What the Normalization of GCC Relations Means for your Business

March 21, 2021

Recent reports of the thaw in the chilled relations between Qatar and the countries of the GCC previously boycotting Qatar are welcome news to businesses operating in the Gulf.

The normalization of political relations between the GCC countries pursuant to the *AlUla Declaration* that was signed in the first week of January 2021 in the Kingdom of Saudi Arabia could result in the impacts to businesses highlighted below.

Although it remains unclear at this time how each country will respond to such a rapprochement, anticipating how normalization might affect such matters as trade routes, immigration, and investment should assist businesses in recognizing opportunities and mitigating risks.

Commercial Relations

Over the course of the embargo against Qatar, businesses operating throughout the Gulf have faced disruptions to, among other things, supply routes, transportation, recruitment, and scheduling obligations. Parties have sought to accommodate the impacts of these disruptions through contractual provisions aimed at providing relief to harmed parties. These "workaround" provisions have resulted in increased costs to business operations, development projects, and ultimately the public at large, throughout the Gulf.

Businesses should consider reviewing current contract obligations and how they would be affected by the elimination of embargo related disruptions. Parties may desire to enter

into Letters of Intent or Memoranda of Understanding to specify actions that would be implemented upon a lifting of restrictions.

Contracts that were suspended or terminated for *force majeure* (or other) causes could be revisited to explore their ability to be reinstated. Where contracts provided extraordinary modes of performance to deal with disruptions to normal operating methods, parties may revert to the original means of contractual performance.

Regional rights (such as those in agency or franchising) could be negotiated with more mutually beneficial terms considering the elimination of restrictions to travel and other impediments.

The cost of insurance for ongoing projects in the GCC may be reduced reflecting a lessening of project risks, thereby reducing costs.

Parties deterred from bidding on projects in a particular GCC country due to political concerns, may revisit tender opportunities in these countries. Businesses may also seek to reestablish relations with business partners in those countries where operations have been suspended.

Trade Routes

The embargo negatively affected imports into Qatar from countries previously supplying goods and services, including Saudi Arabia, Germany, China and the United States. Those countries which realized increased trade relations include India and Turkey. These disruptions to normal trade routes resulted in part from the closure of the border between Saudi Arabia and Qatar, and the rerouting of goods through ports friendly to Qatar.

For global exporters who utilize the Jebel Ali port as a single point-of-entry to the GCC market, the normalization of

GCC relations could result in reinstating efficient access to all markets within the GCC, as the Saudi-Qatar border reopens for sea-land transport. In addition, the ability to freely access all GCC ports would eliminate current port restrictions limiting imports from foreign markets such as India and China.

Immigration and Recruitment

Businesses adapted to the restrictions imposed by the embargo by, in some cases, revising internal governance structures. These revisions were needed to comply with new rules on authorized signatories for labor contracts, bank accounts, and immigration documents. As these rules may ease with a normalization of relations, businesses may wish to revert to more efficient governance structures.

Businesses may also benefit from an easing of restrictions imposed by various GCC countries which limit immigration from specified countries and affect the rights of foreigners to reside in each country.

Enforcement

The ability to seek enforcement of judgments in each country of the GCC should be enhanced with a normalization of relations. As embassies closed during the embargo reopen throughout the GCC countries, the ability to obtain attestation and other services required in the enforcement of foreign judgments will be restored.

In addition, arbitral forums for dispute resolution located in the GCC, such as the Arbitration Centre within the Dubai International Financial Centre, may see an increase in regional cases as parties seek to avoid the higher cost of arbitration in European venues.

In sum, the consequences of normalization of political relations would go well beyond those noted above and could further enhance the GCC as a stable market for foreign direct

investment. We welcome your inquiries on this topic.

Highlights from the AlUla Declaration

Construction of the Gulf railway network:

“Completing the requirements for the Customs Union and the Common Gulf Market. This includes achieving full economic citizenship that grants citizens of GCC countries the freedom to work, move and relocate, and invest in the Member States. As well as equal access to education and health care, the construction of the Gulf railway network, the creation of food and water security systems, and continuing to encourage joint projects that localize investment in the Gulf.“

Anti-corruption:

“Strengthening governance, transparency, accountability, integrity, and anti-corruption mechanisms through Joint-Gulf action and in all entities of the GCC, including its specialized bureaus. As well as benefiting from the agreements of the G20 framework and the “Riyadh Initiative” pertaining to cooperation in investigations of cross-border corruption and the prosecution of the perpetrators in order to mitigate the impact corruption has on economic growth, sustainable development, and mutual trust between governments and their peoples.“

Economic integration:

“The full implementation of the vision put forth by the Custodian of the Two Holy Mosques, King Salman bin Abdulaziz, King of the Kingdom of Saudi Arabia, in the 36th GCC Summit in December 2015. This includes abiding by a timetable, the completion of economic integration, the implementation of joint defense and security systems, and a unified foreign policy for the Member States.“

Customs integration:

"Completing the requirements for the Customs Union and the Common Gulf Market. This includes achieving full economic citizenship that grants citizens of GCC countries the freedom to work, move and relocate, and invest in the Member States. As well as equal access to education and health care, the construction of the Gulf railway network, the creation of food and water security systems, and continuing to encourage joint projects that localize investment in the Gulf."

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Global Guide to Legal Issues arising out of COVID-19

March 21, 2021

The profound impact of the measures being taken to contain the spread of the novel coronavirus ("**COVID-19**") is creating a multitude of issues for businesses and their employees. Legal concerns related to corporate governance, disclosure, contracts, financing, strategic transactions, employment, and others are summarized below.

Here are some key legal issues surrounding COVID-19:

1. Employment

Organizations are required to maintain a safe workplace, which would include taking steps to reduce the risks associated with the COVID-19 outbreak. The steps that an employer should take will vary depending on the type of business but include the

following elements:

- Restrictions on Travel

It is generally permissible for organizations to implement policies that restrict business travel to high-risk destinations and require employees returning from such destinations to self-quarantine for the maximum period. While employers cannot generally restrict personal travel, it is generally permissible to implement a policy requiring that an employee provide advance notice of any personal travel (in particular to high-risk destinations) and requiring that employees self-quarantine upon their return from destinations where there are known cases of COVID-19. Organizations should take care to apply the policy impartially and consistently to help avoid claims of discrimination based on the protected class of impacted employees. Proper documentation of decisions made and consistent application will be key to protecting against such claims.

- Remote Working

Most organizations have commenced remote working of their staff. Where working from home is not possible, and employees are absent due to sickness, quarantine, or childcare needs, employers will need to determine whether and for how long absent individuals will continue to be paid and create flexibility in leave policies.

- Communication and Confidentiality

Organizations should determine how best to communicate the message that an employee has tested positive for COVID-19. Employers do have a general duty to inform the workforce if an employee tests positive or is a probable COVID-19 case. However, the confidentiality and privacy requirements of applicable laws, mean that steps should be taken to preserve the privacy of the impacted employee and not share their identity with the workforce. Organizations have a duty to

protect employees from discriminatory or retaliatory behavior by other employees if they are suspected to have COVID-19 or have self-reported.

2. Supply Chain

As the global economic impact is expanding, organizations are facing increasing disruptions to supply chains as a result of a drop in consumer demand and workforce impacts. Businesses which are affected are seeking to understand their rights and obligations, and any relief which may be available to them.

Such assessments include supply chain exposure and prioritizing critical suppliers (tier 1) that are impacted and implementing a strategy to identify and negotiate any current and future (post-COVID-19) potential benefits that may be obtained. Contracts could be addressed in the following way: (i) negotiation to optimize onward supply, and mitigate supply chain impact; (ii) assessment of contractual options available: suspension, termination or force majeure declaration, frustration, etc (iii) claims which may be brought on a case-by-case basis.

3. Contracts

While each contract will have to be examined on its own, the outbreak of COVID-19 is likely to have a profound impact on commercial contracts. Organizations or their suppliers may find they are unable to perform under an existing commercial contract. Parties to existing contracts that are or may be disrupted by the outbreak of COVID-19 should promptly assess their legal rights and obligations, including:

1. assessing contractual provisions that have been or may be affected;
2. identifying and abiding by any relevant notice requirements;
3. analyzing the risks and consequences of a default or breach under the contract; and

4. determining or negotiating alternative means of performance under the contract, where possible.

Where organizations are currently negotiating contractual contracts, it should proactively consider the impact of COVID-19 and appropriately allocate potential risk in the contract.

- Force Majeure

Contract parties may consider issuing force majeure notices or may receive such notices to excuse a party's non-performance. Any declaration of force majeure must be evaluated under the terms of the agreement and analyzed under the law governing the terms of the contract. Parties should not cease their performance on the basis of a force majeure event without consulting counsel because a mistaken assertion of force majeure or frustration could have serious consequences. Specifically, an incorrect assertion of force majeure or frustration may amount to a breach (or anticipatory breach) of the contract. A declaration of force majeure will generally not avoid payments under a contract.

The consequences flowing from a declaration of force majeure should be considered carefully and may include:

1. Whether the parties' agreement includes notice obligations before declaring force majeure;
2. Whether the force majeure event actually made the party's performance impossible, or just more burdensome (commercially unreasonable, etc);
3. Whether the affected party is required to mitigate by using diligent efforts to end the failure or delay and ensure the effects of the force majeure event are minimized or mitigated;
4. Whether immediate relief is available for the affected party;
5. Whether force majeure-related disputes must be

arbitrated or the potential costs of litigation and/or dispute resolution; and

6. Whether force majeure events are covered by the parties' insurance policies (including general liability, business interruption, contingent business interruption, or other insurance policies), and if so, what conditions must that party meet for its claim to be satisfied.

The declaration of force majeure should also take into account the impact on other agreements and obligations between the same parties or business activity.

- Material Adverse Change

Some agreements contemplate and allocate risk among the parties in the event of a material adverse change/effect to the business. If triggered, it may allow a party to terminate the agreement or otherwise avoid performance. Organizations may consider and evaluate any contractual notice requirements in this regard.

- Frustration or Impossibility

If a contract does not contain a force majeure clause, it may still be possible for a party to argue that the COVID-19 outbreak has frustrated the contract or that the performance of the contract becomes objectively impossible. The concept of "frustration" may excuse the performance of a contract in situations where the performance of a contract is possible, but no longer provides a party with the benefits that induced them to make the bargain because of intervening unforeseeable events. It will not apply when a contract simply becomes less profitable, or even when performance causes one party to sustain a loss.

The concept of "impossibility" excuses a party's non-performance when performance becomes objectively impossible because of the destruction of the subject matter of the contract or the means of performance.

There may be other defenses that may exist at law, for example, unfair contract terms and which should be considered.

4. Data Protection

Some data protection authorities have started to provide guidance, but there are divergent views on how employers should comply with data protection requirements, depending on the jurisdiction. There may be restrictions on organizations' ability to collect information about the body temperature of their employees or visitors to the premises or information about health and possible COVID-19 symptoms from them. If an organization is alerted to a case of COVID-19 amongst its employees, organizations may record the date and identity of the person suspected of having been exposed to the virus and the organizational measures taken (isolation, remote working, contact with the company doctor, etc) and report to the relevant health authorities.

Looking Forward

The above are some legal issues that must be considered alongside a business continuity and resilience plan to ensure that organizations are able to meet the ongoing challenges created by COVID-19. Many governments have launched measures for supporting companies at this time.

The extent of measures taken by the authorities in response to the current Covid 19 threat and the way they are applied vary considerably from one state to another at different points of time. This is partly caused by the fact that states have different constitutions and some states are subject to conventions. While some restrictive measures adopted by certain states may be justified on the ground of constitutional or conventional clauses relating to the protection of health measures of exceptional nature may come into conflict with other rights en freedoms. For instance, the European Court of human rights has granted states in the

European Union a large margin of appreciation in this field. Recently, the Dutch government implemented the NOW-arrangement (Noodfonds Overbrugging Werkgelegenheid), providing financial help for employers to pay their employees' wages in the COVID-19 crisis.

Now is the time to implement strategies for business stability and prioritize the safety and well-being of your employees as well as those around you. How you do this will vary between businesses and may require tailoring. If you would like assistance, we can advise you on planning your next steps.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Foreign Investments in Lebanon for Medical Cannabis Investors

March 21, 2021

On 20 April 2020, the Lebanese Parliament passed a law permitting the cultivation, trade, research, and use of medical cannabis. The passing of the law by Lebanon creates an opportunity for leading medical cannabis companies globally to enter the Lebanese market. There are six classes of license applicants including foreign companies licensed in their home jurisdiction. Other opportunities that foreign investors are

surveying are partnerships and associations with farmers and enterprises in Lebanon. In this article, we detail information regarding foreign investment in Lebanon that is a consideration for foreign investors interested in the medical cannabis industry in Lebanon.

Lebanon is renowned for its liberal economy and strategic location and has consistently attracted significant foreign direct investment ("FDI") inflows. In recent years, FDI flows into the country have shown resilience, despite several challenges to investments globally and regionally. FDI performance has remained above that of similar countries, including the Middle East and North Africa ("MENA") region as a whole. In fact, Lebanon's FDI stock reached USD 68 billion in 2019, an increase of more than USD 20 billion in more than ten years.

The majority of investors come from France, the United Arab Emirates, the United States, Germany, the United Kingdom, the Netherlands, Jordan, and Egypt. FDI in Lebanon is mainly oriented towards trade, real estate, services, tourism, and agriculture. Many other opportunities exist in the healthcare, energy, oil and gas exploration, information and communication technology, and franchising sectors, to name a few.

Lebanese Government Incentives

In order to facilitate investor establishment and administrative formalities, Law No. 360 of 2001 introduced tailored incentives through package deals for large investment projects, including tax exemptions for up to ten years, reductions on construction and work permit fees, and a total exemption on land registration fees. The Law also created a government agency called the Investment Development Authority of Lebanon (commonly known as "IDAL") with the aim of providing national and foreign investors alike with comprehensive sets of services across their various stages of operations in Lebanon in the following sectors: Agriculture,

Agro-Industry, Industry, Tourism, Information Technology, Telecommunications, and Media.

The Development of a Strong Legal and Institutional Framework

Moreover, the government of Lebanon, generally maintaining a non-interventionist position, has recently embarked on a reform drive to improve the legal and institutional framework for investments. A series of new laws have been adopted and almost 70 bills are currently being considered. In several regulatory areas, such as commercial arbitration or environmental assessment, Lebanon is considered a model for other countries to follow.

Specifically, Law 81 of 2018 on Electronic Transactions and Personal Data; Law 85 of 2019 on Offshore Companies and Single Member Offshore Companies; and Law 126 of 2019, which amended the Code of Commerce law from 1946, were adopted to create a new ecosystem where companies and startups can prosper and develop. Their main goal is to make the country more attractive to foreign investments and expose the Lebanese markets to international standards and scale.

The Lebanese Legal Framework for Foreign Investors

Lebanese business law is, in principle, very open to all traditional forms of investment. Foreign private entities may establish, acquire, and dispose of interests in business enterprises and may engage in all types of activities. Lebanese law does not differentiate between local and foreign investors, neither does it dictate who can establish a Lebanese company, participate in a joint venture, and allows for the establishment of a local branch or subsidiary of a company without difficulty. Foreigners doing business in Lebanon through a company, factory, or office must hold work and residency permits. Yet, there are no discriminatory or excessively onerous visas, residence, or work permit requirements.

Additional guarantees for foreign investors are contained in bilateral investment treaties ("BIT"). Lebanon has concluded 50 BITs with traditional investment protection provisions and is a party to seven treaties with investment provisions ("TIPs"). Once established, investors are offered high standards of treatment and protection even though these are not inscribed in the law. Furthermore, expropriation is strictly regulated and a rare occurrence in the nation.

In the event of a commercial dispute, domestic and foreign investors have access to local courts and to commercial arbitration. The BITs signed by Lebanon all grant access to investor-State arbitration. The country has ratified the 1965 Convention on the Settlement of Investment Disputes between States and Investors ("ICSID Convention") and the 1958 Convention on the Recognition of Foreign Arbitral Awards ("New York Convention"). A comprehensive arbitration framework is in place, and although arbitral awards need to be given enforceability through a court exequatur, overall, Lebanese courts are favorable to arbitration.

The Tax System

The country has adopted a corporate tax regime based on a low corporate income tax and a multiplicity of exemptions and exceptions and is constantly working towards increasing transparency. Law 43 of 2015, allows for the exchange of information for tax purposes with the countries which have concluded a double taxation avoidance agreement ("DTAA"), and which contain related provisions, with Lebanon. Industrial investments in rural areas benefit from tax exemptions of six or ten years, depending on the specific criteria. The Lebanese Parliament enacted a law in April 2014 to reduce income tax on industrial exports by 50%. The government grants customs exemptions to industrial warehouses for export purposes.

Foreign Ownership of Lebanese Property

Law No. 296 of 2001 deals with foreign property acquisition matters. The law relaxed some legal constraints on foreign ownership of property, ended discrimination between Arab and foreign nationals, and decreased the fees of real estate registration to the same amount for both. A foreigner may also obtain up to 3,000 square meters of real estate without an authorized permit; a special Cabinet issued Decree, however, must back any exceeding amount. The law also allows foreigners to acquire an area no more than 3% of the area of Lebanon, whatever the geographic site, provided that the total property does not surpass 10% of the region of Beirut.

Protection of Intellectual Property Rights

Lebanon's intellectual property rights ("IPR") legislation is compliant with Trade-Related Intellectual Property Rights ("TRIPs") and World Trade Organization ("WTO") regulations. IPR laws govern copyright, patent, trademarks, and geographical elements. Lebanese law provides patent protection for inventions and plant varieties and unique protection for layout designs of integrated circuits. Furthermore, the law provides protection for undisclosed information. When it comes to trademarks, those are provided protection via Lebanon's membership to the Paris Convention for the Protection of Industrial Property ("Paris Convention"). Moreover, geographical indications are provided protection under the provisions of the new Law on Customs, the Law on Fraud Control, and the Criminal Law. Additionally, the law provides strict penalties for copyright breaches and adequate compensation to the persons whose rights have been infringed. New draft laws and amendments to existing laws aimed at improving the IPR environment, notably for industrial design, trademark, geographical indications, as well as amendments to the copyright law, are in the pipeline.

Prevention of Corruption

Corruption is perceived as a deterrent for business in

Lebanon. However, in April 2018, the government launched a National Anti-Corruption Strategy, and a robust movement is underway to deal with corruption practices. In fact, many laws were adopted in this process: the Access to Information Law, the Anti- Corruption Law, the Whistleblower Protection Law, the Anti-Money Laundering Law, and the Illegitimate Enrichment Law. Also, a modern law on the independence of the judiciary is underway. Public and civil society stakeholders are more than ever actively engaged in new tools and initiatives to address corruption.

Lebanese Customs Duties and Booming Sectors

Lebanon has strong potential to become a regional leader in pharmaceutical production and sales. Through its developed STEM educational curriculum, the country is able to supply a highly specialized labor pool for the pharmaceutical industries. Additionally, it has direct access to the MENA pharmaceutical market, which has one of the highest growth rates – surpassing that of the U.S. Pharmaceutical manufacturing companies – whilst other industries are eligible for a 50% exemption on tariff duties at export. Machinery, equipment, spare parts, and building material imported for the setting up of new industrial firms, are subject to a mere 2% customs duties. Custom duties exemptions are applied to raw materials and semi-manufactured goods. Lebanon’s cosmetics industry ranks amongst the top 5 Lebanese exports indicating its strong position and its potential to grow to address regional and global demand.

Lebanese Labor

Finally, Lebanese labor is inexpensive, maintains a highly entrepreneurial culture and background, and is known to have an elevated educational level and strong linguistic capabilities.

Conclusion

Considering all the above, Lebanon will undoubtedly, and always, be a promising destination for investment opportunities, despite everything.

Author: Chehade Maalouf

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Data Processing Agreements: are they really needed under the GDPR?

March 21, 2021

You may have had a customer approach your organization to enter into a data processing agreement and wonder if it is mandatory to do businesses within the scope of the GDPR or if a simple clause that states "*The Service Provider agrees to comply with applicable data protection and privacy laws*" is sufficient to comply with the General Data Protection Regulation (EU 2016/679) ("**GDPR**"). The GDPR requires that a data controller who engages a data processor must enter into a **written contract** or legal act along the lines set out in Article 28.3 of the GDPR.

The **data processing agreement** as it is commonly called is a key contractual document that sets out the responsibilities and liabilities of both controller and processor. If a processor uses another organization (ie a sub-processor or

“other” processor) to assist in its data processing of personal data on behalf of a data controller, it needs to have a written contract in place with that sub-processor.

WHAT SHOULD BE INCLUDED IN A DATA PROCESSING AGREEMENT?

In order for an organization to meet the requirements of the GDPR, as a data controller who engages the services of a data processor to process personal data on its behalf, it must enter into a data processing agreement (a written contract or other legal act) which is legally binding on the data processor. Article 28.3 of the GDPR sets out what needs to be included in that written contract:

1. the processor must only act on the controller’s documented instructions unless required by law to act without such instructions;
2. the processor must ensure that its personnel processing the data are subject to a duty of confidence;
3. the processor must take appropriate measures to ensure the security of processing;
4. the processor must only engage sub-processors with the controller’s prior authorization and under a written contract (some controllers provides a general authorization to the processor in the data processing agreement);
5. the processor must take appropriate measures to assist the controller to respond to requests from individuals to exercise their rights.
6. taking into account the nature of processing and the information available, the processor must assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
7. the processor must delete or return all personal data to the controller (at the controller’s choice) at the end of the services contract or data processing agreement,

and the processor must also delete existing personal data unless the law requires its storage; and
8. the processor must submit to audits and inspections.
9. the processor must also give the controller whatever information it needs to ensure that both controller and processor are meeting their obligations under Article 28 of the GDPR.

The below details are also required in a data processing agreement and is usually set out in an Appendix for ease of reference:

1. the subject matter of the processing (*does processing include for example erasure, recording, matching conservation of personal data which are required for the service provider to perform the services under the services contract with the controller*);
2. the duration of the processing (*usually this is linked to the duration of the services contract with the supplier, but it may be for a shorter period of time*);
3. the nature and purpose of the processing (*will personal data be processed for a specific purpose and will it be processed via a system or manually*?);
4. the type of personal data involved (*does it include special categories of data or confidential information of the controller?*); and
5. the categories of the data subject (*does the personal data belong to an employee or customer of the controller?*)

IS THERE A SPECIFIC FORMAT FOR A DATA PROCESSING AGREEMENT?

There is no specific format and controllers usually propose their form of data processing agreement when engaging a processor. The essential requirement is that the substance of the data processing agreement meets the legal requirements of the GDPR and then the contracting parties are free to determine the form or layout and any additional clauses that

they may wish to include (e.g data protection indemnities, contacts of data protection officers of either party and procedures for dealing with a personal data breach involving the personal data being the subject of the data processing agreement).

DATA PROCESSING AGREEMENTS IN PRACTICE

Data Processing Agreements vary in complexity depending on the subject matter of the services contract and in practice can take a considerable amount of time for negotiation depending on the relative bargaining strength of the parties to the contract and the financial value of the transaction. Some controllers opt to include the data processing agreement as a part of the services contract while others include it as an Appendix to the services contract. Some examples of data processors include commercial agents such as sale agents OR marketing agents and certain consultancy service providers depending on which party determines the “how” and “why” personal data is processed (ie the data controller) and who acts on those instructions (the data processor).

CLOUD SERVICE PROVIDERS AND DATA PROCESSING AGREEMENTS

Cloud service providers (“CSPs”) now have significant responsibilities as data processors and must act solely on the instructions of the data controller when processing personal data. Currently, most CSPs offer their own standard data processing agreements alongside the Software as a Subscription (SaaS) agreement and these may be non-negotiable by a controller wishing to subscribe to use or access the platform being offered by the CSP (e.g a data controller who wishes to use a customer relationship management to efficiently receive and track its customer requests or complaints).

Many CSPs reserve their right to use personal data for various purposes which have not been agreed with their controller (customer) and this is especially common where cloud services

are provided at no cost by the CSP. Controllers are required to engage data processors who provide sufficient guarantees such personal data will be processed in accordance with the GDPR. Organizations must, therefore, consider whether the use of CSPs will lead to additional complications and risks and, potentially, to infringement of the GDPR.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Entering the Lebanese Cannabis Market Extra-Jurisdictionally

March 21, 2021

On 20 April 2020, the Lebanese Parliament passed a law permitting the cultivation, trade, research, and use of medical cannabis (the "**Lebanese Cannabis Law"**). Despite an emphasis on the use of cannabis for medical purposes, the Lebanese Cannabis Law permits the use of cannabis for "industrial" purposes as well, which many investors seeking to enter the market can benefit from.

The Lebanese Cannabis Law and Licensing

Article (1) of the Lebanese Cannabis Law states:

"All activities dealing with the cultivation of cannabis

plants for medical and industrial use on Lebanese territory shall be subject to the provisions of this current law.”

Additionally, Article (2) of the Lebanese Cannabis Law defines “*Cannabis Product*” as:

“*each product that includes hemp, including fibers for industrial use, oils, extracts and compounds used for medical, pharmaceutical and industrial purposes.”*

With respect to the definition of “*License*” within Article (2) of the Lebanese Cannabis Law, the Law defines this as:

“*Initial permission according to a decision by the Authority to cultivate a certain amount of cannabis plant for medical or industrial use with the processes that derive therefrom as per specific criteria and conditions, and within a controlled space.”*

The “*Authority*” referenced is the Lebanese Authority for the Cultivation of Cannabis Plants for Medical and Industrial Use. This Authority will be responsible for granting license approvals and will act as the governing body for the medical and industrial cannabis industry in Lebanon.

Once the Authority commences operations, investors will be able to apply for one of the nine licenses available pursuant to Article (17) of the Lebanese Cannabis Law. However, investors can begin their operations immediately in order to get ahead of the Lebanese cannabis market, through one of the various jurisdictions where cannabis has already been legalized.

This will allow investors to commence operations and potentially apply under the five licensee types provided under Article 18 of the Lebanese Cannabis Law. Article 18(3) of the Lebanese Cannabis Law states that one of these licensee types is a foreign company, as follows:

"*Foreign companies specialized in the field of agriculture, industry, storage, export or marketing, that have a license from the country to which they belong to carry out one of the operations specified in the license, and whom shall undertake foreign investment into Lebanon through manufacturing locally, in accordance with the mechanism specified in the relevant applicable laws.*"

The Cannabis Market

Keep in mind, when comparing the cost of producing a gram of cannabis, the cost in Canada is USD 1; in Europe, more than USD 0.50; whilst in Lebanon, the cost is expected to fall between USD 0.18 and USD 0.20. It is also expected that the fertile landmass for the cultivation of cannabis in Lebanon would be beyond 6,000 acres. The conditions and natural factors of the climate, land, and soil in areas like Baalbek-Hermel are optimal to produce cannabis and increase the quality significantly. Lebanon will become one of the competing countries in the cannabis industry in cost, production, and quality.

The cannabis industry is growing rapidly, with annual market values expected to reach USD 30 billion by 2025; and with more nations legalizing the plant (for recreational and medical purposes), this value is growing by the day. This not only evidences the potential profits investors could generate from embedding themselves into the industry, but it also indicates the number of players currently dominating the global market. As such, investors wishing to make a significant impact in a short span of time can find themselves benefiting from tapping into the embryonic market of the Lebanese medical cannabis industry.

THC Levels in Industrial Cannabis

Moreover, when discussing the "*criteria and conditions*" for the cannabis plant, the Lebanese Cannabis Law does not specify

said conditions but rather, stipulates that the rate of tetrahydrocannabinol ("**THC**") in the cannabis plant will be "*determined as the Authority decides based on international standards*".

There are currently 779 cannabis strains that have been named and recognized by the international cannabis industry. The internationally approved standard for the levels of THC in these strains for industrial use is 0.3%. The European Union and the United States permit a THC rate of 0.3% for industrial cannabis, with the European Union considering a cannabis plant with less than 0.3% of THC as an agricultural commodity; whereas Colombia permits a THC rate of 1.0% and Switzerland permits 1.5% for industrial cannabis.

Difference between Industrial Cannabis and Medical Cannabis

Industrial cannabis is technically from the same species of plant that is used for medical cannabis; however, it is from a different variety/subspecies. As mentioned above, industrial cannabis has low THC levels compared to cannabis specifically cultivated for medicinal use. The reason for the low THC content is that most THC is formed in resin glands on the buds and flowers of the female cannabis plant. Industrial cannabis is not cultivated to produce these buds; the focus is on the stalk which produces the fibers. These fibers are in turn used to produce an insurmountable number of products such as insulation for construction works, clothing, cosmetics and skincare, cooking oil, biofuel, and more.

On the other hand, medical cannabis is grown with the purpose of producing flowers/buds which are in turn are used to utilize THC or cannabidiol ("**CBD**"). These buds produce THC or CBD that contain enough of those cannabinoids and other compounds, such as terpenoids, to render them medically effective; this is known as the entourage effect. At higher levels THC can become psychoactive; however, the THC can be necessary to produce optimal medical effects.

Whereas industrial cannabis does not contain significant THC or CBD, medical cannabis does, as it can be a natural pain reliever, for anti-inflammatory properties, and used to treat many ailments such as arthritis, insomnia, anxiety, chronic pain, fibromyalgia, and epilepsy.

Conclusion

Both industrial and medical cannabis are multifunctional products that aid us in all spheres of life. However, we will have to wait and see what the Authority sets the THC levels of industrial cannabis at. Depending on the avenue investors want to take, they can either deal in industrial cannabis by selling cannabis with THC levels within the 0.3% range or medical cannabis with THC levels higher. Either way, both will result in substantial profits for the investors.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Space Law and the Galactic Economy: The New Frontier

March 21, 2021

In 1961, Yuri Gagarin was the first man to venture into space; in 1969, Neil Armstrong became the first man to take that a step further by landing on the moon. Between that period, in 1967, the Outer Space Treaty went into effect, being ratified by 105 nations. Currently, the space market is worth approximately $400 billion. The commercial space industry is

heating up – 50 years ago, outer space was reserved for the most powerful of nations and the most dominant governments, but today there is a democratization of space. The commercial industry is inching us closer to the cosmos and in the process, there is a growing interdependence between what is happening hundreds of miles up into space and down below on Earth. The commercial space industry, using multi-million-dollar rockets and satellites, is increasingly playing a part in our everyday lives. Although you may have been hearing about this phenomenon in recent years, this launch into the new world has been ongoing for decades.

There have been five space treaties that have been negotiated since the 1960s. Four of which are widely ratified, however, the Magna Carta of space law, the Outer Space Treaty, is the document that all space lawyers turn to when considering anything happening in space. Recently, NASA Astronaut Anne McClain was accused of illegally accessing her spouse's bank account whilst aboard the International Space Station; this brought up a variety of legal issues and questions about how to litigate a crime committed in space. Is outer space devoid of law? Is it a vast lawless domain? Of course, it's not. The treaties govern countries and the activities of countries, but it also materializes a new dimension. The treaties make states responsible for the activities of their nationals, creating domestic regulations so that nations carefully watch and regulate the activities of those who venture into space.

This brings about the question of property rights. Where does space begin and if there is a dispute in space, who decides it? Australia is the only country in the world that defines where space begins; defining it as 100 kilometers up. However, where the air ends and the air law regime, which is governed by the International Civil Aviation Organization, and where space begins is a matter that the international community has not been able to agree on. People either want to set limits, set a height based on kilometers like Australia has done, or

they take the approach of the United States who look at it as a use; what did you use, are you launching a rocket that is intended to go into orbit or are you just launching a plane that is going to go high into the air. This is important because nations own the air over them. Right now, space is for everybody. No nation can own property in space and no nation can make any territorial claim in space.

You need consent to fly over another country if you are in the airspace, but on the flip side of that, if you believe that you are in outer space, you can fly over any country without consent and engage in espionage legally. Espionage is one part of the political-military contest, but how else is space dealt with from a military perspective? With the recent establishment of the United State's Space Force, we will likely see the same rules of war extended into outer space. The language in the Outer Space Treaty about the use of outer space for exclusively peaceful purposes, is beautifully aspirational language, but the devil is in the interpretation: what does it mean to use space for peaceful purposes? The way that this has been virtually explained is that peaceful purposes only prohibit the aggressive use of military force and as long as you are not engaged in naked aggression, then you are peaceful in your use of outer space. Another restriction is the stationing of weapons of mass destruction in orbit; but it would be naive to believe that the military will be devoid of war. Especially now that the United States has a Space Force, it is all perfectly legal, and it all depends on the course of action that the Space Force will take. At the end of the day, the Space Force is about manufacturing a bureaucratic and political constituency for orbit, whilst simultaneously investing in spacecrafts that can defend themselves (and attack, if necessary), new space sensors to track enemy missiles, and military habitants who are trained in the craft of zero gravity. This means a great deal of money for private companies, with almost half-a-dozen defense agencies already fueling millions into space start-ups

that build everything from radar networks to high-tech materials.

The majority of the money made in space lies on the back of satellite-provided services, and these services are likely to surge the space economy. The significant increase in satellites (currently there are approximately 2,300 operational satellites in space) will bring a multitude of costs and benefits. The spur in investments in new satellite servicing businesses will rise until it reaches space itself. We have seen an uproar of venture capitalists directing millions of dollars towards small satellite companies with big aspirations, such as Spire, Capella Space, Hawkeye360, and Swarm. But these are just a few of the firms who have reeled in massive amounts of cash and launched satellites. And each of these firms varies in the shape of their business models, from communicating with internet devices to tracking radio signals in order to gather radar data and image every angle of the Earth. This all falls on the cost of building and operating a spacecraft to enable the work that they desire.

SpaceX and Boeing are officially in the final phase of their private space transportation service in cooperation with NASA. Soon enough, both companies will have permission to start flying up wealthy tourists, who seek to site see the constellations, or corporate researchers who will aim to find clues in fixing the Earth they just departed from. The uncertainty is there, however, so is the promise of new opportunities for the private sector and new influxes in revenue. Space tourism is nearing existence with Richard Branson from Virgin Galactic stating that the firm has the capital to begin regular tourist trips to the edge of space; and although the seat on this flight costs $250,000, I doubt you will be served peanuts on your way up. On 27 May 2020, NASA launched astronauts into space from U.S. soil for the first time since 2011; these astronauts voyaged to the International Space Station via a vehicle that was purchased

from SpaceX.

Ultimately, NASA’s main focus, is returning humans to the moon. With access to ice water that was discovered on the moon, starry-eyed space seekers see this as the key to the grandest visions of a future space economy. However, it is still unclear whether the United States government can settle the conflicts between its dreams for space exploration and its willingness to alter the way in which NASA does business to the point of establishing a sustainable presence on the moon. But NASA is still continuing its efforts to bolster the space economy by hiring private companies to build rovers, landers, and spacecrafts that will carry scientific instruments to the moon. From an economic standpoint, this program is likely to reinforce the knowledge of private companies when it comes to operations on the moon.

The trends that pilot the optimism towards the space economy are the same as those of the tech economy: the growing power and miniaturization of transistors, solar panels and batteries, partly generated by the smartphone revolution of the last century; the rapid evolution of broadcast media, telecommunications, commerce, and the internet as a whole; and, of course, the geopolitical tensions that have governments anxiously spending on space through the hiring of private companies. The voyage into space is not far, and the economy that will manifest from it has already proven to be grand. All in all, this is simply one small step for man, one giant leap for the private sector.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

The Biggest GDPR Fines to Date

March 21, 2021

If the best way to get a company's attention is to hit them in the pocketbook, then European regulators have the full attention of many companies including data giants like Google and Facebook. Here are some of the biggest GDPR fines to date:

Google L.L.C (Sweden and France)

Back in early 2019, the CNIL, the French data protection watchdog, issued its first GDPR fine of $57 million (€50 million) claiming that Google has failed to comply with the EU's General Data Protection Regulation (GDPR) when new Android users set up a new phone and follow Android's onboarding process. In 2020, the Swedish DPA fined Google approximately Euros 7 Million by for not complying with its obligations regarding the "right to be forgotten". The "right to be forgotten" stems from a landmark ruling nearly six years ago, where the EU court forced the U.S. tech giant Google to remove European links to websites that contain out of date or false information that could unfairly harm a person's reputation Google was ordered to delist certain search results, to stop informing websites when such results occur and to otherwise adapt its data subject rights process. The French Council of State, Conseil d'État, overruled a prior decision to fine Google Euros100,000 in relation to a 2016 right-to-be-forgotten case. The court decided French law does not allow the data protection authority, the CNIL, to order search results to be removed globally, noting that the CNIL can only call for European search results to be removed.

British Airways (UK)

In July 2019, the U.K.’s Information Commissioner Officer fined British Airways and its parent International Airlines Group (IAG) £183.39 million ($230 million) in connection with a data breach that took place in 2018 that affected around 500,000 customers browsing and booking tickets online. In an investigation, the ICO said that it found “that a variety of information was compromised by poor security arrangements including log in, payment card, and travel booking details as well name and address information.

Marriott International Inc. (UK)

In July 2019, the Information Commissioner’s Office intends to fine Marriott £99,200,396 for infringements of the GDPR in relation to a breach of the Starwood hotel’s guest reservation database (339 million guests) with unauthorized access dating back to 2014. The proposed fine reflects the new ability under GDPR to fine companies up to 4% of global turnover. Mariott’s revenue last year was US$20.758 billion, the fine under the GDPR could have been significantly higher.

TIM (Italy)

In January 2020, Italian Data Protection Authority (Garante) issued a €27,8 million fine to TIM (telecommunications operator) for violation of the GDPR, with emphasis on unlawful data processing, non-compliant aggressive marketing strategy, invalid collection of consents and excessive data retention period

Austrian Post (Austria)

The Austrian Data Protection Authority issued an 18 million euro fine against Österreichische Post AG for alleged violations of the EU General Data Protection Regulation that the ÖPAG processed the political affiliation of data subjects and further processed data on package frequency and the frequency of relocations for the purpose of direct marketing.

1&1 Telecom GmbH (Germany)

1&1 Telecom was fined by the German Federal Commissioner for Data Protection and Freedom of Information for not taking appropriate action to prevent unauthorized parties from accessing customer data in their call center since a caller calling their customer service department and giving them the name and date of birth provided access to customer information.

Lessons learnt

The GDPR fines to date should serve as notice to other companies both under investigation now, and that may be investigated in the future that the possibility of fines under the GDPR is very real. Apart from the business disruption and the financial implications, a GDPR fine can take your organization's brand image into a downward spiral, and regaining customers' confidence will be a costly and timely affair. It is therefore worthwhile to consider whether your organization meets the legal requirements of the GDPR and whether it can withstand a regulator's meticulous eye. Please reach out to us to discuss your organization's need to comply with the GDPR or any details of enforcement action under the GDPR.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Arab court qualifies COVID-19

as force majeure event

March 21, 2021

In what could possibly be the first judgment amongst Arab jurisdictions, the Egyptian Administrative Court within the State Council ruled that COVID-19 qualifies as a force majeure event.

To clarify the title of this article; 'Arab court' refers to the fact that this judgement was obtained from *an* Arab court given that there is much cross-jurisdictional reliance on judgements and case law amongst Arab economies such as the United Arab Emirates, Palestine, Iraq, Jordan, Kuwait, Egypt, Lebanon, Gaza, and so on.

Courts in these jurisdictions respect rulings from their Arab counterparts on matters that have not been addressed at length in their own respective jurisdictions.

Hence, the significance of this judgement is that it may have extra jurisdictional effects and be grounds – or be argued as grounds by counsel – in other courts in Arab jurisdictions.

The dispute arose when a president of a government association ordered suspension of a scheduled election until normalization of daily life.

An association member challenged the president's decision before the Administrative Court appealing to nullify the decision.

The association president argued that COVID-19 was a force majeure event and that various Government decisions had been issued prohibiting certain activities which were sufficient grounds for the suspension of the scheduled election.

In June of 2020, the Court ruled qualifying COVID-19 as a

force majeure event as follows:

“As with respect to the current dispute, and in light of the force majeure event that has effected the globe, the World Health Organization has announced that the novel coronavirus (COVID-19) is to be categorized as a pandemic, and as the State has taken action to deter the pandemic and protect the health of its citizens…to temporarily suspend all activities that require mass gatherings for citizens or that require their transport from one governate to another en masse (such as concerts, cultural events, events, and festivals) until further notice…”

The Court also addressed the implications of Sharia law on COVID-19 related disputes as follows:

“…as human life is the most valuable thing that governments, nations, organizations, and associations can protect, it goes without saying that protection of life is an epitome priority under Sharia law, as without human life the world does not prevail, and as in Sharia law; he who saves a single life is as if he saved all human life…and although it is a foundation of democratic life to permit elections to occur as scheduled; no reason can trump the duty to protect human life.”

The GCC and Levant countries are civil law jurisdictions and generally apply the same interpretation of foundational legal principles under civil law; such as those related to force majeure.

Since May 2020, practitioners and courts in Arab jurisdictions have turned to the judgment issued by the Paris Commercial Court in May where the Paris Commercial Court found that COVID-19 could not have been reasonably foreseeable and qualifies as a force majeure event – a judgment that was circulated and discussed widely and relied on regionally given that Arab jurisdictions share the commonality with France as civil law jurisdictions.

Now, parties with business in the Middle East looking to argue that COVID-19 is a force majeure event and relieve themselves of any impossible obligations may draw reference from a much closer jurisdiction; Egypt.

The judgment is also significant as it relies on the World Health Organization's categorization of COVID-19 as a pandemic but further delves into Sharia law principles on the protection of human life, in addition to restrictive Government orders.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

Data Protection Enforcement

March 21, 2021

Regulators globally continue enforcement of data protection and privacy laws including issuing fines against organizations that did not meet the requirements of applicable law. In this article, we summarise some of the recent cases of interest:

Posti Group Oyj (Finland): Direct Marketing

According to the Deputy Data Protection Ombudsman, there were complaints alleging that data subjects received direct marketing from the company although they had requested that their postal data be deleted. Investigations also revealed that the data protection information provided by the company was not transparent enough and a fine of €100,000 was issued.

Consumers are more likely to complain about unsolicited

marketing and in many countries, electronic communication and data protection laws require consent to be obtained before sending emails or SMS messages to consumers. Further, when a consumer has opted out from receiving marketing, organizations are mandated to heed this request.

Banca Comercială Română SA (Romania): Data Security

The National Supervisory Authority for Personal Data Processing ('ANSPDCP') announced, on 5 May 2020, that it had fined Banca Comercială Română SA RON 24,163.50 (approx. €5,000) for violating its obligation to ensure the security of data processing under Article 32 of the GDPR. In particular, Banca Comercială Română had not implemented adequate technical and organizational measures to ensure an adequate level of security in light of the risk of data processing. In addition, the ANSPDCP found that the collection and transmission to the operator via WhatsApp of copies of customers' identity documents constituted a violation of the internal working procedure.

Organizations should assess their current technical and organizational measures to ensure it aligns with Article 32 of the GDPR or applicable local laws.

National Government Service Centre (NGSC) (Sweden): Data Breaches

On 29 April 2020, the Swedish data protection authority ('Datainspektionen') announced its decision to fine the NGSC SEK 200,000 (approx. €18,700) for violations of the GDPR, having failed to notify a data breach. The NGSC had taken almost five months for the NGSC to notify the concerned parties and close to three months for the Datainspektionen to receive a data breach notification. Moreover, the NGSC was ordered to introduce internal policies for the documentation of personal data breaches and to ensure compliance with such procedures.

Organizations are required to comply with requirements to comply with data breach notification requirements within the applicable timeframe and in the method specified by applicable law. personal data breach policies and procedures are a must and can fit into the existing framework of data breach response policies.

Unnamed Company (Netherlands): Biometrics

The organization had required its staff to have their fingerprints scanned to record attendance. The Dutch Supervisory Authority (DSA) identified several violations of data protection law, in particular:

i. no evidence that employees explicitly and freely consented to having their fingerprints scanned;

ii. insufficient information provided to employees about how their biometric data would be used;

iii. over-retention of former employees' biometric templates, which were "blocked" in the system but not actually deleted.

The company's use of biometric data was disproportionate to the aim pursued because the security risks were not particularly high in this case. Moreover, less intrusive means could have been used to achieve the company's objectives. Due to the severity of the violation, its "long" duration of ten months, and the "high" number of individuals concerned (337), the DSA decided to impose a significant fine of €725,000. In an effort to reduce the fine, the company asserted that the encryption of the biometric templates and ISO certification of the technology supplier (and its sub-processor) should serve as mitigating factors. The DSA is using its fining model which it announced last year.

Many jurisdictions restrict the use of biometric data by organizations and in some cases may even require approval from

your data protection authority. There is no time like the present for you to assess your current or proposed use of biometrics and conduct a privacy impact assessment to identify and mitigate any data protection risks.

Proximus SA (Belgium): DPO

The Belgian Data Protection Authority has issued its decision to fine Proximus SA (Belgium's largest telecommunications operator) €50,000 for appointing its head of compliance, audit, and risk as its Data Protection Officer According to the DPA, this combination of roles creates a conflict of interest and therefore constitutes an infringement of Article 38(6) of the GDPR.

The decision is intended to be dissuasive for other companies when appointing a data protection officer. If you need assistance in determining whether you require a DPO, please reach out to us.

Amazon Turkey Retail Services Limited (Turkey): Direct Marketing, Transfers and Policies

On 7 May 2020, the Personal Data Protection Authority ("KVKK") published its decision to fine Amazon Turkey Retail Services Limited TRY 1,200,000 (approx. €160,000) for violations of consent requirements, among others. In particular, the decision concerns Amazon's failures to obtain explicit consent from users for the sending of commercial messages for advertising, campaigns, or promotional purposes as required by Law No. 6563 of 2014 on the Regulation of Electronic Commerce.

In addition, Amazon failed to obtain the explicit consent of users for transfers of personal data abroad and made such transfers without an approved written approval from the KVKK, as well as against the requirements of Article 9 of the Law on Protection of Personal Data No.6698.

The KVKK has instructed Amazon to update its personal data

processing processes and its “Privacy Statement,” “Terms of Use and Sales”, and “Cookie Notification” pages to bring them into compliance with the Turkish law.

Like the GDPR, the Law on Protection of Personal Data No. 6698 has specific requirements to be met before personal data can be transferred outside of Turkey. Further, organizations are required to implement the requisite legal notices on their customer-facing websites.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com

President Trump Signs Into Effect a Policy for Space Cybersecurity

March 21, 2021

The days of the commercial space industry revolution have dawned upon us. With corporations like SpaceX and Virgin Galactic leading the charge, humanity’s grasp for the stars is getting tighter and tighter with each week that passes. But as the commercialization of space becomes a more conventional concept and nations begin to scheme for the future of such, there is an abundance of questions that have to be answered in preparation for the voyage of humanity into space – a step that will certainly capture the zeitgeist of the 2000s.

As the technology evolves, the threat of cyberattacks evolves

along with it. In a domain that is primarily ruled by technology and its cyber-infrastructure, a cyberattack on any form of space system could have massive, widespread repercussions. On 4 September, President Trump issued a new set of cybersecurity protocols to defend the United States' space systems; Space Policy Directive-5 ("SPD-5") will foster practices within the government and commercial space operations to ensure the protection of space systems from cyberthreats.

In a statement regarding the issuance and mission of SPD-5, Scott Pace, the deputy assistant to President Trump and executive secretary of the National Space Council, said "Through establishing cybersecurity principles for space systems, Space Policy Directive-5 provides a whole-of-government framework to safeguard space assets and critical infrastructure."

The framework of SPD-5 essentially establishes cybersecurity measures that will be incorporated into all stages of space system development and operations. Although protective software is a major influence, SPD-5 stipulates other vital elements, such as the vetting of anyone who touches command lines for a spacecraft, monitoring ground-based networks for intrusion, and ensuring that telemetry links between a satellite and the ground are thoroughly encrypted. Furthermore, SPD-5 lays out the recognition of the crucial role played by the private sector in the development of space systems, directing the U.S. government agencies to work with commercial space companies to further define the best practices, establish cybersecurity informed norms, and promote improved cybersecurity behaviors throughout the nation's industrial base for space systems.

In recent years, the long-held space dominance of the U.S. has been challenged like never before by nations like Russia and China; the implementation of SPD-5 falls parallel with this narrative. SPD-5 lays out the following cybersecurity

principles for space systems:

- Space systems and their supporting infrastructure, including software, should be developed and operated using risk-based, cybersecurity-informed engineering.
- Space systems operators should develop or integrate cybersecurity plans for space systems that include capabilities to protect against unauthorized access; reduce vulnerabilities of command, control, and telemetry systems; protect against communications jamming and spoofing; protect ground systems from cyberthreats; promote adoption of appropriate cybersecurity hygiene practices, and manage supply chain risks.
- Space system cybersecurity requirements and regulations should leverage widely adopted best practices and norms of behavior.
- Space system owners and operators should collaborate to promote the development of best practices and mitigation approaches.
- Space system operators should make appropriate risk trades when implementing cybersecurity requirements specific to their system.

As the name suggests, SPD-5 is the fifth space policy directive signed by President Trump. SPD-1 officially put the nation on a crewed course back to the moon, SPD-2 eased regulations on commercial spaceflight companies, SPD-3 dealt with space-traffic management and SPD-4 directed the Department of Defense to create the U.S. Space Force.

With the space race once again heating up – this time around making momentous developments faster than ever – the shift of the human race to the cosmos has become more articulate in its actuality.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile: https://waselandwasel.com/about/mahmoud-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com