the lawful basis for processing, and statutory exemptions. We may need to verify your identity before responding. In the UK, rights requests will generally be handled within the time period required by UK GDPR and applicable UK law. Where EU GDPR applies, requests will be handled in accordance with the applicable EU GDPR time limits and requirements.

XVI. Exercising Your Rights

Email: sales@thistleprecision.com

Please describe the right you wish to exercise or the complaint you wish to raise and provide sufficient information for us to identify the relevant records. We may contact you where clarification or identity verification is reasonably necessary. Rights requests will be handled within the period required by applicable law.

You will not generally be charged for exercising your privacy rights. Applicable law may permit a reasonable fee or refusal to act where a request is manifestly unfounded or excessive.

XVII. Complaints and Supervisory Authorities

You may contact us using the privacy contact details in this Policy if you have a concern about our handling of your Personal Data. Under UK law, we maintain a process for receiving data-protection complaints, facilitate the making of complaints by appropriate means, acknowledge complaints within 30 days of receipt, investigate as appropriate, keep the complainant informed of progress where appropriate, and communicate the outcome without undue delay.

You may also complain to the Information Commissioner's Office (ICO), the UK's independent data-protection regulator. Where EU GDPR applies, you may complain to the relevant EU/EEA supervisory authority, including the authority in the Member State of your habitual residence, place of work, or the place of the alleged infringement, subject to the applicable rules.

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

EU supervisory authorities: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en

XVIII. Automated Decision-Making and Profiling

We do not ordinarily use solely automated decision-making that produces legal or similarly significant effects on individuals. Where such processing is introduced, we will provide the information and safeguards required by applicable UK or EU law, including applicable rights to obtain human intervention, contest a decision, and receive meaningful information about the logic involved.

XIX. Children

Our business services are generally directed to businesses and adults and are not intended for children. We do not knowingly collect children's Personal Data except where necessary for a lawful and documented purpose and with any required safeguards. Where applicable law imposes additional requirements for children and online services, we will comply with those requirements.

XX. Third-Party Websites and Services

Our websites may contain links to third-party websites, applications, or services. We are not responsible for their privacy practices. You should review the privacy notice and cookie information of any third-party service you use.

XXI. Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in our processing activities, technology, legal requirements, or business operations. We will post updates on the applicable website and provide additional notice or obtain consent where required.

XXII. Legal and Regulatory Framework

This Policy is interpreted and applied under the UK GDPR, Data Protection Act 2018 (as amended), PECR, and, where its territorial scope is met, EU GDPR and applicable EU/EEA privacy and electronic-communications requirements.

XXIII. Contact Us

Questions about this Privacy Policy, privacy-rights requests, and data-protection complaints may be submitted to:

Thistle Design (MMC) Limited | 40 Dryden Road, Bilston Glen, Loanhead, Midlothian EH20 9LZ, United Kingdom

sales@thistleprecision.com | <https://www.thistleprecision.com/>