Personal Data Protection Policy

1. Background

In the information society in which we live, personal data plays a crucial role. Personal data protection is therefore a legal response to the phenomenon of the information society, aimed at curbing the potential threat that technological development represents for people's rights and liberties.

2. Purpose and scope

The Cellnex Group, owing to its concern that the processing of personal data should be carried out in accordance with applicable legislation in all its entities, has drawn up this document containing the general principles and guidelines that it promotes across its organisation.

Applicable legislation:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data, which repealed Directive 95/46/EC (the "GDPR").
- Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guaranteeing of Digital Rights.
- Domestic data protection legislation in the countries in which Cellnex operates.

The GDPR is mandatory for all EU companies that process the personal data of European citizens. It is also applicable to companies established outside the European Union that process EU citizens' data in relation to products or services offered to them, or to the analysis of their behaviour within the EU.

Scope of application

This policy is applicable to all the companies that make up the Cellnex Group, which has a presence in Spain, Finland, France, Ireland, Italy, the Netherlands, Switzerland and the United Kingdom, notwithstanding possible adjustments at an international level in line with the legislation and standards of the country concerned.

In addition, the policy will be applicable to all professionals in all areas and departments of the Cellnex Group.

Definitions

- **Personal data:** any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Data controller**: the natural or legal person, public authority, service or other body which, alone or with others, determines the purpose and means of the processing.

- **Data processor**: the natural or legal person, public authority, service or other body which processes personal data for the account of the data controller.

- **Data Protection Officer**: natural person that: (i) informs and advises the data controller and data processor and the employees responsible for the processing of their obligations with respect to data protection, (ii) supervises compliance with the General Data Processing Regulation, other applicable data protection regulations and the data controller's policies, (iii) offers advice on the impact assessment with regard to data protection and supervises its application, (iv) cooperates with and acts as a point of contact between the company and the supervisory authority.

- **Sensitive data or special data categories:** personal data revealing ethnic or racial origin, political opinions, religious or philosophical convictions or trade union membership, and the processing of genetic data, biometric data aimed at identifying a person without any chance of error, data concerning health or data concerning a natural person's sex life or sexual orientation.
- **Transfers of personal data to third countries or international organisations:** data processing that involves a transfer of the data outside the European Economic Area, whether as an assignment or communication of data, or in order to process data on behalf of the data controller.

- **Security breaches, or violations of personal data security**: any breach of security leading to the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or processed.

3. Basic principles

The Cellnex Group and all its personnel must comply with the following 10 Principles in personal data processing:

- **Principle of fairness and transparency**: The personal data processing must be fair and the individuals concerned must be informed of the circumstances relating to the processing of their data in an accessible and understandable manner, using clear, simple language.
- **Principle of lawfulness**: The personal data processing can only be carried out if there is a legal basis that allows it, such as the consent of the individual concerned or another basis of legitimation such as the performance of a contract with the individual concerned, compliance with the legal obligations of the Cellnex Group, satisfaction of the legitimate interests of the Cellnex Group, etc.
- **Principle of purpose limitation**: Personal data may only be processed for specific, explicit and legitimate purposes and will not be processed subsequently in a manner incompatible with said purposes.
- **Principle of data minimisation**: Only personal data which are appropriate, pertinent and restricted to what is necessary in relation to the purposes for which they are obtained should be collected and processed.

- **Principle of accuracy**: The data held must be accurate and up to date.
- **Principle of exercising data protection rights:** The data protection rights of the individuals concerned (access, rectification, erasure, objection, restricting processing and portability) must be respected.
- **Principle of storage limitation**: The personal data must be kept in a format that allows the data subjects to be identified for a time not exceeding that necessary to achieve the purposes for which the personal data was collected, avoiding any abuse that could breach the other data processing principles.
- **Principle of data security**: Appropriate security measures must be established to protect the personal data that is being processed, including the protection thereof against unauthorized or illegal access and against loss, destruction or accidental damage.
- **Principle of proactive responsibility:** The Cellnex Group must guarantee the fulfilment of these principles by its personnel and comply with other requirements laid down in current data protection legislation. A record of processing activities will be managed for this purpose.
- **Principle of privacy by design and by default:** The Cellnex Group will guarantee a level of data protection security from the time when the processing media and purpose are determined and during the actual processing of the data.

4. Strategic lines of action and commitments

Roles and responsibilities

This section includes the envisaged assignment of roles and responsibilities in the organisation which, when necessary, will be complemented by a more detailed assignment in each local Cellnex Group organisation.

The Cellnex Group has appointed a Data Protection Officer and has designed a relational governance model with local data controllers to coordinate this function in the countries in which it operates.

-The Data Protection Officer will be responsible for:

- The governance, supervision and maintenance of this policy and the personal data protection rules.
- The monitoring and measurement of the degree of compliance with this policy and the personal data protection rules.
- Providing advice, recommendations and clarifications to users on the content of this policy and the personal data protection rules.
- Awareness-raising and training associated with this policy and the personal data protection rules.

-Employees will be required to:

- Know their obligations and responsibilities with respect to any personal data processing they need to perform in the course of their work.
- Process personal data in accordance with the principles laid down in the GDPR.
- Ensure that third parties that require access to personal data comply with the technical and organisational measures established in the contract.
- Report any personal data security incident they are aware of.

-The different Corporate Areas must:

- Ensure that employees fulfil their roles and responsibilities in relation to personal data protection.
- Ensure compliance with the provisions of this policy.
- Implement the local procedures required to guarantee the rights and obligations set out in the GDPR, such as the management of the data subjects' rights, management and notification of security incidents or the implementation of information clauses for obtaining consent.
- It is stated hereby that the supervisory authority covering the Cellnex Group's head office is the Spanish Data Protection Agency (AEPD), as the registered office of the Cellnex Group's parent company is located in Spain.

International transfers

In order to fulfil the above objectives we need to allow Cellnex Group entities and third parties or service providers that support us in the services we offer to access your personal data.

For reasons of service efficiency, some of the aforementioned providers are located in territories outside the European Economic Area that do not provide a level of data protection which is comparable to that of the European Union. Despite this, we wish to inform you that we will transfer your data with all appropriate guarantees and will ensure the security of said data by signing with service providers the Standard Contractual Clauses approved by the European Commission, the content of which can be consulted here: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

ARCO+ rights

The applicable data protection regulations recognise a number of rights that may be exercised by data subjects. These rights are as follows:

Right of access: right to know if your personal data is being processed or not and, if so, to be provided with certain information (including the purpose of the processing, the data categories, the data storage period or the category of the recipients).

Right to rectification: requesting the modification of inaccurate or incomplete data.

Right to erasure: requesting the elimination of your personal data.

Right to data portability: right to receive in electronic format the personal data that has been provided, and transfer them to another entity.

Right to processing restriction: requesting that the processing operations that are relevant in each case are not applied to your personal data.

Right to object: requesting that certain personal data processing is not carried out.

Right not to be subject to automated individualised decisions: requesting that personal data processing is not carried out which involves Cellnex taking decisions that affect you in a significant manner and which are carried out automatically without any human involvement.

To exercise any of your rights, please contact Cellnex at the following email address: **personaldata@cellnextelecom.com**, or by postal mail at the following address: DPO – Avda. Parc Logístic, 12-20 08040 Barcelona. You must identify yourself by attaching a photocopy of your ID card or equivalent document together with an indication of the right that you intend to exercise and which processing is involved.

Security measures

The Cellnex Group guarantees the security, secrecy and confidentiality of personal data under its responsibility, adopting the most stringent and robust security measures and technical resources to prevent the loss or misuse of the data or access to the data without your authorisation.

The personal data collected by the Cellnex Group through the various channels will be treated with absolute confidentiality, and it undertakes to keep said data secret and guarantees compliance with the obligation to store the data taking all necessary and reasonable measures to prevent their alteration, loss or unauthorised processing or access, in accordance with applicable legislation.