Code of Conduct for the Protection of Personal Data

The present Code of Conduct of Cloud365, Lda. (hereinafter identified as "Cloud365") for the Protection of Personal Data, was prepared within the scope of article 40 of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, General Data Protection Regulation (GDPR) and binds all Cloud365 Workers regarding the collection, processing and use of personal data concerning Cloud365, the Workers themselves, Customers and third parties with whom Cloud365 has a relationship.

This Code also applies to Cloud365's relationships with all its Collaborators, Partners and Subcontractors.

Article 1

Definitions

For the purposes of this Code, the following definitions established in Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, are considered:

1) "Personal data" - information relating to an identified or identifiable natural person («data subject»); an identifiable person is considered to be identifiable, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, electronic identifiers or one or more specific elements of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2) "Processing" - an operation or a set of operations carried out on personal data or on sets of personal data, by automated or non-automated means, such as collection, registration, organization, structuring, conservation, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, broadcast or any other form of making available, comparison or interconnection, limitation, erasure or destruction;

3) "Limitation of treatment" - the insertion of a mark in the personal data kept with the aim of limiting its treatment in the future;

4) "Profiling" - any form of automated processing of personal data that consists of using such personal data to assess certain personal aspects of a natural person, in particular to analyze or predict aspects related to their professional performance, their economic situation, health, personal preferences, interests, reliability, behavior, location or travel;

5) “Pseudonymisation” - the processing of personal data in such a way that they can no longer be attributed to a specific data subject without resorting to supplementary information, provided that such supplementary information is kept separately and subject to technical and organizational measures to ensure that the personal data cannot be attributed to an identified or identifiable natural person;

6) “File” - any structured set of personal data, accessible according to specific criteria, whether centralized, decentralized or distributed functionally or geographically;

7) “Controller” - the natural or legal person, public authority, agency or other body that, individually or jointly with others, determines the purposes and means of processing personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria applicable to its appointment may be laid down by Union or Member State law;

8) “Subcontractor” - a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller;

9) “Recipient” - a natural or legal person, public authority, agency, or other body that receives communications of personal data, regardless of whether or not it is a third party. However, public authorities that may receive personal data in connection with specific inquiries under Union or Member State law are not considered to be recipients; the processing of such data by these public authorities must comply with the applicable data protection rules depending on the purposes of the processing ;

10) “Third party” - the natural or legal person, the public authority, the service or body that is not the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the subcontractor, are authorized to process personal data;

11) "Consent" of the data subject - a free, specific, informed and explicit expression of will, by which the data subject accepts, by means of an unequivocal positive statement or act, that the personal data concerning him are subject to processing ;

12) "Personal data breach" - a breach of security that causes, accidentally or unlawfully, the destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or subject to any other type of treatment;

13) "Sensitive data" – personal data revealing racial or ethnic origin, political opinions and religious or philosophical beliefs, trade union membership, genetic data and biometric data processed simply to identify a human being, data related to the health and data relating to the person's sex life or sexual orientation;

14) "Genetic data" - personal data relating to the genetic, hereditary or acquired characteristics of a natural person that provide unique information about the physiology or health of that natural person and which result in particular from an analysis of a biological sample from the person individual concerned;

15) "Biometric data" - personal data resulting from a specific technical treatment relating to the physical, physiological or behavioral characteristics of a natural person that allow or confirm the unique identification of that natural person, namely facial images or dactyloscopic data;

16) "Health data" - personal data relating to the physical or mental health of a natural person, including the provision of health services, which reveal information about their health status.

Article 2

Data collection and processing

1. The collection of data for processing must be carried out in accordance with the legislation in force, in strict compliance with the rights, freedoms and guarantees provided for in the Constitution of the Portuguese Republic and be carried out in a lawful, legal and transparent manner.

2. The collection of personal data by Cloud365 must be preceded by the consent of and inform the respective holders about the purpose that determined it and be processed in strict compliance with that consent and that purpose.
3. Cloud365 and its Workers, as well as Subcontractors must absolutely ensure that:

   a) the data subject has previously given his consent and that the processing is carried out only within the scope of the purposes for which they were collected, and cannot be subsequently processed in a way that is incompatible with those purposes;

   b) the collection, use and conservation is carried out only on the minimum personal data, necessary and sufficient, for the respective purpose;

   c) the conservation of personal data is carried out only for the period of time necessary to fulfill either the purpose of the treatment that gave rise to it, or the legally stipulated deadlines for the purpose;

   d) there is no transmission of personal data for commercial or advertising purposes, except for the existence of express consent on the part of their holders in this regard;

   e) the processing of personal data is carried out for legally foreseen purposes or for the pursuit of legitimately contracted services;

   f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by third parties, unless the interests or fundamental rights and freedoms of the holder that require the protection of personal data prevail, in particular if the holder is a child;

   g) personal data are always subject to lawful, fair and transparent processing in relation to the data subject;

   h) personal data are treated in a way that guarantees their security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, adopting appropriate technical or organizational measures.

Article 3

Conditions applicable to consent

1. The controller must be able to demonstrate that the data subject has given his consent to the processing of his personal data.

2. The consent request must be presented in a way that clearly distinguishes it from other matters in an intelligible and easily accessible way and in clear and simple language;
3. The data subject has the right to withdraw his consent at any time. The withdrawal of consent does not compromise the lawfulness of the treatment carried out based on the previously given consent.

Article 4

Physical Files

1. The decision to create physical files should only be taken after all viable alternatives for creating the same files in computer support have been exhausted.
2. In the event that it is necessary to create physical archives, all Cloud365 Workers must respect and promote the safeguarding and security practices of the archive defined by it, as well as ensure that the necessary accesses and levels of control over them follow the same criteria. with the purpose of this Code and with the instructions of Cloud365, namely:

   a) Pay attention to the safe location, controlled and preferably subject to access to physical documents containing personal data (paper, computer media, etc.);

   b) Refrain from saving personal data on the computer at your workplace, unless otherwise instructed in writing by Cloud365 and, in this case, ensuring the measures to restrict access to such data established by it;
   c) Transport or physically transfer paper or computer documents containing personal data, only when this is strictly necessary to carry out the task in question and only for as long as it lasts;
   d) Comply with internal guidelines regarding the creation, maintenance and destruction of working versions and copies of documents containing personal data.

Article 5

Right to information and access

Cloud365 undertakes to inform the holders of the data it collects, as well as the respective purpose and to identify the person responsible for the treatment.

Whenever requested by data subjects, and as long as legally permitted, Cloud365 corrects and updates the personal data contained in its files and databases within a maximum period of 7 (seven) days.

Article 6

Deletion of personal data

When a data subject requests the deletion of the same, and provided that legally permitted, Cloud365 will comply with that request within a maximum period of 7 (seven) days from the legally stipulated term for the purpose, always considering the longer period imposed by law for their conservation.

Article 7

Sensitive data

The sensitive data that Cloud365 has, by law or by contract, to collect, will be kept confidential and only the Workers strictly necessary will be able to know of their existence and have access to them.

Article 8

Safety equipment

1. Cloud365 safeguards security in the processing of personal data, preventing the consultation, modification, destruction, or introduction of data by unauthorized persons.
2. Cloud365, in the pursuit of its activities, uses a set of security procedures and technologies aimed at protecting personal data, protecting unauthorized access or disclosure, namely through:

a) Physical security measures, such as control of physical access to its facilities, fire safety measures, accommodation of equipment in dedicated data centers, with restricted access procedures, and use of online applications (Software-as-a- Service) whose providers certify compliance with GDPR;

b) Logical security measures:

i) in the component of access to systems and workstations through identity management mechanisms, authentication, privileges, access control and registration;

ii) in the network component, the use of firewalls and network segregation (internal, external, demilitarized zone), as well as the use of secure communication channels, namely through the encryption of information.

iii) protection of mobile devices (portable computers, 'smartphones') with software to protect against malicious activity (anti-malware), including antivirus, anti-phishing and firewall.

Article 9

Use of computer resources and information technologies

1. Cloud365 Workers must only use the material and computer resources made available to them by Cloud365, exclusively for professional purposes and diligently, being prohibited to exchange peripherals, carry out backups on media not authorized by Cloud365 or open of computer equipment without prior written authorization from Cloud365.
2. Cloud365 has a central directory system for managing its Workers' accounts and workstations, each of which is assigned a user account and password to access the workstation and other IT resources on the internal network, according to the respective access profile.
3. It is the responsibility of each user to keep their passwords secure, which are strictly personal and non-transferable.
4. Whenever possible, a third authentication factor will be implemented for access to Systems that host personal data.
5. The allocation or alteration of access to the network and computer applications of Cloud365 must always follow the respective internal procedures in force.

6. The detection of anomalies in the operation of equipment and applications or suspected malware must be immediately reported to Cloud365.

Article 10

Relationships between Cloud365 and data transmission subcontractors

1. Cloud365 will only transmit personal data to third parties when required by law or contract or if the holder authorizes or requests it.
2. Whenever Cloud365 transmits or assigns personal data to a subcontractor, it must ensure that they are used in accordance with the previously established purpose and that the conditions of transmission or transfer are reduced to writing, namely regarding their use and purpose.

Article 10

Institutional relations with the national supervisory authority

Cloud365 has a duty to collaborate with the national control authority by providing them with information, whenever requested, and other documentation related to the collection, automated processing, and transmission.

Article 11

Professional secret

1. All Cloud365 Employees, regardless of the type of existing link, as well as service providers and suppliers, who process personal data, are bound by professional secrecy over them, namely not being able to reveal or use such data, except in cases where required by law, namely when public entities duly accredited for the purpose require the transmission of data.
2. The duty of confidentiality and secrecy incumbent on all Cloud365 Collaborators, as well as on service providers and suppliers, does not cease with the end of functions or services provided.

Article 12

Responsibility

1. All Cloud365 Workers are individually responsible for the violation or illegal transmission of personal data that Cloud365 has in its database or to which it has access by contractual means and may incur disciplinary action for the violation or transmission of personal data to which they have authorized or non-authorized access.
2. This responsibility will be assessed according to the seriousness of the situation in question.
3. The remaining Employees, suppliers or service providers are responsible under contractual and legally established terms.

Article 13

Receipt and handling of complaints

1. Pursuant to Article 33(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, in the event of a breach of personal data, the controller shall notify the competent supervisory authority.

Article 14

Breach of personal data

1. If the controller becomes aware of a breach of personal data, likely to pose a risk to the rights and freedoms of natural persons, it must notify the national supervisory authority without undue delay and, whenever possible, within 72 hours after becoming aware of it.
2. If it is not possible to meet the deadline referred to in the previous number, the notification must be accompanied by the reasons for the delay, and the information may be provided in stages and without duly undue delay.

3. When a situation of violation is verified, Cloud365 must open an internal investigation process to determine the causes of that same violation.
4. It is the duty of all Workers who are aware of any situation that may imply a breach of personal data to urgently report it to Cloud365, via the email address admin@cloud365.global or through any other more expeditious means.
5. Interested parties wishing to complain about the violation of their data should do so directly to Cloud365 at the email address: dataprivacy@cloud365.global or through the Cloud365 website, if this facility is available.

Article 15

Clarifications and application of the code

Requests for clarification of doubts regarding the interpretation or application of this Code of Conduct should be sent to Cloud365 to: dataprivacy@cloud365.global .

Article 16

Filling in the gaps

For all omissions, as provided for in this Code of Conduct, the provisions of the General Data Protection Regulation, Law No. 58/2019, of August 8, as well as other national legislation in force on this matter.

Article 17

Implementation

This Code of Conduct will come into force on November 1, 2022.