DATA PROTECTION POLICY

POLICY OWNER/ ISSUED BY	APPROVED BY	DATE ISSUED/ REVIEWED	EFFECTIVE FROM	NEXT REVIEW
Chief Legal and Risk Officer	Group Executive Team	December 2025	December 2025	December 2026

CONTENTS

OVERVIEW

Coats has a legal and ethical responsibility to safeguard Personal Data. We are committed to protecting the privacy of individuals and ensuring that **Personal Data** is collected, used, and stored in a lawful, fair and transparent way.

Protecting Personal Data is a shared responsibility for all personnel, wherever Coats operates.

PURPOSE

The purpose of this Policy is to explain how Coats protects **Personal Data** and to set out what is expected of all personnel when handling it.

SCOPE

This Data Protection policy ("Policy") is applicable to Coats Group plc, each of its subsidiaries and any joint ventures that are controlled by a company within the Coats group ("Coats"). Specifically, this Policy applies to:

All personnel that Process **Personal Data** in the course of their day-to-day activites at Coats.

All locations where Coats operates, even where local regulations do not exist.

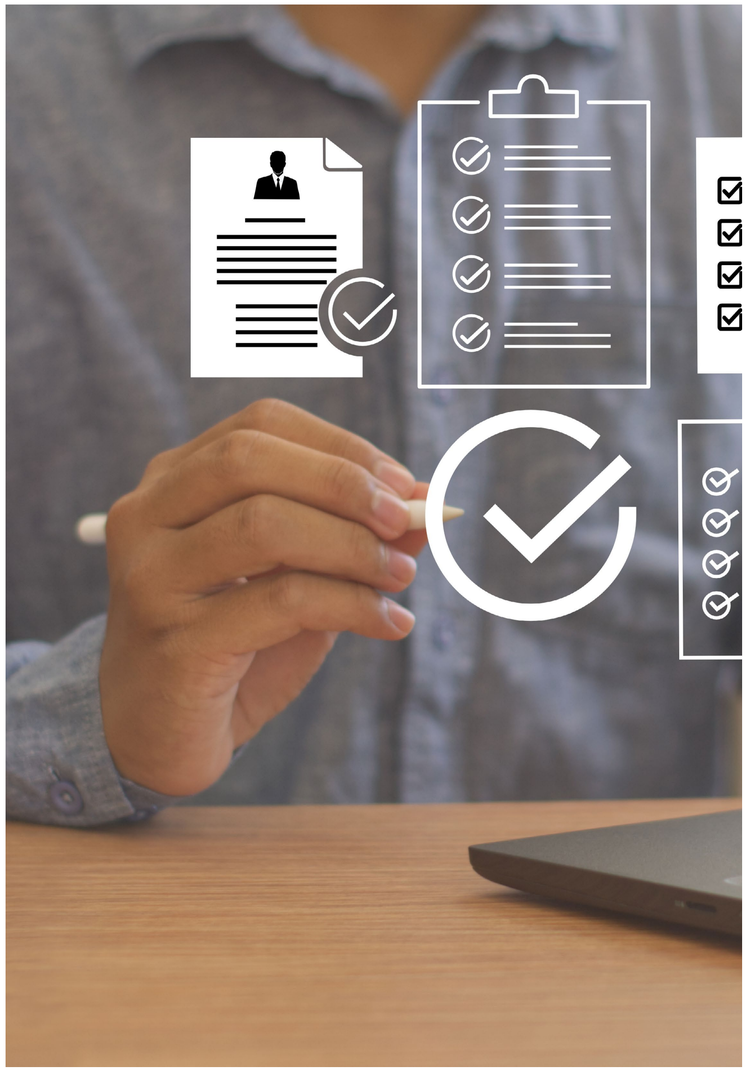
All methods of Processing **Personal Data**, including by automated, electronic, manual or non-automated means.

This Policy should be read together with Coats' other policies covering information security, records retention, acceptable use of IT, and related governance standards. Supporting procedures and guidance are available on Coats World through the Data Protection Hub.

Where there is a conflict between the requirements of this Policy and local law, the requirement that offers greater protection of **Personal Data** will apply.

Coats will Process **Personal Data** for its legitimate Business Purposes. Given Coats' global operations, this may involve sharing **Personal Data** with other Coats group companies or trusted third parties, and in some cases transferring **Personal Data** across borders, including outside the country where the data was originally collected.

Oversight of data protection compliance across Coats is provided by the Group Data Protection Officer, who can be contacted by email to: privacy@coats.com.



POLICY

In line with applicable data protection laws, the following principles set out the standards that everyone at Coats must follow when handling **Personal Data**.

1. Fair and Lawful Use

Personal Data must be collected and used fairly, lawfully, and in line with the rights of the Individuals concerned. This means that there must always be a valid legal basis for Processing, such as:

- the Individual has given clear and informed Consent;
- it is necessary to perform or prepare a contract with the Individual;
- it is required by applicable law;
- it is necessary to protect someone's vital interests (for example, in a medical emergency);
- it is required to establish, exercise, or defend legal claims; or
- it is necessary for Coats' legitimate Business Interests, provided this does not override the Individual's rights or privacy.

If Consent is used:

- it must be freely given, specific, informed, and unambiguous;
- individuals must be told they can withdraw their consent at any time
- silence or inactivity must never be treated as consent.

CONSENT:

Consent is not the default legal basis for using Personal Data. In most business situations, Processing will rely on contract, legal obligation, or legitimate interest.

2. Transparency:

When gathering **Personal Data** or establishing new Processing activities, you must ensure that Individuals whose Personal Data you are Processing receive appropriate notices at the time the Personal Data is obtained.

At a minimum, the privacy notice must explain:

- Who is responsible for deciding how the data is used and how to contact them.
- The purposes for which the data will be used and the legal basis for doing so.
- Who the data may be shared with, and whether it may be transferred across borders.
- How long the data will be kept.
- The rights available to the Individual, including how to make a complaint.
- Privacy notices must be written in plain language and made easily accessible. Example wording and templates are available on Coats World via the Data Protection Hub.

TRANSPARENCY IN PRACTICE

- Always provide a privacy notice when collecting Personal Data.
- If you are unsure how to prepare or delivery the notice, contact the Group Data Protection Officer at **privacy@coats.com**

3. Special Categories of Personal Data:

Special Categories of **Personal Data** (such as health, race, ethnicity, religion, political opinions, trade union membership, sexual orientation, genetic data, and biometric data used for identification) require extra protection.

In most cases, you must obtain the Individual's explicit consent before Processing this type of data, unless there is a clear legal requirement. Consent must be clear, explicit, and confirmed in words – silence or inaction does not qualify as Consent.

SPECIAL CATEGORIES OF PERSONAL DATA

- Never Process Special Categories of Personal Data without first discussing with the Group Data Protection Officer at **privacy@coats.com**
- Explicit consent is normally required and must be documented.
- Contact the Privacy Team immediately is you are asked to collect or use this type of information.

4. Data Integrity, Accuracy and Amendment

Personal Data must be accurate, up to date, relevant, and not excessive for the purpose for which it was collected. If you become aware of inaccurate or outdated information, you must correct it where possible, or report it to the Privacy Team.

Individuals may also ask Coats to update or amend their Personal Data. Coats will take reasonable steps to do so, and any disputes about accuracy must be referred to the Group Data Protection Officer at privacy@coats.com

5. Processing purpose

Personal Data collected for one purpose must not be used for a different, unrelated purpose unless the Individual has agreed or would reasonably expect it.

6. Security, Integrity and Confidentiality

Personal Data must always be protected against loss, misuse, unauthorised access, alteration, or disclosure. You must maintain data security by protecting the confidentiality, integrity and availability of Personal Data.

SECURITY FIRST

- Follow Coats' IT and information security policies at all times.
- Access to Personal Data should only ever be on a "need to know" basis.

7. Service Providers

Personal Data may only be shared with third-party providers if they meet Coats' data protection and security requirements.

Before engaging a provider that will Process **Personal Data** on Coats' behalf, you must consult the Group Legal and Group Cybersecurity Teams.

8. Data Breaches

Any suspected or actual data breach, including the loss, unauthorised access or disclosure, or corruption of **Personal Data**, must be reported immediately in line with the Data Breach Notification Policy.

DATA BREACHES

Data protection law requires certain breaches to be reported to regulators without undue delay and, where feasible, within 72 hours. To ensure compliance, all suspected breached must be escalated to the Privacy Team immediately upon discovery.

9. Data Storage

Personal Data must not be kept longer than necessary for the purpose it was collected, unless the law requires otherwise. Once it is no longer needed, **Personal Data** must be securely deleted or anonymised, in accordance with the Records Retention Policy.

10. International Transfers

Personal Data must not be transferred across borders, including outside the country of origin or the EEA/UK, unless appropriate protections are in place.

This means the transfer must be reviewed and approved in advance by the Group Data Protection Officer at privacy@coats.com to ensure that Individual's rights remain protected.

TIME LIMITS FOR RIGHTS REQUESTS

Data protection law requires that requests from Individuals are responded to without undue delay, and in most cases, within one month. To meet this obligation, all requests must be forwarded to the Privacy Team immediately upon receipt.

Individual's Rights

Individual's have rights when it comes to how we handle their **Personal Data**.

These include rights to:

- **Access:** to know whether we hold their Personal Data and to obtain a copy.
- **Rectification:** to have inaccurate or incomplete Personal Data corrected.
- **Erasure:** to have Personal Data deleted where it is no longer needed or where Consent is withdrawn.
- **Restriction:** to limit how their Personal Data is used in certain circumstances.
- **Objection:** to object to Processing, including direct marketing.
- **Portability:** to receive Personal Data in a structured, commonly used format.
- **Profiling and automated decision making:** not to be subject to a decision based solely on automated Processing that has legal or similarly significant effects.

Any request from an individual must be escalated immediately to the Group Data Protection Officer.

11. Accountability

Coats must be able to demonstrate compliance with data protection laws at all times. This includes keeping records of processing activities, applying appropriate security measures, and carrying our regular audit and reviews.

12. Training and Awareness

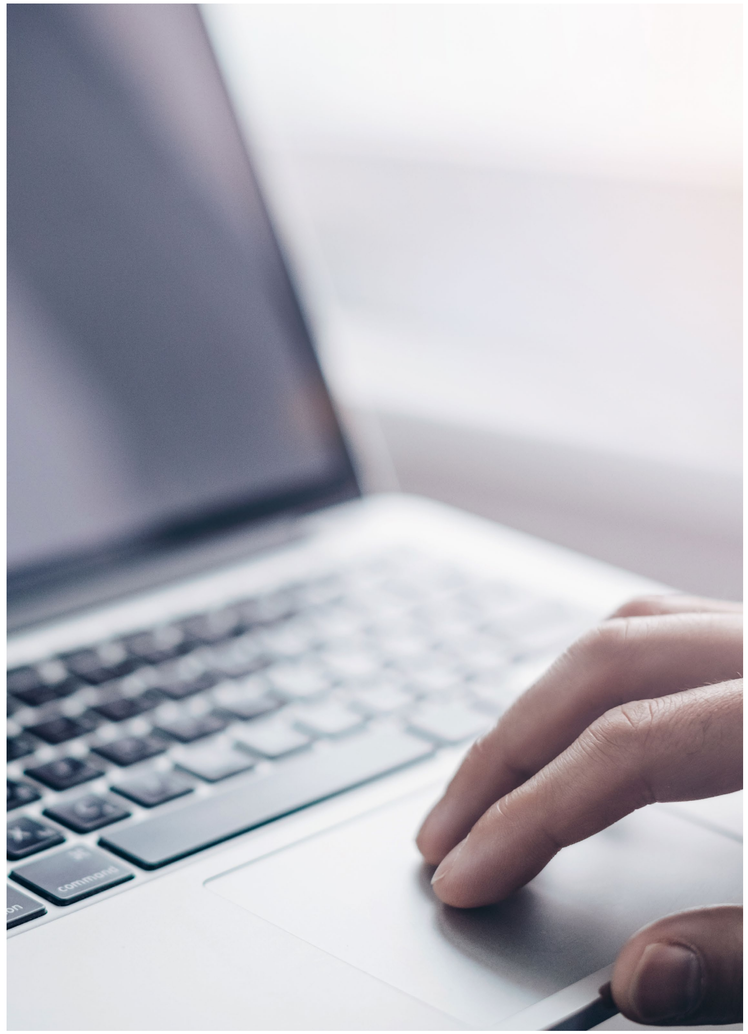
All personnel who handle **Personal Data** must complete data protection training provided by Coats and refresh it regularly. Additional guidance and support is available through the Data Protection Hub on Coats World.

13. Data Protection Impact Assessments (DPIAs)

Where Processing is likely to result in a high risk to Individual, a Data Protection Impact Assessment (DPIA) must be completed before the Processing begins. DPIAs must be reviewed and approved by the Privacy Team.

14. Automated Processing and Profiling

Coats does not generally make decisions about individuals based solely on automated processing or profiling. Where automated decision-making is used, it must be fair, transparent, and include safeguards to protect Individuals' rights.



CONTACT

For questions, feedback, or further information regarding this code, please contact Jeffrey Soal at **Jeffrey.Soal@coats.com**.

Coats Group plc
4th Floor,14 Aldermanbury Square, London EC2V 7HS.
https://www.coats.com/en/

DEFINITIONS

Throughout this Policy, the following definitions and meanings shall apply:

Business Purposes	Means the purposes for which Personal Data may be used by Coats such as employment of personnel, administrative, financial, regulatory, payroll and business development purposes, supply of goods and services as well as in connection with corporate acquisitions and disposals.
Direct Marketing	Means a method of contacting customers and potential customers personally about products and services Coats offers, through the post, telephone calls, emails, social media, text messaging, brochures and coupons.
Individual	Means a living, identified or identifiable individual about whom we hold Personal Data. Individuals may be nationals or residents of any country and may have legal rights regarding their Personal Data.
Personal Data	Means any information relating to an identified or identifiable individual (including but not limited to name, home address, personal telephone number, date of birth, biometric information, medical records, CCTV images and IP addresses, social security number, location data or any identification information).
Process/ Processing	Means any activity involving Personal Data, including obtaining, recording or holding the Personal Data, or carrying out any operation or set of operations relating to the Personal Data, including organising, amending, retrieving, using, disclosing, Profiling, erasing, retaining, sharing, transferring or destroying Personal Data.
Profiling	Means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an Individual, in particular, to analyse or predict aspects concerning an Individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the Individual's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.
Special Categories of Personal Data	Means Personal Data about an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, physical or mental health or condition, sexual life, commission or alleged commission of acriminal offence by the Individual, or related proceedings.

7. REVISION HISTORY

VERSION	AUTHOR	DATE	NOTE
V1.0	DPM	03/02/2019	Initial version, all new content
V2.0	DPO	02/06/2020	Adjustments with input from Gerry Pope, Group Legal, to align policy with global practices
V3.0	DPO	02/11/2021	Replacing should with must
V4.0	DPO	12/12/2022	Amendments to: i) Section 2 – Scope of Policy; and ii) relevant contacts for specific events. Other non-material changes to improve readability.
V5.0	Avinash Kumar and Fernanda Insua	December 2025	Revamp of this policy in the new format