# Bahrain Data Protection- Proposed Regulation of ‘Technical and Organisational Measures’

**Andrew Fawcett** - Partner - Digital & Data
a.fawcett@tamimi.com - Abu Dhabi

Zeina Albuainain
Z.Albuainain@tamimi.com - Bahrain

## Introduction

Using appropriate technical and organisational measures to ensure the security of personal data is a common requirement under data protection regimes, including, most notably, the European Union’s General Data Protection Regulation (“**GDPR**”).

Whilst technical and organisational measures are integral to ensuring security in processing and preventing security breaches, the requirement is usually deliberately left vague by regulators in order to accommodate for the transient, fluctuating nature of developments in cybersecurity, technology and innovation. Consequently, data protection regimes prescribe that security measures must be benchmarked to the “state of the art”, without detailing what this may actually mean.

It is against this background that Bahrain’s Data Protection Authority (“**Authority**”) has issued a Draft Order regarding “the conditions to be met in the technical and organisational measures that guarantee protection of data” (“**Draft Order**”). In contrast to the GDPR, the Draft Order goes considerably further in specifying what security measures must be implemented. This article aims to shed light on Bahrain’s

evolving data protection landscape, with a focus on the technical and organisational measures to protect data.

## Bahrain's Data Protection

The primary legislation in Bahrain is the Personal Data Protection Law (Law No.30 of 2018) ("**PDPL**") which came into force on 1 August 2019. Currently, not all provisions of the PDPL are effective; the resolution issuing the PDPL stipulates that the Authority's Board of Directors ("**Board**") shall issue the necessary implementing regulations for the PDPL's effective application.

Pursuant to the above, the Authority *(currently, the Ministry of Justice, Islamic Affairs and Awqaf)* has now issued a series of draft orders for public consultation, which include the Draft Order (note that the consultation on the Draft Order ended on 30 June 2021).

The Draft Order is intended to supplement Article 8 of the PDPL (Security of Processing) as further detailed below. This Article explicitly assigns the Board to *"issue a regulation prescribing specific conditions to be met in the technical and organisational measures"*.

## Beyond the European Influence

Those familiar with other data protection legislations will find that the majority of the provisions in the PDPL are drafted in comparable terms to the GDPR. However, the Authority's Draft Order proposes to expand the PDPL beyond its European equivalent, as it prescribes specific technical measures to be implemented by data controllers.

## Getting Technical: What Technical and Organisational Measures are Required?

While the term "technical and organisational measures" appears approximately 89 times within the GDPR, it is not definitively defined. Rather, Article 32 of the GDPR on Security of Processing states that, in implementing technical or organisational measures, organisations must "*take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing.*"

Similarly, Article 8 of Bahrain's PDPL on Security of Processing requires organisations to implement appropriate technical and organisational measures, and to ensure an appropriate level of security "*taking into account the latest technological security measures, the associated cost, the nature of the data to be processed and the potential risks involved.*"

With reference to the above, whilst organisations subject to the PDPL are required to take into account the risks involved, this brief reference to "risks" within the PDPL must not be mistaken for a "risk-based" approach in the European sense, which entails a proportionality assessment before adopting security measures.

Unlike the GDPR, where the only technical measures expressly referred to are encryption and pseudonymisation, Article 21 of the Draft Order requires data controller to implement generally accepted best practice/ technical measures, including but not limited to: access control, change management

process, password protection, device authentication, data and hardware encryption solutions, anti-virus applications, wifi security, firewalls and Network Access Control (NAC) which is an approach to computer security that attempts to unify endpoint security technology (e.g. antivirus, host intrusion prevention, and vulnerability assessment).

Other measures prescribed in the Draft Order include the use of dummy data when developing electronic information systems in the organisation to protect personal data from loss or damage.

## Meet the Compliance Trio – Data Protection Guardian, Data Protection Officer, and Information Security Officer

A significant "organisational measure" imposed by data protection legislations such as in the GDPR is the requirement to appoint a Data Protection Officer (DPO). As stipulated above, the GDPR follows a risk-based approach; accordingly it only requires a DPO where there is 'high risk processing'. In contrast, the PDPL – together with the Draft Order – is proposing to create three overlapping *(non-mandatory)* compliance roles. The compliance trio include:

1. The Data Protection Guardian (DPG): the DPG is responsible for ensuring that the data controller processes personal data in compliance with the provisions of the PDPL. The DPG is also responsible for liaising with the Authority, as well as identifying and reporting any violations to the Authority (note that the DPG role is created under Article 10 of the PDPL, and there is a separate draft order regarding the role and functions of the DPG);
2. The Data Protection Officer (DPO): this role highly overlaps with the role of the DPG. The DPO shall monitor compliance of processors and service providers, submit regular reports to the data controller and communicate with the DPG where necessary. The role may also involve direct communication with data subjects to receive requests, complaints and inquiries; and

- The Information Security Officer (ISO): the ISO's role is focused on developing information security strategies and addressing information security risks.

## Mandatory Insurance

The Draft Order proposes that every data controller maintains an insurance policy issued by one of the licensed insurance companies in Bahrain, in order to cover compensations resulting from violating the privacy of data subjects and any damages or expenses incurred by data subjects as a result of that violation. The insurance amount is yet to be determined.

## Conclusion

The Draft Order departs from the European approach to data protection through adopting a more prescriptive approach for the technical and organisational measures that are required to ensure the security of personal data.

Whilst ensuring the security of personal data is a fundamental aspect of data protection, a prescriptive

one-size-fits-all approach will potentially disproportionately increase the compliance burden for small and medium-sized enterprises.

***For further information, please contact Andrew Fawcett.***