Data Privacy Protection in the Region and Worldwide: Stakes and Challenges

INTERVIEW WITH
SCOTT A. WARREN
Partner,
Squire Patton Boggs

With the advent of the digital age and the unprecedented increase in data production, regulations have multiplied. These regulations seek both to protect data providers and to supervise the collection of data (personal data protection regulations). They also tend to penalise hacking (cyber security regulations). Although, to date, no international regulation exists, we are witnessing the emergence of regulatory frameworks for personal data which are having a cross-border impact. Regulation of the use of personal data, however, faces the major difficulty of reconciling two a priori contradictory imperatives: security and transparency on one hand, and commercial exploitation on the other.

.../...

Face à l'avènement de l'ère numérique et à l'augmentation sans précédent de la production de données, les réglementations se sont multipliées. Elles cherchent à la fois à protéger les personnes produisant des données et à en encadrer la collecte (réglementations relatives à la protection des données personnelles). Elles tendent également à pénaliser les actions de piratage (réglementations relatives à la cyber-sécurité).
Même si, à ce jour, aucune réglementation internationale n'existe, on voit émerger un cadre réglementaire global autour des données personnelles, de plus en plus contraignant. La régulation de l'utilisation des données personnelles se heurte toutefois à une difficulté majeure, celle de concilier

.../...

This article seeks to establish the state of play in terms of regulations on personal data protection in the Gulf region and around the world, but also to define the stakes. Scott A. Warren (Partner, Squire Patton Boggs) answers our questions.

des impératifs a priori contradictoires : sécurité et de transparence d'un côté, exploitation commerciale de l'autre.
Cet article cherche à dresser un état des lieux en matière de réglementation relative à la protection des données personnelles dans la région du Golfe et dans le monde, mais aussi à en définir les enjeux. Scott A. Warren (Associé, Squire Patton Boggs) répond à nos questions.

Data protection legislation has to be amended frequently in order to adapt to digital realities. What is the latest legislation that has been adopted in the Middle East region?

Scott A. Warren ◗ Actually, I am not sure I agree with the assertion about the need to amend data protection legislation frequently. It certainly is true that we increasingly rely on newly developed technology to handle our data, and this has greatly expanded our concerns about data protection. However, the essence of data protection itself has remained constant over the years. Protecting a company's trade secrets and data, or a person's information, has long been important to the continuing success of a company and our society. What has changed is the expanding risk of loss, now that so much important information is in a digital form, accessible through the borderless internet.

For these reasons, many countries across the globe have passed or updated their laws relating to cyber security and data privacy. The US's various patchwork of state and federal laws, and the European Union's General Data Protection Regulation (GDPR), whose penalty phase comes into effect on 25 May 2018, are but two examples of laws that govern how companies are to handle personal data. One of the most interesting aspects of these laws is that they are now starting to regulate how you handle data held in other jurisdictions. For example, under the GDPR, if a company collects data about EU consumers or its employees, the company is required to follow the GDPR even if their personal data is held outside of the EU (including by a third-party service provider). That is a significant obligation placed on such data, especially given the ease with which data can be shifted across country lines, and the huge penalties imposed for failure to comply.

Regionally, some countries are passing new laws to address increasing citizen and governmental concerns regarding the protection and loss of personal data. In addition, these laws seem designed to more easily allow data to transfer between the country and the EU, US and other countries that now require a minimum data privacy infrastructure before authorizing a transfer (such as Japan and Korea). Countries passing such laws, are able to apply for an "adequacy finding" from the EU, for example, which will make it easier for them to transmit the data to/from the EU.

Some of the latest data privacy developments in the region include:

Qatar: In late 2016, Qatar passed its Protection of Personal Data Privacy law[1], which had a grace period for compliance to expire in July 2017. On 2 January of this year, a long-expected extension was given, making the grace period to comply 29 January 2018. We expect an additional extension to be announced soon. Until that extension is formally issued, the obligations are to be complied with, with fines of QAR 5 million (USD 1.3 million) for violations.

1. Qatar Law No. 13/2016.

Under this new law, those who collect, process and otherwise handle personal data are, for example, required to:

- Obtain additional consent from the individual for the collection, processing and/or transfer of personal data, except in certain carve-out situations.
- Obtain governmental permission for the collection and processing of any *"personal data of a special nature"* (including ethnic origin, health, religious beliefs, marital/child status, etc.). This has far-reaching effects as such information is often collected by an employer to determine applicable payroll and social benefits.
- Take *"necessary and appropriate precautions"* to protect personal data, including training personnel, and testing and implementing a secure IT network.
- Allow individuals to query and alter their personal data.
- Notify the government and the individual of any breach that would lead to *"serious damage"* to the privacy of the individual.

Abu Dhabi Global Market (ADGM): Another recent development was not at the country level, but within the ADGM, an international financial center located in the United Arab Emirates (UAE), established in order to provide companies a place to operate under an international regulatory framework, with its own judicial and legislative infrastructure based on common law. As such, it governs activity for only the companies created or operating within the ADGM, as opposed to the broader UAE. However, given the number of companies established in the ADGM, its regional impact may be broad.

ADGM's Data Protection Regulations, passed in 2015[2], cover a broad range of obligations, including the collection, processing and maintenance of personal data, as well as its transfer out of the ADGM. The Office of Data Protection was established in December 2017 and a new amendment to the regulations was enacted on 1 February of this year. Among other things, this amendment now requires breach notifications to be made "*without undue delay, and where feasible, not later than 72 hours after becoming aware of it.*" It further increases the penalties applicable to data controllers whom fail to follow the regulations.

2. AGDM Data Protection Regulations 2015, enacted on 4 October 2015.

Do all Gulf countries have an effective legal arsenal in the data privacy protection domain? If not, how does this impact on their business climate?

Scott A. Warren ◗ It is important to separate cyber security laws (i.e., those that punish people that hack into systems) from data protection laws (i.e., those designed to protect an individual's personal information). The first is designed to apply against cyber criminals and the second is to apply to companies whom collect and process personal data.

We are a long way from the "ILoveYou" virus of 2000, where the Philippines Government could not prosecute the perpetrators, due to a lack of applicable cyber laws. Now, most countries in the region have a set of cyber security laws that will punish hackers.

However, most countries in the region have yet to implement a blanket set of laws relating to general data privacy or data protection. Instead, many countries rely on principles within their constitution, criminal laws, or even based on islamic law (*Sharia*). In the latter case, since such decisions are often not reported, and it is not possible to go to an authority that will provide clarity that will apply across the nation, it becomes more difficult for companies to know whether their activity is acceptable under the law. In such settings, it may be wise for the company to overemphasize individual consent for any actions they want to take regarding personal data.

In many GCC nations, there is often an element of data privacy protection that is enforceable through the criminal law. In the UAE, for example, its Penal Code (Articles 378 and 379) sets out statutory offences and punishments for publication of private matters or the unauthorized disclosure of private information without the consent of the subject person (although, it should be noted that private information is not clearly defined). Sanctions for breach include fines of up to AED 20 000 (USD 5 500) and imprisonment for a term not greater than one year. It remains unclear what impact these would have on a corporation that simply lost the data to hackers, whom subsequently posted it on the Internet or to other hackers. However, it would seem to impact corporations that want to sell or otherwise provide personal data of their customers to others. As mentioned earlier, we recommend obtaining proper consent from the party making the disclosure, in order to ensure you are not going to violate these laws.

Some regional investment centers, like the ADGM mentioned above, have passed data privacy laws to apply to the corporations formed or operating within. In 2005, the Qatar Financial Centre implemented its Data Protection Regulations[3]. The Dubai

3. QFC Law No. 7/2005.

International Financial Centre passed its Data Protection Law in 2007[4], and its Data Protection Regulations in 2012[5]. Further, many countries in the region have data protection laws that apply to specific sectors where sensitive data is being handled, such as financial institutions, healthcare providers and others.

4. DIFC Law No. 1/2007.
5. DIFC Law No. 5/2012.

If your company in the Middle East has data from EU consumers or employees on your local servers, and you fail to comply with the EU's GDPR, then you may face fines of up to 4% of your global revenue, or EUR 20 million, whichever is greater.

With existing international, regional and local standards and legislation, what are the main issues and risks to be identified by in-house legal counsel?

Scott A. Warren ◗ In my experience as in-house counsel for more than 13 years with game company Sega and Microsoft, the biggest challenges with compliance issues are 1) understanding the risks you face and 2) implementing an effective program to lessen those risks. Data privacy and cyber security risks are difficult, as the applicable law is only just now starting to impose serious fines for breach of the laws. These areas used to be considered IT concerns, with many companies entrusting them to the IT team. Perhaps because of the different skill-sets needed, it often seems that IT and legal teams speak different languages. Therefore, it is often difficult for in-house counsel to understand the nature of the problem.

What complicates things further is that these new legal obligations extend across regions. No longer is it acceptable for in-house counsel to only consider how local law will apply to the data held locally. If your company in the Middle East has data from EU consumers or employees on your local servers, and you fail to comply with the EU's GDPR, then you may face fines of up to 4% of your global revenue, or EUR 20 million, whichever is greater.

Therefore, I suggest the biggest challenge for in-house counsel is to understand how personal data is at risk within the corporation and then find ways to properly protect it. This usually starts with a cross-group assessment of what data you have, where it came from and where it currently sits. From there, you can analyse the laws that would apply and implement a program to meet those risks. If that seems daunting, there are those who can work with you to bring together the legal and technical expertise to work with your corporate resources to accomplish this.

Most laws realise you may be hacked, but they want to see good faith efforts to follow the rules. Where there has been little to no effort, we can expect increasingly large fines.

What are the coming challenges in the next few years regarding data privacy protection?

Scott A. Warren ◗ In my opinion, the biggest upcoming challenges in data privacy protection involve all of the new attackers and attack vectors to the digital information we have. Since more and more of our important information (whether personal or corporate trade secrets) is being stored digitally, hackers (often motivated by financial gain) and hacktivists (those motivated by political, religious or social reasons) have a greater benefit to finding access to it. Therefore, there is a rise in cyber attacks and those perpetrating them are increasingly doing this in a sophisticated and stealthy manner. Often times, companies are not even aware they have been hacked for many months after the hack first occurred.

In addition, attack vectors have expanded as technology provides more and more ways in. For example, attackers may study an employee's Facebook posts to create an email with an attachment that looks like it is from a friend, but instead has a computer virus attached. That virus could be used to install ransomware across the company, or just to infiltrate the corporate network further. That access could be used to send a fake email from the CEO, who is about to board a long flight, to one of the staff, requesting the immediate

wire transfer of a large amount of money to a designated bank account, in order to "close an urgent deal upon landing". Alternatively, that access could simply be used to look at the company's latest research and development, marketing or acquisition strategies, or other valuable internal information, in order to sell it to the company's competitors.

Some regional cyberattacks have involved the physical destruction of more than 30 000 computer hard drives. New attacks to Internet of Things devices, such as webcams and routers, have used exploits to turn them into a massive robot network of computers that have flooded the Internet with so many site requests that it took down much of the US's East Coast connectivity for a time. Additionally, some countries are using cyber attacks on the critical infrastructure of other countries, or to otherwise disrupt the political or social situation in that country.

Although it would be optimal if all countries could agree on a global data protection standard, I believe this is not likely to happen any time soon. The US and European governments have drastically different views on this subject, and many other countries are still trying to determine how important an issue this will be to them in the future.

Although it would be optimal if all countries could agree on a global data protection standard, I believe this is not likely to happen any time soon.

What is clear is corporations want to maximize the use of customer data to increase sales and develop new products. Governments are increasingly concerned that it is done fairly and with minimal risk to their constituents, and they are looking to enforce their rules across borders. So, it will be interesting to watch, and live through, the next few years as these competing interests collide.

Interview by: **Hermine Decaux** (Legal Writer)

سكوت وارن هو شريك في مكتبنا بطوكيو، مختص في الأمن المعلوماتي، خصوصية البيانات، والكشف عن البيانات الرقمية في آسيا و الشرق الأوسط. كما أن لديه تجربة كبيرة في مجال الحقوق الأدبية، الدعاوى القضائية، الإمتثال، فض النزاعات، وكذا في مجال التشريع الحكومي و التحقيقات الداخلية.

بدأ سكوت مسيرته المهنية كمرافع بكاليفورنيا. إنتقل إلى اليابان سنة 1993 حيث قطن مندئذ. إشتغل لمدة سبع سنوات لدى شركة سجا كوربوريشن كمستشار عام، و لستة سنوات لدى ميكروسوفت كمحامي عام. و ينشط في اللجنة التنفيذية لجمعية مراقبة الفضاء الإلكتروني، وهي منظمة غير ربحية.

وقد ترأس مكتب كرول في اليابان وكرول أونتراك آسيا، كما افتتح في وقت لاحق إبيك سيستمز في اليابان، الذي يوفر حماية في مجال الملكية الفكرية، وحاسوب الطب الشرعي وكذا الحلول المرتبطة بالاكتشافات الإلكترونية.

سكوت هو محام مرخص من كاليفورنيا ومحامي أجنبي مرخص في اليابان. وهو معتمد كمهني في مجال مكافحة الجريمة الإلكترونية و كعضو في معهد تشارترد للمحكمين.

Personal Data – Protection – MENA
Données personnelles – Protection – MENA

BIOGRAPHY

SCOTT WARREN is a partner in Squire Patton Boggs Tokyo office specialising in cybersecurity, data privacy and digital data disclosures in Asia and the Middle East. He also has significant experience in compliance, intellectual property, litigation, dispute resolution and government regulatory and internal investigations.
Scott Warren started his career as a civil litigator in California. He moved to Japan in 1993 where he has lived since. He served 7 years as General Counsel at Sega Corporation and 6 years as a Senior Attorney at Microsoft. He serves on the Executive Board of The Society for the Policing of Cyberspace, a nonprofit organization. He headed Kroll in Japan and Kroll Ontrack across Asia, and later opened Epiq Systems in Japan, providing IP protection, computer forensic and eDiscovery solutions.
Scott Warren is a California-licensed attorney and a licensed Foreign Attorney in Japan. He is a Certified International Counter-Cyber Crime Professional and certified as a Member of the Chartered Institute of Arbitrators (CIArb).