

PERSONAL DATA

TRANSFER IMPACT ASSESSMENT (TIA) by ORANGE BUSINESS for the provision of transversal support activities from its Major Services Center in Egypt

Orange Business Overview

Orange Business is a network and digital integrator and serves enterprises worldwide. With a legal presence in more than 60 countries, Orange Business leverages its global footprint to deploy and manage network and digital solutions. Orange Business provides transversal operational activities for its services, including implementation, management, operations and support from specialised facilities located in several countries called **Major Services Centers**, including its Major Services Center located in Egypt.

Global Personal Data Protection Program

Orange Business has implemented a comprehensive global personal data protection program to ensure compliance with the General Data Protection Regulation (GDPR) and other applicable local data protection laws. This program encompasses its entire organization, regardless of the legal entity or country, and is tailored to its global operational practices. Detailed information on how Orange Business processes and protects personal data for its customers can be found in its [Privacy Notice for Customers and Prospects](#).

Appropriate Safeguards for transfers

All Orange Business entities have signed the 2021 EU Commission Standard Contractual Clauses (SCCs) for processor-to-processor transfers for the transfers to the entities hosting the Major Services Centers:

- Data Exporter: Orange Business legal entities in the EU, EEA, UK, and Switzerland.
- Data Importer: the Orange Business legal entity hosting the Major Services Center.

Compliance with the EDPB Recommendations

In line with the European Data Protection Board's (EDPB) Recommendations 01/2020, Orange Business has reviewed its personal data processing activities related to transversal support activities provided by its Major Services Center in Egypt. This review included an assessment of the laws and practices of Egypt, conducted with the assistance of an internationally recognized law firm and local counsel based in Egypt, to evaluate the effectiveness of the EU Standard Contractual Clauses for personal data transfers.

Orange Business monitors and assesses regularly the legal and regulatory framework in Egypt, to ensure that all the relevant technical, contractual and organisational measures are in place.

This assessment was performed by Orange Business for its own compliance and accountability purposes and does not constitute a legal advice or a contractual commitment.

Part 1 - Overview of the transfer:	
Data Exporter	Orange Business affiliates in the EU, EEA, UK and Switzerland sending personal data to the Data Importer.
Role of the exporter in the processing activity	Processor.
Orange Business department exporting the personal data	Orange Business Departments building up and managing/supporting Orange Business.
Data Importer	Orange Business Egypt (Equant Egypt For Communications S.A.E.).
Role of the importer in the processing activity	Processor.
Sector of activity of the Data Importer	Support services.
Orange Business department which processes the transferred data	Major Services Center (MSC).

PERSONAL DATA
TRANSFER IMPACT ASSESSMENT (TIA) by ORANGE BUSINESS for the provision of transversal support activities from its Major Services Center in Egypt

Third Country	Egypt.
Date TIA updated	March 2025.
Frequency of the transfer	Continuous.

Part 2 - Assessment of the Processing Activity:

Purpose of the Transfer	- To provide operational support to Orange Business customers. - To share required technical and commercial data between the process teams (intradepartmental transfer) and other interlocking teams (interdepartmental).
Categories of Personal Data Transferred (see Annex)	Billing Data, Contact Data, Identity Data, Support Data, Location Data, Marketing and Communications Data [only communication for services/support updates], Profile Data, Technical Data, Traffic / Connection Data, Usage Data, Hosted Data.
Categories of Data Subjects to which the Personal Data Transferred relate	Employees of Orange Business, employees of other Orange Affiliates, employees of customers, individual end-users of the services, employees of suppliers.
Categories of recipients within Orange Business entity in the third country	Orange Business operational and support team accessing the data in accordance with their role.
Categories of recipients - External suppliers of Orange Business in the third country	Not applicable.
Type of processing	<u>Remote access:</u> Orange Business internal applications are mainly hosted in France and in any case in Europe and are accessed remotely by staff. <u>Storage in country:</u> Any operation on personal data as necessary by the local staff to perform their duties, such as consultation, deletion or use to prepare reports etc.
Current Technical, Contractual and Organizational Measures (for the processing activity carried out in the third country)	Contractual measures Obligations set out in the Orange Business intragroup data processing and transfer agreement and the EU Standard Contractual Clauses signed between Orange Business entities. Technical and organizational measures – applied globally across all Orange Business entities [Global] Data Protection Standards; [Global] External Technical and Organisational Measures; [Global] Business Continuity Plan documents; [Global] Data breach process;

PERSONAL DATA
TRANSFER IMPACT ASSESSMENT (TIA) by ORANGE BUSINESS for the provision of transversal support activities from its Major Services Center in Egypt

	[Global] Information Security and Data Privacy training and awareness for the employees; [Global] Procedure and digital tool to handle government access requests; [Global] Personal Data Protection Program. <u>Certifications:</u> - Certifications: ISO 9001, ISO 20000-1, ISO 27001, ISO 14001.
Onward transfers (physical transfer from the third country to another country by Orange Business local entity of by a supplier)	Data might be exchanged between the MSC Egypt teams and their peers in the other MSC in India, Brazil and operational teams in Europe where needed, and especially in case of Business Continuity Plan activation.

Part 3 - Assessment of the Third Country:

Data Protection Law	Personal Data Protection Law No. 151 of 2020 (the "DPL")	Link here The DPL follows principles like the GDPR, it will enter in effect within one (1) year from the date of issuance of its Executive Regulations (not yet published in 2025).
Data Protection Authority	Personal Data Protection Center (the "Center")	The Center is yet to be establish.
International instrument(s) on data protection	Egypt has not ratified the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data (Convention 108). Egypt does not adhere to any international instrument on data protection.	
Overview of the applicable legal framework and the rule of law	Egypt is a unitary semi-presidential republic. The Egyptian Constitution of 2014 establishes the rule of law. The right to privacy and to confidentiality are constitutional rights and freedoms under the Constitution. The DPL is tailored to the protection of personal data of natural persons.	
Data Protection Law	The Personal Data Protection Law No. 151 of 2020 ("DPL").	Personal data related to law enforcement records, proceedings, investigations, and lawsuits are excluded from the DPL. Data and private information can be confiscated and monitored under the following cumulative conditions: - By virtue of a reasoned judicial order; - For a defined period of time; and - Only in the cases defined by law. Controllers and processors must comply with any request from national security authorities without the need for a court order. The main requirement is that the request made by the national security authorities to access the personal data must be for national security.

PERSONAL DATA
TRANSFER IMPACT ASSESSMENT (TIA) by ORANGE BUSINESS for the provision of transversal support activities from its Major Services Center in Egypt

National surveillance Law(s)	Law No. 150 of 1950 instituting the Egyptian Criminal Procedures Code ("CPC").	It gives "Investigative Authorities" the right to seize correspondences and to intercept any communications on the condition that the investigations are serious and credible for a specific period of time not exceeding 30 days subject to renewal for another equivalent period.
	The Cyber and Information Technology Crimes Law No. 175 of 2018 ("CL") and its executive regulation No 1699/2020.	It requires technology and telecommunication service providers to maintain the confidentiality of stored data and refrain from disclosing. Technology and telecommunication service providers are required to secure data and information and are required to undertake technical and control measures to prevent cyberattacks. Investigative Authorities have judicial arrest powers to collect or seize data, to inspect and penetrate databases, and to order service providers to submit any data or information. The order issued by the relevant investigative authorities related to the above powers must be for a maximum of thirty (30) days, extendable for only one similar duration; an appeal of such investigation is possible before competent Courts.
	The Anti-Terrorism Law No. 94 of 2015 ("ATL").	Investigative Authorities have the power, to survey, monitor or intercept correspondences and data for a period not exceeding thirty (30) days subject to renewal for another equivalent period or periods of time.
	The Penal Code in Telecommunications Law No 10/2003 ("The Telecommunications Law").	This law recognizes the right to privacy.
Surveillance practices	The DPL applies to personal data of Egyptians residing in Egypt or abroad, as well as foreigners residing in Egypt, it does not apply to personal data of foreigners not residing in Egypt. Additionally, other laws in Egypt allow public authorities to access personal data in specific cases. The recipient of a request to disclose data may be permitted to inform the data exporter unless explicitly ordered to keep it confidential. Orange Business is not aware of any publicly reported precedents.	
Essential guarantees met by the national surveillance law(s)	Legitimate powers for access to personal data by national law enforcement agencies must:	
Guarantee 1	be based on clear, precise and accessible rules	<u>Somehow.</u> The above-mentioned laws lack specific guidelines regarding the circumstances and procedures for accessing data in Egypt. As a result, each request for data access needs to be evaluated individually. Additionally, access to personal data is often justified using vague terms like "national considerations," and "national security" concerns

PERSONAL DATA
TRANSFER IMPACT ASSESSMENT (TIA) by ORANGE BUSINESS for the provision of transversal support activities from its Major Services Center in Egypt

		may also be invoked. Nonetheless, an appeal is possible before jurisdictional authorities.
Guarantee 2	be subject to a requirement of necessity and proportionality regarding the legitimate objectives pursued need to be demonstrated	<u>Somehow.</u> While the above-mentioned laws set out the purpose of access of personal data by public authorities, access to personal data is generally justified by national considerations, which is a broad term allowing access on a generalized basis.
Guarantee 3	be subject to an independent oversight mechanism	<u>Somehow.</u> Few laws require the issuance of a judicial warrant. In certain cases, and if the access is based on a reasoned judicial order, such an order can be appealed before the competent court.
Guarantee 4	provide effective remedies for the individuals	<u>Somehow.</u> Breaches of personal data or violations of data subjects' rights can lead to penalties like fines and imprisonment under different laws. Data subjects have the right to file complaints and take legal action for damages if their data is breached or if they are unable to exercise their rights. Unjustified access to clients' account data can result in imprisonment and/or fines. If access is granted through a court order or request from investigative authorities, the controller or processor is not considered at fault. Data subjects can challenge court orders or warrants granting access to their data in the appropriate tribunal. However, the DPL is still not in effect in Egypt. The rights granted by the DPL do not apply to data held by public authorities nor to data held by the national security authorities. Organizations must comply with court orders to avoid being seen as obstructing justice, but they can challenge such orders in court.
Government access requests received by Orange Business in respect of the personal data for the processing in scope of this assessment	Orange Business has no record of access requests by a government in respect of the personal data processed within the scope of this assessment.	

PERSONAL DATA
TRANSFER IMPACT ASSESSMENT (TIA) by ORANGE BUSINESS for the provision of transversal support activities from its Major Services Center in Egypt

Part 4 - Orange Business conclusion on the effectiveness of the EU Standard Contractual Clauses:

Orange Business has reviewed its personal data processing activities for the provision of operational support by its Major Services Center in Egypt. Orange Business has reviewed the laws and practices of Egypt with the assistance of an international recognized law firm and local counsel based in Egypt.

Essential Guarantees 1, 2, 3 and 4 are somehow complied with, based on the justifications provided above.

Nonetheless, in light of:

- the scope of the processing activities;
- the personal data processed;
- the existence of an established constitutional, judicial and parliamentary system in Egypt;
- the absence of knowledge of problematic practises;
- the lack of requests for access to personal by government authorities for the activities in scope;
- the existence of safeguards enshrined in the constitution;
- the absence of evidence that the personal data transferred would be of a particular interest for public authorities in Egypt;

Orange Business cannot exclude any risk of it being accessed by judicial or governmental authorities. However Orange Business concludes that it has found no evidence that the laws and practices of Egypt will prevent in practice Orange Business from fulfilling its obligations under the EU Standard Contractual Clauses.

Supplementary measures: the personal data in scope of this assessment is not under the custody or control of Orange Business Egypt. Government access requests are referred to Orange Business Regulatory team.

PERSONAL DATA
TRANSFER IMPACT ASSESSMENT (TIA) by ORANGE BUSINESS for the provision of transversal support activities from its Major Services Center in Egypt

Annex - Categories of Personal Data

Billing Data	the consumption data that Orange Business Services collects from services that it provides to its Customers in order to calculate charging and billing information, to the extent related to natural persons.
Contact Data	first name, last name, email address, address and telephone numbers, job role within the Customer
Identity Data	first name, last name, honorific (e.g. Ms, Mr. Dr.,...), username or similar identifier, password, ID document / number
Support Data	Customer Representative or End User service ticket information, Customer Representative or End User telephone recordings for incident
Location Data	geographic location, device location, SIM card location for mobile services
Marketing and Communications Data	preferences in receiving marketing from us and our third parties and communication preferences
Profile Data	interest, preferences, comments, questions, feedback, and survey responses
Technical Data	internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system, and platform, as well as other technology on the devices natural persons use to access areas of our website or other technical data generated through the use of the service
Traffic / Connection Data	data revealing a communication's origin, destination, route, format, size, time duration, IP address, time zone setting, MAC address.
Hosted Data	any categories of Customer Personal Data that may be recorded or stored (such as voicemails, call recordings, files) by Customer and which is hosted on the infrastructure provided by Orange Business Services
Usage Data	information about how End Users use our products and services, and natural persons use our website
Visual Data	photographs and other visual records we take during Orange Business Services or third-party events or that we process based on your consent
Other	please list as required