Arbitration in Europe: new rules on third-party litigation funding

November 28, 2022

On September 13, 2022, the European Parliament passed a resolution to propose a directive (the "**Directive**") on the regulation of third-party litigation funding. Although not obvious at first sight, the Directive would also apply to arbitration procedures or other alternative dispute resolution mechanisms.[1]

The European Parliament recognizes that, although third-party litigation funding is "virtually non-existent in Europe, it is a booming phenomenon in investment arbitration that multiplies the number and the volume of claims of private investors against States"[2]. As it expects the practice of third-party litigation funding to expand in Europe—considering how it is already prevalent in the United States and many Commonwealth countries—the European Parliament is concerned about the potential for abuse by litigation funders, should the status quo of a regulatory vacuum be maintained. Indeed, litigation funders may be tempted to put their own economic interest over the interest of claimants and thus assume undue control over the funded proceedings.

Notwithstanding those concerns, the European Parliament notes that third-party litigation funding, if properly regulated, could enhance access to justice for claimants. Hence, the proposed Directive establishes common minimum standards on third-party litigation funding for Member States that wish to permit the practice within their territory.

The Directive mandates the creation of an independent public supervisory authority responsible for overseeing the authorisation of litigation funders and monitoring of their activities. Litigation funders would thus have to demonstrate annually that they possess adequate financial resources to pursue their activities and to observe a fiduciary duty of care[3] towards the claimants they are funding. The supervisory authority of a Member State would also be empowered to investigate complaints regarding litigation funders and to share information with the supervisory authorities of other Member States.

The Directive also sets minimum requirements with regards to third-party funding agreements. For instance, such agreements would have to be written in one of the official languages of the Member State in which the claimant and intended beneficiaries are resident.[4] Also, any agreement that would entitle the litigation funder to a share of over 40% of the total award would, absent exceptional circumstances, be deemed to null and void. Finally, unilateral termination of funding agreements by the litigation funder would also be prohibited.

The Directive further seeks to give courts and arbitral bodies more power by requiring claimants to inform the adjudicational authority of the existence of a third-party funding agreement. Such transparency would allow a tribunal to ensure that litigation funders do not get an unreasonable share of an award, to impose penalties for not respecting the Directive and to hold litigation funders responsible for adverse costs arising from unsuccessful litigation.

It is to be noted that the Directive is still in the proposal stage, and the rules relayed above must go through the European parliamentary process and implementation at the national level by each Member State before becoming law. Nonetheless, such rules go hand in hand with arbitration rules that are already in place on a global scale. Indeed, the International Chamber of Commerce’s Arbitration Rules, the

International Centre for Dispute Resolution's International Arbitration Rules, and most recently the International Centre for Settlement of Investment Disputes' Arbitration Rules, already provide for the obligation to disclose to the tribunal any funding arrangement involving a non-party to a proceeding.[5]

Given the *Comprehensive Economic and Trade Agreement* (CETA) in place between Canada and the European Union, and considering how CETA potentially allows for a degree of investor-state dispute settlement through arbitration, the Directive's solidification into law would provide for an interesting playing field where Canadian and European investors would have an enhanced financial ability to seek compensation.[6]

Author: Martin Aquilina

---

[1] In the Directive, "proceedings" is described as including "any voluntary arbitration procedure or alternative dispute resolution mechanism, through which redress before a court or administrative authority in the Union is sought concerning a dispute" and "court or administrative authority" is described as "a competent court, administrative authority, arbitral body or other body tasked with adjudicating on proceedings, in accordance with national law"

[2] Paragraph F of the recitals of the European Parliament resolution of 13 September 2022.

[3] Although the Directive specifically provides for a "fiduciary duty of care", it is interesting to note that the French text of the Directive uses the term *devoir de loyauté* (duty of loyalty). The ambit of the former is of course much wider than that of the latter.

[4] "intended beneficiary" here means a person who is entitled to receive a share of an award in proceedings and whose

interests in the proceedings are represented by the funded claimant or a qualified entity (meaning an organisation representing consumers' interests (and designated as such under Directive (EU) 2020/1828)) bringing the action as a claimant party on that person's behalf.

[5] See article 11(7) of the ICC Arbitration Rules 2021 and article 14(7) of the ICDR International Arbitration Rules (2021 edition) and Rule 14 of the ICSID Arbitration Rules (July 2022 edition).

[6] CETA entered into force provisionally on September 21, 2017, but its provisions on investor-state dispute settlement only come into force when all EU Member States have completed their ratification process. To date, CETA remains to be ratified by 11 Member States (Belgium, Bulgaria, Cyprus, France, Germany, Greece, Hungary, Ireland, Italy, Poland and Slovenia).

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

Highlights of the recently published ICSID 2022 Annual Report

November 28, 2022

The International Centre for Settlement of Investment Disputes of the World Bank (ICSID) published its 2022 Annual Report on 14 October 2022.

Highlights of the report include:

- 346 cases administered by ICSID, marking the largest number of cases ever administered at ICSID in a single fiscal year.
- A record 77 concluded cases, reflecting ICSID's ongoing efforts to reduce the time of cases.
- Individuals of 42 nationalities were represented amongst the appointments made in the fiscal year. This is the second largest number of different nationalities appointed in a single year at ICSID.
- 45% of first-time appointees in FY2022 were women and 25% involved nationals of low- or middle-income economies.

(https://icsid.worldbank.org/news-and-events/news-releases/icsid-publishes-2022-annual-report)

Other notable report highlights in the Report are as follows:

- ICSID administered **18 cases governed by non-ICSID rules** in FY2022 with the majority (13 cases) applying the arbitration rules of the United Nations Commission on International Trade Law (UNCITRAL). (p. 14 of the Report)
- Distribution of cases registered in FY2022 **by region**:
    - 22%: South America
    - 20%: Eastern Europe and Central Asia
    - 12%: Central America and the Caribbean
    - 12%: Middle East and North Africa
    - 12%: Sub-Saharan Africa
    - 8%: South and East Asia and the Pacific
    - 8&: Western Europe
    - 6%: North America (Canada, Mexico, and the US)

(p. 15 of the Report)

- Basis of **consent to establish jurisdiction** in FY2022:
  - 56%: Bilateral Investment Treaty
  - 13%: Investment Contract between the Investor and the Host-State
  - 11%: Energy Charter Treaty
  - 4%: U.S.-Mexico-Canada Agreement
  - 4%: North American Free Trade Agreement
  - 4%: Investment Law of the Host State
  - 2%: Dominican Republic-United States-Central America Free Trade Agreement
  - 2%: Colombia-El Salvador, Guatemala and Honduras Free Trade Agreement
  - 2%: Central America-Panama Trade Promotion Agreement

(p. 15 of the Report)

- Distribution of cases registered in FY2022 **by economic sector**:
  - 24%: Electric Power and Other Energy
  - 22%: Oil, Gas and Mining
  - 12%: Construction
  - 10%: Information and Communication
  - 8%: Other Industry
  - 8%: Water, Sanitation and Flood Protection
  - 6%: Finance
  - 6%: Transportation

(p. 16 of the Report)

- Top three distribution of cases registered in FY2022 **by country**:
  - Peru: 5
  - Romania: 4
  - Spain: 3

(p. 16 of the Report)

- **91% of hearings or sessions were conducted remotely** in cases administered by ICSID during FY2022 using ICSID audio/video conferencing services. (p. 18 of the Report)
- **77 proceedings concluded in FY2022**: 56 original arbitrations, 20 post-award proceedings, and one conciliation proceeding. (p. 19 of the Report)
- Of the 56 original arbitration proceedings that concluded in FY2022, **27 were settled or otherwise discontinued**, and 29 were decided by the tribunal. (p. 19 of the Report)
- **Outcomes of arbitration proceedings** under the ICSID Convention and Additional Facility in FY2022:
    - 25%: Award upholding claims in part or in full.
    - 23%: Proceeding discontinued at the request of both parties.
    - 14%: Award dismissing all claims.
    - 14%: Proceeding discontinued at the request of one party.
    - 11%: Award declining jurisdiction.
    - 9%: Proceeding discontinued for lack of payment of the required advances.
    - 2%: Settlement agreement embodied in an award at parties' request.
    - 2%: Award deciding that the claims are manifestly without legal merit.

(p. 19 of the Report)

Link to the Report in English: https://icsid.worldbank.org/sites/default/files/publications/ICSID_AR.EN.pdf

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

2022 ICSID Arbitration Rules: Seven key takeaways

November 28, 2022

On 01 July 2022, the 2022 ICSID Rules and Regulations for resolving international investment disputes came into effect.

This is the first amendment to the ICSID Arbitration Rules since 2006 aimed at modernizing the ICSID procedures.

Here we cover seven key takeaways:

- Key steps in ICSID procedures will require **mandated case management** conferences with precise deadlines to make procedures more efficient. Tribunals must convene one or more case management conferences to identify uncontested facts, clarify and narrow the issues in dispute, or address any other procedural or substantive issue related to the resolution of the dispute.
- The Rules now provide for **expedited arbitration** procedures reducing case time in half and permitting a tribunal of one or three arbitrators.
- Any **third-party funding** arrangements must be disclosed to the Secretary-General upon registration of the request for arbitration, or immediately upon concluding a third-party funding arrangement after registration.
- The 2022 ICSID Institution Rules now require that at the request for arbitration filed with the Secretary-General include a description of the investment and of its

ownership and control. Previously, no requirement was in place to describe the **control of the investment**. This creates a new consideration for claimants with complex investment structures.

- Consent to **publish awards, orders, and submissions** is now the default position unless one of the parties expressly objects to such publication within 60 days after the dispatch of the document.
- There is now an express provision governing **security for costs** under Rule 53 of the new ICSID Arbitration Rules which provides a procedural timetable for security for costs applications and the considerations that must be made by the tribunal.
- ICSID has also introduced its **2022 ICSID Mediation Rules** for investment-related disputes and its **2022 ICSID Fact-Finding Rules**.
    - The new Mediation Rules provide for an avenue for parties to resort to mediation under ICSID with or without a prior party agreement.
    - The new Fact-Finding Rules offer parties the option to constitute a committee to inquire into and report on relevant circumstances in the pre-dispute phase and provide an impartial assessment of facts arising in the dispute between the parties.

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

Lebanon Pushes for Activation of Medical Cannabis Law

November 28, 2022

On 20 April 2020, the Lebanese Parliament passed a law permitting the cultivation, trade, research, and use of medical cannabis.

As a result of multiple factors, including the socioeconomic health of the nation, progress on the legalization of the cultivation of cannabis has been stagnant in Lebanon. The law establishes an authority named the Regulatory Authority for the Cultivation of Cannabis Plants for Medical and Industrial Use (the "Authority") which would oversee all cannabis-related operations in Lebanon; however, the Authority has been inactive to date and has yet to approve any applications for the license types provided for in the law.

On 28 October 2021, more than a year and a half after the enactment of the law, the Lebanese Ministry of Agriculture confirmed that the cultivation of cannabis will be implemented in Lebanon very soon. Lebanese Minister of Agriculture, Mr. Abbas Al-Hajj Hassan, stipulated that:

"Today I would like to talk about Lebanon as a whole and the Baalbek-Hermel region and the Bekaa in particular, which is the subject of cannabis and is central and essential today for many reasons; we all know that the law exists and is approved, and therefore we await the executive decrees of the cabinet"

Minister Hassan added that "*Prime Minister Najib Mikati promised good things and has begun communicating with the ministries concerned, so that the law can be implemented.*"

Minister Hassan stated that the cultivation of cannabis in Lebanon will "*save the Lebanese economy and the deprived areas of Kekar and Baalbek-Hermel*", stressing that "*this will have internal and external positives, but the interior positive is the revitalization of the region*". Minister Hassan concluded his remarks by emphasizing that "*the cultivation of cannabis will take us* [Lebanon] *far and will be presented at the international stage as an auxiliary solution on the subject of global health security, and we* [Lebanon] *will be strongly present in the international stage as a country that helps the international community in this context*".

Over the past year, Lebanon has seen some drastic events that have deteriorated the health of the nation. With that being said, there is a strong belief within the nation that the legal cultivation of cannabis will be Lebanon's saving grace. The area currently planted with plants producing hashish – the illegal form of cannabis – in the area of Baabalk-Hermel is estimated at 5,000 dunams (1,200 acres), located within the Bekaa Valley; the production of cannabis in the area, which is equivalent to $10,000 per plant, is the most expensive quality cannabis in the world.

With the legalization and regulation of cultivated cannabis in Lebanon, the nation will seek to take advantage of the prosperous geological factors which make the production of cannabis in Lebanon the cheapest and highest quality cannabis currently available in the international markets.

Author: Abdulla Abuwasel

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

Are Arbitral Awards Truly Confidential: Recent Court Judgment Proves Otherwise

November 28, 2022

Arbitration is a dispute resolution mechanism that enjoys a multitude of benefits and advantages; one of the prime benefits being the confidentiality that befalls the proceedings and the subsequent arbitral awards. This is because parties do not see any upside to the publicity as disputes do not look good. And no one wants the world to know confidential information about how one operates their business, much of which may be disclosed in litigation. Despite the consensus that arbitral awards enjoy the utmost confidentiality, a recent judgment has proven otherwise, leaving individuals and companies scavenging for possible determents that could protect their confidentiality.

FACTS

In early 2021, the United States Court of Appeal for the Third Circuit warned that arbitration might not be as confidential as the parties to disputes probably think it is and want it to be. But in their decision, the Court provided some easy measures to preserve the much-desired confidentiality of arbitration.

The case developed when two insurance companies encountered a dispute. The parties took the matter to arbitration where one of the companies won. Accordingly, the arbitrator issued an

award in favor of that company. It is important to note, a winner in arbitration does not automatically have the legal right to enforce an arbitral award against the loser. Instead, the winner needs to go to court, file the award in court, and ask the court to issue a regular court judgment based on the award. This is often referred to as the "enforcement of the arbitral award". That judgment is just like any other judgment issued by a court. The holder of the judgment, the "judgment creditor," can use it against the loser's bank accounts and other property to claim the amount they have been awarded.

The company that won the arbitration did exactly that. It filed the arbitration award in court and requested the court issue a judgment in order to enforce the contents of the award. Furthermore, the company asked the court to seal the court papers, to preserve the confidentiality of the arbitration award. This is when another insurance company, curious about how the arbitration turned out, filed papers asking the court to unseal the award "*under the common-law right of access*".

The Court ruled in favor of the curious third party asking for the Court to unseal the award, declaring that the filing of the award was a judicial record, and therefore should be open to the public. The court ordered it unsealed and the third party got to see the award and whatever secret information it disclosed.

This demonstrates an inconsistency with the structure of arbitration and puts parties in an awkward position: if the party wants to enforce the award by obtaining a court judgment, the party is faced with the risk of losing the confidentiality which may have been a reason the party opted for arbitration in the first place.

WHY THIS IS SIGNIFICANT TO THE UAE?

Despite the jurisdiction of the case in question being the

United States, individuals and companies in the UAE need to be weary as they could face similar difficulties.

In the UAE, after an award is rendered by an arbitrator, the winning party must submit an application to the local courts requesting the enforcement of the award's contents. Article 48 of UAE Federal Law No. 6 of 2017 on Arbitration states:

"The arbitrators' awards shall be confidential, and they may not be published in whole or in part, unless with the written approval of the Parties. The publication of the judicial judgments which cover the arbitration award shall not be considered a violation of this principle."

Hence, UAE legislation acknowledges that arbitral awards are confidential in principle, however, the publicity of the local courts judgment enforcing the contents of the award do not violate the principle of the awards confidential. Therefore, the details of such award can be made public.

Furthermore, in its ruling for case no. 32/23 issued on 08 June 2003, the UAE Federal Supreme Court stipulated that:

"It is sufficient that the arbitrators' award includes a copy of the arbitration agreement, a summary of the statements and documents of the parties, the grounds on which the award is based, its ruling, date, and location of issuance and the signatures of the arbitrators. The court ratifying such an award must verify the fulfilment of such conditions without broaching the subject matter, except of the dispute matters related to the public order."

Thus, for the local courts in the UAE to enforce the arbitral award, the application must include details of the dispute, which the parties may want to keep confidential. This would arguably mean that third parties could have access to said details by being privy to the court judgment for the enforcement of the award.

PROTECTIVE MEASURES TO MAINTAIN CONFIDENTIALITY

There are a number of measures that a party can take to ensure that an arbitral award issued in their favor maintains its illustrious confidentiality.

The first is setting a time limit for the opposing party to comply with the contents of the award. The party can request that when the arbitrator(s) issue(s) an award, the opposing party has a set number of days in which to comply, or to agree to comply within a short time following its issuance. If the time limit for the opposing party's compliance was in place, then there would be no need to file the award with the court and risk a breach of confidentiality.

As a second protection, the parties might agree that they will direct any arbitrator to issue as short and simple and award as possible – ideally just stipulating the amount that the opposing party must pay. Such an award minimizes any loss of confidentiality, as opposed to a "reasoned" award, in which the arbitrator might explain the basis for the award and, in doing so, go into details that the parties might want to keep private.

Finally, the parties might mix and match, directing the arbitrator to issue two awards. One would require payment of a certain amount and could be the basis for a judgment in that amount, although that judgment would inevitably become a public document. The second award would explain the reasoned basis for the award.

CONCLUSION

In his analytical work on arbitration and the confidentiality that they possess, Francois Dessemontet, a Professor of law at the Universities of Lausanne and Fribourg in Switzerland, stipulated that *"the cloak of confidentiality that surrounds the arbitral proceedings puts the parties, their counsel and the arbitrators in a somewhat awkward position in many*

instances.”

This statement is highlighted by the inconsistency that sometimes befall the arbitral proceedings. However, parties can realign those inconsistencies by putting in place protective measures that maintain the confidentiality of their disputes. Every individual or company that is subject to arbitration proceedings, must keep these measures in mind and implement them prior, throughout, and following the conclusion of the proceedings.

Author: **Abdulla Abuwasel**

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

November 28, 2022

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

Dispute Resolution Analysis in First Double Tax Treaty Between GCC Countries

November 28, 2022

The Double Tax Treaty ("DTT") between the UAE and the KSA provides a significant tax incentive for businesses operating in the two contracting states. A positive impact on investment and trade between the two contracting States is expected in the aftermath of its entry into force. Both contracting countries are members of the BEPS inclusive framework and signed the Multilateral Instrument ("MLI").

The treaty provides for a Mutual Agreement Procedure ("MAP") which can be requested to the competent authority in any of the contracting states within 3 years from the first notification of the action resulting in taxation, not in accordance with the provisions of the Convention.

The dispute resolution provision requires the "Competent Authority" of each respective State to communicate with each other directly (not through diplomatic channels) to resolve complaints filed by persons.

Albeit each State's respective courts may have a domestic perception to certain issues, Articles 31 and 32 of the Vienna Convention have generally permitted domestic courts to account

for such the provisions of treaties and analyze them from a domestic perception.

Unlike dispute resolution provisions under domestic law, as general practice on an international level, Article 25 of the DTT can be triggered by a taxable person before a taxation that the taxable person believes is unjust is charged against him, but as a general matter, that complaint must present that the unjust measure of taxation expected is probable – not just possible.

The question arises with respect to each State's administrative and constitutional litigation avenues; if a competent authority of either state takes a decision that is deemed unconstitutional, can it be challenged before the constitutional circuits of either State? If a person disagrees with a decision, can they challenge it before the administrative circuits of either State? Which ruling would take precedent?

Another item to consider is Article 25(1) which requires notification by the person to occur within three years of the "first notification of the action resulting in taxation not in accordance with the provisions of the Convention". This raises questions as to whether the three-period continues to apply if a domestic litigation process is in play, or whether the period would commence after a final and binding judgment occurs. The effect of a taxable person challenging a matter through domestic proceedings and in parallel triggering the DTT is to be seen.

It has also been noted in general commentaries on the OECD Model Tax Convention of 2014 that criminal penalties imposed by domestic courts or prosecution authorities would not be subject to the procedures of a DTT. As a general practice, the "Competent Authority" would not have jurisdiction to decrease or annul such penalties.

As a solution to these uncertainties between challenges and court proceedings, on 21 November 2017, the OECD approved amendments to the OECD Model which the inclusion of arbitral proceedings into Article 25. Article 25(5) of the 2017 version provides that, in the cases where the competent authorities are unable to reach an agreement under a Mutual Agreement Procedure within two years, the unresolved issues will, at the request of the person who presented the case, be solved through an arbitration process. Whether this mechanism will be adopted is a potential given that these novel regulations are in their early stages.

For the time being, the general consensus is that given the lack of no overarching international tax specific court to provide guidance for the interpretation of DTTs, there is no certain unification of interpretations and courts in each of KSA and the UAE may interpret the DTT in a particular manner if issues under the DTT are brought forth in domestic proceedings.

The MLI is meant to improve the dispute resolution mechanisms when the treaties are covered treaties by the contracting parties. Lastly, as GCC investors become more attuned to intra-GCC treaty applications, and given the rise of investment arbitration in the MENA region, Emirati or Saudi investors could potentially look into challenging unfavorable double taxation decision by triggering investment protection treaties; which usually have more flexible dispute resolution provisions. Moreover, investors may choose to directly resort to investment protection treaty protections as direct access to arbitral proceedings without waiting for a competent authority to issue a decision.

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

A Guide to GDPR Compliance

November 28, 2022

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/

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

Investment Treaty Arbitration and USD 3 Billion in Taxes

November 28, 2022

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/

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

ICC Unveils the 2021 Rules of

Arbitration: Adding More Gold to the Pot

November 28, 2022

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/

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