

DEDALUS GROUP GLOBAL DATA PROTECTION POLICY

Dedalus' Commitment to the Protection of Personal Data

INTRODUCTION

The Dedalus Group Global Data Protection Policy (the “**Policy**”) articulates the data protection principles followed by the Dedalus Group (“**Dedalus**”), its business units, and its employees around the world with regards to personal data processing.

These principles are aligned to the highest standards in international trade and commerce and human resource management. Dedalus's commitment to these high standards reflects the value we place on earning and maintaining the trust of our employees, clients, business partners, and other stakeholders whose data is shared with us.

Dedalus will process personal data in accordance with this Policy and the applicable data protection laws.

In the regular course of business, Dedalus collects personal data from its customers, suppliers, employees, website users, job applicants, contractors, shareholders, partners , , other third parties and exceptionally, for products used directly by end users, may collect data from end users.

Dedalus recognises that personal data must be treated with caution. We are committed to conducting our business in accordance with all relevant data protection laws of the countries in which we operate and in line with the highest standards of ethical conduct.

If you have questions or comments about this policy, please contact us at dpo.group@dedalus.eu

SCOPE AND APPLICABILITY

This Policy applies to all Dedalus affiliates and entities. It defines the conduct expected of each Dedalus employee, officer, and director when processing data of Dedalus' customers, suppliers, employees, website users, job applicants, contractors, shareholders, partners, end users of the services, and other third parties.

Personal data may be collected from individuals through a variety of means, including, for example, through websites, other ordering channels, and service or employment processes.

This Policy aims to facilitate data protection by design and by default principles in the engineering and implementation of systems and processes by Dedalus. Therefore, among other things, it is intended to govern customer and employee data protection policies, and to influence system implementation standards, rulebooks, business processes, applications, web, product, and service developments, and technology roadmaps.

This Policy is designed to ensure that personal data will be protected regardless of geography or technology, when used within the Dedalus Group, and applies to Dedalus' processing of personal data.

This Policy is organised around five underlying commitments:

1. Collecting and processing personal data fairly and lawfully
2. Respecting individual rights and choices
3. Managing personal data responsibly and securely
4. Implementing the data protection by design and by default paradigms
5. Cooperation with Supervisory Authorities

This Policy defines Dedalus' uniform and baseline standards which apply in the absence of more stringent rules which may be mandated by local laws.

To the extent legally required or permitted by national laws, this Policy applies worldwide to all directors, officers, executives, employees, and contracted representatives of all Dedalus companies. As well, specific practices shall be tailored to meet the legal, regulatory, and cultural requirements of the countries and regions in which Dedalus operates. Furthermore, in all cases where the negotiated terms in any Dedalus service agreement call for a level of protection for the data processed by or entrusted to Dedalus which exceeds minimal legal requirements, then those negotiated terms shall prevail.

Internal implementation rules, guidelines and training are provided with all necessary supporting documentation to act according to this Policy.

KEY COMMITMENTS

Dedalus is committed to complying with applicable data protection laws. Dedalus is audited regularly internally and by third parties, maintains certifications, and provides industry-standard contractual protections and appropriate technical and organizational measures to strengthen the compliance with applicable data protection laws.

Dedalus will process personal data only as permitted or required by applicable laws and in accordance with the following data protection principles.

COLLECTING AND PROCESSING DATA FAIRLY AND LAWFULLY

Dedalus informs clearly, honestly, and transparently about the nature of the data it collects and what it intends to do with it. The use of data by Dedalus for a different purpose than initially communicated is not authorised, unless adequate information is provided to the concerned individuals, and where applicable, consent for the intended use is given to Dedalus. In general, Dedalus is authorised to use data for secondary purposes when implementing internal controls and audits and complying with its statutory and regulatory obligations.

Dedalus processes data only to the extent that an appropriate legal basis exists, such as a valid and informed consent, Dedalus' legitimate business interests, and/or the necessity to enter or perform contracts and complying with statutory or regulatory commitments.

Any consent given by individuals to the collection and use of their data must be given freely and in response to a clear information by Dedalus about the intended use of the data. Such consent can be withdrawn anytime by the individual without undue complications.

When processing data on behalf of a client or another third party, Dedalus will comply with the guidelines and instructions of the data controller in addition with this Policy.

Dedalus will take reasonable steps to, and where Dedalus is a processor provide customers with a means to, ensure that data is accurate and updated, keep personal data only for as long as necessary for the purposes for which it is collected and used, and to delete or render it anonymous after such retention requirements have been met.

RESPECTING INDIVIDUALS' RIGHTS AND CHOICES

Dedalus recognises the rights of individuals to:

- Request access to the data collected on them by Dedalus and the reason for Dedalus having such data
- Obtain a copy of the personal data held on them

- Request the rectification or deletion of inaccurate or incomplete data
- Withdraw consent given to Dedalus for the collection of their data at any time.

Dedalus will respond to requests made by individuals exercising their rights within a reasonable period after the individual's request or within any specific period that may be required by applicable local laws. Dedalus will handle and investigate complaints made by individuals about any breach of these rules or data protection laws and will respond to such complaints in a timely manner.

We respect customers' rights to object to the use of their data or to opt out of receiving direct marketing communications. When using personal data for marketing purposes, Dedalus will inform individuals in a clear and plain language about the use of their data for such purposes. Dedalus respects the right of its existing and prospective customers to:

- only receive marketing communications from Dedalus if an explicit and specific prior consent has been provided, when required by applicable laws, or if Dedalus can demonstrate that it is authorised to send such communications for its legitimate business purposes
- no longer receive any marketing communications if a specific preference setting, an opt-out or an objection to use such data for marketing purposes has been received by Dedalus.

We use sensitive personal data only if it is necessary. Dedalus recognises that some categories of personal data are particularly sensitive and require a higher level of protection. Sensitive data includes information regarding a person's health, biometric and genetic data, religion, and political opinions, racial or ethnic origin, criminal records and any other information protected specifically by the relevant applicable data protection laws.

Dedalus implements adequate procedures and safeguards to restrict access to sensitive data only by appropriate persons and prevent its unauthorised access, use and dissemination.

MANAGING DATA RESPONSIBLY AND SECURELY

Dedalus is accountable for fulfilling the requirements sets out in this Policy and under applicable law. Dedalus takes the necessary measures to observe the requirements of this Policy and applicable law and have the necessary internal mechanisms in place to demonstrate such observance.

Dedalus employs data protection practices designed to support its compliance with this Policy and applicable law and provides internal controls to verify compliance with data protection laws and related Dedalus policies and procedures.

Dedalus strives to protect data with appropriate technical and organizational measures to ensure their confidentiality, integrity, and availability and to prevent the risk of unauthorised or unlawful access, alteration, destruction, or disclosure.

As far as Dedalus has been managing the data and the security breach was directly involving Dedalus systems and services Dedalus will inform individuals of a security breach affecting their data that could pose a high risk to their rights and freedoms in accordance with applicable laws.

Dedalus requires from its suppliers or subcontractors that they fully comply with Dedalus data protection policies and any applicable data protection legislation and maintain adequate technical and organisational security measures to protect data.

Dedalus limits data access to its employees or suppliers who need to perform specific tasks in relation with such data. Dedalus makes available training and programs to educate and raise awareness

among employees for their individual and collective legal, regulatory, and contractual responsibilities regarding data processing.

In accordance with applicable law, Dedalus provides reasonable assistance to its customers, where Dedalus is a processor, to ensure the security of their processing and will inform the customers of a security breach as required under such laws.

When data is transferred, we ensure that we have taken steps to protect them before transfer. Dedalus transfers personal data across national boundaries only when this is justified for business purposes and safeguards exist to ensure that data will continue to be adequately protected in the jurisdiction of destination.

If the processing is likely to result in a high risk to individuals, Dedalus conducts an impact assessment to identify risks that the processing may cause to the rights of individuals and eliminate or reduce such risks.

Dedalus has set a global data protection office which is responsible to implement this Policy, to promulgate additional data protection related policies, and to provide strategically coordinated data protection related compliance and other services and resources to the Dedalus business units.

IMPLEMENTING THE DATA PROTECTION BY DESIGN AND BY DEFAULT PARADIGMS

Dedalus, from the moment in which data processing activity is designed, implements appropriate technical and organisational measures to effectively implement the principles of data protection, and integrates the necessary safeguards into the processing to meet the regulatory requirements and protect the rights of individuals, considering the technology state of the art, the cost of implementation and the nature, scope, context and purposes of processing, and the risks for rights and freedoms of individuals posed by the data processing.

Dedalus also guarantees that, by default, only data that is necessary for each specific purpose of the processing are processed. This obligation applies to the amount of data collected, the extent of processing, the retention period, and the accessibility to the data.

To adhere to these principles, Dedalus business units must, whenever designing or carrying out new projects, services, systems, or products that entail data processing, ensure they meet the requirements of data protection by design and by default. For this purpose, Dedalus also requires specific pertinent safeguards and functions from suppliers, software developers and other third parties during the design phase of such projects. Wherever a new project, service, system, or activity implies data processing, the business unit engaging in this activity must verify the technical documentation, safeguards, functions, and measures adopted to ensure data minimisation and minimisation of the potential risks for the individuals.

COOPERATION WITH SUPERVISORY AUTHORITIES

Dedalus will cooperate with any competent national or regional supervisory authority responsible for supervising applicable data protection law that has good cause to question any processing of personal data by Dedalus and will comply with such competent supervisory authority's decisions on any issue related to this Policy.

VIOLATIONS

Non-compliance with this Policy may be regarded as a serious breach of the trust Dedalus must be able to place in its staff. Non-compliance by an employee may therefore result in a sanction, such as

suspension or other disciplinary measures or measures under labour law. Non-compliance by staff members that are not employees may result in termination of the relevant contract. Staff will not be penalized for raising issues relating to compliance with this Policy.

CHANGES TO THIS POLICY

This Policy supersedes all previous Dedalus data protection policies to the extent they address the same issues and are not consistent with this Policy or impose less restrictive requirements.

Dedalus reserves the right to modify this Policy. Any material changes will be notified on Dedalus's website.

CONTACT DETAILS OF DATA PROTECTION OFFICER

We also have appointed a data protection officer (“**DPO**”), which you can contact by e-mail at the following address:

for Dedalus S.p.A dpo.group@dedalus.eu

for companies based in UK dpo-uk@dedalus.group.

for companies based in France dpo.france@dedalus.eu

for companies based in Germany/Austria dpo.dach@dedalus.com

for companies based in Italy dpo@dedalus.eu

Current version: Dedalus – privacy policy – v. 2

Last updated: October 2025