# The Data Protection Series: #2 Codes of conduct and Cloud Services

## I. Is there a data protection system in Lebanon and UAE?

Unless you purposefully eschew pop culture, it is been hard to miss the fact that Home Box Office, better known as HBO, was recently hacked, repeatedly. From leaking Game of Thrones' transcripts to releasing over a months' worth of an executive's emails, HBO had a rough month. To make matters worse, it appears as though its distributor in India is also having some security issues after an epic episode was released a couple of days early, albeit in lower quality than one would typically be able to watch on HBO on Sunday night. That distributor is not alone either. Its distributors in Norway also struggled to keep things under the hat, releasing yet another episode days before it was meant to air. All of these security issues have made HBO a bit of a laughing stock and lead one to wonder, what could have been done to prevent it and what is HBO liable for in this past months' worth of leaks?

As malware and hackers continue to expose just how interconnected the internet of things has made us, governments worldwide are making efforts to combat the butterfly effect of an attack on any single member in the system. While legislation has always struggled to keep up with technology, there are concerted efforts, especially in the United States, the United Kingdom, and throughout the European Union to share information, launch a concerted response and think collectively about the safety of data.

Robust growth in e-services has led to ever increasingly sensitive information being collected. The general public's awareness of and concern for the privacy of the data they are entrusting to the services they use grows with the increase in stored information. Even more detailed legislation will follow from state actors with developed data protection legislation while those countries who are newer to the regulatory paradigm will have some catching up to do and quickly. Regardless of what country the services are offered from, it is likely that the internet of things means the services will be subject to data protection regulations in another jurisdiction. More companies, large and small, have already moved towards cloud-based solutions and shared servers or more directly operate in data. They need to be increasingly aware of the regulations and best practices to keep them and their customers safe.

Lebanon is a signatory to various international treaties that acknowledge and enshrine the right to privacy and the protection of personal data, which is simply an


Samantha Bradshaw, Eptalex ATLF Beirut

extension of the right to privacy in a technological age. However, Lebanon currently has no legal framework directed specifically at personal data protection.

There are laws protecting the secrecy of communication and forbidding suppliers form disclosing customer data, but they are not fully enforced. While Lebanon may not have a full framework for the protection of legal data, it already has the foundation set to respect the right to personal data protection and has indicated its intent to do so in signing the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights and co-sponsoring resolutions on the right to privacy in the digital age in the United Nations General Assembly.

The UAE also has no formal federal data protection system, but does acknowledge the right to privacy in its constitution as Lebanon does but only for UAE citizens. However, the UAE has more sector specific laws based on the residency of the person obtaining the data in healthcare, consumer personal information, general cyberspace and personal information. These laws are largely restricted to certain free zones in the UAE though and present limited protection or obligations for those operating outside the industry specific free zones.

Furthermore, for businesses operating out of Lebanon, the lack of data protection legal framework does not prevent them from needing to comply with data protection principles. Apart from the obvious danger to consumers who have no means of determining which companies have what information, many companies use 'cloud' services for archiving, backups and even general storage. Data is typically transferred to server hubs in various countries depending on the service provider and subcontractors they use. The physical servers and, in some cases, even end users of a company's product are located in jurisdictions that have well developed data protection legislation that compels companies not physically present in the legislator's jurisdiction to comply with laws if data if being processed or stored in their country. As such, any company would be wise to begin developing their own codes of conduct for how to store and protect data and contingency plans in the event of a breach.

**II. Basics for your Code of Conduct**

Since data is stored all over the world, it is first necessary to determine where the processing and storage occur, as well as the residency of the people providing the data in some case to determine which data protection laws will apply. However, a simpler solution would simply be to comply with and maintain an up to date code up conduct based on the most stringent regulations in force. Even though any given company is likely


Samantha Bradshaw, Eptalex ATLF Beirut

outsourcing data processing services in some manner, in most cases they are subject to the same strict regulations that a data processor, since it is typically seen that the data controller, i.e the company, retains control of the data and the data processor only acts at the instruction of the data controller.

Generally, data protection laws are based on (i) the fair and lawful collection and processing of personal data, (ii) specified and lawful reasoning for collecting data, (iii) adequate, relevant and not excessive amounts of data related to specified reasoning, (iv) adequate level of protection both in initial recipient and any future recipients. The European Union issued a resolution encompassing these ideas and more which requires all member states to have compliant data protection laws in place by 2018. Canada and the United States already have fairly complex and robust data protection laws in place that evolve further every year. The UK has the Data Protection Act.

With the majority of physical cloud servers located in Europe and North America, even companies in jurisdictions with little to no data protection regulations must abide by the general principles. Without that, they can run the risk of massive fines for not handling data properly or negative images in the press as the public becomes more aware of their rights and which companies respect them. Many companies need to be able to move information about their clients or customers around to other jurisdictions that may not have the adequate level of protection commonly being seen in data protection laws recently. The easiest solution to that is a IT savy contract that ensures all reasonable protective measures are specifically outlined and the liability for failure to comply with them is passed on to the recipient in the country that doesn't impose obligations for a sufficient level of protection for personally identifiable information.

The current trend in data protection principles is Privacy by Design, an acutely original name that titles the approach to projects where privacy and data protection compliance are thought of from the start, rather than an afterthought or ignored aspect. This approach, like most preventative measures, is generally more cost efficient, leads to simpler and more easily remedied issues and less legal liability. Expect governments to add stronger penalties to those who do not comply with Privacy by Design as data becomes more of a concern in coming years.

**III. How to choose a cloud service provider**

What to do?

Know where data is stored and where any person related to any stored or processed data is from to ensure you comply with any data protection laws in all potential jurisdictions.

For example, the UK's new data law restricts the transfer of personal data outside of the European Economic Area unless that country "ensures an adequate level of protection for the rights and freedoms of data subject in relation to processing of personal data."

Energy efficiency is on point to become a major concern for service users, a selling point for providers, and a matter of public policy for technologically savvy governments. Data centers use more electricity than most consumers realize. It goes beyond simply powering the physical servers to maintaining a specific temperature and humidity levels, physical and digital security systems, and mechanical, electrical, plumbing, and fire protection.

Ask about infrastructure redundancy and reliability concepts as well as what standards the data center follows. The sector and nature of each business determines which standards one may need to look for in a data center. There are varieties of standards, both nationally and internationally recognized. If you have clients in the US, then the US standards may apply. For those with international clients or a mix of both, an international standard may be more appropriate. The key is to choose a data center with the appropriate standard and document the due diligence done in seeking it out.

It is essential for every company that collects information to create a set of best practices for data protection. Best practices are a list of recommendations formulated for specific areas, in this case, data protection. Those best practices should comply with multiple countries' data protection laws, as data is rarely limited to one jurisdiction, and are suggested to stakeholders to apply to a segment of some areas.

Although various regulatory authorities can provide best practices or codes of conduct, the more precise ones are in practice much easier to follow than the more general data protection legislation. Companies should look to the regulatory agencies in their respective sectors in various countries to determine what a sound code may look like and stay abreast of changes in the law as technology moves forward.