

Draft for Public Consultation

مسودة للاستشارة العامة

Cloud Policy Statement

وثيقة سياسة الحوسبة السحابية

Deadline to submit Responses:
April 23, 2020

الموعد النهائي لتقديم الردود:
23 ابريل 2020

Version No: 1
Date: March 12, 2020

مسودة رقم: 1
التاريخ: 12 مارس 2020

Cloud Policy Statement

وثيقة
سياسة الحوسبة
السحابية

Table of Contents		جدول المحتويات	
1 Executive Summary	4	4	1. نبذة :
2 Introduction	5	5	2. المقدمة:
3 The objective of the Cloud Policy Statement	8	8	3. الغرض من وثيقة سياسة الحوسبة السحابية:
4 Policy and regulatory recommendations for the development of cloud computing	9	9	4. التوصيات السياسية والتنظيمية لتطوير الحوسبة السحابية:
4.1 Cloud-First Policy	12	12	4.1 سياسة الحوسبة السحابية أولاً:
4.2 Data localization and free flow of data	12	12	4.1 توطين البيانات والتدفق الحر للبيانات
4.2.1 Data localization	12	12	4.2.1 توطين البيانات
4.2.2 Free flow of data	14	14	4.2.2 التدفق الحر للبيانات
4.2.3 Non-personal data	16	16	4.2.3 البيانات غير الشخصية
4.3 Privacy and access to data	16	16	4.3 الخصوصية والوصول إلى البيانات
4.3.1 Privacy	16	16	4.3.1 الخصوصية
4.3.2 Cross border requests	17	17	4.3.2 الطلبات عبر الحدود
4.4 Data Classification	18	18	4.4 تصنيف البيانات
4.5 Data interoperability and data portability	20	20	4.5 قابلية التشغيل البيئي للبيانات وإمكانية نقلها
4.6 Liability regime	21	21	4.6 قواعد المسؤولية
4.7 Security standards	22	22	4.7 معايير الأمان
4.8 Service Level Agreements	25	25	4.8 اتفاقيات مستوى الخدمة
4.9 Hosting and Connectivity	26	26	4.9 الاستضافة والتوصيل
4.10 Environmental Sustainability	27	27	4.10 الاستدامة البيئية.
Annex I – Definitions, characteristics, service and deployment models of cloud computing	28	28	الملحق الأول - تعريف الحوسبة السحابية وخصائصها ونماذج خدماتها ونشرها
1 Definitions	28	28	1. التعريف
2 Essential characteristics	29	30	2. الخصائص الأساسية
3 Service models	30	30	3. نماذج الخدمة
4 Deployment models	32	32	4. نماذج النشر
Annex II – Table on Policy Recommendations and Regulatory Requirements	34	38	الملحق الثاني - جدول متطلبات التوصيات والقواعد التنظيمية السياسية
Annex III – The CRA Cloud Strategy	40	40	الملحق الثالث - استراتيجية هيئة تنظيم الاتصالات 2020 - 2024
Annex IV – Consultation Questions	42	42	الملحق الرابع
Annex V – Consultation Response Template	43	43	الملحق الخامس

1. Executive Summary

1. نبذة:

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.

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 private and public entities to provide better services and, ultimately, for Qatar to become a fully digitalized country.

The Cloud Policy Statement, developed within the framework of the 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.

Embracing the principles of Trust, Security and Transparency, the Cloud Policy Statement identifies policy and regulatory recommendations that are critical for the development of a sound 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.

Given the pervasive nature of cloud computing, the Cloud Policy Statement calls for the highest level of cooperation 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 by government entities to "cloud first" procurement policies that favor cloud solutions is paramount for cloud services to take off.

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

وقد وضعت قطر تعزيز الحوسبة السحابية على رأس أولويات استراتيجيتها التحول الرقمي في قطر. تُطلق 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 النهاية في تحول قطر لتصبح دولة رقمية بالكامل.

يأتي بيان 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.

ودعماً لمبادئ الثقة والأمن والشفافية، حددت وثيقة سياسة الحوسبة السحابية التوصيات السياسية التنظيمية التي تُشكل عصب تطوير صناعة سحابية سليمة في قطر. ولتحقيق أهداف البيئة التنظيمية المواتية للحوسبة السحابية، يلزم بذل الجهود المشتركة والتنسيق فيما بين الجهات الحكومية.

في ضوء الطبيعة المتغلغلة للحوسبة السحابية، تدعو وثيقة سياسة الحوسبة السحابية إلى زيادة التعاون إلى أعلى مستوى بين الكيانات الحكومية 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 بتفضيل الحلول السحابية يُعدّ أمرًا بالغ الأهمية لانطلاق الخدمات السحابية.

2. Introduction

2. المقدمة:

To meet the goals of the Qatar National Vision 2030¹ (QNV 2030) and the Qatar National Second Development Strategy² ("NDS2"), significant investments are required in high quality digital infrastructures and services. The development of next generation data centers and world-class cloud computing services³ is one of the strategic areas that has been identified at the highest political level.

For Qatar, investing in cloud computing 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 security of their data, improve dramatically their efficiency, and grow and, ultimately, for the country to become a fully digitalized country.

In all countries where studies have been conducted, these demonstrate that the adoption of public cloud services has benefitted the economy^{7,8}. Moreover, for the private sector, it is estimated that businesses experience on average a net return in the range of 100%

يتطلب تحقيق أهداف رؤية قطر الوطنية 2030⁴ واستراتيجية التنمية الوطنية الثانية لدولة قطر⁵، استثمارات كبيرة في البنى التحتية والخدمات الرقمية رفيعة المستوى. ويدخل تطوير مراكز البيانات من الجيل القادم وخدمات الحوسبة السحابية ذات المستوى العالمي⁶ ضمن المجالات الاستراتيجية التي تم تحديدها على أعلى مستوى سياسي.

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

في جميع البلدان التي أجريت فيها دراسات بهذا الشأن، أثبتت تلك الدراسات أن تبني الخدمات السحابية العامة قد عاد بالنفع على الاقتصاد^{13,14}. علاوة على ذلك تشير التقديرات، بالنسبة للقطاع الخاص، إلى أن الشركات تُحقق في المتوسط صافي عائداً يتراوح بين 100٪ و250٪ على استثماراتها في الخدمات السحابية^{15,16}. وتُعزى هذه المنافع بالأساس إلى (1) زيادة الإيرادات الناتجة عن الخدمات التي تعتمد على

¹ QNV 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://www.gco.gov.qa/en/about-qatar/national-vision2030/>)

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://www.psa.gov.qa/en/knowledge/Documents/NDS2Final.pdf>)

³ 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".

⁴ تهدف رؤية قطر الوطنية 2030 إلى "تحويل دولة قطر إلى دولة متقدمة قادرة على تحقيق التنمية المستدامة وعلى تأمين استمرار العيش الكريم لشعبها جيلاً بعد جيل". (<https://www.gco.gov.qa/en/about-qatar/national-vision2030/>)

⁵ 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://www.psa.gov.qa/en/knowledge/Documents/NDS2Final.pdf>)

⁶ تتيح الحوسبة السحابية للمستخدم النهائي الوصول إلى البيانات واستخدام القدرة الحوسبية وخدمات البرمجيات في أي وقت وفي أي مكان بالاستفادة من شبكات النطاق العريض عالية السرعة. يمكن للمستخدمين الحصول على قدرة حوسبية غير محدودة تقريباً تحت الطلب مع تخفيض استثماراتهم الرأسمالية. انظر الملحق الأول للاطلاع على تعريف "الحوسبة السحابية".

⁷ Deloitte, 2017. "Measuring the economic impact of cloud computing in Europe." European Commission. Available at: <https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloud-computing-europe>

⁸ Gartner, 2018. Available at: <https://www.gartner.com/en/newsroom/press-releases/2018-01-23-gartner-survey-finds-government-cios-will-increase-spending-on-cloud-cybersecurity-and-analytics-in-2018>

¹³ ديلويت، 2017. "قياس الأثر الاقتصادي للحوسبة السحابية في أوروبا". المفوضية الأوروبية. متاح على الموقع: <https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloud-computing-europe>

¹⁴ جارتنر، 2018. متاح على الموقع: <https://www.gartner.com/en/newsroom/press-releases/2018-01-23-gartner-survey-finds-g>

¹⁵ ديلويت، 2018. "التأثيرات الاقتصادية والاجتماعية لمنصة جوجل السحابية" سبتمبر 2018. متاح على الموقع: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/tecnologia/Deloitte_ES_tecnologia_economic-and-social-impacts-of-google-cloud.pdf

¹⁶ ماكينزي، 2018. إجراء الانتقال الآمن إلى الحوسبة السحابية العامة. متاح على الموقع: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/making-a-secure-transition-to-the-public-cloud>

to 250% on their investments in cloud services^{9,10}. These benefits are mainly due to (i) the increase of revenues deriving from cloud-enabled services, (ii) an increase in the customer base, and (iii) in a drastic reduction of IT costs¹¹. Cloud computing will be an enabler for many broader use cases, for example within the Internet of Things (IoT) and other enterprise offerings such as 5G private networks¹².

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 “**Authority**”) has developed the Cloud Policy Statement as a strategic action that identifies key areas where legal and regulatory review is needed¹⁹.

The Cloud Policy Statement calls for the highest level of cooperation between government entities and private stakeholders, e.g. 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 favor cloud solutions is paramount for cloud services to take off.

الحوسبة السحابية، (2) زيادة في قاعدة العملاء، و(3) انخفاض كبير في تكاليف تكنولوجيا المعلومات¹⁷. كما ان الحوسبة السحابية ستكون عاملاً مساعداً و ضرورياً للعديد من الاستخدامات على نطاق واسع، فعلى سبيل المثال في نطاق انترنت الأشياء وعروض المؤسسات الأخرى مثل شبكات الجيل الخامس الخاصة¹⁸.

إن وجود سياسة رشيدة وإطار تنظيمي سليم استوحيت من مبادئ الثقة والأمن والشفافية بأهمية بالغة في تطوير الحوسبة السحابية. وبالتالي فقد وضعت هيئة تنظيم الاتصالات (يُشار إليها فيما يلي بـ "الهيئة") وثيقة سياسة الحوسبة السحابية لتكون إطاراً استراتيجياً يحدد المجالات الرئيسية التي تتطلب المراجعة القانونية والتنظيمية²⁰.

تطالب وثيقة 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. ولذلك، فإن الالتزام التام من قبل الجهات الحكومية بـ "الحوسبة السحابية أولاً" في سياسات الشراء بتفضيل الحلول السحابية يُعدّ أمراً بالغ الأهمية لانطلاق الخدمات السحابية.

⁹ Deloitte, 2018. "Economic and social impacts of Google cloud." September 2018. Available at: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/tecnologia/Deloitte_ES_tecnologia_economic-and-social-impacts-of-google-cloud.pdf

¹⁰ McKinsey, 2018. Making a Secure Transition to the Public Cloud. Available at: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/making-a-secure-transition-to-the-public-cloud>

¹¹ 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. *Ibidem*

¹² Ericsson, 2020. "Edge computing and deployment strategies for communication service providers". Available at: <https://www.ericsson.com/491f17/assets/local/reports-papers/white-papers/edge-computing-wp.pdf>

¹⁷ 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.

¹⁸ إريكسون ، 2020. "استراتيجيات الحوسبة والنشر لمقدمي خدمات الاتصالات". متاح على

<https://www.ericsson.com/491f17/assets/local/reports-papers/white-papers/edge-computing-wp.pdf>

¹⁹ The Authority is mandated to regulate ICT, Post and Access to Digital Media in the State of Qatar under Decree Law 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.

²⁰ 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 انفتاحاً وتنافسية بغية توفير خدمات اتصالات متطورة وموثوق بها تخدم كافة أنحاء الدولة.

- 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"

Cloud Policy Statement for Qatar

➤ Public and private Stakeholders' objectives in the cloud value chain

➤ Principles of Trust, Security, Transparency

➤ Policy and Regulatory Recommendations

- رؤية قطر الوطنية 2030
- استراتيجية التنمية الوطنية الثانية لدولة قطر

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

وثيقة سياسة الحوسبة السحابية لدولة قطر

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

➤ مبادئ الثقة والأمن والشفافية

➤ توصيات السياسات والتنظيم



3. The Objective of the Cloud Policy Statement

The Cloud Policy Statement sets the scene and provides recommendations for an overall policy and regulatory review that is instrumental to the development of a solid cloud industry. This, in turn, will enable Qatar to:

- ✓ attract investments, both foreign and domestic, in new digital services;
- ✓ support the growth of the national economy;
- ✓ help the transition to a fully digitalized nation;
- ✓ help meet the objective of Qatar becoming a digital hub.

In line with the objectives of its Strategy 2020-2024, the Authority has identified, in the Cloud Policy Statement, a comprehensive set of **legal** and **regulatory** requirements that competent government agencies should adopt or update²¹. Similarly, the Cloud Policy highlights recommendations for stakeholders of the cloud value chain to ensure compliance with national and international laws and best practices.

In the implementation of the Cloud Policy, a key role will be played by competent government entities within their respective mandate, namely the Ministry of Transport and Communications ("MoTC"), the Ministry of Interior ("MoI"), the Ministry of Commerce and Industry ("MoCI"), and the Ministry of Justice ("MoJ"). A clear commitment by public authorities to procurement policies that favor cloud solutions ("Cloud First Policy") is also paramount to the reach the objective.

3. الغرض من وثيقة سياسة الحوسبة السحابية:

تُعد وثيقة سياسة الحوسبة السحابية الطريق وتقدم توصيات للمراجعة الشاملة للسياسة والقواعد التنظيمية التي تلعب دورًا حاسمًا في تطوير صناعة سحابية ذات أساس متين وهذا بدوره سيمكن دولة قطر من:

- ✓ جذب الاستثمارات الأجنبية والمحلية في الخدمات الرقمية الجديدة.
- ✓ دعم نمو الاقتصاد الوطني.
- ✓ المساعدة في التحول الرقمي الكامل بالدولة.
- ✓ المساعدة في تحقيق هدف قطر لتصبح مركزًا رقميًا عالميًا.

وقد حددت الهيئة في وثيقة سياسة الحوسبة السحابية، مجموعة شاملة من الشروط القانونية والتنظيمية التي يجب على الهيئات الحكومية المعنية أن تلتزم بها أو تستوفيها، وذلك تمسًا مع أهداف استراتيجية الهيئة 2020-2024²². كما تسلط سياسة الحوسبة السحابية الضوء على التوصيات الموجهة لأصحاب المصلحة في سلسلة القيمة السحابية لضمان الامتثال للقوانين الوطنية والدولية وأفضل الممارسات.

وفي تنفيذ سياسة الحوسبة السحابية، ستلعب الهيئات الحكومية المعنية – كل في إطار اختصاصها – دورًا رئيسيًا في تنفيذ سياسة الحوسبة السحابية، وبالأخص وزارة المواصلات والاتصالات، ووزارة الداخلية، ووزارة التجارة والصناعة، ووزارة العدل. كما أن التزام الهيئات العامة بسياسات الشراء التي تُعطي الأولوية للحلول السحابية ("الحوسبة السحابية أولاً") من الأهمية أيضًا لبلوغ تلك الأهداف.

²¹ CRA Strategy 2020-2024 (see Annex III), Reference to be added when published

²² - استراتيجية هيئة تنظيم الاتصالات 2020-2024 (انظر الملحق الثالث)، يُرجى إضافة المرجع عند نشره

4. Policy and regulatory recommendations for the development of cloud computing

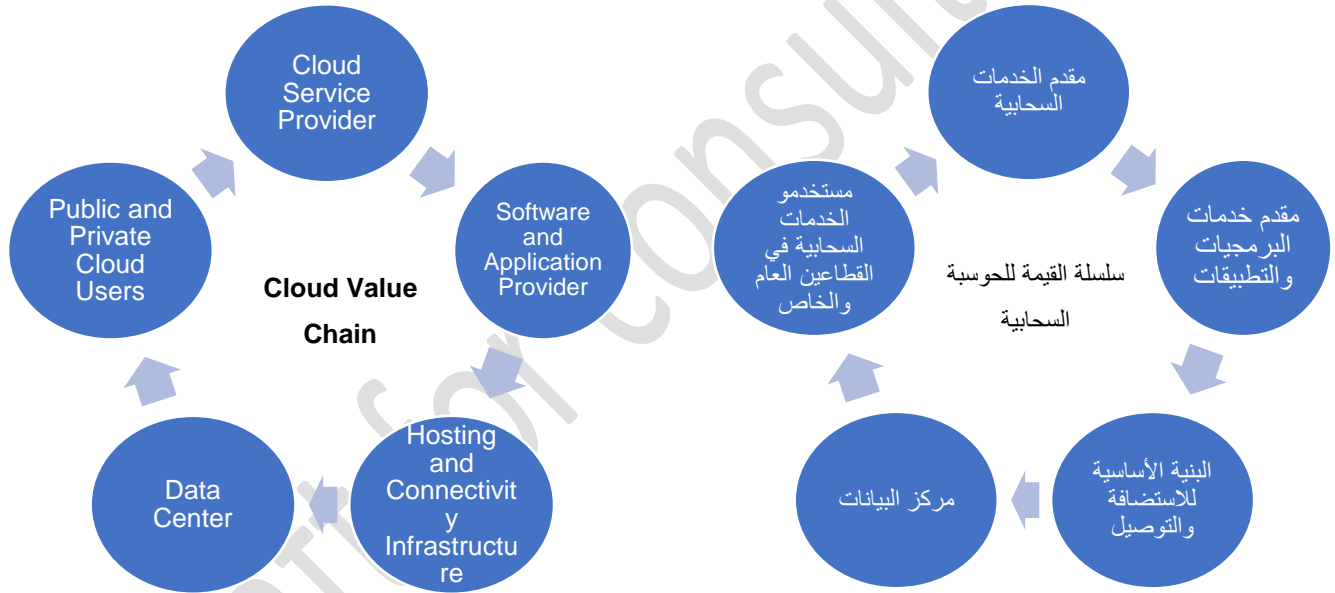
Qatar intends to promote the development of cloud computing services based on open technologies and secure platforms.

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.

4. التوصيات السياسية والتنظيمية لتطوير الحوسبة السحابية:

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

وسيعمل إنشاء إطار عمل واضح وشفاف لتبني 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.



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.

Joint efforts as well as a concerted approach are required from government entities, in their policy-making role, to provide: (i) clarity and transparency, (ii) a cloud-friendly environment, and (iii) the adoption of a “cloud first policy”`

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 standards, network architecture, specifications and certification.

The following policy and regulatory recommendations are critical to contribute to a successful cloud industry in Qatar. For each policy and regulatory area, principles are highlighted below that will require the competent government entities to take appropriate actions by way of policy making or adapting existing rules (see Annex II).

تلعب السياسات العامة دورا هاما في بناء الثقة في خدمات الحوسبة السحابية وكذلك في ضمان أعلى معايير الأمن والشفافية لمقدمي ومستخدمي الخدمات السحابية بغيرية 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.

يجب على الجهات الحكومية في أداء دورها في وضع السياسات بذل جهود مشتركة والتنسيق فيما يضمن: (1) الوضوح والشفافية، (2) بيئة صديقة للحوسبة السحابية، و (3) تبني سياسة "الحوسبة السحابية أولاً".

تتعلق الحوسبة السحابية بمجموعة متنوعة من مجالات السياسات. وتتطلب العديد من هذه المجالات أعلى مستوى من الالتزام بالأطر القانونية الدولية الراسخة أو التي يتم استحداثها، على سبيل المثال من خلال وضع المعايير وبنية الشبكة والمواصفات والشهادات.

علماً بأن للسياسات والتوصيات التنظيمية التالية أهمية بالغة في المساهمة في صناعة حوسبة سحابية ناجحة في دولة قطر. وبالنسبة لكل مجال من المجالات السياسية والتنظيمية، يتم تسليط الضوء على المبادئ أدناه والتي تتطلب من الجهات الحكومية المعنية اتخاذ الإجراءات المناسبة عن طريق وضع السياسات أو تعديل القواعد الحالية (انظر الملحق الثاني).

- Policy and regulatory recommendations

Cloud-First Policy	
Data localization and free flow of data	
Privacy and access to data	
Data Classification	
Data interoperability and data portability	
Liability regime	
Security Standards	
Service Level Agreements	
Hosting and Connectivity	
Environmental Sustainability	

- التوصيات السياسية والتنظيمية:

سياسة الحوسبة السحابية أولاً	
التوطين والتدفق الحر للبيانات	
الخصوصية والوصول للبيانات	
تصنيف البيانات	
إمكانية نقل البيانات وتبادلها	
قواعد المسؤولية	
المعايير الأمنية	
اتفاقيات مستوى الخدمة	
الإستضافة والتوصيل	
الإستدامة البيئية	

4.1 Cloud-First Policy

Qatar Digital Government Strategy 2020²³ aims at the digital transformation of government entities.

Amongst the objectives of the strategy is “to create efficiency in government administration through automation of functions, state of the art applications, and a common ICT infrastructure that saves money, increases security, and enhances the user experience”.

To accelerate the process of digital transformation, Qatar will develop 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. infrastructure, platform and application, and outsourcing management and maintenance overhead.

4.1 سياسة الحوسبة السحابية أولاً:

تهدف استراتيجية الحكومة الرقمية لدولة قطر 2020²⁴ إلى دعم التحول الرقمي في القطاع الحكومي.

ومن أهداف الاستراتيجية: "رفع كفاءة العمليات الإدارية الحكومية من خلال أتمتة الوظائف، وأحدث التطبيقات، وإقامة بنية تحتية مشتركة لتكنولوجيا المعلومات والاتصالات تحسن كفاءة استخدام الموارد العامة للدولة وتزيد الأمن وتعزز تجربة المستخدم".

في سعيها للإسراع بعملية التحول الرقمي، عملت قطر 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 and Regulatory Recommendation

➤ التوصيات السياسية والتنظيمية

Qatar shall develop a common policy for public procurement of cloud services by government entities, that is consistent with the principles of the Cloud Policy Statement. Cloud solutions shall be assessed before any on-premise solutions, and based on a clear data classification policy.

➤ تعمل قطر على وضع سياسة عامة لمشتريات الجهات الحكومية من الخدمات السحابية تتوافق مع مبادئ وثيقة 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 localization and free flow of data

4.2 توطين البيانات والتدفق الحر للبيانات

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.

من 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.

4.2.1 Data localization

4.2.1 توطين البيانات

Cloud Service Providers store data which is then accessible anytime and anywhere.

يتولى مقدمو الخدمات السحابية تخزين البيانات التي يمكن الوصول إليها بعد ذلك في أي وقت وفي أي مكان.

From a technical perspective, it is **no longer necessary for data to be stored in Qatar** and as such it would be counter-productive **to impose a requirement to do so**.

من الناحية الفنية، لم يعد من الضروري تخزين البيانات في دولة قطر، وبالتالي سيكون فرض اشتراط بهذا الصدد غير مُجدي.

²³<https://www.motc.gov.qa/sites/default/files/documents/Qatar%20e-Government%202020%20Strategy%20Executive%20Summary%20English.pdf>

²⁴<https://www.motc.gov.qa/sites/default/files/documents/Qatar%20e-Government%202020%20Strategy%20Executive%20Summary%20English.pdf>

From a security standpoint, and except for highly sensitive government data (see Data Classification *infra*), it is more appropriate to implement **measures that are more efficient than localization** requirements, such as:

- encryption;
- anonymization;
- aggregation; and/or
- storage in pre-defined regional hubs.

ومن الناحية الأمنية، وباستثناء حالة البيانات الحكومية شديدة الحساسية (انظر تصنيف البيانات أدناه)، نجد من الأنسب تنفيذ إجراءات أكثر كفاءة من متطلبات التوطين، مثل:

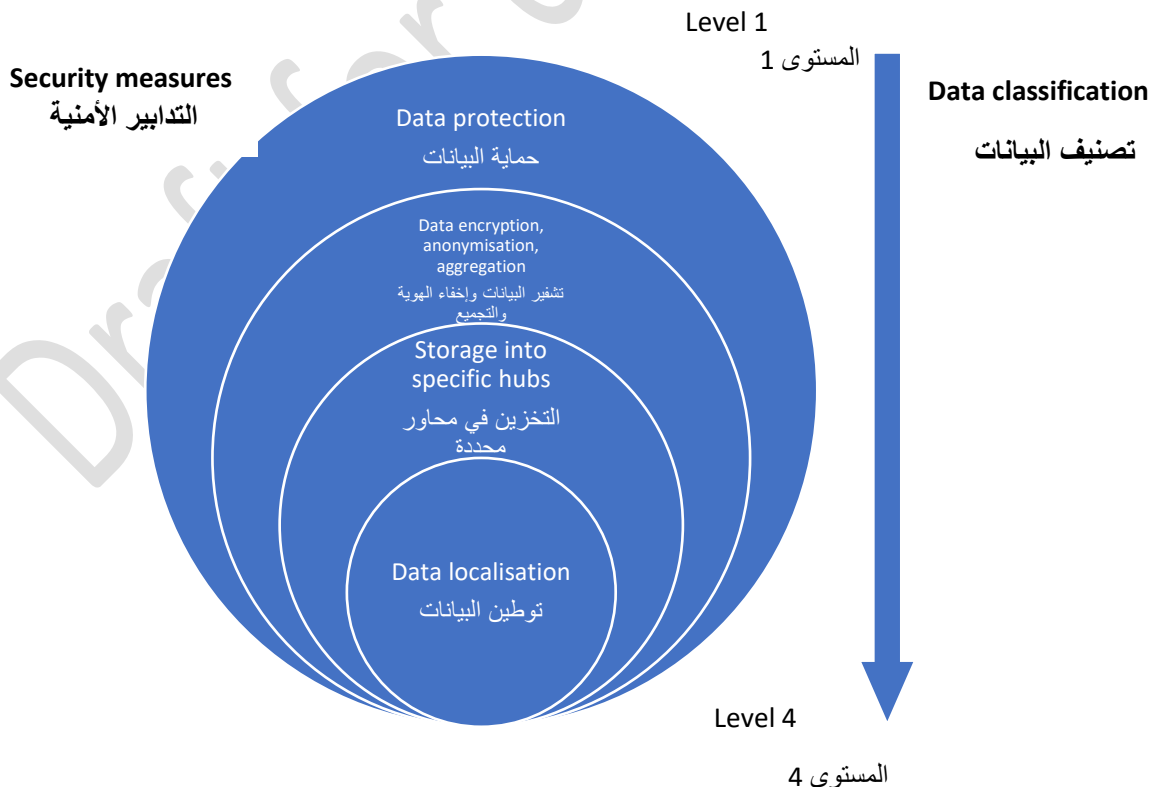
- التشفير
- إخفاء الهوية
- التجميع
- التخزين في مراكز إقليمية محددة سلفاً.

Accordingly, any request for data localization shall be very limited in volume and scope and, following a proper assessment, address only matters for which no alternative exists.

وبناءً على ذلك، فإن أي طلب لتوطين البيانات سيكون محدوداً جداً من حيث الحجم والنطاق، ويجب معالجة المسائل التي لا يوجد لها بديل بعد إجراء التقييم المناسب.

Indeed, the **security and data protection capabilities of Cloud Service Providers are robust and secure** precisely because of their (i) reliance on globally distributed infrastructure that ensure availability, resilience and security, and (ii) compliance with international standards and procedures.

في الواقع، إن قدرات الأمان وحماية البيانات لمقدمي الخدمات السحابية قوية وآمنة على وجه التحديد بسبب (1) اعتمادها على البنية التحتية الموزعة عالمياً التي تضمن التوافر والمرونة والأمان، و (2) الامتثال للمعايير والإجراءات الدولية.



4.2.2 Free flow of data

Cross-border data flows are critical to the growth of Qatar's digital economy and should be enabled in a way that protects privacy and security.

Public and private sector organizations should have the freedom to choose which cloud networks they want to use *provided* these can be held "**accountable**".

As such, Qatar shall provide a wide range of mechanisms to **allow data to flow freely** whilst ensuring an adequate level of protection. Accordingly, the following mechanisms shall be considered for cross border transfers:

- **Contractual arrangements** that set out appropriate data privacy and security standards to be implemented by the organizations transferring data;
- **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;
- **Certified codes of conduct, certifications, privacy marks, seals and international standards**, such as the ISO standards;
- **Bilateral or multilateral arrangements which rely on self-certification** based on a given privacy or security standard, with an enforcement mechanism such as the EU-US Privacy Shield²⁵;

4.2.2 التدفق الحر للبيانات

تُعد تدفقات البيانات عبر الحدود أمرًا بالغ الأهمية لنمو الاقتصاد الرقمي في دولة قطر ويجب تمكينه بطريقة تحمي الخصوصية والأمن.

ينبغي أن تتمتع مؤسسات القطاعين العام والخاص بحرية اختيار الشبكات السحابية التي ترغب في استخدامها على أن تكون "خاضعة للمساءلة".

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

- **الترتيبات التعاقدية** التي تحدد معايير الخصوصية والأمن المناسبة للبيانات التي يتعين تنفيذها من قبل المنظمات التي تنقل البيانات؛
- **القواعد الملزمة للشركات** التي تحدد الحماية المنسقة عالية المستوى والامتثال للخصوصية من قبل جميع الكيانات الوطنية لمقدم الخدمات السحابية المتعددة الجنسيات؛
- **قواعد الخصوصية القابلة للتنفيذ عبر الحدود للشركات** على غرار القواعد المعترف بها عالميًا مثل قواعد الخصوصية عبر الحدود الخاصة بمُنْتَدَى التعاون الاقتصادي لدول آسيا والمحيط الهادئ؛
- **مدونات قواعد السلوك والشهادات وعلامات الخصوصية والأختام والمعايير الدولية المُعتمدة**، مثل معايير الأيزو؛
- **الترتيبات الثنائية أو المتعددة الأطراف التي تعتمد على الاعتماد الذاتي** بناءً على معيار خصوصية أو أمن معينين، مع آلية التنفيذ مثل درع²⁶ للخصوصية بين الاتحاد الأوروبي والولايات المتحدة؛

²⁵ <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg>. The EU-US Privacy Shield deals with, among other things;

- **the information a US organization must provide** to individuals from whom it collects data such as the types of personal data it collects, the purposes for which it collects and uses personal data and how to contact the organization;
- **the choice** US organizations must offer to EU individuals to opt-out of their personal data being disclosed to a third party, or used for a purpose that is materially different from the purpose(s) for which it was originally collected; and
- **the security** US organizations must provide to protect the personal data of EU individuals from loss, misuse and unauthorized access, disclosure, alteration and destruction by taking into account the specific risks involved in the processing and the nature of the personal data.

²⁶ <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg> يختص درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة بالتعامل مع ما يلي من

بين أمور أخرى؛

- **المعلومات التي يجب أن تقدمها المنظمة الأمريكية** إلى الأفراد الذين تجمع منهم البيانات مثل أنواع البيانات الشخصية التي تجمعها والأغراض التي تُجمع من أجلها وتستخدم البيانات الشخصية وكيفية الاتصال بالمنظمة؛

- **Adequacy rulings** with selected third countries; and/or
- If cross-border data transfer restrictions are established, the law should provide for **specific exceptions that permit cross-border transfers**, without prior regulator review of permission, including when such cross-border transfer is in the public interest, or when it is necessary in the establishment or defense of a legal claim.

أحكام الملازمة مع دول أخرى مُختارة؛

إذا تم وضع قيود على نقل البيانات عبر الحدود، فينبغي أن ينص القانون على استثناءات محددة تسمح بعمليات النقل عبر الحدود، دون مُراجعة مسبقة من الجهة المنظمة لمنح الإذن، بما في ذلك عندما يكون هذا النقل عبر الحدود للمصلحة العامة، أو عندما يكون ذلك ضروريًا في إقامة دعوى قانونية أو في دفاعها.

In any event, the data subject's prior consent should be required for personal data. وعلى أي حال، يجب أن تكون الموافقة المُسبقة لموضوع البيانات مطلوبة للبيانات الشخصية.



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 authority.

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

- الخيار الذي يجب أن تقدمه المنظمات الأمريكية لأفراد الاتحاد الأوروبي للانسحاب في حال الكشف عن بياناتهم الشخصية للغير أو استخدامها لغرض يختلف جوهريًا عن الغرض (الأغراض) الذي تم جمعها من أجله في الأصل؛ و
- يجب على المنظمات الأمريكية توفير حماية للبيانات الشخصية لأفراد الاتحاد الأوروبي من الضياع وإساءة الاستخدام والوصول غير المصرح به والإفصاح والتعديل والتدمير من خلال مراعاة المخاطر المحددة التي تنطوي عليها معالجة البيانات الشخصية وطبيعتها.

4.2.3 Non-Personal data

Finally, the **cross-border flows of non-personal data is set to take off** with the rapid development of **Artificial Intelligence**²⁷, the **Internet of Things** and **machine learning**.

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.

4.2.3 البيانات غير الشخصية

أخيراً، من المقرر أن تتطلق تدفقات البيانات غير الشخصية عبر الحدود مع التطور السريع للذكاء الاصطناعي²⁸ وإنترنت الأشياء والتعلم الآلي.

يجب على دولة قطر الدخول في اتفاقيات مع دول أجنبية موثوقة لتسهيل عبور البيانات غير الشخصية عبر الحدود عندما تكون هذه الدول الأجنبية خاضعة لمعايير كافية لحماية البيانات والأمن السيبراني.

➤ Policy and Regulatory Recommendation

Data residency is no longer a requirement as security and encryption technologies now provide a sufficient level of security. As a result, the legislations should provide instead for various mechanisms to allow data to flow whilst ensuring that an adequate level of protection is in place.

➤ التوصية السياسية والتنظيمية

لم يعد إقامة البيانات شرطاً مطلوباً حيث توفر تقنيات الأمان والتشفير الآن مستوى كافٍ من الأمان؛ ونتيجة لذلك، ينبغي أن تنص التشريعات بدلاً من ذلك على آليات مختلفة للسماح بتدفق البيانات مع ضمان وجود مستوى مناسب من الحماية.

4.3 Privacy and access to data

Whilst the data protection regulatory framework should promote customer trust in the digital ecosystem, overly stringent data protection rules could impede the adoption of cloud computing. It is the aim of this Cloud Policy Statement to strike the right balance.

4.3 الخصوصية والوصول إلى البيانات

في حين أن الإطار التنظيمي لحماية البيانات يجب أن يعزز من ثقة العملاء في النظام البيئي الرقمي، إلا أن قواعد حماية البيانات الصارمة بشكل مفرط يمكن أن تعرقل اعتماد الحوسبة السحابية. ويُعد الهدف من بيان نظام السحابة هذا هو تحقيق التوازن الصحيح.

4.3.1 Privacy

In order to strengthen customer trust in digital services, and especially cloud services, the law should require that **all ICT products and services be developed based on** the principles of "**privacy by design**" and "**security by design**". Technical guidelines should be issued that describe how these requirements can be achieved, in collaboration with the MoTC and Q-CERT.

4.3.1 الخصوصية

من أجل تعزيز ثقة العملاء في الخدمات الرقمية وخاصة الخدمات السحابية، يجب أن يشترط القانون تطوير جميع منتجات وخدمات تكنولوجيا المعلومات والاتصالات بناءً على مبادئ "الخصوصية بالتصميم" و "الأمان بالتصميم". ويجب إصدار المبادئ التوجيهية التقنية التي تصف كيف يمكن تحقيق هذه المتطلبات، بالتعاون مع وزارة المواصلات والاتصالات والفريق القطري للاستجابة لطوارئ الحاسب الآلي.

Legislation should introduce **breach notification and response obligations**, aligned with international best

يجب أن يقدم التشريع التزامات الإخطار عن الخرق والتصدي له بما يتماشى مع أفضل الممارسات والعمليات الدولية، فضلاً عن العقوبات

²⁷ Data governance rules on access to and sharing of data is a pillar of the "National Artificial Intelligence Strategy for Qatar" (https://qcai.qcri.org/wp-content/uploads/2019/02/National_AI_Strategy_for_Qatar-Blueprint_30Jan2019.pdf)

²⁸ تعد قواعد حوكمة البيانات بشأن الوصول إلى البيانات ومشاركتها أحد ركائز "الاستراتيجية الوطنية للذكاء الاصطناعي في دولة قطر" (https://qcai.qcri.org/wp-content/uploads/2019/02/National_AI_Strategy_for_Qatar-Blueprint_30Jan2019.pdf)

practices and processes, as well as associated sanctions to encourage the reporting of data breaches, particularly for critical infrastructure.

4.3.2 Cross border requests

Cross-border requests for data should be made through Mutual Legal Assistance Treaties ("MLATs"), ensuring appropriate involvement of the authorities in the countries where the data is stored.

In that context, Qatar should ensure that **MLATs processes are efficient, accessible and transparent**²⁹. For example, MLATs should include:

- i. a timetable for cooperation and response, both by government and Cloud Service Providers;
- ii. a simple process to exchange data pertaining to the source and destination of communications to locate rapidly individuals and devices; and

المرتبطة بها لتشجيع الإبلاغ عن خروقات البيانات، لا سيما في البنية التحتية الحيوية.

4.3.2 الطلبات عبر الحدود

يجب تقديم الطلبات للبيانات عبر الحدود من خلال "معاهدات المساعدة القانونية المتبادلة" بما يضمن المشاركة المناسبة للسلطات في البلدان التي يتم فيها تخزين البيانات.

وفي هذا السياق، يجب على قطر التأكد من أن عمليات "معاهدات المساعدة القانونية المتبادلة" تتسم بالكفاءة ويمكن الوصول إليها وشفافة³⁰. فيجب، على سبيل المثال، أن تتضمن معاهدات المساعدة القانونية المتبادلة ما يلي:

- I. جدول زمني للتعاون والاستجابة، من قبل كل من الحكومة ومقدمي الخدمات السحابية؛
- II. عملية بسيطة لتبادل البيانات المتعلقة بمصدر ووجهة الاتصالات لتحديد الأفراد والأجهزة بسرعة؛

²⁹ Some of the key issues dealt with by MLATs, or bilateral agreements that serve a similar function are:

- The US CLOUD Act (<https://www.congress.gov/bill/115th-congress/house-bill/4943>) which, among other things:
 - 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
 - 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:
 - enables UK investigators to compel the disclosure of electronic data stored outside of the UK using an alternative to a formal MLA request;
 - 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;
 - 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.

³⁰ بعض القضايا الرئيسية التي تعالجها معاهدات المساعدة القانونية المتبادلة أو الاتفاقات الثنائية التي تؤدي وظيفة مماثلة هي:

- قانون السحابة الأمريكي (<https://www.congress.gov/bill/115th-congress/house-bill/4943>) والذي من بين أمور أخرى:
 - 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
 - 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 مباشرةً 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:
 - يُمكن المحققين في المملكة المتحدة من إجبارهم على الكشف عن البيانات الإلكترونية المخزنة خارج المملكة المتحدة باستخدام بديل لطلب المساعدة القانونية المتبادلة الرسمية؛
 - 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؛
 - يلزم 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.

- iii. a requirement by government agencies and Cloud Service Providers to establish single points of contacts for access to data.

Qatar should play an active role in **educating law enforcement agencies and Cloud Service Providers about MLATs** and should encourage cooperation with other countries to ensure effective implementation.

.III وطلب إنشاء نقاط اتصال واحدة للوصول إلى البيانات من قبل الوكالات الحكومية ومقدمي الخدمات السحابية.

على دولة قطر أن تلعب دوراً نشطاً في تثقيف وكالات تطبيق القانون ومقدمي الخدمات السحابية حول "معاهدات المساعدة القانونية المتبادلة" ويجب أن تشجع التعاون مع الدول الأخرى لضمان التنفيذ الفعال.

➤ Policy and Regulatory Recommendation

➤ التوصية السياسية والتنظيمية

Transparency and Certainty are key for stakeholders, especially 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"), ensuring appropriate involvement of the authorities in the countries where the data is stored.

الشفافية واليقين هما مفتاح أصحاب المصلحة، خاصة فيما يتعلق بالقواعد التي تنظم الوصول إلى بيانات الطلبات عبر الحدود. ويجب تقديم الطلبات عبر الحدود للحصول على البيانات من خلال "معاهدات المساعدة القانونية المتبادلة" وضمان المشاركة المناسبة للسلطات في البلدان التي يتم فيها تخزين البيانات.

4.4 Data Classification

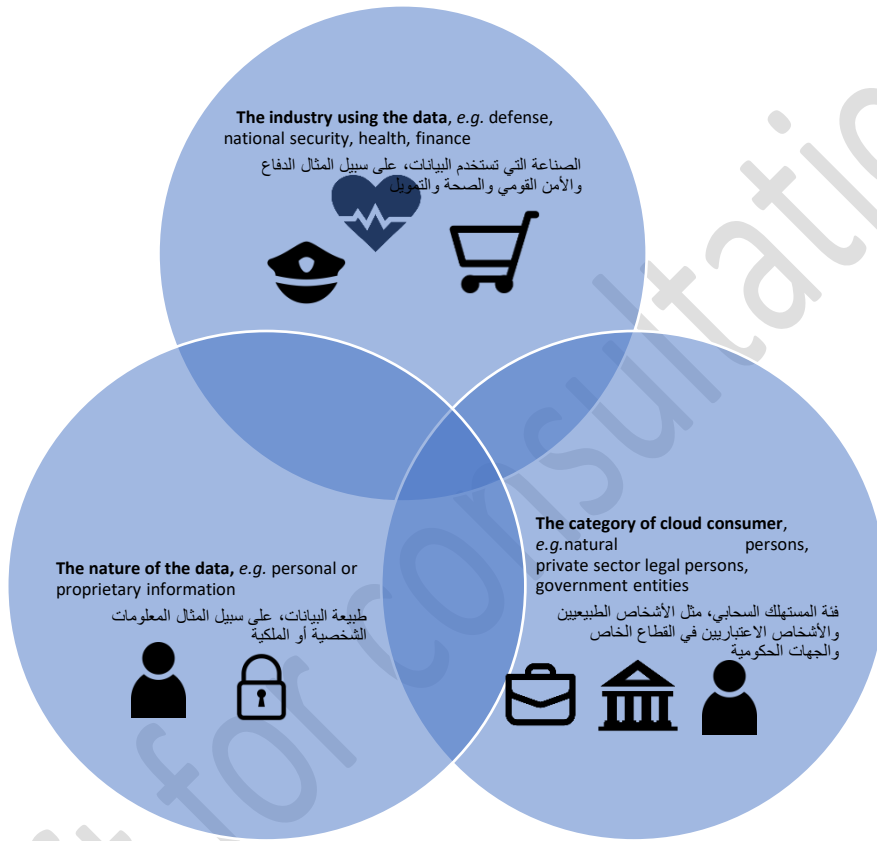
4.4 تصنيف البيانات

Public and private entities should implement a **classification of data, according to the level of confidentiality, integrity and availability.**

يجب على الكيانات العامة والخاصة تنفيذ تصنيف للبيانات، وفقاً لمستوى السرية والنزاهة والتوافر.

Legislation should set out **different requirements of information security levels applicable to different types of data**, based on their level of confidentiality, integrity and availability, considering the following:

يجب أن يحدد التشريع المتطلبات المختلفة لمستويات أمن المعلومات المُطبَّقة على أنواع مختلفة من البيانات بناءً على مستوى السرية والنزاهة والتوافر مع مراعاة ما يلي:



Ultimately, it is **the owner of the data who must be responsible for determining the information security level** which best matches his or her needs.

في نهاية المطاف، يجب أن يكون مالك البيانات هو المسؤول عن تحديد مستوى أمن المعلومات الذي يناسب احتياجاته على أفضل وجه.

For the most sensitive categories of data, such as highly classified government data, it may be appropriate to set up an elevated protection in the form of data localization, specifically when data is at rest. If that is the case, this requirement should be set out clearly.

وقد يكون من المناسب فيما يتعلق بفئات البيانات الأكثر حساسية، مثل البيانات الحكومية عالية السرية، إعداد حماية مرتفعة في شكل توطين البيانات وخاصة عندما تكون البيانات في حالة ساكنة. وإذا كان الأمر كذلك، فيجب تحديد هذا الشرط بوضوح.

In any event, the **sensitive nature of data shall not prevent storage on the cloud (whether local or abroad)**. Secured and dedicated private cloud solutions, coupled with a system of accreditation, may be used instead to provide the necessary security assurance.

على أي حال، لن تمنع الطبيعة الحساسة للبيانات من التخزين على السحابة (سواء محلياً أو خارجياً). فيمكن استخدام حلول السحابة الخاصة الأمانة والمخصصة إلى جانب نظام الاعتماد بدلاً من ذلك لتوفير ضمان الأمان الضروري.

➤ Policy and Regulatory Recommendation

➤ التوصية السياسية والتنظيمية

Clear guidelines around classification of data and associated security controls should be established to guide private and public sector users. In case the location of certain data needs to be restricted, this should be done by restricting the scope of such requirements to highly classified government data.

يجب وضع إرشادات واضحة حول تصنيف البيانات والضوابط الأمنية المرتبطة بها لتوجيه مستخدمي القطاعين العام والخاص. وفي حالة الحاجة إلى تقييد موقع بيانات معينة، يجب أن يتم ذلك عن طريق قصر نطاق هذه المتطلبات على البيانات الحكومية التي هي على درجة عالية من السرية.

4.5 Data interoperability and data portability

4.5 قابلية التشغيل البيئي للبيانات وإمكانية نقلها

Interoperability of cloud services is key to the development of a successful cloud industry.

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

Cloud interoperability allows cloud services to interact with other cloud services by exchanging information.

تسمح إمكانية التشغيل البيئي السحابي للخدمات السحابية بالتفاعل مع الخدمات السحابية الأخرى من خلال تبادل المعلومات.

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**.

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

In order to encourage Cloud Service Providers to embed data portability into their systems, legislation should require Cloud Service Providers to guarantee data portability, meaning to provide built-in technical possibilities for data subjects to move their personal data to other platforms.

من أجل تشجيع مُقدمي الخدمة السحابية على تضمين إمكانية نقل البيانات في أنظمتهم، يجب أن تتطلب التشريعات من مُقدمي الخدمة السحابية ضمان إمكانية نقل البيانات وهو ما يعني توفير إمكانيات فنية داخلية لموضوعات البيانات لنقل بياناتهم الشخصية إلى منصات أخرى.

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).

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

In addition, as part of the procurement process:

بالإضافة إلى ذلك، كجزء من عملية الشراء:

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

- ينبغي إدراج قابلية نقل البيانات وإمكانية التشغيل البيئي للنظام حسب التصميم في التقييم العام كمعيار أساسي؛
- يجب أن يوفر مُقدم الخدمة السحابية للإدارة العامة واجهة برمجة التطبيقات للسماح للإدارة بضمان قابلية التشغيل البيئي بين أنظمة تكنولوجيا المعلومات المختلفة الخاصة بها.

➤ Policy and Regulatory Recommendation

➤ التوصية السياسية والتنظيمية

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 دوليًا بشأن التشغيل البيئي للخدمات السحابية عند التعاقد على الخدمات السحابية وفي عقود المشتريات العامة. كما تُعد إمكانية التشغيل البيئي للخدمات السحابية شرطاً أساسياً لضمان إمكانية نقل الخدمات لمستخدمي السحابة.

4.6 Liability regime

4.6 قواعد المسؤولية

A regulatory regime is needed that limits the liability of Cloud Service Providers regarding third party content stored on the cloud.

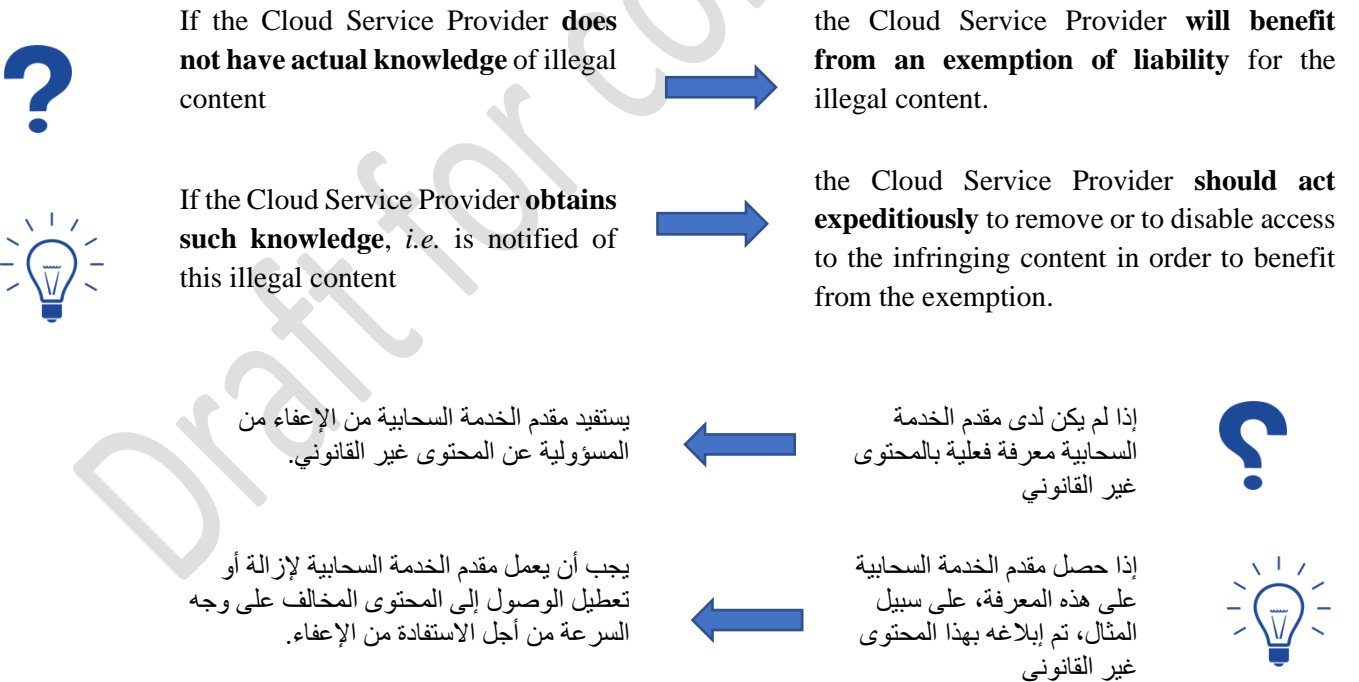
هناك حاجة إلى قواعد تنظيمية تحد من مسؤولية مُقدمي الخدمة السحابية فيما يتعلق بالمحتوى غير المخزن على السحابة.

Legislation should afford a "safe harbor" protection to Cloud Service Providers.

ينبغي أن يوفر التشريع حماية "الملاذ الآمن" لمقدمي الخدمات السحابية.

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

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



Clear rules on “Notice and Take Down” 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; and
- the level of transparency Cloud Service Providers should provide regarding their take-down procedures.

As part of this regulatory regime, **Qatar should not 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.

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.

ينبغي 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 مقدمو الخدمات السحابية وعلى وجه التحديد منحهم وقتاً معقولاً للاستجابة؛
- ومستوى الشفافية الذي يجب أن يقدمه مقدمو الخدمات السحابية فيما يتعلق بإجراءات الإزالة.

يجب على دولة قطر، كجزء من هذا النظام التنظيمي، ألا 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.

أخيراً، يجب أن يتمتع مقدمو الخدمات السحابية بالقدرة 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 and Regulatory Recommendation

➤ التوصية السياسية والتنظيمية

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 أن تمتنع 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.

4.7 Security standards

4.7 معايير الأمان

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 بيانات الحوسبة المشتركة وتعتمد على الإنترنت العام في نقل المعلومات والبيانات. وبالتالي فإنها تثير التساؤلات بشأن الأمان 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.

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

- ensure a level of security appropriate to the risk posed by the data stored; and
- prevent and reduce the impact of incidents affecting the cloud services and any data stored and/or processed.

Such measures should consider:

- i. the security of the Cloud Service Provider's systems and facilities;
- ii. incident handling processes and procedures;
- iii. business continuity management, monitoring, auditing and testing; and
- iv. international standards and certifications that best promote security.

International standards may include the following general standards:

- CSA STAR, ISO 22301 (Business continuity management systems);
- ISO 27001 (Information security management);
- ISO 277001 (Privacy information management)
- ISO 27017 (Cloud security);
- ISO 27018 (Cloud privacy);
- Service Organization Controls Report ("SOC") 1 and 2; as well as
- standards that serve sector-specific security requirements such as the Payment Card Industry Data Security Standard ("PCI DSS") for financial services.

Compliance with international standards should be encouraged as it provides a common language to help

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

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

- ضمان مستوى من الأمان مناسب للمخاطر التي تشكلها البيانات المخزنة؛
- ومنع وتقليل تأثير الحوادث التي تؤثر على الخدمات السحابية وأي بيانات مخزنة أو معالجة أو كليهما.

يجب أن تأخذ هذه التدابير ما يلي بعين الاعتبار:

- I. أمن أنظمة ومراقب مقدم الخدمة السحابية؛
- II. عمليات وإجراءات التعامل مع الحوادث؛
- III. إدارة استمرارية الأعمال والمراقبة والتدقيق والاختبار؛
- IV. المعايير والشهادات الدولية التي تعزز الأمن بشكل أفضل.

قد تتضمن المعايير الدولية المعايير العامة التالية:

- شهادة CSA STAR، الأيزو 22301 (أنظمة إدارة استمرارية الأعمال)؛
- الأيزو 27001 (إدارة أمن المعلومات)؛
- الأيزو 277001 (إدارة معلومات الخصوصية)؛
- الأيزو 27017 (الأمان السحابي)؛
- الأيزو 27018 (خصوصية السحابية)؛
- تقرير ضوابط مؤسسة الخدمة 1 و2؛ بالإضافة إلى
- المعايير التي تخدم متطلبات الأمان الخاصة بقطاع معين مثل معيار أمان بيانات صناعة بطاقات الدفع للخدمات المالية.

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

organizations better comprehend, communicate and manage cybersecurity risks.

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.

Cloud Service Providers should also be obliged to notify, under a reasonable timeframe, the relevant authority of any security incident which has a significant impact on the provision of their services, based on several factors, such as:

- the number of affected users;
- the duration of the incident; or
- the affected geographic area.

Government agencies 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 government data is lost.

بالإضافة إلى ذلك، فإن اتباع المعايير الدولية القابلة للتشغيل البيئي عبر الحدود يجعل من السهل 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.

يجب أن يكون مقدمو الخدمات السحابية مُلزمين أيضًا بإخطار السلطة المختصة بأي حادث أمني له تأثير كبير على تقديم خدماتهم وذلك في إطار زمني معقول، استنادًا إلى عدة عوامل، مثل:

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

يجب أن يكون لدى الوكالات الحكومية خطط طوارئ للتخفيف والدعم الاحتياطي لبياناتها وخدماتها من أجل ضمان استمرارية الخدمة في أوقات الطوارئ واستعادة البيانات في حالة فقدان البيانات الحكومية.

➤ Policy and Regulatory Recommendation

➤ التوصية السياسية والتنظيمية

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 as it can be detrimental to the development of a solid cloud industry.

يتعين أن يكون متاحًا 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 دوليًا. وينبغي تجنب إنشاء المعايير المحلية أو ازدواجية المعايير المُعترف بها دوليًا حيث يمكن أن يكون ذلك ضارًا بتطوير صناعة سحابية متينة.

4.8 Service Level Agreements ("SLAs")

4.8 اتفاقيات مستوى الخدمة

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.

من العناصر المهمة في توفير الخدمات السحابية استخدام "اتفاقيات مستوى الخدمة" لتحديد نطاق استخدام وتوفير الموارد السحابية.

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.

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

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.

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

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

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

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

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

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 (i) reliability, (ii) availability, or (iii) fix; and
- 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.

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 اعتمادًا على الخدمة السحابية ونموذج النشر وحساسية البيانات وطبيعة العميل وقطاع الأعمال.

➤ Policy and Regulatory Recommendation

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.

➤ التوصية السياسية والتنظيمية

يجب أن تكون "اتفاقيات مستوى الخدمة" موضوعة لضمان الشروط المتفق عليها لتقديم الخدمات. إذ تحتاج الخدمات السحابية الموثوقة إلى مقدمي الخدمات والمستهلكين للاتفاق على مؤشرات مستويات الخدمة (الأداء والتوافر والفواتير) التي يتم تقديمها في المنتج السحابي. كما سيساعد اعتماد الشروط والأحكام الموحدة لـ"اتفاقيات مستوى الخدمة" السحابية بما يتماشى مع المعايير الدولية على تعزيز ثقة الجمهور في الخدمات السحابية.

4.9 Hosting and Connectivity

"Hosting" and "Connectivity" services are central elements that will determine investors' choices in the development of cloud services in Qatar. The 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 three different routes.

4.9 الاستضافة والتوصيل

تعد خدمات "الاستضافة" و "التوصيل" من العناصر الأساسية التي ستحدد خيارات المستثمرين في تطوير الخدمات السحابية في دولة قطر. ويعتبر السعر وجودة الخدمة لاستضافة البيانات والاتصال بالشبكة من المسائل الحاسمة (أسعار دول مجلس التعاون الخليجي أعلى من متوسط منظمة التعاون الاقتصادي والتنمية بما يتراوح بين 4 و7 أضعاف). كما يجب ضمان التوصيل الدولي بثلاثة طرق مختلفة.

➤ Policy and Regulatory Recommendation

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.

➤ التوصية السياسية والتنظيمية

تعد أسعار التوصيل الدولي عنصرًا حاسمًا لاختيار المستثمرين ويجب أن تتماشى مع المعايير الدولية. كما ينبغي ضمان التوصيل الدولي بالطرق المتعددة والمختلفة.

4.10 Environmental sustainability

4.10 الاستدامة البيئية

The development of cloud computing may have a significant environmental impact due to energy and water consumption as well as greenhouse gas emissions.

قد يكون لتطوير الحوسبة السحابية تأثير بيئي كبير بسبب استهلاك الطاقة والمياه وكذلك انبعاثات غازات الاحتباس الحراري.

These issues **can be mitigated** with data centers that:

ويمكن تخفيف هذه المشكلات عن طريق مراكز البيانات التي:



use **low/green energy servers**; and

implement **sustainable cooling and heat waste recycling** solutions.

تستخدم خوادم طاقة منخفضة / خضراء؛



وتُنفذ حلول التبريد المستمر وإعادة تدوير النفايات 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 center's 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 حول انبعاثات الطاقة الخاصة بعمليات مركز البيانات وتوفير الحوافز لتشجيع التحول من قبل مشغلي مركز البيانات إلى الممارسات المستدامة والطاقة المتجددة.

➤ Policy and Regulatory Recommendation

➤ التوصية السياسية والتنظيمية

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.

**

Annex I – Definition, characteristics, service and deployment models of cloud computing

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”³¹.

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

الملحق الأول - تعريف الحوسبة السحابية وخصائصها ونماذج خدماتها ونشرها

1. التعريف

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"³².

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

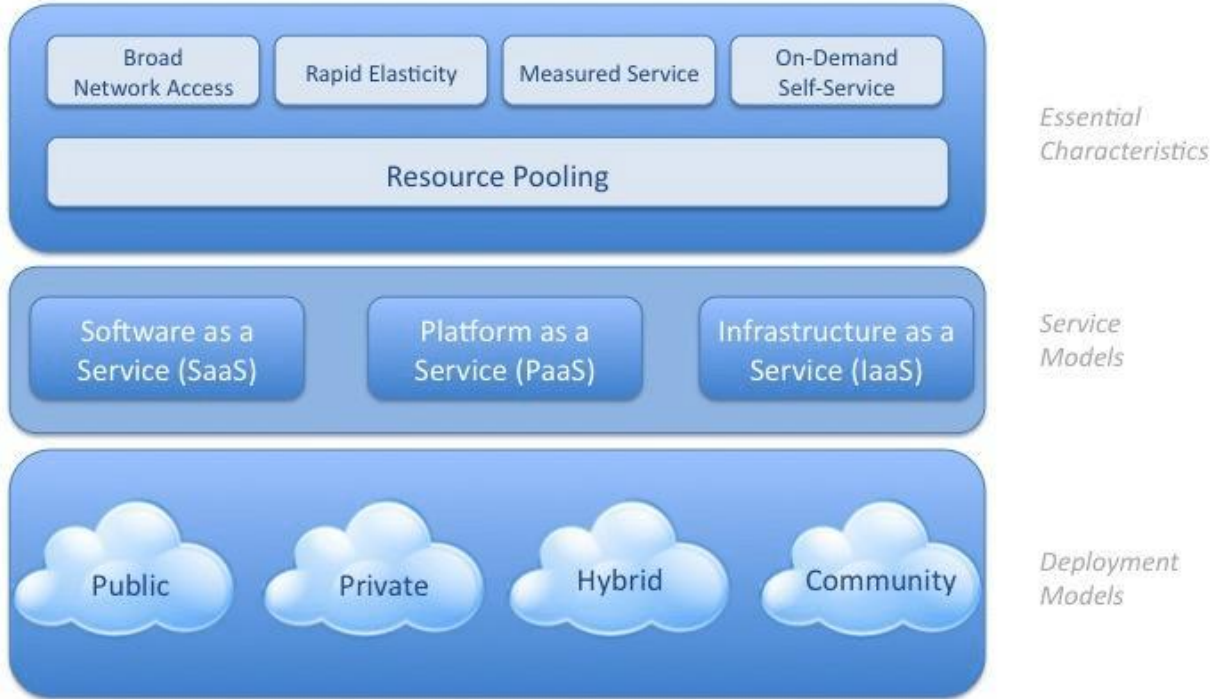


Figure: NIST (National Institute for Standards and Technology) Visual Model of Cloud Computing

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

³¹ Recommendation ITU-TY.3500: “Information Technology-Cloud Computing-Overview and vocabulary”. Available at: <https://www.itu.int/rec/T-REC-Y.3500-201408-I>

³² التوصية ITU-TY.3500: "نظرة عامة على تقنية المعلومات - الحوسبة السحابية والمفردات". متاح على: <https://www.itu.int/rec/T-REC-Y.3500-201408-I>

2. Essential characteristics

2. الخصائص الأساسية³³

Essential characteristics of cloud computing include³⁴:

تشمل الخصائص الأساسية للحوسبة السحابية ما يلي:

Essential characteristics	Description
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 (<i>e.g.</i> , 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 (<i>e.g.</i> , 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 (<i>e.g.</i> , storage, processing and bandwidth) by leveraging a metering capability at some level of abstraction appropriate to the type of service (<i>e.g.</i> , 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.

³³ 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://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-CLOUD-2012-P1-PDF-E.pdf

³⁴ 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://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-CLOUD-2012-P1-PDF-E.pdf

الوصف	الخصائص الأساسية
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.	الخدمة الذاتية عند الطلب
تتوفر الإمكانيات عبر الشبكة ويمكن الوصول إليها من خلال الآليات القياسية التي تعزز الاستخدام بواسطة منصات العمل الرقيقة أو السميكة غير المتجانسة (مثل الهواتف المحمولة وأجهزة الكمبيوتر المحمولة وأجهزة المساعد الرقمي الشخصي).	الوصول إلى شبكة واسعة
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 العمل 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.	تجميع الموارد
يمكن توفير القدرات بسرعة ومرونة، في بعض الحالات تلقائياً، للتوسع بسرعة، وإطلاقها بسرعة لتوسيع نطاقها بسرعة. وبالنسبة لمستخدم الخدمة السحابية، غالباً ما تبدو الإمكانيات المتاحة للتزويد غير محدودة ويمكن شراؤها بأي كمية في أي وقت.	المرونة السريعة
تتحكم الأنظمة السحابية تلقائياً في استخدام الموارد مع الاستفادة المثلى 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 مُقدّم الخدمة السحابية ومستخدم الخدمة السحابية للخدمة المُستخدمة.	الخدمة المُقاسة

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:

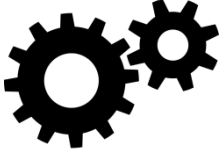
3. نماذج الخدمة

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:



Software as a Service SaaS

- The capability provided to the consumer is to use the provider's applications running 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 select networking components.



البرمجيات كخدمة (سaaS)

- 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 (PaaS)

- 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 قادرًا 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.

4. Deployment models

4. نماذج النشر

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 clouds³⁵.

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.³⁶

Deployment Model	Description
<p>Private cloud</p> 	<p>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.</p>
<p>Public cloud</p> 	<p>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 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 to provide web-based email, online office applications, storage, and testing and development environments.</p>
<p>Hybrid cloud</p> 	<p>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, you can use the public cloud for high-volume, lower-security needs such as web-based email, and the private cloud (or other on-premises infrastructure) for sensitive, business-critical operations like financial reporting. 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.</p>

³⁵ Such deployments models are described at <https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/>
³⁶ يتم وصف نماذج النشر هذه على [/https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds](https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/)

الوصف	نموذج النشر
<p>تتكون السحابة الخاصة من موارد الحوسبة المستخدمة حصرياً من قبل شركة أو مؤسسة واحدة. ويمكن أن تكون السحابة الخاصة موجودة فعلياً في مركز البيانات في مؤسستك أو يمكن استضافتها من قبل مُقدم 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 قبل الوكالات الحكومية والمؤسسات المالية وأي منظمات أخرى متوسطة إلى كبيرة الحجم ذات عمليات هامة في الأعمال التجارية تسعى إلى تعزيز السيطرة على بيئتها.</p>	<p>السحابة الخاصة</p> 
<p>تُعتبر السحابة العامة هي الطريقة الأكثر شيوعاً لنشر الحوسبة السحابية. حيث أن الموارد السحابية (مثل الخوادم ووحدات التخزين) مملوكة لمقدم خدمة سحابية تابع لجهة خارجية ويتم تشغيلها بواسطة وتسليمها عبر الإنترنت. ويُعد "مايكروسوفت أزور" 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 والتخزين وأجهزة الشبكة مع المنظمات الأخرى أو "مستأجري" السحابة. كما يمكنك الوصول إلى الخدمات وإدارة حسابك باستخدام متصفح الويب. ويتم استخدام عمليات النشر السحابية العامة بشكل متكرر لتوفير البريد الإلكتروني على الويب، وتطبيقات المكتب عبر الإنترنت وبيئات التخزين والاختبار والتطوير.</p>	<p>السحابة العامة</p> 
<p>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 الأمان الكبيرة وذات الحجم المنخفض مثل البريد الإلكتروني على الويب والسحابة الخاصة (أو غيرها من البنية التحتية على جهاز العميل) للعمليات الحساسة والمهمة للأعمال مثل إعداد التقارير المالية. وفي السحابة المختلطة، 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.</p>	<p>السحابة الهجينة</p> 

Annex II – Table on Policy Recommendations and Regulatory Requirements

Policy Areas	Policy and Regulatory Recommendations	Relevant Legislative Instrument	Timeline for Adoption/Update
<i>Cloud-First Policy</i>	Qatar shall develop a common policy for public procurement of cloud services by government entities, that is consistent with the principles of the Cloud Policy.	Cloud-First Policy, Procurement Law	
<i>Data Localization, Free Flow of Data, Non-Personal Data</i>	Legislative solutions should not enforce data localization as a restriction to cloud adoption. Data residency is no longer, a requirement as security and encryption technologies now provide a sufficient level of security. As a result, the legislations should provide instead for an array of mechanisms to allow data to flow whilst ensuring that an adequate level of protection is in place.	Cloud-First Policy/Cybersecurity law, Privacy Law, International Agreements, Cloud Security Policy of MoTC, Standard Contractual Clauses, Binding corporate rules	
<i>Privacy and access to data, Cross Borders Requests,</i>	Cross-border requests for data should be made through Mutual Legal Assistance Treaties ("MLATs"), 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	

Annex II – Table on Policy Recommendations and Regulatory Requirements

Policy Areas	Policy and Regulatory Recommendations	Relevant Legislative Instrument	Timeline for Adoption/Update
<i>Data Classification</i>	Clear guidelines around classification of data and associated security controls should be established to guide private and public sector users. In case the location of certain data needed to be restricted, this should be done by restricting the scope of such requirements to classified government data.	Cloud-First Policy/Cybersecurity Law, Government Data Classification Policy	
<i>Data interoperability and data portability</i>	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.	CRA Ruling, Telecom Law, Standard Contractual Clauses	

Draft for

Annex II – Table on Policy Recommendations and Regulatory Requirements

Policy Areas	Policy and Regulatory Recommendations	Relevant Legislative Instrument	Timeline for Adoption/Update
<i>Liability regime</i>	<p>Establish a regulatory regime with an appropriate level of regulation and limits in terms of liability regarding data stored and processed.</p> <p>The State will refrain from imposing intermediary liability on Cloud Service Providers for third party content in order to encourage user services innovation and promote the widespread availability of cloud services to public and private users.</p> <p>Cloud Service Providers should be able to limit or exclude their liability in compliance with the applicable law.</p>	E-commerce Law, Trusted Data Law, Standard Contractual Clauses	
<i>Security Standards</i>	<p>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.</p>	International standardization rules, Codes of Conduct, Certifications, Standard Contractual Clauses	

Annex II – Table on Policy Recommendations and Regulatory Requirements

Policy Areas	Policy and Regulatory Recommendations	Relevant Legislative Instrument	Timeline for Adoption/Update
<i>Service Level Agreements (SLAs)</i>	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	
<i>Hosting and Connectivity</i>	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	
<i>Environmental sustainability</i>	Cloud service Providers and government entities must commit to principles of environmental sustainability, including energy efficiency and carbon neutrality.		

الملحق الثاني - جدول متطلبات التوصيات والقواعد التنظيمية السياسية

الجدول الزمني للاعتماد / التحديث	الصكوك التشريعية ذات الصلة	التوصيات السياسية والتنظيمية	مجالات السياسة
	سياسة السحابة أولاً / قانون المشتريات	يتعين أن تضع دولة قطر سياسة مشتركة للمشتريات العامة للخدمات السحابية من قبل الجهات الحكومية تتوافق مع مبادئ سياسة السحابة.	سياسة السحابة أولاً
	سياسة السحابة أولاً / قانون الأمن السيبراني، وقانون الخصوصية، والاتفاقيات الدولية، وسياسة أمن السحابة الخاصة بوزارة النقل والاتصالات البنود التعاقدية القياسية، قواعد الملزمة للشركة	لا ينبغي للحلول التشريعية أن تفرض توطین البيانات باعتباره قيد على اعتماد السحابة. ولم تعد إقامة البيانات شرطاً، حيث توفر تقنيات الأمان والتشفير مستوى كافٍ من الأمان. ونتيجة لذلك، ينبغي للتشريعات أن توفر بدلا من ذلك مجموعة من الآليات التي تسمح بتدفق البيانات مع ضمان وجود مستوى مناسب من الحماية.	توطین البيانات، التدفق الحر للبيانات، البيانات غير الشخصية
	قانون حماية البيانات، قانون البيانات الموثوق بها، الاتفاقيات المتعددة الأطراف، اتفاقيات المساعدة القانونية المتبادلة، البنود التعاقدية القياسية	الشفافية واليقين هما مفتاح أصحاب المصلحة، خاصة فيما يتعلق بالقواعد التي تنظم الوصول إلى بيانات الطلبات عبر الحدود. ويجب تقديم الطلبات عبر الحدود للحصول على البيانات من خلال معاهدات المساعدة القانونية المتبادلة وضمن المشاركة المناسبة للسلطات في البلدان التي يتم فيها تخزين البيانات.	الخصوصية والوصول إلى البيانات، والطلبات عبر الحدود
	سياسة السحابة أولاً / قانون الأمن السيبراني وسياسة تصنيف البيانات الحكومية	يجب وضع إرشادات واضحة حول تصنيف البيانات والضوابط الأمنية المرتبطة بها لتوجيه مستخدمي القطاع العام والخاص. وفي حالة الحاجة إلى تقييد موقع بيانات معينة، يجب أن يتم ذلك عن طريق قصر نطاق هذه المتطلبات على البيانات الحكومية التي هي على درجة عالية من السرية.	تصنيف البيانات
	قواعد هيئة تنظيم الاتصالات وقانون الاتصالات والبنود التعاقدية القياسية	يتعين اعتماد معايير معترف بها دولياً بشأن التشغيل البيئي للخدمات السحابية عند التعاقد على الخدمات السحابية وفي عقود المشتريات العامة. كما تُعد إمكانية التشغيل البيئي للخدمات السحابية شرطاً أساسياً لضمان إمكانية نقل الخدمات لمستخدمي السحابة.	إمكانية التشغيل البيئي للبيانات وإمكانية نقل البيانات

	قانون التجارة الإلكترونية وقانون البيانات الموثوقة والبنود التعاقدية القياسية	إنشاء قواعد تنظيمية بمستوى مناسب من التنظيم وحدود من حيث المسؤولية فيما يتعلق بالبيانات المخزنة والمعالجة. ستمتنع الدولة عن فرض المسؤولية الوسيطة على مقدمي الخدمات السحابية لمحتوى الغير لتشجيع ابتكار خدمات المستخدمين وتعزيز التوافر الواسع للخدمات السحابية للمستخدمين العام منهم والخاص.	قواعد المسؤولية
	القواعد الدولية للمعايير ومدونات قواعد السلوك والشهادات والبنود التعاقدية القياسية	يجب أن يكون متاحًا 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 دوليًا. ويجب تجنب إنشاء المعايير المحلية أو ازدواجية المعايير المعترف بها دوليًا حيث يمكن أن يكون ذلك ضارًا بتطوير صناعة سحابية متينة.	معايير الأمن
	سياسة السحابة الأولى والبنود التعاقدية القياسية	يجب أن تكون اتفاقيات مستوى الخدمة موضوعة لضمان الشروط المتفق عليها لتقديم الخدمات. إذ تحتاج الخدمات السحابية الموثوقة إلى مقدمي الخدمات والمستهلكين للاتفاق على معلمات مستويات الخدمة (الأداء والتوافر والفواتير) التي يتم تقديمها في المنتج السحابي. كما سيساعد اعتماد الشروط والأحكام الموحدة لاتفاقيات مستوى الخدمة السحابية بما يتماشى مع المعايير الدولية على تعزيز ثقة الجمهور في الخدمات السحابية.	اتفاقيات مستوى الخدمة
	قواعد هيئة تنظيم الاتصالات	تعد أسعار التوصيل الدولي عنصرًا حاسمًا لاختيار المستثمرين ويجب أن تتماشى مع المعايير الدولية. كما يجب ضمان التوصيل الدولي بالطرق المتعددة المختلفة.	الاستضافة والتوصيل
		يجب أن يلتزم مقدمو الخدمات السحابية والهيئات الحكومية بمبادئ الاستدامة البيئية بما في ذلك كفاءة الطاقة ومحايدة الكربون.	الاستدامة البيئية

Annex III – The CRA Strategy 2020-2024

Qatar's government is committed to supporting the development of data centers and cloud infrastructure in Qatar to host its ambitious digitalization plan. Therefore, within the 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 action 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).

However, currently there are very few Tier 3 data centers and no Tier 4³⁷ data centers in the country,

الملحق الثالث - استراتيجية هيئة تنظيم الاتصالات 2020 - 2024

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

وعلاوةً على ذلك، فإن أحد الإجراءات الرئيسية لاستراتيجية هيئة تنظيم الاتصالات 2020 - 2024 هو "تطوير استراتيجية لتوريد الخدمات السحابية ومراكز البيانات داخل دولة قطر. وستكون هذه الاستراتيجية واسعة النطاق وستدرس عوامل العرض والطلب. وستقيم المُعوقات الحالية والمستقبلية في نمو مراكز البيانات والخدمات السحابية، مثل الاستثمار والابتكار والأمن والتنظيم وشروط الوصول والتنسيق مع الحكومة". ويُعد الهدف من الاستراتيجية السحابية هو زيادة المعروض من سعة مركز البيانات وتقديم أفضل الخدمات السحابية للهيئات الحكومية والقطاع الخاص. ويُعد وجود سوق تنافسي لتوريد الخدمات السحابية وكفاءة مركز البيانات أمرًا ضروريًا لتطوير صناعة تكنولوجيا المعلومات الحديثة. حيث أنه يوجد بالفعل لاعبون مهمون تم تأسيسهم بالفعل في هذا السوق في دولة قطر (مثل أريذ وفودافون وميزة).

ومع ذلك، يوجد حاليًا عدد قليل جدًا من مراكز بيانات من المستوى 3 ولا توجد مراكز بيانات من المستوى 4³⁸ في الدولة، مما يشير إلى أن

³⁷ Tier 4 data center certification typically serve enterprise corporations and provide the following:

- 99.995% uptime per year (Tier 4 uptime)
- 2N+1 fully redundant infrastructure (the main difference between tier 3 and tier 4 data centers)
- 96-hour power outage protection
- 26.3 minutes of annual downtime

³⁸ عادةً ما تستخدم شهادة مركز البيانات من المستوى 4 شركات المؤسسات وتوفر ما يلي:

- وقت تشغيل بنسبة 99.995٪ سنويًا (وقت تشغيل من المستوى 4)
- بنية أساسية 1+N2 متكررة بالكامل (الفرق الرئيسي بين مراكز البيانات من المستوى 3 والمستوى 4)
- حماية من انقطاع التيار الكهربائي لمدة 96 ساعة
- 26.3 دقيقة من التعطل السنوي

indicating that Qatar has less capacity than other countries in the region, which impacts strongly Qatar attraction in terms of direct investment. 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. The development of Tier 4 data centers is, therefore, a key part of the Cloud Policy.

دولة قطر لديها قدرة أقل من الدول الأخرى في المنطقة مما يؤثر بقوة على جذب قطر للاستثمار المباشر. كما أن هناك مؤشرات على أن سعر خدمات السحابة ومراكز البيانات في قطر مرتفع بالمقارنة مع المعايير الإقليمية. وستتطلب زيادة المعروض من سعة مراكز البيانات في قطر نهجاً استباقياً من قبل الحكومة لضمان بناء بنية تحتية كافية وأن مركز البيانات وسوق الخدمات السحابية يعملان بفاعلية.

لتلبية احتياجات الاتجاه نحو استخدام الحوسبة السحابية على نطاق واسع، ستحتاج سعة مركز البيانات في قطر إلى النمو. وبالتالي، فإن تطوير مراكز بيانات من المستوى 4 هو جزء أساسي من سياسة السحابة.

Annex IV

Consultation Questions

Question 1. Do you have any comments or suggestions on the Cloud Policy Statement?

Question 2. Do you share the objectives indicated in the Cloud Policy Statement?

Question 3. Do you agree on the proposed approach regarding the policy and regulatory recommendations for the development of cloud computing?

Question 4. Do you have any comments or suggestions on the policy and regulatory recommendations? Please make your comments and suggestions for each of the recommendations listed on the Cloud Policy Statement (Part 4 and related paragraphs)

Question 5. Do you have any suggestions for areas on which the CRA should further develop policy and regulatory recommendations?

الملحق الرابع

أسئلة استشارية

السؤال 1: هل لديك أي ملاحظات أو اقتراحات بشأن وثيقة سياسة السحابة؟

السؤال 2: هل تشارك الأهداف المشار إليها في وثيقة سياسة السحابة؟

السؤال 3: هل توافق على النهج المقترح فيما يتعلق بالسياسات والتوصيات التنظيمية لتطوير الحوسبة السحابية؟

السؤال 4: هل لديك أي ملاحظات أو اقتراحات بشأن التوصيات السياسية والتنظيمية؟ يرجى تقديم ملاحظتك واقتراحاتك لكل من التوصيات المدرجة في وثيقة سياسة السحابة (الجزء 4 والفقرات ذات الصلة)

السؤال 5: هل لديك أي اقتراحات بشأن المجالات التي يجب على هيئة تنظيم الاتصالات أن تطور فيها التوصيات السياسية والتنظيمية؟

Annex V
Consultation Response Template

الملحق الخامس
نموذج الرد على الاستشارة

Respondent	Consultation document reference (question/paragraph)	Response
(company/organization name)	(specify question or paragraph number that response refers to)	(provide comments)

الرد	مرجع وثيقة الاستشارة (السؤال / الفقرة)	الشخص المُستجيب
(تقديم ملاحظات)	(تحديد السؤال أو رقم الفقرة الذي يشير إليه الرد)	(اسم المؤسسة / او الشركة)