الدليل الارشادي لمشتركي خدمات الحوسبة السحابية
دولة الكويت

V1.5

الهيئة العامة للاتصالات وتقنية المعلومات

الفهرس

المقدمة

تحرص الهيئة العامة للاتصالات وتقنية المعلومات على تفعيل دورها الرقابي والتنظيمي بموجب قانون انشائها رقم 37 لسنة 2014 والمعدل بالقانون رقم 98 لسنة 2015، بوضع لوائح لتنظيم قطاعي الاتصالات وتقنية المعلومات بما يتفق مع السياسة العامة للدولة لتحقيق التنمية الشاملة. واستنادا على ذلك فقد تم إنشاء مستند الإطار التنظيمي للحوسبة السحابية لتنظيم استخدام خدمات الحوسبة السحابية داخل دولة الكويت. كما قامت الهيئة بإنشاء هذا الدليل ليدعم الإطار فيما يخص ارشاد مشتركي خدمات الحوسبة السحابية من جهات حكومية أو خاصة، بالإضافة إلى المشتركين الأفراد، الى أوجه الاستفادة من خدمات الحوسبة السحابية والمسؤوليات المترتبة عليهم.

يهدف هذا الدليل الى تسليط الضوء على مفاهيم الحوسبة السحابية بشكل عام والخدمات التابعة لها والتي يمكن للمشتركين الاستفادة منها، بالإضافة الى توضيح الجوانب الأخرى الهامة المتعلقة بتنظيم الحوسبة السحابية المقدمة إليهم مثل: حماية بياناتهم وتصنيفها، أمن معلوماتهم (الأمن السيبراني)، وحمايتهم كمشتركين وتوضيح ما يترتب من مسؤوليات عليهم وفق الإطار التنظيمي للحوسبة السحابية.

نظرة عامة على الحوسبة السحابية

أثارت الحوسبة السحابية ثورة في التقدم والتطور التقني لتكنولوجيا المعلومات والاتصالات، حيث يقوم العديد من المشتركين من الأفراد أو الحكومات أو قطاعات الأعمال في دول العالم باستخدام الحوسبة السحابية نظراً لما توفره من مزايا عديدة في مختلف المجالات، إداريةً كانت أو تقنية، من شأنها المساهمة في تسهيل إجراءات الأعمال وإتاحتها بسهولة ويسر من خلال اتصال بسيط بالشبكة من أي مكان. فعلى سبيل المثال لا الحصر: أصبح بالإمكان عقد اجتماعات العمل إلكترونياً عبر الشبكة، كما أصبح إتمام العديد من المعاملات الكترونياً متاحاً للأفراد والمؤسسات باستخدام الأجهزة الذكية (على سبيل المثال لا الحصر: الهواتف الذكية، أجهزة التلفزة الذكية، الحواسيب). يسلط هذا الفصل الضوء على المعلومات العامة مثل الخصائص الأساسية للحوسبة السحابية، نماذج تثبيت الحوسبة السحابية، ونماذج الخدمة المتوفرة على الحوسبة السحابية.

المصطلحات الواردة في هذا المستند هي ما تم تعريفه من قبل المعهد الوطني للمعايير والتكنولوجيا (NIST) بالإضافة الى التعريفات المذكورة في سياسة الحوسبة السحابية أولاً والإطار التنظيمي للحوسبة السحابية، ويمكن مراجعتها عن طريق الموقع الرسمي للهيئة العامة للاتصالات وتقنية المعلومات (www.citra.gov.kw).

الخصائص الأساسية للحوسبة السحابية

1. **خاصية الخدمة الذاتية حسب الطلب:** يستطيع المشترك من جانبه توفير إمكانيات الحوسبة، مثل النطاق الزمني (time zone) لوقت الخادم (server time) والتخزين عبر الشبكة (network storage)، حسب الحاجة تلقائيًا دون الحاجة إلى طلب ذلك من مقدم الخدمة.
2. **خاصية الوصول الواسع للشبكة:** تتوفر الخدمات والإمكانيات عبر الشبكة ويمكن الوصول إليها من خلال الوسائط المتعددة الثابتة والمحمولة مثل الهواتف المحمولة والحواسيب المكتبية واللوحية والمحمولة.
3. **خاصية تجميع الموارد:** يتم تجميع موارد الحوسبة لمقدم الخدمة من أجل خدمة عدد من المشتركين في نفس الوقت. تتم هذه العملية عن طريق تفعيل نموذج تعدد مستأجري موارد الحوسبة (multi-tenant model) الذي يقوم بدوره في تخصيص وإعادة تخصيص تلك الموارد لكل مشترك حسب الحاجة. كما يضمن نموذج تعدد مستأجري موارد الحوسبة عازلية عمليات وبيانات كل مشترك عن باقي المشتركين كما يضمن عدم قابلية النفاذ غير المخول الى بيانات كل مشترك من المشتركين الآخرين. وتتضمن الأمثلة على خاصية تجميع الموارد: مساحات التخزين والمعالجة والذاكرة وسعة نطاق الشبكة والحواسيب الافتراضية.
4. **خاصية المرونة والسرعة:** هذه الخاصية تمكن المشتركين من توفير الموارد حسب حاجتهم بشكل سريع وسلس وتلقائي (في بعض الحالات) من أجل التوسع السريع او التقلص في حجم ومساحة الموارد بما يتناسب مع حاجة المشتركين. تظهر الموارد للمشترك على أنها غير محدودة ويمكن تخصيصها بأي كمية وفي أي وقت.
5. **خاصية قياس الخدمة:** تتحكم أنظمة السحابة تلقائيًا في استخدام الموارد وتحسينها عن طريق تفعيل دور خاصية القياس الموجودة لدى أنظمة السحابة بشكل يتناسب مع نوع الخدمة ومنها على سبيل المثال: التخزين والمعالجة وعرض النطاق وحسابات المشتركين النشطة. كما يمكن مراقبة استخدام الموارد والتحكم فيها والإبلاغ عنها، مما يوفر الشفافية بالنسبة للخدمة المقدمة لكل من مقدم الخدمة والمشترك الذي يستخدم تلك الخدمات.

نماذج تثبيت الحوسبة السحابية

يمكن للمشترك اختيار نماذج تثبيت الحوسبة السحابية الآتية التي تلائم مدى حساسية وسرية ومتطلبات أمن البيانات الخاصة به المحمية والمصنفة وفق سياسة تصنيف البيانات والإطار التنظيمي للحوسبة السحابية ولائحة حماية خصوصية البيانات الصادرين عن الهيئة.

1. **الحوسبة السحابية العامة (Public Cloud):** يتم توفير البنية التحتية للسحابة للاستخدام العام من قبل الجمهور. قد تكون هذه البنية مملوكة ومدارة ومشغلة من قبل مؤسسة تجارية أو أكاديمية أو جهة حكومية، أو مزيج منهم. وأن تكون موجودة على موقع/مركز مزود او مقدم الخدمة.
2. **الحوسبة السحابية الخاصة (Private Cloud)** يتم توفير البنية التحتية للسحابة للاستخدام الحصري من قبل جهة او شركة واحدة تضم العديد من المستخدمين (على سبيل المثال: الأقسام والإدارات التي تديرها تلك الجهة او الشركة) وتشغل من قبل الجهة\الشركة ذاتها، أو من قبل طرف ثالث (مثل: مقدم خدمات الحوسبة السحابية)، أو كليهما معاً، وقد يكون موقعها المادي داخل مقر الجهة\الشركة أو خارجها. وتدير الجهة\الشركة بنفسها عملية نسخ البيانات، وفي هذه الحالة، يستهلك تطوير الحلول وقتاً أطول نظراً لأن جميع عمليات النشر والاختبار يلزم تنفيذها داخل الجهة\الشركة.
3. **الحوسبة السحابية المشتركة (Community Cloud):** يتم توفير البنية التحتية للسحابة للاستخدام الحصري من قبل مجموعة محددة من المستخدمين الذين ينتمون الى جهات\شركات لديها مصالح مشتركة\متوافقة (على سبيل المثال: مهام الجهة\الشركة، متطلبات الأمن السيبراني، واعتبارات الامتثال). قد تملك هذه البنية التحتية وتديرها وتشغلها جهة\شركة واحدة أو أكثر من الجهات\الشركات المشمولة في تلك المجموعة، أو طرف ثالث (مقدم الخدمة)، أو كلاهما، وقد يكون موقعها المادي داخل مقر الجهة\الشركة أو خارجها. ويتولى مقدم الخدمة إدارة عملية نسخ البيانات (تحقيقاً لاتفاقية مستوى الخدمة (SLA) بين مقدم الخدمة والجهة\الشركة) حيث يدعم هذا النموذج تسريع آلية التثبيت والتشغيل الفوري مما يؤدي إلى تسريع عملية نشر الحلول الجديدة.
4. **الحوسبة السحابية الهجينة (Hybrid Cloud):** البنية التحتية لهذا النوع من السحابة عبارة عن تركيبة لبنيتين أو أكثر من البنى التحتية لأنواع الحوسبة السحابية التي تم ذكرها (الخاصة، أو العامة، أو المشتركة) حيث تبقى كل بنية فريدة في ذاتها وخصائصها، ولكنها مرتبطة ببعضها البعض بتقنية ذات معايير قياسية أو تقنية ذات ملكية

خاصة تُمَكِّن من الربط بين كل بنية سحابية إضافة إلى تمكين نقل البيانات والتطبيقات. على سبيل المثال: قد يتم تحويل المنصة السحابية الخاصة إلى منصة عامة لموازنة الحمل بين منصات الحوسبة السحابية المرتبطة.

نماذج الخدمة للحوسبة السحابية

1. **البرمجيات كخدمة (SaaS):** نموذج توزيع البرامج الذي يستضيف فيه مقدم الخدمة التطبيقات ويجعلها متاحة لمستخدمي خدمات الحوسبة السحابية عبر الإنترنت. ومنها على سبيل المثال لا الحصر: التطبيقات، خدمات الويب (Web Services)، الحواسب الافتراضية، نظم إدارة علاقات العملاء (CRM).
2. **المنصة كخدمة (PaaS):** في هذا النموذج، يوفر مقدم الخدمة البيئة التي تتضمن الأجهزة وأدوات البرامج المطلوبة لتطوير التطبيقات عبر الإنترنت. ويستضيف مقدم الخدمة الأجهزة والبرامج على بنيته التحتية الخاصة وبالتالي يعفي المشتركين من شراء بنية تحتية لتثبيت حلول تكنولوجيا المعلومات والاتصالات الجديدة، ومنها على سبيل المثال لا الحصر: تطوير التطبيقات، قواعد البيانات، البرمجيات الوسيطة، أدوات الاختبار وأدوات المطورين.
3. **البنية التحتية كخدمة (IaaS):** في هذا النموذج، يستضيف مقدم الخدمة مكونات البنية التحتية التي تشكل مركز بيانات مثل الخوادم، والتخزين، وأجهزة الشبكات، وطبقة التمثيل الافتراضي (virtualization layer) للمشتركين. ولا يدير المستخدم أو يتحكم في البنية التحتية السحابية الأساسية لكنه يتحكم في نظام التشغيل والتخزين والتطبيقات وبعض أنظمة الحماية، ومنها على سبيل المثال لا الحصر: الحواسيب المركزية، التخزين، موزعات الحمل (Load Balancers) والأجهزة الافتراضية (Virtual Machines).

ويوضح الجدول التالي المسؤوليات المترتبة على مقدم الخدمة وعلى المشتركين حسب نوعية نموذج الخدمة:

SaaS	PaaS	IaaS
يديرها مقدم الخدمة	**يديرها المشترك**	**يديرها المشترك**
التطبيقات والبرامج	التطبيقات والبرامج	التطبيقات والبرامج
أنظمة الحماية والأمن	**يديرها مقدم الخدمة**	أنظمة الحماية والأمن
قواعد البيانات	أنظمة الحماية والأمن	قواعد البيانات
أنظمة التشغيل	قواعد البيانات	أنظمة التشغيل
الأنظمة الافتراضية	أنظمة التشغيل	**يديرها مقدم الخدمة**
الخوادم	الأنظمة الافتراضية	الأنظمة الافتراضية
التخزين	الخوادم	الخوادم
الشبكات	التخزين	التخزين
مراكز البيانات	الشبكات	الشبكات
	مراكز البيانات	مراكز البيانات

نماذج خدمات الحوسبة السحابية ومسؤوليات إدارتها

أمثلة لخدمات الحوسبة السحابية المتاحة للجهات الحكومية

هذا الفصل يسلط الضوء على بعض خدمات الحوسبة السحابية المستخدمة التي يمكن للجهات الحكومية الاستفادة منها على سبيل المثال لا الحصر: مساحات التخزين، أنظمة تقنية المعلومات، منصات الإنتاجية التي تعمل على الحوسبة السحابية، التطبيقات المؤسسية، منصات التواصل الاجتماعي.

1. مساحات التخزين

توفر الحوسبة السحابية خدمات تخزين ومعالجة البيانات والمعلومات للجميع، حيث يتميز التخزين على الحوسبة السحابية بسهولة الوصول عبر مجموعة من الأجهزة الذكية المتنوعة كالهواتف المتنقلة وأجهزة الحواسيب المكتبية والمحمولة على سبيل المثال لا الحصر.

لدى الجهات الحكومية كمية كبيرة من البيانات، وبالتالي فإن احتياجات الجهات الحكومية الى مساحات التخزين يزداد بشكل سريع. وبسبب حساسية بعض البيانات المتوفرة لدى الجهات الحكومية، فإن مخاطر فقدانها او اختراقها قد يلحق بضرر كبير على تلك الجهات، لذا يعتبر أمن تلك البيانات ومواقع تخزينها من الأولويات الهامة لدة الجهات الحكومية. كما ان معالجة وتخزين البيانات لدى الجهات الحكومية قد يأخذ وقتاً طويلاً حسب طبيعة إجراءات العمل المعمول بها في الجهات الحكومية وحسب حساسية تلك البيانات. بالإضافة الى ذلك فإن الجهات الحكومية تحتاج الى أرشفة بعض البيانات التي قد تكون قديمة ولكن يجب الحفاظ عليها لفترة زمنية قد تمتد لسنوات وان كانت غير مستخدمة. لذلك فإن الجهات الحكومية تحتاج الى مساحات تخزين كبيرة وذات درجة عالية من الأمان وتتميز بسهولة الوصول اليها ومعالجتها وفق ما تحدده الجهات الحكومية من ضوابط نفاذ وغيرها من متطلبات الأمن والوصول، وتكون الحلول التقليدية باهظة التكاليف في غالب الأحيان حيث تقوم الجهات بتخصيص ميزانيات كبيرة من أجل انشاء وإدارة وتوسعة مراكز البيانات الخاصة بها وذلك للحفاظ على بياناتها.

توفر الحوسبة السحابية الحلول النموذجية منخفضة التكاليف اذا ما تم مقارنتها بالأنظمة التقليدية، وتعطي الحلول لجميع الأمور التي ذكرت في الفقرة السابقة، اذ يوفر التخزين عبر الحوسبة السحابية الضمان بعدم ضياع أو تلف البيانات والمعلومات المخزنة وتوفرها على الدوام بسهولة ويسر للمخولين من الجهة الحكومية وتوفر الموارد بشكل تلقائي حسب حاجة الجهات الحكومية، كما يقوم مقدم الخدمة بتوفير مساحات تخزين مجانية (حسب ما تم التعاقد عليه بين الجهة وبين مقدم الخدمة وحسب اتفاقية مستوى الخدمة) لموظفي تلك الجهات لاستخداماتهم الشخصية او المهنية.

2. أنظمة تقنية المعلومات

تستطيع الجهات الحكومية في وقتنا الحاضر من إدارة أنظمتها المتعلقة بتقنية المعلومات عن بعد بفضل الحوسبة السحابية والاستغناء عن إدارة الأنظمة التقليدية داخلياً كما هو معمول به، وذلك عن طريق نقلها الى الحوسبة السحابية لمقدم الخدمة. وبالتالي يمكن للجهات الحكومية من تقليل التكاليف التي تقوم بصرفها على أجهزة ومعدات مراكز البيانات التقليدية بالإضافة الى تكاليف إدارتها بشكل كبير الى تكلفة بسيطة تعتمد على حيز استخدام الجهة للحوسبة السحابية.

ويمكن للجهات التي ترغب بالتحكم ببرامجها وتطبيقاتها بالإضافة الى بياناتها بشكل كامل استخدام نموذج البنية التحتية كخدمة (IaaS) الذي يوفره مقدم الخدمة، حيث يقوم مقدم الخدمة في هذا النموذج بتوفير بيئة الحوسبة السحابية التي تشكل مركز بيانات يمكن للجهات الحكومية من تثبيت تطبيقاتها وبرامجها وتخزين بياناتها عليه وإدارتها بشكل كامل.

3. منصات الإنتاجية التي تعمل على الحوسبة السحابية

يقوم مقدم الخدمة بتوفير نموذج المنصة كخدمة (PaaS) للجهات الحكومية والتي تمكنهم من تطوير التطبيقات والبرمجيات عليها دون الحاجة الى القلق بشأن موارد الحوسبة السحابية اللازمة لهذه المنصة. وبالتالي تمكن هذه الخدمة الجهات الحكومية من التركيز على تطوير التطبيقات والبرمجيات المختلفة التي تلبي احتياجاتها.

4. التطبيقات المؤسسية

يقوم مقدم الخدمة بتوفير التطبيقات المؤسسية للجهات الحكومية (على سبيل المثال لا الحصر تطبيقات إدارة علاقات العملاء، أو تطبيقات معالجة النصوص والجداول والعرض المرئي). حيث تتوفر هذه التطبيقات للمشتركين مقابل اشتراك شهري للاستخدام، حيث يوفر هذا النموذج التكاليف الكثيرة على الجهات الحكومية لشراء مثل هذه التطبيقات واستضافتها على مراكز البيانات لديها. ويقوم مقدم الخدمة بإدارة هذه التطبيقات بشكل كامل (وفق نموذج البرمجيات كخدمة SaaS) بحيث يعفي المشتركين من إدارتها. ويمكن هذا النوع من التطبيقات الجهات الحكومية من التركيز على تحسين جودة الخدمات التي تقدمها للأفراد والمؤسسات والجهات الحكومية الأخرى والجوانب الأخرى وفقاً لمهامها والتزاماتها.

5. الحوسبة السحابية الحكومية

أصبح الربط بين الجهات الحكومية ومؤسسات القطاع العام في دولة الكويت ضرورة ملحة كجزء من التحول الرقمي الحكومي، وذلك لأهداف عديدة منها على سبيل المثال لا الحصر: تسهيل التواصل بين الجهات وتمكين تلك الجهات من تيسير وتبسيط الخدمات المقدمة الى الجمهور وفاءً لالتزاماتها نحوهم. وتوفر الحوسبة السحابية هذه الإمكانية للجهات الحكومية، اذ تستطيع الجهات الحكومية من تشغيل وإدارة الحوسبة السحابية الحكومية بشكل كامل أو جزئي عن طريق التعاقد مع مقدمي الخدمة.

وتتيح الحوسبة السحابية الحكومية توفير منصة آمنة يتم من خلالها تقديم الخدمات الحكومية المختلفة للمواطنين والمقيمين في الدولة بسهولة ويسر بالإضافة الى تمكين الجهات الحكومية من الربط فيما بينها بفاعلية مع مراعاة جميع جوانب أمن المعلومات وسريتها، إذ يمكن للجهات اختيار نوعية الخدمات التي تود مشاركتها وربطها من خلال الحوسبة السحابية الحكومية مع الجهات الأخرى، كما بإمكان الجهات من عزل بعض العمليات والبيانات التي ترى أنها حساسة ولا يجب ربطها او مشاركتها مع الجهات الحكومية ضمن الحوسبة السحابية الحكومية.

6. منصات التواصل الاجتماعي

أصبحت منصات ومواقع التواصل الاجتماعي جزء لا يتجزأ من حياتنا اليومية، ولأنها تعتبر من خدمات الحوسبة السحابية التي تتوفر للمشتركين، فإنها توفر للمشتركين من الجهات الحكومية منصات الحوسبة اللازمة لتمكينهم من التواصل الاجتماعي مع المواطنين والمقيمين بالإضافة الى الشركات والمؤسسات والجهات الأخرى، ويمكن للمشتركين من هذه الشركات تحميل الصور ومقاطع الفيديو والآراء والاستفتاءات والمقالات أو الإعلانات الرسمية المتعلقة بالقرارات الحكومية الرسمية او الخدمات التي تقوم تلك الجهات بتقديمها والتي تهم الجمهور.

المسؤوليات المترتبة من الإطار التنظيمي للحوسبة السحابية على مشتركي الجهات الحكومية

قام الإطار التنظيمي للحوسبة السحابية بتحديد الأحكام والضوابط العامة المترتبة على التعاقد بين المشتركين وبين مقدمي خدمات الحوسبة السحابية. وفي حال المشتركين من القطاع العام فإنه من المهم معرفة ما يترتب عليهم من استخدام خدمات الحوسبة السحابية بشأن: أمن المعلومات وتصنيف البيانات، حماية البيانات، وحماية المشتركين.

1. أمن المعلومات وتصنيف البيانات

يعتبر أمن المعلومات الوسيلة اللازمة للحماية ضد اختراق البيانات ويتعلق أمن المعلومات بمسؤولية كل من:

- مقدم خدمات الحوسبة السحابية وذلك عن طريق استخدام المعايير الدولية المتعارف عليها لحماية بيئة الحوسبة السحابية الخاصة به والتأكد من سريتها وسلامتها وتوفرها بالإضافة الى الالتزام بما يترتب عليه من التزامات حسب نموذج الخدمة الذي يوفره للمشترك (البنية التحتية كخدمة IaaS، المنصة كخدمة PaaS، البرمجيات كخدمة SaaS) كما تم تفصيله في مستند ضوابط والتزامات مقدمي خدمات الحوسبة السحابية.

- مشترك الحوسبة السحابية وذلك عن طريق:

1. اختيار مقدم الخدمة المناسب والمصرح له من الهيئة واستخدام ميزات الأمن التي يوفرها مقدم الخدمة والتأكد من قدرته على تمكين المشترك من الامتثال للقوانين واللوائح المعمول بها في دولة الكويت.
2. معرفة المسؤوليات والالتزامات التي تترتب عليه كمشترك حسب الخدمة التي يرغب بالاشتراك بها، والاطلاع على مسؤوليات مقدم الخدمة بهذا الخصوص، إذ أن استخدام الحوسبة السحابية يولد مسؤوليات مشتركة بين المشترك وبين مقدم الخدمة حسب نوعية الخدمات التي يتم التعاقد فيما بينهم عليها (البنية التحتية كخدمة، المنصة كخدمة، البرمجيات كخدمة)، وقد ذكرت بشكل مفصل في الإطار التنظيمي للحوسبة السحابية وفي مستند ضوابط والتزامات مقدمي خدمات الحوسبة السحابية.
3. الامتثال لأحكام الإطار التنظيمي للحوسبة السحابية الخاصة بتصنيف البيانات الى أربعة مستويات حسب حساسيتها (بيانات عامة، بيانات خاصة غير حساسة، بيانات خاصة حساسة، بيانات عالية الحساسية) وضمان الامتثال لمستويات الأمن المطلوبة.

تزداد صرامة الإجراءات الأمنية المطلوبة لحماية بيانات المشتركين كلما ارتفع مستوى تصنيف تلك البيانات (وبالتالي يرتفع مستوى أمن المعلومات المطلوب). وقد يتوجب على المشتركين تشفير البيانات وزيادة مستوى هذا التشفير كلما ارتفع مستوى تصنيف هذه البيانات، كما قد يتوجب على المشترك توفير النسخ الاحتياطية من هذه البيانات بالإضافة الى أية متطلبات أمنية أخرى من المشترك أو من مقدم الخدمة. أما بالنسبة للبيانات التي تقع ضمن المستوى الرابع من التصنيف (على سبيل المثال لا الحصر: مفتاح التشفير أو المعلومات عالية الحساسية التي تتوفر لدى الجهات الحكومية كالمعلومات العسكرية او المفاوضات الدولية او تلك المتعلقة بأمن الدولة) فإنها تعامل معاملة خاصة ويقرر المشترك كيفية التعامل معها بمعرفته.

يحق للهيئة العامة للاتصالات وتقنية المعلومات من التعديل على مستويات التصنيف ومتطلباتها الأمنية او إصدار اللوائح المتعلقة بأمن المعلومات لتتناسب مع مستويات التصنيف المذكورة في الإطار مستقبلاً وفق ما تراه مناسباً.

قام الإطار التنظيمي للحوسبة السحابية بتعريف تصنيف البيانات كالتالي "هو تصنيف (أو وضع أو ترتيب) للبيانات في مستويات أمنية ملائمة بناء على مدى حساسيتها وذلك لتحديد السبل المثلى لتداولها وحمايتها من المخاطر." ووضع مسؤولية تصنيف البيانات على عاتق مالك البيانات.

وفي هذا السياق، يجب على المشترك معرفة مدى حساسية بياناته وتصنيفاتها قبل نقلها الى الحوسبة السحابية. (راجع مستند الإطار التنظيمي للحوسبة السحابية)

وبإمكان الجهات الحكومية التي لا تعمل ضمن قطاعات حساسة ولا تملك أو تتعامل مع حجم كبير من البيانات الشخصية التي تنتمي للمستوى الثالث من مستويات التصنيف أعلاه ان تقرر بكفاية معايير الأمن المتوفرة للمستوى الأول والثاني (تجدر الإشارة أن بإمكان المشترك من حجب البيانات ومحتوى المشترك الموجود على الحوسبة السحابية العامة من الاطلاع العام وفق الإعدادات المتوفرة والتي يتحكم بها المشترك) من التصنيف واستخدامه لاستضافة هذه البيانات وإن كان الخيار الطبيعي هو اختيار المستوى الثالث المذكور أعلاه. إذ ينبغي على المشترك عدم المبالغة بتصنيف بياناته ومحتوى المشترك الخاص به إذ أن معظم هذه المعلومات تقع ضمن المستوى الأول والمستوى الثاني والبعض منها يندرج تحت المستوى الثالث، والأقل من ذلك قد يندرج تحت المستوى الرابع. كما أن فقد أو ضياع بيانات أو محتوى المستوى الأول أو الثاني لن يلحق ضرراً كبيراً على المشترك. وتقوم الجهة الحكومية بتصنيف بياناتها ضمن المستوى الثالث أو المستوى الرابع بناءً على معرفتها بحجم الضرر الذي قد يقع عليها في حال اختراق هذه البيانات، خصوصاً إذا كانت تعزم على استخدام الحوسبة السحابية لمعالجة أو تخزين هذه البيانات.

ويعطي الإطار التنظيمي للحوسبة السحابية المسؤولية للمشترك (وليس لمقدم الخدمة) لاختيار مستوى أمن المعلومات المطلوب الذي يراه مناسباً بالنسبة لبياناته ومحتوى المشترك الذي يملكه على الحوسبة السحابية وإجراءات الأمن، او اختيار الإطار الذي يقدمه مقدم خدمات الحوسبة السحابية لحماية بيانات المشترك إذا رأى المشترك جدوى استخدامه لتلبية احتياجاته المحددة والتزاماته وواجباته ومتطلباته الأمنية.

كما ينبغي على كل من مقدم خدمات الحوسبة السحابية والمشترك معرفة مسؤوليات كل منهم وهي مفصلة حسب نوع نموذج الخدمة الذي تم التعاقد عليه في الإطار التنظيمي للحوسبة السحابية وفي مستند ضوابط والتزامات مقدمي خدمات الحوسبة السحابية بالإضافة الى التالي:

أ. مسؤوليات مقدم خدمات الحوسبة السحابية:

1. مسؤول عن أمن بيئة الحوسبة السحابية المتوفرة لديه وضوابط الأمن المتوفرة لديه.
2. مسؤول عن توفير مستويات الأمن التي يطلبها المشتركون
3. غير مسؤول عن مراقبة محتوى المشتركين او بياناتهم او تحديد مستوى سرية بيانات المشترك.
4. غير مسؤول عن الضرر الناجم عن اهمال المشتركين من استخدام جميع ضوابط أمن المعلومات التي يوفرها.

ب. مسؤوليات المشتركين:

1. اختيار مقدم الخدمة المناسب (خصوصاً المصرح له من الهيئة العامة للاتصالات وتقنية المعلومات) وذلك لضمان توفيره لمعايير وضوابط الأمن المناسبة لحماية بياناتهم أو محتوى المشترك الذي لديهم.
2. تحديد مستوى أمن المعلومات المناسب لطبيعة أعمال المشترك من الجهات الحكومية ومستويات تصنيف البيانات والمعلومات المتوفرة لديه المتعلقة به او المتعلقة بالأفراد.
3. مسؤول عن ضوابط الأمن والنفاذ وحقوق النفاذ وتحديد صلاحيات الاستخدام بالنسبة لموظفيهم وغيرها من إجراءات العمل المتعلقة بمعالجة واستخدام البيانات ومحتوى المشترك الذي يملكونه (إذا كان نموذج الخدمة هو المنصة كخدمة أو البرمجيات كخدمة).
4. الامتثال للإطار التنظيمي للحوسبة السحابية واللوائح والسياسات التابعة له بخصوص الحوسبة السحابية وتصنيف البيانات وأية لوائح أو قوانين ذات علاقة بالحوسبة السحابية قد تصدرها الهيئة مستقبلاً. كما يجب على المشتركين الامتثال لقوانين دولة الكويت المتعلقة بالجرائم الالكترونية وحقوق الملكية الفكرية وغيرها.
5. يجب على المشتركين بخدمات الحوسبة السحابية العلم بأن مقدم الخدمة لن يكون مسؤولاً ولا محاسباً قانونياً عن اهمالهم فيما يتعلق بضوابط أمن المعلومات المقدمة من مقدم الخدمة، حيث ان المشتركين هم المسؤولون في حال عدم تفعيلهم لكافة الضوابط الأمنية التي يوفرها مقدم الخدمة بما في ذلك ما يترتب عليه قانونياً بسبب حصول الضرر وذلك لعدم التفعيل الكامل للضوابط الأمنية التي يوفرها مقدم الخدمة.
6. التزام الموظفين العاملين لدى المشترك بالقوانين او اللوائح الداخلية خصوصاً إذا كانت تتعلق بخدمات حوسبة سحابية وتتطلب إجراءات أكثر صرامة.

وبالنسبة للمشتركين الأفراد فإن الإطار التنظيمي للحوسبة السحابية قد صنف بياناتهم وفق المستوى الثاني والثالث من مستويات التصنيف، وعليه يجري هذا التصنيف بالنسبة لبيانات العاملين في الجهات الحكومية.

إذا رأى المشترك من الجهات الحكومية بأن جزء من أو كامل بياناتهم تقع وفق المستوى الرابع فإن مسؤولية تأمين تلك البيانات تقع على عاتقهم، وذلك عن طريق التأكد من تطبيق كافة الضوابط أمن المعلومات التي يوفرها مقدم الخدمة، بالإضافة الى التأكد من أن مقدم الخدمة يستطيع توفير المتطلبات اللازمة بأمن المعلومات وذلك لمساعدتهم على الالتزام بالقوانين واللوائح المتعلقة باستخدام الحوسبة السحابية كما هو مذكور أعلاه.

ويلزم الإطار التنظيمي للحوسبة السحابية مقدمي الخدمة بضرورة الإخطار العاجل دون تأخير للمشتركين الذين تعرض أمن المعلومات لديهم لأي انتهاك أو تعرضت بياناتهم لأي اختراق او اطلاع غير مصرح به. وإذا ما كانت هذه البيانات تقع ضمن المستوى الثالث فعلى مقدم الخدمة اخطار الجهات المعنية بذلك أيضاً.

ويجب على المشتركين الأخذ جيداً بعين الاعتبار بأن الاحكام الواردة في الإطار التنظيمي للحوسبة السحابية والسياسات والارشادات المرتبطة به وخصوصا الأحكام ذات العلاقة بالتزامات مقدمي خدمات الحوسبة السحابية غير ملزمة وغير قابلة للفرض والاجبار على مقدمي خدمات الحوسبة السحابية الغير متواجدين في دولة الكويت والغير مصرح لهم من قبل الهيئة، وان هذا الإطار وما يتبعه من سياسات وارشادات تسري أحكامها على مقدمي خدمات الحوسبة السحابية المتواجدين داخل نطاق دولة الكويت والمصرح لهم من قبل الهيئة العامة للاتصالات وتقنية المعلومات ويمتلكون مراكز بيانات تحتوي على بنية تحتية ومنصة تشغيل لبيئة الحوسبة السحابية داخل حدود الدولة.

2. حماية البيانات

يحدد الإطار التنظيمي للحوسبة السحابية الضوابط الخاصة بحماية البيانات الشخصية وبيانات الأفراد من مقدم خدمات الحوسبة السحابية وذلك عن طريق توفير البيئة المناسبة لمتطلبات الأمن الذي قد يطلبها المشترك، بالإضافة الى الالتزام بعدم مشاركتها مع أطراف أخرى. ولا تقتصر الضوابط والأحكام المذكورة في الإطار التنظيمي على البيانات الشخصية وبيانات الأفراد، بل تمتد لتشمل جميع أنواع بيانات المشترك بما في ذلك البيانات التي لا تندرج تحت البيانات الشخصية. ويمنع الإطار التنظيمي للحوسبة السحابية مقدمي الخدمة من نشر بيانات المشتركين أو محتوياتهم أو معلوماتهم الى أي أطراف ثالثة، إذا ما لم يكن مطلوباً وفق قوانين دولة الكويت، أو أن يتم أخذ موافقة المشترك الخطية بذلك.

ومن أمثلة البيانات الأخرى المتوفرة لدى الجهات الحكومية التي تتطلب حماية ولا تندرج تحت البيانات الشخصية: السجلات المالية والطبية والقانونية والموارد البشرية أو تلك المتعلقة بالوثائق السرية المتوفرة لدى المشترك.

وتعتبر ملكية بيانات ومحتوى المشترك والوصول إليها والتعديل عليها حق مطلق للمشترك ولا يحق لمقدم الخدمة الاطلاع او التعديل على تلك البيانات او نقلها او مسحها او الحجز عليها دون أخذ اذن خطي من مالك البيانات. ويجب على مقدمي خدمات الحوسبة السحابية تمكين المشتركين من الوصول الى بياناتهم ومعالجتها أو حذفها أو التعديل عليها بموجب أحكام الإطار التنظيمي للحوسبة السحابية.

3. حماية المشترك

وضح الإطار التنظيمي للحوسبة السحابية الحد الأدنى من الاشتراطات الخاصة بعقود الحوسبة السحابية بين المشتركين (في هذه الحالة المشتركين من الجهات الحكومية) وبين مقدمي خدمات الحوسبة السحابية وذلك حتى تشتمل هذه العقود على أدنى متطلبات الحماية، ولحماية المشتركين من شروط العقود غير العادلة أيضاً.

فقد ذكر الإطار التنظيمي بأن على مقدم الخدمة التزام الشفافية المطلقة في عقود الحوسبة السحابية وبيان نوعية الخدمات التي سيتم تقديمها للمشترك ومستوى تلك الخدمات ومدة تلك العقود ان وجدت وطرق الدفع والمعلومات والتفاصيل المتعلقة باتفاقيات مستوى الخدمة في حال التعاقد والضوابط الأمنية المتوفرة لدى مقدم الخدمة.

كما وضح الإطار التنظيمي التزامات مقدمي الخدمة فيما يتعلق بتعويض المشتركين (عن طريق أرصدة الخدمة) في حال الإهمال من قبل مقدم الخدمة او موظفيه، إذا أدى هذا الإهمال الى حدوث الضرر على المشترك أو انتهاك خصوصيته أو بياناته أو محتوى المشترك الخاص به. وخصوصاً إذا قام المشترك بالتطبيق الصحيح لكل الضوابط الأمنية المترتبة عليه حسب نوع الخدمة التي يشترك بها.

وبناءً على ذلك تدعو الهيئة العامة للاتصالات وتقنية المعلومات المشتركين الى الاطلاع على الإطار التنظيمي للحوسبة السحابية والسياسات والارشادات المتعلقة به والمتوفرة على الموقع الالكتروني للهيئة (https://citra.gov.kw) لمزيد من المعلومات.

أمثلة لخدمات الحوسبة السحابية المتاحة للقطاع الخاص

هذا الفصل يسلط الضوء على بعض خدمات الحوسبة السحابية المستخدمة التي يمكن للقطاع الخاص الاستفادة منها على سبيل المثال لا الحصر: مساحات التخزين، أنظمة تقنية المعلومات، منصات الإنتاجية التي تعمل على الحوسبة السحابية، التطبيقات المؤسسية، منصات التواصل الاجتماعي.

1. مساحات التخزين

توفر الحوسبة السحابية خدمات تخزين ومعالجة البيانات والمعلومات للجميع، حيث يتميز التخزين على الحوسبة السحابية بسهولة الوصول عبر مجموعة من الأجهزة الذكية المتنوعة كالهواتف المتنقلة وأجهزة الحواسيب المكتبية والمحمولة على سبيل المثال لا الحصر. كما يتميز التخزين على الحوسبة السحابية بضمان عدم ضياع أو تلف البيانات والمعلومات المخزنة وتوفرها على الدوام حسب اتفاقية مستوى الخدمة التي يوفرها مقدم الخدمة حين التسجيل او الاشتراك بهذه الخدمة.

في هذا السياق تقوم الشركات الخاصة بالتعاقد مع مقدمي الخدمة لتوفير مساحات التخزين لموظفيها عبر الحوسبة السحابية وبالتالي يعفي الشركات الخاصة من تكاليف شراء وإدارة مراكز بيانات لأجل هذه النوعية من الخدمات.

2. أنظمة تقنية المعلومات

تستطيع الشركات في وقتنا الحاضر من إدارة أنظمتها المتعلقة بتقنية المعلومات عن بعد بفضل الحوسبة السحابية والاستغناء عن إدارة الأنظمة التقليدية داخلياً كما هو معمول به، وذلك عن طريق نقلها الى الحوسبة السحابية لمقدم الخدمة. وبالتالي يمكن للشركات من تقليل التكاليف التي تقوم بصرفها على أجهزة ومعدات مراكز البيانات التقليدية بالإضافة الى تكاليف إدارتها بشكل كبير الى تكلفة بسيطة تعتمد على حيز استخدام الجهة للحوسبة السحابية.

ويمكن للشركات التي ترغب بالتحكم ببرامجها وتطبيقاتها بالإضافة الى بياناتها بشكل كامل استخدام نموذج البنية التحتية كخدمة (IaaS) الذي يوفره مقدم الخدمة، حيث يقوم مقدم الخدمة في هذا النموذج بتوفير بيئة الحوسبة السحابية التي تشكل مركز بيانات يمكن للشركات من تثبيت تطبيقاتها وبرامجها وتخزين بياناتها عليه وإدارتها بشكل كامل.

3. منصات الإنتاجية التي تعمل على الحوسبة السحابية

يقوم مقدم الخدمة بتوفير نموذج المنصة كخدمة (PaaS) للشركات الخاصة والتي تمكنهم من تطوير التطبيقات والبرمجيات عليها دون الحاجة الى القلق بشأن موارد الحوسبة السحابية اللازمة لهذه المنصة. وبالتالي تمكن هذه الخدمة الشركات الخاصة من التركيز على تطوير التطبيقات والبرمجيات المختلفة التي تلبي احتياجاتها.

4. التطبيقات المؤسسية

يقوم مقدم الخدمة بتوفير التطبيقات المؤسسية لشركات القطاع الخاص (على سبيل المثال لا الحصر تطبيقات إدارة علاقات العملاء، أو تطبيقات معالجة النصوص والجداول والعرض المرئي). حيث تتوفر هذه التطبيقات للمشتركين مقابل اشتراك شهري للاستخدام، حيث يوفر هذا النموذج التكاليف الكثيرة على شركات القطاع الخاص لشراء مثل هذه التطبيقات واستضافتها على مراكز البيانات لديها. ويقوم مقدم الخدمة بإدارة هذه التطبيقات بشكل كامل (وفق نموذج البرمجيات كخدمة SaaS) بحيث يعفي المشتركين من إدارتها.
ويمكن للشركات الصغيرة والمتوسطة من الاستفادة من هذه النوعية من الخدمات والتي تعفيها من تكاليف شراء هذه التطبيقات بشكل كامل وادارتها، وتمكنها على التركيز على النمو الاقتصادي والجوانب الأخرى المتعلقة بإدارة الأعمال.

5. منصات التواصل الاجتماعي

أصبحت منصات ومواقع التواصل الاجتماعي جزء لا يتجزأ من حياتنا اليومية، ولأنها تعتبر من خدمات الحوسبة السحابية التي تتوفر للمشتركين، فإنها توفر للمشتركين من الشركات الخاصة ورواد الأعمال منصات الحوسبة اللازمة لتمكينهم من التواصل الاجتماعي مع عملائهم أو مشتركيهم أو زبائنهم، ويمكن للمشتركين من هذه الشركات تحميل الصور ومقاطع الفيديو والآراء والاستفتاءات والمقالات أو المواد الترويجية والتسويقية المتعلقة بالخدمات والمنتجات التي يقدمونها ومشاركتها مع المشتركين الآخرين من الأفراد وغيرهم.

المسؤوليات المترتبة من الإطار التنظيمي للحوسبة السحابية على مشتركي القطاع الخاص

قام الإطار التنظيمي للحوسبة السحابية بتحديد الأحكام والضوابط العامة المترتبة على التعاقد بين المشتركين وبين مقدمي خدمات الحوسبة السحابية. وفي حال المشتركين من القطاع الخاص ورواد الأعمال فإنه من المهم معرفة ما يترتب عليهم من استخدام خدمات الحوسبة السحابية بشأن: أمن المعلومات وتصنيف البيانات، حماية البيانات، وحماية المشتركين.

1. أمن المعلومات وتصنيف البيانات

يعتبر أمن المعلومات الوسيلة اللازمة للحماية ضد اختراق البيانات ويتعلق أمن المعلومات بمسؤولية كل من:

- مقدم خدمات الحوسبة السحابية وذلك عن طريق استخدام المعايير الدولية المتعارف عليها لحماية بيئة الحوسبة السحابية الخاصة به والتأكد من سريتها وسلامتها وتوفرها بالإضافة الى الالتزام بما يترتب عليه من التزامات حسب نموذج الخدمة الذي يوفره للمشترك (البنية التحتية كخدمة IaaS، المنصة كخدمة PaaS، البرمجيات كخدمة SaaS) كما تم تفصيله في مستند ضوابط والتزامات مقدمي خدمات الحوسبة السحابية.

- مشترك الحوسبة السحابية وذلك عن طريق:

1. اختيار مقدم الخدمة المناسب والمصرح له من الهيئة واستخدام ميزات الأمن التي يوفرها مقدم الخدمة والتأكد من قدرته على تمكين المشترك من الامتثال للقوانين واللوائح المعمول بها في دولة الكويت.
2. معرفة المسؤوليات والالتزامات التي تترتب عليه كمشترك حسب الخدمة التي يرغب بالاشتراك بها، والاطلاع على مسؤوليات مقدم الخدمة بهذا الخصوص، إذ أن استخدام الحوسبة السحابية يولد مسؤوليات مشتركة بين المشترك وبين مقدم الخدمة حسب نوعية الخدمات التي يتم التعاقد فيما بينهم عليها (البنية التحتية كخدمة، المنصة كخدمة، البرمجيات كخدمة)، وقد ذكرت بشكل مفصل في الإطار التنظيمي للحوسبة السحابية وفي مستند ضوابط والتزامات مقدمي خدمات الحوسبة السحابية.

3. الامتثال لأحكام الإطار التنظيمي للحوسبة السحابية الخاصة بتصنيف البيانات الى ثلاثة مستويات حسب حساسيتها (بيانات عامة، بيانات خاصة غير حساسة، بيانات خاصة حساسة، بيانات عالية الحساسية) وضمان الامتثال لمستويات الأمن المطلوبة.

تزداد صرامة الإجراءات الأمنية المطلوبة لحماية بيانات المشتركين كلما ارتفع مستوى تصنيف تلك البيانات (وبالتالي يرتفع مستوى أمن المعلومات المطلوب). وقد يتوجب على المشتركين تشفير البيانات وزيادة مستوى هذا التشفير كلما ارتفع مستوى تصنيف هذه البيانات، كما قد يتوجب على المشترك توفير النسخ الاحتياطية من هذه البيانات بالإضافة الى أية متطلبات أمنية أخرى من المشترك أو من مقدم الخدمة. أما بالنسبة للبيانات التي تقع ضمن المستوى الرابع من التصنيف (على سبيل المثال لا الحصر: مفتاح التشفير أو المعلومات عالية الحساسية التي تتوفر لدى جهات القطاع الخاص) فإنها تعامل معاملة خاصة ويقرر المشترك كيفية التعامل معها بمعرفته.

يحق للهيئة العامة للاتصالات وتقنية المعلومات من التعديل على مستويات التصنيف ومتطلباتها الأمنية او إصدار اللوائح المتعلقة بأمن المعلومات لتتناسب مع مستويات التصنيف المذكورة في الإطار مستقبلاً وفق ما تراه مناسباً.

قام الإطار التنظيمي للحوسبة السحابية بتعريف تصنيف البيانات كالتالي "هو تصنيف (أو وضع أو ترتيب) للبيانات في مستويات أمنية ملائمة بناء على مدى حساسيتها وذلك لتحديد السبل المثلى لتداولها وحمايتها من المخاطر." ووضع مسؤولية تصنيف البيانات على عاتق مالك البيانات.

وفي هذا السياق، يجب على المشترك معرفة مدى حساسية بياناته ومحتوى المشترك الخاص به وتصنيفاتها قبل نقلها الى الحوسبة السحابية. (راجع مستند الإطار التنظيمي للحوسبة السحابية)

وبإمكان الشركات التابعة للقطاع الخاص ورواد الأعمال التي لا تعمل ضمن قطاعات حساسة ولا تملك أو تتعامل مع حجم كبير من البيانات الشخصية التي تنتمي للمستوى الثالث من مستويات التصنيف أعلاه ان تقرر بكفاية معايير الأمن المتوفرة للمستوى الأول والثاني (تجدر الإشارة أن بإمكان المشترك من حجب البيانات ومحتوى المشترك الموجود على الحوسبة السحابية العامة من الاطلاع العام وفق الإعدادات المتوفرة والتي يتحكم بها المشترك) من التصنيف واستخدامه لاستضافة هذه البيانات وإن كان الخيار الطبيعي هو اختيار المستوى الثالث المذكور أعلاه. إذ ينبغي على المشترك عدم المبالغة بتصنيف بياناته ومحتوى المشترك الخاص به إذ أن معظم هذه المعلومات تقع ضمن المستوى الأول والثاني والبعض منها يندرج تحت المستوى الثالث، والأقل من ذلك قد يندرج تحت المستوى الرابع. كما أن فقد أو ضياع بيانات أو محتوى المستوى الأول أو الثاني لن يلحق ضرراً كبيراً على المشترك. وتقوم الشركة بتصنيف بياناتها ضمن المستوى الثالث أو المستوى الرابع بناءً على معرفتها بحجم الضرر الذي قد يقع عليها في حال اختراق هذه البيانات، خصوصاً إذا كانت تعزم على استخدام الحوسبة السحابية لمعالجة أو تخزين هذه البيانات.

ويعطي الإطار التنظيمي للحوسبة السحابية المسؤولية للمشترك من القطاع الخاص (وليس لمقدم الخدمة) لاختيار مستوى أمن المعلومات المطلوب الذي يراه مناسباً بالنسبة لبياناته ومحتوى المشترك الذي يملكه على الحوسبة السحابية وإجراءات الأمن، او اختيار الإطار الذي يقدمه مقدم خدمات الحوسبة السحابية لحماية بيانات المشترك إذا رأى المشترك جدوى استخدامه لتلبية احتياجاته المحددة والتزاماته وواجباته ومتطلباته الأمنية.

كما ينبغي على كل من مقدم خدمات الحوسبة السحابية والمشترك معرفة مسؤوليات كل منهم وهي مفصلة حسب نوع نموذج الخدمة الذي تم التعاقد عليه في الإطار التنظيمي للحوسبة السحابية وفي مستند ضوابط والتزامات مقدمي خدمات الحوسبة السحابية بالإضافة الى التالي:

أ. مسؤوليات مقدم خدمات الحوسبة السحابية:
1. مسؤول عن أمن بيئة الحوسبة السحابية المتوفرة لديه وضوابط الأمن المتوفرة لديه.
2. مسؤول عن توفير مستويات الأمن التي يطلبها المشتركون
3. غير مسؤول عن مراقبة محتوى المشتركين او بياناتهم او تحديد مستوى سرية بيانات المشترك.
4. غير مسؤول عن الضرر الناجم عن اهمال المشتركين من استخدام جميع ضوابط أمن المعلومات التي يوفرها.

ب. مسؤوليات المشتركين:
1. اختيار مقدم الخدمة المناسب (خصوصاً المصرح له من قبل الهيئة العامة للاتصالات وتقنية المعلومات) وذلك لضمان توفيره لمعايير وضوابط الأمن المناسبة لحماية بياناتهم أو محتوى المشترك الذي لديهم.
2. تحديد مستوى أمن المعلومات المناسب لطبيعة أعمال المشترك من القطاع الخاص ومستويات تصنيف البيانات والمعلومات المتوفرة لديه المتعلقة به او المتعلقة بالأفراد.
3. مسؤول عن ضوابط الأمن والنفاذ وحقوق النفاذ وتحديد صلاحيات الاستخدام بالنسبة لموظفيهم وغيرها من إجراءات العمل المتعلقة بمعالجة واستخدام البيانات ومحتوى المشترك الذي يملكونه (إذا كان نموذج الخدمة هو المنصة كخدمة أو البرمجيات كخدمة).
4. الامتثال للإطار التنظيمي للحوسبة السحابية واللوائح والسياسات التابعة له بخصوص الحوسبة السحابية وتصنيف البيانات وأية لوائح أو قوانين ذات علاقة بالحوسبة السحابية قد تصدرها الهيئة مستقبلاً. كما يجب على المشتركين الامتثال لقوانين دولة الكويت المتعلقة بالجرائم الالكترونية وحقوق الملكية الفكرية وغيرها.
5. يجب على المشتركين بخدمات الحوسبة السحابية العلم بأن مقدم الخدمة لن يكون مسؤولاً ولا محاسباً قانونياً عن اهمالهم فيما يتعلق بضوابط أمن المعلومات المقدمة من مقدم الخدمة، حيث ان المشتركين هم

المسؤولون في حال عدم تفعيلهم لكافة الضوابط الأمنية التي يوفرها مقدم الخدمة بما في ذلك ما يترتب عليه قانونياً بسبب حصول الضرر وذلك لعدم التفعيل الكامل للضوابط الأمنية التي يوفرها مقدم الخدمة.

6. التزام الموظفين التابعين للمشترك من القطاع الخاص ورواد الأعمال بالقوانين او لوائح المشترك الداخلية خصوصاً إذا كانت تتعلق بخدمات حوسبة سحابية وتتطلب إجراءات أكثر صرامة.

وبالنسبة للمشتركين الأفراد فإن الإطار التنظيمي للحوسبة السحابية قد صنف بياناتهم وفق المستوى الثاني والثالث من مستويات التصنيف، وعليه يجري هذا التصنيف بالنسبة لبيانات العاملين في شركات القطاع الخاص وقطاع الأعمال.

إذا رأى المشترك من القطاع الخاص أو رواد الأعمال بأن جزء من أو كامل بياناتهم تقع وفق المستوى الرابع فإن مسؤولية تأمين تلك البيانات تقع على عاتقهم، وذلك عن طريق التأكد من تطبيق كافة الضوابط أمن المعلومات التي يوفرها مقدم الخدمة، بالإضافة الى التأكد من أن مقدم الخدمة يستطيع توفير المتطلبات اللازمة بأمن المعلومات وذلك لمساعدتهم على الالتزام بالقوانين واللوائح المتعلقة باستخدام الحوسبة السحابية كما هو مذكور أعلاه.

ويلزم الإطار التنظيمي للحوسبة السحابية مقدمي الخدمة بضرورة الإخطار العاجل دون تأخير للمشتركين الذين تعرض أمن المعلومات لديهم لأي انتهاك أو تعرضت بياناتهم لأي اختراق او اطلاع غير مصرح به. وإذا ما كانت هذه البيانات تقع ضمن المستوى الثالث فعلى مقدم الخدمة اخطار الجهات المعنية بذلك أيضاً.

ويجب على المشتركين الأخذ جيداً بعين الاعتبار بأن الاحكام الواردة في الإطار التنظيمي للحوسبة السحابية والسياسات والارشادات المرتبطة به وخصوصا الأحكام ذات العلاقة بالتزامات مقدمي خدمات الحوسبة السحابية غير ملزمة وغير قابلة للفرض والاجبار على مقدمي خدمات الحوسبة السحابية الغير متواجدين في دولة الكويت والغير مصرح لهم من قبل الهيئة، وان هذا الإطار وما يتبعه من سياسات وارشادات تسري أحكامها على مقدمي خدمات الحوسبة السحابية المتواجدين داخل نطاق دولة الكويت والمصرح لهم من قبل الهيئة العامة للاتصالات وتقنية المعلومات ويمتلكون مراكز بيانات تحتوي على بنية تحتية ومنصة تشغيل لبيئة الحوسبة السحابية داخل حدود الدولة.

4. حماية البيانات

يحدد الإطار التنظيمي للحوسبة السحابية الضوابط الخاصة بحماية البيانات الشخصية وبيانات الأفراد من مقدم خدمات الحوسبة السحابية وذلك عن طريق توفير البيئة المناسبة لمتطلبات الأمن الذي قد يطلبها المشترك، بالإضافة الى الالتزام بعدم مشاركتها مع أطراف أخرى. ولا تقتصر الضوابط والأحكام المذكورة في الإطار التنظيمي على البيانات الشخصية وبيانات الأفراد، بل تمتد لتشمل جميع أنواع بيانات المشترك بما في ذلك البيانات التي لا تندرج تحت البيانات الشخصية. ويمنع الإطار التنظيمي للحوسبة السحابية مقدمي الخدمة من نشر بيانات المشتركين أو محتوياتهم أو معلوماتهم الى أي أطراف ثالثة، إذا ما لم يكن مطلوباً وفق قوانين دولة الكويت، أو أن يتم أخذ موافقة المشترك الخطية بذلك.

ومن أمثلة البيانات الأخرى المتوفرة لدى القطاع الخاص ورواد الأعمال التي تتطلب حماية ولا تندرج تحت البيانات الشخصية: البيانات التجارية المتعلقة بأسعار السلع والخدمات، أو البيانات الخاصة بالتسويق، أو المعلومات المتعلقة بأمن المعلومات.

وتعتبر ملكية بيانات ومحتوى المشترك والوصول إليها والتعديل عليها حق مطلق للمشترك ولا يحق لمقدم الخدمة الاطلاع او التعديل على تلك البيانات او نقلها او مسحها او الحجز عليها دون أخذ اذن خطي من مالك البيانات. ويجب على مقدمي خدمات الحوسبة السحابية تمكين المشتركين من الوصول الى بياناتهم ومعالجتها أو حذفها أو التعديل عليها بموجب أحكام الإطار التنظيمي للحوسبة السحابية.

5. حماية المشترك

وضح الإطار التنظيمي للحوسبة السحابية الحد الأدنى من الاشتراطات الخاصة بعقود الحوسبة السحابية بين المشتركين (في هذه الحالة المشتركين من شركات القطاع الخاص) وبين مقدمي خدمات الحوسبة السحابية وذلك حتى تشتمل هذه العقود على أدنى متطلبات الحماية، ولحماية المشتركين من شروط العقود غير العادلة أيضاً.

فقد ذكر الإطار التنظيمي بأن على مقدم الخدمة التزام الشفافية المطلقة في عقود الحوسبة السحابية وبيان نوعية الخدمات التي سيتم تقديمها للمشترك ومستوى تلك الخدمات ومدة تلك العقود ان وجدت وطرق الدفع والمعلومات والتفاصيل المتعلقة باتفاقيات مستوى الخدمة في حال التعاقد والضوابط الأمنية المتوفرة لدى مقدم الخدمة.

كما وضح الإطار التنظيمي التزامات مقدمي الخدمة فيما يتعلق بتعويض المشتركين (عن طريق أرصدة الخدمة) في حال الإهمال من قبل مقدم الخدمة او موظفيه، إذا أدى هذا الإهمال الى حدوث الضرر على المشترك أو انتهاك خصوصيته أو بياناته أو محتوى المشترك الخاص به. وخصوصاً إذا قام المشترك بالتطبيق الصحيح لكل الضوابط الأمنية المترتبة عليه حسب نوع الخدمة التي يشترك بها.

وبناءً على ذلك تدعو الهيئة العامة للاتصالات وتقنية المعلومات المشتركين الى الاطلاع على الإطار التنظيمي للحوسبة السحابية والسياسات والارشادات المتعلقة به والمتوفرة على الموقع الالكتروني للهيئة (https://citra.gov.kw) لمزيد من المعلومات.

أمثلة لخدمات الحوسبة السحابية المتاحة للأفراد

هذا الفصل يسلط الضوء على بعض خدمات الحوسبة السحابية المستخدمة من قبل الأفراد على سبيل المثال لا الحصر: مساحات التخزين، برامج تقنية المعلومات، منصات الترفيه الالكتروني، منصات التواصل الاجتماعي، منصات الإنتاجية.

1. مساحات التخزين

توفر الحوسبة السحابية خدمات تخزين ومعالجة البيانات والمعلومات للجميع، حيث يتميز التخزين على الحوسبة السحابية بسهولة الوصول عبر مجموعة من الأجهزة الذكية المتنوعة كالهواتف المتنقلة وأجهزة الحواسيب المحمولة على سبيل المثال لا الحصر. كما يتميز التخزين على الحوسبة السحابية بضمان عدم ضياع أو تلف البيانات والمعلومات المخزنة وتوفرها على الدوام حسب اتفاقية مستوى الخدمة التي يوفرها مقدم الخدمة حين التسجيل او الاشتراك بهذه الخدمة.

في هذا السياق يقوم مقدمو خدمات التخزين عبر الحوسبة السحابية بتوفير مساحات تخزين للمشتركين بشكل مجاني بسعة محددة يحددها مقدم الخدمة، وبإمكان المشترك من زيادة هذه السعة التخزينية حسب الحاجة مقابل مبلغ مادي للاشتراك بشكل شهري أو سنوي وقد يكون هذا الاشتراك بشكل فردي أو ضمن باقة تتضمن خدمات أخرى.

2. أنظمة تقنية المعلومات

في وقتنا الحاضر وبفضل مرونة الحوسبة السحابية واستخدامها بشكل واسع، أصبح استخدام أنظمة تقنية المعلومات الشخصية والتي كانت تقدم لقطاع الأعمال والشركات فقط، متاحاً للاستخدام للمشتركين الأفراد. لعل أبرز الأمثلة لهذه الأنظمة هو البريد الالكتروني والتقاويم ومكتبات الكتب الرقمية ومكتبات الموسيقى.

ولو أخذنا مثال البريد الالكتروني، فإن مقدم خدمات الحوسبة السحابية يقوم بتوفير جميع متطلبات تشغيل منصة البريد الالكتروني لديه (الخوادم والبنية التحتية اللازمة)، ويقوم المشترك من الأفراد بإنشاء حساب على هذه المنصة واستخدام الخوادم التابعة لمقدم الخدمة دون الحاجة الى تثبيت خادم البريد الالكتروني على جهاز الحاسب الشخصي او الجهاز الذكي الذي يقوم باستخدامه. حيث بإمكانه قراءة وارسال ومعالجة البريد الالكتروني بسهولة ويسر وأقل تكلفة.

وكذلك هو الحال بالنسبة للأمثلة الأخرى المبنية على البريد الالكتروني مثل التقاويم والمفكرات ومكتبات الكتب الرقمية ومكتبات الموسيقى حيث يمكن للمشتركين الأفراد من الاستفادة من هذه الخدمات المتوفرة على الحوسبة السحابية، وذلك بسبب كفاءة تكلفة الحوسبة السحابية التي مكنت مقدمي الخدمة من إدارة أنظمة تقنية المعلومات باحترافية أكبر لتشمل شريحة أكبر من المشتركين وتقديم خدمات أكثر لهم.

3. منصات الترفيه الالكترونية

يستخدم الملايين من الأشخاص بشكل يومي منصات الترفيه الالكترونية، والتي تشمل مواقع البث الحي لمقاطع الفيديو والأفلام (Video Live-Streaming) ومنصات ألعاب الفيديو على الأجهزة الذكية (Mobile Games) والتطبيقات الترفيهية المختلفة المتوفرة على الأجهزة الذكية التي يمتلكها هؤلاء الأشخاص. وتكون هذه المنصات مستضافة على الحوسبة السحابية في أغلب الأحيان، حيث تعفي هذه المنصات المشترك من الحاجة الى توفير أجهزة معقدة للنفاذ والتمتع بخدمات تلك المنصات (على سبيل المثال لا الحصر: أجهزة استقبال الإشارة المنزلية (Satellite Receivers) وغيرها من أنظمة خدمات البث المشغلة بالطريقة التقليدية). ويكتفي المشترك باستخدام الأجهزة الذكية المتوفرة لديه والمزودة باشتراك للإنترنت (مثل الحاسب المحمول أو الهاتف الذكي او أجهزة التلفزة الذكية) لتسجيل الدخول والاستمتاع بخدمات تلك المنصات المتوفرة على الحوسبة السحابية.

فلو أخذنا مثال مواقع البث الحي لمقاطع الفيديو المستضافة على الحوسبة السحابية، فإن مستخدمي هذه المواقع يقومون بمشاهدة المحتوى الترفيهي المتوفر فيها عن طريق التسجيل في هذه المواقع سواءً بصورة مجانية أو بحسب اشتراك شهري يوفره مقدم الخدمة ضمن باقة من الامتيازات. وقد تكون هذه المواقع بصورة تطبيقات يتم تثبيتها على الأجهزة الذكية للمشتركين. ولا يحتاج المشترك في هذه الحالة الى استخدام أجهزة استقبال الإشارة المنزلية (Satellite Receivers) كما هو معمول به في الطرق التقليدية، كما لا يحتاج الى مساحة تخزين كبيرة لتخزين هذا المحتوى بل يقوم بمشاهدته على هيئة بث حي (Live-Streaming) من الموقع او التطبيق بشكل مباشر.

وتتبع بعض منصات ألعاب الفيديو الالكترونية والتطبيقات الترفيهية الأخرى نفس المنهجية، حيث يقوم المشترك بتحميل تطبيق هذه المنصات الترفيهية على الجهاز الذكي المتوفر لديه ومن ثم يقوم بالدخول الى منصة التطبيق المتوفرة على الحوسبة السحابية والاستمتاع بالخدمات الترفيهية التي توفرها دون الحاجة الى توفير البنية التحتية اللازمة لتشغيل هذه الألعاب.

4. منصات التواصل الاجتماعي

أصبحت منصات ومواقع التواصل الاجتماعي جزء لا يتجزأ من حياتنا اليومية، ولأنها تعتبر من خدمات الحوسبة السحابية التي تتوفر للمشتركين الأفراد، فإنها توفر للمشتركين الأفراد منصات الحوسبة اللازمة لتمكينهم من التواصل الاجتماعي فيما بين بعضهم البعض، ويمكن للمشتركين من تحميل الصور ومقاطع الفيديو والآراء والاستفتاءات والمقالات ومشاركتها مع المشتركين الآخرين.

5. منصات الإنتاجية التي تعمل على الحوسبة السحابية

لعل أبرز هذه المنصات وأكثرها شيوعاً هي التطبيقات المختصة بتحرير ومعالجة المستندات بمختلف أنواعها باستخدام الحوسبة السحابية ومنصات البرمجة وتطوير التطبيقات عبر الحوسبة السحابية.

حيث يقوم المشترك باستئجار التطبيقات التي يحتاجها بمقابل مالي من مقدمي الخدمة لاستخدامها عوضاً عن شرائها. وتتميز هذه التطبيقات بتحديثاتها المستمرة من ناحية المنصات الإنتاجية وأمن المعلومات، على عكس التطبيقات القديمة التي يتم شراؤها بالكامل لفترة من الزمن ثم الحاجة لشراء النسخ الجديدة منها بعد بضع سنوات. ويقوم مقدم خدمات الحوسبة السحابية عادةً بتوفير هذه التطبيقات بالإضافة الى خدمات أخرى تتبعها مثل خدمات التخزين وخدمات أنظمة تقنية المعلومات التي ذكرت أعلاه ضمن باقة، وقد تتضمن هذه الباقة خدمات أخرى أيضاً.

المسؤوليات المترتبة من الإطار التنظيمي للحوسبة السحابية على المشتركين الأفراد

قام الإطار التنظيمي للحوسبة السحابية بتحديد الأحكام والضوابط العامة المترتبة على التعاقد بين المشتركين وبين مقدمي خدمات الحوسبة السحابية. وفي حال المشتركين الأفراد فإنه من المهم معرفة ما يترتب عليهم من مسؤوليات والتزامات إزاء استخدام خدمات الحوسبة السحابية وخصوصاً فيما يتعلق في: أمن المعلومات وتصنيف البيانات، حماية البيانات، وحماية المشتركين.

1. أمن المعلومات وتصنيف البيانات

يعتبر أمن المعلومات الوسيلة اللازمة للحماية ضد اختراق البيانات، ويتعلق أمن المعلومات بمسؤولية كل من:

- مقدم خدمات الحوسبة السحابية وذلك عن طريق استخدام المعايير الدولية المتعارف عليها لحماية بيئة الحوسبة السحابية الخاصة به والتأكد من سريتها وسلامتها وتوفرها بالإضافة الى الالتزام بما يترتب عليه من التزامات حسب نموذج الخدمة الذي يوفره للمشترك (البنية التحتية كخدمة IaaS، المنصة كخدمة PaaS، البرمجيات كخدمة SaaS) كما تم تفصيله في مستند ضوابط والتزامات مقدمي مشتركي خدمات الحوسبة السحابية.

- مشترك الحوسبة السحابية وذلك عن طريق:

1. اختيار مقدم الخدمة المناسب والمصرح له من الهيئة واستخدام ميزات الأمن التي يوفرها مقدم الخدمة والتأكد من قدرته على تمكين المشترك من الامتثال للقوانين واللوائح المعمول بها في دولة الكويت.
2. معرفة المسؤوليات والالتزامات التي تترتب عليه كمشترك حسب الخدمة التي يرغب بالاشتراك بها، والاطلاع على مسؤوليات مقدم الخدمة بهذا الخصوص، إذ أن استخدام الحوسبة السحابية يولد مسؤوليات مشتركة بين المشترك وبين مقدم الخدمة حسب نوعية الخدمات التي يتم التعاقد فيما بينهم عليها (البنية التحتية كخدمة، المنصة كخدمة، البرمجيات كخدمة)، وقد ذكرت بشكل مفصل في الإطار التنظيمي للحوسبة السحابية وفي مستند ضوابط والتزامات مقدمي خدمات الحوسبة السحابية.
3. الامتثال لأحكام الإطار التنظيمي للحوسبة السحابية الخاصة بتصنيف البيانات الى أربع مستويات حسب حساسيتها (بيانات عامة، بيانات خاصة غير حساسة، بيانات خاصة حساسة، بيانات عالية الحساسية) وضمان الامتثال لمستويات الأمن المطلوبة.

تزداد صرامة الإجراءات الأمنية المطلوبة لحماية بيانات المشتركين كلما ارتفع مستوى تصنيف تلك البيانات (وبالتالي يرتفع مستوى أمن المعلومات المطلوب). وقد يتوجب على المشتركين تشفير البيانات وزيادة مستوى هذا التشفير كلما ارتفع مستوى تصنيف هذه البيانات خلال جميع مراحل حياة تلك البيانات، كما قد يتوجب على المشترك توفير النسخ الاحتياطية من هذه البيانات بالإضافة الى أية متطلبات أمنية أخرى من المشترك أو من مقدم الخدمة. أما بالنسبة للبيانات التي تقع ضمن المستوى الرابع من التصنيف فإنها تعامل معاملة خاصة ويقرر المشترك كيفية التعامل معها بمعرفته.

يحق للهيئة العامة للاتصالات وتقنية المعلومات من التعديل على مستويات التصنيف ومتطلباتها الأمنية او إصدار اللوائح المتعلقة بأمن المعلومات لتتناسب مع مستويات التصنيف المذكورة في الإطار مستقبلاً وفق ما تراه مناسباً.

قام الإطار التنظيمي للحوسبة السحابية بتعريف تصنيف البيانات كالتالي "هو تصنيف (أو وضع أو ترتيب) للبيانات في مستويات أمنية ملائمة بناء على مدى حساسيتها وذلك لتحديد السبل المثلى لتداولها وحمايتها من المخاطر." ووضع مسؤولية تصنيف البيانات على عاتق مالك البيانات.

وفي هذا السياق، يجب على المشترك معرفة مدى حساسية بياناته ومحتوى المشترك الخاص به وتصنيفاتها قبل نقلها الى الحوسبة السحابية. (راجع مستند الإطار التنظيمي للحوسبة السحابية وسياسة تصنيف البيانات)

وتجدر الإشارة أن بإمكان المشترك حجب بيانات ومحتوى المستوى الأول أو الثاني من الاطلاع للعموم وذلك عن طريق الإعدادات التي يتحكم بها المشترك. كما أن فقد أو ضياع بيانات أو محتوى المستوى الأول لن يلحق ضرراً كبيراً على المشترك.

ويعطي الإطار التنظيمي للحوسبة السحابية الحق للمشترك (وليس لمقدم الخدمة) لاختيار مستوى أمن المعلومات المطلوب الذي يراه مناسباً بالنسبة لبياناته ومحتوى المشترك الذي يملكه على الحوسبة السحابية وإجراءات الأمن، او اختيار الإطار الذي يقدمه مقدم خدمات الحوسبة السحابية لحماية بيانات المشترك إذا رأى المشترك جدوى استخدامه لتلبية احتياجاته المحددة والتزاماته وواجباته ومتطلباته الأمنية.

كما ينبغي على كل من مقدم خدمات الحوسبة السحابية والمشترك معرفة مسؤوليات كل منهم بالنسبة لأمن المعلومات وهي مفصلة كالتالي:

أ. مسؤوليات مقدم خدمات الحوسبة السحابية:

1. مسؤول عن أمن بيئة الحوسبة السحابية المتوفرة لديه وضوابط الأمن المتوفرة لديه.
2. مسؤول عن توفير مستويات الأمن التي يطلبها المشتركون
3. غير مسؤول عن مراقبة محتوى المشتركين او بياناتهم او تحديد مستوى سرية بيانات المشترك.
4. غير مسؤول عن الضرر الناجم عن اهمال المشتركين من استخدام جميع ضوابط أمن المعلومات التي يوفرها.

ب. مسؤوليات المشتركين:

1. اختيار مقدم الخدمة المناسب (خصوصاً المصرح له من قبل الهيئة العامة للاتصالات وتقنية المعلومات) وذلك لضمان توفيره لمعايير وضوابط الأمن المناسبة لحماية بياناتهم أو محتوى المشترك الذي لديهم.
2. الامتثال للإطار التنظيمي للحوسبة السحابية واللوائح والسياسات التابعة له بخصوص الحوسبة السحابية وتصنيف البيانات وأية لوائح أو قوانين ذات علاقة بالحوسبة السحابية قد تصدرها الهيئة مستقبلاً. كما يجب على المشتركين الامتثال لقوانين دولة الكويت المتعلقة بالجرائم الالكترونية وحقوق الملكية الفكرية وغيرها.
3. يجب على المشتركين بخدمات الحوسبة السحابية العلم بأن مقدم الخدمة لن يكون مسؤولاً ولا محاسباً قانونياً عن اهمالهم فيما يتعلق بضوابط أمن المعلومات المقدمة من مقدم الخدمة، حيث ان المشتركين هم المسؤولون في حال عدم تفعيلهم لكافة الضوابط الأمنية التي يوفرها مقدم الخدمة بما في ذلك ما يترتب عليه قانونياً بسبب حصول الضرر وذلك لعدم التفعيل الكامل للضوابط الأمنية التي يوفرها مقدم الخدمة.
4. يجب على المشتركين بخدمات الحوسبة السحابية معرفة أنهم يقعون تحت طائلة المساءلة القانونية في حال وضع بيانات او محتوى مشترك مخالف لقوانين دولة الكويت المتعلقة بشأن الجرائم الالكترونية أو المعاملات الالكترونية أو الملكية الفكرية ويجدر بهم الامتناع عن ذلك لتجنب ما يترتب عليه من عقوبات يجرمها قانون دولة الكويت.
5. الالتزام بأي قوانين او التزامات أخرى غير المذكورة إذا توجب على المشترك الالتزام بها (مثل قوانين او لوائح جهة عمل المشترك الداخلية إذا ما كانت تلك الجهة تقدم لهذا المشترك خدمات حوسبة سحابية وتتطلب إجراءات أكثر صرامة.

وبالنسبة للمشتركين الأفراد فإن الإطار التنظيمي للحوسبة السحابية قد صنف بياناتهم وفق المستوى الثاني والثالث من مستويات التصنيف، فإذا رأى هؤلاء المشتركين بأن جزء من أو كامل بياناتهم تقع وفق المستوى الرابع فإن مسؤولية تأمين تلك البيانات تقع على عاتقهم، وذلك عن طريق التأكد من تطبيق كافة الضوابط أمن المعلومات التي يوفرها مقدم الخدمة، بالإضافة الى التأكد من أن مقدم الخدمة يستطيع توفير المتطلبات اللازمة بأمن المعلومات وذلك لمساعدتهم على الالتزام بالقوانين واللوائح المتعلقة باستخدام الحوسبة السحابية كما هو مذكور أعلاه.

ويجب على المشتركين الأخذ جيداً بعين الاعتبار بأن الاحكام الواردة في الإطار التنظيمي للحوسبة السحابية والسياسات واللوائح والمستندات المرتبطة به وخصوصا الأحكام ذات العلاقة بالتزامات مقدمي خدمات الحوسبة السحابية غير ملزمة وغير قابلة للفرض والاجبار على مقدمي خدمات الحوسبة السحابية الغير متواجدين في دولة الكويت والغير مصرح لهم من قبل الهيئة، وان هذا الإطار وما يتبعه من سياسات وارشادات تسري أحكامها على مقدمي خدمات الحوسبة السحابية المتواجدين داخل نطاق دولة الكويت والمصرح لهم من قب الهيئة العامة للاتصالات وتقنية المعلومات ويمتلكون مراكز بيانات تحتوي على بنية تحتية ومنصة تشغيل لبيئة الحوسبة السحابية داخل حدود الدولة.

2. حماية البيانات

يحدد الإطار التنظيمي للحوسبة السحابية الضوابط الخاصة بحماية البيانات الشخصية وبيانات الأفراد من مقدم خدمات الحوسبة السحابية وذلك عن طريق توفير البيئة المناسبة لمتطلبات الأمن الذي قد يطلبها المشترك، بالإضافة الى الالتزام بعدم مشاركتها مع أطراف أخرى. ويمنع الإطار التنظيمي للحوسبة السحابية مقدمي الخدمة من نشر بيانات المشتركين أو محتوياتهم أو معلوماتهم الى أي أطراف ثالثة، إذا ما لم يكن مطلوباً وفق قوانين دولة الكويت، أو أن يتم أخذ موافقة المشترك الخطية بذلك.

وتعتبر ملكية بيانات ومحتوى المشترك والوصول إليها والتعديل عليها حق مطلق للمشترك ولا يحق لمقدم الخدمة الاطلاع او التعديل على تلك البيانات او نقلها او مسحها او الحجز عليها دون أخذ اذن خطي من مالك البيانات. ويجب على مقدمي خدمات الحوسبة السحابية تمكين المشتركين من الوصول الى بياناتهم ومعالجتها أو حذفها أو التعديل عليها بموجب أحكام الإطار التنظيمي للحوسبة السحابية.

3. حماية المشترك

وضح الإطار التنظيمي للحوسبة السحابية الحد الأدنى من الاشتراطات الخاصة بعقود الحوسبة السحابية بين المشتركين (في هذه الحالة المشتركين الأفراد) وبين مقدمي خدمات الحوسبة السحابية وذلك حتى تشتمل هذه العقود على أدنى متطلبات الحماية، ولحماية المشتركين من شروط العقود غير العادلة أيضاً.

فقد ذكر الإطار التنظيمي بأن على مقدم الخدمة التزام الشفافية المطلقة في عقود الحوسبة السحابية وبيان نوعية الخدمات التي سيتم تقديمها للمشترك ومستوى تلك الخدمات ومدة تلك العقود ان وجدت وطرق الدفع والمعلومات والتفاصيل المتعلقة باتفاقيات مستوى الخدمة في حال التعاقد والضوابط الأمنية المتوفرة لدى مقدم الخدمة.

وبناءً على ذلك تدعو الهيئة العامة للاتصالات وتقنية المعلومات المشتركين الى الاطلاع على الإطار التنظيمي للحوسبة السحابية والسياسات والارشادات المتعلقة به والمتوفرة على الموقع الالكتروني للهيئة (https://citra.gov.kw) لمزيد من المعلومات.

المستندات ذات الصلة

1. سياسة تصنيف البيانات
2. الإطار التنظيمي للحوسبة السحابية
3. لائحة مصطلحات وتعريفات تقنية المعلومات والاتصالات