International cooperation for protected cross-border data flows

ATHENS

31 MAY 2023

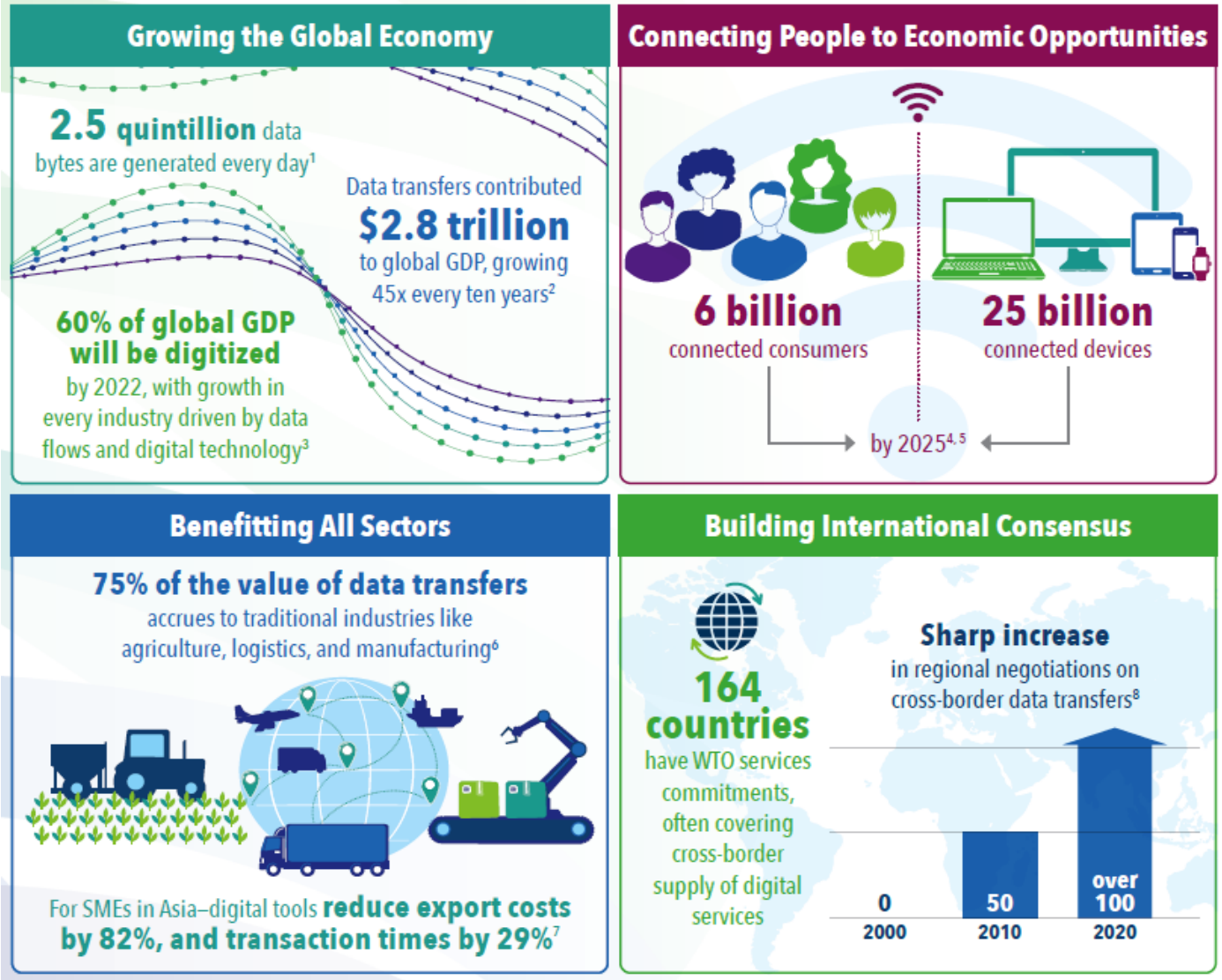
ABOUT DATA AND DATA TRANSFERS

ABOUT DATA AND DATA TRANSFERS

- What is a Data Transfer?
  - “Cross-border data transfers” refer to the movement or transfer of information across IT networks.
  - Consumers and companies of all sizes rely on data transfers across countries, regions, continents.
    - Any communication to a person / device in another country
    - Financial transactions
    - Data for product safety approvals
    - Data and tools to protect consumers from fraud, ID theft, malicious cyberattacks
    - Data to identify dangerous counterfeit products (e.g., distribution patterns / sources / markers of such products)
    - Data to optimize supply chain (reducing carbon intensity of int’l trade)

ABOUT DATA & DATA TRANSFERS

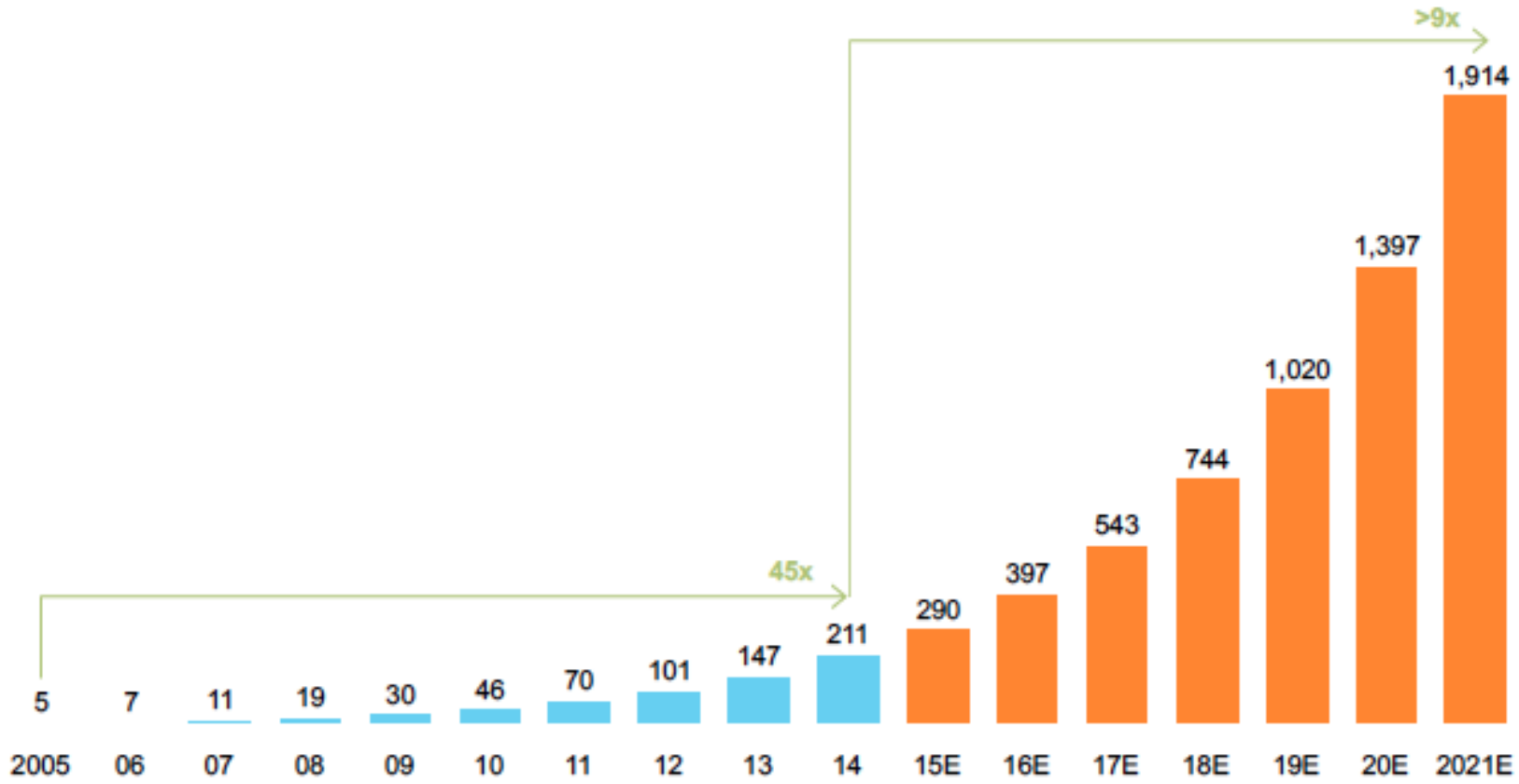
Cross-border Data Transfers – Facts & Figures



ABOUT DATA & DATA TRANSFERS

Cross-border bandwidth has grown 45 times larger over the past decade—and may grow another nine times larger by 2021

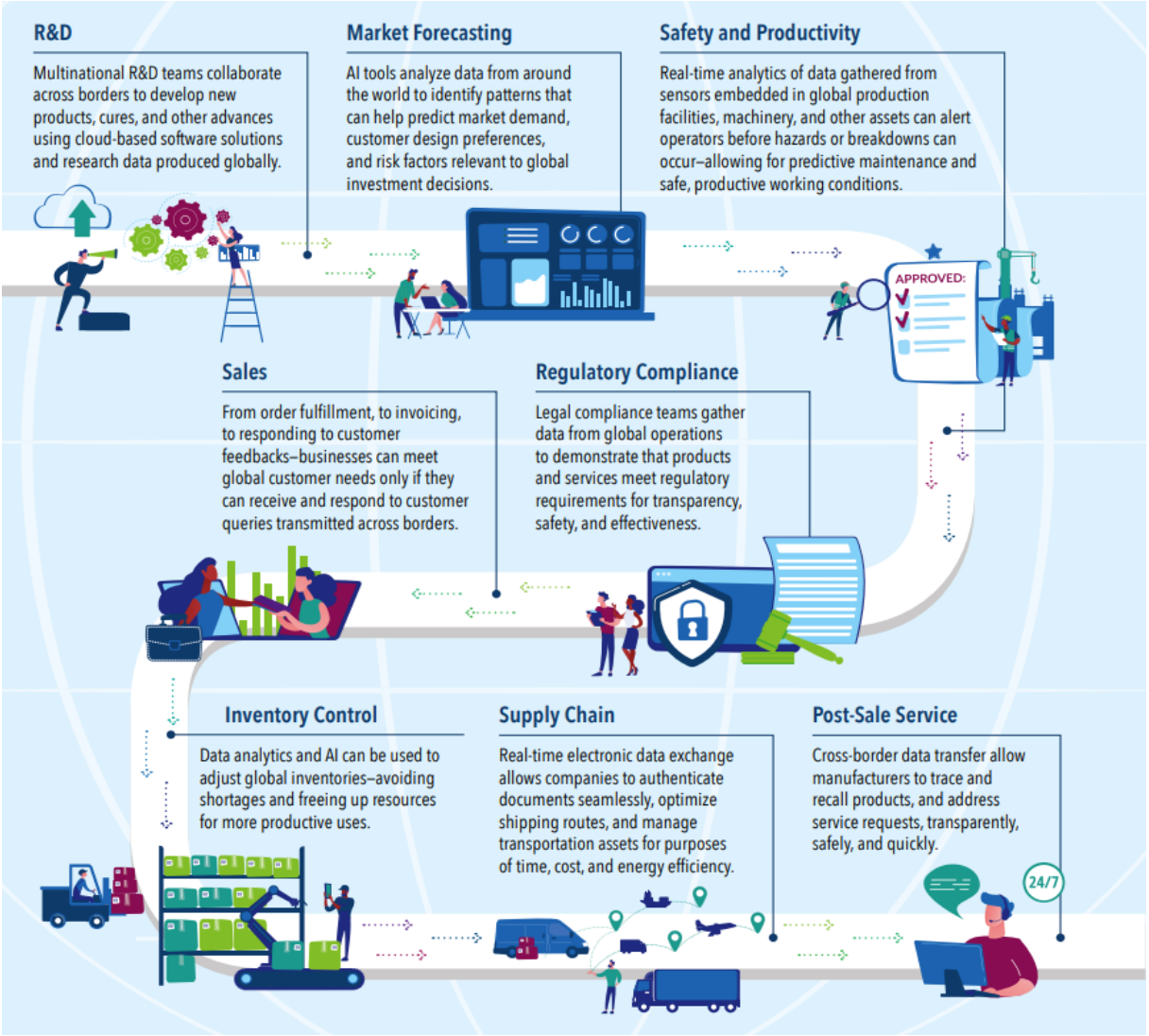
Used cross-border bandwidth, global
Terabits per second



Source: Telegeography – McKinsey Global Institute Analysis

ABOUT DATA & DATA TRANSFERS

Data Transfers at Every Stage of the Value Chain



DATA TRANSFERS AND PRIVACY

DATA TRANSFERS AND PRIVACY

- From an EU perspective
  - Adequacy
  - Standard Contractual Clauses
  - Binding Corporate Rules
  - Other mechanisms foreseen in legislation but not yet used

DATA TRANSFERS AND PRIVACY

- Recent litigation and subsequent enforcement
  - In particular - Schrems II

- Issue at stake is not about companies' use of data but about the level of access that third governments have over the data transferred and the redress available

- In the absence of clear rules – complicated situation and calls for data localization and immunity from third countries government access
  - Guidance for additional safeguards in data transfers
  - e.g. EU Data Act or Health Data Space
  - e.g. Cybersecurity certification

INTERNATIONAL COOPERATION FOR PROTECTED CROSS-BORDER DATA FLOWS

International cooperation for protected cross-border data flows

EU US DATA PRIVACY FRAMEWORK

- **United States:**
  - Implementation of Executive Order 14086 issued in October 2022 by US President Joseph Biden
    - Each intelligence agency to update its privacy policies and procedures to implement privacy and civil liberties safeguards
    - implement regulations issued by the US Attorney General that operationalize the new redress mechanism, including the Data Protection Review Court
    - US Attorney General to adopt a decision recognizing the European Economic Area as an organization that benefits from the new redress mechanism
- **European Union:**
  - EU to formally adopt the adequacy decision

International cooperation for protected cross-border data flows

OECD principles on trusted government access to personal data adopted on December 14, 2022

- **7 principles on trusted government access to personal data address:**

1. Legal basis. Under this principle, government access to personal data held by private sector entities is provided for and regulated by the country's legal framework.
2. Legitimate aims. This principle recognizes that government access is to support the pursuit of specified and legitimate aims, and is carried out in a manner that is not excessive in relation to those aims.
3. Approvals. Under this principle, prior approval requirements for government access are established in the legal framework, to ensure that access is conducted in accordance with applicable standards, rules, and processes.
4. Data handling. This principle recognizes that personal data acquired through government access can be processed and handled only by authorized personnel, and will be subject to internal controls.
5. Transparency. This principle recognizes that a legal framework for government access is clear and easily accessible to the public, and that mechanisms exist for providing transparency about government access to personal data. Those mechanisms include public reporting by oversight bodies, as well as individual notification where applicable. The principles specifically recognize that private sector entities are allowed to issue aggregate statistical reports regarding access requests, in conformity with the legal framework.
6. Oversight. This principle recognizes that mechanisms exist for effective and impartial oversight.
7. Redress. This principle recognizes that the legal framework provides individuals with effective judicial and non-judicial redress to identify and remedy violations. These may include, subject to applicable conditions, terminating access, deleting improperly access or retained data, restoring the integrity of data, and the cessation of unlawful processing, as well as compensation for damages suffered by an individual depending on the circumstances.

International cooperation for protected cross-border data flows

G7 and Data Free Flow with Trust

- Hiroshima May 19-21
- The G7 leaders endorsed operationalizing DFFT through the establishment of the Institutional Arrangement for Partnership, tasking relevant Ministers to work toward delivering substantive Roadmap for Cooperation on DFFT:
  - Data Localisation
  - Regulatory cooperation
  - Trusted Government Access to Data
  - Data Sharing
- The G7 leaders welcomed the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities as an instrument to increase trust in cross-border data flows.