



Declaration of Commitment
**Privacy and Personal Data
Protection of the NOS Group**

Our commitment

The protection of the privacy and personal data of everyone, who in any way is connected to NOS (customers, users of services, staff, partners and others) is a fundamental commitment of our Group.

Personal data are essential for the development of the activities of companies that make up the NOS Group, notably for offering and marketing their products and services, for providing, monitoring and improving the quality of services, for managing their human resources and for compliance with legal obligations, and the related challenges are strongly influenced by technological, economic and social developments.

So our commitment is for us to work on a daily basis to ensure the best levels of privacy and data protection, observing all Portuguese and European, laws, regulations and guidelines that apply in this area.

Today's commitment is reflected in privacy policies and standards, among which are the Customer Privacy Policy, the Employee Privacy Policy, as well as the General Information Security Policy.

In order to better achieve our commitment, we have appointed a Personal Data Protection officer (DPO), who is responsible for advising NOS, monitoring the compliance of data treatment with applicable policies and standards and is a point of contact for the customer and for the control authority.

In addition, NOS has set up a Governance, Risk and Security Compliance Committee, responsible, among other tasks, for the maintenance, development and supervision of information security, the related policies and standards, as well as for raising awareness for security through training and communication.

Through this Declaration of Commitment, we wish to make clear our commitment to privacy, security and data protection, ensuring that all those who deal with personal data in their interactions with NOS subscribe to and act in accordance with the principles that underlie it.

Miguel Almeida
CEO NOS



Principles concerning the collection and processing of personal data and rights of owners of personal data

The processing of personal data undertaken by the companies of the NOS Group follow the following fundamental principles:



As well as compliance with the principles above, the NOS Group is committed to ensuring that the rights of owners of personal data are respected, namely the right to access and to information, the right to rectification, the right to restriction on use, the right to transferability, the right to be forgotten, the right to withdraw agreement, the right to object, the right to not be subject to individual decisions taken in an entirely automatic manner, including the definition of profiles, and the right to make an appeal.

Principle **of legality**

Personal data are used if and to the extent that at least one of the following conditions exist to ensure the legality of this use, namely (i) when agreement has been given by the owner of the data or when use is necessary for (ii) the execution and management of a contract, (iii) compliance with a legal obligation, or (iv) the pursuance of a legitimate interest of the company or of third parties.

Principle **of purpose/good faith**

Personal data are used exclusively for the specific purposes for which they were collected and only used for distinct purposes when legally allowed and via provision of information to the respective owner.

Principle **of transparency**

The owners of data will be informed in a clear and concise manner about relevant aspects relating to the processing of their personal data, namely about the specific purposes for their use and possible transmission to third parties.

Principle **of proportionality and restriction on retention**

Only personal data that are shown to be appropriate, pertinent and not excessive will be used and only for the period of time that is strictly necessary.

Principle **of need-to-know**

Only employees and partners, whose respective duties demand it, will have access to personal data used by companies of the NOS Group..

Principle **of confidentiality, integrity and availability**

personal data will be used in a manner that ensures its security, namely (i) to protect against unauthorized or illegal access, (ii) to protect against unauthorized or accidental modification, loss or destruction and (iii) to ensure that data are available when necessary and permitted and without unnecessary delay.

Principle **of data protection from design and by default**

The products and services of NOS, its support systems and its internal procedures are developed with the protection and privacy of personal data in mind.

Security of personal data

The NOS Group follows best practices for the security and protection of information and personal data, and has adopted a demanding program of policies and standards to ensure the confidentiality, integrity and availability of the information that it processes and is under its responsibility, a fact that is known by all the staff and partners of NOS.

The General Information Security Policy of NOS sets out a wide range of technical and organizational measures, organized in various areas of security, among which are:

Logical measures of security, such as the use of firewalls and intrusion detection systems, the existence of a policy of accesses to information and the register of operations (logging);

Physical measures of security, among which can be highlighted a strict control on the physical installations of NOS, on the part of staff, partners and visitors, as well as very restricted access and continuous monitoring of the essential technological infrastructure of NOS;

Other measures such as masking, encryption, aliasing and rendering personal data anonymous, and also a range of measures that aim to put into effect the principle of privacy from design and by default.

Whenever companies of the NOS Group use sub-contractors or third parties, they will be respectively responsible, in accordance with applicable legislation, for the personal data that they have to transmit and will ensure that: (i) the sharing of information and personal data complies with legal standards in force, (ii) transmission is done securely and that (iii) subcontractors or third parties are contractually obliged to observe the duties of confidentiality and secrecy and ensure the security of personal data, which are for this purpose communicated to them, and cannot use such data for any other purpose whatever, for their own benefit or for third parties, nor correlate them with other data which they have at their disposal.

Compliance with the policies and standards relating to information security and personal data protection is subject to scrutiny, audit and controls, and is also complemented by a demanding program of information and training of the staff and partners of NOS.