Prioritizing PDPA compliance activities in 2022

Article by SafeComs

Bernard Collin, Alex Cespedes

Alex Cespedes.

Alex is a Digital Risk Consultant with over ten years of experience in data risk and compliance across Europe in both public and private sectors. He is co-chair of the Thai KnowledgeNet Chapter of the International Association of Privacy Professionals (IAPP).

In addition, he is the authorized Instructor for the IAPP Certified Information Privacy Professional (CIPP/E) and Certified Information Privacy Manager (CIPM) training across South-East Asia.

Alex has over 10 years of data protection consulting for the private and public sectors in Europe. He advised numerous clients during investigations by supervisory authorities.

His focus areas are providing Chief Privacy Officer (CPO) as a service and Data Protection Officer (DPO) coaching for SMEs and multinational companies. In addition, he is specialized in data risk review and assurance to enable a clear action plan based on the real possible impact on brand or revenue.

Bernard Collin.

Bernard is the CEO of SafeComs Network Security Consulting Co., Ltd. He focused firmly on Cybersecurity, ITIL practices, and Compliance with standards. He is an active member in the various chamber of commerce, including JFCCT and has delivered presentations on Cybersecurity and PDPA for the past years.

He founded SafeComs in Australia in 1999 and launched the Thai office in 2005 and Myanmar in 2014. SafeComs is a BOI-registered company with 30 employees from 11 different nationalities.

Our experts have experience in European countries, as well as ASEAN, covering all aspects of the IT industry and Cybersecurity.

After a management role on the distribution channel in Apple Europe, he became GM of Apple Belgium. He also worked for Digital Equipment in Geneva and then Launched the European branch of Pacer Software. He left after 10 years, migrated to Australia, and launched SafeComs.

Bernard holds a degree in Nuclear electronics and is passionate about flying gliders and small planes.

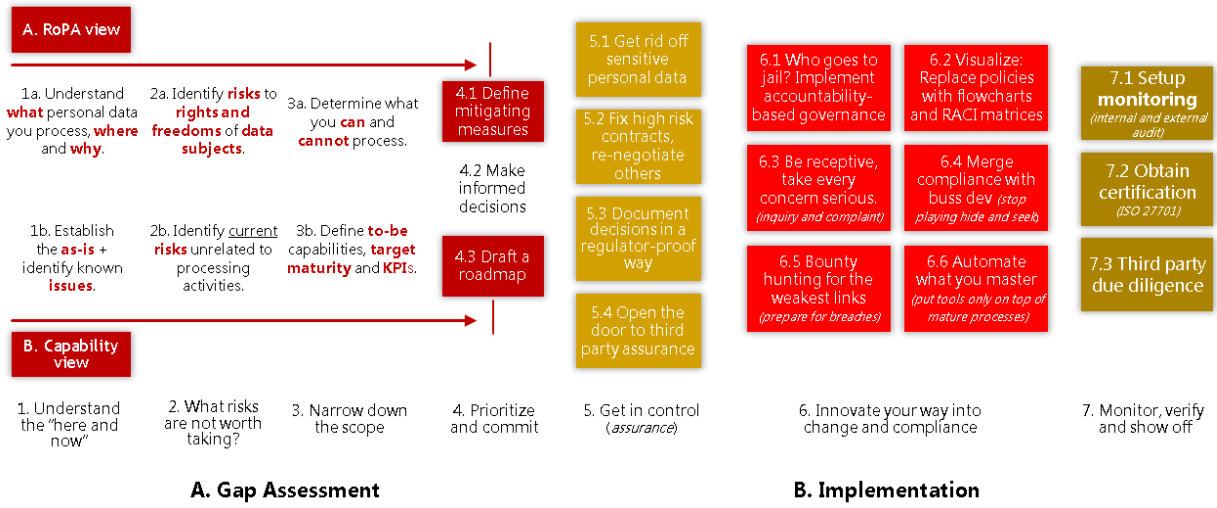
Drop us an email (dpo@safecoms.com) to get a succinct view of what a PDPA success story looks like.

Prioritizing PDPA compliance activities in 2022

Organizations processing personal data need to comply with the Personal Data Protection Act B.E. 2562 (PDPA). Non-compliance may result in administrative fines, criminal penalties and punitive damages. However, the PDPA should be seen as a business enabler. The objective is to mitigate risks and increase trust while we transition into a data driven society.

First of all, compliance is not a one-off exercise, it is about building a capability and achieving continuous improvement. The PDPA wants you to be in control of your personal data and increase your level of assurance. Therefore, if in 2022 you have at least identified the main risks, introduced a couple of measures, and come up with a proper implementation plan, you have a road to follow.

In the following sections we focus on two main actions to take in 2022: "**Prioritize your risks**" and "**achieve quick wins**" representing a summarized view of things to be done up until step 5 in our proven approach for a PDPA success story as visible in the image below.



Prioritize based on risks

The very first step is to understand what personal data you process, why, how and where. Towards this end, work closely with your client facing teams and internal functions. Be sure to distinguish between structured and unstructured data. Often unstructured data is harder to manage and control.

The cornerstone of any PDPA compliance project is the records of processing activities in support of Section 39. Make sure the records represent the combined understanding of your business, IT and legal people. It is important to identify for which processing activities you process (sensitive) personal data, for which purpose and the lawful basis.

Next step is to visualize the records into high level data flows which should be used to support any discussions with management or the regulator. In parallel, you should make a list of systems and applications supporting processing activities and identify transfers to third countries. By the way, understanding the data collection points will enable you to know where a privacy notices should be added.

Then, identify for each processing activity the risks for non-compliance to your organization and the risks to rights and freedoms of data subjects. Perform a threshold assessment based on well accepted criteria used in the EU such as whether the activity may result in profiling or monitoring, whether it is easy to merge data sets, whether you are processing on a large scale, etc. This will allow you to distinguish between high, medium or low risk processing activities.

For the high-risk activities, perform a Data Protection Impact Assessment (DPIA). When doing so, analyze which data protection principles maybe be impacted. We recommend to also take into consideration the rights of the data subject. The key questions are “how bad would it be if something happens?” and “how likely is this to happen?”

Now you can determine whether the level of risk is acceptable for your organization. However, consider that some risks to the rights and freedoms of data subjects should not be accepted. In this context, determine which controls could mitigate which risk. Controls may modify the likelihood, the impact, or both. There are four typical types of controls to be considered: preventive, detective, repressive and corrective.

Achieve quick wins

There may not be enough time to mitigate all risks in 2022. Nevertheless, you should initiate some quick wins and focus on short term pragmatic actions: Remove unused data, determine lawful basis of your processing activities, update your contract templates and draft key policies and notices.

Removing personal data you don’t need equals to removing the risk that something may happen to it. Just imagine how many years of activities have accumulated personal data across your systems. However, remember that the PDPA is not absolute and data retention requirements from other legal obligations may apply.

Managing consent is resource intensive and relying on legitimate basis in some cases is a black box. Try to rely as much as possible on legal obligation and performance of a contract to have a clear-cut answer to “can we process this personal data?”

Sooner or later you will need to review all your contracts with third parties. But this is a project on its own and may take months. At the very least you should identify all types of contracts you have and

update the templates so that it includes the necessary legal language. When doing so be sure to have a placeholder to cover the instruction given from controller to processor and consider having a clause allowing you to audit the processor when relying on its services as a controller.

Lastly, draft your privacy policy in a way that is easy to digest, create the supporting procedures for example to handle data subject requests or report personal data breaches. Also make sure clear notices are created and available at the relevant personal data collection points. Data subjects have the right to know what personal data you collect, what it will be used for, etc.

Conclusion

Don’t try to do everything in 2022. Be smart, and focus on the real risks while creating some success stories to gain credibility from your teams. After this you can continue your efforts to increase your level of assurance, operationalize your practices and monitor compliance.