Arab court qualifies COVID-19 as force majeure event

March 21, 2021

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

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

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

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

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

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

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

In June of 2020, the Court ruled qualifying COVID-19 as a force majeure event as follows:

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

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

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

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

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

civil law jurisdictions.

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

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

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

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

Data Protection Enforcement

March 21, 2021

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

Posti Group Oyj (Finland): Direct Marketing

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

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

Banca Comercială Română SA (Romania): Data Security

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

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

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

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

procedures.

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

Unnamed Company (Netherlands): Biometrics

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

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

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

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

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

Many jurisdictions restrict the use of biometric data by organizations and in some cases may even require approval from your data protection authority. There is no time like the present for you to assess your current or proposed use of biometrics and conduct a privacy impact assessment to identify and mitigate any data protection risks.

Proximus SA (Belgium): DPO

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

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

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

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

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

The KVKK has instructed Amazon to update its personal data processing processes and its "Privacy Statement," "Terms of Use and Sales", and "Cookie Notification" pages to bring them into compliance with the Turkish law.

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

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

Dispute Resolution Analysis in First Double Tax Treaty Between GCC Countries

March 21, 2021

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/

President Trump Signs Into Effect a Policy for Space Cybersecurity

March 21, 2021

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

As the technology evolves, the threat of cyberattacks evolves along with it. In a domain that is primarily ruled by technology and its cyber-infrastructure, a cyberattack on any form of space system could have massive, widespread

repercussions. On 4 September, President Trump issued a new set of cybersecurity protocols to defend the United States' space systems; Space Policy Directive-5 ("SPD-5") will foster practices within the government and commercial space operations to ensure the protection of space systems from cyberthreats.

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

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

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

- Space systems and their supporting infrastructure,

including software, should be developed and operated using risk-based, cybersecurity-informed engineering.

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

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

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

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

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/