Digital Transformation and Cloud-First Policies: Qatar as a Regional Example

With the evolving of digital transformation and cloud computing around the globe, governments have an important role to play in striking a balance between, on the one hand, developing the right policy and regulatory landscape for organizations to harness emerging technologies, and on the other hand, the protection of certain rights, such as privacy. Most States are heading toward adopting open-minded Digital Transformation and Cloud-First Policies that are different from the policies adopted few years ago. This article aims to show examples from local jurisdictions, with a focus on the recent policy initiative in Qatar.

Avec l'évolution de la transformation numérique et de l'informatique en nuage dans le monde, les gouvernements ont un rôle important à jouer pour trouver un équilibre entre, d'une part, le développement du bon paysage politique et réglementaire pour que les organisations exploitent les technologies émergentes, et d'autre part, la protection de certains droits, comme la vie privée. La plupart des États s'orientent vers l'adoption de politiques ouvertes de transformation numérique et de Cloud-First, différentes des politiques adoptées il y a quelques années. Cet article vise à montrer des exemples de juridictions locales, en mettant l'accent sur la récente initiative politique au Qatar.

Dr. Ehab Elsonbaty
Partner
DLA Piper

Yasemin Genc
Corporate, External and Legal Affairs (CELA) Director, Middle East Cluster (MEC)
Microsoft

The Increasing Need for Digital Capabilities and Technologies

Every industry is facing transformational change right now. More and faster than ever. Digital technologies, including mobile, cloud, artificial intelligence, sensors, and analytics, are accelerating progress exponentially.

More than a year into the start of the pandemic, one of most important lessons we have learned is that no business is immune to a crisis and no organization is 100% resilient. However, we have also seen that digital businesses and businesses strengthened with digital capabilities have been able to pivot more rapidly and respond to their customers' or citizens' needs.[1] Digital capabilities and technologies have helped those organizations address uncertainties brought about by COVID-19, which not only required flexibility in how organizations did business[2] and how governments served their citizens, but also triggered the need for:

> *"innovations for recovery in work, collaboration, distribution and service delivery at the heart of which lies artificial intelligence (AI), mobility (including autonomous vehicles), blockchain, drones and the internet of things (IoT) [which] are likely to play a dominant role in what emerges post-pandemic."*[3]

The expectations regarding the acceleration in the pace of technological change aligns with these lessons. The global cloud computing market size was USD 193.60 billion in 2019 and is projected to reach USD 684.55 billion by 2027, exhibiting a Compound Annual Growth Rate of 17.6 % during the forecast period, according to Fortune Business Insights.[4]

IDC predicts that by the end of 2021, based on lessons learned, 80% of enterprises will put a mechanism in place to shift to cloud-centric infrastructure and applications twice as fast as before the pandemic. By 2023, over 55% of enterprises will replace outdated operational models with cloud-centric models that facilitate rather than inhibit organizational collaboration, resulting in better business outcomes. Furthermore, to ensure effective continuity of operations, by 2024, 30% of government agencies will invest in intelligent and prescriptive intelligent digital workspaces supported by digital-led operating models.[5]

Studies show that the organizations which will come out ahead from the global challenges the world is facing will be those that develop a risk-based, business-focused, global regulatory strategy with the ability and flexibility to re-configure themselves based on data intelligence. As WEF Competitiveness Report 2020 Special Edition states,

> *"the pandemic crisis should serve as a wake-up call for countries that need to embrace the digitalization process, incentivize companies to move towards digital business models, and invest in ICT development and digital skills."*[6]

As the use of digital technologies increases, we should expect the efforts in creating the right regulatory environment to accelerate too. Chief Technology Officer of Atlassian, Sri Viswanath states:

> *"In the next five years, increased data and privacy regulation will have a big impact on the way we design Artificial Intelligence / Machine Learning models. As a result, investments in data management are going to be critical in determining the success of AI systems. Companies that have better data management frameworks, platforms and systems will win in building effective AI tools."*

International Standards and Regulations

How we use technology to solve the health, economic and sustainability issues of our day and how we can better serve the communities we are in is and will continue to be of paramount importance. As organizations and governments deal with these challenges, they increasingly rely on data for economic growth, competitiveness, job creation, new business models, better policies, more transparent governance, sustainability and societal impact as our ability to drive insights and intelligence with AI increases by day. For best results, data also needs to move, be governed, processed securely and in some cases be open.[7] This array of needs brings with it the question of how organizations can leverage big data being collected everyday over the internet[8] while protecting privacy, security, cyber-security,[9] considering also the complex IT environments they operate in.[10]

The IDC prediction that 65% of government agencies will protect the security and privacy of digital assets wherever they reside, using predictive analytics to identify, contain, measure, and address security risks by 2025 to ensure trust, also shows the interconnected

[1] According to the WEF Global Competitiveness Report, countries that could leverage flexible work arrangements (the top five are the Netherlands, New Zealand, Switzerland, Estonia, and the United States) and those where digital skills are most widespread (top five are Finland, Sweden, Estonia, Iceland, and the Netherlands) could partially adjust by increasing the digitalization of their economic activity. Despite important disparities between sectors that can be digitalized and those that cannot, economies able to rely on technology and the provision of digital services online were relatively less affected and were also able of using technology for monitoring the evolution of the infection.

[2] As an example, *"Some 89 per cent of UK business leaders reported the coronavirus pandemic has accelerated their move to the cloud, and without it, remote working and business agility would not have been possible."* as per 2020: The year business clouds gathered pace (raconteur.net).

[3] WEF_Global_Technology_Governance_2020.pdf (weforum.org)

[4] Cloud Computing Market Size & Share | Industry Growth [2020-2027] (fortunebusinessinsights.com). *See also* "Clouds trillion-dollar prize is up for grabs", Mckinsey Quarterly, February 26, 2021, on research identifying seven value drivers that could enable cloud to deliver more than USD 1 trillion in 2030 EBITDA value across the Fortune 500 by 2030. These seven drivers are cost optimization of application development and maintenance and IT infrastructure, improved business resilience, implementation of latest technological/digitization achievements in core operations via analytics, IoT, and automation use cases; growth from new and enhanced use cases, adopting accelerated product development, leveraging public- cloud hyper-scalability (innovation-driven growth and cost savings in business operations); adopting emerging technologies by gaining experience in experimentation at low cost. The estimate excludes the last value driver.

[5] A list of IDC predictions can be found here: https://www.idc.com/search/simple/perform_.do?query=predictions+2021&page=1&hitsPerPage=25&sortBy=RELEVANCY&lang=English&srchIn=ALLRESEARCH&src=&athrT=10&cmpT=10&pgT=10&trid=100029554&ptrid=68387256&siteContext=IDC.

[6] https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2020.pdf.

[7] Closing the data divide: the need for open data - Microsoft On the Issues, https://blogs.microsoft.com/on-the-issues/2020/04/21/open-data-campaign-divide/.

[8] 2.5 quintillion bytes of data produced by humans every day as per 2020 statistics: How Much Data Is Created Every Day in 2021? [You'll be shocked!] (techjury.net) . By 2025, it's estimated that 463 exabytes of data will be created each day globally – that's the equivalent of 212,765,975 DVDs per day: How much data is generated each day? | World Economic Forum (weforum.org) . Additionally, IDC predicts that by 2024, 70% of enterprises will have integrated their edge generated data with cloud-based enterprise systems to allow for real-time actioning based on IoT analytics, including AI/ML.

[9] *See* Microsoft's Digital Defense Report on changing cyber threats, including the activities of nation-state actors: Microsoft report shows increasing sophistication of cyber threats - Microsoft On the Issues and UN makes critical progress on cybersecurity - Microsoft On the Issues

[10] *See* Strategy for Data | Shaping Europe's digital future (europa.eu) aimed at providing businesses the confidence and means to digitize. For an analysis of innovative governance frameworks please also see:
WEF_Global_Technology_Governance_2020.pdf (weforum.org)

nature between regulatory and technologicial solutions in terms of security and privacy requiring private and public sector collaboration.

The industry has been pointing to a gap between laws and regulations and the need to protect security and privacy for a while. As new technologies have started becoming an integral part of our lives, the need for modernized laws and frameworks has become even more obvious.

We have seen a lot of movement towards closing this gap, which has resulted in several international, industry and regional standards and regulations emerging in order to level set and provide the tools for the assessment of security and privacy in a consistent way across the world, including:

- the General Data Protection Regulation (which has inspired many local privacy laws);
- CSA Star;
- SOC 1: SOC for Service Organizations: ICFR - Report on Controls at a Service Organization Relevant User Entities' Internal Control over Financial Reporting;
- SOC 2: SOC for Service Organization: Trust Services Criteria - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy;
- ISO/IEC 27001, ISO/IEC 27018 (an addendum to ISO/IEC 27001 and the first international code of practice for cloud privacy);
- ISO/IEC 27701 Privacy Information Management System (which outlines a comprehensive set of operational controls that can be mapped to various privacy regulations, including the GDPR); and
- ISO/IEC 19086-1:2016,[11] (which consists of a set of common cloud Service Level Agreement building blocks (concepts, terms, definitions, contexts) organizations can use to ensure their cloud contract includes all of the critical elements.

At the country level, governments have an important role to play in striking a balance between, on the one hand, creating the right policy and regulatory landscape for organizations to harness emerging technologies and, on the other hand, the protection of certain rights, such as privacy. According to the WEF Global Competitiveness Report 2020,[12] government regulatory and policy priorities should lead to the revival of economies. Governments need to create frameworks that advance the adoption of digital technologies and to implement environmental, social and governance standards, in addition to upgrading their own processes and services.[13] The UK Government's Cloud Guide for the Public Sector (updated on 8 Feb 2021)[14] states the importance of a balanced approach: *"Properly implemented cloud technology can improve speed of delivery, increase security and create opportunities for organizations to innovate."*

Governments that take a practical approach to enable new technologies rather than waiting for circumstances to mature will take a bigger risk but also will have and provide innovators and entrepreneurs in their countries the opportunity to lead in technological development. This approach will require a conversation between governments and industry, which has expressly been called out in the draft Cloud Policy Statement of Qatar[15] as well.

Every digital transformation requires a vision and strategy accompanied by culture, unique potential and capabilities. Setting the vision helps direct the resources and focus toward a single north star. To optimize their effectiveness, policies or regulations should also be considered as part of a bigger national vision, consistent with and incorporated into broader cybersecurity and ICT strategies. Governments willing to digitally transform themselves and their economies while preserving the market's ability to innovate and compete to deliver the best solutions leverage cloud first policies as an important tool.[16] Some examples of these are Australia, New Zealand, the Philippines, Singapore, the UK, the US and Qatar among many others.

Experience based on the existing cloud policies and their implementation show that there are some elements that are key to effective cloud policies.

I. Government Direction for Cloud-First Technologies and Procurement Policies

> *Cloud-first policy is simply a policy of moving all or most of a team's infrastructure to cloud-computing platforms such as AWS, Google Cloud, or Microsoft Azure. Instead of using physical resources like server clusters, they house resources—even mission-critical and secure resources—in the cloud.*

Cloud-first policy is simply a policy of moving all or most of a team's infrastructure to cloud-computing platforms such as AWS, Google Cloud, or Microsoft Azure. Instead of using physical resources like server clusters, they house resources—even mission-critical and secure resources—in the cloud. To teams used to co-located hardware, this might seem radical. However, the opposite is also true. Developers who adopt a cloud-first mentality find the idea of tying servers to a physical location unthinkable. Cloud-first teams don't think of their servers as discrete pieces of hardware or even virtual servers. Instead, they think of them as software to fulfill a business function. That the software eventually runs on some physical CPU is a secondary concern.[17]

The goal of cloud-first policies is usually stated as cost effectiveness, productivity and better services. Smart cloud policies not only save money but also create value by spurring innovation, boosting speed and agility, and increasing security, compliance, and standardization.

Qatar Cloud Policy Statement draft is a good example of this. The Statement departs from a very conservative Cloud Security Policy 2017[18] to a very progressive cloud-first policy.

[11] *See* full text and/or information here: EUR-Lex - 32016R0679 - EN - EUR-Lex (europa.eu); STAR | CSA (cloudsecurityalliance.org); ISO - ISO/IEC 27001 — Information security management; ISO - ISO/IEC 19086-1:2016 - Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1: Overview and concepts; SOC 1 - SOC for Service Organizations: ICFR (aicpa.org); SOC 2® - SOC for Service Organizations: Trust Services Criteria (aicpa.org).

[12] WEF_TheGlobalCompetitivenessReport2020.pdf (weforum.org).

[13] 58% increase in citizen likelihood to trust government institutions if they provide a great digital experience (Foresee – The Foresee Experience Index: E-Gov, Q1 2017).

[14] Cloud guide for the public sector - GOV.UK (www.gov.uk).

[15] Bilingual Draft Public Consultation Cloud Policy Statement.pdf.

[16] For suggestions for an effective regulatory framework see: National Cloud Computing Legislation Principles: Guidance for Public Sector Authorities Moving to the Cloud by Stephen Mutkoski :: SSRN.

[17] Cloud-First Strategy and Its Benefits for Business | Loggly.

[18] cs_cloud_security_policy-2017_english_v1.2.pdf (motc.gov.qa).

In addition, the cloud policies of various countries, such as the UK, Australia and Bahrain, provide a clear direction and prioritization of a public cloud to ensure the benefits are fully harnessed. For example, the UK Cloud First Policy provides that:

> *"When procuring new or existing services, public sector organizations should consider and fully evaluate potential cloud solutions first before considering any other option. This approach is mandatory for central government and strongly recommended to the wider public sector."*

And:

> *"Departments remain free to choose an alternative to the cloud but will need to demonstrate that it offers better value for money."*

The Australian government conducted research in order to understand how to improve their approach and policy and based on feedback from the agencies identified in its Secure Cloud Strategy the blockers in adopting cloud services and how to address them in order to realize the government's cloud aspirations.

II. Risk-Based Approach

The Australian Government's Secure Cloud Strategy astutely confronts the myths around cloud security:

> *"Cloud security fears are often overstated as specific to cloud where the risks to an environment apply equally, whether it is a provider cloud or an in-house implementation. Sound risk management practices to prevent and detect cyber security attacks can be as successfully implemented in cloud as they can in traditional data centres... Cloud services are not inherently more or less secure than any other device with an Internet connection."*

A risk-based approach enables organizations to manage risks for any system or technology, whether on cloud or on premise. Early steps in effectively managing risks include identifying, assessing, and prioritizing them, which help the organization to determine both how its risk profile may be improved by migrating to cloud services and what net new risks need to be managed.

Prioritized risks may be mitigated or transferred by operational or performance requirements through security certifications, audits, or service level agreements.

Cloud policies must also recognize that risk assessments and management decisions are best implemented as a continual process rather than framed as an end state as technology evolves and threat actors grow more sophisticated.

III. Transparency

The Qatar Cloud Policy Draft Statement emphasizes the importance of a clear and transparent framework in ensuring trusted access to such technologies for both national and international users, thus making Qatar a regional hub of cloud services innovation.

Cloud service providers must be transparent partners with government customers both by providing secure, private, and reliable offerings on how they handle data and by partnering with governments throughout this journey of compliance.

We have already touched on the need for collaboration between the public and private sectors for innovative solutions. Transparency is part of this equation, as it will enhance this collaboration and bring flexibility to the policy framework as the technologies and the threat environment change. Similarly, cloud service providers must be transparent partners with government customers both by providing secure, private, and reliable offerings on how they handle data and by partnering with governments throughout this journey of compliance.

IV. Standards-Based Approach

Existing global certifications and attestations provide most government entities with a reasonable set of security domain coverage for cloud services

Existing global certifications and attestations provide most government entities with a reasonable set of security domain coverage for cloud services. Leveraging global standards would help governments optimize for consistency, repeatability and reliability. And as stated in the WEF Global Technology Governance Report 2020, *"In the Fourth Industrial Revolution, old conceptions of regulatory siloes no longer apply."*[19] Therefore, new requirements should only be developed when governments require a security outcome not already covered under the existing certifications. This would entail an outcome-oriented approach rather than defining the method for it in order to permit cloud service providers to find the most innovative and practical solutions. Outcome-based approaches also ensure that ICT security policies are future-proof and that governments can access technology advancements as they develop.[20]

V. Data Governance

Data is the fuel for the new technologies powered by cloud. Data governance and the processes associated with it have become even more important to help large organizations and governments manage the integrity of their data.

A Data Classification Framework determines the data assets of the organization, identifies data levels based on their sensitivity and risk categories, and defines a data classification policy, including roles, responsibilities and permission rights for each category.

Data classification frameworks are usually addressed as an important part of data governance in cloud policies. A Data Classification Framework determines the data assets of the organization, identifies data levels based on their sensitivity and risk categories, and defines a data classification policy, including roles, responsibilities and

[19] WEF_Global_Technology_Governance_2020.pdf (weforum.org).

[20] REVoNc (microsoft.com).

permission rights for each category. This type of a risk-based approach and around 3 levels of data are considered good practices. In 2014, the UK government reduced its six levels of data classification to three: official, secret, and top secret. Cabinet Office Minister noted "There has been a tendency to over-mark documents rather than manage risk properly." After the reduction, 90% of UK government data was marked "official," meaning it could be stored in the public cloud. The remaining 10% required private or hybrid set-ups.

Australia and the United States have experienced similar results through their respective data classification schemes. As a further example, Singapore's SS 584:2015[21], the world's first Cloud Security Standard that covers multiple tiers, is based on three levels of information security for various types of cloud usage. Similar data classification schemes are also followed by leading academic institutions, such as Berkley University (with four levels of information security),[22] Carnegie Mellon University (with three levels)[23] or the University of Michigan (three levels).[24] These independent classification exercises have led to the conclusion that most government data are not sensitive, and it can suitably be hosted and managed in the cloud with the appropriate level of security measures.

VI. Qatar Draft Cloud Policy Statement

The new Cloud Policy Statement is based on Qatar's National Vision 2030 which aim to transform Qatar into an advanced country by 2030, capable of sustaining its own development and providing a high standard of living for its population and future generations. Qatar's vision and strategies combine technological and innovation goals with economic and sustainability targets recognizing the new international order that is knowledge-based and extremely competitive.

The CRA Strategy 2020-2024

The Qatar Communication Regulatory Authority's 2020-2024 strategy emphasizes the government's commitment to supporting the development of data centres and cloud infrastructure in Qatar to host its ambitious digitalization plan. Within the Authority's Strategy 2020-2024, the *"supply of data centres and cloud capacity"* has been identified as a target for the development of the IT sector.

Moreover, one of the key actions of the CRA Strategy 2020-2024 is:

> *"to develop a strategy on the supply of cloud services and data centres within Qatar. This strategy will be broad-ranging and will look at both supply and demand factors. It will evaluate current and future bottlenecks to the growth of data centers and cloud services, such as investment, innovation, security, regulation, terms of access and coordination with the Government".*

The objective of the Cloud Strategy is to increase the supply of data centre capacity and provide a better offering of cloud services to government and private sector entities.

Qatar has embraced the needs entailed by this transformation, including promotion of a high level of trust and customer confidence in the cloud service industry in Qatar through establishing a consistent and transparent legal framework that respects the ownership and control of data by users of cloud services, and promotes Qatar as a regional center for infrastructure and datacenter investment by multinational cloud service providers.

The Qatar Cloud Policy Statement, the draft decision of establishing an AI Committee, and the draft Cloud Handbook for SMEs are all a testament of Qatar's ambitions and determination to lead in this area.

The Qatar Cloud Policy Statement, the draft decision of establishing an AI Committee,[25] and the draft Cloud Handbook for SMEs are all a testament of Qatar's ambitions and determination to lead in this area.

The Qatar Cloud Policy statement draft not only focuses on the benefits of cloud to government, but to the whole economy. It has become a key pillar in the regulatory framework for the digital transformation of Qatar aimed at enabling and fostering investment into the country, the ecosystem and the people. The draft also relies on fundamental principles of trust, security and transparency.

The Qatar Cloud Policy Statement emphasizes the following:

1. Qatar will develop a common policy for public procurement of cloud services by government entities, consistent with the principles of the Cloud Policy.

2. Legislative solutions should not enforce data localization as a restriction to cloud adoption. Data residency is no longer a requirement, as security and encryption technologies now provide a sufficient level of security. As a result, the legislation should provide instead for an array of mechanisms to allow data to flow whilst ensuring that an adequate level of protection is in place.

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

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

5. The adoption of internationally recognized standards on interoperability of cloud services is required when contracting cloud services and in public procurement contracts. Interoperability of cloud services is a prerequisite to guarantee portability of services for cloud users.

6. There is a need to establish a regulatory regime with an appropriate level of regulation and limits in terms of liability regarding data stored and processed. The State will refrain from imposing intermediary liability on Cloud Service Providers for third party content in order to encourage user services innovation and promote the widespread availability of cloud services to public and private users. Cloud Service Providers should be able to limit or exclude their liability in compliance with the applicable law.

[21] https://www.singaporestandardseshop.sg/product/product.aspx?id=88be024c-cead-4a59-801d-9fcedbbab88f.

[22] https://security.berkeley.edu/data-classification-standard.

[23] http://www.cmu.edu/iso/governance/guidelines/data-classification.html.

[24] https://www.safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data/sensitive-data-classification.

[25] Cabinet Approves Draft Decision Setting up Artificial Intelligence Committee (hukoomi.gov.qa).

7. Cloud Service Providers must at all time have in place the technical and organizational measures necessary for managing security risks, to guarantee the continuity of their services. Compliance should be achieved by adopting internationally recognized security standard certifications. The creation of local standards or duplication of internationally recognized standards should be avoided because it can be detrimental to the development of a solid cloud industry.

8. Service Level Agreements (SLAs) must be in place to ensure agreed terms for services provision. Reliable cloud services need providers and consumers to agree on what service levels parameters (performance, availability, billing) the cloud product is offered. The adoption of standardized terms and conditions for cloud SLAs in line with international standards will help reinforce the public's trust in cloud services.

9. Prices of international connectivity are a critical element for investors' choice and must be aligned with international benchmarks. International connectivity must be assured along multiple different routes.

10. Cloud service Providers and government entities must commit to principles of environmental sustainability, including energy efficiency and carbon neutrality.

The adoption of the Cloud Policy Statement will be a progressive move, but will require many legislative, regulatory, and legal initiatives to update the relevant laws and regulations, such as the Cybersecurity Law, the Privacy Law, Cloud Security Policy, and international agreements, in addition to introduction of standard contractual clauses and binding corporate rules.

مع تطور التحول الرقمي والحوسبة السحابية في جميع أنحاء العالم، على الحكومات أن تلعب دورا مهما في تحقيق التوازن بين تطوير السياسات المناسبة والإطار التشريعي للشركات لتسخير التقنيات الناشئة من جهة ومن جهة أخرى حماية حقوق معينة مثل الخصوصية. تتجه معظم الدول نحو تبني سياسات منفتحة للتحول الرقمي وسياسات السحابة-أولا التي تختلف عن السياسات المعتمدة منذ بضع سنوات. تهدف هذه المقالة إلى عرض أمثلة من الولايات القضائية المحلية، مع التركيز على مبادرة سياسة وضعت مؤخرا في قطر.

BIOGRAPHY

DR. EHAB ELSONBATY is a Partner at DLA Piper in the firm's New York office. His practice focuses on corporate law in the Middle East.

Prior to joining DLA Piper, Dr. Ehab was at the Qatar Investment Authority (QIA), Qatar's sovereign wealth fund, where he served as senior legal counsel and head of corporate governance and government affairs and senior advisor to the general counsel on special projects from February 2014 to January 2021.

Dr. Ehab served for six years as senior legal advisor to the Amiri Diwan, the office of the Amir of Qatar at the Royal Court. During this time, he was also a member of many policy and legal committees, including the Permanent Legislative Committee and the Committee for Review of Legislation of the Council of Ministers, as well as a member of the National Committee to Review Commercial Laws of the Ministry of Economy and Trade. Ehab drafted and contributed to several laws and regulations of Qatar, GCC and Middle East.

YASEMIN GENC has been leading the commercial legal and policy work for Microsoft at various roles in the region for more than 13 years. Prior to joining Microsoft, she practised as a lawyer in several law firms including her own. Her focus areas are technology transfer, privacy, contracts, corporate law and mediation. Yasemin has a Bachelor of Law from Istanbul University and LL.M from the London School of Economics.

AI Regulation – Cloud-First Policy – Qatar
Réglementation de l'IA – Politique Cloud-First – Qatar