DATA4DEALS

Data Protection Policy

Version: 1.0 | **Last Update**: 29 October 2024

José Figueiredo
CEO

At Data4Deals, we see ethics and integrity as the foundation of our journey.
Trust is the foundation of the relationships with our partners, investors and clients. Each and everyday, we set a high standard for each of us and we apply it to everything we do. These standards push us to hold ourselves and each other accountable for results and, as important as results, for how we reach such results.

The protection of information, data and our systems is not just a priority for us — it is a cornerstone of how we operate. We demand our own adherence to the highest industry standards and continually push ourselves to exceed them. From robust technical safeguards to comprehensive policies and employee training, we take measures to ensure that information is handled with the utmost care and confidentiality, maintaining that trust by upholding the principles of security, transparency, and accountability in each action we take.

Our commitment to serve aiming at extraordinary results by doing the right thing is the reason why our partners rely on us, employees trust us and shareholders invest in us.

This Policy is merely an example of how we operate, reflecting our strong commitment to these principles.

01

INTRODUCTION

INTRODUCTION

Data4Deals is a company specialized in delivering card-based personalized rewards programs for financial institutions. In the scope of its activity, Data4Deals's activity and solutions may imply processing of personal data directly or indirectly from the data subjects, such as employees, contractors, merchants, business partners, clients and clients' customers ("**data subjects**").

Taking into consideration the increasing relevance that privacy and data protection represents to data subjects - but also the fact that the entities who subscribe Data4Deals solutions, are obliged to comply themselves with data protection, principles, laws, and regulations -, the present Policy is intended to be an essential step towards developing a governing strategy regarding personal data protection. This Data Protection Policy ("**Policy**") establishes the general principles to be considered in the processing and protection of personal data for which the companies that constitute Data4Deals are responsible.

To this end, Data4Deals acts in strict compliance with the principles described in this Policy, Regulation (EU) 2016/679 (General Data Protection Regulation), Law No. 58/2019 of August 8 (Portuguese Data Protection Law), and other applicable data protection legislation in all personal data processing activities under its responsibility **("data protection laws").**

This Policy is part of the Privacy Program, the normative framework for personal data protection of Data4Deals, and is complemented by other documents, which include rules and procedures for managing the security and privacy of personal data.

02

PURPOSE

PURPOSE

01

Align the Data Protection Strategy
Ensure that Data4Deals remains up-to-date with emerging laws, and industry standards for data protection. This includes a periodic review of policies, and practices to ensure the company meets its legal obligations, while also leveraging best practices for data protection.

02

Ensure Awareness Transparency
Provide clear, accessible, and detailed explanations of how personal data is collected, used, shared, and stored by Data4Deals, ensuring data subjects and stakeholders are aware of the purposes behind data processing activities.

03

Promote Data Protection Rights
Ensure that data subjects can easily exercise their data protection rights through accessible channels and processes (Cf. Section 6 of this Policy).

04

Continuous Improvement
Foster continuous improvement of processes related to the security and protection of personal data.

05

Enhance Protection Mechanisms
Increase the effectiveness of mechanisms for protection, response, notification, and communication of personal data breaches.

06

Strengthen Trust
Reinforce and consolidate the relationship of trust between Data4Deals and all its stakeholders. This involves clear communication, accountability, and the consistent implementation of privacy practices that reinforce Data4Deals's commitment to ethical data handling

03

SCOPE OF APPLICATION

SCOPE OF APPLICATION

This Policy applies exclusively to the processing of personal data carried out by all companies that are part of the Data4Deals group, including all subsidiaries, affiliates, joint ventures, and any other entities controlled, directly or indirectly, by Data4Deals, regardless of their geographic location.

The present Policy must be respected and applied by all employees regardless of the nature of their position, service providers and other associates of Data4Deals in activities that may directly or indirectly influence the processing of personal data.

Employees of Data4Deals must be aware of and comply with this and other policies, standards, and procedures included in the Data4Deals Privacy Program.

04

DEFINITIONS

DEFINITIONS

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.

Processor
Means the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the Controller.

Personal data
Means any information of any type relating to an identified or identifiable natural person ("**data subject**"). A person can be identified, directly or indirectly, in particular by reference to identifiers such as name, an identification number, location data, online identifiers, as logins, and other access credentials or, other factors, inter alia, physical, physiological, genetic, economic, cultural or social.

Special categories of personal data
Means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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.

Processing
Means any operation or set of operations performed upon personal data, regardless its manual, logical or automatic nature. Therefore, operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, combination, erasure or destruction, are always data processing.

Consent
Means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

Personal data breach
Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

05

DATA PROTECTION PRINCIPLES

DATA PROTECTION PRINCIPLES

The principles set forth in this Policy shall be considered in the design and implementation of all procedures involving the processing of personal data, as well as in the products and services offered by Data4Deals, and in any contracts entailing the processing of personal data. Additionally, they shall be implemented in all systems and platforms that allow access by Data4Deals professionals or third parties to personal data and the collection or processing of such data.

Therefore, the principles upon which this Policy is founded are detailed below:

LAWFULNESS, FAIRNESS AND TRANSPARENCY

The processing of personal data shall be legitimate, lawful, and fair in accordance with data protection laws, and if there is a specific legal basis that supports Data4Deals' processing activities, such as:

- If the data subject has given consent
- If the processing is necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract
- If Data4Deals is subject to a legal obligation
- For the protection of vital interests of the data subject
- If necessary for the performance of a public interest
- For the purposes of the legitimate interests of Data4Deals.

Also, the processing of personal data shall be transparent in relation to the data subject, providing them with the information on the processing of their data in an understandable and accessible manner.

PURPOSE LIMITATION

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes in accordance with data protection laws.

DATA PROTECTION PRINCIPLES

DATA MINIMIZATION

During data processing activities, particularly in its collection, the principle of data minimization must be followed. This means that Data4Deals should process, and specifically collect, only the personal data strictly necessary for the execution of the intended purpose.

The principle of minimization should also be applied to the sharing and other processing activities of personal data, including internal or external transfers, ensuring that only the strictly necessary personal data is processed, without compromising the correct performance of the activity.

ACCURACY

Data4Deals and its employees must ensure that the personal data they process is accurate and up-to-date. Otherwise, they must be deleted or corrected.

To achieve this, appropriate and reasonable processes must be implemented to ensure the accuracy, integrity, completeness, and adequacy of personal data for the intended purposes, whenever necessary.

STORAGE LIMITATION

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

It may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

DATA PROTECTION PRINCIPLES

INTEGRITY AND CONFIDENTIALITY

The processing of personal data shall ensure, by means of technical and organizational measures, adequate security to protect it from unauthorized or unlawful processing and to prevent its accidental loss, destruction, and/or damage.

Personal data processed by Dat4Deals must be kept with the utmost confidentiality and secrecy and shall not be used for purposes other than those that motivated and authorized its collection, nor communicated or transferred to third parties outside the cases permitted by the applicable laws.

ACCOUNTABILITY

Data4Deals shall be responsible for complying with the principles set forth in this Policy, in line with applicable data protection laws and shall be able to demonstrate such compliance.

To this end, Data4Deals shall conduct a risk assessment on processing activities that entail a high risk to the rights and freedoms of the data subjects, in order to determine the measures to be applied to ensure that personal data is processed in accordance with legal requirements. Where required by law, the risks that new products, services, or systems may entail for the protection of personal data shall be assessed in advance, and the necessary measures shall be adopted to eliminate or mitigate them.

06

DATA PROTECTION RIGHTS

DATA PROTECTION RIGHTS

Data4Deals ensures that data subjects may exercise their rights foreseen in the data protection laws. The data subjects to exercise their rights shall adress a written request to the Data Protection Officer (Section 9 of this Policy).

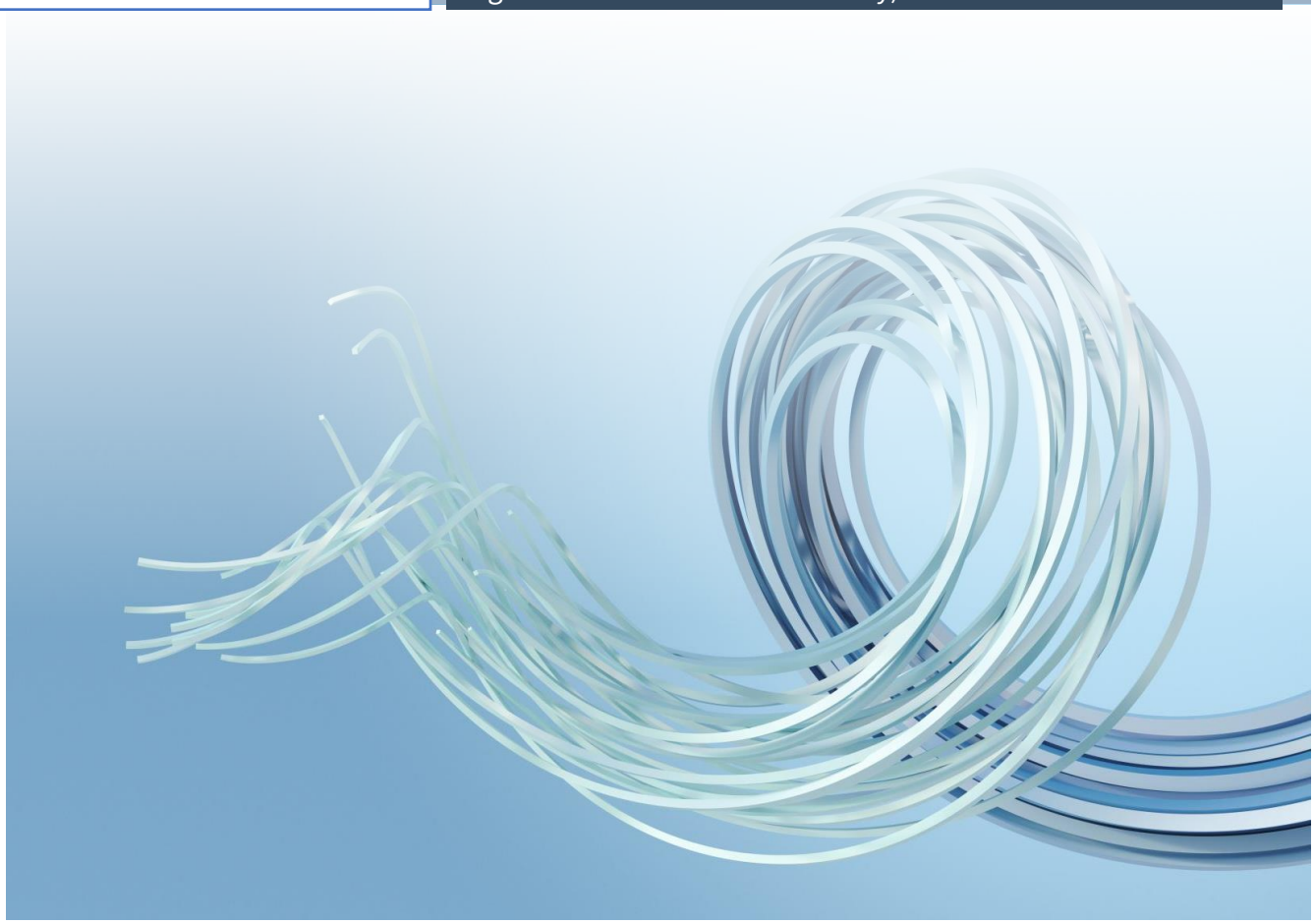
Data4Deals will reply all requests within 30 days. Within this period, Data4Deals must take the necessary actions to fulfill the data subject's rights, such as providing access to their personal data, correcting inaccuracies, deleting data, or complying with other specific requests.

If Data4Deals needs more time to answer adequately due to the complexity of the request or the number of requests received, it can extend the response time by an additional two months. However, the data subject must be informed about the extension and the reasons for the delay within the initial period.

RIGHT OF ACCESS	Data4Deals must provide appropriate means that allow the data subject to access the personal data held about them, the purposes of processing, and related special categories of personal data, the entities with which the data is shared, and the retention periods
RIGHT TO RECTIFICATION	Data4Deals must provide appropriate means that allow the data subject to rectify any incorrect personal data, as well as update personal data that has changed
RIGHT OF ERASURE	Data4Deals must provide appropriate means that allow the data subject to request the erasure of their data, unless there is a legal or contractual requirement that justifies the retention of the personal data
RIGHT TO RESTRICTION OF PROCESSING	Data4Deals must provide appropriate means that allow the personal data subject to restrict the processing of their data in the event of inaccuracy or if the processing is unlawful and the data subject opposes the deletion of their data

DATA PROTECTION RIGHTS

RIGHT TO DATA PORTABILITY	Data4Deals must provide appropriate means that allow the data subject or the new data controller to transmit their data in a structured, commonly used, and easily readable format, as long as it is technically feasible, and the costs are not unreasonable
RIGHT TO OBJECT	Data4Deals must provide appropriate means that allow the data subject to object to the processing of personal data for direct marketing purposes, to the processing of personal data for purposes other than those for which it was collected, and to processing based on the legitimate interests pursued by Data4Deals
AUTOMATED INDIVIDUAL DECISION-MAKING	Data4Deals must provide appropriate means to ensure that the data subject is not subject to decisions made solely on the basis of automated processing, including profiling, except in cases where the legal basis is consent or the conclusion or execution of a contract (unless there are compelling and legitimate reasons to the contrary)



07

PRIVACY PROGRAM

PRIVACY PROGRAM

At Data4Deals, our Privacy Program is designed to ensure compliance with data protection laws and demonstrate accountability in all data protection practices, providing clear evidence of our adherence to these requirements.

The key components of Data4Deals Privacy Program include:

PRIVACY BY DESIGN

RECORD OF PROCESSING ACTIVITIES

DATA PROTECTION IMPACT ASSESSMENTS

PROCESSORS

THIRD PARTIES

INTERNATIONAL DATA TRANSFERS

PRIVACY BY DESIGN

Privacy by design is a fundamental principle that emphasizes the proactive incorporation of privacy measures into the design and scope of development procedures within Data4Deals. All persons subject to the present Policy shall adopt the internal guidelines and apply measures that respect the principals of data protection, safeguarding data subjects' rights.

The goal of these measures is to reduce the risks that may arise from the processing of personal data by implementing the appropriate technical and organizational measures, such as pseudonymization and minimization, both at the time of the selection of the means for processing and at the time of the processing itself.

RECORD OF PROCESSING ACTIVITIES

Data4Deals has implemented a record of processing activities (**RoPA**) that includes a detailed inventory of the types of personal data processed, the purposes of processing, the categories of data subjects involved, any data transfers to third countries, the envisaged retention periods, and the security measures implemented to safeguard the data.

DATA PROTECTION IMPACT ASSESSMENTS

Where the type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, Data4Deals shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data in order to identify potential risks on privacy, and related mitigation actions.

PROCESSORS

Whenever personal data is processed by a processor on behalf of Data4Deals, the latter ensures that it will only engage processors who can provide sufficient guarantees regarding the implementation of appropriate technical and organizational measures to comply with legal requirements and protect the rights of data subjects.

Data4Deals will ensure that all relationships with processors are governed by a data processing agreement.

Additionally, it will be contractually required that the processor obtain explicit, prior written consent from Data4Deals before engaging any sub-processor.

THIRD PARTIES

Communication to third parties refers to the sharing or transfer of personal data by Data4Deals with external entities that are not directly involved in the initial processing of the data.

This transfer may occur for different legitimate purposes, including but not limited to outsourcing services, engaging with business partners, fulfilling legal and regulatory obligations, or providing required information to competent authorities or regulators.

Data4Deals ensures that any sharing of personal data with third parties is conducted in strict compliance with applicable data protection laws, and that such entities are contractually bound to uphold the same high standards of data protection.

Examples of third parties with whom Data4Deals may share personal data include financial institutions (such as banks), insurance providers, government bodies, regulatory authorities.

INTERNATIONAL DATA TRANSFERS

In the case of transferring personal data outside the European Union (i.e., to third countries or international organizations outside the EU), Data4Deals will comply with the provisions of the data protection laws, specifically by:

- ensuring that the third country, a territory, specific sectors of that country, or the international organization in question, has been subject to an adequacy decision by the European Commission, and that this decision remains valid at the time of the intended data transfer; or, if no such decision has been made,
- ensuring that appropriate safeguards are in place and that data subjects have enforceable rights and effective legal remedies.

If the transfer of personal data occurs within the scope of a contractual relationship or another legal framework, Data4Deals must ensure that the receiving entity located in the third country is bound by terms stipulated in standard data protection clauses adopted by the European Commission, or by binding corporate rules approved by the competent supervisory authority, which are in effect at the time of the data transfer.

08

TECHNICAL AND ORGANIZATIONAL MEASURES

TECHNICAL AND ORGANIZATIONAL MEASURES

Data4Deals is required, under applicable data protection laws to implement appropriate technical and organizational measures. Given the nature, scope, context, and purposes of data processing, as well as the risks posed to the rights and freedoms of the data subject, Data4Deals commits to applying the necessary and appropriate technical and organizational measures, both at the time of defining the means of processing and during the processing itself, to ensure the protection of the data subject's information and compliance with legal requirements.

These measures are designed to safeguard against unauthorized access, alteration, or interference, ensuring the confidentiality, integrity, and availability of personal data.

By adhering to this Policy, the Information Security Policy, and other relevant internal guidelines and procedures, Data4Deals demonstrates its commitment to maintaining robust data protection standards.

INTERNAL POLICIES

The internal policies will include the following elements:

- Information on the internal policies concerning data security, and the obligations that result for the employees regarding data protection, especially those related to secrecy, under the terms of the law
- The use of personal data only in accordance with the instructions of Data4Deals or with the legal obligations to which Data4Dealsis bound
- Automatized protocols on personal data access by electronic means and regular monitoring of those protocols by the Department responsible
- Comprehensive documentation of other forms of dissemination, different from the automatized access to data, in order to prove that there was no illegal or unauthorized transmission of data
- Provision of training and appropriate education on data security
- Execution of regular audits, in order to ensure that all measures deemed as appropriate were effectively implemented and are operational.

REINFORCED DUTY OF SECRECY

Personnel who have access to or possess information containing sensitive data are bound by an absolute duty of confidentiality and must refrain from using it for any purpose other than those authorized by Data4Deals. Any violation of these rules will result in appropriate disciplinary and legal actions.

Without prejudice to the necessary technical and organizational measures to protect personal data in accordance with the law, data subjects who possess information containing sensitive data, and in compliance with the Information Security Policy and contractual confidentiality obligations, must:

- Limit the access to such information, within each Department, to only those individuals who require it for the proper performance of their tasks within Data4Deals
- Refrain from making any comments that could directly or indirectly disclose the existence or content of the information
- Use the information exclusively for legitimate purposes related to Data4Deals's clients
- Adhere to the measures that control access to the information and to the documents or other media in which the information is stored
- Ensure that a non-disclosure agreement (or similar document/contractual obligation) is signed in advance whenever it is necessary to make sensitive data available to third parties outside Data4Deals.

LOGICAL MEASURES

Data4Deals has implemented security policies which include specific software for these purposes, particularly:

- Antivirus software, firewall and data prevention loss
- Restrictions to share non-authenticated archives
- Restrictions on peer-to-peer applications
- Database encryption software
- User account password
- Appropriate maintenance services and with approved levels of correction
- In addition, procedural and technical controls are used in order to detect any compliance deviations
- Data transfer is performed, exclusively, through a secure network connection
- In what concerns privileged access, only users who are expressly authorized may request access
- According to the instructions received and to determine which user credentials holders are still authorized by Data4Deals, a periodical verification is carried out as well as an annual revalidation to determine that the accesses are compatible with the existing users
- Regarding incident management, a registration and monitoring process is implemented through the Information Security Policy and Incident Response Plan, which can be updated over time.

DATA BREACH

Data breach incidents highlight the critical importance of adhering to data protection obligations, especially the need for swift and effective responses to such incidents.

Data4Deals is committed to maintaining the highest standards of data security and, in the event of a personal data breach, will notify the Portuguese Data Protection Supervisory Authority (*Comissão Nacional de Proteção de Dados – CNPD*) within 72 (seventy-two) hours, as required by law.

In cases where the breach is likely to result in a high risk to the rights and freedoms of individuals, Data4Deals will also notify the affected data subjects without undue delay.

To ensure transparency and accountability, the following information will be provided in the notification:

- A detailed description of the nature of the data breach, including the specific categories of personal data affected and an estimate of the number of individuals involved
- Contact information for the data protection officer or another designated representative who can provide further details and support to both authorities and affected individuals
- A comprehensive assessment of the potential consequences of the breach, including any potential harm to the individuals affected, such as identity theft, reputational damage, or financial loss
- A summary of the immediate and proposed measures taken by the company to address and contain the breach, as well as any steps aimed at mitigating its potential adverse effects, ensuring that the risk to individuals is minimized.

Data4Deals shall document any data breaches, including the facts relating to the data breach, its effects and the remedial action taken.

09

DATA PROTECTION OFFICER

DATA PROTECTION OFFICER

Data4Deals is committed to maintaining the highest standards of data protection and has appointed a Data Protection Officer ("**DPO**") to oversee the company's Privacy Program and data protection strategy to ensure compliance with data protection laws and regulations.

The DPO acts as a point of contact for data subjects and supervisory authorities on all issues related to the processing of personal data and the exercise of data subjects' rights. The DPO's responsibilities include but are not limited to:

- Ensuring that Data4Deals complies with data protection laws, and internal data protection procedures
- Providing guidance on the necessity and execution of DPIAs, particularly for processing activities that pose a high risk to the rights and freedoms of data subjects
- Conducting training sessions and raising awareness among employees about data protection principles and practices
- Handling requests from data subjects regarding their privacy rights
- Managing and responding to data breaches and other incidents involving personal data, including notifying supervisory authorities and affected data subjects when required.

Data subjects and supervisory authorities can contact the DPO for any inquiries or concerns related to data protection at Data4Deals through the following email address: privacy@datafordeals.com.

10

FINAL PROVISIONS

FINAL PROVISIONS

This Policy shall be interpreted jointly with other applicable policies and procedures implemented by Data4Deals and the legislation in force.

The present Policy will be reviewed from time to time, to detect, and if applicable, to correct any defective situation that may occur in its implementation.

The Policy review may occur, whenever, by virtue of specific circumstances, inter alia, needs arising from Data4Deals's activity, facts, or any legal legislative amendments, may require.

Any queries regarding the content of the present Data Protection Policy or regarding the processing of personal data by Data4Deals, shall be forwarded, in writing, to the DPO, at the following email address privacy@datafordeals.com.