



Supplier Privacy Notice

July 1, 2024

This Supplier Privacy Notice (the “Notice”) applies to [The Dow Chemical Company and its direct and indirect global subsidiaries and controlled affiliates](#) (where Dow owns more than 50 per cent of the voting rights or has the right to control the entity) (collectively, the “Dow Companies”; each a “Dow Company”). The Dow Company that is communicating with you or to which you are providing services (referred to herein as “Dow” or “we” or “our”) is responsible for the processing of your personal data and controls how it is used, in accordance with this Notice. For applicable data protection law, that Dow Company is the primary controller of your data; other Dow Companies may also receive and process your personal data, in the capacity of controller, and this Notice applies equally to them. This Notice explains why and how we collect personal data about you, how we process such data, and what rights you have regarding your personal data.

The Information Dow Collects.

In connection with the contracted services you are providing to Dow, we may collect the following categories of personal data:

- *The business contact information you share with us, such as:* name, job title, nationality, business name and mailing address, email address, telephone numbers, industry/business segment;
- *Additional information you provide to us in the course of our business relations, such as:* data concerning the fulfilment of our contractual obligations and pre-contractual measures, including correspondence data, call/meeting transcripts and recordings, offers, tenders, resume/CV, conditions, contract and order data, invoices, payments, insurance data, records relating to queries/questions/complaints/orders; employee number, passport number, driving license number, vehicle license plate, government identification number, date of birth, travel visa information; interview assessment/feedback; tracking/analytics data; training records; gender; supplier survey and event data; and
- *Electronic identification data and information collected by the communications systems, IT applications and website browser, such as:* information technology usage (system access, IT and internet usage), device identifier, digital alias/signature, analytics ID, browser type, registration and login credentials, IP address, login data and log files, searches, the source of your site visit, time and URL, webpage views and time spent on the website or a particular page, date and time of visit, links clicked, comments shared, emails opened, cookies.

The following types of personal data are only collected and processed, if at all, in accordance with applicable local laws in your country of residence:

- *Data about criminal convictions and offences, such as:* criminal background information



and sanction list information, to the extent required for the purposes of criminal background screening, due diligence, and anti-money laundering obligations;

- *Health related data, such as:* health certificate of your company's employees when allowed or required by local law;
- *To the extent necessary to fulfil our obligations, data obtained from publicly accessible sources, or which are legitimately transmitted by other third parties (e.g., a credit agency), such as:* commercial register data, association register data, creditworthiness data; and
- *If applicable, additional information you provide to us in connection with our supplier diversity program (to the extent, if at all, that such information relates to you and constitutes identifiable personal data), such as:* whether your company is a certified diverse supplier; whether your company is owned and operated by any individual from underrepresented groups (ethnic minorities, LGBTQ+, people with disabilities, veterans, women); whether your company's executive leadership includes women or minorities; the percentage of your workforce that voluntarily and openly identify themselves as having a disability or as being a member of the LGBTQ+ community; the percentage of your company's leadership team that voluntarily and openly identify themselves as diverse individuals; and (for Dow's prime suppliers only), the specific number of individuals in each of your company's board of directors, leadership team, employees, new hires, and Dow account team who identify as Black/African American, Asian, Hispanic/LatinX, Native American, other minority group, female, LGBTQ+, or U.S. veteran.

The purposes for which we use your information.

We may use your personal data as described above for the following purposes:

- Engage, vet, and contract with suppliers; create and maintain supplier accounts; manage contract lifecycle and supplier relationships; process, evaluate, and respond to supplier requests and inquiries; provide supplier support; ensure the accuracy of supplier contact information; conduct supplier surveys and events;
- Carry out supplier management operations relating to Dow's supplier contracts, including, procurement, tendering, orders, deliveries, invoices, accounting management, relationship management, and due diligence;
- Train suppliers; arrange travel for suppliers and suppliers' employees;
- Pay debts, manage supplier invoices and payments, purchase direct and indirect services; manage payment collection and insolvency processes; manage finances, shared accounting services, record-to-report processes, procure-to-pay processes;



- Manage process quality; develop and improve supplier services and products (e.g., by reporting and analyzing relevant information, performance metrics, market intelligence, etc.);
- Reorganize, acquire, and sell activities, business units, and companies;
- Monitor and audit compliance with Dow's corporate policies, contractual obligations, and legal requirements; carry out audits (internal and external), risk and compliance reviews, and regulatory checks to meet applicable legal and regulatory obligations; facilitate compliance with applicable legal obligations (e.g., by conducting due diligence, anti-money laundering reviews, customs/global trade reviews; by screening sanctioned party lists; by implementing security protocols);
- Maintain and protect the security of products, facilities, services, systems, networks, computers, and information; prevent and detect security threats, fraud, and other criminal or malicious activities; manage IT resources generally, including infrastructure management, data back-up, information systems' support and service operations for application management, end user support, testing, maintenance, security (incident response, risk, vulnerability, breach response), user accounts management, software licenses assignment, security and performance testing, and business continuity; and
- Include diverse suppliers in Dow's evaluation of suppliers via strategic sourcing; develop mutually profitable business relationships with small and diverse suppliers who are globally competitive and who demonstrate the ability to add value and meet Dow's expectations of its suppliers as outlined in the Supplier Code of Conduct.

We collect only the personal data from you that we need for the purposes described above. For statistical purposes, improvement of our services and testing of our IT systems we use as much as reasonably possible anonymized data. This means that these data can no longer (in)directly identify you or single you out as an individual.

The legal basis we rely on.

We use your personal data for the purposes described in this notice based on one of the following legal bases, as applicable:

- We may process your personal data for the fulfilment of contractual obligations resulting from contracts with you or your company, or as part of pre-contractual measures we take;
- We may process your personal data to comply with statutory requirements (e.g., in connection with tax or reporting obligations, cooperation obligations with authorities, statutory retention periods, regulatory or judicial proceedings, evidentiary hearings; and the prosecution or enforcement of civil law claims);
- We (or your employer) may ask your consent for the activities described in this privacy notice when required by applicable law—e.g., if we (or your employer) process



information that relates to you and constitutes identifiable personal data in connection with our supplier diversity program;

- We may rely on our legitimate interests to process your personal data within the scope of our business relationship with you or your company insofar as this is not overridden by your own privacy interests. Such interests may include:
 - Conduct, manage, develop, and further our business in the broadest sense possible;
 - Carry out supplier management operations relating to Dow's supplier contracts, including, procurement, tendering, orders, deliveries, invoices, accounting management, relationship management, and due diligence;
 - Monitor, investigate, and ensure compliance with applicable contractual, legal, and regulatory requirements, obligations, and standards and with Dow policies;
 - Prevent and detect security threats, fraud, and other criminal or malicious activities;
 - Transmit personal data within the Dow group for internal administrative purposes as necessary (e.g., to provide centralized services).

We will only process personal data concerning criminal convictions and offences if such processing is permitted by applicable (local) law.

Third parties with whom we share your personal data (in and outside the country where the Dow Company that controls your data is located).

We share your personal data with other Dow Companies or third parties as necessary for the purposes described in this table below:

Recipient	Purpose
Dow affiliates and subsidiaries	The purposes described in this privacy notice
Dow business partners, distributors, and agents The purposes described in this privacy notice	The purposes described in this privacy notice
Service providers working on Dow's behalf— e.g., providing services such as IT tools and infrastructure; marketing; payment processing; professional and advisory (including accountants, auditors, lawyers, insurers, bankers, recruiters, travel agents and other advisors or service providers)	The purposes described in this privacy notice
Insolvency administrators or creditors	For default and insolvency management



Potential or actual acquirers of Dow businesses or assets	For the evaluation of the business or assets in question or for the purposes described in this privacy notice
Recipients as required by applicable law or legal process, to law enforcement or government authorities, etc.	Where required by applicable law or a legitimate request by government authorities, or a valid legal requirement

If we share your personal data with a Dow Company or third party—so that it is transferred to or becomes accessible from outside the European Union (“EU”), the European Economic Area (“EEA”), Switzerland, the UK, or otherwise outside the country where the Dow Company that controls your data is located—we put adequate safeguards in place to protect your personal data. Examples of these safeguards are an adequacy decision of the European Commission ([read more here](#)), Standard Contractual Clauses ([read more here](#)), and the Binding Corporate Rules that some of our suppliers have adopted ([read more here](#)). We have taken additional measures for the transfer of data from within to outside the EU, EEA, Switzerland, the UK, and outside the country where the Dow Company that controls your data is located to protect your personal data.

If you would like an overview of the safeguards which are in place, you may submit a request [here](#) or send an email request to fglpriv@dow.com.

How long we keep your personal data.

Dow will retain your personal data for as long as necessary to fulfill the purposes for which we collect it, including for the purposes of satisfying any legal, accounting, or reporting requirements. In general, personal data is kept for the duration of the contractual relationship and for a minimum period (typically between 5-10 years after the termination of the contract) or for a longer period if required by applicable (local) laws and regulatory requirements. At the same time, applicable data protection laws require that we do not keep personal data in an identifiable form for any longer than is necessary for the purpose for which the personal data is being processed. Through the setting of IT applications and policies we ensure that your personal data is deleted or anonymized when we no longer need it.

Your data privacy rights.

Depending on the jurisdiction in which you are located and in which your personal data is processed, you may have the following rights:

Data privacy rights	What it means
The right to access your data	You are entitled to ask Dow for an overview of or to obtain a copy of the personal data we hold about you.
The right to have your data	You may request immediate correction of inaccurate or incomplete personal data we hold about you.
The right to have your data erased	You may request that personal data be erased when it is no longer needed, where applicable law obliges us to delete the data or the processing of it is unlawful.



The right to restrict data processing	You have the right to restrict the processing of your personal data in specific circumstances.
The right to data portability	You have the right to receive your personal data in a structured, machine-readable format for your own purposes, or to request us to share it with a third party.
The right to object to data processing	You have the right to object to our processing of your personal data where we rely on our legitimate interests as the basis for our processing, where your data protection rights outweigh our reasoning for legitimate interests.
The right to withdraw consent	Where Dow has asked for your consent to process personal data, you may withdraw your consent at any time. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

Please note that the rights described above are not absolute, and that your request cannot always be met entirely. For example, sometimes we cannot delete or restrict the processing of your personal data as we may have legal or contractual obligations to keep certain such personal data.

You may request to enforce your data privacy rights by sending an email request to fglpriv@dow.com or by submitting a request [here](#). No fees or payments are required to exercise your legal rights, though Dow may charge fees for duplicate or excessive requests. Dow may request information from you to allow us to confirm your identity and your rights over the data, as a security measure.

What happens if you ask us to stop processing (or do not provide) your information.

Dow may not be able to adequately establish, conduct, or terminate a business relationship with you or your company (or otherwise perform the purposes described above) without certain personal data. Although we cannot obligate you to share your personal data with us, please note that this then may have consequences which could affect the business relationship in a negative manner, such as not being able to take requested pre-contractual measures to enter into a contract with you or to establish and continue the business relationship you have asked for.

Contact and further information.

If you want to access your personal data, make use of any of your other rights mentioned above or if you have any questions or concerns about how Dow processes your personal data, please contact Dow's Data Privacy Team at fglpriv@dow.com or submit a request [here](#). Questions, requests and inquiries concerning this Notice and the information set out in this Notice may also be directed to your local Dow representative.

For more information about Dow's data privacy practices, including about certain data subject rights that may apply to you under applicable law, please refer to Dow's [Privacy Statement](#).



Should you not be satisfied with our response or believe we are processing your personal data against the law, you may also have the right to file a complaint with the applicable data protection or privacy authority in your country of residence or work or seek a remedy through the courts where you believe an infringement of data privacy laws may have taken place.