Edited by: Dusty S.r.l.

Approved by: Sole Director

Confidentiality Level: Low

Summary

1. Scope, purpose and addressees

DUSTY S.r.l., hereinafter referred to as the "Company", is committed to complying with applicable laws and regulations regarding the protection of personal data in the countries in which it operates. This Policy sets out the basic principles by which the Company processes the personal data of workers of client companies, customers, suppliers, business partners, employees and other persons and indicates the responsibilities of its business departments and employees when processing personal data.

This policy applies to the Company and the companies it directly or indirectly controls that conduct business within the European Economic Area (EEA) or that process the personal data of data subjects within the EEA.

The addressees of this document are all employees, whether permanent or temporary, and all contractors working on behalf of the Company.

2. Reference Documents

- The EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the European Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC)
- Guidelines of the Privacy Authority for the correct application of the GDPR
- Employee Personal Data Protection Policy
- Data Retention Policy
- Description of the Role of the Data Protection Officer
- Guidelines for the Data List and Mapping of Processing Activities
- Procedure for the Data Subject's Request for Access to Data
- Data Protection Impact Assessment Methodology
- Cross-Border Transfer of Personal Data Procedure
- IT Security Policy
- Data Breach Notification Procedure

3. Definitions

The following definitions of terms used in this document are taken from Article 4 of the European Union General Data Protection Regulation (or GDPR):

- **Personal Data**: any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable person is any natural person who can be identified, directly or indirectly, by reference in particular to an identifier such as a name, an identification number, location data, an online identifier or to one or more features of his or her physical, physiological, genetic, mental, economic, cultural or social identity.
- **Sensitive personal data**: Personal data which by their nature are particularly sensitive in terms of fundamental rights and freedoms and deserve specific protection, as the context of their processing is likely to create significant risks to fundamental rights and freedoms. Such personal data should also include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data intended to uniquely identify a natural person, data concerning the health or sex life or sexual orientation of the individual.
- **Data Controller**: The natural or legal person, public authority, service or other body which, individually or jointly with others, determines the purposes and means of the processing of personal data.
- **Data Processor**: a natural or legal person, public authority, service or other body that processes personal data on behalf of the Controller.
- **Processing**: any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic 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.
- **Anonymisation**: irreversible de-identification of personal data in such a way that the person cannot be identified using reasonable time, cost and technology on the part of the

controller or any other person to identify the data subject. The data protection principles should therefore not apply to anonymous information, i.e. information that does not relate to an identified or identifiable natural person.

- **Pseudonymisation**: the processing of personal data in such a way that personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and subject to technical and organisational measures to ensure that such personal data cannot be attributed to an identified or identifiable natural person. Pseudonymisation reduces, but does not completely eliminate, the possibility of linking personal data to the data subject. Since pseudonymised data are nonetheless personal data, the processing of pseudonymised data should be in accordance with the principles of Personal Data Processing.
- **Cross-border processing**: the processing of personal data which takes place in the course of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or the processing of personal data which takes place in the course of the activities of a single establishment of a controller or processor in the Union, but which affects or is likely to affect substantially data subjects in more than one Member State.
- **Supervisory Authority**: The independent public authority established by a Member State pursuant to Article 51 of the EU GDPR; for Italy it is the Privacy Authority.
- **Lead Supervisory Authority**: The supervisory authority with primary responsibility for managing a cross-border data processing activity, e.g. when a data subject lodges a complaint about the processing of their personal data; it is responsible for, among other things, receiving data breach notifications, being notified about risky processing activities and will have full authority regarding its functions to ensure compliance with the provisions of the EU GDPR.

Each "**local supervisory authority**" will, however, maintain in their territory and monitor any local data processing that affects data subjects or is carried out by a controller or processor within the Union or outside the Union in case their processing targets data subjects residing on their territory. Their tasks and powers include conducting investigations and applying administrative measures and sanctions, promoting public awareness of the risks, rules, security and rights in relation to the processing of personal data, as well as access to any premises of the data controller and processor, including any tools and means for processing.

"Main establishment in relation to a controller" with establishments in more than one Member State, the place of its central administration in the Union, unless decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to order the implementation of such decisions, in which case the establishment having taken such decisions shall be considered to be the main one.

"Main establishment with reference to a processor": a controller with establishments in more than one Member State, the place where its central administration in the Union is located or, where the controller does not have a central administration in the Union, the establishment of the controller in the Union where the main processing activities are conducted in the context of the

activities of an establishment of the controller in so far as that controller is subject to specific obligations under this Regulation.

"Business group": a group consisting of a parent undertaking and its controlled undertakings.

4. Principles Applicable to the Processing of Personal Data

The Principles Applicable to Data Protection outline the responsibilities of organisations in handling personal data. Article 5(2) of the GDPR states that "the controller shall be responsible for compliance with the principles, and able to provide evidence thereof."

4.1. Lawfulness, Correctness and Transparency

Personal data shall be processed lawfully, correctly and transparently towards the data subject.

4.2. Purpose Limitation

Personal data are collected for specified, explicit and legitimate purposes, and subsequently processed in a way that is not incompatible with those purposes.

4.3. Data Minimisation

Personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The company shall apply anonymisation or pseudonymisation to personal data, where possible, to reduce the risk to data subjects.

4.4. Accuracy

Personal data shall be accurate and, where necessary, kept up to date; all reasonable steps shall be taken to delete or rectify, in a timely manner, data that are inaccurate in relation to the purposes for which they are processed.

4.5. Limitation of the Period of Retention

Personal data are kept for a period of time not exceeding the achievement of the purposes for which they are processed.

4.6. Integrity and Confidentiality

Considering available technologies and other security measures, the costs of implementation and the likelihood and severity of risks to personal data, the Company shall implement technical and organisational measures to ensure an adequate level of security for personal data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

4.7. Accountability

Data controllers are responsible for compliance with the principles described above and are able to prove it.

5. Building data protection in business activities

In order to demonstrate compliance with data protection principles, an organisation must create data protection in its business activities.

5.1. Notification of Interested Parties

(See section 6 - Guidelines on Fair Processing - Point 1)

5.2. Data Subject Choice and Consent

(See Section 6 - Fair Processing Guidelines - Paragraph 2)

5.3. Collection

The Company is committed to collecting as little personal data as possible. If personal data is collected by a third party, the Controller ensures that the personal data is collected lawfully.

5.4. Use, Storage and Disposal

The purposes, methods, storage limit and retention period of personal data are consistent with the information contained in the Privacy Policy. The company maintains the accuracy, integrity, confidentiality and relevance of personal data according to the purpose of processing. The company uses appropriate security mechanisms to protect personal data against theft, misuse or abuse and to prevent personal data breaches. The Data Protection Officer is responsible for compliance with the requirements listed in this section.

5.5. Disclosure to third parties

Whenever the Company uses a third-party supplier or business partner to process personal data on its behalf, the Data Protection Officer ensures that this processor provides security measures to safeguard personal data that are appropriate to the associated risks. To this end, the Company uses the Processor's GDPR Compliance Questionnaire.

The Company contractually requires the supplier or business partner to provide the same level of data protection. The supplier or business partner must only process personal data to fulfil its contractual obligations to the Company or on the Company's instructions and not for any other purpose. When the Company processes Personal Data jointly with an independent third party, the Company explicitly specifies its own responsibilities and those of the third party in the relevant contract or any other binding legal document, such as the Data Processing Provider Agreement.

5.6. Cross Border Transfer of Personal Data

Before transferring personal data from the European Economic Area (EEA), appropriate safeguards must be in place, including the signing of a data transfer agreement as required by the European Union and, where necessary, permission must be obtained from the relevant Data Protection Authority. The entity receiving the personal data must comply with the principles of personal data processing set out in the Cross-Border Transfer of Personal Data Procedure.

5.7. Right of Access by Data Subjects

The Data Protection Officer is responsible for providing data subjects with a reasonable access mechanism to enable them to access their personal data and allow them to update, rectify, erase

or transmit their personal data. The access mechanism will be further detailed in the Data Subject's Data Access Request Procedure.

5.8. Data Portability

Data subjects have the right to receive, upon request, a copy of the data they have provided to us in a structured format and to transmit this data to another controller, free of charge. The Data Protection Officer is responsible for ensuring that such requests are processed within one month, are not excessive and do not affect the personal data rights of other persons.

5.9. Right to be forgotten

Upon request, data subjects have the right to obtain from the Company the deletion of their personal data, when this right is not in conflict with other legislation (Legislative Decree 81/08 as amended). When the Company acts as Controller, it shall take the necessary actions (including technical measures) to inform third parties who use or process such data to comply with the request.

6. Guidelines on Fair Processing

Personal data must only be processed if explicitly authorised by the Controller.

The Company carries out the Data Protection Impact Assessment for each data processing activity according to the Data Protection Impact Assessment Guidelines.

6.1. Communications to Data Subjects

At the time of or prior to the collection of personal data for any type of processing activity, including but not limited to, the sale of products, services or marketing activities, the Data Controller is responsible for adequately informing Data Subjects of the following: the types of personal data collected, the purposes of processing, the methods of processing, the rights of Data Subjects with respect to their personal data, the retention period, potential international data transfers, whether data will be shared with third parties and the Company's security measures to protect personal data. This information is provided through a Privacy Policy.

Where personal data is shared with third parties, the Data Protection Officer must ensure that data subjects have been informed of this through a Privacy Notice.

Where personal data is transferred to a third country under the cross-border data transfer policy, the Privacy Notice should reflect this and clearly state where and to whom the personal data is transferred.

Where sensitive personal data is collected, the Data Protection Officer must ensure that the Privacy Notice explicitly states the purpose for which such sensitive personal data is collected.

6.2. Obtaining Consents

Whenever the processing of personal data is based on the consent of the data subject, or other lawful grounds, the Data Protection Officer is responsible for keeping a record of that consent; he or she is also responsible for providing data subjects with options for giving consent and must inform them and ensure that their consent (whenever consent is used as a lawful basis for processing) can be withdrawn at any time to the extent permitted by applicable law.

Where the collection of personal data relates to a child under the age of 16, the Data Processor shall ensure that the consent of the holder of parental responsibility is provided prior to collection using the consent form of the holder of parental responsibility.

When requests are made to correct, amend or destroy personal data records, the Data Protection Officer ensures that such requests are dealt with within a reasonable time. He records the requests and keeps a record of them.

Personal data is only processed for the purposes for which it was originally collected. If the Company wishes to process the personal data collected for another purpose, the Company requires the consent of the data subjects in clear and concise written form. Any such request shall include the original purpose for which the data was collected and also any new or additional purposes. The request also includes the reason for the change in purpose(s). The Data Protection Officer is responsible for ensuring compliance with the rules in this paragraph.

Now and in the future, the Data Controller together with the Data Protection Officer shall ensure that collection methods comply with the law, good practice and relevant industry standards.

The Data Protection Officer is responsible for creating and maintaining a register of Privacy Notices.

7. Organisation and Responsibility

The responsibility for ensuring the adequate processing of personal data falls to everyone who works for or with the Company and has access to the personal data processed by the Company.

The main areas of responsibility for the processing of personal data are the following organisational roles:

Chief Executive Officer: makes decisions and approves the Company's general data protection strategies.

The **Data Protection Officer**: is responsible for managing the personal data protection programme and is responsible for developing and promoting personal data protection policies from start to finish, as defined in the Data Protection Officer Role Description.

The **Legal Advisor**, together with the **DPO**, monitors and analyses personal data laws and regulatory changes, develops compliance requirements, and assists business departments in achieving their personal data objectives.

The **IT Manager** is responsible for:

- Ensuring that all systems, services and equipment used to record data meet acceptable security standards.
- Conducting regular checks and scans to ensure that security hardware and software are working properly.

The **Communications** Department is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.

- Responding to any data protection queries from journalists or media such as newspapers.
- Where necessary, working with the Data Protection Officer to ensure that marketing initiatives comply with data protection principles.

The **Human Resources Manager** is responsible for:

- Improving all employees' awareness of the protection of users' personal data.
- Organise data protection skills and awareness training for employees working with personal data.
- Protect employees' personal data from start to finish. Ensure that employees' personal data is processed in accordance with the employer's legitimate business purposes and needs.

The **Purchasing Manager** is responsible for transferring personal data protection responsibilities to suppliers and improving suppliers' levels of awareness of personal data protection, as well as the downward flow of required personal data to any third party suppliers the company uses. The Procurement Department must ensure that the Company reserves the right to conduct an audit of suppliers.

8. Guidelines for Establishing the Lead Control Authority

The Company is not currently in a position to apply the requirements of point 8; should it be in such a position, it will apply the rule as described below.

8.1. Need to Establish the Lead Control Authority

Identifying a Lead Supervisory Authority is only necessary if the Company carries out cross-border processing of personal data.

Cross-border processing of personal data occurs if:

a) The processing of personal data is carried out by subsidiaries of the Company established in other Member States;

or

(b) the processing of personal data takes place in the course of the activities of a single establishment of a Company in the Union, but affects or is likely to affect substantially data subjects in more than one Member State.

If the Company has establishments only in one Member State and its processing activities affect only data subjects in that Member State, there is no need to establish a Lead Supervisory Authority. The only competent authority will be the supervisory authority in the country where the Company is legally established.

8.2. The Main Establishment and the Lead Control Authority

8.2.1. The Main Establishment for the Data Controller

The Company Administrator must identify the main establishment so that the Lead Control Authority can be determined.

If the Company is established in a Member State of the Union and makes decisions concerning cross-border processing activities instead of its central administration, there will be a single lead supervisory authority for the data processing activities carried out by the Company.

If the Company has multiple establishments that act independently and make decisions about the purposes and means of processing personal data, the Company's senior management must recognise that there is more than one lead supervisory authority.

8.2.2. The Main Establishment for the Data Processor

In the event that the Company acts as a data processor, the main establishment will be the seat of central administration. Where the central administration location is not in the EU, the main facility will be the establishment in the EU where the main processing activities take place.

8.2.3. The Main Establishment for Companies outside the Union for Controllers and Data Processors

If the Company does not have a main establishment in the Union and has no subsidiary companies in the EU, it must appoint a representative in the EU and the relevant supervisory authority will be the local supervisory authority where the representative is located.

9. Responding to Personal Data Breach Incidents

When the Company becomes aware of a suspected or actual personal data breach, the Data Protection Officer will conduct an internal investigation and take appropriate corrective action in a timely manner in accordance with the Data Breach Policy. Where there is a risk to the rights and freedoms of data subjects, the Company shall inform the relevant data protection supervisory authority without undue delay and, where possible, within 72 hours.

10. Audit and Accountability

The Data Protection Officer is responsible for auditing how company departments implement this Policy.

Any employee who violates this Policy will be subject to disciplinary action and may also be subject to civil or criminal liability if his/her conduct violates laws or regulations.

11. Conflicts with Law

This Policy is intended to comply with the laws and regulations of the place of establishment and the countries in which DUSTY S.r.l. operates. In case of conflict between this Policy and applicable laws and regulations, the latter will prevail.

12. Records management in accordance with this document

Name of document	Place of archiving	Person responsible for archiving	Document protection controls	Archiving time
Data Subject Consent Form	Company server GDPR DUSTY folder	Data Protection Officer	Only authorised persons may access the forms	10 years
Data subject withdrawal form	Company server GDPR DUSTY folder	Data Protection Officer	Only authorised persons may access the forms	10 years
Parental Responsibility Holder Consent Form	Company server GDPR DUSTY folder	Data Protection Officer	Only authorised persons may access the forms	10 years
Parental Responsibility Holders Withdrawal Form	Company server GDPR DUSTY folder	Data Protection Officer	Only authorised persons may access the forms	10 years
Agreements with Data Processing Providers	Company server GDPR DUSTY folder	Data Protection Officer	Only authorised persons may have access to the folder	5 years after contract termination
Privacy Policy Register	Company server GDPR DUSTY folder	Data Protection Officer	Only authorised persons may have access to the folder	Permanent

13. Validity and document processing

This document shall take effect on 11/02/2019.

The person responsible for this document is the Data Controller, who instructs the Data Protection Officer to check and, if necessary, update the document at least once a year.