Policy

Privacy Policy

v.5 November 2025

amadeus

Amadeus
Digital Trust Office

Document control				
Security level	Public			
Company	Amadeus IT Group SA			
Department	Digital Trust Office (DTO)			
Author	DTO			
Version	Date	Change	Comment	By
v.1	January 2022	N/A	First Version	GPO
v.2	January 2023		Annual Review	GPO
v.3	January 2024		Annual Review	GPO
v.4	24/07/2025	Security level changed to public to ensure the Policy can be shared, reviewed privacy governance and reviewed privacy principles.	Annual Review	GDAO
v.5	14/11/2025		Minor amendments	GDAO
	29/05/2026		Rebranding	DTO

amadeus

1 Purpose

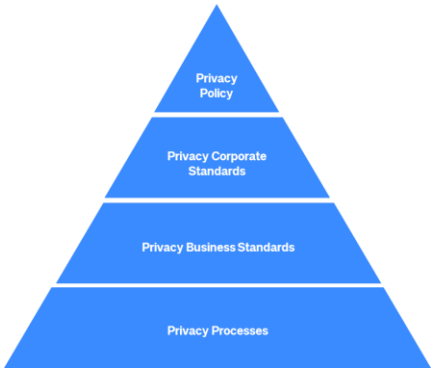
This Privacy Policy ("Policy") outlines Amadeus's main obligations in accordance with applicable privacy laws when processing personal data, and what employees must consider when:

- processing personal data; and/or
- designing products, services, processes, or activities involving personal data.

Personal data includes any information that can directly or indirectly identify an individual, such as a name, ID number, record locator, or IP address. Some types of personal data, due to its sensitivity, are subject to stricter requirements when handled. These types of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. Information related to criminal convictions and offences is also subject to stricter requirements.

If you are unsure whether certain information is personal data, treat it as personal data and consult your relevant privacy contact. It is important to note that **pseudonymised data**, which has been processed to make it more difficult to identify individuals, is still considered as equivalent to personal data and therefore subject to the same legal requirements as personal data.

This **Policy** is supplemented by:



Corporate Standards, that offer more detailed guidelines on certain aspects of privacy compliance applicable to the whole Amadeus organization.

Business Standards, that offer more detailed guidelines on certain aspects of privacy compliance applicable to one Unit, but not to all Units.

Processes, that outline the steps to follow in specific situations. Some processes apply universally within the Amadeus group, while others are tailored to specific teams or stakeholders.

The above address the following areas:

- Governance
- Lawfulness
- Transparency
- Data retention
- Data minimization
- Privacy by design
- Respect for individuals' rights
- Accountability
- Purpose limitation
- Contractual requirements
- Regulatory monitoring
- Risk management

- Privacy by default
- Compliance monitoring and reporting

2 Scope

This Policy applies to **all Amadeus group entities**, employees, contractors, temporary workers, trainees, vendors and other business partners with access to personal data, regardless of their location.

3 Periodic Revision

This policy is reviewed **annually** or updated earlier if deemed necessary prior to the scheduled review.

4 Privacy Principles

Amadeus group entities, including employees and contractors, follow global privacy obligations consolidated into **6 Privacy Principles**:

4.1 Lawfulness

Personal data must be obtained legally (i.e., without violating any applicable laws – e.g., not obtained through force, threat, or deceit) and must be processed upon the existence of an appropriate legal basis, among those foreseen in applicable laws (e.g., consent, fulfilment of an agreement, compliance with a legal obligation, legitimate interest, etc.).

The lack of an appropriate legal basis for the processing of personal data will require the deletion of such data.

It is not appropriate to retain personal data solely for potential future use without a specific purpose or need.

4.2 Transparency

The processing of personal data is inherently associated with a duty of transparency. Beneficiaries of this transparency requirement can be customers when the processing activity occurs at their initiative (for instance, when customers request Amadeus to provide a service that involves processing travellers' personal data), or individuals whose personal data is being processed when the processing activity is initiated by

Amadeus (for example, when Amadeus processes the personal data of its employees or contractors or when Amadeus processes the personal data concerning its points of contact within its vendors or partners).

4.3 Proportionality

The processing of personal data should be limited and restricted to the greatest extent possible. Specifically:

- The purposes for which personal data is processed must be confined to those communicated to the customer and/or the individual whose personal data are being processed. The purpose must also be determined prior to the commencement of the data processing.
- The sharing of personal data, both internally and with external parties or third parties, must be highly restricted and must be done in accordance with legal and privacy requirements.
- The retention period for personal data should be minimized. The retention period must be determined taking into consideration the purpose for which the personal data is processed. The amount of personal data processed, including both in terms of the number of records and the categories of personal data, should be limited to the minimum necessary to achieve the intended purposes.

4.4. Privacy by Design

Privacy compliance must be considered from the inception of any initiative that involves the processing of personal data. Therefore, each initiative involving such processing (or any change to existing data processing activities) requires thorough review before any actual processing occurs.

The Privacy by Design Corporate Standard and its associated processes are essential for ensuring privacy compliance at Amadeus. A review of every single intended activity is required as to:

- Obtain the necessary information to meet privacy compliance requirements (i.e., to ensure the record of processing activity is kept as required by applicable laws);
- Evaluate the privacy risks associated with the proposed activity; and
- Ensure these risks are understood and managed appropriately in accordance with relevant risk management protocols.

4.5 Respect for Individuals' Rights

All personal data processing activities must respect individuals' rights. By design, any personal data processing activity must allow for the ability to:

- Easily extract information related to an individual in a common, simple and machine-readable format;
- Delete personal data of an individual;
- Rectify personal data concerning an individual;
- Put on hold the processing of an individual's personal data, for a certain period or indefinitely; and
- Apply human intervention in cases where significant automatic decisions are made over an individual whose personal data are being processed.

4.6 Security

All personal data must be processed securely, ensuring its **ongoing confidentiality, integrity and availability**. The Security Policies and Standards are to be implemented across the Amadeus organization in accordance with the CISO governance structure.

Please check all Security Policies and Standards for further information.

5 Privacy Governance

To ensure the thorough implementation of these principles throughout the organization, Amadeus has instituted a comprehensive privacy governance framework.

The **Digital Trust Office** is responsible for the following tasks:

- Privacy vision and mission: defining the organization's privacy vision and mission statement to guide the privacy program
- Privacy strategy: developing a comprehensive privacy strategy that aligns with regulatory requirements and organizational goals
- Privacy team structure: structuring the privacy team with clear roles and responsibilities to ensure efficient and visible privacy management.
- Managing the privacy program:
    - Scope and objectives: defining the scope and objectives of the privacy governance program.

- Data inventory and mapping: working with the Amadeus Data Office to ensure comprehensive inventory and mapping of personal data to understand data flows and processing activities.
- Privacy policies, standards and processes: defining and updating privacy policies, standards and processes to guide data handling practices.
- Training and awareness: implementing training and awareness programs to educate employees about privacy requirements and best practices.
- Continuous monitoring: conducting continuous monitoring and auditing of data practices to ensure compliance.

Business Compliance Office: this office is part of the second line of defence and is integrated within a business unit or corporate function. Its responsibility is to ensure adherence to Amadeus' privacy policies, standards and processes, thereby guiding data handling practices within its respective business unit or corporate function.

The Digital Trust Office is required to report to the Amadeus Risk & Compliance Board on a regular basis on material privacy compliance issues:

- Maturity and effectiveness of our program, policies and processes, and escalation of major threats.
- The status of regulatory probes.
- Material risks including emerging risks impacting our compliance efforts.

Additionally, some Amadeus group entities have appointed a **Data Protection Officer** in compliance with applicable laws, whose main functions include:

- Assessing processing activities that are considered to be high risk by the Digital Trust Office.
- Reviewing notification requirements following incidents affecting personal data.
- Dealing with data subject requests directly addressed and/or escalated to the Data Protection Officer.
- Acting as main point of contact before the relevant data protection authorities.
- Internally reporting and escalating potential non-compliances.

6 Training and Awareness

This Policy is a key component of the mandatory training program that all employees are required to complete upon commencement of their employment with Amadeus, and subsequently on an annual basis. The training may involve an assessment that employees must successfully pass.

7 Privacy Objectives

Privacy objectives must always be aligned with Amadeus' overall objectives. These are reviewed annually to ensure they remain synchronised with Amadeus' strategic direction and risk appetite. In their revision, we make the necessary adjustments as to maintain the alignment with Amadeus' evolving priorities.

8 Monitoring Compliance

Adherence to this Policy is required of all Amadeus employees, trainees, contractors, and temporary workers. Compliance with this Privacy Policy is overseen through the following mechanisms:

- Key Performance Indicators ("KPIs") established by the Digital Trust Office, which are reported periodically to the relevant stakeholders.
- Regular audits, including internal audits conducted by the Group Internal Audit team and external audits carried out by independent third parties.

9 Non-compliance

Failure to comply with privacy laws may result in substantial economic fines for Amadeus and could significantly impact the company's reputation.

Non-compliance with this Policy may result in disciplinary action, up to and including termination of employment or engagement.

Employees are encouraged to report instances of non-compliance through the Speak Up reporting channel. Those who report misconduct or concerns in good faith will not face retaliation. For more information, please refer to the Speak-up Policy.