A Guide to GDPR Compliance

March 21, 2021

The GDPR (General Data Protection Regulation) which came into effect on May 25, 2018, in brief, is a European Union data privacy law that requires organizations to keep data safe, whilst also giving people more control over how their data is used. Compliance with this law requires a coherent review of all processes in an organization followed by the implementation of a comprehensive change plan. In previous contributions, we paid attention to the steps to be taken in order to achieve an acceptable level of compliance through such a change program.

In this article, we will focus on infringements and fines.

In search of guidance on how to define its own data protection strategy and prioritize data protection measures, a company will naturally want to look at its peers and the competent authorities' practice. Apart from the lawfulness of each data processing operation, bolstering data security should remain a board room matter for every organization. Litigation of data protection is set to increase in the near future and organizations that maintain up-to-date security measures will be best prepared for the future and be protected from potential litigation.

This article offers an analysis of the provisions cited to support the imposition of fines on GDPR violators. Based on this analysis, in-house legal advisors may be better able to predict which European Union (EU) member countries may take a leading role in enforcement actions and levying future fines under the GDPR. This article may serve as guidance to organizations doing business in the EU. These findings suggest changes in behavior or business location that could reduce both the likelihood and severity of GDPR fines.

During the first year of enforcement, the Data Protection Authorities (DPAs), the independent bodies charged with investigating and enforcing the GDPR, largely followed the European Commission (EC) guidelines for assessing violations and setting associated fines. The guidelines were developed by the EC European Data Protection Board (EDPB), an independent body charged with the consistent application of data protection rules across the EU, and the 28 EU DPAs.

A total of 15 EU Member States brought enforcement proceedings that resulted in the issuance of an estimated 91 fines. The fines levied to date indicate EU DPAs are acting conservatively, generally imposing fines below the maximum allowable under the regulation. Even for more serious violations of data principles and rights, DPAs generally did not impose the maximum allowable fines. In the first year of enforcement, DPAs tended to issue fines in conjunction with corrective measures in what appears to be an attempt to encourage changes in attitude and behavior concerning the protection of personal data.

Under the GDPR, there are two tiers of fines. The lower, tier-one fines – up to €10 million or 2% of the firm's worldwide annual revenue from the previous financial year, whichever is higher–are applied for less severe infringements. Typically, violations of Articles 8, 11, 25-39, and 42-43 receive tier-one fines. These articles generally address rules governing data collection, control, and processing (i.e., data collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction);

The higher, tier-two fines – up to €20 million or 4% of the firm's worldwide annual revenue from the previous financial year, whichever amount is higher – are applied to more severe infringements. Generally, violations against Articles 5, 6,

75, 9, 12-22, and 44-49 warrant higher fines because these infringements "*go against the very principles of the right to privacy and the right to be forgotten that are at the heart of the GDPR.*"

Germany, Hungary, the Czech Republic, Bulgaria, and Cyprus issued the most fines during the first year of GDPR enforcement. Of these countries, Germany issued more fines than any other EU Member State (about 45), while France issued the highest fine (€50 million against Google). In the coming years, DPAs from Germany, France, the United Kingdom (UK), and Ireland are likely to be among the most influential in terms of calculating and setting fines. The sheer volume of multinational corporations headquartered and/or doing business in these countries suggests the fines issued by these DPAs will be precedent-setting.

Importantly, in late 2015, the European Court of Justice (ECJ) – Europe's highest court – invalidated the US-EU Safe Harbor Agreement between the EC and the U.S. Department of Commerce. The Safe Harbor agreement was succeeded by the Privacy Shield Framework in 2016, which, along with binding corporate rules and standard contract clauses, allowed for the legal transfer of EU residents' personal data from the EU to the United States. However, "*organizations that self-certified under the Privacy Shield are not GDPR compliant simply by virtue of their self-certification and must take additional steps to document their compliance with the GDPR.*" Therefore, an organization that is certified under the Privacy Shield program may not be GDPR compliant and may be exposed to fines and other enforcement actions under the GDPR.

In the future, one country may emerge as the most influential DPA—Ireland. Ireland's Data Protection Commission (DPC) may play an outsized role among all EU DPAs. Ireland is home to approximately a thousand globally recognized U.S. multinational companies across the financial, information, communication, technology, and pharmaceutical industries.

Companies such as Google, Apple, Facebook, PayPal, Microsoft, Yahoo, eBay, AOL, Twitter, all have a presence in Ireland. DPC enforcement actions, therefore, will have an extraterritorial impact on some of the world's most recognized companies and serve as a model for how the GDPR should be enforced by other EU DPAs. As interpreted by more than one U.S. law firm, this expansive view of jurisdiction under the GDPR leads to the conclusion that a firm not located within the EU *"will still be subject to the GDPR if it processes personal data of data subjects who are in the EU where the processing activities are related 'to the offering of goods or services' (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or 'the monitoring of their behavior' (Article 3(2)(b)) as far as their behavior takes place within the EU."*

EU data regulators focused on four GDPR Articles – Articles 5, 6, 15, and 32 – to substantiate the bulk of levied fines. By far the most frequently cited was Article 5 (principles relating to the processing of personal data). The principles of Article 5 include protecting personal data by ensuring appropriate levels of security to reduce the risk of unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures ("*integrity and confidentiality*"). Article 5 also ensures personal data is collected in a limited manner, for a specific, explicit, and legitimate purpose. Article 5 violations were cited an estimated 30 times from among the 91 fines levied. Many regulators from across the EU found Article 5 infringements such as failure to process personal data lawfully, fairly, and in a transparent manner; prevent the use of personal data for new purposes incompatible with the purpose for which the data were initially collected; delete personal data; and, prevent indiscriminate access to an excessive number of user data.

In addition, Article 6 ("*lawfulness of processing*") was the second most often cited infringement with a total of twelve

violations. Under Article 6, lawful processing of personal data requires one (or more) of six factors: (1) obtained consent of the data subject; (2) data processed in the performance of a contract; (3) data processed to comply with a legal obligation of the Member State or EU; (4) data processed to protect vital interests (i.e., interests essential for the life of the data subject or for humanitarian purposes); (5) data processed to perform a task that is in the public interest (e.g., a local government authority using personal data to collect taxes); or (6) data processed where necessary to fulfill legitimate controller (individual or entity that determines the purpose and means of processing personal data, such as a payroll management company) or third-party interests.

Articles 32 (“*security of processing personal data*“) and 15 (“*right of access by the data subject*“) were the third most cited infringements with a total of 7 violations each. Under Article 32, appropriate technical and organizational measures must be implemented to ensure security appropriate to the risk including, but not limited to, the pseudonymization and encryption of personal data. Article 15 provides a right of access whereby the data subject may request information about how personal data is being processed. Data subjects have a right to request a copy of the data being processed, the purpose for processing the data, categories of data being processed (e.g., name, address, phone number), and any third-party recipients of the personal data, among others. Generally, regulators tend to levy fines for failures related to the lawful processing of personal data, including security measures to protect personal data.

A review of the types of infringements and associated fines shows DPAs – at this stage – want to change the perception of data protection, to view data as an asset to be protected. DPAs seek to change attitudes and behaviors via both compliance with the rules and, for egregious infringements,

application of the stick – the fine. One of the EC guiding principles is that fines should "*adequately respond to the nature, gravity and consequences of the breach*" and DPAs should "*identify a corrective measure that is effective, proportionate and dissuasive.*" Neither the guidelines nor Article 83 ("*general conditions for imposing administrative fines*") define what is meant by "*effective, proportionate and dissuasive*" but the guidelines specify that the DPA may consider whether to "*reestablish compliance with the rules or to punish unlawful behavior (or both).*" As a rule, DPAs did not issue maximum allowable fines, but when they did, they tended to follow EC guidelines.

In accordance with the guidance, DPAs tend to apply higher fines when any one or more of four circumstances are present. First, where "*the number of data subjects affected*", and subsequent level of damage, warrants it. For data beaches that are found, for example, that originate from "*systemic breach or lack of adequate routines in place*" and impact a number of data subjects, higher fines might be levied. For example, the Danish DPA issued a €161,000 fine against a Danish taxi company after an investigation found the company stored personal data of approximately nine million customers without a legitimate reason. Here, the number of data subjects impacted warranted a higher fine.

Second, if there are "*several different infringements committed in any one particular case*", the DPA may impose a higher fine and/or prescribe corrective measures. For example, the DPA of France – the Commission Nationale de l'Informatique et des Libertés (CNIL) – characterized Google's data processing as "*massive and intrusive in nature*" and levied a €50 million fine against Google in part for violating multiple articles: lack of transparency (Article 5), insufficient information (Articles 13 and 14), and lack of legal basis (Article 6). Though Google is appealing the decision before France's Supreme Administrative Court, the depth of the fine

was in part substantiated by the breadth of different infringements.

Third, "*intentional acts or negligence triggers the possibility of higher fines*." The guidance specifies, for example, that "*willful conduct on the data controller's part, or failure to take appropriate preventive measures, or inability to put in place the required technical and organizational measures*" weighs into the DPA's assessment of the level of a fine. For example, the Portuguese DPA levied a €400,000 fine against a hospital as a result of failure to protect patient data, allowing hospital staff to indiscriminately access patients' data. The Portuguese DPA substantiated the fine by finding violations of three Articles: Article 5 for allowing indiscriminate access to an excessive number of users, Article 83 for violating basic data processing principles, and Article 32 for failing to ensure "*continued confidentiality, integrity, availability and resilience of treatment systems and services*" and failure to implement "*measures to ensure a level of security adequate to the risk*."

Fourth, the "*duration of an infringement*" is another factor. For example, if data is exfiltrated as a result of a data breach and that data breach goes undetected for a long period of time, the length of time will likely be a factor in determining the damage to data subjects and the resulting fine.

The data supports the conclusion that DPAs largely followed the EC guidelines in assessing and levying fines during the first year of enforcement. Most of the fines were for violations of the aforementioned Articles: 5, 6, 32, and 15. By far the most frequently cited was Article 5 ("*principles relating to the processing of personal data*"); Article 6 ("*lawfulness of processing*") was the second most cited infringement; and, Articles 32 ("*security of processing personal data*") and 15 ("*right of access by the data subject*")

were the third most cited infringement.

Generally, violations against Articles 5, 6, 7, 9, 12-22, and 44-49 warrant higher fines because these infringements "*go against the very principles of the right to privacy and the right to be forgotten that are at the heart of the GDPR.*" However, in the first year of enforcement, fines were generally conservative and did not reach the maximum threshold. As more fines are levied, and some appealed through the courts, the guidelines will need to be updated to reflect current thinking on interpreting the GDPR enforcement provisions. For example, the outcome of the €50 million fine the French CNIL levied against Google will affect how other DPAs assess and apply fines. The outcome also is likely to influence future guidance issued by the EC.

While only 15 EU Member States issued fines during the first year, the increase in DPA budgets and staff suggests many more Member States will be active in the coming years. Addressing data protection complaints, launching investigations, closing cases, and levying fines and/or corrective action are resource-intensive activities. The European Data Protection Board shows France, Germany, Ireland, Italy, Poland, and Spain have the largest staff to support their respective DPAs. While budget and staff are not the only drivers of future GDPR fines, these well-resourced and staffed Member States are likely to be able to process complaints and issue fines more quickly than less-resourced countries. Of these, Ireland's DPC may play an outsized role among all EU because of the number of large U.S. multinational corporations headquartered or doing business there. The breadth of fines issued by Ireland's DPC as well as the depth of investigative supporting evidence could serve as a roadmap for other EU DPA enforcement actions.

In October 2017, the EC issued guidelines for DPAs to use when applying and setting GDPR fines. The guidelines were developed by the EC European Data Protection Board (EDPB), an independent body charged with the consistent application of

data protection rules across the EU, and the 28 EU DPAs. The guidelines include four principles that shape how the DPAs approach assessing fines:

1. Infringement should result in "equivalent sanctions"

This principle encourages DPAs to apply a consistent approach to their "*use of corrective powers*" including the "*application of administrative fines in particular*." The EU Member States want to "*remove the obstacles to flows of personal data within the Union*" by ensuring a standard of data protection across all 28 EU countries. The guidance specifies that while DPAs are independent and may choose corrective measures within their authority in accordance with Article 58, DPAs should avoid different corrective measures, including fines for similar cases.

2. *Administrative fines should be "effective, proportionate and dissuasive"*

Fines should "*adequately respond to the nature, gravity and consequences of the breach*" and DPAs should "*identify a corrective measure that is effective, proportionate and dissuasive*." Neither the guidelines nor Article 83 defines "*effective, proportionate and dissuasive*" but the guidelines specify the DPA may consider whether to "*reestablish compliance with the rules or to punish unlawful behavior (or both).*"

3. Individual assessments should be conducted on each case

The GDPR requires an individual assessment of each case (Article 83). The DPAs are charged with investigating complaints on a case-by-case basis within a reasonable period of time and in an impartial, fair manner. This principle calls on the DPAs to "*use a considered and balanced approach in their use of corrective measures, in order to achieve both an effective and dissuasive as well as a proportionate reaction to the breach*" and "*not to use them in a way which would*

devalue their effectiveness as a tool." The EDPB issues a binding decision if disputes arise between authorities regarding the existence of an infringement.

4. *Administrative fines should be harmonized across EU member country DPAs*

In order to attain consistency, DPAs are directed to cooperate with each other and the EC "*to support formal and informal information exchanges, such as through regular workshops.*" The purpose of the information exchange is to share the methodology used to formulate fines and the practice of applying fines to "*achieve greater consistency*" across the EU.

In addition to the guiding principles, DPAs are required to consider a number of factors under the GDPR when determining the scope and level of a fine. Article 58 details supervisory authority or DPA powers, including the imposition of administrative fines pursuant to Article 83. Article 83 is significant because it directs the DPA to consider many factors when determining the amount of a fine.

The GDPR applies to companies outside the EU because it is extra-territorial in scope. Specifically, the law is designed not so much to regulate businesses as it is to protect the data subjects' rights. A "*data subject*" is any person in the EU, including citizens, residents, and even, perhaps, visitors.

What this means in practice is that if you collect any personal data of people in the EU, you are required to comply with the GDPR. The data could be in the form of email addresses in a marketing list or the IP addresses of those who visit your website.

You may be wondering how the EU will enforce a law in a territory it does not control. The fact is, foreign governments help other countries enforce their laws through mutual assistance treaties and other mechanisms quite

frequently. Article 50 of the GDPR addresses this question directly. So far, the EU's reach has not been tested, but no doubt data protection authorities are exploring their options on a case-by-case basis.

Organizations doing business in the EU (or targeting through their marketing programs EU citizens) are advised to regularly assess their level of compliance with the GDPR. One of the means to do so is the GDPR compliance checklist;

GDPR compliance checklist

- Conduct an information audit for EU personal data

Confirm that your organization needs to comply with the GDPR. First, determine what personal data you process and whether any of it belongs to people in the EU. If you do process such data, determine whether "*the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.*" Recital 23 can help you clarify whether your activities qualify as subject to the GDPR. If you are subject to the GDPR, continue to the next steps.

- Inform your customers why you're processing their data

Consent is only one of the legal basis that can justify your use of other people's personal data. You can find the other "*lawfulness of processing*" justifications in Article 6 of the GDPR. If you choose to process data on the basis of consent, there are extra duties involved. Finally, Article 12 requires you to provide clear and transparent information about your activities to your data subjects. This likely will mean updating your privacy policy.

- Assess your data processing activities and improve protection

A data protection impact assessment will help you understand the risks to the security and privacy of the data you process

and decide ways to mitigate those risks. Next, begin implementing data security practices, such as using end-to-end encryption and organizational safeguards, to limit your exposure to data breaches. When beginning new projects, you must follow the principle of "*data protection by design and by default*."

- Make sure you have a data processing agreement with your vendors

You, as the data controller, will be held partly accountable for your third-party clients if they violate their GDPR obligations. So it's important to have a data processing agreement that establishes the rights and responsibilities of each party. This includes your email vendor, cloud storage provider, and any other subcontractor that handles personal data. You can find a data processing agreement template here.

- Appoint a data protection officer (if necessary)

Many organizations (especially larger ones) are required to designate a data protection officer. The GDPR specifies some of the qualifications, duties, and characteristics of this management-level position.

- Designate a representative in the European Union

Article 27 specifies which non-EU organizations are required to appoint a representative based in one of the EU member states. Recital 80 provides further details about this role.

- Know what to do if there is a data breach

Articles 33 and 34 layout your duties in the event personal data is exposed, whether through a hack or any other kind of data breach. The use of strong encryption can mitigate your exposure to fines and reduce your notification obligations if there's a data breach.

- Comply with cross-border transfer laws (if applicable)

As with previous EU regulations on the transfer of personal data to non-EU countries, Article 45 of the GDPR retains tough requirements for organizations wishing to do so. You may be required to self-certify under the Privacy Shield Framework.

By following these steps, along with the steps in our GDPR compliance checklist, you can help avoid drawing scrutiny from EU regulatory authorities. The information and guidance we can offer vary from technical review to providing several forms and templates.

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

Investment Treaty Arbitration and USD 3 Billion in Taxes

March 21, 2021

In 2007, Vodafone International Holding, a Dutch company, bought 100% of the shares of CGP Investments, a Cayman Island-based company, for USD 11.1 billion for the indirect control of 67% of Hutchison Essar Limited, an Indian company. The Indian tax department determined that the deal was designed to avoid capital gains tax in India, and thus, imposed a tax demand.

However, in 2012, the government's contention was rejected by the Indian Supreme Court. The Supreme Court noted that the Indian tax authorities' demand for capital gains tax "*would*

amount to imposing capital punishment for capital investment since it lacks the authority of law." To prevent the indirect transfers of Indian assets, the government subsequently amended the law to make transfers of this nature taxable in India; this resulted in a new tax demand being placed on Vodafone.

In 2014, Vodafone initiated international arbitration proceedings after an out-of-court settlement with the Indian government failed. The Permanent Court of Arbitration in The Hague ruled in favor of Vodafone. Interestingly, the decision was unanimous with India's own appointed arbitrator – Rodrigo Oreamuno – ruling in favor of Vodafone as well. The tribunal held that any attempt by India to enforce such tax demand would be a violation of India's obligations towards international law.

In August of this year, the International Court of Arbitration ruled that the Indian government – which was seeking USD 3 billion in taxes from Vodafone – was in "*breach of the guarantee of fair and equitable treatment*" which is guaranteed under the bilateral investment protection pact between India and the Netherlands, by using retrospective legislation.

Now, the Indian government is considering its legal options after losing the case regarding the retrospective taxation against Vodafone. The award will potentially be challenged before a court in Singapore in an attempt to limit the damages not only in Vodafone's case but also in a separate lawsuit with Cairn Energy PLC, a United Kingdom company, which could involve much more significant damages.

The British oil and gas explorer, Cairn Energy PLC, began its investments in India during the 1990s; in 2004, the company made its biggest hydrocarbon discovery of the Mangala oil field in the Rajasthan state. This was subsequently followed by discoveries of the Bhagyam and Aishwarya oil fields. So far, Cairn Energy PLC has invested approximately USD 6.15

billion in various projects in India.

In January 2014, Cairn Energy PLC received notice from the Indian tax authorities requesting information related to the reorganization of the company in 2006. The tax department accompanied this notice with details of the near 10% shareholding of Cairn Energy PLC in its former subsidiary, Cairn India, and implemented retrospective tax demands on the company. In 2015, Cairn Energy initiated international arbitration proceedings against the Indian government to challenge the retrospective taxation.

When it comes to the case against Cairn Energy PLC, the Indian government could potentially end up paying USD 1.5 billion – the losses Cairn Energy PLC claims to have incurred from the expropriation of its investments to enforce the retrospective tax demand – should a separate arbitration panel determine that India's tax demands are illegal.

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

ICC Unveils the 2021 Rules of Arbitration: Adding More Gold to the Pot

March 21, 2021

The ICC International Court of Arbitration is without a doubt

the most preferred arbitral institution worldwide. The ICC Rules of Arbitration provide the greatest deference to party autonomy – allowing parties to arbitration the opportunity to select the arbitral tribunal – and offers a high level of flexibility, by implementing any procedural option chosen by the parties that are not incompatible with the core principles of the ICC Rules.

The ICC Rules include rigid provisions aimed at ensuring the arbitrations are conducted efficiently and in the utmost compliance with the fundamental principles of due process. They also establish unique standards of transparency, with the decisional practice of the Court aiming to ensure any conflict disclosures are made in a timely and forthcoming manner. When it comes to drafting awards, the ICC scrutiny process – a unique characteristic of ICC arbitration – offers a careful review of each draft award by the ICC Court with the assistance of the ICC Secretariat – a key component to the structure of the arbitration. This ensures the highest quality of the award by avoiding any possible errors and enhancing the likelihood of the award's enforcement.

With the end of the year closing in and thousands of ICC arbitration's having taken place since 2017 (when the ICC Rules were last amended), the ICC has unveiled the 2021 ICC Rules of Arbitration that are set to take effect on 1 January 2021. These new rules include a multitude of new provisions making arbitration under the ICC even more alluring.

With the unveiling of the 2021 Rules, the President of the ICC Court, Alexis Mourre, stated:

"*The amendments to the Rules… mark a further step towards greater efficiency, flexibility, and transparency of the Rules, making ICC Arbitration even more attractive, both for large, complex arbitrations and for small cases.*"

Joindering Additional Parties

The first amendment to the 2021 ICC Rules is the joindering of additional parties. The ICC has acquired a global reputation for its experience in dealing with complex, high-value, multi-party, and multi-contract arbitrations. A new provision allowing for the joinder of additional parties in the course of arbitration under Article 7(5) of the 2021 Rules, as well as an amendment to Article 10(b) of the 2017 Rules, allows for the consolidation of cases in the presence of different parties which will make the ICC Rules even more suitable to these cases.

Enhanced Transparency

As a result of the introduction of a requirement for the parties to disclose third-party funding arrangements under Article 11(7) of the 2021 Rules, transparency will be further increased. The protection of the integrity of the proceedings will be advanced by the introduction of Article 17(2) which empowers the arbitral tribunal to exclude any new counsel, in the presence of a conflict of interest, from the proceedings; furthermore, Article 12(9) allows the ICC Court to disregard unconscionable arbitration agreements that may pose a risk to the validity of the award.

Investment Treaty Arbitrations

The 2021 Rules include two new provisions to be applied specifically to investment arbitrations based on a treaty. The first – Article 13(6) – aims at ensuring the complete neutrality of the arbitral tribunal in cases involving the public interest, by establishing that no arbitrator shall have the same nationality as that of any of the parties; the second – Article 29(6)(c) – codifies the ICC Court's existing practice that emergency arbitrations are not applicable in investor-State disputes.

Expedited Procedure Provisions

The immensely successful expedited procedure provisions found

under Article 30 and Annex VI of the 2017 Rules have been expanded by the 2021 Rules with respect to their scope of application. The 2021 Rules increase the threshold for the opt-out application from USD 2 million to USD 3 million.

Remote Hearings

If the COVID-19 pandemic has taught us anything, it's that in most circumstances, remote working can be just as efficient as in-person work. The ICC has taken this into account with the 2021 Rules pursuant to Article 26(1) and the introduction of Article 36(3), regarding additional awards, which confirm that arbitral tribunals may – after proper consultation with the parties – decide to hold hearings by remote means of communication.

Conclusion

Ahead of the 2021 Rules coming into force, the ICC Court will be releasing an updated version of its Note to Parties and Arbitral Tribunals on the Conduct of Arbitration, which was last amended in January 2019. The ICC has a series of events planned between now and 1 December 2020, which will mark the culmination of the flagship launch of the Rules.

In the years that have passed, the ICC has been tremendously successful in its arbitration procedures and the ICC Rules are a key factor to that success. With the implementation of the 2021 Rules, one can only imagine how much more efficient and fluid the arbitrations will be.

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

English Translation of The Lebanese Medical Cannabis Law

March 21, 2021

On 20 April 2020, the Lebanese Parliament passed a law permitting the cultivation, trade, research, and use of medical cannabis. W&W has drafted an unofficial English translation of the law:

Click Here to Download

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

Who owns the content that influencers post?

March 21, 2021

Influencer marketing has become one of the most successful trends in marketing over the past few years. In 2018, 81% of marketers reported that using influencers to bolster their marketing plans was an effective strategy. But as the influencer marketing wave becomes increasingly more popular,

the emerging nature of the industry is causing a variety of legal issues; as a result, businesses are being advised to draw up iron-clad contracts with Instagram influencers.

In early 2019, Legacy – a Melbourne café – entered into an influencer agreement with Chole Roberts. Roberts is a fitness influencer with 210,000+ followers on Instagram and can earn a reported USD 1,200 per sponsored post. The owner of the café, Con Katsiogiannis, engaged Roberts for a series of Instagram advertisements, but over the course of their relationship a disagreement broke out over the fees. Katsiogiannis took issue with the posts about his café when they were archived by Roberts. Archived posts are not visible on Instagram; however, the account holder can re-upload them.

Roberts claimed that 90% of the views on her posts occurred within the first week of posting and that archiving posts was a method to prevent a large number of old posts from building up on her page. This belief holds some merit as a recent study found that 49% of consumers expect content on a daily basis from the influencers they follow. There was no written contract between the two parties outlining their business relationship, but rather, a series of verbal agreements, which meant there was no contract specifying how long Roberts would display each post. Roberts argued that she was entitled to be paid for the posts she later hid. This resulted in a dispute over Roberts claiming USD 2,500 that was adjudicated by the Victorian Civil and Administrative Tribunal("VCAT").

The VCAT deputy president reached the conclusion that "in a general sense", Katsogiannis did not lose value when the old posts were archived. However, it was unclear whether the influencer was permitted to delete posts at any time, and pursuantly VCAT ruled that the cafe owner (Katsogiannis) pay the influencer (Roberts) two-thirds of the USD 2,500 that being claimed by Roberts.

Sophie Light-Wilkinson, the VP of marketing EMEA at

Bazaarvoice, voiced her opinion on the matter stating:

"This latest debate asks questions around who owns the content ultimately paid for by advertisers but created by influencers. The simple answer is that these conundrums should be answered by the details of any contracts drawn up between brands and internet personalities. After all, brands need to ensure some rules safeguard their public identity from content that is either too materialistic or misrepresents real-life."

Therefore, if the influencer does delete the posts and the relationship with the entity paying for the sponsorship was not agreed upon contractually, then the influencer is not in breach of any regulations. In Roberts' case, because there was no contract in place, the VCAT ruled that Roberts could archive the posts, however, could not decide who the posts belonged to. With that being said, this brings about the issue of moral rights versus economic rights and leads us into copyright territory.

The concept of moral rights relies on the connection between a person and their creation, as moral rights constitute the right of the creator to protect the integrity and ownership of their work and to maintain the "indestructible creational bond" that exists between their personality and their creation. The term economic rights refer to the exclusive right of the right holder to authorize or prohibit the reproduction, distribution, exportation or importation, or other exploitative activities. Moral rights cannot be relinquished, whereas economic rights can be. Therefore, when an influencer publishes a sponsored post, the moral rights remain with the influencer perpetually, however, if the influencer is paid for the post, they have relinquished their economic rights to the post.

The Berne Convention for the Protection of Literary and Artistic Works is the fundamental body of work for copyright law. As of September 2020, there are 179 nations that are

signatories to the Convention – these signatories have all adopted the text of the convention to create their own respective copyright laws (albeit the application of the law varies from state to state).

In the UAE, moral rights are covered under Article 5 of Federal Law No. 7/2002 (the Copyright law), however, economic rights are not referenced as they fall under contractual obligations which are stipulated under UAE Federal Law No. 5/1985 (the Civil Code).

In the circumstance of influencers in the UAE, the moral and economic rights of the post/content belong to the influencer; if the post is a sponsored post and the influencer gets paid by an entity for publishing the post, the influencer has transferred the economic rights of the post to the said entity upon payment. If there is no agreement in place that outlines the specifications for the post (i.e. the type of post or the length for which the post remains visible on the influencer's account) then the influencer may unilaterally decide what to do with the post.

The influencer and the entity must also take into account that in the UAE, the influencer is required to have an influencer license in order to be permitted to monetize their social presence; if the influencer does not have an influencer license and is subsequently paid by the entity for their posts, they may be fined AED 5,000 by the National Media Council for each post they make without a license, and both the influencer and the entity will be in violation of UAE laws.

Entities seeking the services of influencers must ensure that the influencer has the required licenses – pursuant to UAE laws – that will allow them to advertise their product. For example, if it is an entity that specializes in cosmetics seeking the influencer services, they must ensure that the influencer has obtained prior approval from the Ministry of

Health for the advertising of their products.

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

General Data Protection Regulation – Two years on, are you compliant?

March 21, 2021

The EU General Data Protection Regulation came into effect on 25th May, 2018 ("**GDPR**") and is coined as the most comprehensive changes to data protection around the world in the last 20 years. The GDPR rules apply to almost all private sector processing by organizations in the EU or by organizations outside the EU which target EU residents. The maximum fines for non-compliance are the higher of €20m and 4% of an organization's worldwide turnover.

Many organizations state on their websites and represent to their customers that they are GDPR compliant. But what exactly are the practical steps that organizations need to take to meet these legal requirements of the GDPR?

1. Determine whether your organization is subject to GDPR and needs an EU Representative

The GDPR applies to controllers and processors established in the EU and to non-EU establishments "offering goods or

services” to or “monitoring” the behavior of persons in the EU. Such non-EU controller or processor within the extra-territorial reach of the GDPR must designate a representative in a Member State in which data subjects are being offered goods and services or behavior monitored unless an exception applies.

2. Determine your organization’s Main Establishment

If controllers or processors have establishments in more than one EU Member State, it should determine which of its establishments is the “main establishment” using the criteria set out in the GDPR and assess which Supervisory Authority is the lead Supervisory Authority that will enforce the GDPR in respect of cross border processing.

3. Data Governance and Accountability

Organizations must implement measures to reduce the risk of non-compliance with the requirements of the GDPR and be able to demonstrate that data protection has significant prominence as well as board attention and support. Data protection officers should report directly to the highest management level within the organization. Large organizations should implement a formal data protection program. A Controller must be able to demonstrate compliance with the obligations on a Controller set out in the GDPR (e.g data protection principles or legal basis for processing personal data).

4. Data Processing Inventory or Article 30 Register

Controllers are required to create and maintain a formal, written record of processing activities under its responsibility except where the Controller employs less than 250 persons and the processing is not likely to result in a risk for the rights and freedoms of data subjects, is not occasional, or is not of special categories of data. Processors are required to record all categories of personal data processing activities carried out on behalf of a

controller and to provide a copy to the Controller or a data protection authority on request.

5. Appointing a Data Protection Officer (DPO)

Controllers and Processors must assess whether they are required to appoint a DPO, for example including (a) where its core activities consist of processing operations which require "regular and systematic monitoring" of data subjects on a "large scale"; or (b) where its core activities consist of processing of special categories of data on a "large scale"; or (c) where required under Member State law. The DPO should report to the highest management level of that organization and should be supported by skilled and appropriate resources. The DPO's contact details must be notified to the Supervisory Authority as the first point of contact in relation to data protection matters.

6. Conducting Data Protection Impact Assessments

Controllers are required to conduct data protection impact assessments where a type of processing is likely to result in a high risk to the rights and freedoms of individuals and is required at least in the following cases:

- a systematic and extensive evaluation of the personal aspects of an individual, including profiling;
- processing of sensitive data on a large scale;
- systematic monitoring of public areas on a large scale.

Data Protection Authorities, in consultation with the European Data Protection Board may provide a white list where a DPIA would be required. The controller may consult with the Data Protection Authority prior to commencing the processing activity regarding any residual risks that cannot be mitigated.

7. Privacy Notice

Organizations are required to provide an information notice to data subjects including the source of the data, the legal basis for processing the personal data, the period for which the personal data will be retained, and the third party recipients of the data. The information duty differs where the personal data has been obtained directly from the data subject or from a third party. Unlike privacy policies that previously sat in website footers, the GDPR requires that the notice must be given in a concise, transparent, intelligible and easily accessible form using clear and plain language. Icons may be used. Where presented electronically the information conveyed by the icons must be machine-readable.

8. Subject Access Requests

Controllers are required to comply with subject access requests which include:

1. To information about a Controller’s processing (right to be informed)
2. To restrict the processing of personal data (right to object)
3. To request that personal data held by the Controller is rectified were inaccurate (right of rectification)
4. To have a copy of personal data and information (right of access)
5. To have personal data transmitted to the data subject or another controller in a commonly used machine-readable format (data portability)
6. To require the controller to erase personal data in certain circumstances and where the data has been made public to take reasonable steps to inform controllers that are processing the data that the data subject has requested its erasure of any links to, copies or replication of it (right to be forgotten or right of erasure)
7. To object to automated decision making or profiling

9. Data Breach

Organizations are required to notify Data Protection Authorities within 72 hours and data subjects without undue delay in certain high-risk circumstances. A personal data breach register is also required.

10. Data Processing Agreements

Controllers are required to engage processors who provide sufficient guarantees of compliance with the obligations of the GPDR on a processor and must enter into a data processing agreement meeting the requirements of Article 28.3 of the GDPR.

Is your organization compliant or on the journey towards compliance?

Every organization is unique but there are many milestones that must be achieved before it can say that it is GDPR compliant as part of its data protection compliance program. The fines for non-compliance with GDPR may be up to €20 million, or 4% of the annual worldwide turnover of the preceding financial year, whichever is greater. Is your organization compliant or on the journey towards compliance? If not, create a team led by your legal compliance experts along with HR, commercial, finance, and marketing teams. Implementation of a data protection compliance program will entail more than a simple communication of these concepts to your organization but also the creation of new processes, policies and procedures, training and awareness and ultimately the building of a privacy culture across your business in order to manage data protection risk.

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

Commentary on Lebanon's Medical Cannabis Law

March 21, 2021

On 20 April 2020, the Lebanese Parliament passed a law permitting the cultivation, trade, research, and use of medical cannabis. The law covers an array of topics ranging from the types of licenses available to the prevention of monopolization in the industry. In providing a deeper look at the law, W&W has drafted a commentary on the articles therein.

Article 2: Definition of Terms:

Inter alia, the Article defines "Output", "Import", "Export", "Transport", "Medical Product", and "Pharmaceutical Product".

Each of these definitions utilizes the terms "controlled substance" or "controlled substances". The use of these terms under Lebanese law differs from the usage in the United States under federal law and the drug laws for the majority of the states. For instance, in the United States, the definition of "controlled substance" excludes most hemp or CBD derived from hemp. This is due to the fact that under federal law, certain hemp and CBD derived from it still remains illegal if it is not in complete compliance with various statutory and administrative requirements.

Definition of "International Agreements"

The three treaties mentioned under this definition have been signed by almost all of the nations across the world, including countries in which cannabis is already allowed in

whole or in part. Thus, these treaties are somewhat vague in their implementation. These treaties may be cited by anti-drug groups to stymie the implementation of the law.

Definition of "Law on Drugs"

Depending on specific provisions in the 1998 law, some complications may arise despite the moderate admonition in Article 3 of the law.

Article 4(5) and Article 4(8):

The use of the term "coordination" with "international bodies" may cause complications. Historically, such international bodies have tended to oppose efforts by countries to loosen restrictions on cannabis. We may be seeing a moderation in that opposition, as more jurisdictions permit legal cannabis (medical or otherwise), however, any significant changes will take time.

Article 4(9):

The Article specifies compliance "*with provisions of international treaties*" which could potentially cause the same complications as those mentioned under Article (4)(5) and Article (4)(8).

On 2 December 2020, the United Nations' Commission on Narcotic Drugs removed cannabis from the category of the world's most dangerous drugs. By a vote of 27 to 25, the Commission voted to follow the recommendation of the World Health Organization to remove cannabis and cannabis resin from Schedule IV of the 1961 Convention on Narcotic Drugs, where it had been listed alongside heroin and other highly addictive opioids.

Despite this reclassification, cannabis still remains subject to a high level of international control, however, the development could lead to further loosening of international restrictions on cannabis. Moreover, this downgrading of the

perceived dangers of cannabis may open the field in adding countries for further research and for more recognition of the medical benefits derived from cannabis.

Article 4(18):

Elsewhere, we have seen that the regulations governing testing laboratories can be an obstacle in the growth of successful cannabis programs. For example, the price of required tests, the percentage of product that must be subject to test, the test sample sizes, the number of chemicals that must be tested for, the allowable tolerances for the presence of those chemicals, and many other details related to testing protocols, can greatly delay – and in some circumstances, prevent – cannabis from successfully getting into the market.

Accordingly, when the specifications are developed for lab testing, it will be helpful if the operational philosophy is that the cannabis testing requirements should be no more onerous than the testing mandates for any other commercially cultivated product consumed by man.

Article 16:

The retention of electronic records of "*address[es]*" and the "*details of places and properties*" pursuant to Subsections (1) and (3) are vital, however, there may be safety or security issues if too much of such data is made publicly available. Thus, the Authority may want to keep this in mind, should it choose to publish the data when "*taking into consideration*" the protection of stakeholders under Subsection (4).

Article 18(4):

The definition of "*agricultural cooperatives*" may vary in Lebanon, however, in many states in the United States, they are a special kind of corporation subject to unique laws that may be useful for various agricultural businesses. Depending on the definition in Lebanon, this may be a beneficial option

for some clients.

Conclusion

With the legalization of medical cannabis in Lebanon and the development of the new industry, it is likely that we will see growth in the Lebanese economy in the coming years, as we have seen in the United States and other nations that have taken the same route. In 2019, Colorado – a state with a slightly lower population than Lebanon – collected more than USD 302 million in taxes and fees on medical and recreational marijuana. Sales in the state totaled over USD 1.7 billion. As Lebanon implements the law and opens doors to foreign investors, the nation will potentially see a boom in its economic and business growth.

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

ICC Issues Guidance on Arbitration During COVID-19

March 21, 2021

On 9 April 2020, in light of the COVID-19 pandemic the International Chamber of Commerce ("ICC") assured that the International Court of Arbitration (the "Court") remains operational and continues to progress pending arbitrations and accept new cases, and issued a guidance note on possible measures aimed at mitigating the effects of the COVID-19 pandemic.

The guidance note addresses various issues including mitigating COVID-19 related delays, modification of the procedural timetable or adoption of appropriate procedural measures, guidance on virtual hearings, cyber-protocol, and sample clauses.

Here we outline some of the highlights of the ICC's guidance note.

Mitigating COVID-19 related delays

The guidance note ensures consistency and compliance with Article 22(1) of the ICC Arbitration Rules (the "Rules") which require tribunals to conduct any arbitration in an expeditious and cost-effective manner and Article 25(1) of the Rules which requires tribunals to proceed with as short a time as possible to establish the facts of the case by all appropriate means.

The ICC advocated that the pandemic should not create an unnecessary delay to tribunals' deliberations or draft awards as such can be conducted remotely, with the time-limits for submission of draft awards to the Court as well its policy to reduce arbitrator fees in cases of unjustified delays remain in effect.

Notwithstanding, the ICC will take into consideration specific cases where delays are genuinely attributable to specific COVID-19 caused situations, such as the illness of an arbitrator.

The ICC has also noted that it will be accountable for any hardship faced due to COVID-19 in assessing advances for fees.

Modification of the procedural timetable or adoption of appropriate procedural measures

The guidance note provides a non-exhaustive list of procedural options that parties, counsel, and tribunals may adopt in line with Article 24(3) of the Rules to mitigate potential delays

caused by COVID-19 such as:

- Identifying whether the entirety of the dispute or discrete issues may be resolved on the basis of documents only, with no evidentiary hearing.
- Considering whether site visits or inspections by experts can be replaced by video presentations or joint reports of experts.
- Using either audioconference or videoconference for conferences and hearings where possible and appropriate.
- Considering whether and how the number and size of submissions can be limited.
- Considering whether the parties would agree to opt-in to the ICC Expedited Rules Provisions.

As of 17 March 2020, new requests for arbitration must be filed in electronic format, and the ICC encourages tribunals and parties to conduct the arbitration digitally as is reasonably possible, including the electronic signing of terms of reference, counterparts to an award signed separately and assembled in a single electronic file, and submitting all exhibits in electronic format.

Guidance on virtual hearings

The guidance note clarifies that the language of Article 25(2) of the Rules which requires that a tribunal "shall hear the parties together in person if any of them so requests" should not be misconstrued to permit virtual means of the appearance, but should be read in that it refers to parties having an opportunity for a live, adversarial exchange in person.

However, Section 15 of the guidance note also states that:

"While tribunals have often erred on the side of caution and decided to hold at least one face-to-face hearing on the merits if a party so requires, the COVID-19 pandemic may mean that it is not possible to hold a face-to-face hearing in a reasonable time and that waiting until it becomes possible

would produce unwarranted and even prejudicial delay. Accordingly, a tribunal may, in appropriate circumstances, adopt different approaches as it exercises its authority to establish procedures suitable to the particular circumstances of each arbitration and fulfills its overriding duty to conduct the arbitration in an expeditious and cost-effective manner."

The guidance note encourages parties and tribunals to be appreciative of restrictions on travel, and health and safety concerns, but where the tribunal determines that convening in a single physical location is vital but not currently possible, efforts should be made to reschedule the hearing or convene in a way that mitigates delay.

If it is an absolute necessity to convene in a single physical location, the guidance note advises that specific rules and guidance on the location and appropriate sanitary measures should be put in place to ensure the safety of the participants.

Cyber-protocol and sample clauses

The guidance note emphasizes that virtual hearings require the creation of a cyber-protocol (implementing measures) subject to consultation between the tribunal and the parties. Sample clauses provided for by the guidance note include:

- How parties, counsel, the tribunal, witnesses, expert, transcribers, other participants, and support staff and technicians take part in the virtual hearing including detailing their log-in locations and points of connection.
- Minimum system specifications and technical requirements, and hardware, equipment, and any location-specific requirements, and test runs to ensure connectivity.
- Confidentiality, privacy, and security including no

recording of any part of the hearing and inclusion of support or technical staff or consultants as participants.

- Online etiquette and due process considerations such as muting microphones when not speaking, avoiding the use of equipment that interferes with connectivity, and mechanisms for objections.
- Presentation of evidence and examination of witnesses and experts in a clear and visible manner on screen, coordination towards the connection time and duration for each witness or expert, virtual sequestration of witnesses and experts, permissibility or prohibition of synchronous or asynchronous communications, whether witnesses or experts will be giving testimony whilst alone or with the assistance of anyone on location, and other matters.

The guidance note also emphasizes adherence to data privacy controls and regulations in the application of a cyber-protocol and virtual hearings.

To access the guidance note, click here.

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

Land and Costs for Investing

in Lebanon’s Medical Cannabis Industry under the new Medical Cannabis Law

March 21, 2021

In April of 2020, the Lebanese Government legalized the use of cannabis for medical purposes. In this article, we discuss some of the practical expectations regarding the investment dynamics in the current Lebanese environment and under the new Law.

The currently fertile land in Lebanon for the growth of cannabis is expected to be between 5,000 to 6,000 acres. It is also expected that the landmass for the legal cultivation of cannabis would increase beyond 6,000 acres as the cultivation of medicinal and industrial cannabis expands in Lebanon.

The cost of setting up factories for the manufacturing of cannabis varies from country to country. No factories are currently established and/or operational for the manufacturing of medicinal cannabis in Lebanon, given the fact that the legislation was passed a few months ago and no licenses have yet to be granted by the Authority for Cannabis Cultivation for Medical and Industrial Use (the authority that will be overseeing the industry in Lebanon). However, we can make a distinct comparison with factories that have been newly established in countries that have recently legalized medical and/or recreational marijuana. For instance, a 55,000 square foot laboratory with 24 heat-adjusted production halls in the Canadian province of Québec costs approximately USD 31.6 million. Another plant in Canada, consisting of 14,600 square feet with 11 farming halls that are capable of producing

approximately 4,500 kilograms of cannabis per year, costs approximately USD 12 million.

According to a recent study, Lebanon is expected to make a revenue of USD 1 billion by 2025 from the export of cannabis products for medical use. It is expected that Lebanon will be one of the leading competitors in cannabis cultivation due to the excellence of its land and climate and will perhaps produce the best quality medicinal and industrial cannabis in the near future.

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. The conditions and natural factors of the climate, land, and soil in areas like Baalbek-Hermel are optimal for the production of cannabis and increase the quality significantly. Lebanon will without a doubt be one of the competing countries in cost, production, and quality.

Currently, there are around a dozen pharmaceutical plants in Lebanon. With the passing of Lebanon’s Medical Cannabis Law, some of these plants may be enticed to enter the market for the production of medicinal materials made from the cannabis plant, and other cannabis-related goods. However, as per Article 18(1) of the Lebanese Medical Cannabis Law, these pharmaceutical companies must obtain prior approval from the Ministry of Public Health in order to obtain a license. Similarly, for a farmer/owner/tenant to obtain a license for the cultivation of cannabis, they must abide by the requirements set out in Article 18(5) of the Lebanese Medical Cannabis Law. This Article stipulates that the individual must be a Lebanese natural person residing in Lebanon, who is at least twenty-one years old. Both the farmer/owner/tenet and the pharmaceutical companies must obtain a Good Agriculture and Collection Practices Certificate (“GACP Certificate”) and a Good Storage Practices Certificate (“GSP Certificate”); additionally, the pharmaceutical company will also have to

obtain a Good Manufacturing Practices Certificate (“GMP Certificate”).

Along with the pharmaceutical companies and the Lebanese farmers/owners/tenets, there are four other classes that are eligible for one of the nine licenses that will be made available at the start of 2021. Article 18 of the Lebanese Medical Cannabis Law specifies these other classes like the following: (1) Lebanese industrial companies approved by the Ministry of Industry for the manufacture of fibers for industrial use, oils, extracts, and preparations in which the cannabis is included (i.e., cosmetic products, tires, etc.). (2) Foreign companies specialized in the field of agriculture, industry, storage, export, marketing, or that have a license from the country to which they belong to carry out the operations specified in the license they obtain, and who shall undertake foreign investment into Lebanon through local manufacturing. (3) Agricultural cooperatives duly established in Lebanon, which have the capacity to respond and adapt to the licensing requirements specifically for the agricultural aspect; these cooperatives will also have to obtain a GACP and a GSP Certificate. (4) Recognized research centers, laboratories, and institutes, provided they have the professional and scientific qualifications that require specialization to use the substances under supervision.

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

First Arab Medical Cannabis Law (Lebanon)

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 government began first studying the legalizing of medical cannabis in 2018 where projected government revenue was expected to amount to USD 1 billion per annum.

Lebanon is not the first country in the extended region to legalize cannabis for medical use. Turkey passed laws in 2016 permitting doctors to prescribe certain cannabis-based medicine, and regulated cannabis cultivation in 19 out of its 81 provinces for medical and scientific purposes. In 2019, President Erdogan announced that soon all Turkish provinces should be allowed to cultivate cannabis for industrial use, i.e. for manufacturing textiles, foods, paper, personal care products, plastics, and building materials.

The passing of the law by Lebanon creates an opportunity for leading medical cannabis companies, such as those in the US and Canada, that have globalized their business in the past years.

For example, the legalization of medical cannabis in Germany resulted in substantial market entry to the German local cannabis cultivation market by Canadian companies controlling substantial market share.

In this brief, we focus on the highlights of Lebanon’s recent medical cannabis legislation.

How is cannabis defined?

Cannabis is defined in the law as a controlled plant that has psychoactive properties. It includes the fertilized or unfertilized buds and the seeds of the hemp plant, for medical and industrial use, that contains tetrahydrocannabinol (THC) by a percentage not exceeding 1% of its content and other medicinal materials other than the anesthetic of the cannabinoids in different proportions including the cannabidiol (CBD).

The percentages and contents of the plant are identified pursuant to the methods approved by the Authority.

Cannabis products are defined as every product including fibers for industrial use, and oils, extracts and compounds used for medical and pharmaceutical purposes

Overseeing authority?

The law establishes an authority named the Regulatory Authority for the Cultivation of Cannabis Plants for Medical and Industrial Use (the "Authority").

The Authority is responsible for issuing licenses, and among other things:

- Entering into agreements with public authorities, or private sector entities, whether domestic or foreign, for the execution of the provisions of the law, including for purposes of knowledge transfer.
- Identifying the geographic parameters where cultivation of cannabis may take place, and other details such as soil types, investment, light accessibility, and so on.
- Identifying the permitted percentage of THC and CBD in industrial, medical, pharmaceutical products.
- Overseeing research and development centers, and laboratories, that are renowned and have the professional and academic skillsets for cannabis

cultivation for the permitted uses.

- Establishing rules on production waste and the administrative and security measures to avoid illicit use of waste including that of cannabis stems or any other illicit activity resulting from cannabis cultivation waste management.
- Establishment of central test facilities or contracting with a private sector test facility to ensure compliance with the law.
- Ensuring anti-dumping and anti-trust compliance.

A committee is also established pursuant to the law responsible for the review of licensing applications and compliance with the law and any instructions by the Authority.

Licenses

There are nine licenses that shall be available as follows:

1. License to import seeds and seedlings
2. License to establish a cannabis plantation
3. Cannabis harvesting operations license
4. Manufacturing license
5. Research centers and laboratories license
6. Export license
7. Transport and storage license
8. Sales and distribution license
9. License to import related chemicals

There are six classes of applicants:

1. Foreign companies licensed in their home jurisdiction.
2. Renowned research and development centers, laboratories, and academic institutions.
3. Lebanese companies approved for the manufacture of medicines by the Ministry of Public Health.
4. Lebanese companies approved for industrial activities by

the Ministry of Industry.
5. Lebanese agricultural cooperatives.
6. Lebanese natural persons.

Globally

The law clearly addresses the globalization of medical cannabis trade and industry. In addition to Lebanon, countries that have legalized the medical use of cannabis include Australia, Brazil, Canada, Chile, Colombia, Croatia, Cyprus, Czech Republic, Finland, Germany, Greece, Italy, Jamaica, Luxembourg, North Macedonia, Malta, the Netherlands, New Zealand, Peru, Poland, Portugal, Sri Lanka, Thailand, the United Kingdom, and Uruguay.

In the United States, the use of cannabis for medical purposes is legal over 30 states and the District of Columbia, and although medical use of cannabis has not been legalized at a Federal level, prosecuting individuals acting in accordance with state medical cannabis laws is prohibited.

As for international law governing global medical cannabis trade and industry, Schedule IV of the United Nations' Single Convention on Narcotic Drugs addresses cannabis making it subject to special restrictions. Article 2 of Schedule IV provides as follows:

"A Party shall, if in its opinion the prevailing conditions in its country render it the most appropriate means of protecting the public health and welfare, prohibit the production, manufacture, export and import of, trade in, possession or use of any such drug except for amounts which may be necessary for medical and scientific research only, including clinical trials therewith to be conducted under or subject to the direct supervision and control of the Party."

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