

THE GLOBAL DIWAN'S

# Newsletter

CONNECTING  
EAST-WEST  
LEADERS



EDITORIAL

**Last 8 & 9 September, the Nice Forum hosted 180 attendees representing more than 15 nationalities that convened for two days in an atmosphere both welcoming and conducive to exchanges.**

A thrilling success leading us to a second edition at the Mediterranean University Center in Nice on 12 & 13 October 2023. Our work, with high level guests and panels, will focus on the critical subject for the 21st century of data security governance.

One may read in today's newsletter extracts from the inaugural speeches of Prince Albert II of Monaco and Princess Hala Al Saud on the issues of Blue Security.

A first contribution of Shathil Nawaf Taqa of the Global Diwan team on the subject of data security governance, a topic to be addressed in the next issues until October 2023.

In an interview, Jus Mundi reminds us of the relevance of arbitration and mediation in an environment of different legal practices. The core principles of the rule of law are

essential to secure transactions and increase exchanges between the MENA region and Europe as Guillaume Deroubaix rightly reminds us in his article. We are excited he is taking the lead alongside Advisory Board member Matthias Fekl of yet another dimension of our club : the Global Diwan Legal.

The Global Diwan does not forget one of its foundational pillars, that is to support young leaders and women to find their way between the East and the West. We are proud to introduce you to the 4 laureates of our Startup Pitch Contest of September 8 in Nice.

Our events will continue during the following weeks with Oman, Kuwait, the United Arab Emirates, Algeria and Turkey. All countries where we have projects for the Global Diwan, a platform more necessary than ever as a place for dialogue in a world in turmoil.

**Éric Schell**

Executive Chairman of the Global Diwan

From left to right / HE Maurice Gourdault-Montagne, Christian Estrosi, HRH Princess Hala Khaled Al Saud, HH Sheikhha Intisar Al Sabah, HSH Prince Albert II of Monaco

**The Global Diwan 1st Annual Forum in Nice** 2

**Executive Roundtable** 6  
with RCU's CEO Amr AlMadani

**Startup Pitch Contest Laureates** 7

**The Rule of Law in the MENA Region** 8  
Guillaume Deroubaix

**Interview with Jus mundi's CEO** 9

**Data Security and Governance** 10  
Shathil Nawaf Taqa

## THE GLOBAL DIWAN NICE FORUM

# A thrilling success for the Global Diwan 1<sup>st</sup> Annual Forum in Nice

ON 9 SEPTEMBER 2022, 180 ATTENDEES COMING FROM MAGHREB, MIDDLE EAST, GULF COUNTRIES, EGYPT AND TURKEY, WITH SOME INDIAN, JAPANESE AND AFRICAN GUESTS CONVENED IN NICE FOR THE GLOBAL DIWAN ANNUAL FORUM ON BLUE AND GREEN SECURITY.

THE FIRST EDITION OF THIS YEARLY MEETING HAS SEEN THE HOLDING OF SUBSTANTIVE THEMATIC PANELS ON FOOD AND WATER SECURITY, TOURISM, ENERGY AND INFRASTRUCTURES, WITH DISTINGUISHED SPEAKERS COMING FROM THE MENA REGION AND EUROPE.

↓ VIP Dinner in the old city of Nice the night before the Forum



↓ HH Sheikhha Intisar Al Sabah is knighted by M<sup>r</sup> Estrosi, Mayor of Nice



↑ Lunch break on the sea front



↑ In the audience



## THE GLOBAL DIWAN NICE FORUM

Networking never stops in the corridors



The closing of the event, a garden party at the Villa Massena



HE Maurice Gourdault-Montagne's speech

## THE GLOBAL DIWAN NICE FORUM

# H.S.H. Prince Albert II of Monaco

IS THE PRESIDENT OF THE EPONYMOUS FOUNDATION ESPECIALLY ENGAGED IN THE PROTECTION OF OCEAN'S BIODIVERSITY.



“

Today we are all neighbours. Recognising this proximity, understanding the responsibility it implies, accepting being united by issues that concern our planet as a whole, and therefore humanity as a whole: this is the key challenge we are faced with today. Particularly with regard to all matters related to our seas.

“

The Mediterranean represents the link between us, far more than the division between us. This requires new collaboration on our part, because the actions needed are essentially unprecedented.

“

As with the fight against pollution, there is one requirement which I would like to touch on before I finish: to build on the work carried out by scientists to the broadest extent possible. First and foremost we need to support marine research and disseminate the results to political decision-makers, economic players and public opinion. These Mediterranean examples can easily be replicated in other maritime areas.

“

No solution will suffice, if it is limited to a country, a region, or a shore. And no action will be effective, if it does not involve all the maritime players: political leaders of course, but also businesses, consumers, NGOs, beyond even the areas directly concerned...



## THE GLOBAL DIWAN NICE FORUM



## H.R.H. Princess Hala Khaled Al Saud

IS THE BOARD DIRECTOR OF THE KHALED BIN SULTAN LIVING OCEANS FOUNDATION, A NON-PROFIT ENVIRONMENTAL SCIENCE ORGANISATION AND OCEAN RESEARCH FOUNDATION ESTABLISHED TO HELP PRESERVE, PROTECT AND RESTORE THE WORLD'S OCEANS AND AQUATIC RESOURCES THROUGH RESEARCH, EDUCATION, AND OUTREACH.

**At the invitation of H.H. Sheikha Intisar Al Sabah, H.R.H. Hala Khaled Al Saud has enthusiastically accepted to become a member of our Advisory Board.**

The spirit of dialogue and friendship between peoples at the core of the Global Diwan endeavor, as well as its efforts towards promoting women and young entrepreneurs resonates with her own convictions.

“

One scientist estimates that one out of every six person on earth depends upon these ecosystems for food or income. Every person on this planet benefits from their existence, including our future generations. The loss of these ecosystems and the benefits they provide would have a profound impact on the lives and livelihood of billions of people around the world.

“

The loss of healthy oceans is not just an environmental issue, it is rather a security and humanitarian issue as well. If these ecosystems disappear, the communities that rely upon them disappear too.

“

We are using our research and expertise to build resiliency models, so we can focus our limited time and resources on conserving the places most likely to survive in a rapidly changing world.

“

How can we, as a global community, turn slogans into actionable steps?

With our experience conducting field research and designing education and community outreach programmes, we combine our passion with deep knowledge to save our oceans. Our ocean conservation efforts defy borders and defy individual institutions and affect people's quality of life.

“

As my father [H.R.H. Khaled Bin Sultan Al Saud] wisely stated many years ago: « We do not hope to stop human development, only to ensure it is sustainable to future generations to benefit from healthy oceans ».



# Executive Roundtable with the Royal Commission for Al Ula's CEO Amr AlMadani



FOLLOWING THE SUCCESS OF OUR FIRST EXECUTIVE ROUNDTABLE WITH NEOM'S CEO NADHMI AL NASR IN JUNE, WE WERE VERY PROUD TO WELCOME FOR THIS SECOND EDITION AMR AL MADANI, CEO OF THE ROYAL COMMISSION FOR ALULA.

On October 17, Mr Al Madani [in](#) was in Paris to share his vision and discuss with Laurent Germain [in](#), CEO of Egis, partner of the Global Diwan, and Valérie Levkov [in](#), Senior Vice-President Africa and Middle East of EDF. Amid rich exchanges with our guests, Amr Al Madani underlined the formidable business opportunities represented by a project of this magnitude. The skills required are numerous and the ambitions are high as tourism itself is to be redefined in a more sustainable

and qualitative way as much as it needs to be inclusive of local communities.

This encounter was organised thanks to the strong support of HE Fahad Al Ruwaily, Ambassador of the Kingdom of Saudi Arabia to France, as part of a cycle of event: The Saudi-French Cooperation & Vision 2030 : Strengthening the Economic Relations ; where Saudi large-scale projects are presented in front of business leaders from the CAC 40 and French SMEs.

# Startup Pitch Contest Laureates



ON 8 SEPTEMBER 2022, THE GLOBAL DIWAN, WITH THE SUPPORT OF THE MUNICIPALITY OF NICE, HOSTED ITS FIRST STARTUP PITCH CONTEST THE DAY BEFORE THE BLUE AND GREEN SECURITY FORUM.

More than 50 participants coming from North Africa, the Middle East, the Gulf countries and Turkey, with Indian, African and Japanese guests gathered at the Mediterranean University Center in Nice.

On the topics of foodtech, cleantech and women and young entrepreneurs, with competing entrepreneurs from France, Algeria and Morocco and the support of our sponsors (Municipality of Nice, Metropole of Nice, Egis, Saur, Jolt Capital, JCDecaux, Xerys Invest, Azur Drones and ODDO BHF).

Chaired by Hervé Novelli, Advisory Board member and former Minister, the jury was comprised of Advisory

Board co-Chairs Maurice Gourdault-Montagne [in](#), Ambassador of France ; H.H. Sheikha Intisar Al Sabah [in](#), philanthropist and business woman, Eric Schell [in](#), Executive Chairman of the Global Diwan, Christian Nakhle [in](#), former Ambassador of France to Kuwait ; Camille Angué [in](#), Deputy Managing Director of Services of the Metropole de Nice, Olivier Ossipoff [in](#), Chairman of Xerys Invest, Philippe Perez [in](#), Head of marketing of Jolt Capital, Clément Maclou [in](#), Senior Portfolio Manager at Oddo BHF, Anne Le More [in](#), United Nations Food Systems Champion and Salem Massalha [in](#), co-Founder of Very Nile.

## THE JURY UNANIMOUSLY SELECTED 4 LAUREATES :



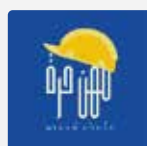
**Inalve** : manufacturing and selling of seaweed for the food industry

[www.inalve.com](http://www.inalve.com)



**Livmed's** : fast medicine delivery

[www.livmeds.com](http://www.livmeds.com)



**Mehanhoura** - قرح ندم : a platform to find the right craftsperson

[www.mehanhoura.com](http://www.mehanhoura.com)



**Oghji** : manufacturing smart electrical panels that save energy

[www.oghji.com](http://www.oghji.com)



# The Rule of Law in the MENA Region

Guillaume Deroubaix 

DEFINED IN THE 19<sup>th</sup> CENTURY, THE CONCEPT OF RULE OF LAW HAS EXPERIENCED UNPRECEDENTED GROWTH FOR SEVERAL YEARS. AS A KEY ELEMENT IN BUILDING A BUSINESS-FRIENDLY CLIMATE, THE RULE OF LAW HAS BECOME A PRIORITY FOR SEVERAL GOVERNMENTS IN THE MENA REGION.

## How to define the Rule of Law?

No international treaty defines the Rule of Law, and in fact, there are many definitions of the concept. However, the largest international institutions (the UN, the World Bank, NGOs) agree on common pillars.

- Equality: Laws must be universal and apply to all.
- Foresight: Laws should not be retroactive.
- Publicity and clarity: Laws must be made public, clear and relatively stable.
- Accessibility: Access to the legal system should be as simple as possible.
- Independence: The independence of the judiciary must be guaranteed. Corruption must be punished.
- Procedures: Essential principles must be applied, such as the right to a fair trial, the impartiality of judges.

The NGO World Justice Project establishes each year a ranking that measures the level of Rule of Law of 140 countries, around the following 4 factors:

### Accountability

“The government as well as private actors are accountable under the law.”

### Just Law

“The law is clear, publicised, and stable and is applied evenly. It ensures human rights as well as property, contract, and procedural rights.”

### Open Government

“The processes by which the law is adopted, administered, adjudicated, and enforced are accessible, fair, and efficient.”

### Accessible and Impartial Justice

“Justice is delivered timely by competent, ethical, and independent representatives and neutrals who are accessible, have adequate resources, and reflect the makeup of the communities they serve.”

### Why is it an element of attractiveness?

Many criteria are analysed by local or foreign economic operators when it comes to investing. They will look, among other things, at the political situation of the State, the quality of infrastructure, the health situation, the level of education...

They will also look at the level of sophistication of the country's legal and judiciary situation, and the extent to which the rule of law is respected. Indeed, every investor seeks security and legal stability.

## The Rule of Law in the MENA Region

In the reference ranking, the Rule of Law index published by the World Justice Project (WJP), 8 factors are analysed for each country, compared to the 4 pillars seen above.

1. Constraints on Government Powers
2. Absence of Corruption
3. Open Government
4. Fundamental Rights
5. Order and Security
6. Regulatory Enforcement
7. Civil Justice
8. Criminal Justice

In 2022, Denmark is the most recognised country in the world as having the highest level of Rule of Law (in total, 140 countries join this ranking).

As for the MENA Region, 8 countries in the MENA Region are ranked. In first place is the United Arab Emirates (37th in the world ranking). The following 7 countries are: Jordan, Tunisia, Algeria, Morocco, Lebanon, Iran and Egypt.

## The Rule of Law and the Global Diwan

Of course, the promotion of the Rule of Law is part of the objectives of the Global Diwan in general and the Global Diwan Legal in particular. Because we consider that the law is a factor of stabilisation of economies, a progress for everyone and a factor of peace, we will work at our level, for its promotion and primacy.





## INTERVIEW



**Sponsor of the Global Diwan, Jus Mundi is a very promising legal tech company specialised in international arbitration. Its CEO, Jean-Remi de Maistre, presents the company he created and its strategy in the MENA Region.**

### Can you introduce us to Jus Mundi?

Our mission is to power World justice by facilitating access to global legal resources using artificial intelligence and machine learning.

By combining law & technology, Jus Mundi enhances lawyers' decision-making by giving them access to critical legal information and analytics on arbitrators, lawyers, and law firms. As a mission-led company, all legal document on Jus Mundi is freely available to everyone.

### What are the needs to which Jus Mundi particularly responds?

We make international lawyers' and global in-house counsels' work easier and more efficient. On average, lawyers spend 30% of their time on legal research. That is not accounting for complex cross-border cases which require legal information usually scattered around the world, if accessible at all. Not to speak of the cost of such lengthy research, which many times do not yield any accurate results. Yet, information is power and often determines the outcome of a case. Similarly, finding specialised professionals meeting specific criteria and who are not conflicted can be a headache for lawyers. We made access to legal information and legal practitioners easy.

Jus Mundi has built the only platform that provides a single source of comprehensive and reliable data for international law and arbitration. We cover international trade law and public international law and offer the world's largest database for investment and commercial arbitration on a single platform. Thanks to our AI-powered technology, Jus Mundi also provides lawyers with data-driven due diligence tools for arbitration, analytics, and alerts.

To address the lack of readily available and data-based information on practitioners, we also created Jus Connect, the professional

network tailored-made for the arbitration industry. Jus Connect allows lawyers and in-house counsel to access analytics, caseload data, and factual & validated information on counsel, arbitrators, and experts. Our Conflict Checker also enables them to monitor potential conflicts of interest in just a few clicks.

At Jus Mundi, we dare to prove every day that finding legal information around the globe can be easy, fast, and accurate!

### Here's what makes Jus Mundi so unique:

- A multilingual search with over 20 filters: Quickly narrow your research in multiple languages.
- Exclusive institutional partnerships: Thanks to our partnerships with the \*\*IBA, ICC, HKIAC, AAA-ICDR\*\*, and many other major arbitral associations & institutions around the globe. The inaccessible awards are now accessible. And a new one will be announced during Dubai Arbitration Week. Stay tuned!
- Secondary sources you can trust:
  - > Wiki Notes: 250+ key legal concepts in investment law and arbitration to guide you through the latest and most relevant case law;
  - > The renowned \*\*ICC Dispute Resolution Library, which contains over 400 books, 2,500 documents, including 85 ICC-exclusive Enforcement Guides.\*\*
  - > and more.
- Conflict Checker: Arbitration due diligence made easy! Track past relationships for arbitrators, tribunal secretaries, lawyers, law firms, and States to avoid potential conflicts of interest.
- Jus Connect: Gain visibility with your target audience. Find lawyers, arbitrators, States,

law firms, and experts in a few clicks, thanks to filters and data-backed analytics.

### What strategy are you pursuing in the MENA region in particular?

Part of Jus Mundi's work in MENA as a region is to support arbitration institutions in their work to make arbitration more understood and more widely used in the region.

Arbitration and alternative dispute resolution have a steady and well-founded base in the institutions of MENA, but we believe more can be done in the region.

Our collaboration with institutions in the name of the public good, making non-confidential arbitration materials freely available to the public, is a significant step towards greater global understanding and use of arbitration.

We also look forward to working with local law firms, governments, & universities.

### What are your next key dates?

We are attending Dubai Arbitration Week soon (Nov. 14-18).

We will be hosting an event on Nov. 15 at 5 pm at the Ritz-Carlton DIFC where renowned speakers will share their practical tips to enforce a final award in construction arbitration & recover money in the post-pandemic era. Register here.

We will also be present at the Sharm El Sheikh Conference Series in Cairo, Egypt in December.



# Data security and governance

Shathil Nawaf Taqa 

## Understanding the new challenges

Today, data is possibly one of the most important assets a business owns. The 21<sup>st</sup> century is characterised by a data economy where companies find enormous value in collecting, sharing and using data about customers or users. The combination of all the processes and tools related to utilising and managing large data sets has made the concept of Big Data an essential element for governments and businesses. This concept was born out of the need to understand preferences, trends and patterns in the huge database generated when people interact with different systems and each

“

Today, data is possibly one of the most important assets a business owns.

The 21<sup>st</sup> century is characterised by a data economy where companies find enormous value in collecting, sharing and using data about customers or users.

other. With Big Data, operators can use analytics, and figure out the most valuable customers. It also helps businesses to create new experiences, services, and products. In the 2010s, personal data belonging to millions of Facebook users was collected without their consent by British consulting firm Cambridge Analytica, predominantly to be used for political advertising. The illegal and dishonest use of this data has opened a great debate in the world on the way in which companies but also States use this mass of data that new technologies have used.

Transparency and compliance with the data related legislation are today vital to building trust with customers who naturally expect privacy as a human right. Businesses are rigorous in their way to request consent to keep personal data, abide by their privacy policies, and manage the data that they've collected. Today, if customers can't rely on that privacy, they're unlikely to trust the business.

No one is safe from cybercrimes, Facebook, itself, was victim of a data leak where personal data of over 533 million Facebook users was posted in a low-level hacking forum. A user in a low-level hacking forum published the phone numbers and personal data of hundreds of millions of Facebook users for free. The exposed data included the personal information of users from 106 countries, including over 32 million records

“

The reflection around data governance as well as data security is intimately linked to a legal framework that has become a reference: the European Union one.

on users in the US, 11 million on users in the UK, and 6 million on users in India. It included phone numbers, Facebook IDs, full names, locations, birthdates, bios, and, in some cases, email addresses.

The European Union is today one of the international actors with the most innovative and protective legal activity in the field of data. The European legislator seeks to strike a balance between freedom of enterprise and consumer protection. The current EU legal framework was put forward through the EU Data Protection Reform in January 2012 to make Europe fit for the digital age. More than 90% of Europeans say they want the same data protection rights across the EU – and regardless of where their data is processed.

The reflection around data governance as well as data security is intimately linked to a legal framework that has become a reference: the European Union one. Today, companies and governments start from this repository to understand the major challenges of data.



## 1. The European legal framework as a reference

On 8 April 2016 the Council adopted the regulation and the directive. On 14 April 2016 they were adopted by the European Parliament. On 4 May 2016, the official texts were published in the EU Official Journal in all the official languages. The regulation came into force on 24 May 2016 and will apply from 25 May 2018. The directive entered into force on 5 May 2016 and EU countries have to transpose it into their national law by 6 May 2018. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data also called GDPR – General Data Protection Regulation. Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data.

The regulation was seen as an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the digital single market. A single law will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. If you process the personal data of EU citizens or residents, or you offer goods or services to such people, then the GDPR applies to you even if you're not in the EU. And the fines for violating the GDPR are very high. There are two tiers of penalties, which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages. The GDPR defines an array of legal terms at length. If you process data, you have to do so according to seven protection and accountability principles outlined in Article 5.1-2 of the GDPR:

- Lawfulness, fairness and transparency — Processing must be lawful, fair, and transparent to the data subject.
- Purpose limitation — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
- Data minimisation — You should collect and process only as much data as absolutely necessary for the purposes specified.
- Accuracy — You must keep personal data accurate and up to date.
- Storage limitation — You may only store

“

All Arab and other oriental countries are adopting new data protection laws (...) Qatar and the United Arab Emirates are at the forefront of this high ambition.

personally identifying data for as long as necessary for the specified purpose.

- Integrity and confidentiality — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
- Accountability — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Several challenges are posed today within the framework of European law, including the transfer of data from the Union abroad, such as in the United States for example, where several companies are based on American soil. The possibility of lawful transfer of personal data from the EU to the US, while ensuring a strong set of data protection requirements and safeguards, has been discussed in front of the European courts.

On April 2022, the European Commission and the United States announced that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in the Schrems II decision of July 2020.

Details have not been released of the Agreement but the White House Fact Sheet explains that the new Framework will address the concerns about intelligence activities raised in the Schrems II decision, among other things. Indeed, the Fact Sheet explains that the U.S. has committed to: The agreement aims to provide a durable basis for trans-Atlantic data flows, which are critical to protecting citizens' rights and enabling trans-Atlantic commerce in all sectors of the economy.

## 2. Data security in the Middle East

Countries in the Middle East have bold plans for economic growth, new technologies, innovation and urban development in the next ten to twenty years. All Arab and other oriental countries are adopting new data protection laws, maturing existing rules or expanding the scope of technology regulation.

Qatar and United Arab Emirates (UAE) is at the forefront of this high ambition. Bahrain and Oman are also resource-rich and intend to diversify to meet a changing world. Saudi Arabia is a giant player today with confident plans for urbanisation and diversification of its economy. These policy shifts seek to protect individual rights, build trust in new technologies and increase international and regional data flows. Data protection is trending in the Middle East, because the region is investing heavily in data, technology, automation, smart cities and scientific innovation.

Turkey is a notable regional neighbour; most fully aligned to international data protection and EU standards. Turkey serves as a reference point for the wider region. The overall regional picture is not uniform. There are different approaches, differing levels of data protection maturity, variable enforcement, many timelines and a range of expectations.



### a. Turkey

The main piece of legislation covering data protection in Turkey is the Law on the Protection of Personal Data No. 6698 dated April 7, 2016 (LPPD). The LPPD is primarily based on EU Directive 95/46/EC. To date, the legislature has enacted several regulations to implement various aspects of the LPPD.



### b. United Arab Emirates

In November 2021, the United Arab Emirates issued Federal Law No. 45 of 2021 (the UAE Data Protection Law), which set stricter standards for data privacy and protection and further increased awareness around the importance of data protection compliance. We have put together this data privacy handbook to try to simplify the requirements and help you kick-start your data privacy compliance journey.

DIFC Law No. 5 of 2020

The DIFC Data Protection Law (DIFC

Law No. 5 of 2020) has been effective since 1 July 2020 and enforceable as of 1 October 2020. The law is applicable to all DIFC registered entities.

Influenced by the EU General Data Protection Regulation, the DIFC law combines the best practices from a variety of world class data protection laws.

The law aims to safeguard the personal data of individuals whose data is processed by organisations registered in the DIFC. Non-compliance with the law may result in fines.



#### c. Saudi Arabia

The KSA Personal Data Protection Law was issued on 16 September 2021 with the aim of protecting and providing guidelines of processing personal data within the Kingdom of Saudi Arabia (KSA). The Law applies to all organisations which operate or do business within KSA.

This law is officially enforceable 180 days after its announcement – 23rd March 2022. However, there is a grace period of one year that data controllers can use to modify their arrangements to ensure compliance.

The PDPL will be supplemented by executive regulations that should provide additional clarity on many provisions. The draft version of executive regulations open for public discussion was published on 10th March 2022. If an organisation fails to protect personal data and comply with the Law within one year, the fines can reach up to SAR 5,000,000 (EUR 1,300,000) and prison sentences up to 2 years.



#### d. Egypt

Egypt published a Personal Data Protection Law in July 2020 that addresses the right to personal data protection and gives multiple rights to individuals.

According to the Law, personal data should only be collected for specific legitimate purposes and should not be retained longer than necessary.

Organisations may need to acquire a license to process both personal and sensitive personal data. Additionally, organisations involved in the processing of personal information are expected to appoint an authorised Data Protection Officer (DPO) who will be responsible for the application of this law within the organisation.

The Personal Data Protection Law has provisions for administrative fines and criminal penalties for non-compliance which

could be up to a maximum of EGP 5m or a potential sentence of imprisonment of more than six months.



#### e. Qatar

Qatar implemented Law No. (13) of 2016 (“the Personal Data Privacy Protection Law”) to protect the privacy of individuals’ personal data. With this, Qatar became the first Gulf Cooperation Council (GCC) member state to issue a personal data protection law. The Ministry of Transport and Communications has been tasked to enforce the law.

Any organisation involved in the processing of personal data should adhere to the principles of transparency, fairness and respect for human dignity. Additionally, adequate technical and organisational measures should be put in place to ensure a safe custody of the personal data.

The PDPL prescribes financial penalties for non-compliance or legislative breaches which could be up to a maximum of QAR 5,000,000 (EUR 1,300,000).



#### f. Bahrain

On 1 August 2019, Bahrain Law No. 30 of 2018 promulgating the Personal Data Protection Law (PDPL) came into force in the Kingdom. Modelled on European Union data protection laws, the PDPL is the second national law in the Gulf region to directly address the right to personal data protection and will impose obligations on businesses that collect personal data in relation to how organisations use and secure it.

Penalties go further than the GDPR by including provisions for prison sentences of up to 1 year.

The law includes additional requirements for organisations to submit their data processing registers monthly to the Authority and has shorter timelines for compliance with individuals’ rights.



#### g. Oman

In February 2022 the Sultanate of Oman issued the Personal Data Protection Law, which set stricter standards for data privacy and protection and further increased awareness of the importance of data protection compliance.

The law comes into force on 13 February

2023 – and it is highly important for organisations to fully prepare themselves for compliance with the new legal requirements by this date.



#### h. Kuwait

Kuwait does not have a specific personal data protection law. However recently the Communications and Telecommunications Regulatory Authority (CITRA) issued Decision No. 42 of 2021 on Data Privacy Protection Regulation (“Regulation”) imposing obligations in relation to data protection on Telecommunication Services Providers and related industry sectors.

The Regulation sets out detailed guidelines for the collection, storage, process and transfer of data by private sector and public sector service providers. The most interesting part of the Regulation is the wider ambit of the definition of ‘Service Provider’, which ranges from traditional telecommunications service providers to anyone who operates a website, smart application or cloud computing service, collects or processes personal data or directs another party to do so on its behalf through information centres owned or used by them directly or indirectly.

Exclusions to the obligations under the Regulation are for the collection and processing of private personal or family data by an individual; or for security agencies for the purposes of controlling crimes and implementing state security measures.

This is in addition to the obligations under Law No. 20 of 2014 (the E-Commerce Law) which requires that client data relating to positional affairs, personal status, health status, certain financial information and other personal information must be retained privately and confidentially by the recipient and its employees. Such data may not be disclosed without client consent or a court order.



#### i. Lebanon

Under Law No. 81 of 10 October 2018 on Electronic Transaction and Personal Data, data controllers who operate within Lebanon are responsible for upholding the following data protection principles: The principle of purpose limitation. The principle of lawful, safe, specific, and transparent processing.



**Other countries:**

- Jordan published a draft data protection law in 2021.
- Iraq, Iran, Palestine, Syria and Yemen do not have a comprehensive national or international facing data protection laws.

**3. Data protection in the Maghreb****a) Morocco**

Morocco's law governing privacy and data protection is Law No 09-08, dated February 18, 2009 relating to protection of individuals with regard to the processing of personal data and its implementation Decree n° 2-09-165 of May 21, 2009 (together the DP Law). Data Protection Law regulates automatic and some manual processing of personal data and sensitive personal data. Processing of personal data means any operation or set of operations performed by automatic or non-automatic means and that forms part of a filing system.

The Data Protection Law regulates the collection and processing of personal data of individuals in Morocco (referred as "data subjects" in the following Q&A) and does not protect legal persons such as limited liability companies and private limited companies. The National Control Commission for the Protection of Personal Data (Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel) (the "CNDP") is responsible for enforcing the Data Protection Law and has also issued several binding decisions on personal data processing for different purposes.

**b) Algeria**

Algeria has Law No. 18-07 of 10 June 2018 on protection of natural persons in personal data processing ("Law No. 18-07").

**c) Tunisia**

Law n° 2004-63 dated July 27, 2004, on the Protection of Personal Data, regulates personal data, but even before that, Tunisia was already a pioneer in its region since 2002 in the field of personal data protection. This law was endorsed by the 2014 constitutional embodiment of the protection of privacy, which has placed this protection at the forefront of the rights

## “ Businesses can no longer have perimeter protections in place and call it a day.”

and freedoms to be guaranteed in the new Republic.

Additionally, articles 56, 61 and 75 of the Organic Law n° 2015-26 of August 7, 2015 on the Fight Against Terrorism and the Prohibition of Money Laundering addresses the subject of personal data and when the use of personal data is permitted.

Tunisia became the 51st Member State of the Council of Europe Convention 108 on November 1, 2017.

In March 2018, it introduced a new draft law on the protection of personal data in line with the new European GDPR in Parliament.

**4. Defining the scope**

Different concepts are linked to the question of data security, protection and privacy: each refer to a different field and different considerations but which can be linked. Companies and States are equally interested in all three, but at different levels. Various fields of expertise are involved to meet the needs of companies in the three areas mentioned.

i. Data governance is the capability within an organisation to help provide for and protect for high quality data throughout the lifecycle of that data. This includes data integrity, data security, availability, and consistency. Data governance includes people, processes, and technology that help enable appropriate handling of the data across the organisation. Data governance programme policies include: delineating accountability for those responsible for data and data assets, assigning responsibility to appropriate levels in the organisation for managing and protecting the data, determining who can take what actions, with what data, under what circumstances, using what methods, identifying safeguards to protect data and providing integrity controls to provide for the quality and accuracy of data.

ii. Data security or protection Data security/protection is about protecting data from compromise by external attackers and malicious insiders. The term data protection or data security deals with the technical framework of keeping data secure and available.

iii. Data privacy governs how the data is collected, shared and used. A business may have to meet legal responsibilities about how they collect, store, and process personal data, and non-compliance could lead to huge fines under regulations such as GDPR or another legislation. If the business becomes the victim of a hack or ransomware, the consequences in terms of lost revenue and lost customer trust could be even worse.

In order to protect against threats, organisations and States need to know what data to protect and how to help keep it protected. Information protection is at the core of security, but how can an entity protect it if it doesn't know what data it has, where its data is, how it is used, who it is shared with (and how it is shared). Businesses can no longer have perimeter protections in place and call it a day. The perimeter of utilisation has expanded to suppliers, cloud vendors, partners, and so on. Therefore, data management in a structured, responsible, and law-abiding way will make it more efficient for security professionals to protect it.

**5. French views on the upcoming security challenges**

On July 13, 2022, Stéphane Bouillon, Secretary General of The Secretariat-General for National Defense and Security (SGDSN) was auditioned by the French National Assembly's Defense commission. The SGDSN, is a governmental organ under the authority of the Prime Minister of France. Hereafter, the major outcomes of his audition:

**i. An evolving global context**

Threats have changed. The crises have changed in dimension. Previously they were localised and short, called 'short kinetics', the 'shots' were easy, sometimes it looked like an American movie with a happy ending. The Covid crisis has upset this pattern. The crises have become long-lasting, generalised, their effects are very widespread in domestic territories and beyond. During the Covid crisis, France applied 95% of the plan to fight the pandemic, but after about ten

days, it had become inapplicable for lack of vaccines and other means.

French authorities were overwhelmed. Globalisation, after the fall of the iron curtain, has disappeared. The world has returned to a system of state selfishness and closed borders to which decision makers must adapt in terms of planning.

## ii. The type of threats

1. Countries witness an explosion in the number of digital attacks and file extractions, espionage, sabotage, ordered by States and State proxies. In 2021, ANSSI (French National Cybersecurity Agency) observed 1082 proven intrusions, which represent an increase of 37% compared to 2020.
2. Some countries, like France, suffered attacks from a foreign state, which aimed to destabilise the population and allow the leader of this country to reassert his authority over his community says Bouillon.
3. The third type of hybrid threat (after cyber and disinformation) is Law Fare attacks against French companies. This is the application by a foreign state of its law on another country. The United States are experts in this field.

Another hybrid threat is attacks on economic security. This ranges from the intern who hangs around after the office hours to copy files, to the visit of a foreign delegation who forgets small objects under the table or takes photos. Very large companies are aware of it but small and medium-sized companies, which are sometimes infiltrated without knowing it, are very vulnerable. Other attacks are committed like reputational attacks and stock market attacks.

Cyber and disinformation attacks are from the weak to the strong. Faced with attacks from small or medium-sized countries, France has little response capacity because it often faces autocracies without a free press, where accidents are censored. It is hard to react.

## iii. Predictions

Cybersecurity attacks

Countries must prepare for the conflicts of the 21<sup>st</sup> century and global warming. Access to water and food, to raw materials will lead to a form of conflict that will have consequences in daily lives, and not only in the 'military corner'.

Faced with new forms of conflictuality, the French National Cybersecurity Agency which has €176 million under the recovery plan, has helped 600 entities. Ongoing legal reforms will aim to strengthen its prerogatives to oblige platforms to report vulnerabilities and attacks to their customers.

For instance, if, under 130 km per hour, the direction of the car that I have just bought starts to falter, the manufacturer has the obligation to warn me. But if I use a vulnerable computer, exposed to an external control attack or sabotage, the company has no obligation to tell me. This has to be corrected for Bouillon.

During the war in Ukraine, many cyberattacks were expected from Russia, but France had had very few to date. The only notable attack was against a VIASAT satellite, operated by Eutelsat. In France, this only affected emergency relays. In Germany, a good part of the wind turbines stopped.

## iv. Awareness of public actors

The awareness of public actors is a complex subject. Every day, security authorities read briefing notes informing them that a university or a laboratory has agreed to take this or that. France subsidises laboratories and companies, through recovery plans, and gives them aid so that they can develop and not serve a foreign state. Also, France is trying to stop fakenews as soon as possible to avoid conflagration because, once it spreads, authorities can't stop it. Security agencies' role is not to denounce a lie, but to alert to the fact that they are discussing with a spy from such and such a country. Countries need to make it clear that spreading information can be artificially amplified, constructed and expanded. French citizens have to understand that they are not talking to ordinary people but to agents who are repeating propaganda talk.

National authorities are working to enhance trustful clouds. They are negotiating and working with operators like Microsoft and with French companies so that they set up "hybrid" offers accepted by French National Cybersecurity agency. For the Olympic Games of 2024, a negotiation is underway between France and Alibaba because it's the official Cloud provider for the Olympic Games.

French authorities are trying to have a sovereign Cloud which will allow them to host and therefore protect all sensitive data in France.

## 6. Information systems security, the extra-legal issue

Information systems security deals with the protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

In France, the National Security Agency (ANSSI) is the entity in charge of these issues. This body manages state security at the state level. Its director explains: the question is no longer whether or not a company will be the target of attackers, but it is knowing when this will happen. No risk does not exist. This is to limit the consequences of a probable attack.

ANSSI was created in 2009. It must respond to crises that threaten information systems. They issue alert bulletins on products and vulnerabilities (1). It designs and implements the secure interministerial means of electronic communication necessary for the President of the Republic and the Government (2). It issues product approvals to service providers intended to protect company information systems (3). It leads and coordinates interministerial work on digital security. It develops information system protection measures and carries out controls. The world of data security is a small, fairly restricted world. The mains players are the following:

- The 1<sup>st</sup> family "Steering, organization of safety and risk management" brings together all the professions with high responsibilities in terms of managing the information system security and risk management:

- > Head of Information Systems Security (RSSI)
- > Security Correspondent
- > Responsible for the Business Continuity Plan

- The 2<sup>nd</sup> family "Management of security projects and security life cycle" brings together all the professions related to system security development projects of information. They are either supervisors of these projects or major players:

- > Director of security program
- > Security project manager
- > Security Developer
- > Security architect



“

The data economy attracts a multitude of crimes that states and companies must identify and process because the time of technology is as fast as the time of cybercrimes.

- The 3<sup>rd</sup> family known as “maintaining security in operational condition” covers all the operational professions in charge of configuring and deployment of security patches and the application of security measures on the infrastructure technique:
  - > Security Administrator
  - > Security Technician

- The 4<sup>th</sup> family “Support and management of security incidents” concerns the professions intervening directly on cybersecurity incidents such as viruses, ransomware or ransomware, information leaks. They also participate in the continuous improvement of detection and prevention methods of these security incidents:
  - > SOC Analyst (Security Operations Center)
  - > Incident response manager

- The 5<sup>th</sup> family “Advice, audit and expertise in security” brings together the expertise professions in cybersecurity. These professionals are generally commissioned by companies to meet a specific need or because they have skills that these companies do not have:
  - > Risk and compliance governance consultant and auditor

- > Technical security consultant and auditor
- > Assessor / security assessor of systems and products
- > Cryptologist
- > Legal expert in cybersecurity
- > Data Protection Officer (DPO/DPD)
- > Security trainer

In 2020, 60% of companies saw at least one cyberattack and according to the European Commission, Europe recorded 756 cyberattacks this year, an increase of 75% compared to 2019. In this context, the most prevalent attack vectors in 2020 are phishing (80%) and exploits (52%). Shadow IT is for 44% of companies one of the main causes of cyber risks.

In cybersecurity of information systems, the company only succeeds with the unfailing support of the general management. It is the head of the establishments which must be involved in the security process, on several levels, at the decision-making level (orientation / strategy), at the hierarchical level (security action) and at the budgetary level (to put the means and the staffs).

## Conclusion

Data security and governance integrates several sectors, the main ones being IT and law. The first allows the second to consolidate its objectives in accordance with the law. Computer scientists are on the front line to deal with data issues raised by the development of new technologies, including the exponential increase in the mass of data. The data economy attracts a multitude of crimes that states and companies must identify and process because the time of technology is as fast as the time of cybercrimes.

CALL FOR  
**papers**

For more details  
[contact@theglobaldiwan.org](mailto:contact@theglobaldiwan.org)

Besides being a business club, intellectual work and curiosity – the gate to understanding other cultures – hold a distinct place in our Diwan. We welcome people from different horizons and nothing interests us more than to have contributors sharing their insightful and challenging views in our columns.

Please do not hesitate to get in contact with us if you wish to share your work with our audience.



THE GLOBAL  
DIWAN

CONNECTING EAST-WEST  
LEADERS

**Editor-in-chief**

Vincent Tabourdeau 

**Publication Director**

Éric Schell 

[contact@theglobaldiwan.org](mailto:contact@theglobaldiwan.org)

[www.theglobaldiwan.org](http://www.theglobaldiwan.org)