IJIEF: International Journal of Islamic Economics and Finance
Vol. 2(1), pg 109-130, July 2019

Should Islamic Banking & Financial Institutions go with General Data Protection Regulation Compliance?

Vijaya Kittu Manda
GITAM Deemed to be University, India, vijaykittu@hotmail.com

Radwan Eskhita
Johanes Gutenberg University Mainz, Germany, Radwanesk@gmail.com

Article History
Received: June 6, 2019 Revised: June 20, 2019 Accepted: July 8, 2019

Abstract

The new European Union (EU) data protection law - General Data Protection Regulation (GDPR)that is enforceable on all entities, within and outside the territory of European Union requires that follow entities dealing with private data of EU individuals should follow due procedures in regard to safe data handling and storage. This regulation is forcing all countries globally, including those in the Islamic countries to take special precautions. Islamic banks and financial institutions are key intermediaries fostering smooth foreign trade between Islamic and European countries. Lack of sufficiently strong data protection legislation in most of the Islamic countries is hampering conformity with GDPR. This leads to non-compliance and thereby paves way to heavy monetary penalties in the short-run and hurts business prospects with the European counties in the long-run, both of which are detrimental. This paper helps institutions in building frameworksby taking them through a series of compliance checks, build teamsto enforce standards, make knowledge repositories and to undertake necessary technical measures. Findings from this study can help Islamic companies in general and Islamic Banking & Financial institutions in particular in meeting GDPR compliance.Finally, this paper makes some key recommendations to the Governments, Regulators, Financial Institutions, Organizations and Individuals so that they can become GDPR complaint.

Keywords: GDPR, GDPR compliance, Data Protection Laws, data privacy

JEL Classification: K20, F41, K41

DOI:
https://doi.org/10.18196/ijief.2117

Web:
http://journal.umy.ac.id/index.php/ijief/article/view/6387

Citation:
Manda, V. K., & Eskhita, R. (2019) Should Islamic Banking & Financial Institutions go with General Data Protection Regulation compliance?. ***International Journal of Islamic Economics and Finance (IJIEF)***, *2*(1), 109-130. Doi: https://doi.org/10.18196/ijief.2117.

Introduction

Individuals leave an information trail as a part of their digital interactions - every time they visit website, use a mobile app or even when simply physically move from one place to another because their laptop or smartphone is constantly online, capturing and disseminating personal and private information. While consented and fair use of this private information is allowed and ethical, dissented and unfair use is not allowed. Though several countries brought legislations restricting such collection and usage, commercial entities are just not stoppable. The "commodification of digital identities" led to the evaluation of a new industry – Data brokers – those who collect, harvest and mine individual personal data using technologies such as Big Data, Cloud storage etc. and optimize data using Artificial Intelligence and Machine Learning algorithms for better targeting by commercial entities.(Parra-Arnau, 2018). Increased digital technology usage leads to increased data volumes and thereby the need to use high-end technology for securely storing personal data in digital format.

While collection of personal data has both good and bad dimensions, increased focus of data privacy has led to a new modern branch of law called the Data Protection Laws (DPLs). So much is its importance that counties across the globe are taking a serious look at bringing legislations to protect individuals from falling into the clutches of entities who can potentially misusing it. Experts say that in this digital age, data is getting polluted and that protecting data is akin to environmental challenges.

The New European regulation called General Data Protection Regulation (GDPR) is one refreshed personal data protection law. It included several provisions in regard to data privacy compliance requirements for organizations and has come into force from May 2018.The legislation has increased the territorial jurisdiction insisting that companies and organizations across the world who deal with private and personal information of any EU citizen be complaint with their regulations. Because modern businesses are globally spread and interconnected, the new regulations forces organizations even outside EU to have to take a tough call –they either stop doing business with European region totally or be complaint with their regulations. The mechanism and the required steps are still in the theoretical books and are not yet well defined for real world implementations because of the short time available for the enforcement date. Added, extending GDPR to cross border regulation has meant that a lot needs to be done to increase awareness because non-compliance will mean hefty fines by violators. Lack of sufficient legislation data protection laws in Islamic counties is the biggest reason why the topic is not sufficiently dealt in earlier research.

GDPR and Banking & Financial Services

GDPR is so far the strictest data compliance requirement and the Banking & Financial Services industry is far from implementing it. A study by (Gartner, 2017) says that 50 percent companies were not fully complaint to GDPR by the May 25, 2018 deadline. Unfortunately, even post-deadline, the compliance levelsare still poor.One in four UK firms are even unaware(LCCI, 2018)and Hiscox says that 40% of UK firms do not understand which organizations will be affected by it. The situation is not much different in the US and Canada either (Miglicco, 2018) or for other countries globally. Non-complaint companies will have to pay heavy penalties if they are not properly handling personally identifiable information (PII) and global corporates such as Google have already paid heavily in fines within the first nine months of the legislation. Countries who do not have data protection laws will lose their abilities to attract foreign investments.

Banking & financial services industry business itself gives extreme high importance to data and cybersecurity. As many as 89 percent institutions put it as the top most priority in the course of their activities(EY, 2018).However, this new regulation compliance increases the necessity beyond normal security that is envisaged so far. Statistics show that financial service, in general, are a little laggard and take three to four years on a average to be complaint as against to the two years global average as seen in other sectors (Bernik, 2018). Adapting to restrictive policies, reducing relationships with third-party vendors but raising expectations from them where ever they are involved etc. can help in GDPR compliance.

Compliance as Future Standards

Institutions need to understand this need to be GDPR complaint is only the beginning and that such compliance requirements will be enforced by other countries going forward. The California Consumer Privacy Act of 2018,for example, comes into effect from 2020. Other countries too will insist on such regulations sooner or later and hence data protection will become a global standard. In fact, the data security compliance is not new and has established global enterprises have already dealt with this topic in the context of Dodd-Frank Wall Street Reform and Consumer Protection Act, HIPPA, FDA or MiFID II earlier albeit with a different data set. Hence institutions should take data security as a necessary requirement. Inclination towards compliance is necessary right from the beginning of systems design. This gives businesses a chance to build an entire compliance framework keeping in mind present and future regulations (Garber, 2018).

Europe and Islamic Banking & Finance

Islamic businesses are well connected with Europe now than ever before. Banks and financial institutions are the vital link and the *de facto* facilitators of smooth money flow between the Islamic and European countries in the course of trade and commerce. Islamic finance aggregate to $2 trillion in 2017 and is expected to raise to $3.5 trillion in 2021 (Thompson Reuters, 2018).Top three countries – Saudi Arabia, Iran and Malaysia make out 50 per cent of the total Islamic finance. The important contributors for Islamic Financial Assets are Islamic banking (71%), Sukuk (17%), Other Islamic Financial Institutions (6%), Islamic Funds (4%) and Takaful (2%). The financial interconnectedness between European and Islamic countries is increasing (Shalhoub, 2017).

Banks with global networks have implemented frameworks for GDPR well in advance to the May 2018 deadline. Asian banks in general and Islamic banks in particular are less prepared towards GDPR compliance and this will lead to loss of business going forward if prolonged. Delay in compliance will mean Islamic banks will be less keen to serve European clients and vice-versa. Islamic Fintech is gaining momentum.

Islamic Country Data Protection Laws & GDPR

Several Islamic countries are proactive in adopting latest technologies, particularly in governmental sectors. The technology investments are in-line with the governments' plans to diversify the region's economy. Smart Dubai, Vision 2030 KSA, e.oman are some examples towards this. With increased technology comes the need for increased security against breaches. There is an increased need to have dedicated regulations for protecting the data that is getting accumulated and increasing every year. Countries like the Kingdom of Bahrain and the State of Qatar made legislation enactments to bring in new data protection laws. UAE still does not have a national data protection law but the UAE Federal law 5/2012 included penalties for violating of privacy. However, the Penal Codes does not yet have a definition of Cybersecurity or privacy crime(Hopps & Paterson, 2018). This, however, does not apply to Dubai International Financial Centre because the DIFC enacted the DIFC Law No. 1 of 2007 that deals with data protection issues within DIFC(Dowle, 2019).Bahrain enacted Law No. 30 of 2018 which regulates personal data protection. This code comes into force from August 1, 2019(Ford N. , 2018).

From the cross-border side, GDPR, with came into force since May 2018, bring new significant changes with in comparing to the old regulations. Its territorial scope extends the application of EU data protection law far

beyond the borders of the EU(Hert & Czerniawski, 2016). When the controller or the processor has no establishment in the EU, the GDPR will apply to the processing of personal data of data subjects who are in the EU, where the processing activities are related to the offering of goods or services to the data subjects in the EU, or to the monitoring of the behavior of those data subjects (Taka, 2017).

UAE being one of the most well-developed countries in the region and a hub for global businesses in the Middle East will soon have to make steps towards GDPR compliance. Global organizations with their establishments or offices in the UAE, for example, will have to complying with GDPR provisions in order to avoid fines, particularly those companies who are processing personal information of EU residents. This is also necessary to bring about a positive perception that from the companies are trustworthy and responsible before their customers(Allam, 2018).

A recent increasing trend of data breaches in the Gulf area unfortunately hampering the make-good feeling. These are happening despite several initiatives being taken both at the Government and private sector levels. Overall, the trend is that Islamic businesses have been working to put in place policies and measures in order to be complied with the new requirements and to avoid the results of non-compliance.

Literature Review

Theory

GDPR is the legislation that specifies how organizations collect, store and protect personal data of European citizens. (Miglicco, 2018) explained in simple terms on how to obtain consent, right to be forgotten, data transfer, offline data protection and security breach notifications. He says that GDPR applications are not well understood and that there is no magic wand to become complaint overnight.A study by (Choi, Jeon, & Kim, 2019) found that the current informed consent model amidst the privacy regulatory framework is ineffective to address privacy concerns and hence a monopolist model is suggested which was then compared between social planner'sand the monopoly firm's optimal data collection policy concerning consumer types and information types.

Increased focus on data security helps change the fundamental way in which data is handled and thereby reduces insider threats. Companies in the UK, German and the EMEA regions are able to reduce insider-based cyber

incidents because employees are more sensitive about handling data, thanks to GDPR (ClearSwift, 2018).

Previous Studies

(Makulilo, 2012), in his doctoral thesis has dealt with the concept of privacy and data protection in the light of international laws including Islamic and Arabic countries. (Malgieri & Custers, 2017) feels that individuals get lured to "free" wifi and discount offers and part with their personal information and that by showing a price tag or worthiness of their personal information online will bring about seriousness in them. (Prince, 2017) suggested privacy controls encouraging user control of private data flow. (Natamiharja, 2018) discussed about 2018 data breach at Facebook of Indonesian citizens personal data and suggested the need for short-term and long-term actions that both citizens and the Government need to take up. It also suggested the appointment of a Privacy Commissioner to handle such instances. Malaysian bank employees are aware of policy towards protecting customer data but they tend to ignore practical implementation of such policies and thereby give opportunity to data theft and fraud, according to findings by (Abidin & Nawawi, 2019).

According to the statement of the Article 29, an international agreements as general rule for law enforcement in third countries has been founded as suggested solution to apply GDPR as cross boarder regulation (request access or disclosure from EU data controllers (working party 2017). The organizations must consider implementing international standards to minimize data privacy risks, they still need to grip with the GDPR to fulfill its requirements. They must handle the data for EU citizens according to the principles of the GDPR, because the risk for breach of data is high(Ford N. , 2018). The companies in Islamic countries could start the road of GDPR compliance through implementing five capabilities: Locate, Search, Minimize, Protect and monitor (Karam, 2017).

Research Gap

Although few researchers have addressed the problem of applying the GDPR as cross boarder regulation outside EU, available literature fails to address the situation and the requirements of applying GDPR in Islamic countries in general and Islamic banking & financial institutions in particular, as it is uncertain how to enforce the GDPR in the light of national laws.

Further, the authors could not find enough research work on the availability of frameworks or methods for the practical implementation or in the light of technicalities. Hence, there clear exists a research gap that this paper intends to bridge.

Research Methodology

Exploratory research methodology is used for the purpose of this research owing to the still evolving concept of data privacy. Only secondary data obtained from reputed authentic publicly accessible and available sources such as journals, websites, books, legislation documents etc. are being used.

Results

Statistics & Situation Description

Several papers have statistically showed the consequences and damage caused by the data misuse. Corporate resources in the UAE alone have an estimated loss of about AED 3.27 trillion by 2020. Therefore, companies must change their strategy and culture around information management. Additionally, lack of technology makes the process of GDPR compliance more complicated. According to recent research from the 2017 Veritas GDPR report, globally, about 47 percent of companies won't meet GDPR requirements. The biggest challenge for most corporates is understanding what data resides in their complex IT environments, how to manage the process of protecting the data, automating the process of deleting the data from the network when requested or when it is no longer needed. According to Veritas research, 32 percent of organizations globally have not enough level of technology to be compliant with GDPR(Karam, 2017).

Rapid growth in digitalization increases the importance and need for newer strategies in dealing with the data. The recently announced digitalization projects such as Smart Dubai and Saudi Arabia's National Transformation Plan 2020 (NTP) opens the door for increasing the usage of region's digital capabilities, adding up to the smart infrastructure such as networked devices and high level of internet and mobile penetration. As much as 76% of GCC population are internet users. Cities such as Dubai position itself among the world's first smart cities using wide ranging smart technology. Surveys showed that as many as 68% of GCC companies have invested 5% of their revenues in digital transformation in 2018. These include investments made in latest technologies such as Cloud computing, Internet of Things (IoT), Business Intelligence (BI), Robotics etc. This transformation also raises the

need for rapid movement on the legal side to make a regional and international cooperation such as, for example, by building a co-operated framework, by which data protection can be implemented on a massive scale through these new digital projects(Vilnius University, 2017). Companies that use Big Data should keep in mind of privacy, autonomy, transparency and nondiscrimination when handling data.

Adequacy

Currently, very few countries were classified as save countries according to the decision of European Commission (Adequacy decisions, 2019). None of the GCC countries are included in this list so far. Therefore, the compliance task is harder is harder for the Islamic countries according to Art. 44, 45 GDPR which restrict Cross-Border Data Transfers to a recipient in a third country unless it receives an Adequacy Decision from the Commission (Gabel, 2019). The recommended exception is to follow what is commonly known as Safeguard, which requires appropriate level of data security and enforceable data subject rights in the target country.

In general, there are three main protective measures to gain approval for transferring the data outside EU to countries without classified level of adequate. Some popular protective measures are Standard Contractual Clauses, Binding Corporate Rules and Certification for the privacy shield (Cave, 2018).

A major problem is in the case of further transferring data to non-EU country or corporate (onward transfer). This situation can happen often according the high level of cooperation between Islamic and other eastern Asian countries which are the source of personnel for regions like GCC. In such a case, a recommended module can be used to secure the compliant with the GDPR in the case of multi transfer of data outside EU. The module recommends that data transfer from a controller in EU to controller in non-EU country must be governed by agreement includes the same obligations of the original contractual clauses between EU and non-EU controllers (Bryan Cave, 2018). Another method for onward transfer is to enforce the controller in non-EU country (B) to consult the original controller in EU (A) and to let him entitle the data directly to the target controller (C) using the same contractual clauses, see following figure.

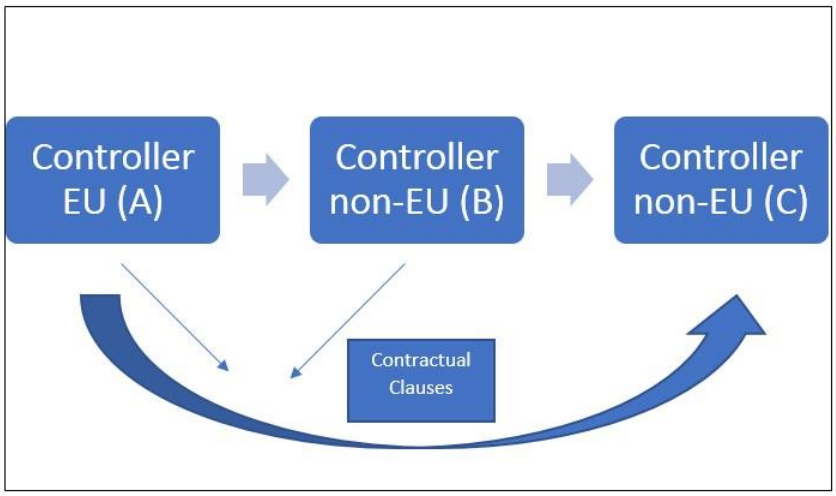

Figure 1. Onward Transfer

Source: Author

GDPR Compliance Principles

All businesses that store, and process data of EU citizens will get applicable to the territorial scope of GDPR and thereby the need to be GDPR compliant. They must review their processes, IT systems and internal controls to ensure of compliance. In addition, they must conduct data risk impact assessments for every time they are dealing with personal data as collecting, storing, processing or controlling.

The Key points from the Article 5 of the GDPR, in regard to data protection law are:

- Process the data in fair and transparent way.
- Collect the data just as far as the purpose requires, applying the concept of data minimization.
- Accurate and limited to the date, which the data still required, make the concept of right of deleting applicable.
- Process the data in secure and confidential way according to the concept of appropriate technical and organizational measures required by the GDPR (Ford R. , 2018).

GDPR Compliance Checks

Islamic countries that works with EU or processing the data of EU citizens will now have to take a tough call - to be or not to be complaint with GDPR. It will be a costly mistake to ignore thinking about GDPR (Perry, 2019). Compliance requires that a complete legal framework with each stepin the data processing to be a formal defined in the framework. This applies to

each firm or personal data processer who want to be compliant with GDPR and be still able to deal with the data of European citizens and avoiding the fines of GDPR (IT Governance, 2018).

These steps are suggested to be followed in manner and order below:

a) Main Check
    1. To check if the territorial scope of GDPR touch his business activity
        a. Offering services or good in EU
        b. Monitoring behavior of EU residents
        c. Your business has establishment in EU
    2. Appointing data officer to manger the processing of personal data
    3. Adding the evaluation of compatibility with GDPR in general and local data protection law specifically in the incorporated process inside the corporate
b) Internal check
    1. Identifying the points subject to GDPR
    2. Identifying the territories and the applicable jurisdictions in addition to specify the involved part of business
c) Data check
    1. To check the process of data flow
    2. Identifying the amount and relationship of the data
d) Technical check
    1. To evaluate the system where the data is stored
    2. check system vulnerabilities
e) Violation check
    1. Check the conflicts with the local data protection law
    2. Check the conflicts with the GDPR(Hayes & Curran, 2017)

Compliance as Knowledge

Compliance check could be more systematically be defining in advance. These steps could be applicable for most of the companies or organizations as prerequisites steps on the road of GDPR compliance. Further, these steps must be part of the team knowledge and are to be considered in each data processing stage. The following diagram illustrates the required points of knowledge:

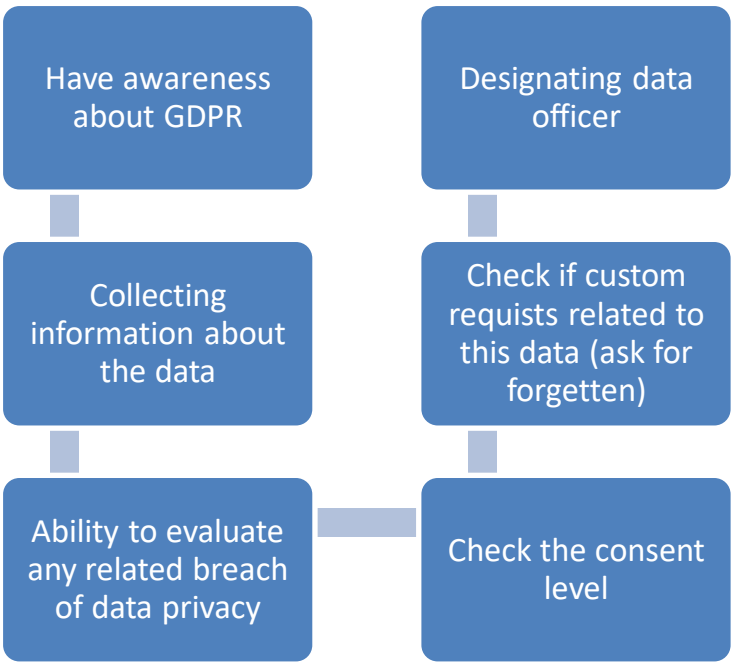

Figure 2. GDPR Compliance Steps
Source: Author

Essentially, the team must possess:

a. Awareness about the scopes of GDPR and its cross-border application.
b. Through data collection, it must be able to identify, if the data has special characteristics (sensitive, related to health, race…) in order to sort it and apply the right legal procedures to it.
c. Enough knowledge about the types of breaches and the required procedures in case of incidents.
d. Ability to determine the level of consent and the related level of data processing, in addition to proper knowledge about cases which not requires a consent to process the data.
e. To understand the related custom rights on the data like the right of be forgotten, the right to be informed, the right of access, the right to rectification or the right to data portability.

An essential point in this context is that transferring the EU resident's personal data outside EU boundaries should only be done under specific conditions. The easiest way is to transfer to a country with an adequacy decision, or in other words, to a country which is listed by European commission as a country with an adequate level of protection essentially equivalent to that ensured within the EU according to Art. 45 GDPR(Myers, 2017). The second way is to transfer the data to a country without adequacy decision under specific conditions listed in Art. 46-47-48 GDPR.

If none of Islamic countries have the compliance, at least currently, the country should at least be listed with adequacy decision and the evaluation of the data transfer and processing in Islamic countries must be done under the condition of cross-border data transfer in GDPR.

Technical Compliance

Data is the "new oil" of the digital economy. Much of the data processing these days is through electronic means. GDPR is aware of this and hence been definedin the main principles for getting compliant status. It is mentioned under the common principal "Technical and Organizational Measures".

It will be a hard task to check individually if the proper technical and organizational is available to process the data of EU residents or to be compliant according to the art. 32 GDPR in other words.

In order to guarantee the basic level of technical security as demanded by GDPR, the following points are suggested:

a. To apply SSL on all data transferring
b. To implement firewall technology between intern network and the Internet
c. To enable multi authentication systems for all kind of login to the personal data
d. To prevent any storing of data outside the protected network, unless it is sufficiently encrypted
e. To implement a system capable of deleting or amending the data upon the request of the data subject within the legal deadline

Implementing some common standards in the field of data security and IT system protection can help in gaining the required level of compliance with GDPR, at least from the technical side firstly. ISO 27000, ISO 27001 and BS-10012 "Information Governance" are some topics related to those certifications. Because most international organizations are still coming to grips with the GDPR, it is high time that organizations and businesses to implement policies and procedures to safeguard all the data and information, as the reputational risk for loss or breach of data is high (Ford R. , 2018).

New Laws on The Road of GDPR

Countries like Brazil, Australia, USA, Japan, South Korea and Thailand already have GDPR-like or even stronger legislations already in place. So, the task of becoming complaint is only difficult if not impossible. Islamic countries mentioned in three data sets are best placed in order to be complaint quickly:

a) Digitally competitive countries would be best placed towards quicker data protection compliance because their knowledge, technology and future readiness would be high(IMD, 2018).
b) Counties having good score according to the Global Competitiveness Index 4.0 from World Economic Forum(WEF, 2018).
c) Counties mentioned in the Islamic Finance Development Report 2018 that covered over 1000+ institutions from 131 Islamic countries (Thompson Reuters, 2018)

Table 1. Digital Competitiveness Rankings 2018 of select Islamic countries

Country	Overall Rank	Factors		
		Knowledge	Technology	Future Readiness
Saudi Arabia	42	40	50	38
Jordan	45	56	48	41
Malaysia	27	17	22	29
UAE	17	36	7	12
Indonesia	62	61	59	62
Kazakhstan	38	35	39	40
Qatar	28	37	27	16
Turkey	52	59	45	42

Source: IMD World Digital Competitiveness Ranking 2018

Table 2.Global Competitiveness Index 4.0 of select Islamic countries

Country	Rank	Score	Country	Rank	Score
Albania	76	58.1	Malaysia	25	74.4
Algeria	92	53.8	Mali	125	43.6
Azerbaijan	69	60	Mauritania	131	40.8
Bahrain	50	63.6	Morocco	75	58.5
Bangladesh	103	52.1	Nigeria	115	47.5
Bosnia & Herzegovina	91	52.2	Oman	47	64.4
Brunei	62	61.4	Pakistan	107	51.1
Burkina Faso	124	43.9	Qatar	30	71
Chad	140	35.5	Saudi Arabia	39	67.5
Egypt	94	53.6	Senegal	113	49
Guinea	126	43.2	Sierra Leone	134	38.8
Indonesia	45	64.9	Tajikistan	102	52.2
Iran	89	54.9	Tunisia	87	55.6
Jordan	73	59.3	Turkey	61	61.6
Kazakhstan	59	61.9	UAE	27	73.4
Kuwait	54	62.1	Yemen	139	36.
Lebanon	80	57.7			

Source: World Economic Forum, 2018

Table 3.The Most Developed Islamic Finance Markets

2018 Rank	Country	2016IFDI Value	2018 IFDI Value
1	Malaysia	123	132
2	Bahrain	87	74
3	UAE	66	71
4	Pakistan	46	59
5	Saudi Arabia	47	56
6	Jordan	42	53
7	Oman	53	52
8	Kuwait	45	51
9	Brunei	23	50
10	Indonesia	28	50

Source: Islamic Finance Development Report 2018

1. United Arab Emirates

GCC states have recently started building new regulations and laws encompassing the basics of GDPR. The new UAE Health Data Protection Law has been published under the name of Federal Law No 2 of 2019 concerning the Use of the Information and Communication Technology in the Areas of Health, it regulates the processing of electronic health data originating in the UAE, the data includes the patient names, consultation, diagnosis, and treatment data, medical scan images and lab results. The law applies to all entities operating in the UAE and the Free Zones that provide healthcare,

health insurance, healthcare IT and other directly/indirectly related services. The law introduces common data protection concepts representing in purpose limitation, accuracy, security measures and consent to disclosure. The violation fine is up to AED 1 million (Lsgar, n.d.).

The Law is published in the Federal Gazette on 14 February 2019 and will come into force three months from publication data. It includes many points showings how it was enacted depending on the modern data protection laws and GDPR formation, two important points to note are:

- Transferring the health data outside UAE is principally prohibited, the exception must be issued by the health authority.
- Like purpose limitation except with the prior consent of the patient
- Security measures to ensure that the health data are protected sufficiently from unauthorized processing, damage or amendment
- Patient consent to ensure not to disclose patient data to any third party without the prior consent of the patient(Janssens, 2019).

2. Qatar Data Protection Law

Law No. (13) of 2016 is the modern personal Data protection law. It consists of 30 articles and included many compliance regulations that tend to make it similar in many points with the regulations of GDPR. Consent as main principle is included as prerequisite for using the personal data by an organization, the consent of the data subject is necessary to achieve a legitimate purpose(DLA Piper, 2019).

The similarity between Qatari Law and GDPR represented in many points, some of them are:

1. Informing the individuals, who his data are processing, including the identity of the data controller and the purpose of processing.
2. Protecting the data using appropriate measures.
3. Keep personal data as long as the purpose of processing and the consent is allowed.
4. Applying effective tools to protect data from loss, damage, alteration or unlawfully access.
5. Data breach notification, where the organizations that suffer a data breach that would cause possible harm for the individuals concerned must notify the ministry of communication in addition to the data subjects affected(Biscoe, 2019).

3. Indonesia

The draft Personal Data Protection Bill of 2015 is a step towards addressing the data protection needs in Indonesia.The Minister of Communication and Informatics Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic Systems (MOCI Regulation 20) deals with how Electronic System Providers (ESPs) have to deal with personal data. Consent and processing personal data are given highest importance. Small and Medium Enterprises (SMEs) form the bulk of businesses in Indonesia and hence compliance cost will be too high. Government need to hand-hold and provide assistance in the form of capacity building.

4. Saudi Arabia

Shari'a is the principles of laws in Saudi Arabia. It is mainly derived from the Holy Quran and Sunnah. The Holy Quran and the Sunnah do not give a penalty for disclosure of secrets; but some dangerous disclosure may be punishable according to the discretion of the judge. Also, any exporting of the personal data required the consent of the data subject according to Sharia principle. Penalty may include a fine or even imprisonment.

Currently the protection of personal data is covered through some related legislation issued by Shura Council. In case where personal data is related to specific sectors, like banking and finance corporations, the applied regulation will be managed through Saudi Arabian Monetary Authority who take the responsibility to issue the required regulations regarding saving the data of bank customers and similar investment or finance corporations.

5. Bahrain

Bahrain advanced in the field of data protection laws with its enactment of Law No. 30 of 2018 as National Personal Data Protection Law. The PDPL came into force from 1 August 2019. It has many points of similarity to GDPR, where it provides the individuals with rights to decide about their personal data, how to collect, process and store. The new law also paved the way for the creation of an authority, which can issue orders against any violations. PDPL imposed even criminal penalties for violations of certain provisions.

Businesses that have already gained a data protection compliance under the GDPR may be also compatible with the PDPL; however not every compatible business with the GDPR is guaranteed to have compliance with the PDPL. An important example the differences between PDPL and GDPR is the fines and penalties, the risk of criminal penalties is not found in the GDPR.

For the investment and banking corporations, they may need to determine if their activities fall within the definitions of personal data. If they do, then the collected data must be sorted to determine if it contains sensitive personal data to be processed in appropriate manner, including notifying the Authority of their processing activities according to Art. 9 PDPL. In general, PDPL help to build secure and stable investment market in Bahrain and guide to better compatibility with GDPR according to the DLA Piper's Middle East study in September 2018.

6. Malaysia

There are several data breaches in Malaysia in the past. Trade between Malaysia is increasing and is at RM 15.46 billion of which RM 8.61 billion is in the form of exports. Thus, trade activities of Malaysian companies will get effected if they do not go for GDPR compliance. The Malaysia Personal Data Protection Act 2010 applies domestically and not outside Malaysia.The Communications and Multimedia Ministry has proposed amendments which will necessitate large-scale business process alterations.

Conclusion and Recommendations

Findings

The major findings from our research work are as follows:

1. GDPR compliance must be done through enforcing prerequisites for any company deals with the data of EU residents.
2. A series of checks are suggested to secure a good initial level of compliance. These checks are still in the basic level but can be developed to include more detailed and comprehensive checks according to the need of the region and the enforced laws.
3. Technical requirements are very crucial for the compliance of GDPR and similar regulations. The firms and organizations must give more attention to this field to assure better and secure level of data processing and to be more eligible for compliancy.
4. Adopting compliance certifications can be helpful to reach the required level of compliance through predefined steps according to the certification requirements, currently ISO 27000, ISO 27001 are recommended example of such certificate, more of them will be developed in the next period according to the need of the market.

5. The new enacted national laws must follow the international laws and it considered a recommended way to make the compliance with GDPR easier.
6. A regulation at the region level will be more effective and easier to be managed, a real example is GDPR, it is EU level regulation makes the application of it easier than enacting each of the 28 country its own regulation.

Conclusions

GDPR leads the new era of legislations starting from enacting new level of laws like communication law, health data protection law and many other laws. The enforcement in cross-border form also related to the new trend of laws, which try to protect the residents of its countries inside and outside the country boundaries as long as the right of its residents has been breached. Countries in Middle East especially suffer from high number of attacks and data breaches, according to Gartner Summit, Organizations in the Middle East take more time on average to identify and contain a data breach – 260 days compared with Europe's average of 138 day (Sharma, 2018).

We conclude that GDPR compliance is a crucial factor for Islamic firms and organizations who wish to stay in the market and continue their business with their European counterparts. Malaysia, UAE, Qatar and Bahrain are leading now through enacting partially or nationally new modern and compatible data protection laws. Applying obligatory checks for processing the data in the firms to raise the level of compliancy in general. This paper suggests the need to build frameworks to build awareness about GDPR compliancy about care to be taken when handling data.

Recommendations

Islamic Financial Institutions should increase technology spending and setup dedicated teams to build frameworks for handling personal data, create and train employees, ensure careful handling of data and for dissemination of breaches if any.

At the national level, Governments of all Islamic countries have an urgent need for the enactment of new legislations that specifically award punishment for data breach and to ensure better security. Leading innovative countries such as Malaysia, UAE, Qatar and Bahrain have starting to build the awareness of this situation and are already on road towards global legal trends. Governments from other countries should give priority in

bringing about legislations in the wake of newer international data protection laws.

Regulators should be given quasi-judicial powers to penalize violators of rules and regulations in regard to failure to comply with the national data protection laws.

Academicians can use this opportunity to study legislation across all Islamic countries and evaluate the pros and cons that might exist between them. Another area of study is to evaluate possible imbalances that might be formed because of shift in business from one country to another depending on the compliance levels.

References

Abidin, M., & Nawawi, A. (2019). Customer data security and theft: a Malaysian organization's experience. *Information & Computer Security*. doi:10.1108/ICS-04-2018-0043

Adequacy decisions. (2019). *Adequacy decisions*. Retrieved April 7, 2019, from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

Allam, Y. (2018). *The impact of the GDPR on organisations in the UAE*. Retrieved from https://www.itgovernancegulf.com/blog/the-impact-of-the-gdpr-on-organisations-in-the-uae

Bernik, J. (2018, April 12). *Financial Services and GDPR: What 200 Professionals Told Us About Their Data Protection*. Retrieved from Mcafee: https://securingtomorrow.mcafee.com/business/financial-services-gdpr-200-professionals-told-us-data-protection/

Biscoe, C. (2019). *Qatar's Data Privacy Law*. Retrieved from https://www.itgovernancegulf.com/blog/qatars-data-privacy-law-what-gcc-organisations-need-to-know

Cave, B. (2018). *CNIL Module: Complying with the EU GDPR.*

Choi, J., Jeon, D.-S., & Kim, B.-C. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics*, 113-124. doi:10.1016/j.jpubeco.2019.02.001

ClearSwift. (2018). *GDPR and the Insider Threat: How new regulations are changing our data handling habits.* ClearSwift. Retrieved from https://www.clearswift.com/blog/2018/07/30/gdpr-and-insider-threat-how-new-regulations-are-changing-our-data-handling-habits

DLA Piper. (2019). *Data Protection Laws of the World*. Retrieved from DLA Piper Data Protection: http://www.dlapiperdataprotection.com

Dowle, C. (2019). *Data protection in Dubai International Financial Centre (DIFC): Overview*. Retrieved from https://uk.practicallaw.thomsonreuters.com/8-635-5552?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1

EY. (2018). *Global banking outlook 2018*. Retrieved from EY: https://www.ey.com/Publication/vwLUAssets/ey-global-banking-outlook-2018/$File/ey-global-banking-outlook-2018.pdf

Ford, N. (2018). *Data protection law in the Gulf vs the EU*. Retrieved from IT Governance Gulf: https://www.itgovernancegulf.com/blog/data-protection-law-in-the-gulf-vs-the-eu

Ford, R. (2018). *The impacts of the GDPR on Corporate Governance practices in the GCC.* LexsisNexsis. Retrieved from https://www.lexis.ae/wp-content/uploads/2018/06/GDPR-Corporate-Governance-GCC-Lexis-Nexis-ME-edit-final.pdf

Gabel, D. (2019). *Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation.* WhiteCase.

Garber, J. (2018). *GDPR – compliance nightmare or business opportunity?* Computer Fraud & Security. Retrieved from

https://www.sciencedirect.com/science/article/pii/S1361372318300551

Gartner. (2017, May 13). *Gartner Says Organizations Are Unprepared for the 2018 European Data Protection Regulation*. Retrieved from Gartner.com: https://www.gartner.com/en/newsroom/press-releases/2017-05-03-gartner-says-organizations-are-unprepared-for-the-2018-european-data-protection-regulation

Hayes, M., & Curran. (2017). *Getting Ready for the General Data Protection Regulation.*

Hert, P., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law, 6*(3), 230–243. doi:https://doi.org/10.1093/idpl/ipw008

Hopps, & Paterson, S. (2018). *Cyber Security United Arab Emirates - Herbert Smith Freehills*. Retrieved from IT Governance: https://www.itgovernancegulf.com/eu-general-data-protection-regulation-gdpr

IMD. (2018). *IMD World Digital Competitiveness Ranking 2018.* IMD World Competitiveness Centre. Retrieved from https://www.imd.org/globalassets/wcc/docs/imd_world_digital_competitiveness_ranking_2018.pdf

IT Governance. (2018). Retrieved from https://www.itgovernancegulf.com/eu-general-data-protection-regulation-gdpr

Janssens, E. (2019). *UAE Issues Law to Protect Health Data and Restrict Its Transfer Outside The Country*. Retrieved from https://www.bakermckenzie.com/en/insight/publications/2019/03/uae-issues-law

Karam, J. (2017). *Is the GCC ready for GDPR?* Retrieved from https://www.commsmea.com/17510-is-the-gcc-ready-for-gdpr

LCCI. (2018). *One in four London businesses unaware of new data protection regulation.* London Chamber of Commerce and Industry. Retrieved from http://www.londonchamber.co.uk/news/press-releases/one-in-four-london-businesses-unaware-of-new-data/

Lsgar, S. (n.d.). *Regulatory Alert (2) Healthcare & Data Privacy*. Retrieved from https://bsabh.com/uae-legal-update-regulatory-alert-2-healthcare-data-privacy/

Makulilo, A. (2012). *Protection of Personal Data in sub-Saharan Africa.* Retrieved from https://elib.suub.uni-bremen.de/edocs/00102854-1.pdf

Malgieri, G., & Custers, B. (2017). Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review*. doi:10.1016/j.clsr.2017.08.006

Miglicco, G. (2018, September 9). GDPR is here and it is time to get serious. *Computer Fraud & Security*, pp. 9-12. doi:https://doi.org/10.1016/S1361-3723(18)30085-X

Myers, A. (2017). *Top 10 operational impacts of the GDPR: Part 4 - Cross-border data transfers.* IAPP. Retrieved from https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/

Natamiharja, R. (2018). A Case Study on Facebook Data Theft in Indonesia. *Fiat Justisia*, 206-223.

Parra-Arnau, J. (2018). Optimized, direct sale of privacy in personal data marketplaces. *InformationSciences, 424*, 354-384. doi:10.1016/j.ins.2017.10.009

Perry, R. (2019, January). GDPR – project or permanent reality? *Computer Fraud & Security*, pp. 9-11.

Prince, C. (2017). Do consumers want to control their personal data? Empirical Evidence. *International Journal of Human-Computer Studies*. doi:10.1016/j.ijhcs.2017.10.003

Shalhoub, L. (2017, January 31). *Islamic finance sees big growth in Europe*. Retrieved from ArabNews: http://www.arabnews.com/node/1046871/business-economy

Sharma, A. (2018). *GCC shelling out 66% more than global average.The National.* Retrieved from https://www.thenational.ae/business/technology/gcc-shelling-out-66-more-than-global-average-on-every-data-breach-gartner-says-1.783196

Taka, A. (2017). Cross-Border Application of EU's General Data Protection Regulation (GDPR) - A private international law study on third state implications. Retrieved from http://www.diva-portal.org/smash/get/diva2:1127596/FULLTEXT01.pdf

Thompson Reuters. (2018). *Islamic Finance Development: Resilient Growth*. Retrieved from Thompson Reuters: https://repository.salaamgateway.com/images/iep/galleries/documents/20181125124744259232831.pdf

Vilnius University. (2017). Digitalization in Law. *6th International Conference of PhD Students and Young Researchers* (p. 7). Vilnius, Lithuania: Vilnius University. Retrieved from http://lawphd.net/wp-content/uploads/2018/09/International-Conference-of-PhD-studentand-and-young-researchers-2018.pdf

WEF. (2018). *Global Competitiveness Index 4.0.* World Economic Forum. Retrieved from http://reports.weforum.org/global-competitiveness-report-2018/competitiveness-rankings/