This document lays out the DPA's narrative on Digital Trust and recommendations for policymakers on how we can collectively achieve a trusted digital ecosystem.

Key Message 1: Digital Trust is crucial for the continued growth of the digital economy

- Today, the world is increasingly relying on digital technologies and services in our daily lives. It has helped to keep us connected with our families and friends, enhance productivity at the workplace and seamlessly conduct online transactions for digital payments.
- Digital trust underpins the ability for everyone to be able to access and use digital technology securely.
    - Individuals need to trust that their data is protected, that their online identities are secure and that they can interact safely online.
    - Businesses need to demonstrate their competence and commitment to keeping their customers' personal data and transactions private and secure
    - Governments need to establish a regulatory environment that promotes digital trust, including strong data protection laws, risk-based cyber-security measures and enabling seamless cross-border data flows. Governments should avoid protectionism and other measures that ultimately undermine security by limiting access to best-in-class technology solutions.

Key Message 2: Security and privacy are foundational pillars of digital trust

<u>Security</u>

- Risk-based international standards provide a common language that facilitates trade, accelerates innovation, and enables people to work together toward greater common goals that cut across disciplines and borders. By contrast, a patchwork of conflicting national technical standards and legal standards raises costs and poses barriers to small businesses when entering new markets, and creates security risks if high standards for data protection and security are not aligned. At the same time, governments should also avoid imposing overburdensome data security requirements that extend beyond what is typically covered in data protection or government data classification frameworks. This is likely to result in over-classification of data, leading to confusion and more burden on businesses.

<u>Privacy</u>

- Individuals need to be able to trust the organizations with which they share their personal data. Organizations need to have the appropriate security policies put in place within their digital systems to protect their customers.
- Individuals are rightly concerned about data breaches and cyberattacks. But governments should not resort to reactive reactions such as imposing data localization requirements. This will do nothing to reduce such incidents.
    - Governments need to recognize that physical location of data has no bearing on risk mitigation or cyberthreats. Data localization policies simply increase costs and barriers

to entry for service providers and limit the availability of services to consumers including preventing the country from benefiting from digital trade.
    - Additionally, these requirements might undermine cybersecurity instead, as businesses and consumers could be prevented from accessing the most state-of-the-art secure infrastructure, applications or software. Furthermore, the cross-border sharing of data is needed to identify systemic vulnerabilities and for the security community to work together to address these vulnerabilities.
- We need to ensure that good data protection policies and best practices are being adopted and that the responsibilities of data processors and data controllers are clear. Governments should also ensure that there are interoperable data privacy frameworks in the region.

Policy recommendations:

- For governments to harmonize data privacy and security frameworks through alignment and adoption of international standards and best practices
- For governments to adopt risk-based and accountability-driven approaches to cybersecurity
- For governments to not impose data localization requirements, which could end-up undermining cybersecurity and increase costs and barriers for businesses