Origin UK Operations Limited Trading as Origin Fertilisers

Data Privacy Policy (External)

Contents

1. About Origin

Origin UK Operations Limited trading as Origin Fertilisers ("Origin," "we," or "us"), a UK registered company with registration number 2465499 and having its registered office at 1-3 Freeman Court, Jarman Way, Orchard Road, Royston, Hertfordshire, SG8 5HW. This Privacy Policy outlines what personal data we collect, how we use that information and other information about how we protect your privacy. Origin UK Operations Limited ("Origin") is a leading manufacturer and supplier of fertiliser products.

2. Purpose

Origin recognises the need to maintain the confidentiality of private, sensitive, and proprietary information. This Data Privacy Policy ("Policy") sets out Origin's overarching approach to data privacy, including how the company protects the confidentiality of private, sensitive and proprietary information ("Company Confidential" or "Client Confidential" information). This Policy is designed to foster compliance with all applicable laws, directives, and regulations and other Origin policies governing the security and confidentiality of all types of information – paper, electronic and verbal. Origin do not sell, transfer, lease or share your information with 3rd parties other than described here in this policy. In circumstances where we do share information it is only in what would reasonably be expected to support Order Fulfilment.

3. Scope and Application of Law

A. Scope

This Policy covers all sensitive, private, and proprietary information that is both internally and externally transmitted, irrespective of the medium of storage or transfer. Types of data covered by this Policy may include but are not limited to, client data, personal information, confidential legal data, confidential client data, non-public financial data and proprietary research data. Collectively, these data types are referred to as "confidential data." This Policy applies to all Origin employees and others performing work for the Company who may handle and store confidential data on behalf of Origin, its Customers or Suppliers.

B. Application of Laws

This Policy comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws. The relevant national law will take precedence if it conflicts with this Policy, or it has stricter requirements than this Policy. The content of this Policy must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed.

4. Principles

At a high level, data processing principles that Origin will comply with include[1]:

4.1. **Fairness and lawfulness:** When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.

4.2. **Restriction to a specific purpose:** Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

4.3. **Transparency:** The data subject must be informed of how his/her data are being handled. In general, personal data must be collected directly from the individual concerned. When the data are collected, the data subject must either be aware of, or informed of: the identity of the Data Controller; the purpose of data processing; and third parties or categories of third parties to whom the data might be transmitted.

4.4. **Data reduction and data economy:** Before processing personal data, you must determine whether and to what extent the processing of personal data is necessary to achieve the purpose for which it is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymised or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

4.5. **Deletion:** Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. In some cases, there may be an indication of interests that merit protection or historical significance of this data in individual cases. Please see Data Retention police for further information.

4.6. **Factual accuracy:** Personal data on file must be correct, complete, and (if necessary) kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

4.7. **Confidentiality and data security:** Personal data are subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorised access, illegal processing or distribution, as well as accidental loss, modification or destruction.

5. Reliability of Data Processing

Collecting, processing and using personal data is permitted only under the following legal basis.

A. Consent given to process data

Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed in accordance with this Policy. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

1. GDPR, Article 5

B. Data processing pursuant to legal authorisation
The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions.

C. Processing of sensitive data
Sensitive personal data can be processed only if the law requires this or if the data subject has given consent for the same. This data can also be processed if it is mandatory for asserting, exercising or defending legal claims regarding the data subject. If there are plans to process sensitive data, the Responsible Person must be informed in advance.

D. Legitimate Interest
In some circumstances Origin will rely on the legitimate interest concept to justify our processing of personal data but only in circumstances where such processing should be reasonably expected by the Data Owner. The below Section is not exhaustive list of these circumstances and therefore we suggest you consult your Origin representative in case of doubt.

6. Customer Data

A. Processing of an Order
Origin will process a customer's order(s) and personal data with the intention of fulfilling the order management process. Specific examples of data processed are as follows:

- Customer's personal and financial data to set them up as a customer on the order management system
- Delivery location to enable the delivery of the product to the correct location
- Personal data required to process an invoice related to the order
- Customer's financial data to process payment for the order
- Customer's premises access information where provided

B. Business Development
Origin will store business network contact information, with the intention of engaging the network with information about Origin's products and services. Examples of such engagements include:

- Origin employees managing their own personal contact list with the intention of engaging the contact to develop business
- Origin marketing teams making direct contact with customers who have provided consent, to inform them of products and services that may be of interest to them

C. Profiling of Customers
Origin will process customer data and profile customer segments with the intention of enhancing the relevance of Origins products and services. Specific examples of this include the following:

- Analysis of trends in ordering of specific products against specific customers, and identifying opportunities to alternative product or service for customers
- Analysis of ordering data to identify opportunity to offer complimentary products or services to customers

D. Third Parties

Origin shares data with 3rd party haulage entities as required with the intention of fulfilling customer orders where customers require delivery. Specific examples include:

- Sharing delivery details with haulage companies so that products can be delivered to the required location
- Sharing contact details such as name and telephone number of customer so haulier can arrange delivery

7. Rights of the Data Subject

Every data subject has the following rights:

7.1. The data subject may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected.[2]

7.2. If Personal Data are transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients.[3]

7.3. If Personal Data are incorrect or incomplete, the data subject can demand that it be corrected or supplemented.[4]

7.4. The data subject can object to the processing of his or her data for purposes of advertising or market research. The data must be blocked from these types of use.[5]

7.5. The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.[6]

7.6. The data subject generally has a right to object to his/her data being processed, and this must be considered if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.[7]

7.7. Additionally, every data subject can assert the rights as per national privacy laws.[8]

[2] GDPR Rec. 58, 60; Art 13-14
[3] GDPR Rec.62; Art. 17(2), 19
[4] GDPR Rec.39, 59, 65, 73; Art 5(1)(d), 16
[5] GDPR Rec.50,59,69-70, 73; Art. 21
[6] GDPR Rec. 65-66, 68; Art. 17
[7] GDPR Art. 21
[8] GDPR Art. 90

7.8. When a data subject makes an application to exercise his/her data subject rights, the application must be handled immediately by the Responsible Person.

8. Appendix A: Terms and Definitions

A. **Personal Information** is information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

B. **Data are anonymised** if personal identity can never be traced by anyone, or if the personal identity could be recreated only with an unreasonable amount of time, expense and labour.

C. **Consent** is the voluntary, legally binding agreement to data processing.

D. **Data breach incidents** are events where there is justified suspicion that Personal Data are being illegally captured, collected, modified, copied, transmitted or used.

E. **Data subject** under this Policy is a natural person whose data can be processed. In some countries, legal entities can be data subjects as well.

F. **Sensitive data** are data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership or the health and sexual life of the data subject. Under certain national laws, other data categories can be considered sensitive or the content of the data categories can be structured differently.

G. **Personal Data** are all information about certain or definable natural persons. A person is definable for instance if the personal relationship can be determined using a combination of information with even incidental additional knowledge.

H. **Processing personal data** means any process, with or without the use of automated systems, to collect, store, organise, retain, modify, query, use, forward, transmit, disseminate or combine and compare data. This also includes disposing of, deleting and blocking data and data storage media. Processing personal data is required if the permitted purpose or justified interest could not be achieved without the personal data, or only with exceptionally high expense.

I. **Data Controller** is a natural or legal person, alone or jointly with others, who determine the purposes and means of the processing.

J. **Data Processor** is a natural or legal person, who processes personal data on behalf of the data controller.

K. **Responsible Person** is the person appointed by the parent company, Origin Enterprises PLC, for data protection responsibility within a business unit.