Communications Regulatory Authority
State of Qatar

هيئة تنظيم الاتصالات
دولة قطر

CLOUD COMPUTING

A HANDBOOK FOR SMEs

الحوسبة السحابية

دليل المؤسسات الصغيرة والمتوسطة

Foreword from the President of the Communications Regulatory Authority

"As part of Qatar National Vision 2030, Qatar's ambition is to establish itself as a leading digital hub in the Middle East. As such, Qatar has placed the promotion of cloud computing at the heart of its transformative digital journey.

Cloud computing offers many opportunities for small and medium-sized enterprises (SMEs): it is a solution to growing bandwidth demands and, with cloud-based services, it's easy to scale up your computing capacity by drawing on the service's remote servers. Such level of flexibility can give businesses using cloud computing a real advantage by improving their overall operational efficiency.

A growing number of SME's around the world are adopting cloud computing because of its capacity to minimise IT costs whilst improving flexibility, streamlining operations and enhancing security. Indeed, from fundamental functions like email services, web services and data storage, to highly technical and tailored services like data security, data management and analytics, artificial intelligence and machine learning, cloud computing is a cost-effective and easy-to-use tool that allows for the flexibility to choose the services that best suit the needs of a business.

This Handbook is part of the instruments issued by the Communications Regulatory Authority to create a safe cloud environment and to facilitate a large-scale adoption of cloud computing by SMEs, in line with the digital development of Qatar.

مقدمة من رئيس هيئة تنظيم الاتصالات

"كجزء من الرؤية الوطنية 2030، تهدف قطر لتأسيس نفسها كمركز رقمي رائد في الشرق الأوسط. وعلى هذا النحو، وضعت قطر ترويج الحوسبة السحابية في قلب رحلتها الرقمية التحويلية.

توفر الحوسبة السحابية العديد من الفرص للمؤسسات الصغيرة والمتوسطة: هو حل لمتطلبات النطاقات الترددية المتزايدة، ومع الخدمات السحابية، انه لمن السهل توسيع نطاق قدرة الحوسبة من خلال الرسم على خوادم الخدمة المعزولة. لمثل هذه الدرجة من المرونة، من خلال استخدام الحوسبة السحابية، بإمناكها افادة الاعمال التجارية بواسطة تعديل الكفائة العملية.

يشهد العالم اعداداً متزايدة من المؤسسات الصغيرة والتموسطة والتي تعتمد على الحوسبة السحابية بسبب كفائتها على تقليل تكلفة تكنولوجيا المعلومات وفي الوقت ذاته تحسن المرونة وتبسيط العمليات وتعزيز الأمن. في الواقع من الجوهري وظائف مثل خدمات البريد الإلكتروني وخدمات الويب وتخزين البيانات ، الي الخدمات التقنية المتخصصة مثل أمن البيانات وإدارة البيانات والتحليلات والذكاء الاصطناعي والتعليم الآلي ،ان الحوسبة السحابية فعالة من حيث التكلفة وسهولة الاستخدام التي تسمح بالمرونة في العمل. واختار الخدمات التي تناسب احتياجات العمل التجارية على أفضل وجه.

هذا الدليل جزء من الصكوك الصادرة من هيئة تنظيم الاتصالات لانشاء بيئة سحابية آمنة وتيسير اعتماد الحوسبة السحابية على نطاق واسع من قبل المؤسسات الصغيرة والمتوسطة، تمشياً مع التطور الرقمي في مجال تكنولوجيا المعلومات والاتصالات في قطر.

In this Handbook, the reader will find an explanation, in simple words, of what cloud computing is, the meaning of typical cloud contractual provisions and key points that SMEs should pay close attention to before subscribing to such services. The Handbook also provides a section on data classification principles that will help SMEs classifying their data in their transition to the cloud."

وفي هذا الدليل، سيجد القارئ توضيح مبسط للحوسبة السحابية، ومعنى الاحكام التعاقدية النموذجية للحوسبة والنقاط الرئيسية التي يجب ان تتولى اهتمامها المؤسسات الصغيرة والمتوسطة قبل الاشتراك في خدمة كهذه. كما يوفر هذا الدليل جزء يخص أسس تصنيف البيانات التي ستساعد المؤسسات الصغيرة والمتوسطة في تصنيف بياناتها عند الانتقال الى الحوسبة."

Mohammed Ali Al Mannai

President of the Communications Regulatory Authority

محمد علي المناعي

رئيس هيئة تنظيم الاتصالات

Table of Contents

جدول المحتويات

1. Introduction to Cloud Computing

There are three main categories of cloud services: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service ("IaaS). Your company's business profile, its needs and requirements shall drive the decision to adopt one or more of these models. Different Cloud Service Providers (CSP) offer a variety of services in each of these models.

There are also different deployment models of cloud computing: public cloud, private cloud, hybrid cloud, community cloud and Multi-cloud.

You shall have a clear picture of the objectives and resources of your organization to determine, together with the CSP, what the most appropriate category of service and deployment model is for your company.

Categories of cloud services:

1. مقدمة الى حوسبة السحابية

هناك ثلاث فئات رئيسية من خدمات السحابة: البرمجيات كخدمة، والنظام الأساسي كخدمة والبنية التحتية كخدمة. يجب ان يقود الملف التجاري الخاص بشركتك واحتياجاتها ومتطلباتها الى اتخاذ قرار بتبني واحدة او أكثر من هذه النماذج. يوفر مختلف مقدمو الخدمات السحابية مجموعة متنوعة من الخدمات في كل من هذه النماذج.

هناك أيضا نماذج نشر مختلفة للحوسبة السحابية: الحوسبة العامة والحوسبة الخاصة والحوسبة الهجينة والسحابة المجتمعية والسحابة المتعددة.

يجب ان يكون لديك صورة واضحة عن اهداف وموارد مؤسستك لتحديد، تضامنا مع موفر الخدمة السحابية، فئة الخدمة ونموذج النشر الأنسب لشركتك.

فئات الخدمات السحابية

ON - PREMISE في مكان العمل	CLOUD SERVICES خدمات السحابة INFRASTRUCTURE AS A SERVICE البنية التحتية كخدمة	 PLATFORM AS A SERVICE المنصة كخدمة	 SOFTWARE AS A SERVICE البرمجيات كخدمة
Applications التطبيقات	Applications التطبيقات	Applications التطبيقات	Applications التطبيقات
Data البيانات	Data البيانات	Data البيانات	Data البيانات
Runtime وقت التشغيل	Runtime وقت التشغيل	Runtime وقت التشغيل	Runtime وقت التشغيل
Middleware الوسيطة	Middleware الوسيطة	Middleware الوسيطة	Middleware الوسيطة
Operating System نظام التشغيل	Operating System نظام التشغيل	Operating System نظام التشغيل	Operating System نظام التشغيل
Virtualization الاستخدام الافتراضي	Virtualization الاستخدام الافتراضي	Virtualization الاستخدام الافتراضي	Virtualization الاستخدام الافتراضي
Networking الربط الشبكي	Networking الربط الشبكي	Networking الربط الشبكي	Networking الربط الشبكي
Storage التخزين	Storage التخزين	Storage التخزين	Storage التخزين
Servers الخوادم	Servers الخوادم	Servers الخوادم	Servers الخوادم

Managed by customer يتم ادارتها من قبل العميل Managed by Cloud Service provider يتم ادارتها من قبل مقدم خدمة السحابة

Categories of Cloud Services - GSMA, "Telco Edge Cloud: Edge Service Description and Commercial Principles", October 2020

SaaS (Software as a service)

SaaS is a is a software delivery business model in which a provider or third party hosts an application and makes it available to customers on a subscription basis.

The application itself is physically deployed on servers owned, controlled, or managed by the CSP.

A customer subscribing to SaaS will receive the benefit of the software, and of any underlying platforms and infrastructure. The customer simply needs to be able to access the Internet and use the login credentials provided by the provider to access the service.

Examples of SaaS services are webmail (e.g. Office 365, Gmail), social media sites (e.g. Facebook), and online gaming platforms (e.g. Steam).

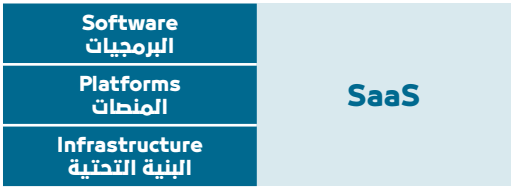
البرنامج كخدمة

SaaS هـو نمـوذج أعمـال لتوصيـل البرامـج حيـث يسـتضيف فيـه الموفـر أو الطـرف الثالـث ملـف التطبيـق وإتاحته للعملاءعلى أسـاس الاشـتراك.

يتـم نشـر التطبيـق نفسـه فعليـاً علـى الخوادم التـي يمتلكهـا أو يتحكـم فيهـا أو يديرها CSP.

سـيحصل العميـل المشـترك فـي SaaS علـى الاسـتفادة مـن البرنامـج وأي منصـة وبنيـة تحتيةاساسـية. العميـل يحتـاج ببسـاطة إلـى أن يكون قـادرًا على الوصـول إلى الإنترنت واسـتخدم بيانـات اعتماد تسـجيل الدخـول المقدمـة من قبل مـزود للوصـول إلـى الخدمـة.

ومن الأمثلـة على خدمات SaaS البريـد الإلكتروني (على سـبيل المثـال).(Office 365، Gmail)، وعلى مواقـع التواصـل الاجتماعـي (Facebook)، وعلـى منصات الألعـاب على الإنترنـت (Steam).



PaaS (Platform as a service)

Platform as a Service (PaaS) offers hosted application servers that have near-infinite scalability resulting from the large resource pools that they rely on. PaaS permits the customer to access a platform to create and manage software applications or services on top of the platform provided by the CSP.

PaaS also offers necessary supporting services, including storage, security, integration infrastructure, and development tools for a complete platform.

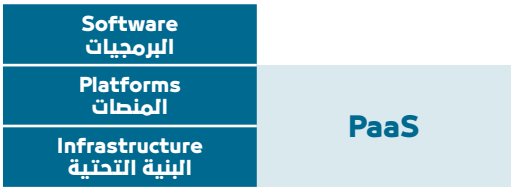
Examples of PaaS services are Microsoft Azure, AWS Elastic, Beanstalk, Force.com, and Google App Engine.

PaaS (المنصة كخدمة)

توفر المنصة كخدمة خوادم تطبيقات مستضيفة تتمتع بقابلية توسع شبه لا نهائية ناتجة عن تجمعات الموارد الكبيرة التي يعتمدون عليها. تسمح PaaS للعميل بالوصول الى منصة لإنشاء تطبيقات او خدمات برمجية وادارتها فوق النظام الأساسي الذي يوفره مقدم الخدمة السحابية.

كما يوفر PaaS خدمات دعم مهمة، لا سيما التخزين والامن توحيد البنية التحتية والأدوات التطويرية لمنصة شاملة.

ومن امثلة خدمات: PaaS Microsoft Azure, AWS Elastic , Beanstalk, Force.com, و Google App Engine.



IaaS (Infrastructure as a service)

IaaS is the most bare-bone category of cloud, under which the customer subscribes only for access to underlying infrastructure. It is like traditional hosting, in which a business uses the hosted environment (physical and virtual servers) as a logical extension of the on-premises datacenters.

The customer still needs to deploy a platform and software on top of IaaS. IaaS is about providing the most basic computing resources — storage capacity, processing power, networking etc. The customer does not own servers, data center space or network equipment but rather purchases access to each of those, as an on-demand service.

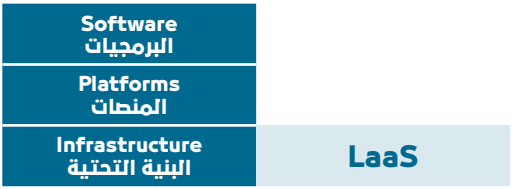
IaaS (البنية التحتية كخدمة)

IaaS هي اكثر فئات السحابة كشوفا، حيث يشترك العميل فقط للوصول الى البنية التحتية الأساسية. فهي اشبه بالاستضافة التقليدية، حيث تستخدم الشركة البيئة المستضيفة (خوادم مادية وظاهرية) كامتداد منطقي لمراكز البيانات المحلية.

سيحتاج العميل بحاجة لنشر منصة وبرنامج إضافةً الى IaaS. يوفر IaaS مصادر الحوسبة الأكثر أساسية – سعة التخزين وقوة المعالجة والشبكات وما الى ذلك. لا يمتلك العميل خوادم او مراكز بيانات او معدات الشبكة، بل يقوم بشراء الوصول الى كل منها، كخدمة عند الطلب .

ومن امثلة خدمات IaaS :
Amazon EC2،Microsoft Azure،و Google Compute Engine.

Examples of IaaS services are Amazon EC2, Microsoft Azure, and Google Compute Engine.



نماذج نشر الحوسبة السحابية:

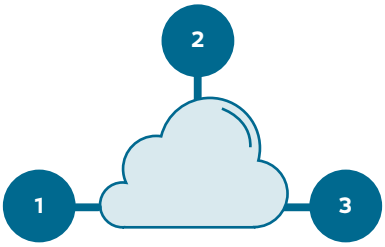
Cloud computer deployment models:

السحابة العامة

يتيح موفر الخدمات السحابية البنية التحتية للسحابة بما يتضمن التخزين والبرامج على الانترنت لاي شخص يريد اقتناءها لدى هذا النموذج.

Public Cloud

In a public cloud model, the CSP makes its cloud infrastructure, including storage and applications. available over the internet to any person who wishes to procure them.

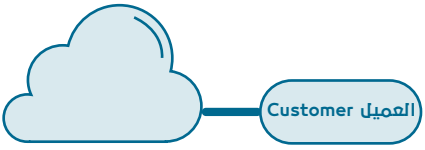


السحابة الخاصة

تشبه السحابة الخاصة السحابة العامة من حيث الفعالية لكنها مخصصة لمؤسسة واحدة. يمكن تولي ادارتها من قبل المؤسسة او مقدم خدمة السحابة.

Private Cloud

A private cloud resembles a public cloud in terms of functionality but is dedicated to a single organization. It may be managed by that organization or by a cloud service provider.



Hybrid Cloud

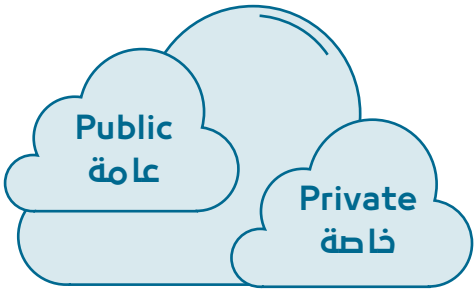
A hybrid cloud provides the use of private and public cloud solutions such that there is a degree of interaction between the two systems. Public or private environments remain unique entities but are bound together with on-premises ICT by common technology that enables data and application portability, allowing the user to move between public cloud, private cloud, and traditional on-premises environments.

A common use of this model allows users to deal with peaks of website traffic, also known as 'cloud bursting'. For example, a private cloud may be appropriate to cope with day-to-day demand but may be susceptible to crashing during product launches or sales promotions. A hybrid cloud may therefore be used to enable the excess volumes to overflow into public cloud infrastructure.

السحابة الهجينة

توفر السحابة المختلطة استخدام حلول السحابة الخاصة والعامة بحيث تكون هناك درجة من التفاعل بين النظامين. تظل البيئات العامة او الخاصة كيانات فريدة، ولكنها مرتبطة مع تكنولوجيا المعلومات والاتصالات المحلية من خلال تقنية مشتركة تتيح إمكانية نقل البيانات والتطبيقات، مما يسمح للمستخدم بالتنقل بين السحابة العامة والسحابة الخاصة والبيئات المحلية التقليدية.

يسمح الاستخدام الشائع لهذا النموذج للمستخدمين بالتعامل مع ذروة حركة المرور على الموقع، والمعروفة أيضا باسم "انفجار السحابة". على سبيل المثال، قد تكون السحابة الخاصة مناسبة للتعامل مع الطلب اليومي ولكنها قد تكون عرضة للانهيار اثناء اطلاق المنتج او عروض المبيعات الترويجية. لذلك يمكن استخدام سحابة هجينة لتمكين الاحجام الزائدة من التدفق الى البنية التحتية السحابية العامة.

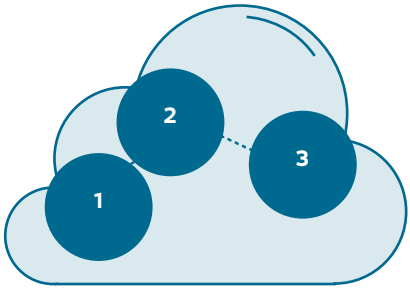


Community Cloud

A community cloud is a cloud service established for and shared by organizations or persons with similar interests or concerns.

السحابة المجتمعية

تم انشاء السحابة المجتمعية كخدمة سحابية لتشاركها مؤسسات او مجموعة افراد يمتلكون اهتمامات مشتركة.

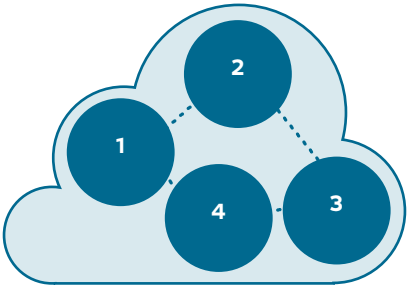


Multi-cloud

A multi-cloud environment is a cloud service that makes use of two or more distinct cloud services, which are typically public cloud services.

السحابة المتعددة

ان بيئة السحابة المتعددة هي خدمة سحابية تستخدم واحد او اثنان او أكثر من الخدمات السحابية الخاصة، والتي عادةً ما تكون خدمات سحابية عامة.



2. Meaning of typical cloud contractual provisions [1]

2.1 Term

This clause means the period during which the cloud service provider will provide the services to your company, the customer, under the contract, *e.g.* one month, one year, five years.

The Term will typically commence on the date the contract is signed (this is often referred to as the "Effective Date") and end on either:

- a specific date which will be mentioned in the contract (this specific date will often be referred to as the "Expiry Date"); or
- an earlier date if the parties decide to terminate the contract before the Expiry Date

2. معنى الاحكام التعاقدية النموذجية للحوسبة [1]

2.1 فترة

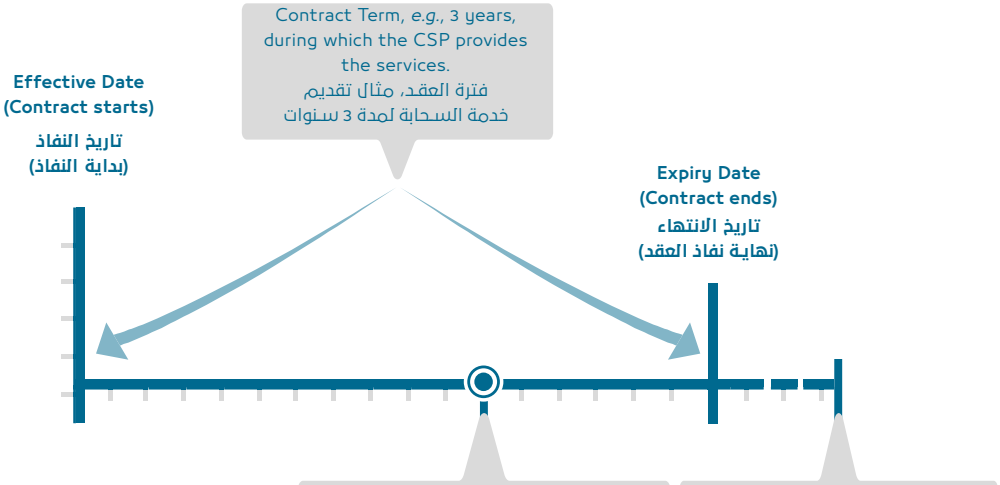
يقصد بهذا البند الفترة التي يقدم فيها مقدم الخدمة السحابية الخدمات لشركتك والعميل، بموجب العقد، مثال شهر، سنة، خمس سنوات.

تُفعل الفترة في تاريخ توقيع العقد (يشار به احياناً بتاريخ بدء السريان) وينتهي إما:

- في تاريخ معين والذي سيذكر في العقد (ان هذا التاريخ عادةً ما يشار به بتاريخ الانتهاء) او
- تاريخ مسبق إذا اتفق الطرفان بتوقف نفاذ فترة سريان العقد قبل انتهائه.

[1] This handbook should not be considered as a legal advice. SMEs should consult a lawyer or a legal representative to help evaluate contracts governing cloud computing services.

[1] يجب ان لا يعتبر هذا الدليل كنصيحة قانونية. على المؤسسات الصغيرة والمتوسطة استشارة محامي او ممثل قانوني لمساعدة تقييم العقود التي تحكم خدمات الحوسبة السحابية.



Key points:

In addition to making sure that the duration of the contract, i.e., the duration for which the services will be provided, is adequate from a business perspective, you should pay particular attention to the consequences of expiry or termination, including the length of time that data and logs are retained after termination, the process for notification of service termination, the return of data and assets as well as the following provisions.

النقاط الرئيسية

بالإضافة الى التأكد من ان فترة العقد، على سبيل المثال الفترة التي تُقدم فيها الخدمة، هي مناسبة من منظور تجاري، يجب عليك الانتباه بشكل خاص لعواقب الانتهاء او التوقف، ويشمل ذلك على المدة الزمنية التي تحتفظ فيها البيانات والسجلات بعد التوقف، وإجراءات التنبيه عند توقف الخدمة، وعودة البيانات والأصول، بالإضافة الى الاحكام التالية.

Automatic renewals

The CSP may include in the contract an automatic renewal mechanism which would typically be found in the Term clause. If it is included, look carefully at what the deadline and process are to notify the CSP of your intention not to renew the contract.
Equally, if the contract does not contain an automatic renewal mechanism, be aware that the services would normally automatically stop at the end of the Term.

التجديد التلقائي

قد يشمل مقدم الخدمة السحابية ميكانيكية التجديد التلقائي في العقد والذي عادةً ما توجد في بند الفترة. في حال تم اضافته، انظر بعناية الى موعد الانتهاء والاجراء لإبلاغ مقدم الخدمة السحابية عن نيتك في عدم تجديد العقد.
وبصورة متساوية، إذا لم يحتو العقد على بند ميكانيكية التجديد التلقائي، كن على علم بأن الخدمات ستتوقف تلقائياً عند نهاية الفترة.

Changing conditions

It is also possible that, when renewed, some of the conditions in the contract could automatically change, *e.g.* the charges. You should check the Term clause for this possibility.

الشروط المتغيرة

من الممكن ايضاً ان تتغير شروط العقد بشكل تلقائي عند التجديد، على سبيل المثال الرسوم. عليك مراجعة بند الفترة لهذا الاحتمال.

Different durations

The Term refers to the duration of the contract itself, *i.e.* how long the services will be provided for. However, it is possible that other obligations under the contract will last for different durations, *e.g.,* duration for which the data will be stored in the cloud.

You should look out for these different durations and understand how they could impact your business.

الفترات المختلفة

يشار بالفترة بمدة العقد نفسه، على سبيل المثال ما المدة التي ستُقدم فيها الخدمات. رغم ذلك، هناك احتمال استمرارية بعض الالتزامات تحت فترات مختلفة، على سبيل المثال الفترة التي ستخزن فيها البيانات في السحابة.

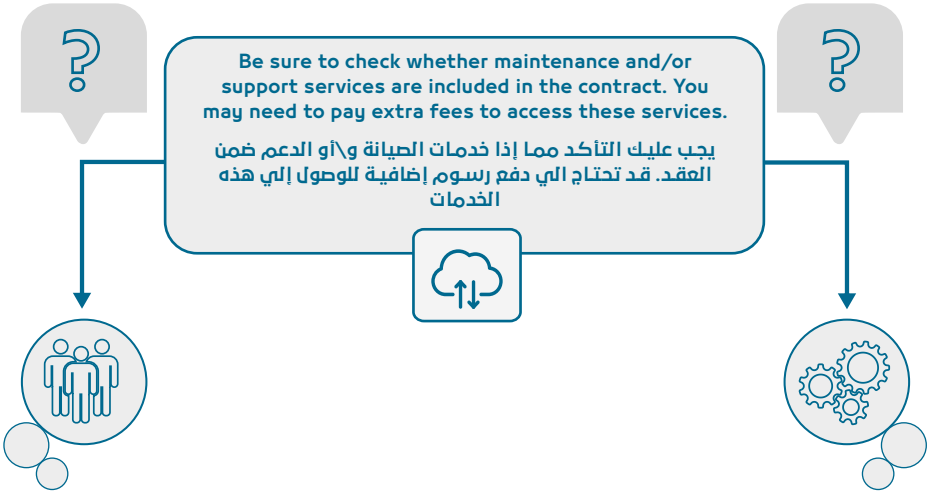
يجب عليك مراجعة الفترات المختلفة وإدراك كيف يمكن لذلك ان يؤثر بتجارتك.

2.2 Service

This clause will describe the cloud services that will be provided, or made available, by the CSP to your company under the contract.

2.2 الخدمة

سيصف هذا البند خدمات السحابة التي سيتم تقديمها، او تكون متاحة، من قبل مقدم الخدمة السحابية لشركتك بمقتضى العقد.



Key points:

النقاط الأساسية:

You should review the description of the services carefully to confirm that the services described in the contract meet all your business needs.

يجب عليك مراجعة وصف الخدمات بعناية للتأكد من ان الخدمات الموصوفة في العقد تلبي جميع احتياجات تجارتك.

When reading this clause, you should also look out for any of the following exclusions or restrictions to the services.

عند قراءة هذا البند، يجب عليك ايضاً الاحتراس من استثناءات او قيود الخدمة التالية.

Exclusion

الاستثناءات

The cloud contract may exclude maintenance and support services from the scope of the services, e.g., a service desk hotline. Customers often mistakenly think that maintenance and support services are automatically included within the services. This should not be assumed.

قد يستثني العقد الصيانة وخدمات الدعم من نطاق الخدمات، على سبيل المثال خدمة الخط الساخن. يعتقد بعض العملاء ان الصيانة وخدمات الدعم تكون متوفرة تلقائياً ضمن الخدمات. لا ينبغي افتراض ذلك.

You may have to pay extra for maintenance and/or support services.

قد تضطر الى دفع مبلغ إضافي مقابل الصيانة و \أو خدمات الدعم.

Restriction

القيود

A typical restriction the customer may find in a cloud contract relates to the transfer of data after the contract ends. For example, the CSP may state that it will not automatically transfer your data back to you (or a new CSP engaged by your company) at the end of the contract.

القيود التي يجدها العميل العادي في عقد السحابة تكون ذات صلة بنقل البيانات بعد انتهاء العقد. على سبيل المثال، قد يصرح مقدم خدمة السحابة عدم نقل بياناتك لك بشكل تلقائي (او الى مقدم خدمة جديد تم تعينه من قبل شركتك) في نهاية العقد.

You should look to provisions on data portability. Data portability ensures you can transfer your data to another solution, which is a foundational necessity to establish a working exit plan. Several aspects have to be considered such as the data being accessible for transfer; use of in a machine-readable data format that can be understood by receiving applications correctly for instance through use of documented application programming interfaces (APIs) ; applicable metadata that is required for the data to be meaningful; data security measures such as use of data encryption and related key management/protection and finally data compliance requirements where laws or regulations prohibit transfer to a certain location/region[2] .

يجب عليك النظر الى احكام قابلية نقل البيانات. تضمن قابلية البينات قدرتك على نقل بياناتك الى حل اخر، والذي يُعتبر أهمية أساسية لإنشاء خطة خروج. يجب الاخذ بالاعتبار بعض الجوانب مثل توفر البيانات للنقل؛ استخدام تنسيق بيانات قابل للقراءة الياً والذي يمكن فهمه من قبل استقبال الطلبات بشكل صحيح، على سبيل المثال من خلال استخدام واجهات برمجة التطبيقات (API)؛ البيانات الوصفية القابلة للتطبيق المطلوبة لتكون البيانات ذات مغزى؛ تدابير حماية البيانات مثل استخدام تشفير البيانات واساسيات إدارة\ حماية البيانات الأخرى ذات الصلة، واخيراً متطلبات امتثال البيانات حيث تمنع القوانين واللوائح النقل الى موقع\منطقة معينة.

[2] To go further:
- ISO/IEC 19941 on Cloud Interoperability and Portability highlights in more detail these different facets that must be considered when migrating data between different environments.
- Draft ISO/IEC 19944 on Data Flows, Categories and Use highlights a possible data taxonomy that can help in planning data migration activities.

2.3 Customer Responsibilities

This clause will describe all the actions that your company, the customer, is:

- obliged to perform; and
- restricted from performing.

In other words what the customer promises to do or not to do. If you do not meet these obligations and restrictions, you will be in breach of your responsibilities which may allow the CSP to, among other things, stop providing the services.

2.3 "مسؤولية العميل"

سيصف هذا البند جميع الإجراءات التي تكون بها شركتك، بمعنى اخر العميل:

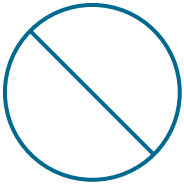
- ملزمة باتباعها؛ و
- مقيدة من تنفيذها.

وبعبارة أخرى، يعد العميل بالتزامه باتباع او عدم اتباع هذه الإجراءات. إذا لم تلتزم بهذه المتطلبات والقيود، ستقوم بانتهاك مسؤوليتك والذي يسمح لمقدم خدمة السحابة، ضمن أمور أخرى، بتوقف تقديم الخدمات.

OBLIGATIONS الالتزامات

You **must** perform your obligations
يجب عليك القيام بالالتزاما ت

RESTRICTIONS القيود



You **must not** do anything that is restricted
لا تفعل أي شيء مقيد

Key points:

You should ensure that your company can meet its obligations under the contract and that it does not perform any of the restricted activities.

النقاط الأساسية:

يجب عليك التأكد من ان شركتك تلبي جميع التزاماتها بموجب العقد وأنها لا تتبع الممارسات المحظورة.

Obligations

Common obligations include:

- the customer should pay all its invoices on time; and
- the customer should provide the CSP with all information and documents that the CSP needs to deliver the services.

الالتزامات

تتضمن الالتزامات الشائعة:

- يجب ان يقوم العميل بتسديد جميع الفواتير في الموعد المحدد؛ و
- يجب ان يوفر العميل جميع المعلومات والوثائق الى مقدم خدمة السحابة والذي يحتاجها مقدم الخدمة لتسليم الخدمات.

The customer's failure to perform its obligations may allow the CSP to:

- suspending the services (and potentially terminate the contract); or
- require the customer to pay additional costs to the CSP. This is further explained in "Relief Events" below.

ان فشل العميل في تلبية المهام قد يسمح لمقدم خدمة السحابة بأن:

- تعليق الخدمات (واحتمال انهاء العقد)؛ او
- اشتراط العميل بتسديد تكاليف إضافية لمقدم خدمة السحابة. انظر لقسم "فعاليات الاعانة" لمعرفة المزيد من التفاصيل.

Restrictions

You need to understand all the restrictions imposed on your company and the consequences of breaching them.

A common restriction found in a cloud contract would, for example, be that your company is not allowed to share the service with a third party outside your company. This is further explained in "Usage Rights and Restrictions" below.

القيود

يجب عليك فهم جميع القيود المفروضة على شركتك وعواقب الانتهاك.

بعض القيود الشائعة المذكورة في عقد السحابة قد تنص على عدم السماح بمشاركة الخدمة مع طرف ثالث خارج شركتك. انظر لقسم "قيود وحقوق الاستخدام" لمعرفة المزيد من التفاصيل.

2.4 Supplier Responsibilities

This clause will describe all the activities that the CSP (the "Supplier" in a cloud contract) is:

- obliged to perform; and
- restricted from performing.

In order words, this clause describes what the CSP promises to do and not do. If the CSP does not follow these obligations and restrictions, then the CSP will be in breach of its responsibilities under the contract. This breach may allow your company, the customer, to terminate the contract early.

2.4 مسؤولية المورد

سيصف هذا البند جميع الاجراءات التي يكون مقدم خدمة السحابة ("المورد" في عقد السحابة):

- ملزم باتباعها؛ و
- مقيد من تنفيذها.

وبعبارة أخرى، يعد المورد بالتزامه باتباع او عدم اتباع هذه الإجراءات. إذا لم يلتزم بهذه المتطلبات والقيود، سيقوم بانتهاك مسؤوليته والذي يسمح للعميل، ضمن أمور أخرى، بإنهاء العقد في وقت مبكر.

OBLIGATIONS الالتزامات

You **must** perform your obligations

RESTRICTIONS القيود

You **must not** do anything that is restricted

Key points:

You should make sure that the cloud contract clearly states what the CSP is required to do, and what activities the CSP is restricted from doing.

النقاط الرئيسية:

يجب عليك التأكد ان عقد السحابة ينص بوضوح متطلبات مقدم خدمة السحابة والأنشطة المقيدة.

Obligations

Common obligations on the CSP include:

- the CSP must provide the services as described in the contract;
- the CSP must meet all service levels as described in the contract; and
- the CSP must use reasonable security technologies when storing data.

الالتزامات

تتضمن الالتزامات الشائعة لمقدم خدمة السحابة:

- يجب على مقدم خدمة السحابة تقديم الخدمات كما هي موصوفة في العقد؛
- يجب على مقدم الخدمة تلبية جميع مستويات الخدمة كما هي موصوفة في العقد؛ و
- يجب على مقدم الخدمة استخدام تكنولوجيا حماية معقولة عند تخزين البيانات.

Restrictions

You should pay particular attention to restricted activities that could put the activities of your business at risk.

A common restriction imposed on the CSP is that the CSP should not change the services or the material functions of the services in the contract in a way that would make them unusable by the customer.

القيود

يجب عليك الاخذ بعين الاعتبار الأنشطة المقيدة التي قد تضع أنشطة تجارتك في خطر.

بعض القيود الشائعة المفروضة على مقدم خدمة السحابة تتضمن عدم تغيير الخدمات او الوظائف المادية للخدمات في العقد بطريقة تجعل العميل غير قادر على استخدامها.

2.5 Relief Events

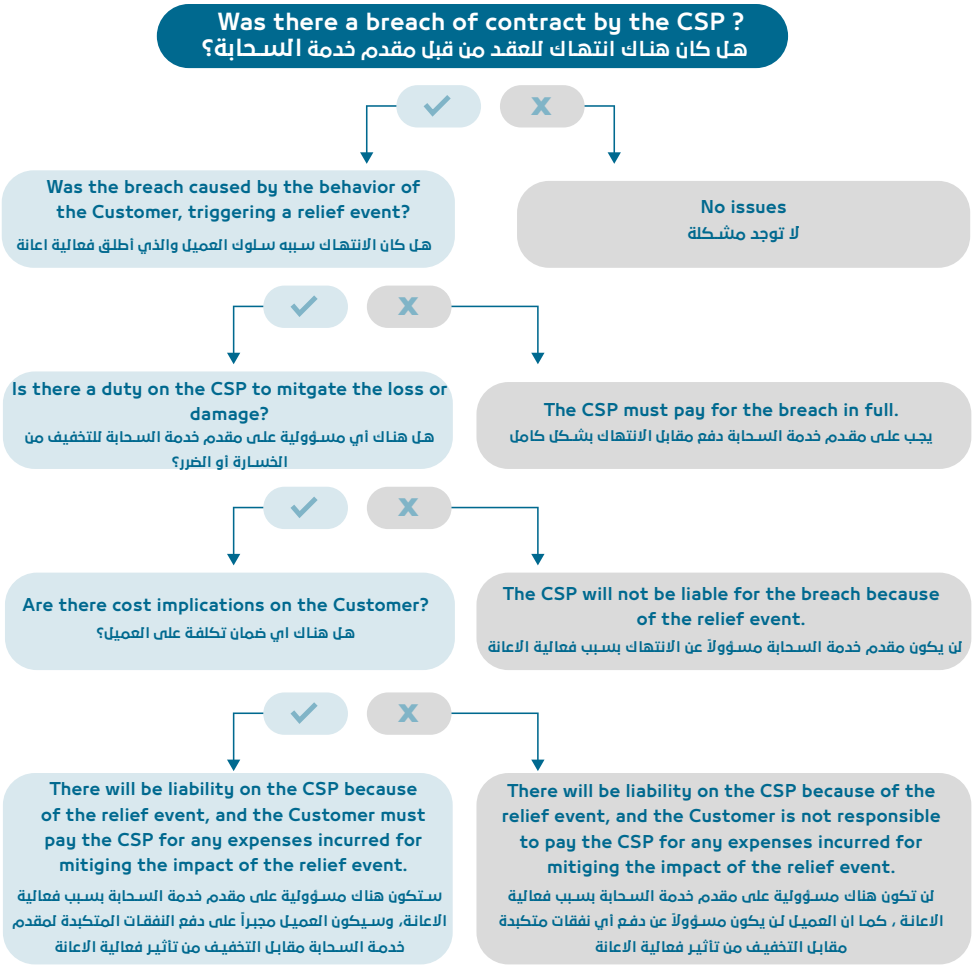
This clause describes the circumstances where the CSP will not be in breach of the cloud contract, even if the CSP:

- fails to perform its obligations; or
- is late in performing its obligations.

2.5 فعاليات الاعانة

يصف هذا البند الظروف حيث لن يعتبر مقدم خدمة السحابة منتهك لعقد السحابة، حتى وإن:

- فشل مقدم الخدمة في اتباع التزاماته؛ او
- تأخر مقدم الخدمة في ممارسة التزاماته.



Key points:

Typically, the CSP will not be in breach of the contract if the failure or delay in performing its obligations is the customer's fault. In other words, if the CSP's failure or delay results from your company's own failure to perform its obligations, the CSP will not be in breach of the contract.

You should still be aware that the contract may provide that the CSP may not be entitled to a relief and that the CSP must perform the services regardless of the customer's delay or failure if performance is still possible.

النقاط الأساسية:

إذا كان التأخر او الفشل في تقديم الأداء من قبل مقدم خدمة السحابة سببه العميل، فذلك عادةً ما يعني ان مقدم الخدمة لم ينتهك العقد. بمعنى اخر، إذا كان فشل او تأخر مقدم خدمة السحابة نتيجة فشل أداء شركتك لالتزاماتها، فمقدم الخدمة لن يكون منتهكاً للعقد.

يجب ان تكون على علم بأن قد ينص العقد على عدم حصول مقدم خدمة السحابة على احقية الاعانة، وعليه يجب ان يؤدي الخدمات على الرغم من تأخر العميل او فشله إذا كان الأداء ما زال ممكناً .

In addition to understanding the importance of performing your obligations, you should also consider the following mitigation requirements and cost implications.

بالإضافة الى فهم أهمية أداء الالتزامات، يجب عليك الاخذ بالاعتبار متطلبات التخفيف والاثار المترتبة من حيث التكليف.

Mitigation

التخفيف

The contract may state that the CSP has the responsibility to mitigate (reduce the impact) of any incident that may result in a relief event.

قد ينص العقد ان مقدم خدمة السحابة يحمل مسؤولية تخفيف (التقليل من اثار) أي حادثة قد تكون نتيجة فعالية إغاثة.

Cost implications

الاثار المترتبة من حيث التكليف

You should also be aware that the contract may make you responsible for any additional costs or expenses incurred by the CSP to mitigate the impact of an incident and continue providing services.

يجب عليك ان تكون على دراية ان العقد قد يجعلك مسؤولاً عن أي تكاليف إضافية او نفقات تم تكبدها من قبل مقدم خدمة السحابة للتخفيف من اثار أي حادثة والاستمرار في تقديم الخدمات.

If that is the case, you should consider whether those additional costs are appropriate and reasonable for your company.

ففي تلك الحالة، يجب عليك الاعتبار ما إذا كانت التكاليف الإضافية مناسبة ومعقولة لشركتك.

2.6 Usage Rights And Restrictions

2.6 القيود وحقوق الاستخدام

This clause describes how the customer may use the services, as well as any restrictions on the way such services can be used.

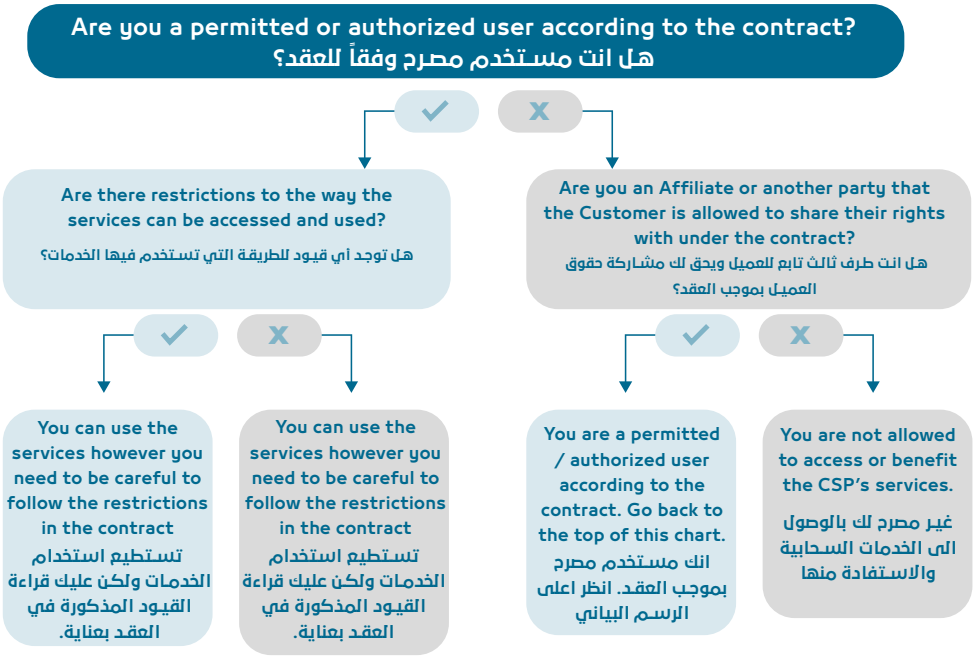
يصف هذا البند كيفية استخدام العميل للخدمات، بالإضافة الى أية قيود مفروضة على طريقة استخدام خدمة كهذه.

This section will typically state:

ينص هذا القسم على:

- what rights the customer has over the use of the services;
- who else, in addition to the customer, is permitted to use the services;
- the maximum number of users that can use the services at any given time; and
- any restrictions on the customer's permitted use.

- حقوق العميل بخصوص استخدام الخدمات؛
- **من بإمكانه استخدام الخدمات غير العميل** نفسه ؛
- العدد الأقصى من المستخدمين الذين يستطيعون استخدام الخدمات في أي وقت؛ و
- أي قيود مفروضة على العميل عند الاستخدام المسموح به.



Key points:

This section will list who is entitled to use, access, or receive the services. You should also watch out for any restrictions on how the services can be used, accessed, or received.

Grant of Right and Permitted Users

The CSP will usually provide the customer a non-exclusive, non-transferable right to use, receive or access the services for business purposes.

It is also typical for the CSP to allow the customer to share the services with:

- employees, of the customer (they are often referred to as "Authorized Users") depending on the service and the licensing model; and
- a subsidiary of the customer (often referred to as an "Affiliate").

النقاط الأساسية:

سوف يسرد هذا القسم من يحق له استخدام الخدمات او الوصول اليها او تلقيها. يجب عليك ايضاً الانتباه لأي قيود على كيفية استخدام الخدمات او الوصول اليها او تلقيها.

منح الحق والمستخدمين المصرح لهم

عادةً ما يوفر مقدم خدمة السحابة للعميل حقاً غير حصري وغير قابل للتحويل لاستخدام الخدمات او تلقيها او الوصول اليها لأغراض تجارية.

من المعتاد ايضاً ان يسمح مقدم خدمة السحابة للعميل بمشاركة الخدمات مع:

- الموظفين والعميل (يشار إليهم غالباً باسم "المستخدمون المعتمدون") اعتماداً على الخدمة ونموذج الترخيص؛ و
- شركة تابعة للعميل (يشار اليها غالباً باسم "الشركة التابعة").

Do not assume that the cloud contract automatically allows you to share the services with anyone. If this is important to your company, you must ensure that the contract allows you to do so.

لا تفترض ان العقد السحابي يسمح لك تلقائياً بمشاركة الخدمات مع أي شخص. إذا كان هذا مهماً لشركتك، فيجب عليك التأكد من ان العقد يسمح لك بالقيام بذلك.

In addition, you must be aware that your company will be responsible and fully liable for the Authorized Users' and Affiliates' use of the services.

بالإضافة الى ذلك، يجب ان تدرك ان شركتك ستكون مسؤولة بالكامل عن استخدام المستخدمين المعتمدين والشركات التابعة للخدمات.

Restrictions

القيود

The CSP may include restrictions on the way you, your Authorized Users and Affiliates can use the services.

Common examples include:

- The CSP restricts the maximum number of users that the customer (including its Authorized Users and Affiliates) can allow to use the services at any one time;
- the customer is not allowed to sub-license the right to use the services to an unauthorized third party; and
- the customer is not allowed to reverse engineer the services.

Having a clear understanding of the restrictions will help you make sure your company can avoid being in breach.

قد يتضمن مقدم خدمة السحابة قيوداً على الطريقة التي يمكنك بها انت والمستخدمون المعتمدون والشركات التابعة لك استخدام الخدمات.
تشمل الأمثلة الشائعة ما يلي:

- يقيد مقدم خدمة السحابة الحد الأقصى لعدد المستخدمين الذي يمكن للعميل (بما في ذلك المستخدمون المعتمدون والشركات التابعة) السماح لهم باستخدام الخدمات في أي وقت؛
- لا يُسمح للعميل بترخيص من الباطن الحق في استخدام الخدمات لطرف ثالث غير مصرح له؛ و
- لا يسمح للعميل بإجراء هندسة عكسية للخدمات.

سيساعدك فهم القيود بشكل واضح على التأكد من ان شركتك يمكن ان تتجنب الانتهاك.

2.7 Compliance With Service Levels

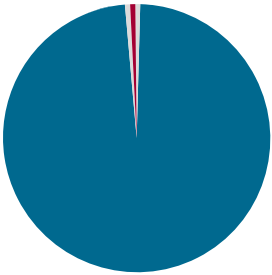
2.7 الامتثال لمستويات الخدمة

This clause describes the level at which the services will be performed by the CSP as well as the customer's potential remedies if the Service Levels are not met.

يصف هذا البند المستوى الذي سيتم عنده أداء الخدمات بواسطة مقدم خدمة السحابة بالإضافة الى الحلول المحتملة للعميل إذا لم يتم الوفاء بمستويات الخدمة.

This clause should always be read in conjunction with (if it exists) the associated schedule generally entitled "Service Level Agreement" or "SLA".

يجب دائماً قراءة هذا البند بالاقتران (إن وجد) بالجدول المرتبط المسمى بشكل عام "اتفاقية مستوى الخدمة" أو "اتفاقية مستوى الخدمة".



Service uptime means time that services are available (e.g. 23h 45m)
يُقصد بوقت التشغيل ان الخدمات متاحة (مثال 23 ساعة و 45 دقيقة)

Service downtime means time that services are unavailable (e.g. 15m)
يُقصد بفترة التعطل ان الخدمات غير متاحة (مثال 15 دقيقة)

Key points:

This provision is typically very short as specific details are contained in the "SLA".

You should pay particular attention to the provisions related to service availability and unavailability (also commonly referred to as "Service Downtime") and determine what level of service availability is required to the success of your company.

Service Availability and Downtime

The CSP will often set out the service availability as a percentage.

You should calculate the exact hours of service availability and downtime, and carefully consider the financial and reputational implications to your business of any service downtime. In practice, cloud service providers offer to their customers a service level agreement (SLA) that stipulates (among other things) the amount of time their systems will be up and running throughout the year. This is critically important for businesses that rely upon high levels of system availability to deliver their own products and services.

النقاط الأساسية:

عادةً ما يكون هذا الحكم قصيراً جداً نظراً لوجود تفاصيل محددة في "اتفاقية مستوى الخدمة".

يجب ان تولي اهتماماً خاصاً للأحكام المتعلقة بتوافر الخدمة وعدم توفرها (يشار اليها ايضاً باسم "تعطل الخدمة") وتحديد مستوى توفر الخدمة المطلوب لنجاح شركتك.

توفر الخدمة ووقت التعطل

غالباً ما يحدد مقدم خدمة السحابة مدى توفر الخدمة كنسبة مئوية.

يجب عليك ان تحسب ساعات اتاحة الخدمة ووقت التعطل بشكل دقيق، والنظر بعناية في الاثار المادية والمتعلقة بالسمعة لشركتك في حال توقف الخدمة.

من الناحية العملية، يقدم مقدمو الخدمات السحابية لعملائهم اتفاقية مستوى الخدمة التي تنص (من بين أشياء أخرى) على مقدار الوقت الذي سيتم فيه تشغيل أنظمتهم على مدار العام. هذا أمر بالغ الأهمية للشركات التي تعتمد على مستويات عالية من توافر النظام لتقديم منتجاتها وخدماتها.

A good SLA should cover a variety of factors, but none are more important than uptime reliability. Uptime reliability is generally expressed as a percentage that gets as close as possible to perfection. The more 9s of availability, the more time servers will be up and running throughout the year. An SLA downtime provision that promises 99.99% system availability, for example, is more reliable than one that promises 99.9% uptime.Accordingly, you shall consider the consequences of a service downtime during business-critical hours and agree with the CSP to an SLA which is compatible with your business requirements. For example, an uptime percentage of 99.9% corresponds to an average of 8.76 hrs. annual SLA downtime, while an uptime percentage of 99.9999% corresponds to an annual downtime of 3.15 sec.

The SLA will also state the financial remedy that you are entitled to if the CSP fails to meet the service level (provided that your actions or inactions did not cause the service level failure). This remedy often comes in the form of a service credit (explained below).

Service Credit

When the CSP fails to achieve a service level, you will generally become entitled to a service credit. A service credit is a pre-determined amount of money which can be used by the customer to deduct from the financial amount paid or payable under the contract.

You should know that service credits are typically the only remedy available for certain service level failures and that it is common for service credits to have a fixed maximum limit.

يجب أن تغطي اتفاقية مستوى الخدمة الجيدة مجموعة متنوعة من العوامل، ولكن لا شيء أكثر أهمية من موثوقية وقت التشغيل. يتم التعبير عن موثوقية وقت التشغيل بشكل عام كنسبة مئوية تقترب قدر الإمكان من الكمال. كلما زاد توافر 9 ثوان، زادت مدة تشغيل الخوادم على مدار العام. شرط وقت تعطل اتفاقية مستوى الخدمة الذي يعد بتوافر النظام بنسبة 99.99٪، على سبيل المثال، أكثر موثوقية من ذلك الذي يعد بوقت تشغيل بنسبة 99.9٪.وفقًا لذلك، يجب أن تفكر في عواقب تعطل الخدمة أثناء ساعات العمل الحرجة وتتفق مع مقدم خدمة السحابة على اتفاقية مستوى الخدمة التي تتوافق مع متطلبات عملك. على سبيل المثال، نسبة وقت التشغيل 99.9٪ تقابل متوسط 8.76 ساعة. وقت تعطل اتفاقية مستوى الخدمة السنوية، في حين أن نسبة وقت التشغيل البالغة 99.9999٪ تقابل وقت تعطل سنوي قدره 3.15 ثانية.

ستحدد اتفاقية مستوى الخدمة أيضًا التعويض المالي الذي يحق لك الحصول عليه إذا فشل مقدم خدمة السحابة في تلبية مستوى الخدمة (بشرط ألا تتسبب أفعالك أو عدم تصرفك في فشل مستوى الخدمة). غالبًا ما يأتي هذا العلاج في شكل ائتمان خدمة (موضح أدناه).

ائتمان الخدمة

عندما يفشل مقدم خدمة السحابة في تحقيق مستوى الخدمة، ستكون بشكل عام مؤهلاً لائتمان الخدمة. ائتمان الخدمة هو مبلغ محدد مسبقاً من المال حيث يستطيع العميل استخدامه للخصم من المبلغ المالي المدفوع او يمكن دفعه بموجب العقد.

يجب ان تكون على دراية بأن ائتمان الخدمة هو عادةً العلاج المتاح لفشل معين في مستوى الخدمة وانه من الشائع تواجد حد اقصى ثابت بالنسبة لائتمان الخدمة.

2.8 Charges

This clause means the amount of fees payable by your company to the CSP in return for the services.

2.8 الرسوم

يقصد بهذا البند مقدار الرسوم المستحقة على شركتك لمقدم خدمة السحابة مقابل الخدمة.

Key points:

You should make sure to pay the charges on time and should also watch out for any unexpected additional charges or lack of transparency with charges.

You should check the price plans with your CSP. You may be able to leverage specific pricing plans offered by the CSP to significantly lower your total cost of service.

Additional charges / Lack of transparency

The CSP may state charges for the services clearly but may not be transparent in relation to any additional charges that may be payable for additional services such as associated maintenance, recovery, add-ons and upgrades.

You should pay particular attention to what charges are payable for the services described in the contract, and what additional fees may be charged by the CSP.

النقاط الأساسية:

يجب عليك التأكد من دفع الرسوم في الوقت المحدد، كما يجب عليك الانتباه لأي رسوم إضافية غير متوقعة او عدم شفافية الرسوم.

يجب عليك التحقق من خطط الأسعار مع مقدم خدمة السحابة الخاص بك. قد تكون قادراً على الاستفادة من خطط التسعير المحددة التي يقدمها مقدم خدمة السحابة لتقليل التكلفة الاجمالية للخدمة بشكل ملحوظ.

رسوم إضافية/نقص الشفافية

قد يذكر مقدم خدمة السحابة رسوم الخدمة بشكل واضح، ولكن قد لا يكون شفافاً فيما يتعلق بأي رسوم إضافية من المحتمل دفعها مقابل خدمات إضافية، مثل الصيانة المصاحبة، او الاسترجاع، او الاضافات، او التحسينات.

يجب عليك الانتباه من تكاليف مدفوعة للخدمات التي تم وصفها في العقد، وما هي الرسوم الإضافية التي قد يطالب بها مقدم خدمة السحابة.

2.9 Customer Data

This clause describes how all the data the customer provides to the CSP (generally called "Customer Data") is protected and securely stored.

The CSP will typically state that it will take all steps to ensure that the Customer Data is protected in accordance with the security measures set out in the contract.

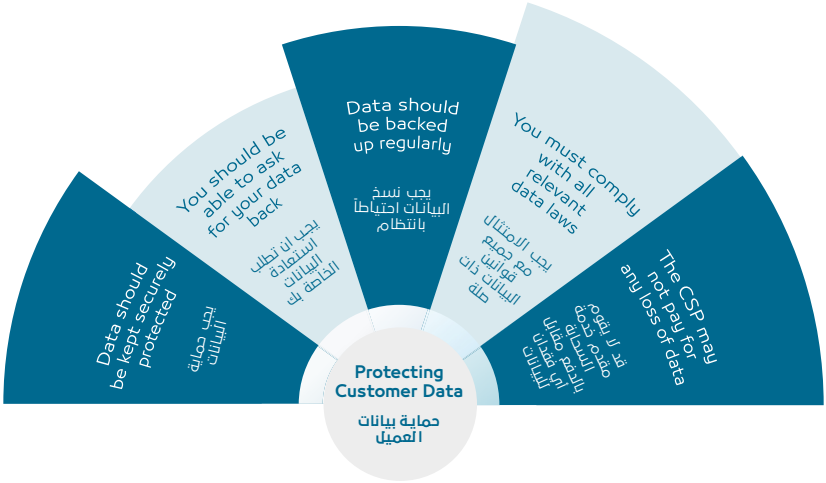
There may be a schedule at the end of the contract entitled "Data Management" which will provide additional detail on the CSP's data management policies, and the CSP's security measures.

2.9 بيانات العميل

يصف هذا البند كيفية حماية جميع البيانات التي يقدمها العميل الى مقدم خدمة السحابة (تسمى بشكل عام "بيانات العميل") وتخزينها بشكل آمن.

سيذكر مقدم خدمة السحابة عادةً انه سيتخذ جميع الخطوات لضمان حماية بيانات العميل وفقاً للتدابير الأمنية المنصوص عليها في العقد.

قد يكون هناك جدول زمني في نهاية العقد بعنوان "إدارة البيانات" والذي سيوفر تفاصيل إضافية حول سياسات إدارة البيانات الخاصة بمقدم خدمة السحابة والتدابير الأمنية الخاصة بمقدم خدمة السحابة.



Key points:

You should pay attention to the following security measures and assess whether they are adequate to protect your Customer Data and the interest of your company.

النقاط الأساسية:

يجب عليك الانتباه من التدابير الأمنية التالية لتحديد ما إذا كانت مناسبة لحماية بيانات العميل ومصالح شركتك.

Back up

You should check whether the CSP has a regular back up, restoration and integrity check process to preserve the Customer Data in the event of any security breach.

دعم

يجب عليك التحقق مما إذا كان مقدم خدمة السحابة لديه عملية فحص الاستعادة الاحتياطية والتكامل للحفاظ على بيانات العميل في حال حدوث أي خرق أمني.

Some of the considerations in this respect are:
- the number of data backups made in a period,
- the methods of backup and backup verification,
- the backup retention period, the number of backups retained,
- the location of backup storage,
- the number of restoration tests and the availability of test reports, and
- the alternative methods for restoring data.

تتضمن بعض الاعتبارات في هذا الصدد ما يلي:
- رقم النسخ الاحتياطية للبيانات المؤلفة في هذه الفترة،
- طرق النسخ الاحتياطي وتدقيقه،
- فترة الاحتفاظ بالنسخ الاحتياطية، رقم النسخ الاحتياطية التي تم الاحتفاظ بها،
- موقع مخزن النسخ الاحتياطية،
- رقم اختبارات التجديد وتوفر تقارير الاختبارات، و
- الطرق البديلة لتجديد البيانات.

Security classification

The CSP may use security classification to protect Customer Data. This involves you or the CSP assigning certain labels (or classifications) to Customer Data depending on the level of criticality and sensitivity of the data set.

You should therefore:

- determine whether the classification scheme is adequate and appropriate to protect your company's business critical and sensitive data; and
- consider the impact of a security breach in relation to Customer Data.

A typical data classification process is provided in Annex 1

التصنيف الأمني

قد يستخدم مقدم خدمة السحابة التصنيف الأمني لحماية بيانات العميل، يتضمن ذلك قيامك انت او مقدم خدمة السحابة بتعيين تسميات (او تصنيفات) معينة لبيانات العميل اعتماداً على مستوى الأهمية والحساسية لمجموعة البيانات.

لذلك يجب عليك:

- تحديد ما إذا كان مخطط التصنيف مناسباً لحماية البيانات المهمة والحساسة لأعمال شركتك؛ و
- النظر في تأثير الخرق الأمني فيما يتعلق ببيانات العميل.

يتم توفير عملية تصنيف بيانات نموذجية في الملحق 1.

Data location

You may want to ask your CSP for a list of the geographic locations that Customer Data may be processed and stored, and if you can specify location requests.

موقع البيانات

قد ترغب في ان تطلب من مقدم خدمة السحابة الخاص بك قائمة بالمواقع الجغرافية التي قد تتم معالجة بيانات العميل وتخزينها، وإذا كان بإمكانك تحديد طلبات الموقع.

Transferability / Portability

You should ensure that you are entitled to transfer your Customer Data back to you or a new CSP upon request. If you cannot transfer the Customer Data immediately or at all, then you should carefully consider the practical implications on the business.

Liability regime

The CSP will typically state that it will restore the lost or damaged Customer Data from the latest back-up of the Customer Data maintained by the CSP in the event of any loss, destruction, or corruption of Customer Data.

It is also common for the CSP to state that they will not be liable for any loss, destruction, or corruption of Customer Data if it was caused by the customer, or a third party engaged by the customer.

2.10 Data Protection

This clause describes how the CSP will use personal data provided by you, the customer.

Typically, the CSP will be permitted to use the personal data only for a specific purpose related to the services that will be provided under the contract.

It is also common for the parties to sign an entirely separate agreement dealing with the obligations of each party for handling personal data (often referred to as the "Data Processing Agreement"). This would be attached as a schedule to the main contract.

قابلية النقل

يجب عليك التأكد من انه يحق لك نقل بيانات العميل الخاصة بك اليك او الى مقدم خدمة سحابة جديد عند الطلب. إذا لم تتمكن من نقل بيانات العميل على الفور او على الاطلاق، فعليك التفكير بعناية في الاثار العملية على شركتك.

نظام المسؤولية

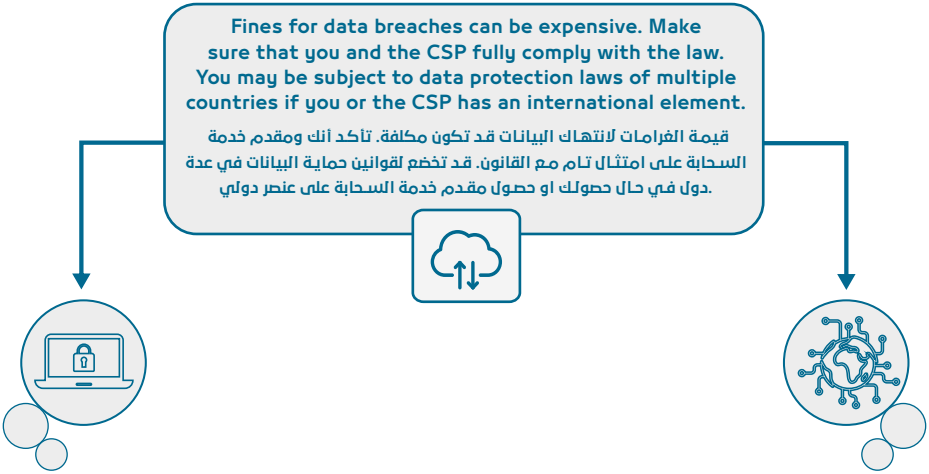
قد ينص مقدم خدمة السحابة انه سيجدد بيانات العميل الضائعة او المتلفة من اخر نسخة احتياطية من بيانات العميل المحفوظة من قبل مقدم خدمة السحابة في حال حصول فقدان او اتلاف او تشويه لبيانات العميل.

كما انه من الشائع ان ينص مقدم خدمة السحابة انه لن يكون مسؤول عن أي نوع من فقدان او اتلاف او تشويه لبيانات العميل إذا كان سببه يرجع للعميل نفسه، او عن طريق طرف ثالث يشمله العميل.

2.10 حماية البيانات:

يصف هذا البند على كيفية استخدام مقدم خدمة السحابة للبيانات الشخصية المقدمة منك، ا لعميل .
سيكون من المشروع لمقدم خدمة السحابة عادةً باستخدام البيانات الشخصية لغرض متعلق بالخدمات فقط والذي سيكون متوفر بموجب ا لعقد .

كما انه من الشائع للأطراف بتوقيع اتفاق منفصل يتعلق بمتطلبات كل طرف عند استخدام البيانات الشخصية (والذي يشار اليه عادةً "باتفاقية معالجة البيانات"). يتم ارفاق ذلك في شكل جدول في العقد الأساسي.



Key points:

Under most data protection legislations, as customer, your company is the "data controller", Therefore, you must ensure that you have all the necessary consents and notices in place to enable lawful transfer of the personal data to the CSP.

Once you have all necessary consents and notices to enable the lawful transfer, you must then assess whether the CSP has adequate security measures and understand the CSP's responsibility to protect the personal data.

You should pay particular attention to:

- the ownership and who has control over data;
- the definition of Customer Data and CSP data;
- the details of how the personal data is processed;
- the rights of each party concerning the personal data; and
- the obligations of each party concerning the personal data.

To ensure that the CSP will adequately protect personal data, you should ensure that the CSP has agreed in the contract that:

النقاط الأساسية:

تحت معظم قوانين حماية البيانات، تعتبر شركتك "جامع البيانات" كعميل. ولذلك، يجب عليك التأكد من ان بحوزتك جميع الموافقات والاخطارات الضرورية لتمكين التحويل القانوني للبيانات الشخصية الى مقدم خدمة السحابة.

عندما تكون بحوزتك جميع الموافقات والاخطارات الضرورية لتمكين التحويل القانوني، يجب عليك تقييم ما إذا مقدم خدمة السحابة لديه التدابير الأمنية المناسبة وفهم مسؤولية مقدم خدمة السحابة لحماية البيانات الشخصية.

يجب عليك الانتباه للنقاط الاتية:

- الملكية ومن يتحكم في البيانات؛
- تعريف بيانات العميل وبيانات مقدم خدمة السحابة؛
- تفاصيل عن كيفية إتمام معالجة البيانات الشخصية؛
- حقوق كل طرف بخصوص البيانات الشخصية؛ و
- متطلبات كل طرف بخصوص البيانات الشخصية.

للتأكد من ان مقدم خدمة السحابة سيقوم بحماية البيانات الشخصية بشكل مناسب، يجب عليك التأكد من ان مقدم خدمة السحابة قد قام بالموافقة على الآتي في العقد:

- it complies with the applicable data protection legislation;
- it will only process any personal data upon your instructions;
- it has the appropriate technical and organizational security to protect against unauthorized or unlawful processing of personal data;
- it has the appropriate technical and organizational solutions to deal with accidental loss, destruction or damage to personal data;
- it will ensure that any CSP employees or representatives who have access to the personal data are required to keep this information confidential; and it will not transfer any personal data outside the jurisdiction stated in the contract without first receiving your written consent;
- it will only engage a sub-processor with your authorization and the sub-processor will have the same obligations as the CSP; and
- it will remain liable for the compliance with all the data protection requirements of any sub-processor it engages.
- it will completely delete Customer Data within defined minimum and maximum times in accordance with a data deletion process and a data deletion notification policy.

- الامتثال مع قانون حماية البيانات المعمول بها ؛
- سيقوم بمعالجة أي بيانات شخصية بناءً على تعليما تك ؛
- لديه متطلبات الامن المناسبة والفنية والتنظيمية لحماية البيانات الشخصية ضد المعالجة غير المصرح بها وغير القانونية؛

- لديه الحلول المناسبة والفنية والتنظيمية للتعامل مع الفقدان العرضي او التلف او الضرر للبيانات الشخصية؛

- التأكد من ان أي موظف مقدم خدمة السحابة او ممثلين لديهم تصريح الوصول الى البيانات الشخصية ملزمين للاحتفاظ بتلك المعلومات بشكل سري؛ وعدم نقل أي معلومات شخصية خارج النطاق المنصوص عليه في العقد بدون الحصول على موافقة خطية منك؛

- انه سيستخدم معالجاً فرعياً فقط مع تصريح منك، وان المعالج الفرعي لديه التزامات مقدم خدمة السحابة؛ و
- سيكون مسؤول عن أي امتثال مع متطلبات حماية البيانات لأي معالج فرعي يقوم بالتعامل معه .
- سيقوم بحذف شامل لبيانات العميل مع الامتثال لأوقات الحد الأدنى والاقصى بما يتماشى مع عملية معالجة حذف البيانات وسياسة اخطار حذف البيانات.

2.11 Security

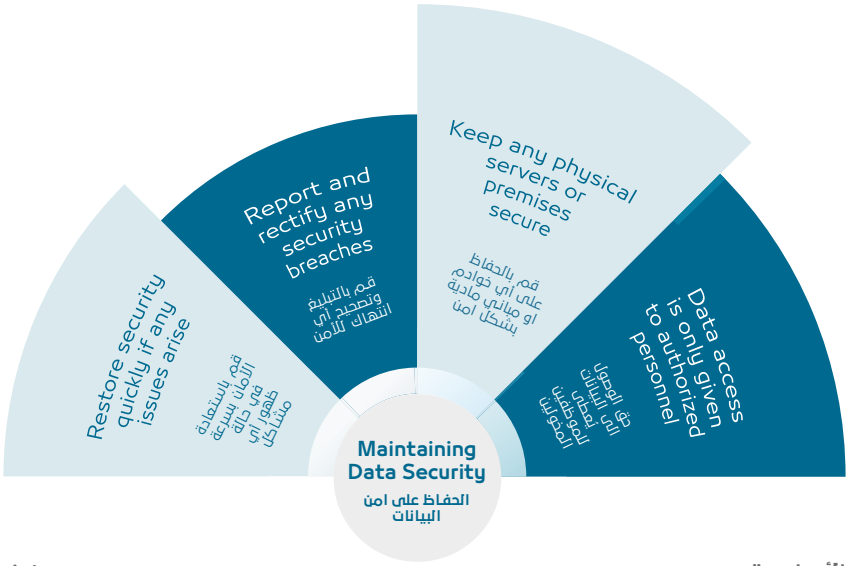
This clause describes the CSP's obligation to apply and maintain a reasonable level of security when providing the service to the Customer. This includes having security measures ready to protect the storage and processing of Customer Data (including personal data).

Further details of the CSP's security obligations, certification requirements, safeguards, and privacy features are often contained in a schedule to the cloud contract entitled "Security Management".

2.11 الامن:

ينص هذا البند على التزامات مقدم خدمة السحابة لتطبيق والمداومة على مستوى معقول من الحماية عند تقديم الخدمة للعميل. يشمل ذلك على إبقاء تدابير الحماية جاهزة لحماية المخزن ومعالجة بيانات العميل (تعتبر البيانات الشخصية ضمن هذه القائمة).

تحتوى التفاصيل الأخرى عن متطلبات الامن من مقدم خدمة السحابة ومتطلبات التصديق والضمان وخصائص الخصوصية في جدول في عقد السحابة تحت عنوان "إدارة الامن".



النقاط الأساسية:

يجب عليك الانتباه جيداً على الاتي عند تقييم الضابط الأمنية المقدمة من قبل مقدم خدمة السحابة:

- هل يقدم مقدم خدمة السحابة تشفير بيانات مناسب؟
- ما هي التدابير الأمنية المتوفرة للحماية من الدخول غير المصرح به؟
- كيف يقوم مقدم خدمة السحابة بمراقبة الدخول للبيانات؟
- هل مقدم خدمة السحابة ملزم بتبليغ العميل في حال حدوث أي خرق أمني؟ وإذا كان الامر كذلك، ما مدى سرعة اخطار مقدم خدمة السحابة العميل؟
- هل مقدم خدمة السحابة ملزم للتخفيف ضد أي خرق أمني؟
- ماهي الخطة الموضوعة من قبل مقدم خدمة السحابة لاستعادة الامن في حال حدوث خرق أمني؟

Key points:

You should pay particular attention to the following when assessing the security controls offered by the CSP

- does the CSP provide adequate encryption of data?
- what security measures are in place to prevent unauthorized access?
- how does the CSP monitor the access to data?
- is the CSP obliged to notify the customer in the event of any security breaches? If so, how quickly should they notify the customer?
- is the CSP required to mitigate against any security breaches?
- what plan does the CSP have to restore the security in the event of a breach?

Physical and environmental security

You must consider whether the CSP maintains the following physical and environmental security measures as a minimum:

- Secure physical access to facilities where Customer Data is located;
- Data encryption; and
- Appointment of security officers responsible for coordinating and monitoring the security.

الحماية المادية والبيئية

يجب عليك النظر فيما إذا مقدم خدمة السحابة يحافظ على التدابير المادية والبيئية الاتية كحد أدنى:

- حماية الدخول المادي الى المرافق حيث توجد بيانات العميل؛
- تشفير البيانات؛ و
- تعيين موظفي امن مسؤولين عن تنسيق ومراقبة الحماية.

Data access controls

You must consider whether the CSP maintains the following data access controls to ensure the protection of Customer Data:

- Access authorization, i.e. the CSP's policy on authorizations and access logs; and a clear definition of the purposes for which your CSP can use Customer Data;
- Authentication, i.e. measures to identify and authenticate users who attempt to access the Customer Data, for example passwords.

You must also ensure that it has a policy to govern data and access controls within its organization as well as secure access credentials.

ضوابط الوصول الى البيانات

يجب عليك النظر فيما إذا مقدم خدمة السحابة يحتفظ بضوابط الوصول الى البيانات الاتية لضمان حماية بيانات العميل:

- الوصول المصرح به، ويقصد بذلك سياسة مقدم خدمة السحابة بخصوص التصريحات وسجل الوصول؛ وتعريف واضح للأغراض التي يمكن لمقدم خدمة السحابة الخاص بك استخدام بيانات العميل من اجلها؛
- التوثيق، ويقصد بذلك التدابير لتعريف وتوثيق المستخدمين الذين يحاولون الوصول الى بيانات العميل، على سبيل المثال كلمة السر.

يجب عليك ايضاً التأكد من ان مقدم خدمة السحابة لديه سياسة لحوكمة البيانات وضوابط الوصول داخل المنظمة، بالإضافة الى مؤهلات وصول مضمونة.

Incident management

You must consider whether the CSP maintains data incident management policies to ensure that security breaches are identified, reported, and rectified.

إدارة الازمات

يجب عليك النظر فيما إذا مقدم خدمة السحابة يحتفظ بسياسات إدارة ازمات البيانات لضمان تحديد خروقات الامن، والتبليغ عنها وتصحيحها.

2.12 Indemnities

The term "Indemnity" means a promise by one party to pay back the other for the loss suffered by the other party as a result of a specified event.

This clause, generally referred to as "Indemnities", describes the circumstances where the parties have agreed to indemnify the other party, or in other words, be liable to pay the loss, expenses, or damage suffered by the other party as a result of a particular event.

2.12 التعويضات:

يقصد بمصطلح "التعويضات" وعد من قبل طرف لتسديد الطرف الاخر اي خسائر تعرض اليها الطرف الاخر نتيجةً لحدث معين.

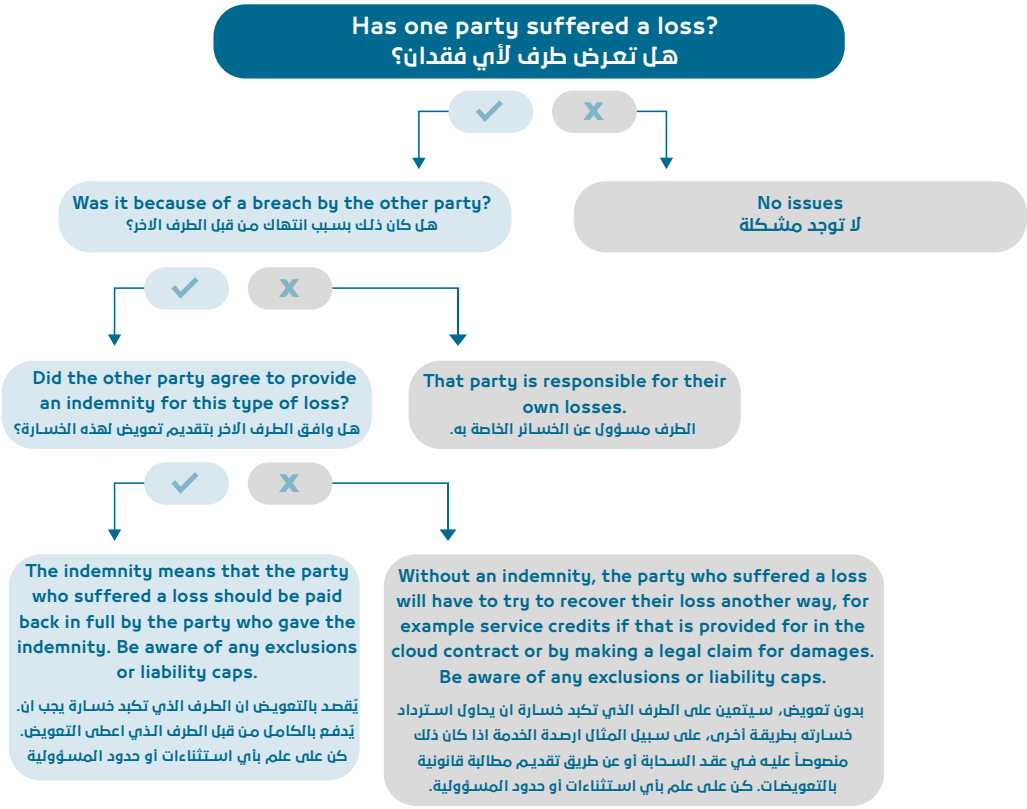
هذا البند، والذي يشار اليه عادةً "بالتعويضات"، يصف الظروف التي أدت الى موافقة الأطراف لتعويض الطرف الاخر، او بمعنى اخر، يكون مسؤول عن تسديد خسائر او تكلفة او ضرر تعرض اليها الطرف الاخر نتيجةً لحدث معين.

The CSP will typically be required to indemnify the Customer for all losses, liability, damages, or expenses incurred by the Customer as a result of:

- any claims that the receipt or use by the Customer of the services infringes any third-party intellectual property rights; and
- the CSP's failure to comply with data protection legislation and data protection provisions set out in the contract.

يكون مقدم خدمة السحابة عادةً ملزم بتعويض العميل نتيجة لجميع الخسائر، او المسؤوليات، او الاضرار، او التكاليف المتكبدة من قبل العميل نتيجة للآتي:

- أي ادعاء ان استلام او استخدام من قبل العميل للخدمات ينتهك حق من الحقوق الملكية الفكرية لطرف ثالث؛ و
- فشل مقدم خدمة السحابة للامتثال مع قانون حماية البيانات واحكام حماية البيانات المنصوص عليها في العقد.



Key points:

In addition to making sure that the CSP will indemnify you for the events specified above, you need to also consider the following pitfalls.

Limits

You must pay particular attention to whether there are any financial limits to the amount of money the CSP or Customer can be indemnified for.

The actual financial limit is often set out in the section titled "Limitation of Liability" which is detailed in "Limitation of Liability" below.

Exclusion

There will be "exclusions" to the indemnities, which are situations where the CSP will not indemnify or reimburse you at all. You should be aware of these exclusions.

Customers Indemnity

It is common for the CSP to require that the Customer indemnify the CSP for all losses, liability, damages, or expenses incurred by the CSP for any claim by a third-party alleging that the CSP's use of the Customer Data or Customer's systems infringes any third-party intellectual property rights.

2.13 Warranties

The term "Warranty" means a promise that certain statements made in the contract are true. A party breaches a warranty if the statement they made was or becomes untrue. If a party breaches a warranty and the other innocent party suffers a loss, the innocent party may be entitled to claim damages from the party that gave the warranty.

النقاط الأساسية:

اضافةً للتأكد من ان مقدم خدمة السحابة سيقوم بتعويضك للحوادث المنصوص عليها أعلاه، يجب عليك الانتباه للسلبيات الاتية.

الحدود

يجب عليك الانتباه جيداً ما إذا كانت هناك أي حدود مالية لقدر الثمن الذي يمكن لمقدم خدمة السحابة او العميل تعويضه:

ان الحد المالي الفعلي يكون منصوص عليه في قسم بعنوان "حدود المسؤولية"، وهو مفصل ادناه تحت مسمى "حدود المسؤولية".

الاستثناء

ستكون هناك "استثناءات" للتعويضات، وهي الحالات التي لن يقوم فيها مقدم خدمة السحابة بتعويضك على الاطلاق. يجب عليك ان تكون مدركاً لهذه الاستثناءات.

تعويض العميل

من الشائع ان يطلب مقدم خدمة السحابة من العميل تعويض مقدم خدمة السحابة عن جميع الخسائر، او المسؤولية، او الاضرار، او النفقات التي يتكبدها مقدم خدمة السحابة عن أي مطالبة من قبل طرف ثالث تزعم ان استخدام مقدم خدمة السحابة لبيانات العميل او أنظمة العميل ينتهك أي حقوق الملكية الفكرية للغير.

2.13 الضمانات

مصطلح "الضمان" يعني الوعد بصحة بعض البيانات الواردة في العقد. ينتهك أحد الأطراف الضمان إذا كان البيان الذي ادلى به غير صحيح او أصبح غير صحيح. إذا انتهك أحد الطرفين الضمان وتعرض الطرف البريء لخسارة، فقد يحق للطرف البريء المطالبة بتعويضات من الطرف الذي قدم الضمان.

Did one party make a warranty?
هل قدم طرف من الاطراف ضماناً؟

✓ / X

Was that warranty untrue, inaccurate or breached?
هل كان الضمان غير صحيح أو غير دقيق أو منتهك؟

The wronged party cannot rely on a breach of warranty.
لا يمكن للطرف المخطئ الاعتماد على خرق الضمان.

✓ / X

Did the party relying on the warranty suffer loss or damage?
هل تعرض الطرف المعتمد على الضمان للفقدان او التلف؟

The wronged party cannot rely on a breach of warranty.
لا يحق للطرف المخطئ الاعتماد على خرق الضمان.

✓ / X

Was that type of loss or damage excluded in the contract?
هل كان نوع الفقدان أو التلف مستبعد في العقد؟

The party is not entitled to damages if there has been no loss.
لا يحق للطرف الحصول على تعويضات في حال عدم حصول أي فقدان.

✓ / X

The party is not entitled to damages if that type of damage is excluded in the contract.
لا يحق للطرف الحصول على تعويضات في حال كان نوع التلف مستبعد في العقد.

Is the loss or damage covered by an indemnity?
هل تغطي التعويضات على الفقدان أو التلف؟

✓ / X

The indemnity means that the party who suffered a loss should be paid back in full by the party who gave the indemnity. Beware of any liability caps which will be the maximum amount the wronged party will be paid back.
ذلك يعني ان الطرف الذي تكبد خسارة يجب ان يُسترد بالكامل من قبل الطرف الذي اعطى التعويض. احذر من أي سقف للمسؤولية والذي سيكون الحد الأقصى للمبلغ الذي سيتم سداده للطرف المظلوم.

Without an indemnity, the party who suffered a loss will have to try to recover their loss another way, for example, service credits if that is provided for in the cloud contract or by making a legal claim for damages. Beware of any liability caps which will be the maximum amount the wronged party will be paid back.
بدون تعويض، سيتعين على الطرف الذي تكبد خسارة محاولة استرداد خسارته بطريقة أخرى، على سبيل المثال، ارصدة الخدمة إذا كان ذلك منصوصاً عليه في عقد السحابة او عن طريق تقديم مطالبة قانونية بالتعويضات. احذر من أي حدود للمسؤولية والتي ستكون الحد الأقصى للمبلغ الذي سيتم سداده للطرف المظلوم.

Key points:

In addition to understanding exactly what warranties or promises you are making under the contract, you should carefully consider:

- what warranties or promises the CSP is making; and
- any exclusions to those warranties the CSP has stated.

Warranties made by both parties

You should not agree to give a warranty in the contract unless you are absolutely certain that you have the knowledge and expertise to confirm that information about your business.

Warranties made by the CSP

You must ensure that you fully understand the warranties the CSP is making. You should assess whether these warranties are enough to make you comfortable with any business risks.

Exclusions

You must be aware of when the CSP will not provide a warranty. This will typically be stated as an "exclusion" to the warranties provided.

Limitation of liability

You should pay particular attention to whether there are any financial caps or limits to the amount of damages that you are entitled to recover from the CSP if the CSP breaches a warranty.

The actual financial limit is often set out in the section titled "Limitation of Liability" which is detailed in "Limitation of Liability" below.

النقاط الأساسية:

بالإضافة الى فهم الضمانات او الوعود التي تقدمها بموجب العقد، يجب عليك النظر في الاتي بعناية:

- ماهي الضمانات او الوعود التي يقدمها مقدم خدمة السحابة؛ و
- أي استثناءات لتلك الضمانات التي نص عليها مقدم خدمة السحابة.

الضمانات التي تم ابرامها من قبل الطرفين

يجب عليك الا توافق على إعطاء اي ضمان في العقد الا في حال كنت متأكداً تماماً ان لديك المعرفة والخبرة لتأكيد المعلومات عن تجارتك.

الضمانات التي تم ابرامها من قبل مقدم خدمة السحابة

يجب عليك ان تتأكد أنك على دراية بالضمانات التي يبرمها مقدم خدمة السحابة. كما يجب عليك تقييم ما إذا كانت هذه الضمانات كافية لتجعلك ان تشعر بالراحة فيما يخص أي مخاطرة تجارية.

الاستثناءات

يجب عليك ان تكون على دراية عندما لا يقدم مقدم خدمة السحابة أي ضمان. سيكون ذلك منصوص عليه "كاستثناء" للضمانات المقدمة.

حدود المسؤولية

يجب عليك الانتباه جيداً ما إذا كانت هناك أي غطاءات مالية او حدود لقيمة الاضرار التي قد تكون مسؤولاً في تصحيحها من مقدم خدمة السحابة في حال انتهاك مقدم خدمة السحابة لضمان.

ان الحد المالي الفعلي يكون منصوص عليه عادةً في قسم بعنوان "حدود المسؤولية" وهو مفصل في "حدود المسؤولية" ادناه.

2.14 Limitation Of Liability

This clause seeks to limit or exclude the amount one party has to pay to the other innocent party if the innocent party suffers a loss because of certain breaches of the party's obligations or responsibilities in the contract.

2.14 حدود المسؤولية:

يسعى هذا البند لوضع حد او استثناء للمبلغ الذي يجب على أحد الأطراف تسديده للطرف البريء في حال تعرضه للخسائر بسبب انتهاك الطرف لالتزاماته او مسؤولياته المنصوص عليها في العقد.

Key points:

You need to pay particular attention to the following limitations of liability to manage business risk:

- liability caps – the maximum amount of money that the party would pay the other party for any breach or indemnity under the contract;
- unlimited liability – the types of losses that each party accepts to pay the other party for without limit (for example for fraud, death, and personal injury); and
- exclusions – the types of losses each party excludes totally and therefore will not pay the other party for.

النقاط الأساسية:

يجب عليك الانتباه جيداً للحدود التالية حتى تتمكن من إدارة الخطر التجاري:

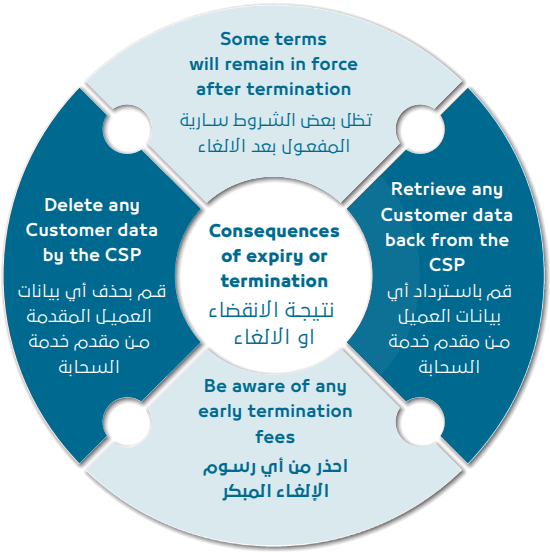
- غطاءات المسؤولية – الحد الأقصى لمبلغ المال الذي يجب على احد الأطراف تسديده للطرف الاخر لأي انتهاك أو تعويض بموجب ا لعقد ؛
- مسؤولية غير محدودة – أنواع الخسائر التي يوافق عليها كل طرف لتسديد الطرف الاخر بدون أي حدود (على سبيل المثال التزوير او الوفاة او إصابة شخصية)؛ و
- الاستثناءات – أنواع الخسائر التي يستثنيها الأطراف وعليه لن يقوموا بتسديدها للطرف ا لاخر.

2.15 Consequences Of Expiry Or Termination

This clause describes what happens after the contract ends.

2.15 نتيجة الانقضاء او الإلغاء:

يشرح هذا البند ما يحدث عند انقضاء فترة سريان العقد.



Key points:

You should be aware that once the contract ends, you will no longer have the right to access or use the services. You need to pay also particular attention to the following other consequences.

النقاط الأساسية:

يجب ان تكون على دراية بأن عند انقضاء فترة سريان العقد، لن يكون لديك الحق للدخول او استخدام الخدمات. يجب عليك ايضاً الانتباه جيداً للعواقب الأخرى التالية:

Retrieval and Deletion of Customer Data

You should always make sure that you have the right to retrieve all of your Customer Data from the CSP upon the expiry or termination of the contract and that the CSP will delete Customer Data within a defined period of time. You must follow the process for doing so as set out in the contract, e.g. making the request to the CSP in writing within a certain timeframe after expiry or termination.

استرداد بيانات العميل وحذفها

يجب عليك دائماً التأكد من ان لديك الحق في استرداد جميع بيانات العميل الخاصة بك من مقدم خدمة السحابة عند انتهاء او إنهاء العقد وان مقدم خدمة السحابة سوف يقوم بحذف بيانات العميل خلال فترة زمنية محددة. يجب عليك اتباع عملية القيام بذلك على النحو المنصوص عليه في العقد، على سبيل المثال تقديم الطلب كتابياً الى مقدم خدمة السحابة في غضون إطار زمني معين بعد انتهاء الصلاحية او الانهاء.

Return of confidential information and property

Each party will be required to return all confidential information and property it has of the other party within defined timelines.

استرداد المعلومات السرية والممتلكات

سيطلب من كل طرف ارجاع جميع المعلومات السرية والممتلكات التي تكون بحوزة الطرف الاخر في غضون إطارات زمنية محددة.

Extra fees

You should make sure that you understand exactly when you will be required to pay additional fees or penalty fees if you terminate the contract early, in other words before the agreed contract Expiry Date.

You should be aware also that if the CSP terminates the contract early, meaning prior to the agreed contract Expiry Date, you may be entitled to receive money back from the CSP for any amounts you have already paid.

الرسوم الإضافية

يجب ان تتأكد من أنك تفهم بالضبط متى سيُطلب منك دفع رسوم إضافية او رسوم عقوبة إذا قمت بإنهاء العقد مبكراً، أي قبل تاريخ انتهاء العقد المتفق عليه.

يجب ان تدرك ايضاً انه إذا أنهى مقدم خدمة السحابة العقد مبكراً، أي قبل تاريخ انتهاء العقد المتفق عليه، فقد يحق لك استرداد الأموال من مقدم خدمة السحابة عن أي مبالغ قمت بدفعها مسبقا .

Survival

It is very common for some contractual rights to stay in effect and in force even after the termination or expiration of the contract. In other words, you should pay attention to any obligations or responsibilities you will continue to have even after the contract has ended.

Some examples of those rights include:

- Data protection requirements;
- Confidentiality obligations; and
- Intellectual property rights and indemnities.

الاستمرارية

من الشائع جداً ان تظل بعض الحقوق التعاقدية سارية المفعول ونافذة حتى بعد إنهاء العقد او انتهاء صلاحيته. بمعنى آخر، يجب الانتباه الى أي التزامات او مسؤوليات ستستمر في تحملها حتى بعد انتهاء العقد.

تتضمن بعض الأمثلة على هذه الحقوق ما يلي:

- متطلبات حماية البيانات؛
- التزامات سرية؛ و
- حقوق الملكية والتعويضات.

2.16 Boiler Plate Provisions – Cloud Specific

"Boiler plate" is the term used to refer to standard clauses that usually appear at the end of the contract. You should carefully consider some of the most important ones that are detailed below.

2.16 احكام الصيغة الشكلية – خاصة بالحوسبة

يستخدم هذا المصطلح للإشارة الى البنود القياسية التي تظهر عادةً في نهاية العقد. يجب ان تفكر ملياً في بعض أهمها الموضحة ادناه.

2.17 Force Majeure

This clause describes when a party's obligations or liabilities under the contract change as a result of a Force Majeure Event occurring.

Key points:

"Force Majeure Event" means any extraordinary circumstance that is not within a party's reasonable control arising from:

- acts of god, flood, drought, earthquake, fire or other natural disasters;
- terrorist attacks, riots or war;
- imposition of sanctions or embargos;
- epidemic or pandemic; or
- labor or trade disputes.

You should be aware of the consequences to your business if a Force Majeure Event prevents the CSP from providing the services.

2.17 القوة القاهرة

يصف هذا البند عندما تتغير التزامات الطرف أو مسؤولياته بموجب العقد نتيجة لحدث قوة قاهرة.

النقاط الأساسية:

يقصد "بالقوة القاهرة" أي حدث استثنائي خارج عن نطاق سيطرة طرف معيين نتيجة للآتي:

- القضاء والقدر، فيضان، قحط، زلزال، حريق او أي نوع من الكوارث الطبيعية؛
- الهجمات الإرهابية، اعمال الشغب أو الحروب؛
- فرض العقوبات أو حظر؛
- وباء أو جائحة؛ او
- المنازعات العمالية أو التجارية.

يجب ان تكون على دراية بالعواقب التي ستلحق تجارتك في حال منعت قوة قاهرة معينة مقدم خدمة السحابة من تقديم الخدمات.

2.18 Sub-Contracting

This clause describes the circumstances where the CSP is permitted to sub-contract its obligations to another party (a "Sub-contractor").

Key points:

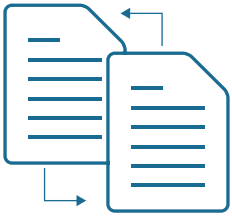
You should be careful in case the cloud contract states that the CSP's obligations may be sub-contracted to a third party without your written consent. You should also pay attention to the "Flow down of obligations" explained below.

2.18 التعاقد من الباطن

يشرح هذا البند الاحداث حيث يكون من المسموح من مقدم خدمة السحابة بالتعاقد من الباطن لالتزاماته لطرف اخر ("متعاقد من الباطن").

النقاط الأساسية:

يجب عليك الانتباه في حال ينص عقد السحابة ان التزامات مقدم خدمة السحابة قد تكون متعاقدة من الباطن مع طرف ثالث دون موافقة خطية منك. كما يجب عليك تولي اهتماماً "لتدفق الالتزامات" الموضح ادناه.



2.19 Flow Down Of Obligations

The CSP should still be responsible and fully liable for the Sub-contractor's performance, compliance, and breach of the contract.

Key points:

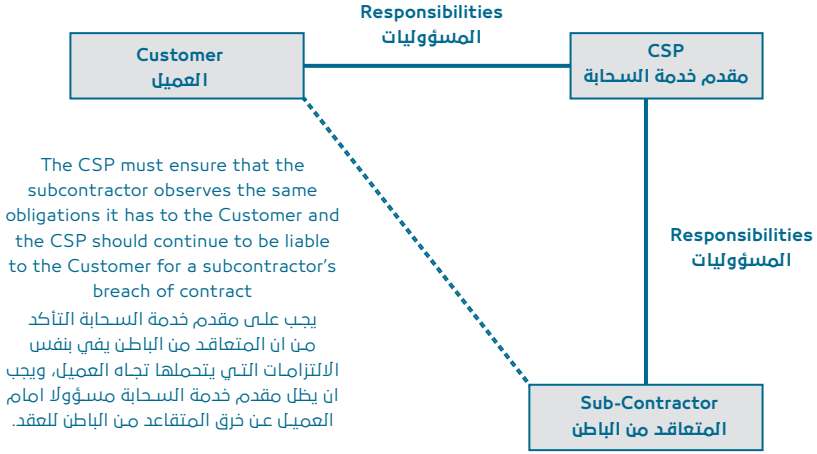
You should carefully consider whether the contract states that the CSP's obligations must be explicitly flowed down to the sub-contractors. This will protect you from any breaches that may arise from the sub-contractor's failure to perform the services.

2.19 تدفق الالتزامات

يجب ان يكون مقدم خدمة السحابة مسؤولاً لممارسات التعاقد من الباطن، والامتثال وانتهاك العقد.

النقاط الأساسية:

يجب عليك النظر فيما إذا ينص العقد ان التزامات مقدم خدمة السحابة يجب ان تكون متدفقة بشكل صريح للتعاقد من الباطن. سيحميك ذلك من أي انتهاكات قد تحصل إثر فشل المتعاقد من الباطن لممارسة الخدمات.



2.20 Governing Law And Jurisdiction

This clause, generally called "Governing Law and Jurisdiction", sets out:

- which country's laws govern the contract i.e. which country's laws will be used to interpret and give effect to the terms of the contract; and
- which country's courts have jurisdiction to resolve any disputes arising out of the contract.

2.20 القانون الحاكم والمختص

يفصل هذا البند والذي يدعى "القانون الحاكم والمختص" عادةً ما يلي:

- ما القوانين المحلية التي تحكم العقد. بمعنى اخر ما هي القانونين المحلية التي ستستخدم لتفسير وإعمال شروط العقد؛ و
- ما المحاكم المحلية التي تتمتع بالصلاحية لحل أي منازعات ناشئة عن العقد.

This clause is important because it will affect the way the contractual clauses are interpreted and where disputes are settled.

ان هـذا البند مهـم جداً بسـبب تأثيره علـى طريقة تفسـير البنـود التعاقديـة وحيـث تتـم تسـوية المنازعـات.

3. Cloud Computing Terms

Below are some of the terms commonly used in the context of cloud computing.

3. شروط الحوسبة السحابية

فيما يلي قائمة بالمصطلحا ت الأكثر استخداماً في سياق الحوسبة السحابية.

Artificial Intelligence الذكاء الاصطناعي	A system or network of computers designed to imitate human intelligence. نظام او شبكة أجهزة حاسوب صنعت لتحاكي الذكاء الإنساني.
Big Data البيانات الكبيرة	Extremely large volumes of complex data that can be analyzed to reveal patterns. كميات كبيرة للغاية من البيانات المعقدة التي يمكن تحليلها للكشف عن الأنماط.
Cloud Computing الحوسبة السحابية	Computing services provided remotely over a network, most commonly the internet. خدمات الحوسبة المقدمة عن بعد عبر الشبكة، وغالباً ما تكون الانترنت.
Cloud Contract عقد السحابة	A contract for cloud services. عقد للخدمات السحابية.
Cloud Service خدمة السحابة	Any cloud computing service which is delivered remotely and on-demand. أي خدمة حوسبة سحابية يتم تقديمها عن بعد وعند الطلب.
Cloud Service Provider مقدم خدمة السحابة	A company that provides cloud services. شركة تقدم خدمات السحابة.
Community Cloud السحابة المجتمعية	A cloud service established for, and shared by, organisations or persons with similar interests or concerns. خدمة سحابية تم انشاؤها ومشاركتها من قبل المنظمات او الأشخاص الذين لديهم اهتمامات او مخاوف مماثلة.
Customer Data بيانات العميل	Any data provided by the customer to the CSP. أي بيانات يقدمها العميل الى مقدم خدمة السحابة.
Data Analytics تحليل البيانات	The process of understanding and interpreting raw data to draw conclusions or identify patterns. عملية فهم البيانات الأولوية وتفسيرها لاستخلاص النتائج أو تحديد الأنماط.
Data Availability توافر البيانات	How readily accessible necessary information, tools, and resources are for the business or service to operate. مدى سهولة الوصول الى المعلومات والأدوات والموارد اللازمة لعمل الشركة او الخدمة.
Data Centre مركز البيانات	A physical facility with a network of computer servers that store applications and data. منشاة مادية مع شبكة من خوادم الحاسوب التي تخزن التطبيقات والبيانات.
Data Classification تصنيف البيانات	The classification of data into categories depending on how sensitive it is, e.g. public, confidential or highly confidential. تصنيف البيانات الى فئات اعتماداً على مدى حساسيتها، على سبيل المثال عامة، سرية أو عالية السرية.
Data Encryption تشفير البيانات	Converting data from a readable format into a coded format which requires a key or password to read. تحويل البيانات من تنسيق قابل للقراءة الى تنسيق مشفر يتطلب مفتاحاً او كلمة مرور للقراءة.
Data Integrity نزاهة البيانات	The quality, accuracy, and consistency of data secured by, for example, preventing data loss or alterations. جودة ودقة واتساق البيانات التي يتم تأمينها على سبيل المثال، من خلال منع فقدان البيانات أو التعديلات.

Data Privacy خصوصية البيانات	Managing personal data that protects each individual's identity and other rights. إدارة البيانات الشخصية التي تحمي هوية كل فرد والحقوق الاخرى.
Hybrid Cloud السحابة الهجينة	The use of private and public cloud solutions such that there is a degree of interaction between the two systems. استخدام حلول السحابة الخاصة والعامة بحيث تكون هناك درجة من التفاعل بين النظامين.
Hyperscale النطاق المفرط	Technological network infrastructure that can be scaled up to increase power in line with the requirements of the customer›s business. البنية التحتية للشبكة التكنولوجية التي يمكن زيادتها لزيادة الطاقة بما يتماشى مع متطلبات عمل العميل.
IaaS (Infrastructure as a Service) البنية التحتية كخدمة	A basic category of cloud services where the customer subscribes for access only to underlying infrastructure such as storage capacity, processing power and networking. فئة أساسية من الخدمات السحابية حيث يشترك العميل للوصول فقط الى البنية التحتية الأساسية مثل سعة التخزين وقوة المعالجة والشبكات.
Machine Learning التعليم الالي	A subset of artificial intelligence where computers learn to improve their outputs with experience of running models without being specifically programmed. مجموعة فرعية من الذكاء الاصطناعي حيث تتعلم أجهزة الحاسوب تحسين مخرجاتها من خلال تجربة تشغيل النماذج دون ان تكون مبرمجة بشكل خاص.
PaaS (Platform as a Service) المنصة كخدمة	A category of cloud services where the platform applications and infrastructure are provided by the CSP, and the customer deploys its own software applications. فئة من الخدمات السحابية حيث يتم توفير تطبيقات النظام الأساسي والبنية التحتية بواسطة مقدم خدمة السحابة، وينشر العميل تطبيقات البرامج الخاصة به.
Personal Data البيانات الشخصية	Any information relating to an identified or identifiable natural person. أي معلومات تتعلق بشخص طبيعي محدد او يمكن التعرف عليه.
Platform المنصة	The environment in which a software operates, e.g. the operating system or a web browser. البيئة التي يعمل فيها البرنامج، على سبيل المثال نظام تشغيل أو مستعرض الويب.
Private Cloud السحابة الخاصة	A cloud which hosts a cloud service that is dedicated to one organisation. سحابة تستضيف خدمة سحابية مخصصة لمؤسسة واحدة.
Public Cloud السحابة العامة	A cloud where a CSP makes services available over the internet to any customer سحابة حيث يتيح مقدم خدمة السحابة الخدمات عبر الانترنت لأي عميل.
Scalability قابلية التوسع	The capacity of a technological network infrastructure to change in size and power as required. قدرة البنية التحتية التكنولوجية على التغيير في الحجم والقوة حسب الحاجة.
SaaS (Software as a Service) البرمجيات كخدمة	A category of cloud services where multiple customers access the same software application via the internet فئة من الخدمات السحابية حيث يقوم العديد من العملاء بالوصول الى نفس تطبيق البرنامج عبر الانترنت.
Smart Applications التطبيقات الذكية	An application which adapts to be more efficient based on insights provided by data analysis. تطبيق يتكيف ليكون اكثر كفاءة استناداً الى الرؤى التي يوفرها تحليل البيانات.
XaaS ("X" as a Service, or Anything as a Service) "X" كخدمة، او أي شيء كخدمة	A general category of cloud services that does not fit other models, i.e. any function that is transformed into a cloud service فئة عامة من خدمات السحابة لا تناسب النماذج الأخرى، مع أي وظيفة يتم تحويلها الى خدمة سحابية.

4. Data Classification Guidelines for Private Organizations

4.1 CATEGORIES OF DATA CLASSIFICATION

Data classification is central to cybersecurity risk management.

The process of data classification involves an Organization determining (i) how sensitive the data is, and (ii) the likely impact to the Organization if the data is disclosed, altered, lost or compromised.

It is through classification that data can be managed in ways that reflect its actual sensitivity and value to the Organization, instead of treating all data in the same way. Practically, in the context of the move to cloud computing, data classification is a tool for your Organization to identify which data may be immediately suitable for migration to the cloud and which data may need to be subject to additional security controls, in order to mitigate risks identified, prior to being suitable for migration to the cloud.
Categories of data classification indicate the different levels of sensitivity of data and the impact on the Organization should that data be disclosed, altered, lost or compromised [1].

Data classification is a starting point for determining the appropriate level of controls which should be applied to data, taking into account the confidentiality, integrity, and availability requirements for that data.

- CONFIDENTIALITY: access to the data only by authorized persons within your Organization;
- INTEGRITY: correctness and authenticity of the data and absence of unauthorized alterations;
- AVAILABILITY: need for timely and easy access to the data when required by authorized persons.

4. إرشادات تصنيف البيانات للمنظمات الخاصة

4.1 فئات تصنيف البيانات

إن تصنيف البيانات هو امر أساسي لإدارة مخاطر الامن السيبراني.

تتضمن عملية تصنيف البيانات منظمة تحدد (1) مدى حساسية البيانات، و (2) التأثير المحتمل على المنظمة اذا تم الكشف عن المعلومات أو تغييرها أو فقدها أو تعرضها للخطر.

فمن خلال التصنيف يمكن إدارة البيانات بطرق تعكس حساسيتها الفعلية وقيمتها بالنسبة الى المنظمة، بدلاً من معالجة جميع البيانات بنفس الطريقة.
عملياً، في سياق الانتقال الى الحوسبة السحابية، يعد تصنيف البيانات أداة لمؤسستك لتحديد البيانات التي قد تكون مناسبة على الفور للترحيل الى السحابة وأي البيانات قد تحتاج الى ان تخضع لضوابط امان إضافية، سعياً الى الحد من المخاطر التي تم تحديدها، قبل ان تكون مناسبة للانتقال الى السحابة.
تشير فئات تصنيف البيانات الى المستويات المختلفة لحساسية البيانات وتأثيرها على المنظمة في حالة الكشف عن تلك البيانات أو تغييرها أو فقدها أو الاضرار بها.

تعد عملية تصنيف البيانات نقطة انطلاق لتحديد المستوى المناسب من الضوابط التي ينبغي تطبيقها على البيانات، مع الاخذ في الاعتبار متطلبات السرية والسلامة والتوافر لتلك البيانات.

- السرية: الوصول الى البيانات من قبل الأشخاص المصرح لهم داخل منظمتك فقط.
- النزاهة: صحة البيانات ومصداقيتها وعدم وجود أي تغيرات غير مصرح بها.
- التوافر: الحاجة الى الوصول السهل وفي الوقت المناسب الى البيانات عند طلب الأشخاص المصرح لهم.

[1] Government entities must refer to the National Information Assurance Policy as these Guidelines are address only private organizations.

The CRA would encourage that Organizations by any categorized all data they own, use, create or maintain into one of the following four data classification categories:

1. PUBLIC – information which is in the public domain; its disclosure, alteration, loss or compromise would cause no damage to the Organization;

2. INTERNAL – information not in the public domain but which unauthorized disclosure, alteration, loss or compromise would only have a minimal impact on the operational interests of the Organization;

3. RESTRICTED – information which unauthorized disclosure, alteration, loss or compromise would cause a serious adverse effect to the interests of the Organization; and

4. HIGHLY-SENSITIVE – information, which unauthorized disclosure, alteration, loss or compromise would cause a significant and severe adverse effect to the interests of the Organization.

ستقوم هيئة تنظيم الاتصالات بتشجيع جميع المنظمات بتصنيف جميع البيانات التي تمتلكها أو تستخدمها أو تنشئها أو تحتفظ بها الى احد فئات تصنيف البيانات الاربعة التالية:

1. المعلومات العامة – المعلومات الموجودة في المجال العام؛ إن إفشاءها أو تعديلها أو فقدها أو تعرضها للخطر لن يؤدي الى الاضرار با لمنظمة ؛

2. المعلومات الداخلية – المعلومات التي ليست في النطاق العام ولكن الكشف عنها الغير مصرح به أو تعديلها أو فقدها أو تعرضها للخطر لن يكون لها سوى تأثير ضئيل على الاهتمامات التنفيذية للمنظمة؛

3. المعلومات المقيدة – المعلومات التي قد يؤدي الكشف عنها الغير مصرح به أو تعديلها أو فقدها أو تعرضها للخطر الى اثار سلبية خطيرة على مصالح المنظمة؛ و

4. المعلومات شديدة الحساسية – المعلومات التي قد يؤدي الكشف عنها الغير مصرح به أو تعديلها أو فقدها أو تعرضها للخطر الى إحداث تأثير سلبي كبير وشديد على مصالح المنظمة.

Table 1 below sets out in detail the four categories of data with useful examples to assist you in determining into which category you should place a particular data for your Organization.

يوضح **الجدول 1 ادناه** بالتفصيل الفئات الأربع للبيانات مع أمثلة مفيدة لمساعدتك في تحديد الفئة التي يجب ان تضع فيها بيانات معينة لمنظمتك .

Table 1: Data Classification Requirements

الجدول 1: شروط تصنيف البيانات

	Public عامة	Internal داخلية	Restricted مقيدة	Highly-Sensitive شديدة الحساسية
Description **الوصف**	Information which is in the public domain/widely shared publicly. المعلومات العامة الموجودة في المجال العام \ مشتركة على نطاق واسع بشكل عام.	Information that may be seen by all employees of the Organization but would not normally be available to those outside of the Organization. المعلومات الداخلية التي يمكن ان يراها جميع موظفي المنظمة ولكنها لا تكون متاحة عادة لمن هم في خارج المنظمة.	Information that is accessible by a restricted number of employees of the Organization on a need to know basis to carry out their specific roles. المعلومات المقيدة التي يمكن الوصول اليها من قبل عدد محدود من موظفي المنظمة على أساس الحاجة لأداء ادوارهم المحددة.	Information that is only accessible by a restricted number of specifically designated employees. It is the most sensitive information for the Organization therefore requiring the highest level of protection. المعلومات شديدة الحساسية التي يمكن الوصول اليها من قبل عدد محدود ومخصص من موظفي المنظمة على أساس الحاجة. هذه المعلومات هي الاشد حساسية في المنظمة ويترتب عليها اعلى مستوى من الحماية.
Examples of Data **امثلة على البيانات**	• **Internet webpages;** • **Marketing material;** • **Press releases and announcements.** • **مواقع الانترنت** • **المواد التسويقية** • **البيانات الصحفية والاعلانات.**	• Internal correspondence via emails and otherwise; • Internal policies and procedures; • Routine operating documentation; • Certain agreements relating to service levels; • Intranet webpages • المراسلات الداخلية وعكس ذلك؛ • السياسات والعمليات الداخلية؛ • التوثيق العملي الروتيني؛ • اتفاقات معينة بما يتعلق بمستويات الخدمة؛ • صفحات الانترانت	• Documents containing special or sensitive categories of personal data, including spreadsheets or databases with personal data; • HR data; • Financial reports and information (other than publicly reported financial information); • Confidential commercial contracts. • الوثائق التي تحتوي على فئات خاصة أو حساسة من البيانات، ويتضمن ذلك على الجداول أو قاعدة بيانات التي تحتوي على بيانات خاصة؛ • بيانات الموارد البشرية؛ • التقارير والمعلومات المالية (عدا المعلومات والتقارير التي تم نشرها)؛ • العقود التجارية السرية.	• Trade secrets, such as formulas, ingredients, methods etc.; • Security information; • Medical records of employees; • Software codes of critical systems; • Legally privileged information • الاسرار التجارية مثل المعادلات والمكونات والأساليب وغيرها؛ • معلومات الامن؛ • السجلات الطبية للموظفين؛ • شيفرات برمجية للأنظمة المهمة؛ • معلومات قانونية ذات امتياز.

Business Impact if released or compromised **التأثير التجاري اذا تم نشر المعلومات أو تعرضها للخطر**	None. لا يوجد.	Minimal adverse impact.. الحد الأدنى من التأثير السلبي.	Serious adverse impact. تأثير سلبي خطير.	Exceptionally serious or severe adverse impact. تأثير ضار وخطير أو شديد بشكل سلبي.
Markings **العلامات**	PUBLIC or no marking. عام أو لا علامات.	INTERNAL داخلية	RESTRICTED مقيدة	HIGHLY-SENSITIVE شديدة الحساسية

Once data is classified into one of the four categories, you should attach to each category a specific and tailored set of security measures. The objective is for your Organization's data to be protected at an appropriate level.
When moving to the cloud, Cloud Service Providers shall implement measures, in accordance with internationally recognized standards [2], that guarantee an appropriate level of protection against security threats and which are in line with the security measures that your Organization has determined as being appropriate.

عند الانتهاء من عملية تصنيف البيانات الى احد الفئات الأربعة، يجب عليك ان ترفق بكل فئة مجموعة محددة ومخصصة من اجراءات الأمان. الهدف من ذلك هو حماية بيانات منظمتك على مستوى مناسب.

عند الانتقال الى السحابة، سوف يقوم مقدمي الخدمة السحابة بتنفيذ الإجراءات وفقاً للمعايير المعترف بها عالمياً[4]، التي تضمن مستويات مناسبة من الأمان ضد التهديدات الأمنية والتي تتماشى مع التدابير الأمنية التي حددتها منظمتك على انها مناسبة.

Examples of security measures applied by cloud service provider include:

- encryption;
- anonymization;
- certification of security controls;
- aggregation in pre-defined hubs;
- data governance standards; and
- classification frameworks.

تتضمن الإجراءات الأمنية التي يطبقها مزود الخدمة السحابية ما يلي:

- التشفير؛
- إخفاء الهوية؛
- شهادة الضوابط الأمنية؛
- التجميع في محاور محددة مسبقاً؛
- معايير حوكمة البيانات؛ و
- أطر التصنيف.

Descriptors

The categories of data classifications described above are the principal means of indicating the sensitivity of a particular data set and the requirements for its protection.

In addition, your Organization may decide to use "Descriptors".

Descriptors are additional markings that Organizations may apply to further describe in a simple and efficient way certain categories of information and to indicate the need for common sense precautions to deal with the data.

Please note that the CRA would recommend that descriptors be used in conjunction with a data classification and applied in the following format:

الواصفات

ان اوصاف فئات تصنيفات البيانات المذكورة أعلاه هي الوسيلة الرئيسية للإشارة الى حساسية مجموعة بيانات معينة ومتطلبات حمايتها.

بالإضافة الى ذلك، قد تقرر منظمتك استخدام "الواصفات".

الواصفات هي علامات إضافية قد تطبقها المنظمات لوصف اكثر بطريقة بسيطة وفعالة فئات معينة من المعلومات وللإشارة الى الحاجة الى احتياطات معقولة للتعامل مع البيانات.

يرجى ملاحظة ان هيئة تنظيم الاتصالات توصي باستخدام الواصفات جنباً الى جنب مع تصنيف البيانات وتطبيقها بالتنسيق التالي:

[2] Such as ISO/EC 27001, ISO/EC 17789, ISO/EC 38500 and ISO/EC 385050.
[4] مثال ISO/EC 27001, ISO/EC 17789, ISO/EC 38500 و ISO/EC 385050

HIGHLY SENSITIVE – [DESCRIPTOR]

The CRA would recommend that Organizations use the following list of core descriptors to ensure that a consistent approach is adopted across the entire Organization and, ultimately by all Organizations across all sectors of activities:

- TRADE SECRET: information, including trade secrets, engineering information, formulas, methods, processes, know-how, source codes, pending unpublished patent applications and business plans;
- PERSONAL: information relating to an identifiable individual, for example, medical records;
- FINANCIAL: information relating to the finances of an Organization; it includes budgets, pro forma reports, production worksheets and financial statements;
- LEGAL: information relating to a legal issue including brochures, product disclosure statements, information summaries or fact sheets, presentations given at conferences, in seminars, webinars and other training sessions, newsletters and blogs, websites including business websites and websites operated by law firms as well as legal advice.

حساس للغاية - [الواصفات]

توصي هيئة تنظيم الاتصالات المنظمات باستخدام القائمة التالية من الواصفات الأساسية لضمان اتباع نهج متسق عبر المنظمة بأكملها، وبالتالي عبر جميع قطاعات الأنشطة:

- الأسرار التجارية: المعلومات، بما في ذلك الأسرار التجارية والمعلومات الهندسية والصيغ والأساليب والعمليات والمعرفة والشيفرة البرمجية وبراءة اختراع البرامج المعلقة الغير منشورة وخطط الاعمال؛
- الشخصية: المعلومات المتعلقة بفرد يمكن التعرف عليه، على سبيل المثال السجلات الطبية؛
- المالية: المعلومات المتعلقة بالشؤون المالية للمنظمة، لا سيما الميزانيات والتقارير المبدئية وبيانات أوراق العمل الإنتاجية والمالية؛
- القانونية: المعلومات المتعلقة بمسألة قانونية بما في ذلك الكتيبات وبيانات الكشف عن المنتجات وملخصات المعلومات أو صحائف الوقائع والعروض التقديمية المقدمة في المؤتمرات وجلسات الندوات عبر الانترنت والنشرات الإخبارية والمدونات والمواقع الالكترونية والمواقع الإلكترونية التي تديرها مكاتب المحاماة بالإضافة الى المشورة القانونية.

4.2 Data Ownership, Data Custodianship And Data Management

To classify data, each organization should define [3] roles and functions internally to ensure that the individuals who are responsible for this classification are clearly identified and aware of their duties.
For the purpose of this section, it is useful to clarify some of the terms that are used in relation to the handling of data.

✓ **DATA OWNERS** are individuals, whether persons or legal entities, who generate and control content such as the data of an Organization. The data owner is the original creator of the data.

4.2 ملكية البيانات والوصاية على البيانات وإدارة البيانات

بالنسبة لتصنيف البيانات، يجب على كل منظمة تحديد [5] الأدوار والوظائف داخلياً لضمان تحديد الافراد المسؤولين عن هذا التصنيف بوضوح وإدراكهم لواجباتهم.

ولغرض هذا القسم، انه من المفيد توضيح بعض المصطلحات المستخدمة فيما يتعلق بمعالجة البيانات.

✓ **مالكو البيانات** هم افراد، سواء كانوا اشخاصاً أو كيانات قانونية، يقومون بإنشاء والتحكم في المحتويات مثل بيانات المنظمة. مالك البيانات هو المؤسس الأصلي للبيانات.

[2] Data owners, data processors and data controllers are defined in Law n. (13) of 2016 (the Data Protection and Privacy Law)

[5] تعريف مالك البيانات ومعالج البيانات ومراقب البيانات في القانون رقم (13) لسنة 2016 (قانون حماية وخصوصية البيانات)

✓ADMINISTRATORS are responsible for ensuring that the integrity of the data is maintained. Administrators are different from data owner or user and, in fact, many administrators provide management services without having access to the data, e.g. backup and restoration of the data, maintaining records of the assets, and choosing, acquiring, and operating the devices and storage that house the assets.

✓تقع مسؤولية المدراء في المحافظة على ضمان سلامة البيانات. يختلف المدراء عن مالكو أو مستخدمو البيانات، وفي الواقع يوفر العديد من المدراء خدمات التنظيم دون الوصول الى البيانات، على سبيل المثال النسخ الاحتياطي واستعادة البيانات والاحتفاظ بسجلات الأصول واختيار وانتقاء وتشغيل الأجهزة والتخزين الذي يضم الأصول.

✓USERS are individuals, whether persons or legal entities, who are granted access to the data.

✓المستخدمين هم الافراد سواء كانوا اشخاصاً أو كيانات قانونية، يتم منحهم حق الوصول الى البيانات.

Generally, when a file is created within the Organization, the CRA would recommend that the OWNER should assign a classification. In other words, it is the person who has generated the data who should, as a first step, be tasked with assigning a classification to this data.
As an additional step, and if appropriate for your Organization, the CRA would recommend that each Organization designate at least one individual who should:

بشكل عام، عند إنشاء ملف داخل المنظمة، توصي هيئة تنظيم الاتصالات بأن يقوم المالك بتعيين تصنيف. بمعنى اخر، يجب أن يُكلف الشخص الذي أنشاء البيانات، كخطوة أولى، بتعيين تصنيف لهذه البيانات.
كخطوة إضافية، واذا كان ذلك مناسباً لمنظمتك، توصي هيئة تنظيم الاتصالات ان تعين كل منظمة شخصاً واحداً على الأقل للقيام بما يلي:

1. review the classification assigned by the OWNER;
2. provide any guidance within his/her Organization with respect to data classification;
3. assign a classification to unclassified data.

1. مراجعة التصنيف المكلف من قبل المالك؛
2. تقديم الارشادات داخل المنظمة فيما يتعلق بتصنيف البيانات؛
3. تكليف تصنيف للبيانات الغير مصنفة.

The purpose of having one individual carry out the above tasks is to provide consistency throughout the Organization with respect to data classification.

ان الغرض من قيام فرد واحد بتنفيذ المهام المذكورة أعلاه هو توفير الاتساق في جميع انحاء المنظمة فيما يتعلق بتصنيف البيانات.

To assist that individual and to ensure consistency, the CRA strongly recommends that each OWNER, as well as the individual with oversight, document their rationale when assigning a classification to a particular data set.

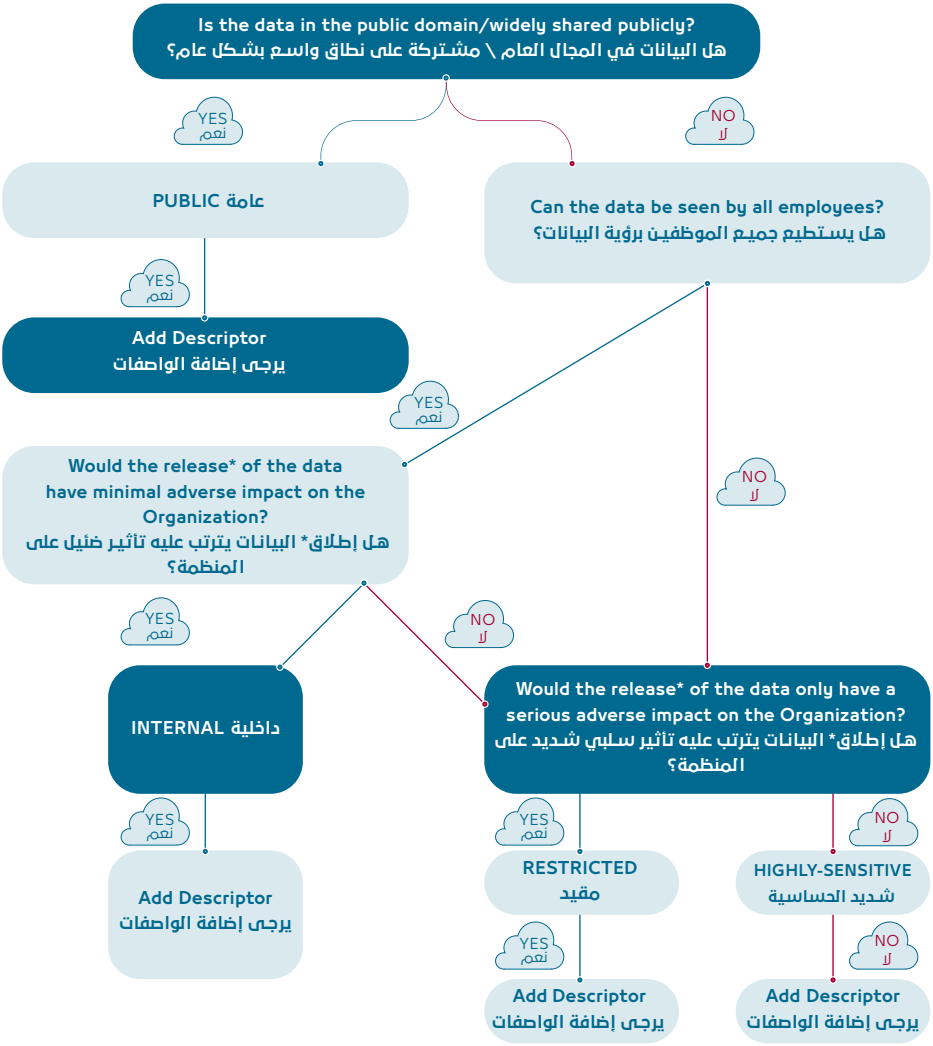
لتوفير وضمان الاتساق، توصي هيئة تنظيم الاتصالات بشدة ان يقوم كل مالك، وكذلك الفرد الذي يخضع للأشراف، بتوثيق الأساس المنطقي عند تعيين تصنيف لمجموعة بيانات معينة.

4.3 Classification Process And Flowchart

4.3 عملية تصنيف البيانات والمخطط الانسيابي

Once organizations have defined (I) categories of data classification (see section 2 above), **(ii)** the individual(s) responsible for actually classifying the data (see section 3 above), and **(iii)** the individual(s) with oversight of the data classification process (see section 3 above), the CRA suggests that the following flowchart be followed to help Organizations classify the data:

بمجرد أن تحدد المنظمات (1) فئات تصنيف البيانات (انظر للقسم رقم 2 أعلاه), (2) الفرد أو الافراد المسؤولين عن التصنيف الفعلي للبيانات (انظر للقسم رقم 3 أعلاه) و (3) الفرد أو الافراد الخاضعين للأشراف لعملية تصنيف البيانات (انظر للقسم رقم 3 أعلاه), تقترح هيئة تنظيم الاتصالات ان يتم اتباع المخطط الانسيابي التالي لمساعدة المنظمات في عملية تصنيف البيانات:



- Please note that for the purpose of this flow chart, we have used the term "*release*" to mean "*disclosure, alteration, loss or compromise*".

- "No" in this scenario would indicate that the release of the data would have more than a "*serious adverse impact*" on your Organization but rather an "*exceptionally serious or severe adverse impact*" on your Organization.

- يرجى الملاحظة انه لأغراض هذا المخطط الانسيابي، استخدمنا مصطلح "*إطلاق*" ليعني "*الكشف أو التغيير أو الخسارة أو التسوية*".

- تشير كلمة "لا" في هذا السيناريو الى ان اصدار البيانات سيكون له اكثر من "*تأثير سلبي خطير*" على منظمتك بل سيكون له "*تأثير سلبي خطير أو شديد بشكل استثنائي*" على منظمتك.

cra.gov.qa