Acclaiming Accountability. Preaching Best Practices

7

Noriswadi Ismail

Management of many is the same as management of few. It is a matter of organisation – The Art of War

(Sun Wu, known as Sun Tzu, Military General and Tactician, 544 BC-496 BC)

Abstract

This chapter advocates about leadership and strategy that company, organisation and institution should be able to adopt. It brings the readers to consider how crucial accountability plays its role and the need to continuing such best practices. This is neither a secret recipe, nor, exceptional in data protection, as it may also be applicable to other subject matters. Data protection, at times, is slightly understated, but certainly, it is not underrated. It raises the eyebrows of the board of directors, executive committee and senior management if breach happened. Otherwise, it may be regarded as another mundane, routine and monotonous compliance tick-in-the box exercise if it is fully complied with. In order to debunk the latter, I attempt to impress the readers that data protection is not another area of law that adds the burden; rather, it boosts the brand, governance and leadership of your company, organisation and institution.

7.1 From Top to Bottom

In Chaps. 4 and 5, I have, in some occasions, supplicated the involvement of the board, executive committee and senior management to appreciate data protection. This is followed by the executive, supporting employee, business partner and

N. Ismail (✉)
Quotient Consulting, 29 Duffell House, Loughborough Street, London SE11 5PX, UK
e-mail: noris@qconsultant.com

N. Ismail and E.L. Yong Cieh (eds.), *Beyond Data Protection*,
DOI 10.1007/978-3-642-33081-0_7,

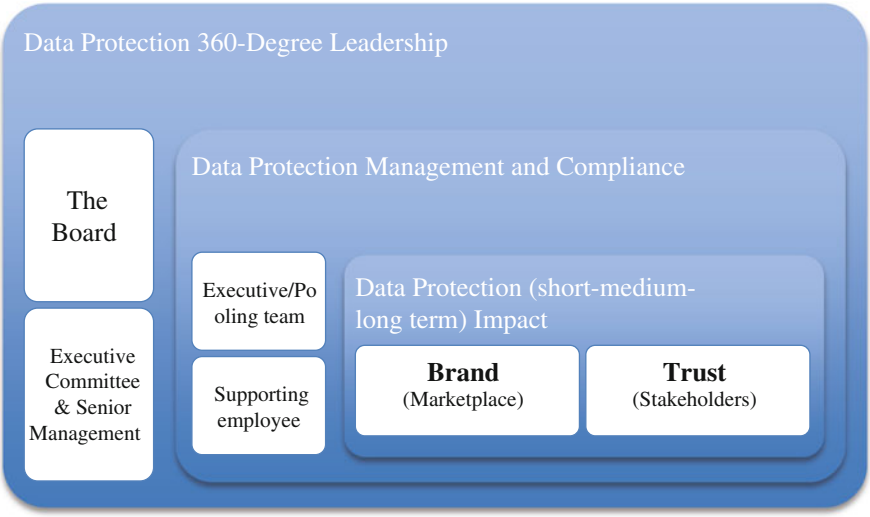

Fig. 7.1 Data protection leadership

associate (who may have the contractual obligation and commercial transaction interest) with a company, organisation or institution—either as a data user, data processor or a third party. In data protection leadership, it is a 360-degree exercise. It is not isolated and a stand-alone leadership that is helmed by a general counsel, data protection advisor, consultant and expert. The leadership flows from top to bottom of a company, organisation and institution's hierarchy, as figured (Fig. 7.1):

Instilling data protection 360-degree leadership culture within the 'DNA' of a company, organisation and institution is the key to accountability. This may also apply to the exempted entities of the PDPA (the Federal and State Governments and credit reporting agencies). Everyone should be able to take the lead and appreciate data protection not within the commercial transaction setting, but also in his or her personal life. To execute the leadership, I have considered useful strategic guidance for potential adoption:

7.1.1 Strategic Guidance: For the Board

Data protection governance should be one of the main agenda to be deliberated and resolved at the board level. The Chairman of the Board may propose an independent non-executive board member to lead the strategic deliberation on matters pertaining to data protection for the board's resolution. For example, a special board committee on data protection could be established to ascertain whether the company's business, deployed technologies, products and services are data protection compliant and friendly. The committee members may be composed of an executive board member, independent board member, independent data protection auditor/

consultant/counsel/expert (by invitation) and the general counsel/data protection advisor of the company. The frequency of the special board committee in data protection may be convened quarterly (for public listed company—Berhad) or mid-yearly (if the company is a private limited company—Sdn. Bhd). Alternatively, the Chairman of the Board's Audit Committee (the Committee) could compulsorily outline data protection governance as a compulsory agenda that requires attention to the Committee. If this alternative may be the preferred route, the company's data protection team shall be accountable to report, present and highlight this, through the Audit Committee. Once the Committee deliberated and resolved the agenda, it will form the company's state of internal control that is required for disclosure to the shareholders (in annual report).

7.1.2 Strategic Guidance: For the Executive Committee/Senior Management

Subject to the size of the company, organisation and institution, data protection leadership may be helmed by a dedicated data protection counsel/advisor, having a pool of diversified executives. They may represent the company's division, department, unit, and projects that are exposed to critical data processing activities. Data protection leadership role may be led by the general counsel, risk management advisor and internal auditor. Typically, start-up and semi-medium sized company may initiate the leadership role to the nearest group/team or unit, which deals with data processing activities, management and compliance on a daily basis. Clear key performance indicators (*kpis*) on data protection leadership must be spelled out so that it may be achievable based on the mission and vision of the company/organisation/institution's business. If cost and resource is the main constraint to execute the leadership role, the owner of the start-up and semi-medium sized company may outsource the required roles and functions by way of terms of reference to data protection consultant/solicitor/expert. Nonetheless, it should be cautiously borne in mind that accountability will never be acclaimed if it is totally outsourced!

7.1.3 Strategic Guidance: For the Executive and Pooling Team

The execution of *kpis* should be updated quarterly. This is to accelerate the reporting process by the Executive Committee and the Senior Management. A template report on data protection governance and compliance should be established and adopted throughout the company/organisation/institution. In order to reduce duplication of reporting, and in the interest of time, cost and resource, an agreed template report should be agreed beforehand and it's best to develop this via online. If and when necessary, a lead executive in the pooling team should be able to raise the critical concerns of such data protection issues to the Executive Committee for decision making. If such issues require greater attention at the

board level, this shall be brought to being one of the agenda in the special board committee on data protection or alternatively, at the Audit Committee level.

7.1.3.1 Everyone Can Lead

Looking into the scheme of data protection leadership and its actors, I take the position and view that everyone can lead in data protection. Lead, in the sense that, it is not about power struggle and tussle. Lead, in the sense that, it is a collective accountability that mirrors and reflects the company/organisation/institution's vision and mission. Of relevance, and most importantly, the leadership should be parallel with its 'DNA', its culture and its day-to-day governance and operations.

7.2 From Outside to Inside

At the time of this writing, data protection is a new subject matter in Malaysia and also in ASEAN. There are not many experts specialising in this area, although some advocates and solicitors tend to specialise based on their prior and existing industrial relations, capital market, corporate and commercial (which includes banking and finance), and perhaps, the nearest; technology, media and telecommunications' practice. This is a positive sign that takes place. For company, organisation and institution, it is worthwhile to get engage with these professionals in order to gauge the comprehensive understanding on how PDPA works. Subject to the size of the company, organisation and institution, appointing an independent professional (whether it is a legal firm, consulting firm or information security expert firm) requires cautious consideration too, as follows:

7.2.1 Consideration 1

If your company, organisation or institution has had its panel of professionals, ensure that they are continuingly equipped with the breadth of understanding on data protection. It may not be restricted to the laws, regulations/guidance only, but also extendable to the understanding of technologies and its interrelationship with your data processing activities within a commercial transaction setting.

7.2.2 Consideration 2

Careful consideration should be given to professionals who claim they are expert, but not qualified to deliver a legal advice, or consult your company, organisation or institution not only from the PDPA's viewpoint, but also from the viewpoints of the EU, US, APEC and the OECD. A good and commendable data professional should be able to have the global breadth of understanding, at least, on comparative jurisdictional approaches of data protection, besides the local/regional content and expertise derived from his or her local/regional experience.

7.2.3 Consideration 3

To further enhance the transfer of knowledge and skills, it's recommended to consider 'secondment' engagement between the professionals and your company, organisation and institution. On the one hand, this may help to appreciate the diversity of issues, challenges and practice faced and on the other hand, this shall equally determine whether the required professionals possess the right knowledge and skills in data protection. If the secondment route may not be practicable, consider to retain the professionals based on ad-hoc basis and if the quality of advice/consultation is exceptionally well, consider retaining the professionals on a retainer basis.

7.2.4 Consideration 4

Professionals are also people like us (in a career context). They need to attend training and be retrained. They need to be certified in a specialised data protection professional certification. It's best to consider their professional learning development, certification plans and match the same with your company, organisation and institution's plan too. At present, the leading certified data protection professional is managed by the International Association Privacy Professionals (IAPP), based in the US. It is highly recommended to be certified by IAPP to being a Certified Information Privacy Professional (CIPP). For future planning, consider to identify potential members who should be able to get certified. This consideration could also be extended to the professionals who have not secured certification.

7.2.5 Consideration 5

Consider to having a diversity of professionals, instead of one. A diversity of legal firm, consulting firm, information security expert firm and in some cases, academic consultant is the best combination. Subject to your company, organistion and institution's budget, and the complexity of the subject matter in data protection, a diversity of professionals deemed to be invaluable. This is due to the 360-degree viewpoints that you may secure from their professional advice and opinion.

7.2.5.1 The Public Relations in Data Protection

Data protection leadership is partly incomplete without the role of Public Relations (PR)/corporate communications. Company, organisation and institution with PR budget and pre-planned data protection campaign may not face such hindrance to effectuate. The best practice is to design the campaign through stages. Strategically, they are:

- *Stage 1:* data protection campaign in the working place;
- *Stage 2:* data protection accountability statement and commitment in existing products and services; and

- *Stage 3:* data protection accountability statement and commitment in all marketing collaterals (brochure, website and existing branding platform)
  Start-up or medium-sized company may consider these:

7.2.6 Consideration 1

Outsource the function to an independent Public Relation (PR) consultant and highlight your positioning in relation to data protection leadership. For instance, if the products and services are related to data processing activities, such branding collaterals (brochure and website) should highlight whether they are data protection compliant and friendly.

7.2.7 Consideration 2

Partially outsource the function to the PR consultant if cost and resource is a key constraint. In certain instance, you may periodically position your business' undertaking in relation to the operations, products and services that may affect data protection. This could be done through existing social media platform or reasonable marketing collaterals that suits the business.

7.2.8 Consideration 3

Engage and communicate effectively with your client, business partners and associates in relation to new products and services' offerings that may affect data protection. Such updates may be useful to be consistently communicated throughout. This may lead to potential impression to your client, business partners and associates' on how pivotal data protection is, in your business,

7.3 Global Engagement

Inevitably, it's best to develop potential regional and global engagement to raising potential policy based issues in data protection. Although this seems to be quite high level, company, organisation and institution, which have deep interest in data protection within their business models, products and services may consider to establishing the engagement.

The APEC Electronic Commerce Steering Group is the potential platform. This may be done through public policy engagement with the Commissioner or any related governmental ministries or agencies that may have the similar interest. The OECD Directorate for Science, Technology and Industry is also another regional platform that may be considered for engagement. These two organisations shape the influence amongst its members towards any policy-based discussions and

consultations relating to data protection. Although the outcome of such position and strand is partly not binding, nonetheless, it's advisory and influential. It may also potentially shape the regional and global data protection's trend.

For the Commissioner, relevant governmental agencies, ministries and officials, the yearly international conference of data protection and privacy commissioners is a global platform that must not be missed. At the time of this writing, the forthcoming conference will be held from 23rd October to 24th October 2012 at Punta Del Este, Uruguay.[1] This yearly conference gathers all data protection commissioners, authorities, professionals, experts and interested stakeholders to get engage, articulate, discuss and debate on topical issues relating to data protection across the globe. Invariably, such developments from the European and American parts should also add the value to the engagement. Global platforms and engagements organised by the IAPP are also worthy to consider.[2] These global engagements shall enable company, organisation and institution to:

- **Keep abreast** with the global issues relating to data protection;
- **Explore** specific data protection issues that may potentially arise from, and contributed by, existing and new technologies;
- **Learn** the best practices on formality and enforcement approaches of different jurisdictions;
- **Develop** potential ideas and opportunities to implement the lessons learned from the engagements;
- **Expand** the network of data protection experts globally;
- **Engage** in continuing training and development by potentially collaborating with the relevant officials, experts and consultants towards capacity building engagement; and
- **Contribute** the necessary knowledge and skills through potential transfer of knowledge.

7.3.1 Grooming More Data Protection Experts

It is exceedingly daunting to groom more data protection experts especially when the subject matter is new to Malaysia and ASEAN. As I pointed out in **Sect. 7.2** above, due to the evolutionary development in this part of the region, data protection professionals are in scarcity. To be called an expert, I am of the view that he or she should be able to fulfill the necessary grounded knowledge on data protection fundamentals, not only at the local level, but also at the global level. In addition, he or she should be able to appreciate the interrelationship of existing technologies, business and compliance at the same time. To reach this level, it requires

[1] See 34th International Conference of Data Protection and Privacy Commissioner's website. http://www.privacyconference2012.org/english/home/. Accessed 1 July 2012.

[2] See IAPP https://www.privacyassociation.org/. Accessed 1 June 2012.

multidisciplinary understanding and exposure. In view of the present landscape, I propose these:

- **Creation** of a local data protection certification in Malaysia that is generally transferrable and recognisable in ASEAN;
- **Complement** the existing international certifications that is issued by the IAPP, once, and if, such certification is introduced; and
- **Consult** the relevant professional-based bodies in Malaysia and ASEAN that may have potential interest in data protection to regionally harmonise the certification.

Although the above proposal sounds idealistic and perhaps, viable in 5 years time (or more), if considered, it may boost Malaysia and ASEAN data protection leadership as a whole. This, however, could not be materialised without the involvement of the Commissioner, relevant governmental agencies, ministries and interested stakeholders who may want to contribute to this capacity building. Malaysia and ASEAN requires more talents in data protection. In order to do groom these talents, it must begin from the top to the bottom of the company, organisation and institution. Likewise, from the outside to the inside's contributions of professionals who have the breadth expertise in data protection.

7.4 Brief Guidance to Malaysian and ASEAN Companies Having Establishment in the EU and the US

There are some Malaysian and ASEAN companies, which have had investments and operations in the EU and the US. Depending upon the business structure; whether it is project based or as a subsidiary, unincorporated joint venture or an incorporated joint venture, the need to understand the local data protection laws is paramount. It is unmissable. These are the strategic guidance for consideration:

7.4.1 Strategic Guidance 1: Apply the Local Data Protection Laws

If the company has business operations in several member states of the EU, the rule of thumb is that, the local data protection laws apply. Nonetheless, there are certain conditions that must be complied with in relation to, transfer of, personal data and sensitive personal data from Malaysia and ASEAN countries to the EU; whether the company is a data controller, data processor or acting as a data importer or an exporter. In this respect, it is best to consult the local laws and the relevant provisions on data transfer.

If the company has business operations in some states in the US, cautious consideration should be made to the nature of data processing in the respective areas of businesses. The states in the US have different legislation governing sector-specific legislation. On a broader scale, the company must also consider the adoption of the US Safe Harbor, being the self-regulatory requirements in relation to data privacy.

7.4.2 Strategic Guidance 2: Appoint Local Data Protection Professional(s)

The appointment of data protection professional(s) to coordinate and advice on such formality, requirements, enforcement and governance issues of the local laws is vital. The professionals should be able to work closely with the company's data protection team, its in-house counsels and local-based advocate and solicitor to addressing the required subject matter relating to its business and data protection compliance. The appointed professional(s) will be the key contact or the lead to act on the company's behalf whilst dealing with the formalities, governance and compliance required under the national laws. If and when necessary, they will also act on your behalf to coordinate such data protection matters with the data protection authorities and advise on potential issues relating to data transfer agreement or any preferred options that may be relevant to the business' needs and objectives.

7.4.3 Strategic Guidance 3: Pursue Periodic Data Protection Audit with the Data Protection Professional(s)

To further improve the company's business operations, products and services that affect data protection, it is recommended to commence a periodic (quarterly) audit with the data protection professional(s). The company's data protection team, its local professionals and advocate & solicitor may also be involved to this audit (if necessary). The rationale of the proposed periodic audit is to exercise the recommended best practice—certain national data protection authorities of the EU require audit trails (if severe security breach happened). In the US, the requirements differ form one state to another state. Subject to the business model, project structure and involvement of the company in its data processing activities, it is still indispensable to pursue periodic audit as pre-emptive measure.

7.4.4 Strategic Guidance 4: Review and Improve Data Protection Management and Governance

Throughout the business operations in the EU and the US, it is also prevalent to review and improve the company's data protection management and governance. In the interest of data protection leadership, the outcome of review, proposed rectification strategies and plans should be tabled at the board and executive level of the company. This may benefit the year-on-year operations and potential strategic and consultative engagement with the relevant data protection professionals.

List of Materials

Asia-Pacific Economic Cooperation (APEC) CBPR System – Policies, Rules and Guidelines (2012) Purpose: Consideration. Submitted by: DPS Chair. http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_009.pdf. Accessed 30 May 2012

ComputerWeekly (2012) You Can Outsource Responsibility, But Not Accountability – Identity, Privacy, Trust. http://www.computerweekly.com/blogs/the-data-trust-blog/2010/08/you-can-outsource-responsibili.html. Accessed 30 June 2012

Data Protection Accountability: The Essential Elements (October 2009) A Document for Discussion. http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf. Accessed 1 April 2012

Hunton & Williams Centre for Information Policy Leadership, Accountability-based Privacy Governance (2012) http://www.informationpolicycentre.com/accountability-based_privacy_-governance/. Accessed 28 March 2012

IAPP: Demonstrating Privacy Accountability (2012). https://www.privacyassociation.org/publications/demonstrating_privacy_accountability/. Accessed 8 February 2012

IAPP Certification – Certified IAPP Privacy Professional (2012). https://www.privacyassociation.org/certification/. Accessed 15 February 2012

International Chamber of Commerce Discussion Paper on Data Protection Principle of Accountability (2012). http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/ICC-discussion-paper-on-data-protection-principle-of-accountability/. Accessed 28 March 2012

Nymity (2012) Privacy Interview with Experts, Interview on Demonstrating Accountability. http://www.nymity.com/About_Nymity/~/media/Nymity/Files/Interviews/2011-04-McQuay.ashx. Accessed 15 March 2012

Office of the Privacy Commissioner Office of Canada (2012) Walk the Talk and Show It: Demonstrable Accountability for Data Protection. http://www.priv.gc.ca/media/sp-d/2012/sp-d_20120417_pk_e.asp. Accessed 18 June 2012