EFFICIENT PRIVACY OPERATIONS

OR ‘A DPO FEEDBACK’

ABOUT ME

Professional in the Data Privacy and Security field for more than 17 years and presently managing a Global Data Privacy Program for a global US asset manager, I believe privacy is one of the most important factors for trust and liberty, and managed my programs, as such.

My previous experiences include managing technical subjects in Data Privacy and Security, as well as, business metrics and reports.

Doing so, I concluded that a pragmatic approach to privacy is a must and the implementation of a series of one-off projects, one after the other, without clear targets will result in failure.

INTRODUCTION

> "When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else."
> — David Brin
> (Author of The Transparent Society: Will Technology Force Us to Choose Between Freedom and Privacy?)

Privacy has always been relegated to a secondary role, an afterthought, with the business considering it as part of a legal checklist. But now, and certainly driven by recent data breaches (like Facebook-Cambridge Analytica), countries or even entire regions across the globe, have implemented new regulations and/or laws, or are working on new draft laws.

Some of the recent breaches have shown that using personal data unlawfully can escalate from disclosing an individual's private life, up to potentially changing elections results.

Everyone is involved at different levels; we all have an impact on privacy. It could be from the amount of our information that we willingly disclose or, as employees, when we handle individual's personal data. This is clear; organisations have a role to play but it starts with each employee of those organisations.

> Would you do something, as an employee, that you would not expect to happen to your own data as a data subject?

Prepare a Privacy program instead of a program top reply to GDPR.

So that when regulation changes, or when a new regulation comes, you just have to adapt instead of building a new project.

"Find a group of people who challenge and inspire you, spend a lot of time with them, and it will change your life."
– Amy Poehler

DEVELOP YOUR NETWORK

As quoted from the CCL white paper, Developing Network Perspective: *Understanding the Basics of Social Networks and their Role in Leadership:*

"Network perspective is a 21st century leadership imperative. Network perspective is the ability to look beyond formal, designated relationships and see the complex web of connections between people in and beyond your organisation."

IAPP

The International Association of Privacy Professionals (IAPP) is a resource for professionals who want to develop and advance their careers by helping their organisations successfully manage these risks and protect their data. In fact, we're the world's largest and most comprehensive global information privacy community.
The IAPP is the only place that brings together the people, tools and global information management practices you need to thrive in today's rapidly evolving information economy.

Industry peer networks

Some examples include:
- European Finance Association
- Independent Health Professionals Association
- WorldSteel Association

Being a member of such groups, I can find ideas as to how peers are implementing specific part of privacy regulations, considering the specific needs of our industries.

Local privacy groups

For example, the Luxembourg group called APDL, aims at facilitating contacts and exchanges of experience and ideas.

It is also a forum where people interested in legal, economic, engineering and research matters can meet and discuss personal data-related issues.

"A GOAL WITHOUT A PLAN IS JUST A WISH"
- ANTOINE DE SAINT-EXUPÉRY

USE A STANDARDISED FRAMEWORK

Organisations that have not already developed their own privacy compliance frameworks should use a standardised framework to ease their path to Privacy compliance.
It is important to agree to a framework, to document obligations and review their relative importance.

I have tested several and a variety of frameworks; I find a combination, depending on the covered area, supply the best result.

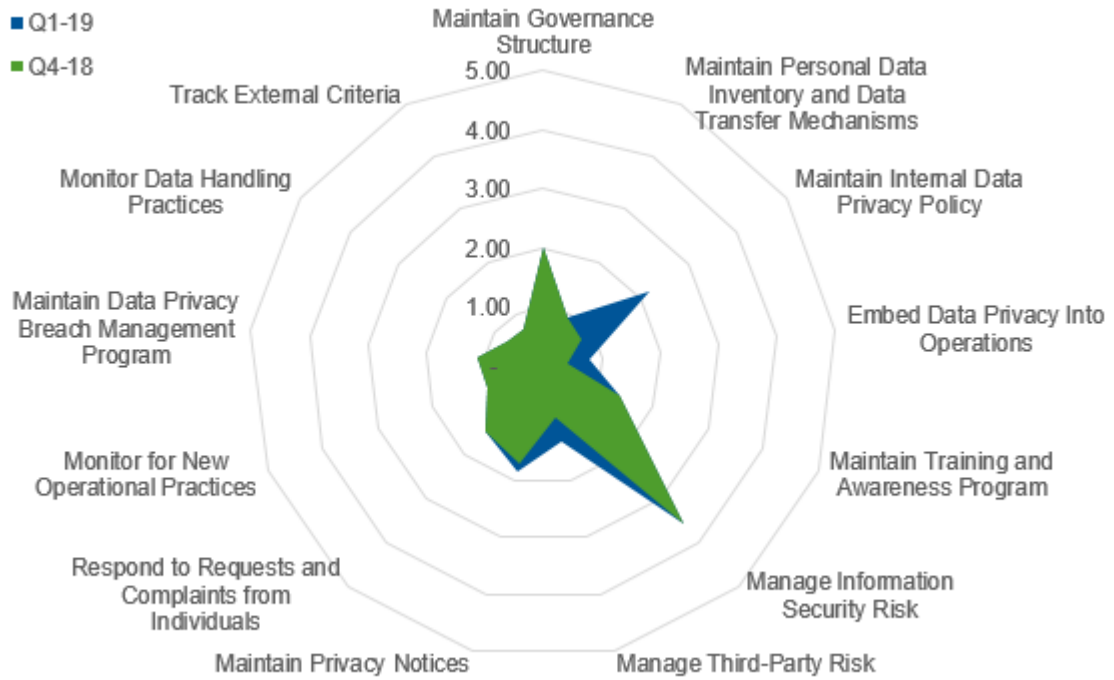
One should be mindful when selecting a framework, some might fit your organisation's profile better than others.

NYMITY PRIVACY MANAGEMENT ACCOUNTABILITY FRAMEWORK™

Maintain Governance Structure Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures	1	
Maintain Personal Data Inventory and Data Transfer Mechanisms Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border	2	
Maintain Internal Data Privacy Policy Maintain a data privacy policy that meets legal requirements and addresses operational risk and risk of harm to individuals	3	
Embed Data Privacy Into Operations Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and ops risk mgt objectives	4	
Maintain Training and Awareness Program Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks	5	
Manage Information Security Risk Maintain an information security program based on legal requirements and ongoing risk assessments	6	
Manage Third-Party Risk Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance	7	
Maintain Notices Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance	8	
Respond to Requests and Complaints from Individuals Maintain effective procedures for interactions with individuals about their personal data	9	
Monitor for New Operational Practices Monitor organizational practices to identify and ensure the implementation of Privacy by Design principles	10	
Maintain Data Privacy Breach Management Program Maintain an effective data privacy incident and breach management program	11	
Monitor Data Handling Practices Verify operational practices comply with the data privacy policy and operational policies and procedures, and measure and report on their effectiveness	12	
Track External Criteria Track new compliance requirements, expectations, and best practices	13	

NYMITY
innovating compliance

Nymity Framework first self-assessment
Example of a measurement methodology



Score	Definition
0	Not addressed yet
1	Addressed locally
2	Addressed and enforced locally
3	Addressed Globally
4	Addressed and Enforced Globally
5	Addressed, Enforced and Audited Globally

Adherence to **GDPR** requirements and principles
73%

Adherence to **CCPA** requirements and principles
6%

"A GOAL WITHOUT A PLAN IS JUST A WISH"
- ANTOINE DE SAINT-EXUPÉRY

OTHER STANDARDIZED FRAMEWORK

BS 10012:2017 Personal Information Management System (PIMS)
The second recognized standard is called BS 10012:2017 Personal Information Management System (PIMS).

NIST
https://www.nist.gov/privacy-framework
The NIST Privacy Framework is currently under development.

GOOGLE
https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf
Google has published a proposed framework for data protection legislation ahead of an appearance before the US Senate to discuss GDPR-style safeguards for consumer data privacy.

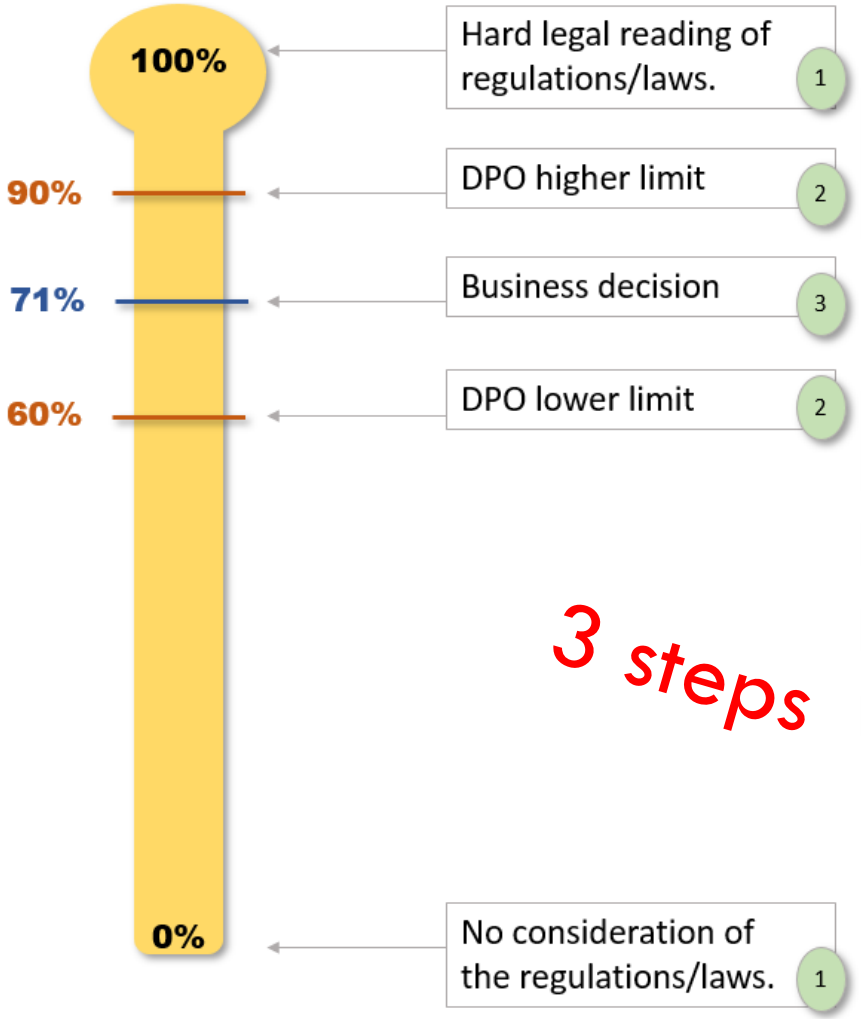
RISK SHOULD BE YOUR MAIN DRIVER FOR SETTING UP YOUR PRIVACY PROGRAM.
THE WORD "RISK" IS WRITTEN 75 TIMES IN GDPR!

RISK BASED APPROACH – COOPERATION WITH BUSINESS

A privacy program must be driven as a good risk management program and must also coincide with the organization's global risk program.
Privacy risk must be considered as a risk for the whole organization, and not as something that a Privacy Office manages in isolation.

Privacy programs and risk management programs are intimately linked.
The value of understanding your data processing activities, as required by many privacy requirements, can be an incredible source of information for your broader risk management efforts. In addition, assessing risk, given the potential impacts of privacy issues, is a key element of protecting personal data for most organisations today. Finding commonalities in your processes and consolidating efforts can improve both programs.

Positioning privacy in decision-making process



GOVERNANCE MODEL

> "Coming together is a beginning.
> Keeping together is progress.
> Working together is success"
>
> - Henry Ford

A Governance model should be designed to help:

- Detect new personal data collection (new process, new tool, new vendor, etc.)
- Detect incidents
- Raise awareness in your organization
- Manage daily privacy operations
- Implement agreed requirements

Setting up a 3-lines of defense model

As mentioned before, this 3-lines of defense model might not be easy to implement in all organisations, however even if not fully supported by different individuals, management should still assign roles to two different individuals. This will strengthen the robustness of your organization's program.

DPO Role

The DPO is not an easy fit for a single individual. The organization should regard this role as a coordinator, using all available resources to reach targets.

Subject matter experts spread in the organization

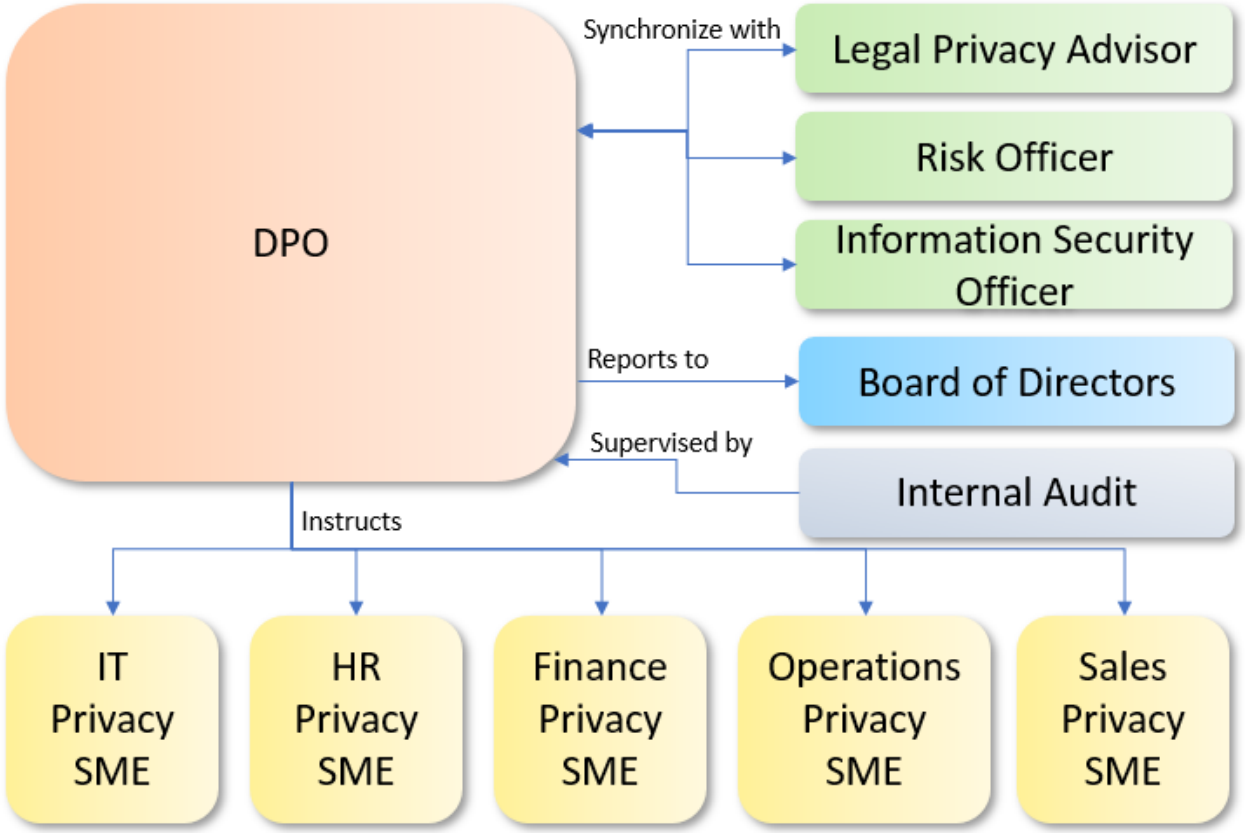
After several attempts and failures, I believe the best model is to have a coordinator, called the DPO or any other name, and the people close to the processing activities report to them, directly or indirectly.

GOVERNANCE MODEL

"COMING TOGETHER IS A BEGINNING.
KEEPING TOGETHER IS PROGRESS.
WORKING TOGETHER IS SUCCESS"

- HENRY FORD

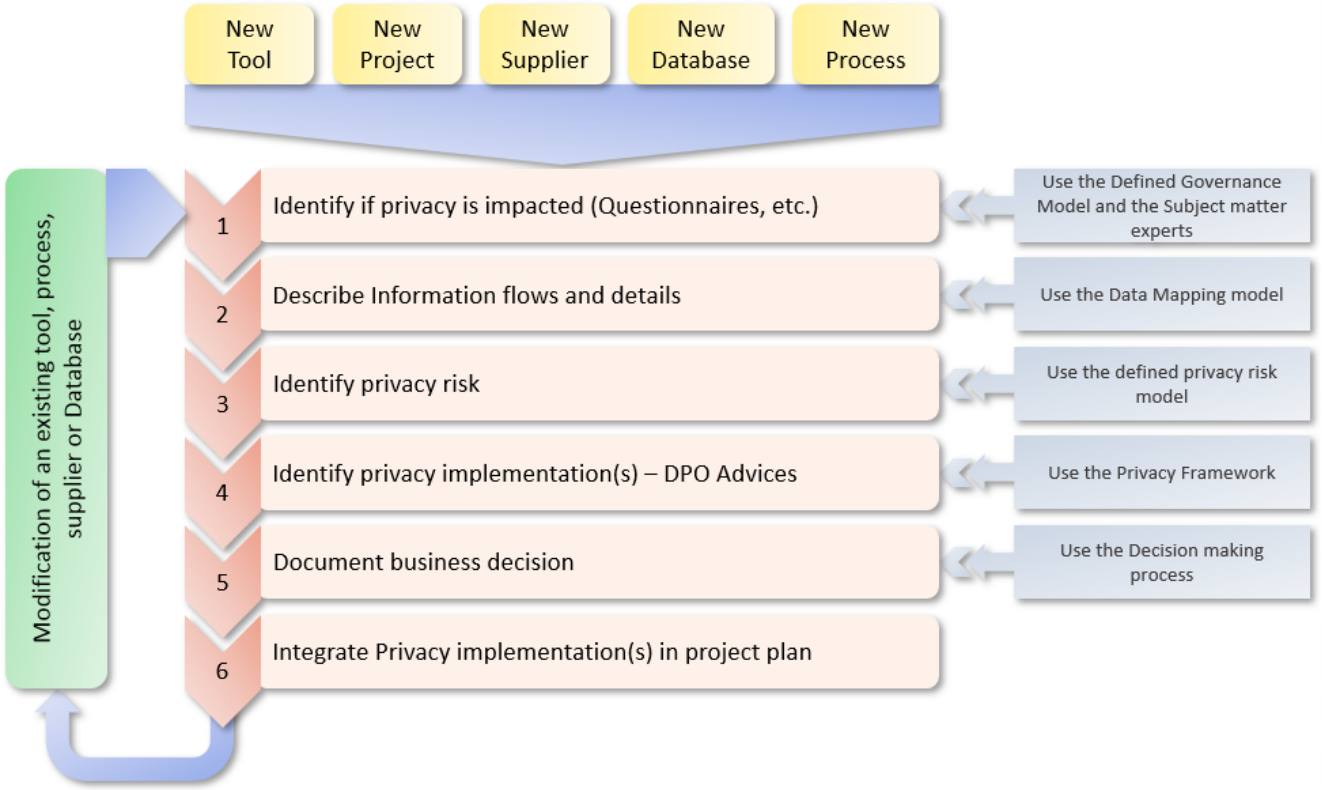
Possible Governance Model



IMPLEMENTING A PRIVACY BY DESIGN MODEL

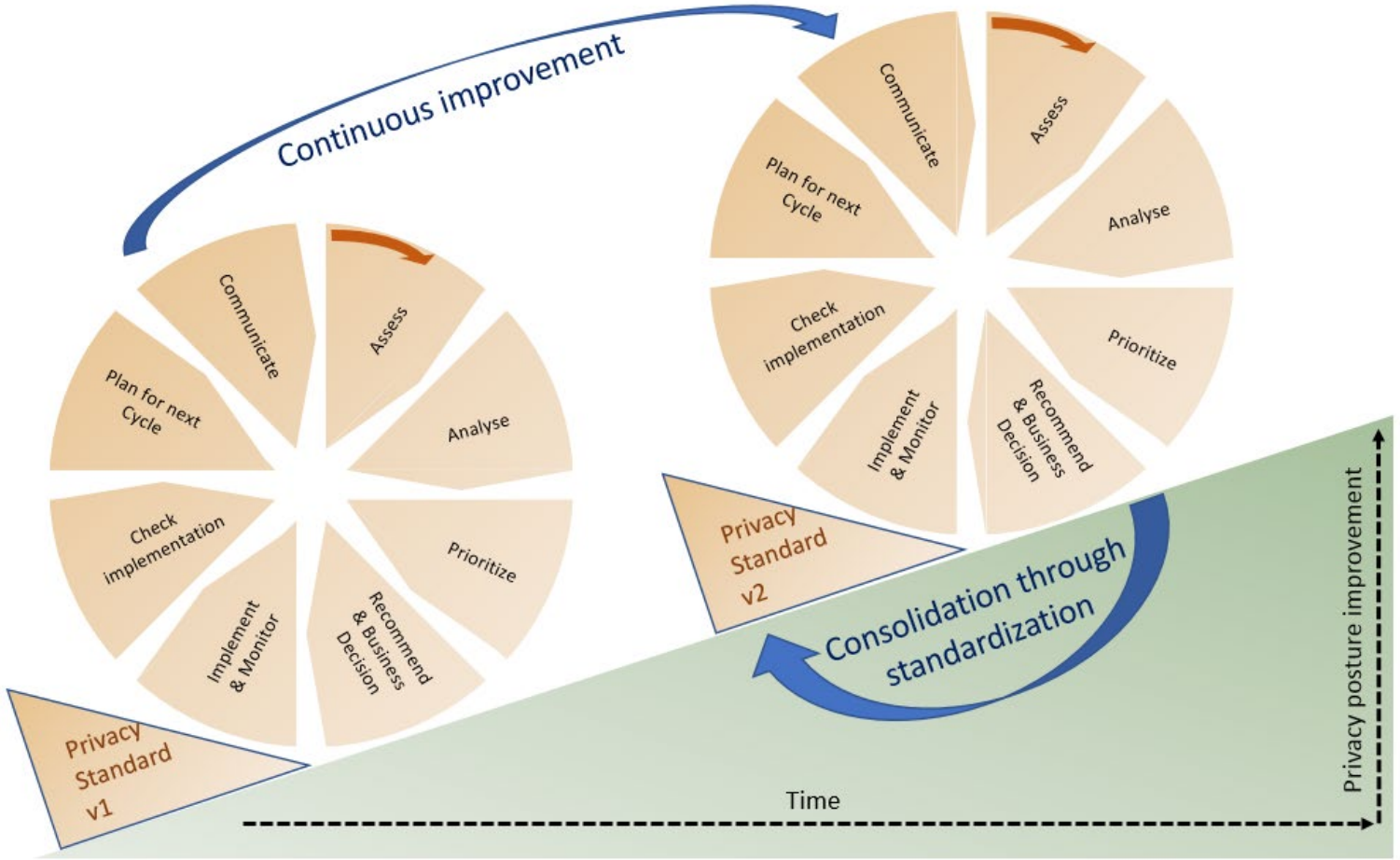
This “new” concept of Privacy by Design has been defined in the GDPR as:

“When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.”



PRIVACY CONTINUOUS IMPROVEMENT PROGRAM

It is unrealistic to believe that every privacy requirement can be implemented fully or to the expected level, in one project.



"Experience is simply the name we give our mistakes."
- Oscar Wilde

INCIDENT/BREACH MANAGEMENT PROCESS

The key success factor for an efficient incident/breach management process is the adherence by all the organization's employees. Therefore, it is not advisable to use a "finger pointing" or "naming and shaming" approach.

Implementing a culture of learning from mistakes will help create a feeling of comfort, encouraging people to report instead of trying to hide errors.

There should be four key steps in responding to a privacy breach:
1. Contain the breach
2. Evaluate the associated risks
3. Consider notifying affected individuals
4. Prevent a repeat event

Tip

Following any breach, assessments and evaluations of how well the matter was handled should be conducted. In some circumstances, preparing a documented breach response plan can assist an organisation in responding to a breach in a timely manner and help mitigate potential harm to affected individuals.

TRAINING/AWARENESS

> "TELL ME AND I FORGET,
> TEACH ME AND I MAY REMEMBER,
> INVOLVE ME AND I LEARN."
> – BENJAMIN FRANKLIN

To avoid human errors or unlawful management of personal data, a proper privacy program needs engagement, from both the employees and from management via an efficient awareness and training plan.

"THE TEMPTATION TO FORM PREMATURE THEORIES UPON INSUFFICIENT DATA IS THE BANE OF OUR PROFESSION."
- SHERLOCK HOLMES (FICTIONAL DETECTIVE)

PREPARE FOR THE FUTURE
DATA ETHICS (ALSO CALLED "BIG DATA ETHICS")

This theme is the founding ambition of landscaping data ethics, as a new branch of ethics that studies and evaluates moral problems related to data including:

- Data usages (generation, recording, curation, processing, dissemination, sharing and use);
- Algorithms (including artificial intelligence, artificial agents, machine learning and robots); and
- Corresponding practices (including responsible innovation, programming, hacking and professional codes).

Concretely, the next step of Privacy should focus on what an organization should do with personal information in order act ethically in relation to its consumers, employees or others, instead of solely considering compliance to existing laws and regulation.

Data Ethics asks the question:
"Would individuals expect me to do this with their personal data, if not, even if it is legally acceptable, should I do it?"

> “Privacy is not something that I'm merely entitled to, it's an absolute prerequisite.”
>
> — Marlon Brando