Communications Regulatory Authority
State of Qatar

هيئة تنظيم الاتصالات
دولة قطر

CLOUD POLICY FRAMEWORK

June 2022

إطار عمل سياسة الحوسبة السحابية

يونيو 2022

Table of Content

جدول المحتويات

1. Executive Summary

1. نبـذة

As part of Qatar National Vision 2030, Qatar's ambition is to establish itself as a leading digital hub in the Middle East, a home to international digital players and an attractive destination for domestic and foreign investments in innovative digital services.

تتطلع قطر في إطار رؤيتها الوطنية 2030 إلى ترسيخ مكانتها كمركز رقمي عالمي رائد في الشرق الأوسط، وموطن للمتعاملين الرقميين الدوليين ووجهة جذابة للاستثمارات المحلية والأجنبية في مجال الخدمات الرقمية المبتكرة.

Qatar has placed the promotion of cloud computing at the heart of its transformative digital strategy. Cloud computing unlocks efficiency and productivity worldwide and is an opportunity for Qatar-based businesses to grow, for public and private entities to provide better services and, ultimately, for Qatar to become a fully digitalized country.

وقد وضعت قطر تعزيز الحوسبة السحابية على رأس أولويات استراتيجية التحول الرقمي في قطر. وتُطلق الحوسبة السحابية العنان لزيادة الكفاءة والإنتاجية في جميع أنحاء العالم وهي فرصة كبرى للنمو بالنسبة للشركات في قطر، كما تتيح للكيانات الخاصة والعامة تقديم خدمات أفضل، وهو ما يصب في نهاية المطاف إلى تحول قطر لتصبح دولة رقمية بالكامل.

The Cloud Policy Framework, part of the going Communications Regulatory Authority's Strategic Plan 2020-2024, supports the objectives of the Qatar National Vision 2030 as well as of the Qatar National Second Development Strategy.

يأتي إطار عمل سياسة الحوسبة السحابية، الذي وُضع ضمن إطار الخطة الاستراتيجية لهيئة تنظيم الاتصالات 2020-2024، دعماً لأهداف رؤية قطر الوطنية 2030 وكذلك استراتيجية التنمية الوطنية الثانية لدولة قطر.

Embracing the principles of Trust, Security and Transparency, the Cloud Policy Framework identifies policy and regulatory recommendations that are critical for the development of a robust cloud industry in Qatar. To meet the objectives of a cloud-friendly regulatory environment, joint efforts and a concerted approach are required from government entities.

وجدير بالذكر أن إطار عمل سياسة الحوسبة السحابية حددت التوصيات السياسية التنظيمية التي تُشكل عصب تطوير صناعة سحابية سليمة في قطر وذلك دعماً منها لمبادئ الثقة والأمن والشفافية. ولتحقيق أهداف البيئة التنظيمية المواتية للحوسبة السحابية، فإنه يلزم بذل الجهود المشتركة والتنسيق فيما بين الجهات الحكومية.

Given the pervasive nature of cloud computing, the Cloud Policy Framework calls for the highest level of cooperation

في ضوء الطبيعة المتغلغلة للحوسبة السحابية، يدعو إطار عمل سياسة الحوسبة السحابية إلى زيادة التعاون إلى أعلى مستوى بين الكيانات الحكومية

between government entities and private stakeholders, e.g. cloud service providers, infrastructure and connectivity providers, software developers, on-line platforms and cloud users. To this extent, a clear commitment to policies that support cloud solutions is paramount for cloud services to take off.

وأصحاب المصلحة في القطاع الخاص، مثل مقدمي الخدمات السحابية، ومقدمي خدمات البنية التحتية والاتصالات، ومطوري البرمجيات، والمنصات الإلكترونية ومستخدمي الخدمات السحابية. وبناءً عليه، فإن الالتزام التام من قبل الجهات الحكومية بـ "الحوسبة السحابية أولاً" في سياسات الشراء بدعم الحلول السحابية يُعدّ أمراً بالغ الأهمية لانطلاق الخدمات السحابية.

2. Introduction

2. المقدمة

To meet the goals of the Qatar National Vision 2030[1] (QNV 2030) and of the Qatar National Second Development Strategy[2] (NDS2), significant investments are required in high quality digital infrastructures and services. In Qatar, very high capacity fixed and mobile broadband is today largely accessible to both the public and the private sectors[3]. Given the high availability of ultrabroadband, the development of next generation data centers and world-class cloud computing services[4] have been identified as one of the strategic areas at the highest political level.

يتطلب تحقيق أهداف رؤية قطر الوطنية 2030[1] واستراتيجية التنمية الوطنية الثانية لدولة قطر[2]، استثمارات كبيرة في البنى التحتية والخدمات الرقمية رفيعة المستوى. ويمكن حالياً داخل قطر أن يصل القطاعي العام والخاص بصورة كبيرة وسهلة إلى نطاقات البرودباند الثابتة والمتنقلة ذات السعة العالية[3] ونظراً للتوافر الكبير لخدمات البرودباند فائق السرعة، يدخل تطوير مراكز البيانات من الجيل القادم وخدمات الحوسبة السحابية ذات المستوى العالمي[4] ضمن المجالات الاستراتيجية التي تم تحديدها على أعلى مستوى سياسي.

1- تهدف رؤية قطر الوطنية 2030 إلى "تحويل دولة قطر إلى دولة متقدمة قادرة على تحقيق التنمية المستدامة وعلى تأمين استمرار العيش الكريم لشعبها جيلا بعد جيل". (https://bit.ly/3g9oYbC)

2 - نجد في النتائج المستهدفة باستراتيجية التنمية الوطنية الثانية لدولة قطر ما يلي: "إقامة بنية تحتية مستدامة على أعلى مستوى تدعم الاقتصاد الوطني وقادرة على مواكبة أحدث التقنيات الذكية ". (https://bit.ly/38aZvvB)

3- وفقًا لتقرير الاتصالات الذي نشرته هيئة تنظيم الاتصالات ، فإن 92٪ من اشتراكات خدمات البرودباند الثابت عبارة عن توصيلات ألياف ، كما أن 86٪ من الشبكات لها سرعة معلنة تبلغ 30 ميجابت / ثانية أو أكثر و يبلغ انتشار خدمات البرودباند المتنقل نسبة 129٪ من السكان ، مع توفر تقنية شبكات الجيل الخامس الخاصة فعليا. (https://bit.ly/3gapKFu).

4- تتيح الحوسبة السحابية للمستخدم النهائي الوصول إلى البيانات واستخدام القدرة الحوسوبية وخدمات البرمجيات في أي وقت وفي أي مكان بالاستفادة من شبكات النطاق العريض عالية السعة. يمكن للمستخدمين الحصول على قدرة حوسبية غير محدودة تقريبًا تحت الطلب مع تخفيض استثماراتهم الرأسمالية. انظر الملحق الأول للاطلاع على تعريف "الحوسبة السحابية".

1- Qatar National Vision 2030 is aimed at "transforming the country into an advanced country, capable of sustaining its own development and providing for high standards of living for all its people for generations to come"(https://bit.ly/2VtwnL6).

2- Qatar National Second Development Strategy defines the following target outcome: "Develop a sustainable and high-quality infrastructure that supports the national economy and is capable of keeping abreast of the latest smart technologies" (https://bit.ly/2AhPGQe).

3- According to the Telecommunication Report published by the CRA 92% of fixed broadband subscriptions are fiber connections, and 86% of connections have an advertised speed of 30 Mb/s or more. Mobile broadband penetration is at 129% of the population, while 5G technology is already available (https://bit.ly/2NGysz8).

4- Leveraging on high-capacity broadband networks, cloud computing allows the end-user to access data, use computing) power and software services anytime and anywhere. Users can command almost unlimited computing power on demand whilst minimizing their capital investments. See Annex I for a definition of "cloud computing".

For Qatar, investing in cloud computing capabilities is a priority. It represents an opportunity for public entities to improve the provision of high quality services to citizens, for businesses and organizations to improve dramatically their efficiency and the security of their data and, ultimately, for the country to become fully digitalized.

جديراً بالذكر أن الاستثمار في الحوسبة السحابية من الأولويات بالنسبة لقطر: فهو أيضاً يمثل فرصة للكيانات العامة لتقديم خدمات عالية الجودة للمواطنين والشركات والمنظمات؛ تعزيزاً لأمن البيانات الخاصة بهم، وزيادة الكفاءة والنمو بشكل كبير، مما يؤدي في نهاية المطاف إلى أن تصبح الدولة رقمية بالكامل.

Cloud computing is an enabler for many broader use cases, for example within the Internet of Things, Artificial Intelligence and other enterprise offerings such as 5G private networks and, worldwide, the adoption of public cloud services has benefitted the economy[5,6].For the private sector, it is estimated that businesses experience on average a net return in the range of 100% to 250% on their investments in cloud services[7,8]. Globally, public cloud spending will grow from $229 billion in 2019 to nearly $500 billion in 2021[9].

وتعد الحوسبة السحابية من العوامل الداعمة للعديد من الاستخدامات ذات النطاق الأوسع، حيث تستخدم على سبيل المثال داخل إنترنت الأشياء والذكاء الاصطناعي وغيرها من العروض المقدمة من الشركات مثل شبكات الجيل الخامس الخاصة والعالمية، كما أن اعتماد الخدمات السحابية العامة قد انعكس بالفائدة على الأنشطة الاقتصادية [5,6]، وتشير التقديرات، بالنسبة للقطاع الخاص، إلى أن الشركات تُحقق في المتوسط صافي عائداً يتراوح بين ٪100 و٪250 على استثماراتها في الخدمات السحابية[7,8] وعلى الصعيد العالمي، سوف يزيد الإنفاق العام على خدمات الحوسبة السحابية من 229 مليار دولار في عام 2019 حتي يصل إلى ما يقرب من 500 مليار دولار في عام 2021 [9].

5- ديلويت، 2017. "قياس الأثر الاقتصادي للحوسبة السحابية في أوروبا". المفوضية الأوروبية. متاح على الموقع (https://bit.ly/2YBVwVU).

6- جارتنر ، 2018. متاح على الموقع (https://gtnr.it/2Ze50Wx).

7- ديلويت، 2018. "التأثيرات الاقتصادية والاجتماعية لمنصة جوجل السحابية" سبتمبر 2018. متاح على الموقع. (https://bit.ly/3g3BCJi).

8- ماكينزي، 2018. إجراء الانتقال الآمن إلى الحوسبة السحابية العامة. متاح على الموقع.(https://mck.co/3eBcLMy).

9- https://bit.ly/2Zo8aqA.

5- Deloitte, 2017, "Measuring the Economic Impact of Cloud computing in Europe." European Commission (https://bit.ly/2YBVwVU).

6- Gartner, 2018 (https://gtnr.it/2Ze50Wx).

7- Deloitte, 2018, "Economic and Social Impacts of Google Cloud." September 2018. (https://bit.ly/3g3BCJi).

8- McKinsey, 2018, "Making a Secure Transition to the Public Cloud".(https://mck.co/3eBcLMy).

9- https://bit.ly/2Zo8aqA.

These benefits are mainly due to:

- An increase of revenues deriving from cloud-enabled services.
- An increase in the customer base of organizations moving to cloud services.
- A drastic reduction of IT costs[10].

وتُعزى هذه المنافع بالأساس إلى ما يلي:

- زيادة الإيرادات الناتجة عن الخدمات التي تعتمد على الحوسبة السحابية.
- زيادة في قاعدة العملاء للمؤسسات التي تنتقل إلى الخدمات السحابية.
- انخفاض كبير في تكاليف تكنولوجيا المعلومات[10].

A sound policy and regulatory framework, inspired by the principles of Trust, Security and Transparency is of utmost importance for cloud computing to develop. Consequently, the Communications Regulatory Authority (the "CRA") has developed the Cloud Policy Framework as a strategic action that identifies key areas where legal and regulatory review is needed[11].

إن وجود سياسة رشيدة وإطار تنظيمي سليم استوحيت من مبادئ الثقة والأمن والشفافية يعتبر له أهمية بالغة في تطوير الحوسبة السحابية. ومن ثم، فقد وضعت هيئة تنظيم الاتصالات (يُشار إليها فيما يلي بـ "الهيئة") إطار عمل سياسة الحوسبة السحابية لتكون إطاراً استراتيجياً يحدد المجالات الرئيسية التي تتطلب المراجعة القانونية والتنظيمية[11].

The Cloud Policy Framework calls for the highest level of cooperation between government entities and private stakeholders, e.g. Cloud Services Providers, data centers providers, infrastructure and connectivity providers, software developers, on-line platforms and cloud users. To this extent, a clear commitment by government entities to implement procurement policies that support cloud solutions is paramount for cloud services to take off.

يطالب إطار عمل سياسة الحوسبة السحابية الهيئات الحكومية وأصحاب المصلحة من القطاع الخاص، مثل مقدمي خدمات مراكز البيانات، ومقدمي خدمات البنية التحتية والاتصالات، ومطوري البرمجيات، والمنصات الإلكترونية ومستخدمي الخدمات السحابية تحقيق أعلى مستوى من التعاون المشترك، لذا، فإن الالتزام التام من قبل الجهات الحكومية بـ "الحوسبة السحابية أولاً" في سياسات الشراء بدعم الحلول السحابية يُعدّ أمراً بالغ الأهمية لانطلاق الخدمات السحابية.

10- للخدمات الحوسبة السحابية إسهام واضح في نمو الناتج المحلي الإجمالي في كل من الاقتصادات المتقدمة والنامية وتظهر فوائدها بالأساس في نمو الإنتاجية وكفاءة التكلفة. المرجع السابق

11- تتولى الهيئة تنظيم قطاع الاتصالات وتكنولوجيا المعلومات والبريد والنفاذ إلى الإعلام الرقمي في دولة قطر بموجب المرسوم بقانون رقم (42) لسنة 2014. وهدفها الرئيسي تقديم التشجيع والدعم لجعل قطاع تكنولوجيا المعلومات والاتصالات أكثر انفتاحا وتنافسية بغية توفير خدمات اتصالات متطورة وموثوق بها تخدم كافة أنحاء الدولة.

10- The contribution of cloud computing services to GDP growth is visible both in advanced and in developing economies with its benefits mainly visible in productivity growth and cost efficiencies (see footnote 7).

11- The CRA is mandated to regulate ICT, Post and Access to Digital Media in the State of Qatar under Emiri Decree No. (42) of 2014. Its key objective is to encourage and support an open and competitive ICT sector that provides advanced, innovative and reliable communications services in the State of Qatar.

رؤية قطر الوطنية 2030
استراتيجية التنمية الوطنية الثانية لدولة قطر

"تطوير بنية تحتية مستدامة على أعلى مستوى تدعم الاقتصاد الوطني وقادرة على مواكبة أحدث التقنيات الذكية"

استراتيجية هيئة تنظيم الاتصالات 2020-2024

إطار عمل سياسة الحوسبة السحابية لدولة قطر

أهداف أصحاب المصلحة في القطاعين العام والخاص في سلسلة القيمة للحوسبة السحابية

مثال: (تصنيف البيانات)

مبادئ الثقة والأمن والشفافية

مثال: (دليل المنشآت الصغيرة والمتوسطة)

توصيات السياسات والتنظيم

مثال: (سياسة الحوسبة السحابية أولاً - سياسة تأمين المعلومات الوطنية)

QATAR NATIONAL VISION 2030
NATIONAL DEVELOPMENT STRATEGY 2

"Develop a sustainable and high-quality infrastructure that supports the national economy and is capable of keeping abreast of the latest smart technologies"

CRA Strategy 2020-2024

Cloud Policy Framework

Public and Private Stakeholders' objectives in the cloud value chain

e.g. data classification

Principles of Trust, Security, Transparency

e.g. SME handbook

Policy and Regulatory Recommendations

e.g. Cloud First Policy, NCSA security requirements, National Information Assurance Policy

3. The Objective Of The Cloud Policy Framework

A solid cloud industry will enable Qatar to:

- Attract investments, both foreign and domestic, in new digital services.
- Support the growth of the national economy.
- Enable the transition to a fully digitalized nation.
- Help meet the objective of Qatar becoming a digital hub.
- Manage carbon footprint by reducing scattered traditional on-premises data centers and promoting carbon neutral facilities.

In line with these objectives and with its Strategy 2020 - 2024, the CRA has identified, in the Cloud Policy Framework, a comprehensive set of legal and regulatory requirements that competent government agencies should adopt or update. Similarly, the Cloud Policy Framework highlights recommendations for stakeholders of the cloud value chain to ensure compliance with national and international laws and best practices.

3. الغرض من إطار عمل سياسة الحوسبة السحابية

إن تطوير صناعة سحابية ذات أساس متين سيمكن دولة قطر من:

- جذب الاستثمارات الأجنبية والمحلية في الخدمات الرقمية الجديدة.
- دعم نمو الاقتصاد الوطني.
- التحول الرقمي الكامل بالدولة.
- المساعدة في تحقيق هدف قطر لتصبح مركزاً رقمياً عالمياً.
- الحد من الأثر الكربوني عن طريق الحد من مراكز البيانات التقليدية وتعزيز المرافق المحايدة للكربون.

وقد حددت هيئة تنظيم الاتصالات في إطار عمل سياسة الحوسبة السحابية، مجموعة شاملة من الشروط القانونية والتنظيمية التي يجب على الهيئات الحكومية المعنية أن تلتزم بها أو تستوفيها، وذلك تمشياً مع أهداف استراتيجية الهيئة 2020 - 2024. كما تسلط سياسة الحوسبة السحابية الضوء على التوصيات الموجهة لأصحاب المصلحة في سلسلة القيمة السحابية لضمان الامتثال للقوانين الوطنية والدولية وأفضل الممارسات.

In the implementation of the Cloud Policy Framework, a key role will be played by competent government entities within their respective mandates. For instance, the Ministry of Communications and Information Technology (MCIT) has developed a "Cloud First Policy" as a clear commitment to procurement policies that support cloud solutions and NCSA has defined security requirements.

وفي تنفيذ سياسة الحوسبة السحابية، ستلعب الهيئات الحكومية المعنيّة – كل في إطار اختصاصها – دوراً رئيسياً في تنفيذ سياسة الحوسبة السحابية، فعلى سبيل المثال قامت وزارة الاتصالات وتكنولوجيا المعلومات بوضع "سياسة الحوسبة السحابية أولاً" كالتزام واضح لسياسات الشراء التي تدعم الحلول السحابية، كما قام الفريق القطري للاستجابة لطوارئ الحاسب "كيوسرت" بتحديد المتطلبات الأمنية.

4. Policy Recommendations for The Development of Cloud Computing

4. التوصيات السياسية لتطوير الحوسبة السحابية

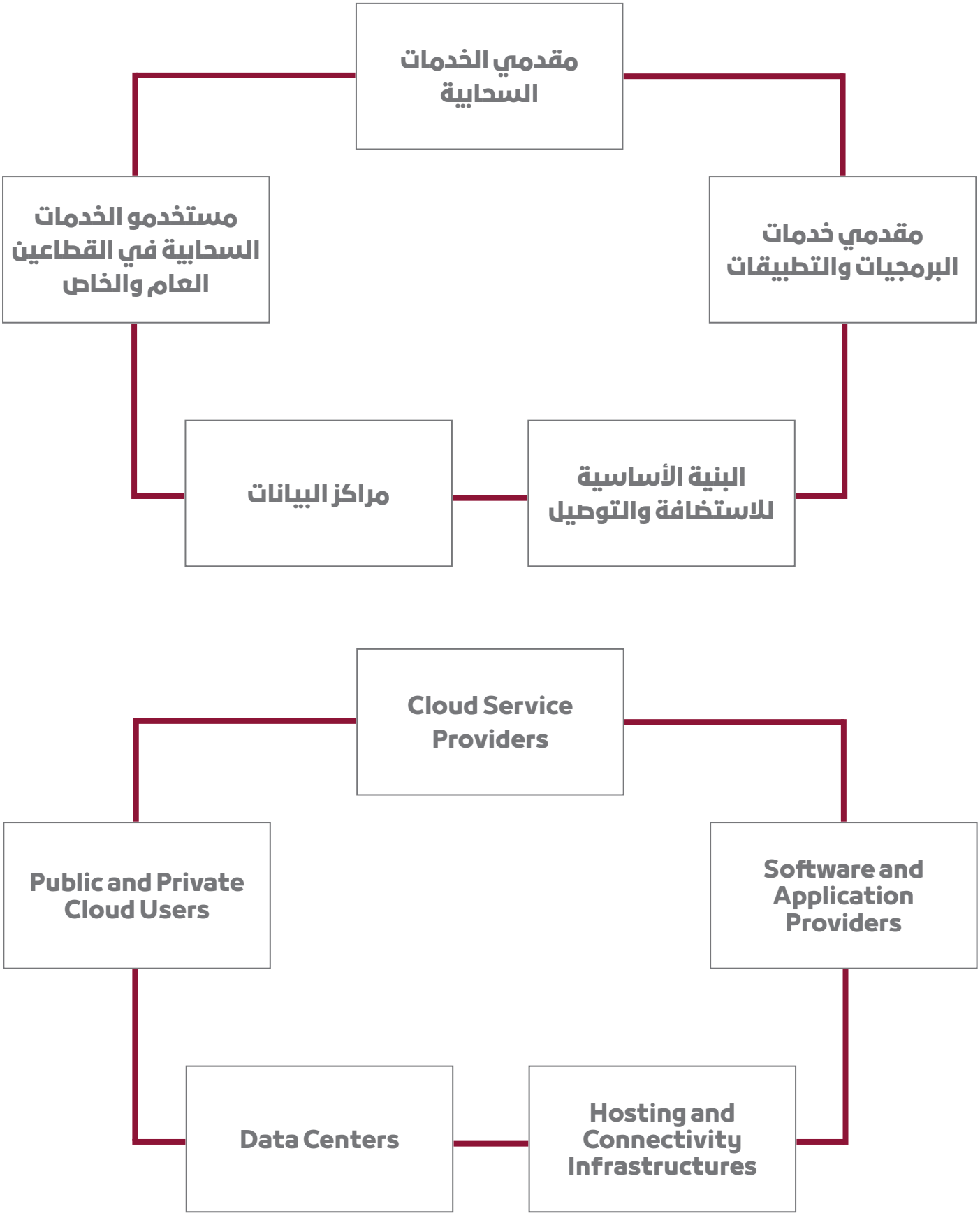
Qatar intends to promote the development of cloud computing services based on open technologies and secured platforms.

تعتزم قطر الارتقاء بتطوير خدمات الحوسبة السحابية انطلاقاً من التقنيات المفتوحة والمنصات الآمنة.

Establishing a clear and transparent framework for adoption of cloud services will ensure that this technology provides trusted access for both national and international users and make Qatar a regional hub of cloud services innovation. Indeed, a successful cloud industry largely depends on the highest possible degree of trust amongst all stakeholders of the value chain.

وسيعمل إنشاء إطار عمل واضح وشفاف لتبنّي الخدمات السحابية على ضمان توفير هذه التكنولوجيا الوصول الموثوق لكل من المستخدمين المحليين والدوليين على حد سواء، وسيجعل من قطر مركزاً إقليمياً لتطوير الخدمات السحابية؛ حيث إن الصناعة السحابية الناجحة تعتمد إلى حد كبير على وجود أعلى درجات الثقة بين جميع أصحاب المصلحة في سلسلة القيمة.

Cloud Value Chain
سلسلة القيمة السحابية



To unleash the potential of the Cloud, public policies have an important role in building trust in cloud computing services as well as in ensuring the highest standards of security and transparency for Cloud Service Providers and cloud users. It is only through widespread trust in secure cloud services and a transparent normative environment that a successful cloud industry will flourish in Qatar.

تلعب السياسات العامة دوراً هاماً في بناء الثقة في خدمات الحوسبة السحابية وكذلك في ضمان أعلى معايير الأمن والشفافية لمقدمي ومستخدمي الخدمات السحابية بُغية تحرير إمكانات الحوسبة السحابية، حيث لا سبيل إلى نجاح وازدهار صناعة الحوسبة السحابية في قطر إلا من خلال الثقة الكبيرة في الخدمات السحابية الآمنة والبيئة التنظيمية الشفافة.

Joint efforts as well as a concerted approach are required from government entities, to:

- Provide clarity and transparency,
- Support a cloud-friendly environment; and
- Move to "cloud-first".

على الجهات الحكومية في أداء دورها في وضع السياسات بذل الجهود المشتركة والتنسيق فيما يضمن التالي:

- الوضوح والشفافية.
- وجود بيئة صديقة للحوسبة السحابية.
- تبنّي عملية "الحوسبة السحابية" أولاً.

Cloud computing touches on a variety of policy areas. Many of these areas require the highest level of compliance with internationally established or developing legal frameworks, e.g. through accessibility, digital inclusion, standards, network architecture, specifications and certifications.

تتعلق الحوسبة السحابية بمجموعة متنوعة من المجالات السياسية. وتتطلب العديد من هذه المجالات أعلى مستوى من الالتزام بالأطر القانونية الدولية الراسخة أو المستحدثة، على سبيل المثال: من خلال إتاحة إمكانية الوصول والدمج الرقمي ووضع المعايير وبنية الشبكة والمواصفات والشهادات.

The following policy and regulatory recommendations will contribute to a successful cloud industry in Qatar.

علماً أن للسياسات والتوصيات التنظيمية الواردة أدناه أهمية بالغة في المساهمة في صناعة حوسبة سحابية ناجحة في دولة قطر، وذلك على النحو التالي:

4.1 Cloud-First Policy

Security is not any more a primary inhibitor to the adoption of cloud services. Accordingly, the sensitive nature of data shall not prevent storage on the cloud (whether local or abroad).

Cloud computing can significantly improve public sector Information Technology management and efficiency. Therefore, to accelerate the process of digital transformation, MCIT has developed a Cloud-First Policy focused on procurement processes and aimed at reducing deployment time and cost, leveraging the latest technologies across the three layers, i.e. infrastructures, platforms and applications, and outsourcing management and maintenance overhead.

4.1 سياسة الحوسبة السحابية أولاً

جدير بالذكر إنه لم تعد المسائل الأمنية عائقاً أساسيا يحول دون اعتماد وتبني الخدمات السحابية. ومن ثم، فإن الطبيعة الحساسة للبيانات لا تمنع من تخزينها على السحابة (سواء كانت محلية أو خارجية).

يمكن للحوسبة السحابية تحسين إدارة وكفاءة تكنولوجيا المعلومات في القطاع العام؛ لذلك ،و للمضي قدماً في عملية التحول الرقمي عملت وزارة الاتصالات وتكنولوجيا المعلومات على صياغة سياسة الحوسبة السحابية أولاً، والتي تركز على عمليات الشراء وتهدف إلى تقليل وقت التنفيذ وتكاليفه، والاستفادة من أحدث التقنيات على المستويات الثلاث: البنية التحتية والبرامج والتطبيقات، والاستعانة بمصادر خارجية للنفقات العامة في الإدارة وأعمال الصيانة.

Policy Recommendation	التوصيات السياسية
Qatar shall implement a cloud-first policy for public procurement of cloud services by government entities that is consistent with the principles of the Cloud Policy Framework. Cloud solutions shall be assessed before any on-premise solutions and based on a clear data classification policy.	يجب أن تطبق قطر سياسية الحوسبة السحابية أولاً على المشتريات العامة من الخدمات السحابية التي تقوم بها الجهات الحكومية، وذلك بما يتفق مع المبادئ الواردة في إطار عمل سياسة الحوسبة السحابية. على أن يتم تقييم الحلول السحابية أولاً قبل بحث الحلول الأخرى داخل مقر الهيئة استناداً إلى سياسة تصنيف بيانات واضحة

4.2 Data Classification

Data classification is a foundational step in cybersecurity risk management. Regardless of whether data is processed or stored "on premises" or "in the cloud", data classification is a starting point for determining the appropriate level of controls for the confidentiality, integrity, and availability of data based on the risks identified by public and private organizations. It involves identifying the types of data that are being processed and stored in an information system owned or operated by an organization.

Data owners (i.e. those who generate and control content, such as business or public entities) and data processors (i.e. custodians who handle data in order to provision services) should be subject to requirements appropriate for the roles they play. For instance, Cloud ServiceProviders and government customers have responsibilities for different aspects of the cloud system; therefore, both parties must implement a set of practices to sufficiently secure their respective environments. To this extent, control on encryption (at least the mechanism whereby the encryption keys are stored and managed) should lie with the owner of the information for government classified data.

4.2 تصنيف البيانات

يُعد تصنيف البيانات خطوة أساسية في إدارة مخاطر الأمن السيبراني. ويعتبر تصنيف البيانات نقطة انطلاق لتحديد المستوى المناسب من ضوابط سرية البيانات وسلامتها وتوافرها وذلك استنادًا إلى المخاطر التي تحددها المؤسسات العامة والخاصة. ويتضمن تصنيف البيانات تحديد أنواع البيانات التي يجري تجهيزها وتخزينها في نظام معلومات تملكه أو تديره أحد المنظمات.

يجب أن يخضع أصحاب البيانات (أي أولئك الذين يقومون بإنشاء المحتوى والتحكم فيه، مثل الكيانات التجارية أو العامة) ومعالجي البيانات (أي المراقبين الذين يتعاملون مع البيانات من أجل توفير الخدمات) لمتطلبات مناسبة للأدوار التي يضطلعون بها، فعلى سبيل المثال، يتحمل مقدمي الخدمات السحابية وعملاء الجهات الحكومية المسؤوليات ذات الصلة بالجوانب المختلفة من نظام الحوسبة السحابية، لذا، يجب على الطرفين تنفيذ مجموعة من الممارسات لتأمين بيئات كل منهما بصورة كافية. ومن هذا المنطلق، فإنه يجب أن يتحكم مالك المعلومات الخاصة بالبيانات الحكومية المصنفة في التشفير (على الأقل الآلية التي يتم بها تخزين مفاتيح التشفير وإدارتها).

ويجوز لمالكي البيانات تحديد المتطلبات المختلفة لمستويات أمن المعلومات فيما يتعلق بأنواع البيانات المختلفة، استناداً إلى مستوى السرية والسلامة والتوافر.

Different requirements of information security levels may be defined by data owners in relation to different types of data, based on their level of confidentiality, integrity and availability.

الصناعة التي تستخدم البيانات

مثل الدفاع والأمن القومي والصحة والتمويل

فئة المستهلك السحابي

مثل الأشخاص الطبيعيين والأشخاص الاعتباريين في القطاع الخاص والجهات الحكومية

طبيعة البيانات

مثل المعلومات الشخصية أو الملكية

The industry using the data

e.g. defense, national security, health, finance

The category of cloud consumer

e.g. natural persons, private sector legal persons, government entities

The nature of data

e.g. personal or proprietary information

يتعين على المنظمات النظر في المبادئ التالية لتصنيف البيانات:

- تقيَّم البيانات على أساس الحساسية والتأثير على الأعمال التجارية والاقتصاد.
- يجب أن يوازن تصنيف البيانات بصورة فعالة بين كل من أهداف الأمن والكفاءة والاقتصاد وتحديث تكنولوجيا المعلومات.

Organizations should consider the following principles for data classification:

- Data shall be evaluated based on sensitivity, business and economic impact.
- Data classification shall effectively balance security, efficiency, economic and IT modernization goals.

- Data should be classified according to a risk profile for sensitivity and business impact, on a scale from 0 to 4, for safeguarding sensitive or critical data with appropriate levels of protection.

- يجب تصنيف البيانات وفقاً لبيان تقييم المخاطر ذات الصلة بالحساسية والتأثير على الأعمال التجارية بحيث تصنف من خلال استخدام مقياس من صفر إلى 4، وذلك لأغراض حماية البيانات الحساسة أو الهامة بمستويات حماية مناسبة.

المستوى	الفئة	الطبيعة
0	بيانات غير حساسة	يجوز مشاركة تلك البيانات مع الجمهور
1	بيانات داخلية	البيانات المستخدمة داخلياً، والمتاحة لجميع الموظفين
2	بيانات مقيدة	البيانات المتاحة لعدد محدود من الأشخاص أو الوظائف داخل المنظمة أو خارجها
3	بيانات سرية	البيانات المقيدة والتي يجري مشاركتها على أساس "الحاجة إلى المعرفة"
4	بيانات عالية الحساسية والأسرار التجارية	البيانات ذات الصلة بالأسرار التجارية أو الأمن القومي

Level	Category	Nature
0	Non-sensitive data	Data which can be shared with the public
1	Internal data	Data used internally, available to all the staff
2	Restricted data	Data accessible to a limited number of persons/functions in or outside the organization
3	Confidential data	Restricted data which is shared on a "need to know" basis
4	Highly sensitive data/Trade secrets	Data related to trade secrets or related to national security matters

- Data should not be over-classified: over-classification will incur unwarranted expenses by putting into place costly controls that can additionally impact business operations, i.e. broadly classifying large disparate sets of data at the same sensitivity level is counterproductive.

- يجب عدم المبالغة في تصنيف البيانات: فسوف يترتب على الإفراط في التصنيف نفقات غير مبررة وذلك من خلال وضع ضوابط مكلفة يمكن أن تؤثر بصورة إضافية على العمليات التجارية ، أي أن تصنيف مجموعات كبيرة متباينة من البيانات على نفس مستوى الحساسية من شأنه أن يؤدى إلى حدوث نتائج عكسية.

Ultimately, it is the owner of the data who must be responsible for determining the information security level which best matches the classification requirements[12]. Indeed, complex organizations or entities dealing with data should develop their own classification of data.

ويجب في النهاية أن تقع مسؤولية تحديد مستوى أمن المعلومات على مالك البيانات والذي يطابق متطلبات التصنيف[12] بأفضل صورة. ويتعين فعلياً على المنظمات أو الكيانات المعقدة المتعاملة مع البيانات أن تضع تصنيفها الخاص للبيانات.

Policy Recommendation	التوصيات السياسية
When moving to the cloud, organizations shall implement data classification schemes based on their level of confidentiality, integrity and availability of data. For the most sensitive categories of data, it may be appropriate to set up an elevated protection in the form of private cloud.	سوف تقوم المؤسسات عند انتقالها للحوسبة السحابية بتنفيذ مخططات خاصة بتصنيف البيانات تستند على أساس مستوى سريتها وسلامتها وتوافر البيانات. وفي حالة أنواع البيانات الأكثر حساسية، فعندئذ سيكون من المناسب توفير حماية أكبر في مرحلة البيانات الخاصة .

12- يجب أن تشير الكيانات الحكومية إلى سياسة تأمين المعلومات الوطنية (NIAP) وذلك لتصنيف البيانات الحكومية.

12- For the classification of government data, government entities shall refer to the National Information Assurance Policy (NIAP).

4.3 Data Localization, Free Flow of Data and Non-Personal Data

Cloud Service Providers store data which is then accessible anytime and anywhere. An important factor to guarantee that cloud services take off is by ensuring that the regime governing the localization and the flow of data is uniform, streamlined and applies equally to foreign and domestic Cloud Service Providers.

4.3.1 Data localization

From an operational perspective, it is no longer necessary for data to be stored "on premises" or "locally" and as such it would be counter-productive to impose a requirement to do so, specifically when data is at rest[13]. Instead, from a security standpoint, organizations must, for the most sensitive categories of data, implement measures setting up an elevated protection that are more efficient than localization requirements, such as:

- Encryption[14].
- Anonymization.
- Aggregation and/or storage in pre-defined hubs to the choice of the customer with processing facilities that are highly secured and certified by Cloud Service Providers.

4.3 توطين البيانات والتدفق الحر للبيانات والبيانات غير الشخصية

يتولى مقدمو الخدمات السحابية تخزين البيانات التي يمكن الوصول إليها بعد ذلك في أي وقت وفي أي مكان. ومن أهم العوامل لضمان انطلاق الخدمات السحابية التأكد من تناسق وتبسيط النظام المطبق على التوطين وتدفق البيانات وسريانه على مقدمي الخدمات السحابية الأجانب والمحليين بلا تفرقة.

4.3.1 توطين البيانات

من ناحية التشغيل، فإنه لم يعد من الضروري تخزين البيانات على "جهاز العميل" أو "محلياً"، ومن ثم سيكون فرض اشتراط هذا الصدد غير مُجدي. وخاصة عندما تكون البيانات في حالة ساكنة[13]، فبدلاً من ذلك، ومن الناحية الأمنية، فإنه يتعين على المؤسسات تنفيذ إجراءات لإعداد حماية مرتفعة أكثر كفاءة من متطلبات التوطين، وذلك فيما يتعلق بفئات البيانات الأكثر حساسية، مثل:

- التشفير[14].
- إخفاء الهوية.
- التجميع أو التخزين في مراكز محددة سلفاً باختيار العميل مع مرافق معالجة مؤمنة إلى حد كبير ومعتمدة من مُقدّمي الخدمات السحابية.

13- يشكل تصنيف البيانات (انظر أعلاه) ومعايير الأمان الأدوات الأساسية لأمان البيانات.

14- قد يتم تأمين عملية التشفير في العديد من المراحل، ويشمل ذلك آليات التشفير التي توفر مفاتيح تخضع مباشرة لسيطرة مالك البيانات.

13- Data Classification (see above) and security standards constitute the primary tools for the security of data.

14- Encryption may be secured at many layers, including through encryption mechanisms that provide keys under the direct control of the data owner.

- Security certification guaranteed by third-party audits that demonstrate robust security controls to address unauthorized third-party access to data, systems and assets[15].

With such measures cloud solutions are more secure than on-premises solutions, are less vulnerable to cyber-attacks and reduce the total cost of ownership. Moreover, contractual clauses can be agreed between the customer and cloud service providers that ensure security of data and recovery mechanisms in case of accidents or breaches, including requirements for the full control of encryption keys for access to data.

Accordingly, any request for data localization should be very limited in volume and scope and, address only trade secrets or national security requirements for which no alternative exists.

Indeed, the security and data protection capabilities of Cloud Service Providers are robust and secure precisely because of:

- Their reliance on globally distributed infrastructures that ensure availability, resilience and security.
- Their compliance with international standards and recognized procedures.
- Additional security ensured by Private Clouds.

- شهادة في المجال الأمني ممنوحة من جهة خارجية تقوم بإجراء عمليات مراجعة لإثبات وجود ضوابط أمنية قوية، وذلك بغية إحباط أي محاولة من أي جهات خارجية غير مصرح لها للوصول إلى البيانات والأنظمة والأصول[15].

ومع تلك الإجراءات ، تكون الحلول السحابية أكثر أمانًا من الحلول الاعتيادية ، فهي أقل عرضة للهجمات الإلكترونية وتقلل التكلفة الإجمالية للملكية. علاوة على ذلك ، يمكن الاتفاق على البنود التعاقدية بين العملاء ومقدمي الخدمات السحابية التي تضمن أمان البيانات وآليات الاسترداد في حالة الحوادث أو الخروقات ، بما في ذلك متطلبات التحكم الكامل في مفاتيح التشفير للوصول إلى البيانات.

وبناءً على ذلك، فإن أي طلب لتوطين البيانات يجب أن يكون محدوداً جداً من حيث الحجم والنطاق، كما أنه يجب معالجة الأسرار التجارية أوالمسائل المتعلقة بالأمن القومي أو وقت الاستجابة الأقل الذي لا يوجد له بديل.

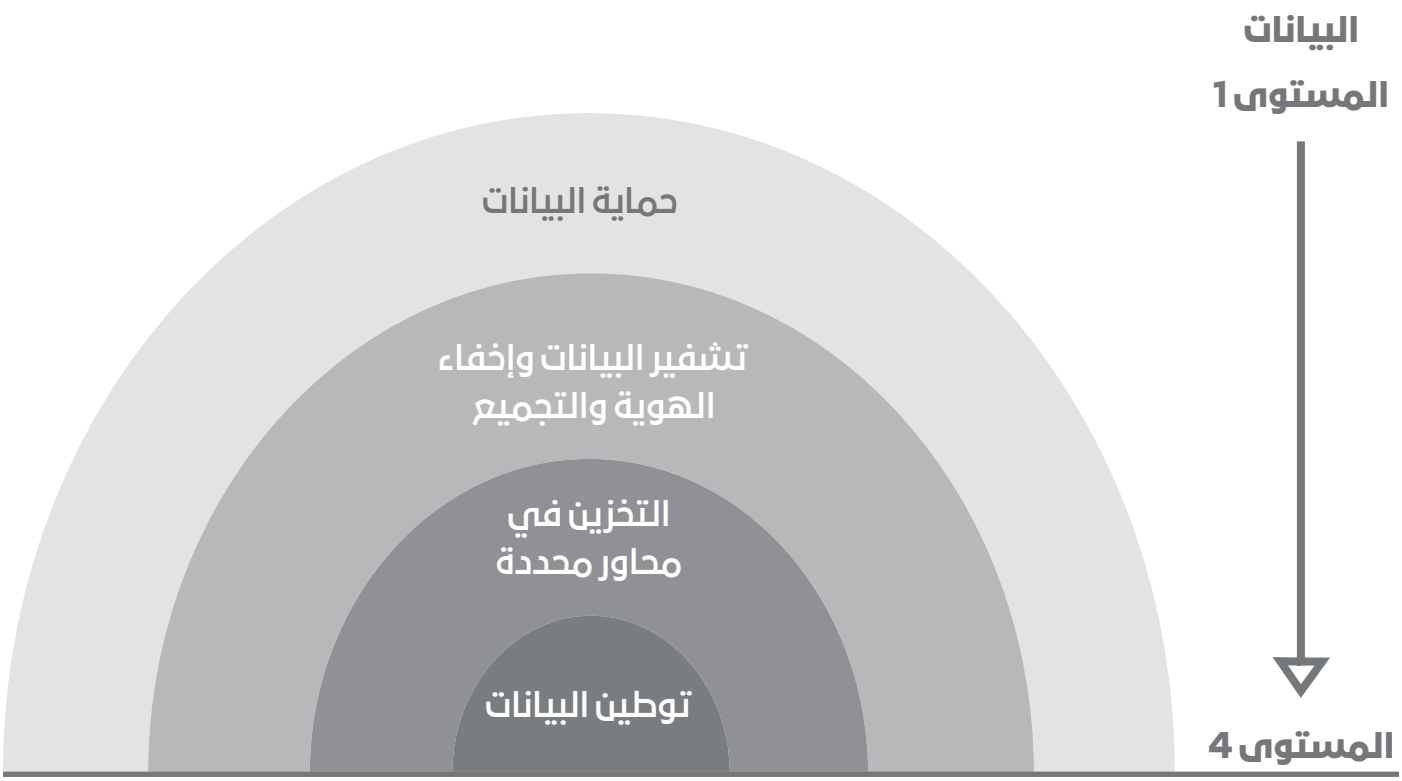
في الواقع، تعد قدرات الأمان وحماية البيانات لمقدمي الخدمات السحابية قوية وآمنة على وجه التحديد بسبب:

- اعتمادها على البنية التحتية الموزعة عالميًا التي تضمن التوافر والمرونة والأمان.
- الامتثال للمعايير والإجراءات الدولية المعترف بها.
- السحابات الخاصة.

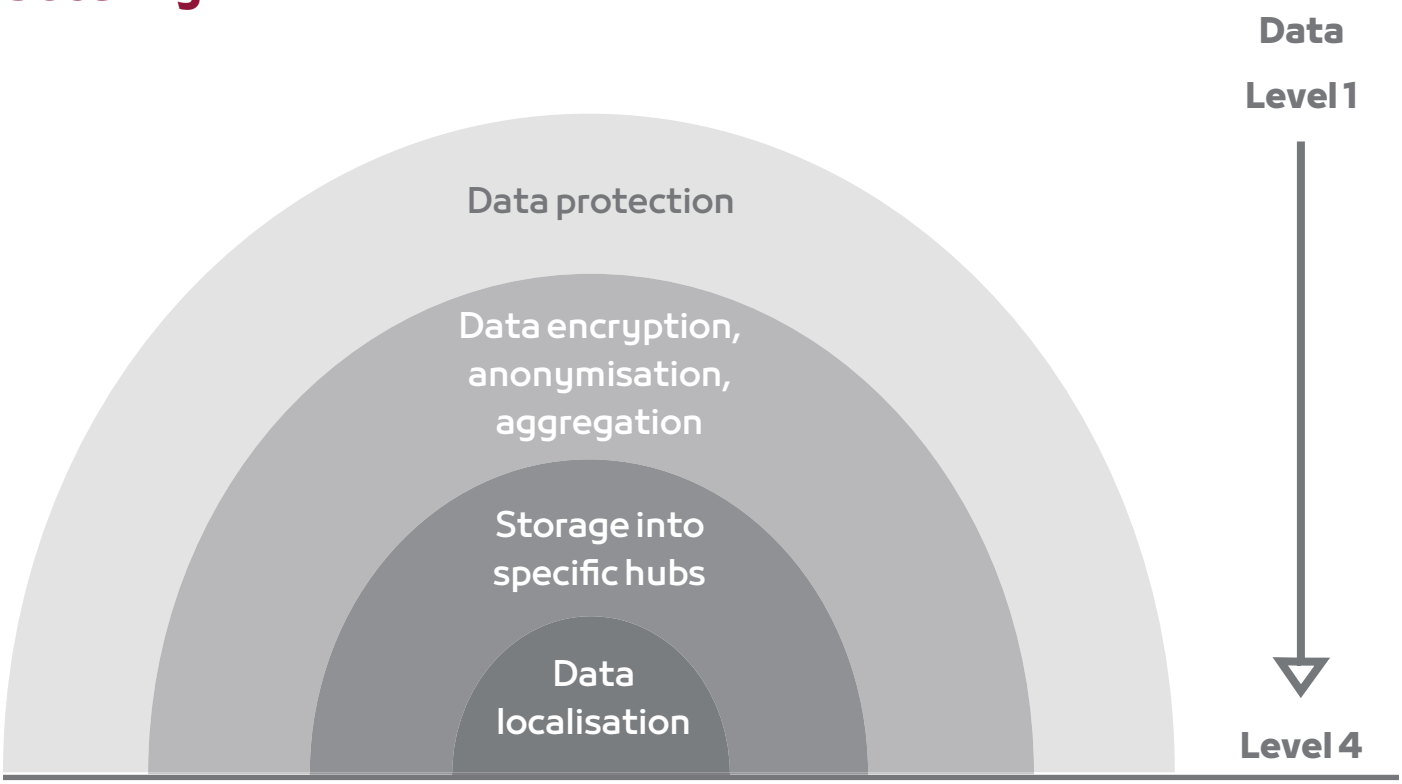
15- الأمن مضمون أيضًا بمتطلبات المعايير الدولية لتصنيف البيانات ، على سبيل المثال ISO 27001

15- Security is also guaranteed by the requirement of internationally standards on classification of data, e.g. ISO 27001

الأمن



Security



4.3.2 Free Flow of Data

Cross-border data flows are inherent to the cloud architecture and should be enabled in a way that protects privacy and security.

Qatar shall provide a wide range of mechanisms to allow data to flow freely whilst ensuring an appropriate level of protection. Accordingly, one or more of the following mechanisms shall be considered as solutions for cross border transfers:

- Contractual arrangements that set out appropriate data privacy and security standards.
- Alignment with international standards and recognized procedures to be implemented by the organizations transferring data (i.e. data processors and Cloud Service Providers).
- Binding corporate rules that set out harmonized and high-level protection and privacy compliance by all national entities of a multinational Cloud Service Provider
- Enforceable corporate cross-border privacy rules modeled on internationally recognized rules such as the APEC Cross-Border Privacy Rules[16].
- Certified codes of conduct, certifications, privacy marks, seals and international standards, such as the ISO standards.

16- https://bit.ly/31nN1zz

4.3.2 التدفق الحر للبيانات

تُعد تدفقات البيانات عبر الحدود أمراً اساسياً في البنية السحابية. ويجب تمكينه بطريقة تحمي الخصوصية والأمن.

على هذا النحو، فإن دولة قطر توفر مجموعة واسعة من الآليات للسماح بتدفق البيانات بحرية مع ضمان مستوى مناسب من الحماية. وبناءً على ذلك، يتم النظر في آلية أو أكثر من الآليات التالية باعتبارها حلول لعمليات النقل عبر الحدود:

- الترتيبات التعاقدية التي تحدد معايير الخصوصية والأمان المناسبة للبيانات.
- أحكام المواءمة والتي تتماشى مع المعايير والإجراءات المعترف بها دولياً بغرض قيام المنظمات التي تنقل البيانات بتنفيذها (أي معالجي البيانات ومقدمي الخدمات السحابية).
- القواعد المُلزمة للشركات التي تحدد الحماية المنسقة عالية المستوى والامتثال للخصوصية من قبل جميع الكيانات الوطنية لمُقدّم الخدمات السحابية المتعددة الجنسيات.
- قواعد الخصوصية القابلة للتنفيذ عبر الحدود للشركات على غرار القواعد المعترف بها عالمياً مثل قواعد الخصوصية عبر الحدود الخاصة بمُنتدى التعاون الاقتصادي لدول آسيا والمحيط الهادئ[16].
- مدونات قواعد السلوك والشهادات وعلامات الخصوصية والأختام والمعايير الدولية المُعتمدة، مثل معايير الأيزو.

16- https://bit.ly/31nN1zz

- Bilateral or multilateral arrangements which rely on self-certification based on a given privacy or security standard, with an enforcement mechanism such as the Trans-Atlantic Data Privacy Framework[17].

Finally, for personal data, it is recommended that the data subject's prior consent be required[18], and controller-processor transfers permitted when the processor offers adequate guarantees to protect the data.

- الترتيبات الثنائية أو المتعددة الأطراف التي تعتمد على الاعتماد الذاتي بناءً على معيار خصوصية أو أمان معينين، مع آلية التنفيذ مثل إطار خصوصية البيانات عبر المحيط الأطلسي[17].

وختاماً، يجب أن تكون الموافقة المُسبقة لموضوع البيانات مطلوبة للبيانات الشخصية[18]، كما أنه يتم السماح بنقل معالج وحدة التحكم عندما يقدم المعالج ضمانات كافية لحماية البيانات.

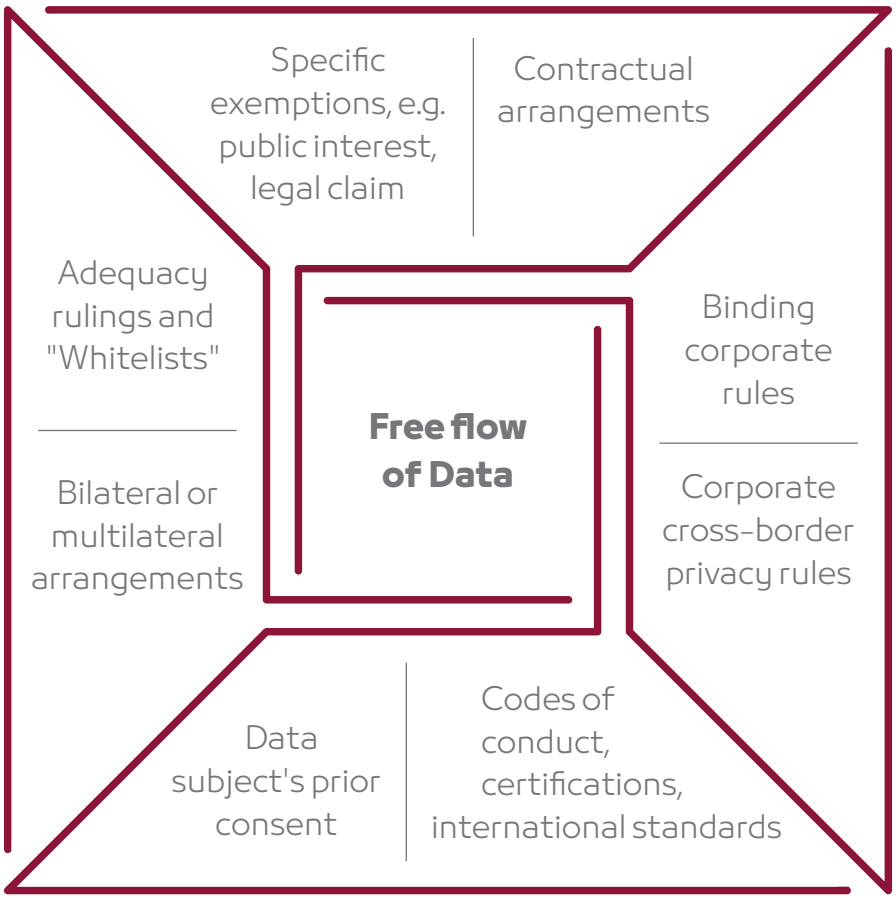
17- سيتم نشره بحلول نهاية 2022 (https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.pdf)، و (https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/).

18- يجب تفسير الموافقة بموجب القانون رقم 13 لسنة 2016 بشأن الخصوصية وحماية البيانات الشخصية، المادة 15

17- To be issued by the end of 2022 (see https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.pdf, and https://www.whitehouse.gov/briefing-room/statements-releases/202225/03//fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/).

18- Consent shall be interpreted as per Law No. 13 of 2016 concerning privacy and protection of personal data, Article 15.


الإعفاءات المحددة، مثل المصلحة العامة والمطالبة القانونية
الترتيبات التعاقدية
أحكام الملاءمة والقوائم البيضاء
قواعد الشركة الملزمة
التدفق الحر للبيانات
الترتيب الثنائي أو متعدد الأطراف
قواعد الخصوصية عبر الحدود للشركات
السلبيات السابقة لموضوع البيانات
مدونة قواعد السلوك والشهادات والمعايير الدولية


Specific exemptions, e.g. public interest, legal claim
Contractual arrangements
Adequacy rulings and "Whitelists"
Binding corporate rules
Free flow of Data
Bilateral or multilateral arrangements
Corporate cross-border privacy rules
Data subject's prior consent
Codes of conduct, certifications, international standards

Administrative processes should be minimized and straightforward in order to ensure a wide adoption, especially by SMEs. Specifically, there should be no requirement that the above categories of cross-border transfers be notified to or approved by the relevant authorities.

يجب التقليل من العمليات الإدارية بشكل واضح لضمان اعتمادها على أوسع نطاق، وخاصة من قبل الشركات الصغيرة والمتوسطة. وعلى وجه التحديد، لا ينبغي أن يكون هناك شرط بإخطار السلطات المعنية بالفئات المذكورة أعلاه من عمليات النقل عبر الحدود أو الموافقة عليها.

4.3.3 Non-Personal Data[19]

The cross-border flows of non-personal data is set to take off with the rapid development of Artificial Intelligence[20], the Internet of Things and machine learning.

4.3.3 البيانات غير الشخصية[19]

من المقرر أن تنطلق تدفقات البيانات غير الشخصية عبر الحدود مع التطور السريع للذكاء الاصطناعي[20] وإنترنت الأشياء والتعلم الآلي.

Qatar should enter into agreements with trusted foreign countries to facilitate the cross-border of non-personal data when these foreign countries are subject to adequate data protection and cybersecurity standards.

يجب على دولة قطر إبرام اتفاقيات مع دول أجنبية موثوق بها لتسهيل عبور البيانات غير الشخصية عبر الحدود في حال كانت هذه الدول الأجنبية خاضعة لمعايير كافية لحماية البيانات والأمن السيبراني.

Policy Recommendation	التوصيات السياسية
Data residency shall not be any longer a requirement as data classification schemes, security and encryption technologies now secure a high level of protection controls. Data localization may be required for highly sensitive data only. When the location of certain data needs to be identified, the localization requirement shall be limited in scope and volume according to the specific nature of the data. Private cloud solutions shall be chosen to guarantee security and data protection.	لم يعد إقامة البيانات شرطاً مطلوباً حيث توفر أنظمة تصنيف البيانات وتقنيات الأمان والتشفير الآن مستوى عالٍ من ضوابط الحماية. قد يكون أمر توطين البيانات مطلوباً للبيانات شديدة الحساسية فقط. في حالة الحاجة إلى تحديد موقع بيانات معينة، يجب أن تقتصر متطلبات التوطين على بيانات محدودة في النطاق والحجم وفقًا للطبيعة المحددة للبيانات.، كما يجب اختيار الحلول السحابية الخاصة لضمان الأمن وحماية البيانات.

19- تتعلق "البيانات غير الشخصية" بالبيانات التي لا تعتبر "بيانات شخصية" بموجب القانون رقم 13 لعام 2016، المادة 1.

20- تعد قواعد حوكمة البيانات بشأن الوصول إلى البيانات ومشاركتها أحد ركائز "الاستراتيجية الوطنية للذكاء الاصطناعي في دولة قطر" (https://bit.ly/3iaHNNB).

19- "Non-Personal Data" relates to data which are not considered as "Personal Data" as per the Law No. 13 of 2016, Article 1.

20- Data governance rules on access to and sharing of data is a pillar of the "National Artificial Intelligence Strategy for Qatar" (https://bit.ly/3iaHNNB).

4.4 Privacy and Access to Data (Cross-Border Requests)

Customers' trust shall be a Cloud Service Provider's top priority, and Cloud Service Providers must deliver governance-focused, audit-friendly services that are built with global data privacy and protection best practices in mind. Whilst the data protection regulatory framework promotes customer trust in the digital ecosystem, it is important to avoid overly stringent data protection rules that can impede the adoption of cloud computing. This framework aims to strike the right balance, to deliver fairness to cloud providers while maintaining trust and security.

4.4.1 Privacy

In order to strengthen customer trust in digital services, and especially for cloud services, the relevant laws should require that all ICT products and services be developed based on the principles of "privacy by design" and "security by design". Technical guidelines, including incident management[21], should be issued by competent authorities that describe how these requirements can be achieved, in collaboration with the MCIT and NCSA.

4.4.2 Cross-Border Access

Cross-border requests for data shall be made through Mutual Legal Assistance Treaties ("MLATs"), or through bilateral agreements, ensuring appropriate involvement of the

4.4 الخصوصية والوصول إلى البيانات (الطلبات عبر الحدود)

ستكون ثقة العملاء هي الأولوية الأولى لمقدمي الخدمات السحابية، كما يتعين أن يقوم مقدمي الخدمات السحابية بتوفير خدمات ترتكز على حوكمة البيانات والتدقيق فيها بسهولة، إذ يتم إعدادها مع مراعاة خصوصية البيانات العالمية واتباع أفضل الممارسات لحمايتها. وفي حين أن الإطار التنظيمي لحماية البيانات تعزز ثقة العملاء في النظام البيئي الرقمي ، فمن المهم تجنب قواعد حماية البيانات الصارمة التي يمكن أن تعرقل اعتماد الحوسبة السحابية. كما يهدف هذا الإطار إلى تحقيق التوازن الصحيح ، لتحقيق العدالة لموفري الخدمات السحابية مع الحفاظ على الثقة والأمان.

4.4.1 الخصوصية

يجب أن تشترط القوانين ذات الصلة تطوير جميع منتجات وخدمات تكنولوجيا المعلومات والاتصالات بناءً على مبادئ "الخصوصية بالتصميم" و "الأمان بالتصميم"، وذلك بغرض تعزيز ثقة العملاء في الخدمات الرقمية وخاصة الخدمات السحابية، كما يجب إصدار المبادئ التوجيهية التقنية التي تصف كيف يمكن تحقيق هذه المتطلبات، بما في ذلك إدارة الحوادث [21]، بالتعاون مع وزارة الاتصالات وتكنولوجيا المعلومات والفريق القطري للاستجابة لطوارئ الحاسب الآلي.

4.4.2 الوصول إلى عبر الحدود

يجب تقديم الطلبات للبيانات عبر الحدود من خلال "معاهدات المساعدة القانونية المتبادلة" أو من خلال اتفاق ثنائي بشكل يضمن المشاركة المناسبة

21- "معايير الأمان" ، وتحديداً ISO / IEC 27035

21- "Security Standards", specifically ISO/IEC 27035

authorities in the countries where Cloud Service Providers are established.

In that context, Qatar should ensure that MLATs processes are efficient, accessible and transparent[22]. For example, MLATs should include:

- A timetable for cooperation and response, both by government and Cloud Service Provider.
- A simple process to exchange data pertaining to the source and destination of communications to locate rapidly individuals and device.
- A requirement by governments agencies and Cloud Service Providers to establish single points of contacts for access to data.

للسلطات في البلدان التي يتم فيها إعداد مقدمي الخدمات السحابية.

وفي هذا السياق، يجب على قطر التأكد من أن عمليات "معاهدات المساعدة القانونية المتبادلة" تتسم بالكفاءة ويمكن الوصول إليها وشفافة[22]. فيجب، على سبيل المثال، أن تتضمن معاهدات المساعدة القانونية المتبادلة ما يلي:

- جدول زمني للتعاون والاستجابة، من قبل كل من الحكومة ومقدمي الخدمات السحابية.
- عملية بسيطة لتبادل البيانات المتعلقة بمصدر ووجهة الاتصالات لتحديد الأفراد والأجهزة بسرعة.
- وطلب إنشاء نقاط اتصال واحدة للوصول إلى البيانات من قبل الوكالات الحكومية ومقدمي الخدمات السحابية.

22- بعض القضايا الرئيسية التي تعالجها معاهدات المساعدة القانونية المتبادلة أو الاتفاقات الثنائية التي تؤدي وظيفة مماثلة هي:

• قانون السحابة الأمريكي (https://bit.ly/2ZdLXeU) والذي من بين أمور أخرى:

o يمنح مسؤولي إنفاذ القانون الأمريكيين سلطة صريحة لإصدار مذكرات استدعاء أو طلب ضمانات أو أوامر محكمة تفرض على مقدمي الخدمات السحابية الخاضعين للولاية القضائية الأمريكية الحفاظ على البيانات المخزنة في الخارج وإنتاجها؛ و

o يمنح السلطة التنفيذية للحكومة الأمريكية سلطة إبرام "اتفاقيات تنفيذية" ثنائية جديدة مع الحكومات الأجنبية للسماح بالوصول إلى البيانات الإلكترونية وتبادلها عبر الحدود. وفي حالة وجود مثل هذه الاتفاقية، فإنه يجوز للحكومة الأجنبية الاتصال مباشرة بمقدم خدمة أمريكي أو الاتصال بسلطات إنفاذ القانون المحلية الأمريكية مباشرة والطلب من مقدم الخدمة الكشف عن البيانات المخزنة على الأراضي الأمريكية.

• القانون الجنائي الخاص بالمملكة المتحدة (أوامر الإنتاج في الخارج) الذي من بين أمور أخرى:

o يُمكن المحققين في المملكة المتحدة من إجبارهم على الكشف عن البيانات الإلكترونية المخزنة خارج المملكة المتحدة باستخدام بديل لطلب المساعدة القانونية المتبادلة الرسمية؛

o يطلب من الشخص الذي صدر الأمر ضده والذي يجب أن تمنحه المحكمة الملكية لإنتاج أو منح الوصول إلى البيانات الإلكترونية المحددة أو الموصوفة في الأمر، طالما أنها لا تخضع للامتيازات القانونية أو التسجيل الشخصي السري؛

o يُلزم الشخص الذي صدر الأمر ضده بالامتناع عن إخفاء أي من البيانات الإلكترونية المُدرجة في الأمر أو إتلافها أو تغييرها ومن الكشف عن الحقيقة التي صدر الأمر بشأنها دون إذن من المحكمة.

22- Some of the key issues dealt with by MLATs, or bilateral agreements that serve a similar function are:

• The US CLOUD Act (https://bit.ly/2ZdLXeU) which, among other things:

o grants US law enforcement officials explicit authority to issue subpoenas or seek warrants or court orders forcing Cloud Service Providers subject to U.S. jurisdiction to preserve and produce data stored overseas; and

o gives the US government's executive branch the authority to make new, bilateral "executive agreements" with foreign governments to allow for cross-border electronic data access and exchange. Where such an agreement exists, a foreign government may contact a US provider or local US law enforcement directly and request the provider disclose data stored on US territory.

• The UK Crime (Overseas Production Orders) Act which, among other things:

o enables UK investigators to compel the disclosure of electronic data stored outside of the UK using an alternative to a formal MLA request;

o requires the person against whom the order is made and which must be granted by the Crown Court to produce or to give access to the electronic data specified or described in the order, as long as it is not subject to legal privilege or a confidential personal record;

o requires the person against whom the order is made to refrain from hiding, destroying or altering any of the electronic data listed in the order and from disclosing the fact that the order has been made without permission from the court.

يجب أن تلعب وكالات إنفاذ القانون [23] في قطر دوراً فعلياً وأن تشجع على التعاون مع الدول الأخرى بالاستعانة باتفاقيات المساعدة القانونية المتبادلة أو الاتفاقيات التنفيذية الثنائية لضمان التنفيذ الفعال للقوانين التي تحكم الوصول إلى البيانات.

Qatar law enforcement agencies[23] should play an active role and encourage cooperation with other countries using MLATs or bilateral executive agreements to ensure effective implementation of the laws governing access to data.

التوصيات السياسية	Policy Recommendation
تعد الشفافية واليقين بمثابة العوامل الرئيسية لدى أصحاب المصلحة، خاصة فيما يتعلق بالقواعد التي تنظم الوصول إلى بيانات الطلبات عبر الحدود. كما يجب تقديم الطلبات عبر الحدود للحصول على البيانات من خلال "معاهدات المساعدة القانونية المتبادلة" أو الاتفاقيات الثنائية التي تضمن المشاركة المناسبة للسلطات في البلدان التي يتم فيها تخزين البيانات.	Transparency and Certainty are key for stakeholders, both in the implementation of privacy principles and in relation to the rules that regulate access to data in cross-border requests. Cross-border requests for data should be made through Mutual Legal Assistance Treaties ("MLATs") or bilateral agreements ensuring appropriate involvement of the authorities in the countries where the data is stored.

23 - وكالات إنفاذ القانون هي وكالات مكلفة بموجب قوانين دولة قطر في وظائفها المتعلقة بالتحقيق في الجرائم الجنائية.

23-Law enforcement agencies are agencies mandated by the laws of the State of Qatar in their functions of investigating criminal offences.

4.5 Accessibility and Digital Inclusion

The development of large-scale public and private cloud computing services will contribute to the achievement of accessibility and digital inclusion objectives of the country[24]. One of the key objectives of Qatar is to move towards becoming a knowledge-based economy: the availability of advanced cloud computing services will help all members of society benefit from the knowledge, education and culture brought about by Information Technology and Innovation. Similarly, cloud computing can play a fundamental role in helping the country objectives of promoting digital inclusion and building a technology-based community that meets the needs of persons with functional limitations (PFLs), persons with disabilities (PWDs) and the elderly in Qatar[25].

4.5 إمكانية الوصول والشمول الرقمي

سيساهم تطوير خدمات الحوسبة السحابية العامة والخاصة واسعة النطاق في تحقيق أهداف إمكانية الوصول والشمول الرقمي للبلاد [24]. تتمثل إحدى الأهداف الرئيسية لدولة قطر في التقدم نحو أن يصبح الاقتصاد قائماً على المعرفة: سيساعد توافر خدمات الحوسبة السحابية المتقدمة جميع أفراد المجتمع على الاستفادة من المعرفة والتعليم والثقافة كنتيجة لتكنولوجيا المعلومات والابتكار. وبالمثل، يمكن أن تلعب الحوسبة السحابية دوراً أساسياً في ترسيخ الأهداف القطرية المتمثلة في تعزيز الشمول الرقمي وبناء مجتمع قائم على التكنولوجيا يلبي احتياجات الأشخاص ذوي القيود الوظيفية (PFL) والأشخاص ذوي الإعاقة (PWDs) والمسنين في قطر [25].

Policy Recommendation	التوصيات السياسية
Government entities' policies and actions on accessibility and digital inclusion should take into utmost account the use of cloud computing services in meeting their objectives. Strong collaboration between government entities' and Cloud Service Providers is recommended to make cloud services largely available for persons with functional limitations, persons with disabilities and the elderly.	فيما يتعلق بإمكانية الوصول والشمول الرقمي وعند وضع سياسات وإجراءات الجهات الحكومية، يجب الأخذ في الاعتبار استخدام خدمات الحوسبة السحابية في تحقيق الأهداف المتوخاة منها إلى أقصى حد ممكن. ويوصى بالتعاون الوثيق بين الجهات الحكومية ومقدمي الخدمات السحابية لجعل الخدمات السحابية متاحة إلى حد كبير للأشخاص يعانون من قصور وظيفي والأشخاص ذوي الإعاقة والمسنين.

24- See MCIT Digital Inclusion Strategy (https://bit.ly/31pOAgf) aims to ensure that all members of society have the ability to access the technologies and are part of the Information Society.

25- https://bit.ly/2BneZAJ

24- يمكنك الاطلاع على استراتيجية وزارة الاتصالات وتكنولوجيا المعلومات للشمول الرقمي على الموقع الإلكتروني هذا: (https://bit.ly/38fbTuD)، وهي تهدف إلى ضمان أن جميع أفراد المجتمع لديهم القدرة على الوصول إلى التقنيات وأن يشكلوا جزءًا لا يتجزأ من مجتمع المعلومات.

25- https://bit.ly/2Zm72Uq

4.6 Data Interoperability and Data Portability

Interoperability of cloud services is key to the development of a successful cloud industry. Cloud interoperability allows cloud services to interact with other cloud services by exchanging information. Indeed, a major benefit of cloud computing is the flexibility to avoid traditional vendor lock-in.
The lack of interoperability between cloud service products and the absence of standards that facilitates data portability may make it difficult for customers to switch supplier, hence frustrating innovation and decreasing customer's benefits.
In order to encourage Cloud Service Providers to embed data portability into their systems, Cloud Service Providers should guarantee data portability, meaning to provide built-in technical competences for data subjects to move their data to other platforms.

In this context, Qatar needs to support the adoption of internationally recognized industry-led standards, such as ISO/IEC 19941 (Cloud Computing Interoperability and Portability).
In addition, as part of the procurement process:

- Data portability and system interoperability by design should be included in the general assessment as an essential criterion.

4.6 إمكانية التشغيل البيني للبيانات وإمكانية نقل البيانات

تعد قابلية التشغيل البيني للخدمات السحابية عاملاً أساسياً لتطوير صناعة سحابية ناجحة.

تسمح إمكانية التشغيل البيني السحابي للخدمات السحابية بالتفاعل مع الخدمات السحابية الأخرى من خلال تبادل المعلومات. في الواقع، تتمثل إحدى الفوائد الرئيسية للحوسبة السحابية في المرونة لتجنب تقيد البائعين التقليديين بمنتج واحد.

قد يؤدي الافتقار إلى إمكانية التشغيل البيني بين منتجات الخدمات السحابية وغياب المعايير التي تسهل نقل البيانات إلى صعوبة تغيير العملاء للمورد وبالتالي إحباط الابتكار وتقليل فوائد العملاء.

من أجل تشجيع مقدمي الخدمات السحابية على تضمين إمكانية نقل البيانات في أنظمتهم، يجب أن يضمن مقدمو الخدمات السحابية أولاً إمكانية نقل البيانات، مما يعني توفير الكفائة الفنية المضمنة لموضوعات البيانات لنقل بياناتهم إلى منصات أخرى.

في هذا السياق، تحتاج دولة قطر إلى دعم اعتماد المعايير المعترف بها دولياً والتي تقودها الصناعة، مثل الأيزو / اللجنة الكهرو تقنية الدولية 19941 (قابلية التشغيل البيني للحوسبة السحابية وقابلية النقل).

بالإضافة إلى ذلك، كجزء من عملية الشراء:

- ينبغي إدراج قابلية نقل البيانات وإمكانية التشغيل البيني للنظام حسب التصميم في التقييم العام كمعيار أساسي.

- The Cloud Service Provider should make available to the public administration the Application Programming Interface ("API") to allow the administration to ensure the interoperability between its various IT systems.

- يجب أن يوفر مُقدم الخدمة السحابية للإدارة العامة واجهة برمجة التطبيقات للسماح للإدارة بضمان قابلية التشغيل البيني بين أنظمة تكنولوجيا المعلومات المختلفة الخاصة بها.

Policy Recommendation	التوصيات السياسية
The adoption of internationally recognized standards on interoperability of cloud services is required when contracting cloud services and in public procurement contracts. Interoperability of cloud services is a prerequisite to guarantee portability of services for cloud users.	يتعين اعتماد معايير معترف بها دولياً بشأن التشغيل البيني للخدمات السحابية عند التعاقد على الخدمات السحابية وفي عقود المشتريات العامة. كما تُعد إمكانية التشغيل البيني للخدمات السحابية شرطاً أساسياً لضمان إمكانية نقل الخدمات لمستخدمي السحابة.

4.7 Liability Regime

Qatar supports the "culture of legality". Nonetheless it may happen that an end customer uploads so called "illegal content", such as a content protected by copyright or trade secrets, or content that is not appropriate for the public. In this case, in line with international best practices a regulatory regime is needed that clarifies that Cloud Service Providers are not liable for such third-party content stored on the cloud.

In order to benefit from this protection, certain conditions in line with international practices would need to be fulfilled, for example:

4.7 قواعد المسؤولية

تدعم قطر "ثقافة القاعدة الحقوقية". ومع ذلك، قد يحدث أن يقوم العميل النهائي بتحميل ما يسمى "المحتوى غير القانوني" ، مثل المحتوى المحمي بحقوق الطبع والنشر أو الأسرار التجارية أو المحتوى غير اللائق. في هذه الحالة، يتعين توفير اللوائح التنظيمية التي تخلي مسؤولية مقدمي الخدمات السحابية عن محتوى الغير المخزن على السحابة بما يتماشى مع أفضل الممارسات الدولية.

للاستفادة من هذه الحماية، يجب استيفاء شروط معينة تتماشى مع الممارسات الدولية، ومنها على سبيل المثال:

If the Cloud Service Provider does not have actual knowledge of illegal content

the Cloud Service Provider will benefit from an exemption of liability for the illegal content.

إذا لم يكن لدى مقدم الخدمة السحابية معرفة فعلية بالمحتوى غير القانوني

يستفيد مقدم الخدمة السحابية من الإعفاء من المسؤولية عن المحتوى غير القانوني.

If the Cloud Service Provider obtains such knowledge, i.e. is notified of this illegal content

the Cloud Service Provider should act expeditiously to remove or to disable access to the infringing content in order to benefit from the exemption.

إذا حصل مقدم الخدمة السحابية على هذه المعرفة، على سبيل المثال، تم إبلاغه بهذا المحتوى غير القانوني

يجب أن يعمل مقدم الخدمة السحابية لإزالة أو تعطيل الوصول إلى المحتوى المخالف على وجه السرعة من أجل الاستفادة من الإعفاء.

By “infringing content”, this Cloud Policy Framework refers to serious criminal offenses which are obviously contravening to the laws of the State of Qatar, such as terrorism, drug trafficking, human trafficking, child abuse in all its forms, copyright infringement or money laundering.

من خلال "انتهاك المحتوى" ، تشير سياسة الحوسبة السحابية بذلك إلى الجرائم الجنائية الخطيرة التي من الواضح أنها تتعارض مع قوانين دولة قطر ، مثل الإرهاب والاتجار بالمخدرات والاتجار بالبشر وإساءة معاملة الأطفال بجميع أشكاله ، وانتهاك حقوق الطبع والنشر أو غسيل الأموال .

Clear rules on “Notice and Take Down” legal procedures should be established, dealing with:

- How Cloud Service Providers should be notified of illegal content.
- The detailed information to be set out in the notice.
- How fast Cloud Service Providers should act and more specifically giving them reasonable time to respond.
- The level of transparency Cloud Service Providers should provide regarding their take-down procedures.

كما يتعين وضع قواعد واضحة لإجراءات "الإخطار والإزالة" تتناول ما يلي:

- كيفية إبلاغ مقدمي الخدمات السحابية عن المحتوى غير القانوني.
- المعلومات التفصيلية التي يجب تحديدها في الإخطار.
- مدى السرعة التي يجب أن يتصرف بها مُقدمو الخدمات السحابية، وعلى وجه التحديد منحهم وقتاً معقولاً للاستجابة.
- ومستوى الشفافية الذي يلتزم مُقدمو الخدمات السحابية بتوفيره فيما يتعلق بإجراءات الإزالة.

As part of the applicable laws and regulations, Qatar should implement a law clarifying the rules and processes to follow in relation to access to data stored in the Cloud in order to facilitate international cooperation, and by no means impose any general filtering or monitoring obligation on Cloud Service Providers over the information they store, or any general obligation to look for or prevent unlawful activity. Such approach has already been adopted in advanced jurisdictions like the EU and the US.

على دولة قطر، وحسب القوانين واللوائح المعمول بها، تفعيل قانون يوضح القواعد والعمليات الواجب اتباعها فيما يتعلق بالوصول إلى البيانات المخزنة في السحابة من أجل تسهيل التعاون الدولي ، وليس بأن تفرض أي التزام عام على الفلترة أو المراقبة على مقدمي الخدمات السحابية حول المعلومات التي يخزنونها، أو أي التزام عام للبحث عن النشاط غير القانوني أو منعه. وقد تم بالفعل اعتماد هذا النهج في الولايات القضائية المتقدمة مثل الاتحاد الأوروبي والولايات المتحدة.

Finally, Cloud Service Providers should have the ability to limit or exclude their liability, albeit mandatory consumer and data protection rules, e.g. liability for personal injury or death, fraudulent behavior, intentional harm or gross negligence.

أخيراً، يجب أن يكون لدى مقدمي الخدمات السحابية القدرة على الحد من مسؤوليتهم أو استبعادها رغم كونها قواعد إلزامية لحماية المستهلك والبيانات، على سبيل المثال المسؤولية عن الإصابة الشخصية أو الوفاة أو السلوك الاحتيالي أو الأذى المتعمد أو الإهمال الجسيم.

Policy Recommendation	التوصيات السياسية
The State will refrain from imposing intermediary liability on Cloud Service Providers for third party content to encourage user services innovation and promote the widespread availability of cloud services to public and private users. Cloud Service Providers should be able to limit or exclude their liability in compliance with the applicable law.	يتعين على الدولة الامتناع عن فرض المسؤولية الوسيطة على مقدمي الخدمات السحابية لمحتوى الغير؛ لتشجيع الابتكار في خدمات المستخدمين وتعزيز التوافر الواسع للخدمات السحابية للمستخدمين العام منهم والخاص. ويجب أن يكون مقدمو الخدمات السحابية قادرين على الحد من مسؤوليتهم أو استبعادها وفقًا للقانون المعمول به.

4.8 Standards for Cloud Services

4.8 المعايير الخاصة بالخدمات السحابية

Cloud computing uses shared computing environments and relies on the public internet to transmit information and data. It therefore raises concerns about security and personal data protection.

تستخدم الحوسبة السحابية بيئات الحوسبة المشتركة وتعتمد على الإنترنت العام في نقل المعلومات والبيانات. وبالتالي فإنها تثير التساؤلات بشأن الأمن وحماية البيانات الشخصية.

In this context, there is a need to set up an information security framework setting out the security obligations of digital service providers, including Cloud Service Providers.

وفي هذا السياق، هناك حاجة إلى إعداد إطار عمل لأمن المعلومات يحدد الالتزامات الأمنية لمُقدمي الخدمات الرقمية، بما في ذلك مُقدمي الخدمات السحابية.

Under such framework, Cloud Service Providers should take appropriate measures to:

بموجب هذا الإطار، يجب على مقدمي الخدمات السحابية اتخاذ التدابير المناسبة من أجل:

- Ensure a level of security appropriate to the risk posed by the data stored.

- ضمان مستوى من الأمان مناسب للمخاطر التي تشكلها البيانات المخزنة.

- Prevent and reduce the impact of incidents affecting the cloud services and any data stored and/or processed.

منع وتقليل تأثير الحوادث التي تؤثر على الخدمات السحابية وأي بيانات مخزنة أو معالجة أو كليهما.

Such measures should consider:

- The security of the Cloud Service Provider's systems and facilities.
- Incident handling processes and procedures.
- Business continuity management, monitoring, auditing and testing.
- International standards and certifications that best promote security.

يجب أن تأخذ هذه التدابير ما يلي بعين الاعتبار:

- أمان أنظمة ومرافق مُقدّم الخدمة السحابية.
- عمليات وإجراءات التعامل مع الحوادث.
- إدارة استمرارية الأعمال والمراقبة والتدقيق والاختبار.
- المعايير والشهادات الدولية التي تعزز الأمن بشكل أفضل.

International standards may include the following general standards:

- CSA STAR, ISO 22301 (Business continuity management systems).
- ISO/IEC 27001 (Information security management).
- ISO/IEC 27701 (Privacy information management).
- ISO/IEC 27017 (Cloud security).
- ISO/IEC 27018 (Cloud privacy).
- ISO/IEC 27035 (Incident reporting).
- Service Organization Controls Report "SOC" 1 and 2.
- Standards that serve sector-specific security requirements such as the Payment Card Industry Data Security Standard ("PCI DSS") for financial services.

قد تتضمن المعايير الدولية المعايير العامة التالية:

- شهادة CSA STAR، الأيزو 22301 (أنظمة إدارة استمرارية الأعمال).
- الأيزو/ آي إي سي 27001 (إدارة أمن المعلومات).
- الأيزو/ آي إي سي 27701 (إدارة معلومات الخصوصية).
- الأيزو/ آي إي سي 27017 (الأمان السحابي).
- الأيزو/ آي إي سي 27018 (خصوصية السحابة).
- الأيزو/ آي إي سي 27035 (الإبلاغ عن الحوادث).
- تقرير ضوابط مؤسسة الخدمة 1 و 2.
- المعايير التي تخدم متطلبات الأمان الخاصة بقطاع معين مثل معيار أمان بيانات صناعة بطاقات الدفع للخدمات المالية.

Compliance with international standards should be encouraged as it provides a common language to help organizations better comprehend, communicate and manage cybersecurity risks.

يجب تشجيع الامتثال للمعايير الدولية لأنها توفر لغة مشتركة لمساعدة المؤسسات على فهم مخاطر الأمن السيبراني والتواصل معها وإدارتها على نحو أفضل.

In addition, following international standards which are interoperable across borders makes it easier for Cloud Service Providers to trade across borders and for consumers in Qatar to better benchmark the security features of a product, reducing security concerns and, ultimately, boosting cloud adoption.

الإضافة إلى ذلك، فإن اتباع المعايير الدولية القابلة للتشغيل البيني عبر الحدود من شأنه أن يُسهِل على مُقدّمي الخدمات السحابية التجارة عبر الحدود وللمستهلكين في قطر قياس الميزات الأمنية للمنتج بشكل أفضل والحد من المخاوف الأمنية، ومن ثم تعزيز اعتماد السحابة.

As per ISO/IEC 27035, Cloud Service Providers should also be obliged to notify, under a reasonable timeframe, the relevant authorities of any security incident based on several factors, such as:

وفقاً لشهادة الآيزو/ أي ايه سي 27035، يجب أن يكون مقدمو الخدمات السحابية مُلزمين أيضاً بإخطار السلطة المختصة بأي حادث أمني وذلك في إطار زمني معقول، استناداً إلى عدة عوامل، مثل:

- The number of affected users.
- The duration of the incident.
- The affected geographic area.

- عدد المستخدمين المتأثرين.
- مدة الحادث.
- المنطقة الجغرافية المتأثرة.

Organizations should have mitigation and redundancy contingency plans in place for their data and services in order to guarantee service continuity in times of emergency and data recovery in case data is lost (Failover / Failback databases from the recovery region to replicas in the original region and vice-versa in order to minimize impact to tenants in a multitenancy cloud environment, and ensure no data loss and zero off-line period per tenant).

يجب أن يكون لدى المؤسسات خطط طوارئ للتخفيف والدعم الاحتياطي لبياناتها وخدماتها من أجل ضمان استمرارية الخدمة في أوقات الطوارئ واستعادة البيانات في حالة فقدان البيانات (يتمثل الهدف من استخدام قواعد بيانات تجاوز الفشل (Failover) والعودة من الفشل (Failback) المعنية بنقل النسخ الاحتياطية من منصات التخزين الاحتياطي إلى المنصة الرئيسية والعكس بالعكس، في الحد من التأثير على مستأجري الخدمات السحابية في بيئة سحابية تخدم العديد من المستأجرين (Multitenancy)، بالإضافة إلى ضمان عدم فقدان البيانات أو حدوث أعطال تحول دون أن يستفيد كل مستأجر من الخدمات السحابية).

Policy Recommendation	التوصيات السياسية
Cloud Service Providers must at all time have in place the technical and organizational measures necessary for managing security risks and to guarantee the continuity of their services. Compliance should be achieved by adopting internationally recognized security standard certifications. The creation of local standards or duplication of internationally recognized standards should be avoided as it can be detrimental to the development of a solid cloud industry.	يتعين أن يكون متاحاً لدى مقدمي الخدمات السحابية في جميع الأوقات الإجراءات الفنية والتنظيمية اللازمة لإدارة المخاطر الأمنية وذلك لضمان استمرارية خدماتهم. كما يجب تحقيق الامتثال من خلال اعتماد شهادات معايير الأمان المُعترف بها دولياً. ويجب تجنب وضع المعايير المحلية أو ازدواجية المعايير المعترف بها دولياً حيث يمكن أن يكون ذلك ضاراً بتطوير صناعة سحابية متينة.

4.9 Service Level Agreements ("SLAs")

An important element in the provision of cloud services is the use of SLAs to define the scope of usage and provision of cloud resources.

Cloud consumers need SLAs prior to migrating their data to the cloud centers, in order to have certainty about the level of the services that they provide.

In turn, Cloud Service Providers must set SLAs for the terms and conditions of the services they provide to users, the charging framework, provisioning schemes and standards of maintenance.

Cloud stakeholders should adopt standardized terms and conditions for cloud SLAs in line with international standards, modeled on ISO/IEC 19086 (Service Level Agreements).

4.9 اتفاقيات مستوى الخدمة

يُعد استخدام "اتفاقيات مستوى الخدمة" من العناصر المهمة في توفير الخدمات السحابية، وذلك بغية تحديد نطاق استخدام الموارد السحابية وتوفيرها.

يحتاج مستهلكو السحابة إلى "اتفاقيات مستوى الخدمة" قبل تحويل بياناتهم إلى المراكز السحابية من أجل التأكد من مستوى الخدمات التي يقدمونها.

في المقابل، يجب على مقدمي الخدمات السحابية تحديد "اتفاقيات مستوى الخدمة" لشروط وأحكام الخدمات التي يقدمونها للمستخدمين وإطار التكاليف وخطط التوفير ومعايير الصيانة.

يجب أن يتبنى أصحاب المصلحة السحابية أحكاماً وشروطاً موحدة لـ"اتفاقيات مستوى الخدمة" السحابية بما يتماشى مع المعايير الدولية، على غرار الأيزو 19086 (اتفاقيات مستوى الخدمة).

يجب على أصحاب المصلحة الذين يتفاوضون بشأن اتفاقية الخدمة السحابية استخدام إرشادات مُعترف بها دولياً مثل "إرشادات توحيد معايير اتفاقية مستوى الخدمة السحابية الخاصة بالمفوضية الأوروبية"[26] كأداة مفيدة للتفاوض على العقود من أجل معالجة القضايا التجارية والقانونية المعنية بشكل صحيح.

Stakeholders negotiating a cloud service agreement should use internationally recognized guidelines, such as the European Commission Cloud SLA Standardization Guidelines[26], as a useful contract negotiation tool in order to properly address the business and legal issues at stake.

في سياق المشتريات العامة للخدمات السحابية، يجب على الحكومة اتخاذ ما يلي:

- إجراء مراجعة واختيار للشروط والأحكام والتعاريف الخاصة بالعقود السحابية التي قد تستفيد من توحيدها عبر الوكالات مثل (1) الموثوقية أو (2) التوافر أو (3) الإصلاح.
- واعتماد إرشادات تحدد عناصر الحوسبة السحابية الرئيسية التي يجب تضمينها في اتفاقية مستوى الخدمة اعتماداً على الخدمة السحابية ونموذج النشر وحساسية البيانات وطبيعة العميل وقطاع الأعمال.

In the context of public procurement of cloud services, the government should:

- Carry out a review and selection of terms, conditions and definitions specific to cloud contracts that would benefit from being standardized across agencies such as (1) reliability, (2) availability, or (3) fixing.
- Adopt a guidance specifying the key cloud computing elements that need to be included in a SLA, depending on the cloud service and deployment model, the sensitivity of the data, the nature of the customer and its business sector.

التوصيات السياسية والتنظيمية	Policy Recommendation
يجب إنفاذ "اتفاقيات مستوى الخدمة" لضمان استيفاء الشروط المتفق عليها لتقديم الخدمات؛ إذ تحتاج الخدمات السحابية الموثوقة إلى مقدمي الخدمات والمستهلكين للاتفاق على مؤشرات مستويات الخدمة (الأداء والتوافر وإعداد الفواتير) التي يتم تقديمها في المنتج السحابي. كما سيساعد اعتماد الشروط والأحكام لـ"اتفاقيات مستوى الخدمة" السحابية بما يتماشى مع المعايير الدولية على تعزيز ثقة الجمهور في الخدمات السحابية.	SLAs must be in place to ensure agreed terms for services provision. Reliable cloud services need providers and consumers to agree on what service levels parameters (performance, availability, billing) the cloud product is offered. The adoption of terms and conditions for cloud SLAs, in line with international standards, will help reinforce the public's trust in cloud services.

26- https://bit.ly/2NGbckM

4.10 Hosting and Connectivity

High-speed broadband networks, reliable open access and robust infrastructure are critical for expanding and connecting to the cloud. Similarly, "Hosting" and "Connectivity" services are central elements that will determine investors' choices in the development of cloud services in Qatar. Open access, price and Quality of Service for data hosting and network connectivity are critical issues (GCC pricing is 4 to 7-fold higher than the OECD average). Also, international connectivity must be assured along multiples routes.

4.10 الاستضافة والتوصيل

تعد شبكات النطاق العريض عالية السرعة وإمكانية الوصول المفتوح الموثوق والبنية التحتية القوية أمراً بالغ الأهمية للتوسع والاتصال بالسحابة. وبالمثل، تُعد خدمات "الاستضافة" و"التوصيل" من العناصر الأساسية التي ستحدد خيارات المستثمرين في تطوير الخدمات السحابية في دولة قطر. ويعتبر السعر والوصول المفتوح وجودة الخدمة من المسائل الحاسمة لاستضافة البيانات والاتصال بالشبكة (أسعار دول مجلس التعاون الخليجي أعلى من متوسط منظمة التعاون الاقتصادي والتنمية بما يتراوح بين 4 و7 أضعاف). كما يجب ضمان التوصيل الدولي بثلاث طرق مختلفة.

Policy Recommendation	التوصيات السياسية
Prices of international connectivity are a critical element for investors' choice and must be aligned with international benchmarks. International connectivity must be assured along multiple different routes.	تعد أسعار التوصيل الدولي عنصراً أساسياً لاختيار المستثمرين ويجب أن تتماشى مع المعايير الدولية. كما ينبغي ضمان التوصيل الدولي بالطرق المتعددة والمختلفة.

4.11 Environmental Sustainability

In order to avoid environmental impact due to energy and water consumption as well as greenhouse gas emissions data centers should:

- Use low/green energy servers.
- Implement sustainable cooling and heat waste recycling solutions.

4.11 الاستدامة البيئية

من أجل تجنب التأثير البيئي الناتج عن استهلاك الطاقة والمياه وكذلك غازات الاحتباس الحراري، يجب على مراكز البيانات:

- استخدام خوادم طاقة منخفضة/خضراء.
- تنفيذ حلول التبريد المستمر وإعادة تدوير النفاسيات الحرارية.

It is nonetheless important to remember that cloud services themselves constitute valuable tools for improving energy efficiency. Indeed, the use of cloud-based connected smart systems which can use real-time information can drive energy, power and water efficiency gains.

إلا أنه من المهم ملاحظة أن الخدمات السحابية نفسها تشكل أدوات قيمة لتحسين كفاءة الطاقة. والواقع أن استخدام الأنظمة الذكية المتصلة بالسحابة والتي يمكنها استخدام المعلومات في الوقت الفعلي يمكن أن تؤدي إلى مكاسب في الطاقة والكهرباء وكفاءة المياه.

To contribute to these efforts, policy considerations should be explored around promoting transparency about the energy footprint of data centers' operations and providing incentives to encourage the switch by data center operators to sustainable practices and renewable energy.

للمساهمة في هذه الجهود، يجب استكشاف اعتبارات السياسة حول تعزيز الشفافية بشأن انبعاثات الطاقة الخاصة بعمليات مركز البيانات وتوفير الحوافز لتشجيع التحول من قبل مشغلي مركز البيانات إلى الممارسات المستدامة والطاقة المتجددة.

Policy Recommendation	التوصيات السياسية
Cloud Service Providers and government entities must commit to principles of environmental sustainability, including energy efficiency and carbon neutrality.	يتعين على مقدمي الخدمات السحابية والهيئات الحكومية الالتزام بمبادئ الاستدامة البيئية، بما في ذلك كفاءة الطاقة ومحايدة الكربون.

5. Annex I - Definition, Characteristics, Services and Deployment Models of Cloud Computing

5. الملحق الأول - تعريف الحوسبة السحابية وخصائها ونماذج خدمتها ونشرها

1- Definitions

The International Telecommunications Union ("ITU") defines cloud computing as a "paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand where examples of resources include servers, operating systems, networks, software, applications, and storage equipment"[27].

The visual model of cloud computing is further described in paragraphs 2, 3 and 4 below.

1- التعاريف

يُعرّف الاتحاد الدولي للاتصالات الحوسبة السحابية على أنها "نموذج لتمكين الوصول الشبكي إلى مجموعة قابلة للتوسع ومرنة من الموارد المادية أو الافتراضية القابلة للمشاركة مع توفير الخدمة الذاتية والإدارة عند الطلب حيث تتضمن أمثلة الموارد الخوادم وأنظمة التشغيل والشبكات والبرامج والتطبيقات ومعدات التخزين"[27].

ويرد وصف للنموذج المرئي التالي للحوسبة السحابية في الفقرات 2 و3 و4 أدناه.

27- التوصية ITU-TY.3500: "نظرة عامة على تقنية المعلومات - الحوسبة السحابية والمفردات". متاح على: (https://bit.ly/3eGZUZq). لتعريف إعادة الحوسبة السحابية انظر أيضًا ISO / IEC 17788 بند النظرة العامة والمفردات من خلال الدخول على الرابط: (https://bit.ly/3ijAXWf) و ISO / IEC 17789 في الهيكلية المرجعية (https://bit.ly/3dPQKsp).

27-Recommendation ITU-TY.3500: "Information Technology-Cloud Computing-Overview and vocabulary". Available at: (https://bit.ly/3eGZUZq). For a definition re. cloud computing see also ISO/IEC 17788 on overview and vocabulary (https://bit.ly/3ijAXWf) and ISO/IEC 17789 on reference architecture (https://bit.ly/3dPQKsp).

الشكل: (المعهد الوطني للمعايير والتكنولوجيا) نموذج مرئي للحوسبة السحابية

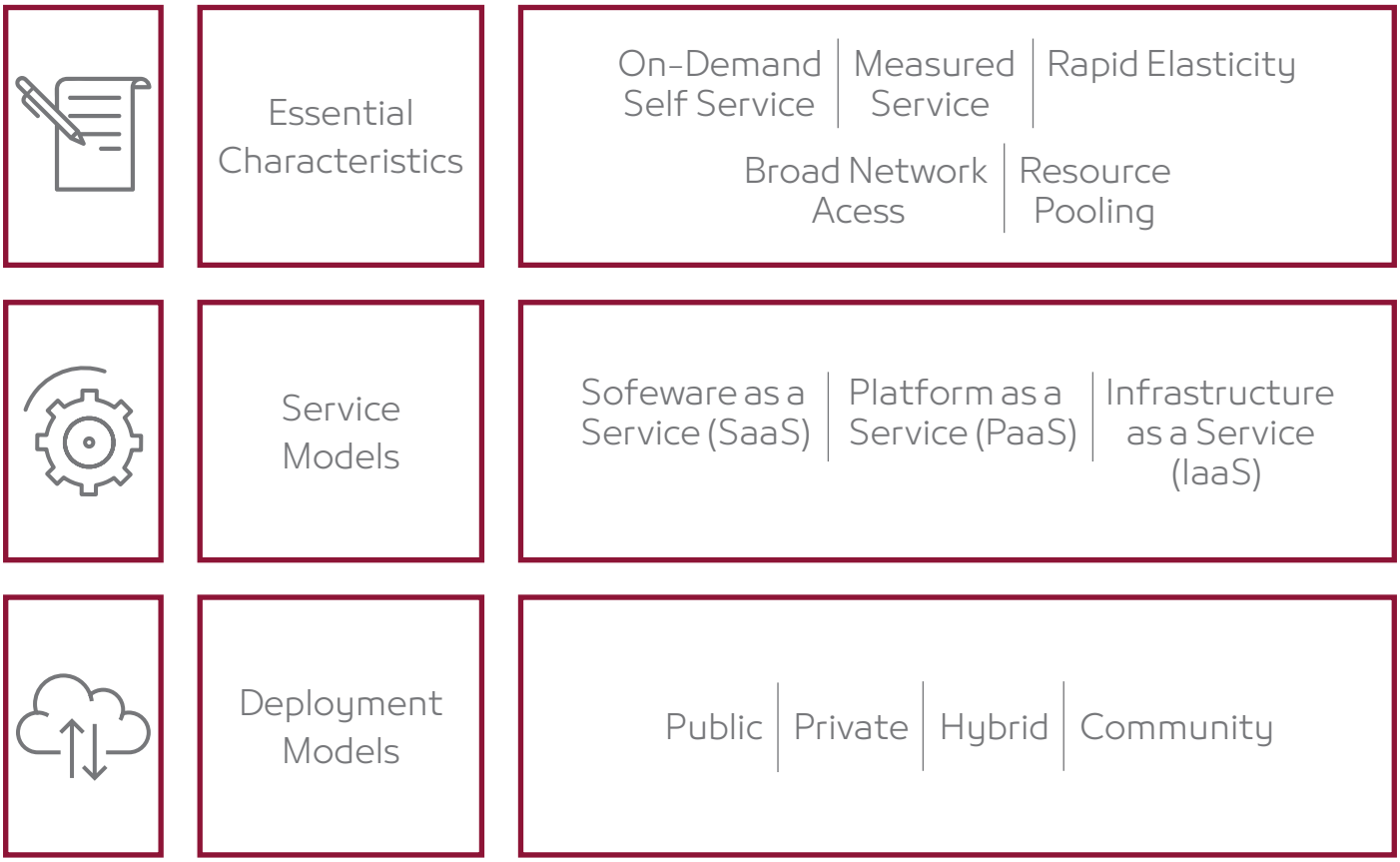


Figure: NIST (National Institute for Standards and Technology) Visual Model of Cloud Computing

2- الخصائص الأساسية

تشمل الخصائص الأساسية للحوسبة السحابية ما يلي[28]:

2- Essential Characteristics

Essential characteristics of cloud computing include[28]:

الخصائص الأساسية	الـوصـف
الخدمة الذاتية عند الطلب	يُمكن لمستخدم الخدمة السحابية توفير إمكانات الحوسبة من جانب واحد مثل وقت الخادم وتخزين الشبكة وخدمات الاتصال والتعاون حسب الحاجة تلقائياً دون الحاجة إلى تفاعل بشري مع مُقدّم الخدمة السحابية لكل خدمة.
الوصول إلى شبكة واسعة	تتوفر الإمكانيات عبر الشبكة ويمكن الوصول إليها من خلال الآليات القياسية التي تعزز الاستخدام بواسطة منصات العميل الرقيقة أو السميكة غير المتجانسة (مثل الهواتف المحمولة وأجهزة الكمبيوتر المحمولة وأجهزة المساعد الرقمي الشخصي).
تجميع الموارد	يتم تجميع موارد الحوسبة لمُقدّم الخدمة السحابية لخدمة العديد من المستخدمين باستخدام نموذج متعدد البرامج مع موارد مادية وظاهرية مختلفة يتم تعيينها وإعادة تعيينها ديناميكياً وفقاً لطلب المستخدم. وهناك شعور باستقلالية الموقع من حيث أن العميل بشكل عام ليس لديه تحكم أو معرفة بالموقع الدقيق للموارد المتاحة، ولكن قد يكون قادراً على تحديد الموقع على مستوى أعلى من التجريد (على سبيل المثال، الدولة، الولاية، مركز البيانات). تتضمن أمثلة الموارد التخزين (عادةً على محركات الأقراص الثابتة أو الضوئية) والمعالجة والذاكرة (عادةً على ذاكرة الوصول العشوائي الديناميكية) وعرض النطاق الترددي للشبكة والأجهزة الافتراضية.
المرونة السريعة	يمكن توفير القدرات بسرعة ومرونة، في بعض الحالات تلقائياً، للتوسع بسرعة، وإطلاقها بسرعة لتوسيع نطاقها بسرعة. وبالنسبة لمستخدم الخدمة السحابية، غالباً ما تبدو الإمكانات المتاحة للتزويد غير محدودة ويمكن شراؤها بأي كمية في أي وقت.
الخدمة المقاسة	تتحكم الأنظمة السحابية تلقائياً في استخدام الموارد مع الاستفادة المُثلى منها (مثل التخزين والمعالجة وعرض النطاق الترددي) وتعمل على تحسينها من خلال الاستفادة من إمكانية القياس عند مستوى ما من التجريد المناسب لنوع الخدمة (على سبيل المثال، عدد حسابات المستخدمين النشطة). ويمكن مراقبة استخدام الموارد والتحكم فيه والإبلاغ عنه مما يوفر الشفافية لكل من مُقدم الخدمة السحابية ومستخدم الخدمة السحابية.

28- تقرير الاتحاد الدولي للاتصالات والفريق المتخصص المعني بالحوسبة السحابية، الجزء الأول: مقدمة عن النظام البيئي السحابي: التعريفات والتصنيفات وحالات الاستخدام والمتطلبات عالية المستوى. متاح على: https://bit.ly/389v74S

28- ITU, Focus Group on Cloud Computing Technical Report, Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements. Available at: https://bit.ly/389v74S

Category	Nature
On-Demand Self Service	A cloud service user can unilaterally provision computing capabilities, such as server time, network storage and communication and collaboration services, as needed automatically without requiring human interaction with each service's Cloud Service Provider.
Broad Network Access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
Resource Pooling	The Cloud Service Provider's computing resources are pooled to serve multiple users using a multi-tenant model, with different physical and virtual resources that are dynamically assigned and reassigned according to user demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify the location at a higher level of abstraction (e.g., country, state, data center). Examples of resources include storage (typically on hard or optical disc drives), processing, memory (typically on DRAM), network bandwidth, and virtual machines.
Rapid Elasticity	Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the cloud service user, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
Measured Service	Cloud systems automatically control and optimize resource use (e.g., storage, processing and bandwidth) by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., the number of active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the Cloud Service Provider and cloud service user of the utilized service.

3- Service Models

Cloud services involve different data activities and cover a broad range of services including software, platforms and infrastructure. Accordingly, cloud computing can be classified by the model of service it offers into one of three different groups:

3- نماذج الخدمة

تتضمن الخدمات السحابية أنشطة بيانات مختلفة، وتغطي مجموعة واسعة من الخدمات، بما في ذلك البرامج والمنصات والبنية التحتية. ووفقاً لذلك، يمكن تصنيف الحوسبة السحابية وفقاً لنموذج الخدمة التي تقدمها إلى واحدة من ثلاث مجموعات مختلفة:

	البرمجيات كخدمة (ساس)	• تتمثل القدرة المقدمة للمستهلك في استخدام تطبيقات مُقدم الخدمة التي تعمل على البنية التحتية السحابية. ويمكن الوصول إلى التطبيقات من أجهزة العميل المختلفة من خلال واجهة عميل رقيقة مثل متصفح الويب (مثل البريد الإلكتروني على الويب) أو واجهة البرنامج. • لا يدير المستهلك أو يتحكم في البنية التحتية السحابية الأساسية بما في ذلك الشبكة أو الخوادم أو أنظمة التشغيل أو التخزين أو حتى إمكانات التطبيق الفردية مع استثناء محتمل لإعدادات تكوين التطبيق المحدودة الخاصة بالمستخدم.
	المنصة الخدمية	• تتمثل القدرة المقدمة للمستهلك في النشر على التطبيقات السحابية التي تم إنشاؤها باستخدام لغات البرمجة والمكتبات والخدمات والأدوات التي يدعمها مُقدم الخدمة. • لا يدير المستهلك أو يتحكم في البنية التحتية السحابية الأساسية، بما في ذلك الشبكة أو الخوادم أو أنظمة التشغيل أو التخزين، ولكنه يتحكم في التطبيقات المنشورة وربما إعدادات بيئة استضافة التطبيقات.
	البنية التحتية كخدمة	• تتمثل القدرة المقدمة للمستهلك في توفير المعالجة والتخزين والشبكات وموارد الحوسبة الأساسية الأخرى حيث يكون المستهلك قادراً على نشر البرامج المتعادلة وتشغيلها، والتي يمكن أن تشمل أنظمة التشغيل والتطبيقات. • لا يدير المستهلك أو يتحكم في البنية التحتية السحابية الأساسية ولكنه يتحكم في أنظمة التشغيل والتخزين والتطبيقات المنشورة وربما له سيطرة محدودة على مكونات الشبكة المُحددة.

	Software as a Service (SAAS)	• The capability provided to the consumer is to use the provider's applications runing on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g. web-based email), or a program interface. • The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
	Platform as a Service (PAAS)	• The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. • The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application-hosting environment configurations.
	Infrastructure as a Service (IAAS)	• The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. • The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of selected networking components.

4- Deployment Models

Cloud service can be deployed within an organization or across multiple organizations. Three main deployment models are widely referred to as private clouds, public clouds and hybrid clouds[29].

4- نماذج النشر

يمكن نشر الخدمة السحابية داخل مؤسسة أو عبر مؤسسات متعددة. ويشار إلى النماذج الثلاثة الرئيسية الخاصة بالنشر على نطاق واسع بالسحابة الخاصة والسحابة العامة والسحابة الهجينة[29].

نموذج النشر	الـوصـف
الساحبة الخاصة 	تتكون السحابة الخاصة من موارد الحوسبة المستخدمة حصرياً من قبل شركة أو مؤسسة واحدة. ويمكن أن تكون السحابة الخاصة موجودة فعليًا في مركز البيانات في مؤسستك أو يمكن استضافتها من قبل مُقدّم خدمة تابع لجهة خارجية. ولكن في السحابة الخاصة، يتم الحفاظ على الخدمات والبنية التحتية دائماً على شبكة خاصة والأجهزة والبرامج مخصصة لمؤسستك فقط. وبهذه الطريقة، يمكن أن تجعل السحابة الخاصة من السهل على المؤسسة تخصيص مواردها لتلبية متطلبات تكنولوجيا المعلومات المحددة. وغالباً ما يتم استخدام السحابة الخاصة من جانب الوكالات الحكومية والمؤسسات المالية والمؤسسات الأخرى متوسطة إلى كبيرة الحجم ذات العمليات بالغة الأهمية في مجال الأعمال التجارية والتي يتمثل الهدف منها في تعزيز السيطرة على بيئتها.
السحابة العامة 	تُعتبر السحابة العامة هي الطريقة الأكثر شيوعاً لنشر الحوسبة السحابية؛ حيث إن الموارد السحابية (مثل الخوادم ووحدات التخزين) مملوكة لمُقدم خدمة سحابية تابع لجهة خارجية ويتم تشغيلها بواسطته وتسليمها عبر الإنترنت. ويُعد كل من "مايكروسوفت أزور" و خدمات أمازون ويب (AWS) و منصة جوجل السحابية (GCP) خير مثال على السحابة العامة. فباستخدام السحابة العامة، يمتلك مُقدم السحابة ويدير جميع الأجهزة والبرامج والبنية التحتية الداعمة الأخرى. وفي السحابة العامة، فإنك تشارك نفس الأجهزة ووحدات التخزين وأجهزة الشبكة مع المؤسسات الأخرى أو "مستأجري" السحابة. كما يمكنك الوصول إلى الخدمات وإدارة حسابك باستخدام متصفح الويب. يلجأ المستخدمون من القطاع الخاص وكذلك الهيئات الحكومية والمؤسسات المالية والمؤسسات متوسطة إلى كبيرة الحجم إلى استخدام عمليات النشر السحابية العامة بشكل متكرر للاستفادة من المجموعة الشاملة أو عروض المنصة الخدمية (باس) والبرمجيات كخدمة (ساس) والبنية التحتية كخدمة التي يوفرها مشغلو السحابة العامة.
السحابية الهجينة 	تجمع السحابة الهجينة بين البنية التحتية على جهاز العميل أو السحابة الخاصة مع السحابة العامة حتى تتمكن المؤسسات من جني مزايا الاثنين. في السحابة الهجينة، حيث يمكن للبيانات والتطبيقات الانتقال بين السحابة الخاصة والعامة لمزيد من المرونة والمزيد من خيارات النشر. فعلى سبيل المثال، يُمكنك استخدام السحابة العامة لتلبية احتياجات الحوسبة كبيرة الحجم ذات النطاق الواسع مثل مهام الحوسبة المكثفة والسحابة الخاصة (أو غيرها من البنية التحتية على جهاز العميل) لإدارة التخزين الأرشيفي لسجلات المؤسسة طويلة الأجل. وفي السحابة الهجينة، يعد "انتقال السحابة" أحد الخيارات. ويحدث هذا عندما يتم تشغيل تطبيق أو مورد في السحابة الخاصة حتى يكون هناك ارتفاع كبير في الطلب (مثل حدث موسمي كالتسوق عبر الإنترنت أو تقديم الإقرارات الضريبية)، وعندها يمكن للمؤسسة "الانتقال" إلى السحابة العامة للاستفادة من المزيد من موارد الحوسبة.

29- يرد وصف لنماذج النشر هذه على: https://bit.ly/31slYD2

29- Such deployments models are described at: https://bit.ly/31slYD2

Deployment Model	Description
Private Cloud 	A private cloud consists of computing resources used exclusively by one business or organization. The private cloud can be physically located at your organization's on-site datacenter, or it can be hosted by a third-party service provider. But in a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organization. In this way, a private cloud can make it easier for an organization to customize its resources to meet specific IT requirements. Private clouds are often used by government agencies, financial institutions, any other mid- to large-size organizations with business-critical operations seeking enhanced control over their environment.
Pulic Cloud 	Public clouds are the most common way of deploying cloud computing. The cloud resources (like servers and storage) are owned and operated by a third- party Cloud Service Provider and delivered over the Internet. Microsoft Azure, AWS and GCP is an example of a public cloud. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider. In a public cloud, you share the same hardware, storage, and network devices with other organizations or cloud "tenants". You access services and manage your account using a web browser. Public cloud deployments are frequently used by private users as well as government agencies, financial institutions and mid-large size organizations to use the wide array or PaaS, SaaS and IaaS offerings made available by public cloud operators.
Hybrid Cloud 	Hybrid clouds combine on-premises infrastructure, or private clouds, with public clouds so organizations can reap the advantages of both. In a hybrid cloud, data and applications can move between private and public clouds for greater flexibility and more deployment options. For instance, the public cloud can be used for high volume, large scale computing needs such as intensive compute jobs and the private cloud (or other on-premises infrastructure) for managing archival storage of long-term corporate records. In a hybrid cloud, "cloud bursting" is also an option. This is when an application or resource runs in the private cloud until there is a spike in demand (such as seasonal event like online shopping or tax filing), at which point the organization can "burst through" to the public cloud to tap into additional computing resource.

6. Annex II - Table on Policy Recommendations and Regulatory Requirements

6. الملحق الثاني - جدول التوصيات السياسية والمتطلبات التنظيمية

مجالات السياسة	التوصيات السياسية	الصكوك ذات الصلة	الجدول الزمني للاعتماد/ التحديث
سياسة السحابة أولاً	ستطبق قطر سياسة السحابة أولاً للمشتريات العامة للخدمات السحابية الجهات الحكومية المتوافقة معها مبادئ إطار عمل السياسة السحابية. يجب تقييم الحلول السحابية قبل أي حلول اخرى محلية، وعلى أساس سياسة تصنيف بيانات واضحة.	سياسة السحابة أولاً قانون المشتريات	
تصنيف البيانات	عند الانتقال إلى السحابة، يتعين على المؤسسات أن تلتزم بتنفيذ خطط تصنيف البيانات، وفقاً لمستوى السرية والنزاهة والتوافر، و فيما يتعلق بفئات البيانات الأكثر حساسية أو في حال تطلب الأمر وقت الاستجابة المنخفض يتعين إعداد حماية مرتفعة في شكل توطين البيانات.	سياسة السحابة أولاً / قانون الأمن السيبراني وسياسة تصنيف البيانات الحكومية	
توطين البيانات، التدفق الحر للبيانات، البيانات غير الشخصية	في حالة الحاجة إلى تحديد موقع بيانات معينة، يجب ان تقتصر متطلبات التوطين على حجم محدود جدًا من البيانات إما شديدة الحساسية أو في حال تطلب الأمر وقت استجابة منخفض.	سياسة السحابة أولاً / قانون الأمن السيبراني، وقانون الخصوصية، والاتفاقيات الدولية، وسياسة أمن السحابة الخاصة بالوكالة الوطنية للأمن السيبراني ، البنود التعاقدية القياسية، القواعد المُلزمة للشركات	
الخصوصية والوصول إلى البيانات، والطلبات عبر الحدود	تعد الشفافية واليقين من العناصر الأساسية لدى أصحاب المصلحة، سواء في تنفيذ مبادئ الخصوصية أو فيما يتعلق بالقواعد التي تنظم الوصول إلى بيانات الطلبات عبر الحدود. كما يجب تقديم الطلبات عبر الحدود للحصول على البيانات من خلال "معاهدات المساعدة القانونية المتبادلة" أو الاتفاقيات الثنائية التي تضمن المشاركة المناسبة للسلطات في البلدان التي يتم فيها تخزين البيانات	قانون حماية البيانات، قانون البيانات الموثوق بها، الاتفاقيات المتعددة الأطراف، اتفاقيات المساعدة القانونية المتبادلة، البنود التعاقدية القياسية	

مجالات السياسة	التوصيات السياسية	الصكوك ذات الصلة	الجدول الزمني للاعتماد/ التحديث
إمكانية الوصول والشمول الرقمي	فيما يتعلق بإمكانية الوصول والشمول الرقمي وعند وضع سياسات وإجراءات الجهات الحكومية، يجب الأخذ في الاعتبار استخدام خدمات الحوسبة السحابية في تحقيق الأهداف المتوخاة منها إلى أقصى حد ممكن. ويوصى بالتعاون الوثيق بين الجهات الحكومية ومقدمي الخدمات السحابية لجعل الخدمات السحابية متاحة إلى حد كبير للأشخاص الذين يعانون من قصور وظيفي والأشخاص ذوي الإعاقة والمسنين.	استراتيجية الشمول الرقمي لوزارة الاتصالات وتكنولوجيا المعلومات	
إمكانية التشغيل البيني للبيانات وإمكانية نقل البيانات	يتعين اعتماد معايير معترف بها دولياً بشأن التشغيل البيني للخدمات السحابية عند التعاقد على الخدمات السحابية وفي عقود المشتريات العامة. كما تُعد إمكانية التشغيل البيني للخدمات السحابية شرطاً أساسياً لضمان إمكانية نقل الخدمات لمستخدمي السحابة.	إنفاذ المعايير الدولية والبنود التعاقدية القياسية	
قواعد المسؤولية	يتعين على الدولة الامتناع عن فرض المسؤولية الوسيطة على مقدمي الخدمات السحابية لمحتوى الغير؛ لتشجيع الابتكار في خدمات المستخدمين وتعزيز التوافر الواسع للخدمات السحابية للمستخدمين العام منهم والخاص. ويجب أن يكون مقدمو الخدمات السحابية قادرين على الحد من مسؤوليتهم أو استبعادها وفقاً للقانون المعمول به.	قانون التجارة الإلكترونية وقانون البيانات الموثوقة قانون الملاذ الآمن والبنود التعاقدية القياسية	
معايير الأمن	يتعين أن يكون متاحاً لدى مقدمي الخدمات السحابية في جميع الأوقات الإجراءات الفنية والتنظيمية اللازمة لإدارة المخاطر الأمنية وذلك لضمان استمرارية خدماتهم. كما يجب تحقيق الامتثال من خلال اعتماد شهادات معايير الأمان المُعترف بها دولياً. ويجب تجنب وضع المعايير المحلية أو ازدواجية المعايير المعترف بها دولياً حيث يمكن أن يكون ذلك ضاراً بتطوير صناعة سحابية متينة.	القواعد الدولية للمعايير ومدونات قواعد السلوك والاعتمادات والبنود التعاقدية القياسية	
اتفاقيات مستوى الخدمة	يجب إنفاذ "اتفاقيات مستوى الخدمة" لضمان استيفاء الشروط المتفق عليها لتقديم الخدمات؛ إذ تحتاج الخدمات السحابية الموثوقة إلى مقدمي الخدمات والمستهلكين للاتفاق على مؤشرات مستويات الخدمة (الأداء والتوافر وإعداد الفواتير) التي يتم تقديمها في المنتج السحابي. كما سيساعد اعتماد الشروط والأحكام لـ"اتفاقيات مستوى الخدمة" السحابية بما يتماشى مع المعايير الدولية على تعزيز ثقة الجمهور في الخدمات السحابية.	سياسة السحابة أولاً والبنود التعاقدية القياسية	

مجالات السياسة	التوصيات السياسية	الصكوك ذات الصلة	الجدول الزمني للاعتماد/ التحديث
الاستضافة والتوصيل	تعد أسعار التوصيل الدولي عنصراً أساسياً لاختيار المستثمرين ويجب أن تتماشى مع المعايير الدولية. كما ينبغي ضمان التوصيل الدولي بالطرق المتعددة والمختلفة.	قواعد هيئة تنظيم الاتصالات	
الاستدامة البيئية	يتعين على مقدمي الخدمات السحابية والهيئات الحكومية الالتزام بمبادئ الاستدامة البيئية، بما في ذلك كفاءة الطاقة ومحايدة الكربون.		

Policy Areas	Policy Recommendations	Relevant Instrument	Timeline for Adoption / Update
Cloud-First Policy	Qatar shall implement a cloud-first policy for public procurement of cloud services by government entities that is consistent with the principles of the Cloud Policy Framework. Cloud solutions shall be assessed before any on-premise solutions and based on a clear data classification policy.	Cloud-First Policy, Procurement Law	
Data Classification	When moving to the cloud, organizations shall implement data classification schemes based on their level of confidentiality, integrity and availability of data. For the most sensitive categories of data, it may be appropriate to set up an elevated protection in the form of private cloud.	Cloud-First Policy, Cybersecurity Law, Government Data Classification Policy	
Data Localization, Free Flow of Data, Non-Personal Data	When the location of certain data needs to be identified, the localization requirement shall be limited in scope and volume according to the specific nature of the data. Private cloud solutions shall be chosen to guarantee security and data protection.	Cloud-First Policy, Cybersecurity Law, Privacy Law, International Agreements, NCSA Cloud security policy, Standard Contractual Clauses, Binding Corporate rules.	

Policy Areas	Policy Recommendations	Relevant Instrument	Timeline for Adoption / Update
Privacy and access to data, Cross Borders Requests	Transparency and Certainty are key for stakeholders, both in the implementation of privacy principles and in relation to the rules that regulate access to data in cross-border requests. Cross-border requests for data should be made through Mutual Legal Assistance Treaties ("MLATs") or bilateral agreements ensuring appropriate involvement of the authorities in the countries where the data is stored.	Data Protection Law, Trusted Data Law, Multilateral Agreements, MLATs, Standard Contractual Clauses	
Accessibility and Digital Inclusion	Government entities' policies and actions on Accessibility and Digital Inclusion should take into utmost account the use of cloud computing services in meeting their objectives. Strong collaboration between government entities' and cloud service providers is recommended to make cloud services largely available for persons with functional limitations, persons with disabilities and the elderly.	MCIT Digital Inclusion Strategy	
Data interoperability and data portability	The adoption of internationally recognized standards on interoperability of cloud services is required when contracting cloud services and in public procurement contracts. Interoperability of cloud services is a prerequisite to guarantee portability of services for cloud users.	Standard Contractual Clauses, International Standard enforcement	
Liability regime	The State should refrain from imposing intermediary liability on Cloud Service Providers for third party content to encourage user services innovation and promote the widespread availability of cloud services to public and private users. Cloud Service Providers should be able to limit or exclude their liability in compliance with the applicable law.	E-commerce Law, Safe Harbor Regulation, Trusted Data Law, Standard Contractual Clauses	

Policy Areas	Policy Recommendations	Relevant Instrument	Timeline for Adoption / Update
Security Standards	Cloud Service Providers must at all time have in place the technical and organizational measures necessary for managing security risks, to guarantee the continuity of their services. Compliance should be achieved by adopting internationally recognized security standard certifications. The creation of local standards or duplication of internationally recognized standards should be avoided because it can be detrimental to the development of a solid cloud industry.	International standardization rules, Codes of Conduct, Certifications, Standard Contractual Clauses	
Service Level Agreements (SLAs)	SLAs must be in place to ensure agreed terms for services provision. Reliable cloud services need providers and consumers to agree on what service levels parameters (performance, availability, billing) the cloud product is offered. The adoption of standardized terms and conditions for cloud SLAs in line with international standards will help reinforce the public's trust in cloud services.	Cloud-First Policy, Standard Contractual Clauses	
Hosting and Connectivity	Prices of international connectivity are a critical element for investors' choice and must be aligned with international benchmarks. International connectivity must be assured along multiple different routes.	CRA Ruling	
Environmental sustainability	Cloud service Providers and government entities must commit to principles of environmental sustainability, including energy efficiency and carbon neutrality.		

7. Annex III - The CRA Strategic Objectives

Qatar's government is committed to supporting the development of data centers and cloud infrastructure in Qatar to host its ambitious digitalization plan. Therefore, as part of the ongoing Authority's Strategy 2020 - 2024, the "supply of data centers and cloud capacity" has been identified as a target for the development of the IT sector.

Moreover, one of the key actions of the CRA Strategy 2020 - 2024 is "to develop a strategy on the supply of cloud services and data centers within Qatar. This strategy will be broad-ranging and will look at both supply and demand factors. It will evaluate current and future bottlenecks to the growth of data centers and cloud services, such as investment, innovation, security, regulation, terms of access and coordination with the Government". The objective of the Cloud Strategy is to increase the supply of data center capacity and a better offering of cloud services to government and private sector entities. A competitive market for the supply of cloud services and data center capacity is essential for a modern IT industry to develop. There are significant players already established in this market in Qatar (e.g., Ooredoo, Vodafone and Meeza).

7. الملحق الثالث - الأهداف الاستراتيجية لهيئة تنظيم الاتصالات

تلتزم حكومة دولة قطر بدعم تطوير مراكز البيانات والبنية التحتية السحابية في دولة قطر لاستضافة خطتها الرقمية الطموحة. ومن ثم، تم تحديد "توفير مراكز البيانات والقدرة السحابية" كهدف لتطوير قطاع تكنولوجيا المعلومات، وذلك ضمن استراتيجية الهيئة القائمة 2020-2024

بالإضافة إلى ذلك، تتمثل إحدى الإجراءات الرئيسية لاستراتيجية هيئة تنظيم الاتصالات 2020 – 2024 في "وضع استراتيجية لتوفير الخدمات السحابية ومراكز البيانات داخل دولة قطر، على أن تكون هذه الاستراتيجية واسعة النطاق وتضع في اعتبارها العوامل المتعلقة بالعرض والطلب. كما يجب أن تعمل هذه الاستراتيجية على تقييم المُعوقات الحالية والمستقبلية التي تحول دون نمو مراكز البيانات والخدمات السحابية، مثل الاستثمار والابتكار والأمن والتنظيم وشروط الوصول والتنسيق مع الحكومة". ويتمثل الهدف من هذه الاستراتيجية في زيادة المعروض من سعة مركز البيانات وتقديم أفضل الخدمات السحابية للهيئات الحكومية والقطاع الخاص. ويُعد وجود سوق تنافسي لتوفير الخدمات السحابية وكفاءة مركز البيانات أمراً ضرورياً لتطوير صناعة تكنولوجيا المعلومات الحديثة؛ حيث إنه يوجد بالفعل أطراف هامة فاعلة ورائدة في هذا المجال في السوق القطري (مثل أوريدو وفودافون وميزة).

There are also indications that the price of cloud and data center services in Qatar is high by regional standards. Increasing the supply of data center capacity in Qatar will require a proactive approach by the government to ensure that enough infrastructure is built and that the data center and cloud services market is working effectively.

To meet the needs of the trend towards cloud computing large-scale use, data center capacity in Qatar will need to grow.

كما تجدر الإشارة إلى أنه هناك مؤشرات على أن سعر خدمات السحابة ومراكز البيانات في قطر مرتفع بالمقارنة مع المعايير الإقليمية. لذا، ستتطلب زيادة المعروض من سعة مراكز البيانات في قطر أن تقوم الحكومة باتباع نهج استباقي من أجل ضمان إنشاء بنية تحتية قوية وكافية، بالإضافة إلى عمل مركز البيانات وسوق الخدمات السحابية على نحو يستم بالفاعلية.

وعملاً على تلبية احتياجات الاتجاه نحو استخدام الحوسبة السحابية على نطاق واسع، ستحتاج سعة مركز البيانات في قطر إلى النمو.

cra.gov.qa