

Milliken & Company

EU Customer/Vendor Data Protection Notice

I. Introduction and scope

Milliken is committed to Processing Personal Data responsibly and in compliance with the applicable data protection laws in all countries in which Milliken operates. Please refer to the Milliken General Data Protection Policy for more information on definitions, our overall data protection principles and our approach to data protection compliance, which can be found at www.milliken.com/privacy.

This European Union (“EU”) Customer/Vendor Data Protection Notice (the “Notice”) describes the types of Personal Data Milliken collects, how Milliken uses that Personal Data, with whom Milliken shares your Personal Data, and the rights you, as a Data Subject, have regarding Milliken’s use of the Personal Data. This Notice also describes the measures Milliken takes to protect the security of the data and how you can contact us about our data protection practices.

II. Contact details of the Data Controllers

The Milliken entities responsible for the collection and use of your Personal Data (the Data Controllers) in your home country for the purposes described in this Notice are contained in the attached Annex 1.

III. Contact details of the Data Protection Manager

A Milliken Data Protection Manager (DPM) is designated at the pan-European level. If required by local law requirements a Data Protection Officer may be appointed in a specific country.

The DPM is involved in all issues related to the protection of your Personal Data. In particular, the DPM is in charge of monitoring and ensuring compliance with this Notice and the applicable data protection laws. They will also provide advice on data protection matters upon request.

For any clarification or additional information you may need in order to fully understand this Notice, please contact the DPM (or the DPO as may be required by applicable law) at Privacy@milliken.com.

IV. Purposes of data Processing and legal basis

Milliken processes Personal Data in accordance with applicable data protection laws and regulations and only for limited, explicit and legitimate purposes. Milliken will not use Personal Data for any purpose that is incompatible with the original purpose for which it was collected unless you provide your prior explicit consent for further use.

Personal Data relating to Customers/Vendors may be Processed for the purposes of:

- Administering and managing commercial relationships with current and potential clients (such as order fulfillment, payment and invoicing for goods & services, contacting customer, review creditworthiness, IT support);
- Fraud detection & prevention

- Administering and managing commercial relationships with current and potential suppliers and vendors;
- Responding to regulatory and technical services requests;
- Carrying out promotional operations, direct marketing;
- Conducting statistical surveys and marketing studies, etc.;
- Compliance with legal obligations
- Security (such as managing security access badges) and recording visitors to our sites and guest house; and
- Responding to website enquiries (as more adequately defined in our Website Data Protection Policy available at www.milliken.com/privacy)

The legal basis for each purpose is as follows:

Customer Related Data:

<u>Purpose of processing</u>	<u>Legal basis</u>
Administer and manage Customer Relation (e.g., Order Fulfillment, Payment & Invoicing for Goods & Services, Contacting Customer, Review Creditworthiness, IT Support, responding to technical and regulatory requests)	Contract
Compliance with Legal Obligations	Legal Obligation
Fraud Detection & Prevention	Legitimate Interests
Security Access Control System and Video Surveillance System (e.g., security access badge)	Legitimate Interests
Direct Marketing and promotional activities	Consent

Supplier/Vendor Related Data:

<u>Purpose of processing</u>	<u>Legal basis</u>
Security – video surveillance System	Legitimate Interests, Legal Obligation
Security – Access Control System	Legitimate Interests, Legal Obligation
Security – Emergency Mass Notification System	Legitimate Interests, opt-in
Security – Travel Risk Management System	Legitimate Interests, opt-in
Administer Vendor/Supplier Relation (e.g., Payment & Invoicing for Goods & Services, Contacting Vendor/Supplier)	Contract

Milliken ensures that our internal governance procedures clearly specify the reasons behind decisions to use Personal Data for alternative Processing purposes. Prior to using your personal data for a purpose other than the one for which it was initially collected, you will be informed about such new purpose.

V. Categories of Personal Data processed

The provision of Personal Data is a requirement necessary to enter into a contract with Milliken or a requirement by law or regulation for Milliken to administer your customer/vendor relationship. The Personal Data processed is limited to the data necessary for carrying out the purpose for which it is collected.

Personal Data processed includes the following:

- Business information (such as name of organization, business unit, website, department, job title and business bank details);
- Customer and Vendor/supplier personal information (such as name & initials, photographs, age, family details, spouse name, date of birth, birth certificate number, marital status, interests, language preference, allergies, special requests, gender, other directorships, prior employment)
- Contact information (such as business postal address, email address, telephone number, business cellular and fax number)
- Contractual information (such as date of agreement, type of commercial relationship, etc.).
- Financial account information (such as BAT number and bank details)
- Security/location information (such as photographs, video surveillance images and access control logs on site)

Milliken will not collect Personal Data if such collection is prohibited under the applicable data protection laws.

In no case shall Personal Data revealing religious beliefs, racial or ethnic origin, political opinions, philosophical beliefs, trade union membership or concerning sex life be processed in the customer/vendor context.

Milliken will maintain Personal Data in a manner that ensures it is accurate, complete and up-to-date.

VI. Data Security

Milliken has implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk, such risk analysis includes an analysis of the risk of compromising the rights of the Data Subject, costs of implementation, and the nature, scope, context and purposes for Data Processing.

The measures include:

- (i) Encryption of personal data where applicable/appropriate;
- (ii) Entry controls. Technical and organizational measures to control access to premises and facilities, particularly to check authorizations are in place. Any stranger seen in entry-controlled areas should be reported. Technical (ID/password security) and organizational (user master data) measures for user identification and authentication are implemented for all electronic systems including segregation of duties and restrictions based on job need;
- (iii) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- (iv) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (v) Secure lockable desks and cupboards should be kept locked if they hold confidential information of any kind;
- (vi) Paper documents are confidentially destroyed;
- (vii) Digital storage devices should be physically destroyed when they are no longer required; and
- (viii) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

Milliken has developed various security policies and procedures to implement the aforementioned measures appropriately.

VII. Recipients of Personal Data

Milliken will only grant access to Personal Data on a need-to-know basis, and such access will be limited to the Personal Data that is necessary to perform the function for which such access is granted.

Authorization to access Personal Data will always be linked to the function so that no authorization will be extended to access Personal Data on a personal basis. Service providers will only receive Personal Data according to the purposes of the service agreement with Milliken and subject to confirmation that they have their own suitable technical and organizational measures in place.

Third parties shall include:

- cloud providers and IT storage solutions;
- marketing agencies,
- event organizers and event photographers; and
- auditors.

VIII. International data transfers

International data transfers refer to transfers of Personal Data outside of the European Economic Area (“EEA”).

The international footprint of Milliken involves the transfer of Personal Data to and from other group companies or third parties, which may be located outside the EEA, including the United States of America. Milliken will ensure that when Personal Data is transferred to countries that have different standards of data protection, appropriate safeguards to adequately protect the Personal Data are implemented to secure such data transfers in compliance with applicable data protection laws. Milliken has implemented Data Transfer agreement based on EU model clauses to cover international data transfers and a copy of these agreements can be obtained by contacting the Milliken Data Protection Manager.

IX. Retention of Personal Data

Milliken will not retain your Personal Data for longer than is allowed under the applicable data protection laws and regulations or for longer that is justified for the purposes for which it was originally collected or otherwise processed, subject to applicable local retention requirements. Retention policies pertaining to specific types of documents and data are implemented within the organization to comply with legal retention periods.

X. Data protection rights

Under applicable data protection laws, you will benefit from the following rights. You can exercise these rights at any time by contacting the Milliken DPM or DPO, where applicable:

- Right to access to, rectification and erasure of Personal Data;
- Right to restriction of Processing and to object to Processing;
- Right of data portability to the extent applicable;
- Right to withdraw consent where the Processing is based on consent; and
- Right to lodge a complaint with the supervisory authority.

XII. Notice Compliance and Contact Information

Monitoring and ensuring compliance of the Personal Data Processing within Milliken with this Notice and applicable data protection laws and regulations is the responsibility of the DPM and any applicable DPO where required by local law requirements.

You may contact the DPM at privacy@milliken.com with regard to any issue related to Processing of your Personal Data and to exercise your rights as mentioned above.

XIII. Miscellaneous

This Notice shall be effective as of 25 May 2018 and shall be applicable to all Milliken entities in the EU.

This Notice may be revised and amended from time to time and appropriate notice about any amendments will be given.

Milliken is allowed to adapt the text of this Notice only in order to be compliant with local legislation by means of an addendum attached to this Notice. In case of any discrepancies between this Notice and a specific local addendum made in accordance with local law, the terms of the latter shall prevail.

Annex 1
Milliken legal entities

Milliken Fabrics SAS
37 rue du Nouveau Monde,
80240 Roisel,
France

Milliken Industrials Ltd
Gidlow Lane,
Wigan,
WN6 8RN
United Kingdom

Milliken Europe BVBA
Ham 18-24
9000 Gent
Belgium

Milliken Textiles BVBA
Ham 24
9000 Gent
Belgium

Milliken Luxembourg SARL
102, Rue des Maraîchers,
L-2124, Luxembourg

Milliken Luxembourg Holding SARL
102, Rue des Maraîchers,
L-2124, Luxembourg