Orange’s policy on the protection of personal data

Foreword

Orange is deeply committed to protecting personal data and privacy. The Group is determined to be recognized as a responsible player with its customers, users, employees and partners.

With the quick development of digital technology, users are sharing more and more data, which can expose them to increased risks of identity theft, fraud, loss of confidentiality. That is why authorities and digital players are working together to strengthen online security and protect users' data.
In line with its raison d'être, Orange is working towards a safer and more transparent digital world. This is reflected in a number of commitments, including protecting users' data and ensuring that their privacy is respected.

The Group mobilizes all its stakeholders, including its employees, suppliers, and partners, to promote the protection of users' personal data and is committed to three key areas: security of their personal data; transparency on the use of this data; respect of their rights over this data, in accordance with local and international regulations, and in particular their control when interacting with Orange.

This policy reflects Orange's commitments in compliance with internationally recognized principles relating to the protection of personal data and human rights. It complements the Group's internal policy.
It applies to all Group entities and employees, regardless of their location.

I count on our employees, suppliers and partners to rigorously and carefully apply and implement the Group's personal data protection policy in order to embody Orange's raison d'être as a trusted player.

Christel Heydemann
Chief Executive Officer

Introduction

Digital users are sharing more and more information, especially personal data. This data sharing is increasingly promoted and regulated, particularly in the European Union, which has adopted a real data strategy to promote the free circulation of data within the EU. Access to and the ability to use data is now seen as critical to innovation and economic growth.

In a world of constant technological, regulatory and economic changes, where the development of services involves multiple chains of players, it is essential that users have confidence in the use of their personal data.

This policy (hereinafter "Policy") meets the needs of our users, employees, customers and the requirements of regulators, authorities, or other stakeholders. It reflects the commitments of Orange to respect internationally recognized principles relating to the protection of personal data and the fundamental rights from which they stem.

As such, the principles enshrined in Article 12 of the Universal Declaration of Human Rights, in the European Charter of Human Rights, those of Council of Europe Convention 108 and 108+, those of the ECOWAS Additional Act drive the process of protecting personal data. Orange focuses on their application in its activities all over the world as well as compliance with the various local regulations applicable in the countries where Orange operates, such as the General Data Protection Regulation (known as GDPR) in Europe.

Regulatory frameworks may be in place, under development and sometimes only cover part of geographical areas. Orange is therefore committed to adopting a global approach, in compliance with local regulations, incorporating measures to anticipate and monitor these developments, following the example of its approach to the ethical and responsible use of artificial intelligence (AI).

For more information:

Article 12 of the Universal Declaration of Human Rights
https://www.un.org/en/about-us/universal-declaration-of-human-rights

European Charter of Human Rights
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016P/TXT

Council of Europe Convention
https://www.coe.int/en/web/data-protection/convention108-and-protocol

ECOWAS Additional Act
https://ictpolicyafrica.org/es/document/z69cbq7b51

As a key player in digital services, which can only develop in a secure and trusted environment, Orange makes the protection of personal data a collective value.

Orange promotes this commitment to its employees. Thus, when dealing with issues that have an impact on the protection of personal data, group entities cooperate with each other.

Data protection is also promoted to partners and suppliers who are also subject to specific obligations under applicable laws. This policy highlights the importance of such an approach, including in Orange's business relationships with these third parties. In so far as it meets all legal obligations in terms of data protection, this policy applies to all actors in the chain of processing of personal data.

This Policy applies to all Orange entities and its personnel, regardless of their location and jurisdiction. It covers all the processing of personal data carried out by Orange, whether by its entities directly or by entrusted third parties (suppliers, partners, subcontractors) and regardless of the categories of data subjects such as employees, customers, and users of services. It covers both the data processing carried out under the responsibility of Orange and those carried out by Orange as a data processor on behalf of third parties.

This Orange Policy is made available to all of stakeholders on orange.com institutional website. In addition, it is specifically adapted for stakeholders likely to be affected, as close as possible to the business lines and according to methods adapted to the local situation: for example, there is a version for business customers, published on orangebusiness.com website, versions for customers and users of its services on the commercial sites of countries and an internal version for employees. It is also reflected throughout the user experience. Targeted communication actions are carried out when the Policy is updated.

Table of contents

01 Compliance with Key Data Protection Principles

Orange implements the principles of personal data protection :

Lawfulness and legitimacy

Orange ensures the lawfulness of the processing carried out by ensuring that they are based on the legitimate legal bases provided for by the applicable data protection laws and/or any other applicable law or regulation. Personal data is processed for specific, limited, well-defined and legitimate purposes.

Transparency and loyalty

Orange is committed to ensuring the transparency of its processing activities. To this end, Orange informs data subjects in advance of the processing of their data in a concise, easily accessible, and understandable manner, using clear and simple terms. The information is accessible on the Group's websites and applications.

Data minimization

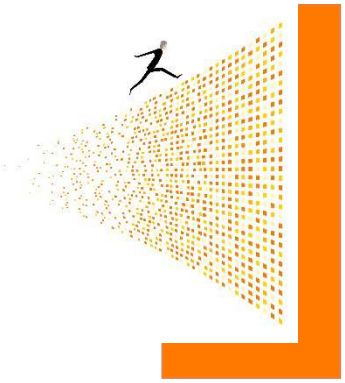
Orange undertakes to only process personal data that is adequate, relevant and limited to what is necessary in relation to the specific purpose pursued by the processing. Where appropriate, Orange encourages the use of pseudonymization methods or techniques.

Data accuracy

Orange takes all necessary measures to ensure, with a reasonable degree of certainty, that personal data is accurate and up to date.

Limitation of the data retention period

Orange retains personal data for defined periods of time, depending on the purposes for which such personal data is to be processed, which are made known to data subjects in accordance with applicable laws.



Security

Orange implements the necessary technical and organizational measures to preserve confidentiality and protect personal data against any accidental, unauthorized or unlawful access, use, modification, disclosure, loss, destruction or damage, in accordance with the Group Security Policy.

Orange has set up a governance system to ensure the protection of information systems and data entrusted to it by its customers and employees. Orange works to ensure that its services are used with confidence, and that the personal data entrusted to it is protected. This important aspect of Orange's strategy is the subject of a continuous safety improvement policy, based on risk assessment and risk management.

Incident management and notification of personal data breaches are carried out in accordance with the applicable laws and Group security policies.

For more information :

Group Security Policy

https://gallery.orange.com/rse/GroupSecurityPolicy2023

Respect for the rights of individuals

Individuals have rights that can be exercised at any time. These are the rights of access, rectification, erasure, limitation, opposition, portability and not to be the subject of an automated individual decision.

To this end, Orange sets up an organization and mechanisms to respond to it.

Orange's customers have, for each of the Group's entities, the necessary information to contact the data protection officer. Generally available in privacy notices, this allows anyone who wishes to send their request to exercise rights through an online form or by mail according to the means made available by the entity concerned.

Data Protection by Design

Orange is committed to proactively integrating the protection of personal data within its products and services. To do this, the requirements of personal data protection are integrated into the design of Orange's products and services.

On a daily basis, Orange seeks the continuous improvement of its products and services, requiring risk management throughout the entire design chain.

02 Governance

Orange's personal data protection Policy is implemented in each entity under the responsibility of its General Manager, who ensures that risks are mapped and addressed.

At entity level, processes related to the design and deployment of products, services, or tools, those related to risk management or even those concerning the responsible use of AI integrate the protection of personal data.

Each entity sets up an internal organization in which the actors who are part of the support network for the protection of personal data contribute on an ad hoc or permanent basis to its integration into the Group's projects.

At Group level, a Data Protection Officer (hereinafter "Group DPO") has been appointed by the Executive Committee to coordinate actions within the governance set up. She participates in internal data governance committees within the Group to provide insight and expertise. She animates a network of data protection officers (DPOs) and other key players in the various entities in Europe and outside the European Union. The network includes a representative from each of the data strategic divisions, and/or data protection officers or legal advisors.

03 Evaluation and documentation under the accountability principle

Orange implements documentation and actions to demonstrate compliance and enable continuous improvement in data protection.

Personal data process mapping

Orange implements various mapping tools (applications, processing, data typologies) to adopt risk management measures for personal data, depending on the circumstances.

Audits

In addition to security policy audits, through its missions, the internal audit team helps the Group maintain an appropriate control system by assessing its effectiveness and efficiency and by issuing observations and recommendations for continuous improvement. Compliance with personal data protection laws and corporate policies within Group subsidiaries is a specific subject examined during internal audit assessments using a risk-based approach.

Certifications

At the crossroads of security requirements, and contributing to data protection, certifications are strongly present within Orange. With several dozen 27001 certifications, Orange is one of the first in Europe to meet the requirements of ISO 9001, 22301, 27001, 27018 and 14001 standards, which means that Orange exercises a uniform control over the documentation, a process map and a uniform method for monitoring the compliance of its management system with the requirements of the standards.

04 Evaluation and involvement of providers, suppliers, and partners in data protection

Many processing operations involve providers, which implies special attention to the relationship with them, from the moment they are selected.

Indeed, the commitments of suppliers, but also of suppliers' suppliers, have a direct impact on Orange. As a responsible operator, Orange expects its suppliers to do the same and requires them to respect best practices in terms of personal data protection.

Security and compliance with personal data protection regulations are systematically considered in internal processes and procurement decision-making bodies as well as in contractual relations with suppliers. The latter must commit and pass on the requirements of Orange throughout their supply chain (suppliers, agents, partners, subcontractors, etc.) when the stakeholders participate directly or indirectly in the supply of products or services for Orange. These requirements include compliance with applicable regulations, compliance with the principles of personal data protection, training of employees who process personal data in good practices, limiting the collection, use and sharing of personal data within the scope of the services provided, limiting the retention of data to the period necessary to achieve the purposes for which it was collected. A data deletion or anonymization procedure should be applied when the data is no longer needed. In general, an appropriate level of security is required to protect the data from unauthorized access, disclosure, alteration, or destruction.

Orange establishes relationships based on trust and loyalty with its suppliers and always ensures their full cooperation in matters of personal data, in order to guarantee that the rights of data subjects are exercised, as well as in terms of security.

In particular, as soon as a supplier is confronted with a security incident that could lead to a personal data breach, it has the obligation to notify all relevant information to Orange for its incident management process and within the deadlines defined by the applicable regulations.

Finally, suppliers must be able to demonstrate at all times compliance with the laws applicable to personal data in their country, such as the GDPR in the European Union. To this end, suppliers must implement and document the measures put in place to protect personal data and ensure its confidentiality and integrity. This documentation must be made available to Orange for accountability purposes but also to enable audits.

05 International Transfers of Personal Data

With operations worldwide, Orange processes personal data in several countries and from different sources.

Under this Policy, and in a context where the framework for international transfers responds to various legal regimes, Orange undertakes to take the necessary steps to ensure data protection and security conditions during international transfers in compliance with applicable laws and regulations.

Whether in the context of the circulation of personal data within the Group itself or in the relationship with third parties, in particular its suppliers, Orange ensures that adequate guarantees are implemented both at the contractual level (legal guarantees) and in the effective implementation of the processing (technical and organisational guarantees).

Thus, when transferring personal data, Orange ensures that the exporter and importer of personal data contractually undertake to comply with applicable local data protection law and/or relevant local transfer mechanisms.

Orange pays particular attention, when selecting third parties (suppliers, subcontractors, partners...) who act on behalf of any Orange entity or for their own account, to their ability to offer sufficient guarantees in terms of the protection of personal data, in particular when transferring international data.

06 Access to data by competent authorities

As a telecommunications operator, Orange must respond to requests from the competent authorities, in accordance with the requirements of national security, justice or the protection of human life.

To verify and process these requests, Orange regularly interacts with public authorities in various countries on requests that may concern its customers.

The reviews may concern the jurisdiction of the authority from which the request originates, the formalism of the request, as well as the legal basis and regulations in force in the country. Once these elements have been checked, the request is either executed, rejected, or sent back to obtain the missing information required for its analysis.

Requests may concern customer identification data, geolocation, or call details.

07 Promoting a culture of personal data protection

Orange uses various levers to encourage the development of a genuine culture of personal data protection, both internally and externally:

Employee awareness and training

The day-to-day protection of personal data at Orange involves the participation of all its businesses and employees. Orange sets up awareness-raising campaigns for everyone, whose implementation is monitored at the highest management level.

A range of in-house training courses on the principles of data protection is provided for all employees and personalized in relation to the business lines. More specific training courses are also implemented within Orange for data protection correspondents, project managers, legal services and human resources.

Orange's awareness initiatives also result in a set of documents accessible from the Group's intranet space, such as an internal privacy policy, a charter on the protection of employees' personal data and a general guide on the protection of personal data, available in five different languages.

Through the animation of the networks of referents, and the cooperation of the group's DPOs, multiple topics of expertise are the subject of presentations.

Data protection, a collective issue

Orange is aware that addressing data protection issues in all its forms is a collective challenge on an international scale. It thus participates in its promotion through its participation in various bodies, organizations, or projects.

Orange has joined the Global Network Initiative (GNI), an alliance of international players committed to protecting individuals' right to privacy on the Internet.

In the Middle East & Africa region in particular, Orange works to promote data protection by actively participating alongside government bodies, data protection authorities and economic actors, in events and reflections promoting data protection and security in an increasingly digital world.

Orange participates in several international think tanks and standardization bodies on issues relating to privacy protection. Its participation in ISO standardization work on security management and cryptographic algorithms is testimony to this.

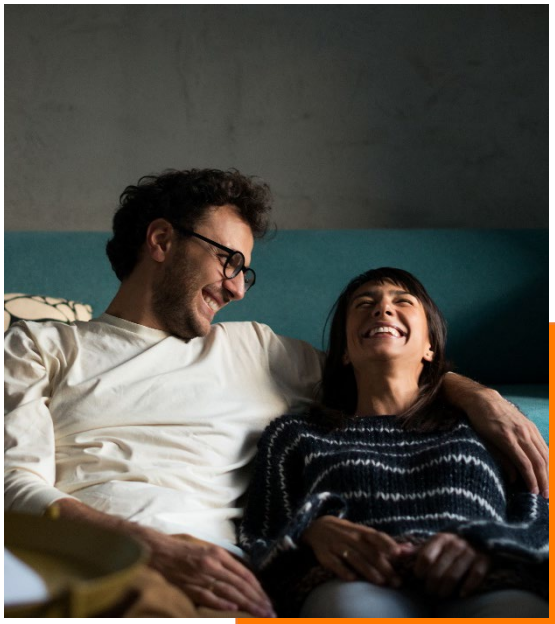
Contribution to research and innovation

Orange is committed to multi-disciplinary, partnership-based Research & Innovation to study the uses and impacts of digital technology and to design technical solutions to strengthen the protection of personal data and respect for privacy. Orange researchers are involved in numerous French (ANR) and European (H2020) collaborative projects, as well as supervising theses. Orange also contributes to the funding of research chairs related to data protection.

Support and dissemination of good practices for the public

Orange attaches particular importance to supporting and disseminating good privacy practices. To contribute to a safer digital world, Orange provides information and best practices in various formats, such as the website "Bien vivre le digital" or videos on social networks, as well as digital workshops.

As part of the Group's activities in Africa and the Middle East, Orange capitalizes on its strong local roots through, for example, the network of Orange Digital Centers, digital learning centers that help to meet the challenge of training and professional integration.



The Group aims to be at the forefront of responsible digital uses, and its “raison d'être” illustrates its commitment to informing and raising awareness of good digital practices.

All Group stakeholders have a role to play in protecting personal data. It is the responsibility of each one to be trained and vigilant so that this protection is constantly maintained.


orange™