Introduction to Our Data Protection Policy and General Definitions

About Us

Where reference is made to 'we', 'us', 'our' and 'the company' this means Oxyplast UK Ltd which is registered as a limited company in England and Wales at companies house under the company number **5132917** and whose registered address is

Oxyplast UK Ltd

Bradley Hall Trading Estate

Units 37 & 37A

Bradley Lane

Standish

Lancashire

WN6 0XQ

Where reference is made to our data protection officer then our nominated data protection officer is Jayne Higgins and their contact details are jayne.higgins@oxyplastuk.com

Where reference is made to 'our website' or 'website' then this is defined as the website on which this notice appears.

General statement of data protection principles

- We respect the privacy of your personal data and we limit our processing of your data to the minimum necessary to complete our ordinary business operations.
- We will not hold your data for longer than is necessary to meet our financial and legal obligations
- We will not sell or transfer your details to a third party without your express and informed consent
- We will take due diligence and all reasonable measures to keep your data secure and private
- All relevant business practises are carried out in line with these principles and policies.

The background of GDPR regulations

The General Data Protection Regulations sets out a number of principles with regards to the handling and processing of personal data. There are 6 basic principles under the GDPR regulations which are

- **Lawfulness, fairness and transparency** – Any organisation that collects personal information must do so in compliance with the law, and be transparent in why it is collected the information and what type of data will be collected
- **Purpose limitation** – Organisations should only collect information for a specific purpose, clearly state what that purpose is and only collect data for as long as necessary to complete that purpose.
- **Data minimisation –** Organisations must only process the personal data that they need to achieve its processing purposes.
- **Accuracy –** Organisations must take every reasonable step to erase or rectify data that is inaccurate or incomplete
- **Storage Limitation –** Organisations should delete data when it is no longer necessary to keep it
- **Integrity and confidentiality -** The GDPR states that personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

Third Parties

Contracts between the company and any party whether employees, suppliers, data processors, other third parties or authorised individual are subject to these policies.

Specifically, where it is necessary to share any personal data with a third party (such as an accountant, payroll provider, pension authority, sub-contractor, supplier or data processor) we will undertake our best endeavour to ensure third-party compliance with our policies.

During the procurement and renewals of contracts we will undertake to ensure that the party is made aware of our policies and their requirement to act accordingly.

Our policy documents

Our policy documents which are available at our registered company address and where appropriate published on our website(s) include

- Introduction to our data policy and definitions (This document)
- Our data privacy notice for customers and suppliers
- Our data privacy notice for Employees
- Our data breach policy
- Our staff data protection training policy
- Our subject access request policy
- Our website terms of use
- Our website acceptable use policy
- Our cookie policy

These policies are subject to review and may be updated

GDPR: 8 rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

GDPR: 5 protection principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

i) at least one of the conditions in Schedule 2 is met, http://www.legislation.gov.uk/ukpga/1998/29/contents#sch2

ii) and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
http://www.legislation.gov.uk/ukpga/1998/29/contents#sch3

2) Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4) Personal data shall be accurate and, where necessary, kept up to date.

5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6) Personal data shall be processed in accordance with the rights of data subjects under this Act.

7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Definitions

Included below are the main definitions used in our GDPR policy documents. These are as defined in the following source https://gdpr-info.eu/art-4-gdpr/

GENERAL DEFINITIONS

GDPR – General data protection regulations. The full text of which can be found here https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

Data controller - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Data processor - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Data subject - Natural person that could be uniquely identified from the data

Processing - Any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Authorised Individuals including Third parties - A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Pseudonymisation - Pseudonymisation enhances privacy by replacing most of the identifying fields of personal data with an artificial identifier or pseudonym. Data encryption is an example of a data pseudonymisation process

Specifically, the GDPR defines pseudonymization in Article 3, as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." To pseudonymise a data set, the "additional information" must be "kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person."

Anonymisation – There is a legal distinction between anonymised and pseudonymised data in that pseudonymised data still allows for some form of re-identification or attribution to a data subject where anonymised data does not.

Responsibility - The Controller's responsibility to implement appropriate technical and organisational measures to ensure compliance with **GDPR**.

Types Of Data Storage

Data storage is the recording and storing on information on a storage medium, whether that be a physical media such as paper or microfiche, or a digital medium such as magnetic or optical devices or punched tape.

Physical data – Any data stored on a physical medium for example Paper or microfiche.

Digital storage – Any data stored electronically for example on a computer, phone, online or on a cloud service. Digital storage will also include data stored on magnetic, optical and punched tape devices as they are only electronically readable.

Categories of Data

Personal data -The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier such as a name, identification number, online identifier, location or address etc.

The GDPR applies to both; automated or digitally stored personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to an individual.

Sensitive and Special categories personal data

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9 https://gdpr-info.eu/art-9-gdpr).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10 https://gdpr-info.eu/art-10-gdpr).

Other examples include racial and ethnic origin, sexual orientation, health data, trade union membership and political opinions, religious or philosophical beliefs.