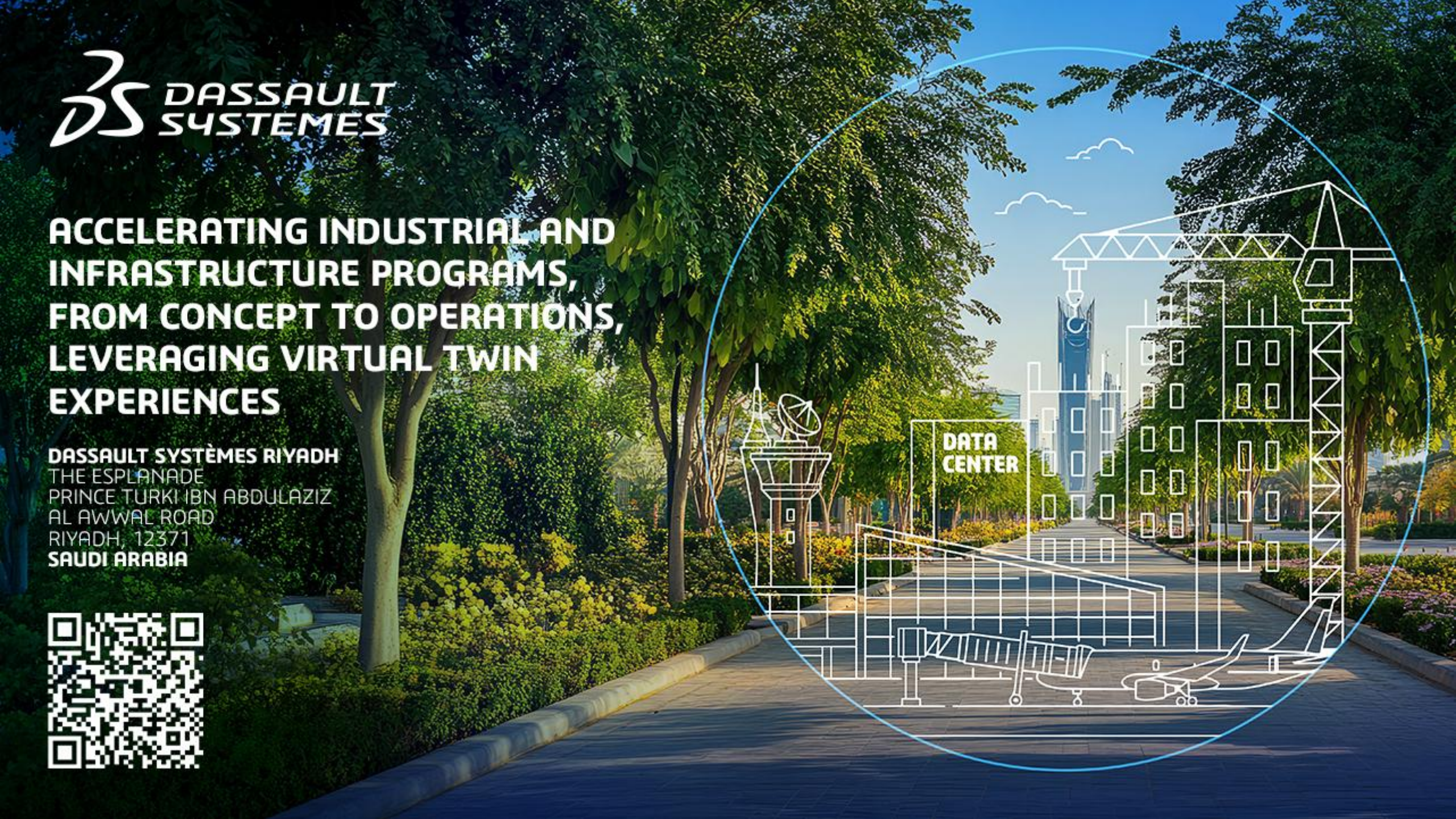
Part 5 – Living, Operating and Doing Business in Saudi Arabia

DASSAULT SYSTEMES

ACCELERATING INDUSTRIAL AND INFRASTRUCTURE PROGRAMS, FROM CONCEPT TO OPERATIONS, LEVERAGING VIRTUAL TWIN EXPERIENCES

DASSAULT SYSTÈMES RIYADH
THE ESPLANADE
PRINCE TURKI IBN ABDULAZIZ
AL AWWAL ROAD
RIYADH, 12371
SAUDI ARABIA



4. Telecoms, internet, ICT, data and PDPL

By Dassault Systèmes

DASSAULT SYSTEMES
The Esplanade, Prince Turki Ibn Abdulaziz Al Awwal Road
Riyadh 12371, Saudi Arabia
https://www.3ds.com/

4. Telecoms, internet, ICT, data and PDPL

MOBILE AND INTERNET SETUP

Saudi Arabia has three main nationwide mobile network operators: stc, Mobily and Zain, alongside smaller players such as GO (Atheeb), all offering 4G and extensive 5G coverage plus fixed fiber services in major cities.

Prepaid SIMs are widely available in airports and malls, while postpaid and business packages (bundling mobile, fixed internet and sometimes cloud or collaboration tools) target corporate and RHQ clients.

SIM cards must be registered to a verified identity, and for residents this means linking the SIM to the individual's iqama (resident ID) under Communications, Space and Technology Commission (CST, formerly CITC) rules. This iqama-linked number is then used to access almost all government services (Absher, Qiwa, tax, banking, national address) and many corporate platforms, so executives should secure a local number early and avoid frequent number changes.

Home and office connectivity is typically provided via fiber (100–500 Mbps and higher) or 5G fixed-wireless, with common business offers in the SAR 200–300/month range for 100 Mbps+ fixed connections, and SAR 100–200/month for generous 5G mobile data plans.

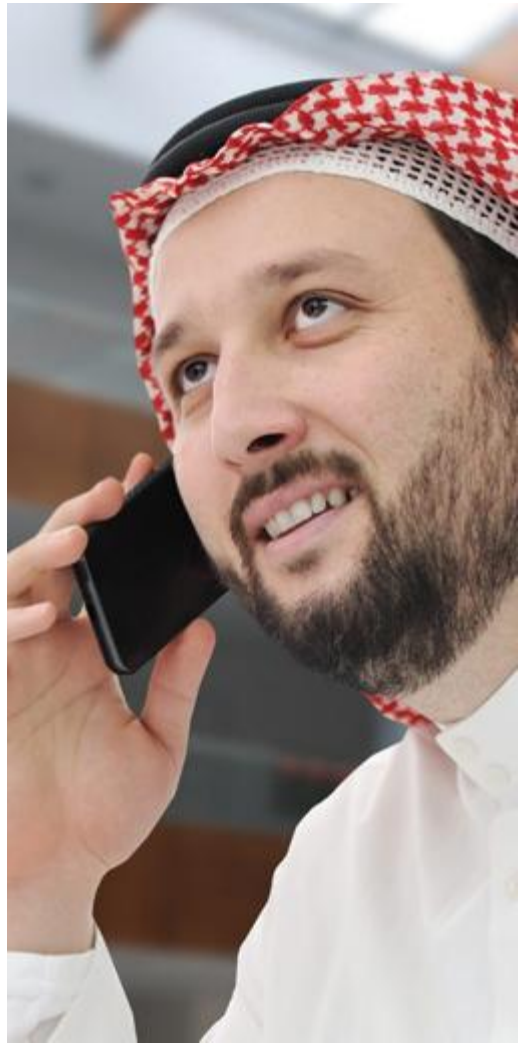
Installation of fixed lines usually requires iqama details, a registered national address and a lease or office contract, and can generally be completed within a few days for standard locations in Riyadh, Jeddah and Dammam.

DATA LOCALISATION AND SECTOR FRAMEWORKS

Saudi Arabia does not impose blanket data-localisation for all private-sector data, but it does maintain strict localisation for government data and certain regulated sectors, and expects organisations to classify data accordingly.

Under CST's Cloud Computing Regulatory Framework (Version 3.0), "Saudi Government Data" may not be transferred outside the Kingdom, and must be hosted with registered providers that meet specific technical and security requirements. Private-sector subscribers must perform their own data classification and ensure that any Level 3 or government-related datasets are kept on Saudi soil or within approved data-center services.

Additional CST regulations on data-center and outsourcing services, effective from 2024, create a dedicated regime for commercial data-center operators in the Kingdom and set conditions for outsourcing telecom and cloud functions abroad (including resilience and security controls). For multinational groups, this means global cloud and network architectures should be reviewed to ensure that workloads or support functions touching government related or regulated telecom data remain within Saudi-compliant infrastructures.



4. Telecoms, internet, ICT, data and PDPL

PDPL: SCOPE, CONSENT AND CROSS-BORDER TRANSFERS

Saudi Arabia's PDPL is a horizontal data-protection law applying to any processing of personal data pertaining to individuals in the Kingdom, by controllers or processors inside or outside Saudi Arabia. "Personal data" is broadly defined to cover any information that identifies or could identify a natural person, while "sensitive data" includes health, genetic, biometric, security, criminal, religious, political and similar categories.

Controllers must have a clear legal basis for processing, with consent being central but not exclusive: PDPL and its regulations also allow processing for contract performance, legal obligations, vital interests and other specified purposes. Consent must be specific, informed and freely given, and individuals benefit from rights of access, correction, deletion and restriction, which controllers must handle via documented procedures and response timelines.

Cross-border transfers are permitted but tightly framed. In general, a controller may transfer personal data outside the Kingdom if:

- The transfer serves a permitted purpose (performance of a contract with the data subject or an international obligation, or other SDAIA-defined purposes).
- The recipient country offers an "adequate" level of protection or, failing that, appropriate safeguards (such as SDAIA-approved standard contractual clauses or binding corporate rules) are in place.
- Explicit consent is obtained where required, and sensitive data is subject to additional restrictions.

The 2024–2025 transfer regulations add requirements: mapping all international transfers, documenting legal bases, performing transfer risk assessments and maintaining records of safeguards and security controls. Certain derogations remain available for limited cases (vital interests, legal claims) when safeguards cannot be used, but these are exceptional and subject to conditions.

CORE OBLIGATIONSS FOR FOREIGN SUBSIDIARIES AND RHQ

Governance and accountability: Appointing a responsible function for PDPL compliance in the Kingdom, maintaining processing records, and being able to demonstrate "privacy by design and by default" in systems and processes.

Risk & DPIAs: Performing data-protection impact assessments for high-risk processing and documenting mitigations.

Security: Implementing appropriate technical and organisational measures, including encryption in transit and at rest, access management, logging and incident response plans aligned with SDAIA and CST expectations.

Vendor & intra-group management: Ensuring that processors offer sufficient guarantees, are bound by PDPL-aligned contracts, and respect any localisation and cross-border requirements.

Breach management & notifications: Establishing internal escalation pathways and external notification processes towards SDAIA and affected data subjects, based on thresholds defined in the implementing regulations.

RHQs, in particular, should design a Saudi-compliant but globally consistent model for records of processing, transfer registers and group policies, to avoid conflicting obligations between PDPL and other regimes such as GDPR.

PDPL and its regulations contain exemptions or relaxations in certain cases, for example for purely domestic personal or household activities, for anonymised data, and for processing required to comply with legal obligations or to protect vital interests where consent cannot be obtained. However, corporate groups should treat these as narrow carve-outs.