Whitepaper -

Efficient Privacy Operations

Or

Feedback from a DPO experience

"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?)

AUTHOR
ERIC BEDELL

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 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.

LinkedIn

I also want to thank April Ponton for the reviews of my text.

As always April, you rock!

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?

Everyone tends to agree that it is not an easy move from the old world to the new, especially for interconnected areas of mass data collection. Sometimes one part of an organisation does not know what the other parts are doing. Ever more difficult is the budget allocations for financing something that appears to provide no direct return on investment.

Sizing, targeting, prioritizing and preparing for continuous improvement cycles in privacy management, instead of implementing a succession of one-off projects (per jurisdiction) will surely help your organisation overcome the challenges.

About this eBook

This eBook will give you some non-exhaustive ways to operationalise an organisation-wide privacy program.

The quoted solutions will be mostly free of charge but some of the products, sold by vendors, will also be mentioned. Please bear in mind that I have no advantage in any of the companies mentioned; whichever solution mentioned in this eBook are those that I believe can achieve my goals.

Some of the offered solutions might also not fit your organisation's needs, but nevertheless, they are inspirational; keep in mind too that all investments need to be sized according to your organisation's size, profile and risk appetite.

Privacy is about compliance to regulations and laws and those might differ slightly depending on your organisation's jurisdiction, so this eBook is not meant to replace any lawyer or legal advice for your location. It is always good practice to have an external legal review of your program once designed.

We will discuss principles of compliance but in the last chapter I will recount a completely different mind-set. Instead of examining at what must be done, why not consider what should be done: Data Ethics.

Finally, the expressed advice and suggestions are personal and based on my personal experience, I do not exhort having a single truth, and even if you only heed to one of my points, I would consider it a success ☺.

Let's start now with the real fun!

Develop your privacy network

Size your effort

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."

Individuals do not exist in isolation and their connections provide opportunities, access to valuable information and resources. The people to whom they are connected influence their ideas, attitudes and behaviours. Purposeful (strategic) and authentic networking is the key to developing healthy solutions that prevent insularity.

Relying on formal, vertical channels alone hinders capacity to adapt to emerging issues and challenges. Innovation first requires new and creative ideas. But new ideas are not enough; they must be tested, challenged and even better, already implemented by peers.

IAPP

One of the most efficient networks I am part of is the 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.*
>
> Quote from the IAPP Website: https://iapp.org/

The IAPP is a non-profit association founded in 2000 with a mission to define, support and improve the privacy profession globally. The IAPP is committed to providing a forum for privacy professionals can share best practices, track trends, advance privacy management issues, standardise the designations for privacy professionals and provide education and guidance on opportunities in the field of information privacy.

Being a member has some expense (some sections of the site are free) but the return on the investment is substantial and one can quickly reap the benefits value from some of IAPP's tools.

The IAPP Privacy List (Membership required)

When registered to this list, members can exchange (by email) with all the other registered members.

Several queries and questions are addressed daily, where participants in the forum may receive a multitude of answers from qualified individuals on a global scale.
I have found some useful answers to setup part of my organisation's Global Privacy Program and I also use it as a knowledge base when working with my team.

The Daily Dashboard (Free access)
https://iapp.org/news/daily-dashboard/

The dashboard supplies a news feed focused on Privacy topics. I started using some of the published articles to raise awareness at my organisations by linking news to our Intranet page.
This tool can also be used to demonstrate some regulations (mostly in the EEA) that Privacy is embedded in the Organisation's Culture.

The IAPP Resource Center - Samples, Tools and Templates (Some sections are gratis)
https://iapp.org/resources/tools/

This resource center offers numerous documents, templates and other useful materials as its name suggests.
Users can explore things like lists of data protections authorities, cookies notice templates, external DPO service agreement template, privacy professionals' job descriptions, etc.

Other associations/groups

Industry peer networks

You can also find other associations or groups for specific industry groupings (health, finance, etc.).

Often in these groups, when big enough, there are sections which focus on privacy/information security. Other industry professionals published white papers, information on conferences and seminars on privacy topics can be found in these peer network sites.
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

In some countries, one can find smaller groups, focussing on the local implementation of privacy practices.

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.

Use a standardised framework

Target your effort

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. There should be a method of managing the overarching program to prioritise and achieve each of the obligations. The system of controls and processes can become very complex and intricate; companies need to build their systems on a firm foundation. There is rarely the need to reinvent the wheel when it comes to data privacy controls, as there are internationally recognised standards to assist in building and organising framework.

The three key areas of a privacy compliance framework combine an accountability framework, management systems and compliance with data protection principles.

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.

> Selecting the proper privacy framework must be considered very seriously and the process should not take less than one month in my view.
>
> "A goal without a plan is just a wish"
> - Antoine de Saint-Exupéry

Nymity framework (free but requires registration)

https://www.reuters.com/article/us-germany-politics-cyber/german-data-breach-prompts-calls-for-improved-online-security-idUSKCN1P112M

The Nymity framework will be helpful when as quoted below from Nymity' s website:

Structuring the Privacy Program

Structure your organisation's privacy program based on "the 13 Privacy Management Categories". This process-based approach helps ensure privacy management is implemented not as a project but as an ongoing process.

Benchmarking

Use baseline information to compare the program with other industry peers using the structure of 'Not Applicable', 'Desired', 'In Progress', or 'Implemented'.

Baselining and Program Planning

Quickly baseline privacy management across your organisation by simply removing the 'Not Applicable' privacy management activities and identifying which of the remaining activities have been implemented, planned, or desired.

Understanding Best Practices

Use the framework as a comprehensive and up-to-date listing of privacy management activities. Gain insight into how other organisations are implementing activities to enhance privacy management and to demonstrate their accountability.

Personal note: I have found this framework very pragmatic, easy to use and rapid to deploy. The downside is that it might be a bit excessive for smaller organisations.

ISO standards (free of charge)

ISO19600

The International Organisation for Standardization publishes a standard, ISO19600, aimed at general support for compliance programs instead of any one specific risk. The idea behind ISO19600 is that it provides broad guidance, based on internationally agreed best practice, rather than a requirement standard for which certification is possible. Its use can differ depending on the size and level of maturity of an organisation and on the context, nature and complexity of the activities carried out.

ISO 27001:2013

There are currently two recognised standards or frameworks that could be used as part of a privacy compliance framework to demonstrate privacy compliance including the ISO 27001:2013 **I**nformation **S**ecurity **M**anagement **S**ystem (ISMS).

This one focuses more on the information security side, the prevention of hacks and other system-related threats and is based on risk methodologies.

BS 10012:2017 Personal Information Management System (PIMS)

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

BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR mostly. It outlines the core requirements organisations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals. Easily integrated with other popular management system standards, BS 10012 brings big benefits to companies of all sizes, including:

- Helps to identify and manage risks to personal information
- Supports regulatory compliance with data protection legislation
- Inspires customer trust
- Protects your organisations reputation
- Benchmarks your own personal information management practices with recognised best practice

Other frameworks

Some other frameworks are being developed or are already relatively ready but I have not personally tested them yet, so I am adding them for reference.

NIST

https://www.nist.gov/privacy-framework

The NIST Privacy Framework is currently under development. NIST envisions that it will be a voluntary tool for organisations to better identify, assess, manage, and communicate about privacy risks so that individuals can enjoy the benefits of innovative technologies with greater confidence and trust.

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. The framework is comprised of privacy practices by which Google already abides or with which they could easily comply.

Sound practices combined with strong and balanced regulations can help provide individuals with confidence and that they are in control of their personal information.

Risk evaluation

Focus your effort

This section is inspired by Steve Schlarman's work on RSA's blog.

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

> Risk should be your main driver for setting up your privacy program.
>
> The word "Risk" is written 75 times in GDPR!

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.

Key elements

Several key elements of both privacy and risk programs can be accelerated or strengthened when approached in an integrated fashion.

For example:

- Issues will invariably be identified through activities such as Privacy Impact Assessments (PIA), as well as general risk and compliance activities. A key foundation for both programs is the ability to manage issues generated from risk and control assessments and audits.
- A framework is needed for establishing a scalable and flexible environment to document and manage your organisation's policies and procedures.
- The control universe, i.e. the organisational and technical controls, for privacy, general risk and compliance should be systematically documented and tested.
- Third parties are a critical element in both general risk and privacy. The risks associated with relying on third parties who support critical business processes or process personal data are considerable.

Positioning privacy in decision-making process

I have tested several ways to bring privacy interests into the decision-making process. The most successful way I have determined is when the business has enough information and awareness to make its own risk-based decision.

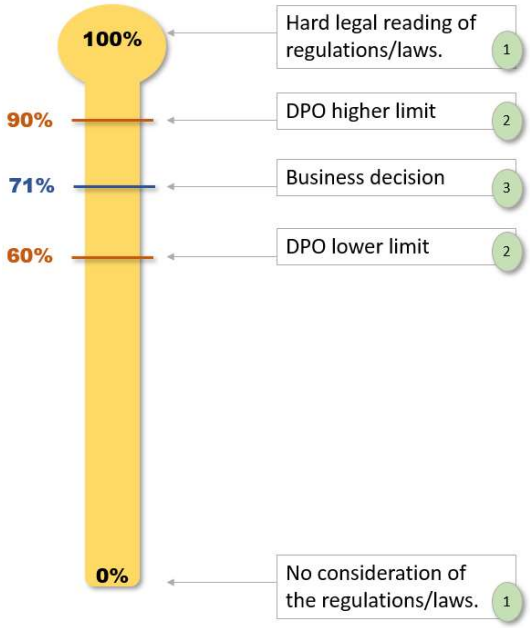

Fig.1 Positioning the DPO advice

Step 1:

- ✓ After reading the law literally, without considering any mitigation factors, you can set up the full implementation with 100% requirements.
- ✓ You can also setup the 0% which does not consider any requirements.

Step 2:

- ✓ Using market knowledge, the organisation's specificities and feasibilities, the DPO or the privacy specialist responsible will set acceptable lower and higher limits for the implementation of requirements.
- ✓ The DPO must also consider the organisation's risk appetite.
  - Below the lower limit, it would become too risky for the individuals about whom personal data is collected and for the organisation (fines, reputational risk, loss of trust from customers, etc.)
  - Above the higher limit, it will be difficult to achieve requirements implications and will cost a lot of effort, time and money for a limited outcome.

Step 3:

- ✓ The business or the process owner should position themself between the DPO limits and decide what will be implemented.
- ✓ During the subsequent reviews of the process, they will be expected to improve implementations to move closer the DPO higher limit level. The DPO will support this effort by recommending gradual improvements.

Risk assessments methodologies

There are numerous risk assessments methodologies but the aim of this book is not to address them in detail, so I will refer to the NIST methodology. It is clear, pragmatic and free; one that can do the job very well.

https://www.nist.gov/sites/default/files/documents/2017/06/05/privengworkshop_preso.pdf

The most important outcomes of this risk assessment should be the risk level of your processing activities so that you can:

- Define reviewing and monitoring periods
- Decide where to invest your effort
- Identify more closely the needs for information protection measures.

Deploy a privacy program

Once a Framework has been selected, based on network capability, external elements and developed in line with risk assessment, the DPO can start to build a privacy program. Most of the requirements and actions should be detailed in the selected framework, I will only focus on the most critical ones here, as required for success.

Governance model

Considerations

One of the most important aspects of a privacy program will be the Governance model.

Size and profile of the organisation will heavily influence the size of your model but I recommend sufficient investment in this model. If challenges cannot be sorted before they become issues, implementation could be impacted/delayed. If enough time cannot be assigned to find and solve challenges, managing the issues' consequences may become even more time consuming and potentially expensive.

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 organisation
- Manage daily privacy operations
- Implement agreed requirements

Setting up a 3-lines of defence model

As mentioned before, this 3-lines of defence 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 organisation's program.

The first line of defence (i.e. the business) must ensure personal data processing activities comply with data protection requirements reviewed by the Privacy Office or whoever acts as the privacy specialist.

The second line of defence (i.e. Privacy Office, security, risk, compliance) must set guidelines for the appropriate technical and organisational controls.

The third line of defence (i.e. audit) must ensure the organisation meets privacy and data protection compliance from top to bottom.

DPO role

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

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

I have been asked several times: “What is the perfect profile for a DPO: legal, technical or audit?”, my personal answer has always been: “the best DPO profile is an individual who knows how to get expertise from a lawyer, a technician and an auditor. No one, alone, can have expertise on such a wide variety of topics.”

Subject matter experts spread in the organisation

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.

> When peeking over a wall, one can only observe.
>
> Only upon passing through the doorway, one is close enough to the action and can interact when needed

Therefore, the more people in the business who can be assigned (even for part of their time) to privacy, the more control the DPO will have when driving the Privacy Program.

Example of a Governance Model

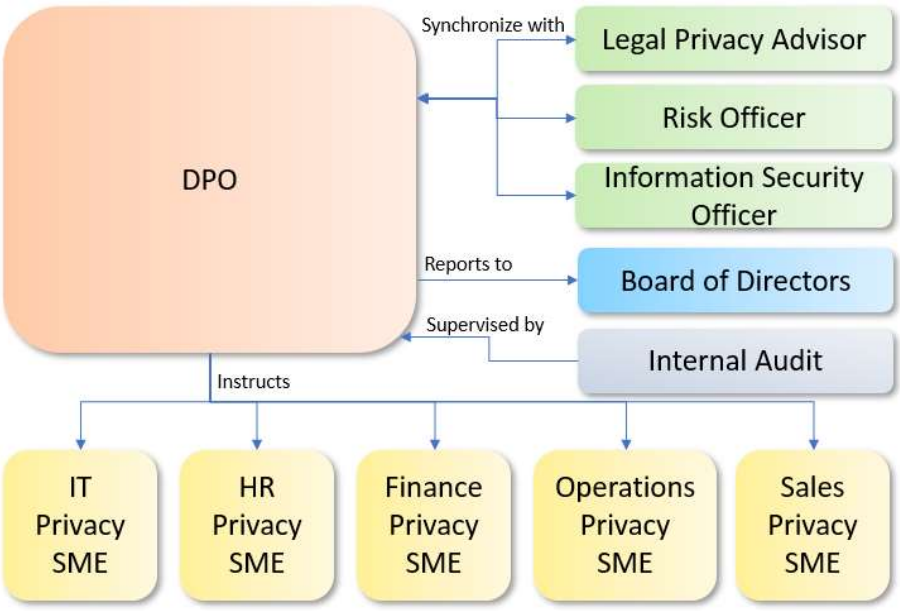

Fig.2: Possible Governance Model

Privacy by Design

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."

This means that for any new tool, process, collection point, etc. the organisation must determine how it can fit with privacy principles.

> Even if it is not mandatory in some laws, a best practice is the earlier privacy requirements are addressed, the easier it is.

A good example is during the design phase of a database, it is easy to decide what information will be collected (including personal information). If the collection of personal data is examined after implementation and that application contains superfluous and unnecessary personal data, it may be

a considerable effort to remove even one field, that might not be needed or justified, without breaking the database's integrity and without impacting downstream systems.

Data Mapping

Before taking any decision and assessment of privacy principles' adherence, it is necessary to know what data the organisation might have, why it is collected, where it is located, and how it is transferred. etc.

Data mapping is a system of cataloguing what data is collected, how it is used, where it is stored, and how it travels throughout the organisation and beyond. There are various ways to achieve this goal, whether through a simple spreadsheet or a dedicated data mapping program, and the extent or limit of data mapping will depend on the size of the organisation.

No matter the size of your organisation most data maps should include the following information:

- What data is collected
- Whether that data is sensitive personal data (such as under Articles 9 or 10 of the GDPR or will cause considerable reputational or financial damage to the organisation)
- The legal basis for processing that data or the "Why" that data is being collected
- Where data is stored and for how long
- Under what conditions data is stored (what protective measures are in place?)
- Where data is transferred /other jurisdictions, within the organisation, to which third-party and where they are located
- What protocols or contractual agreements are in place to protect data during transfers (EU-U.S. Privacy Shield Framework, EU model clauses, Binding Corporate Rules, etc.)

Proper Data mapping is a combination of data inventory and data flow analysis.

Some free online templates for conducting data mapping can be found easily at:

ONETRUST (Free of charge)

https://www.onetrust.com/resources/data-mapping-ebook/

NICVA (Free of charge)
http://www.nicva.org/data-protection-toolkit/templates/document-your-processing-activities

CNIL (Free of charge)
https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Implementing a Privacy by Design model

There should be two entry points in a Privacy by Design model, "new" and "modification of the existing".

This is where having Subject Matter Experts (SMEs) spread throughout the organisation will bring considerable value, as they will help in the identification of such new or modified processes, tools, etc.

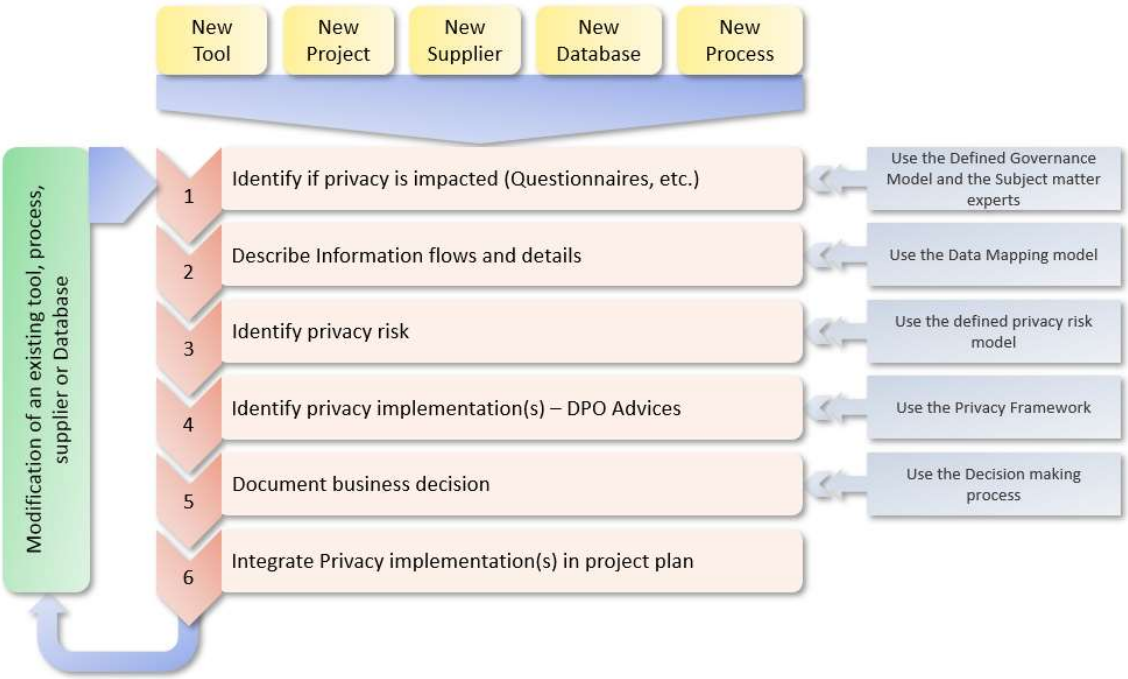

Fig.3: Possible Privacy by Design Model

Step 1:

- ✓ Upon being informed that new data will be collected, managed, transferred, etc. via a new database, tool, process, supplier, etc., there will be a need to detect if personal data is impacted.
- ✓ One way to accomplish this is by using questionnaires.

Step 2:

- ✓ If the questionnaires show that there is an impact on privacy, then details about information flows must be collected. This is where the selected Data Mapping tool can help.

Step 3:

- ✓ Using the selected risk methodology and applying it to the collected information in step 2, one can now assess the risk of this new or modified bit.

Step 4:

- ✓ In order to mitigate the risks, some implantation may be required. These dependencies are based on the risk rating and should be advised by the DPO who can chose them from the selected privacy framework elements.

Step 5:

- ✓ The business needs to decide how and when to implement the advised elements.
- ✓ This must be documented and integrated in the Privacy Continuous Improvement Program.

Step 6:

- ✓ Decided elements which require immediate implementation must be integrated into the project plan. This is why it is important to perform the privacy assessment before the Budget Allocation phase of the project.

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. Privacy is a sort of never-ending project that needs to be managed in a continuous improvement style.

Adapted methods I have used, personally, in review cycles attempt to ameliorate with each cycle, while securing improvements by documenting standards.

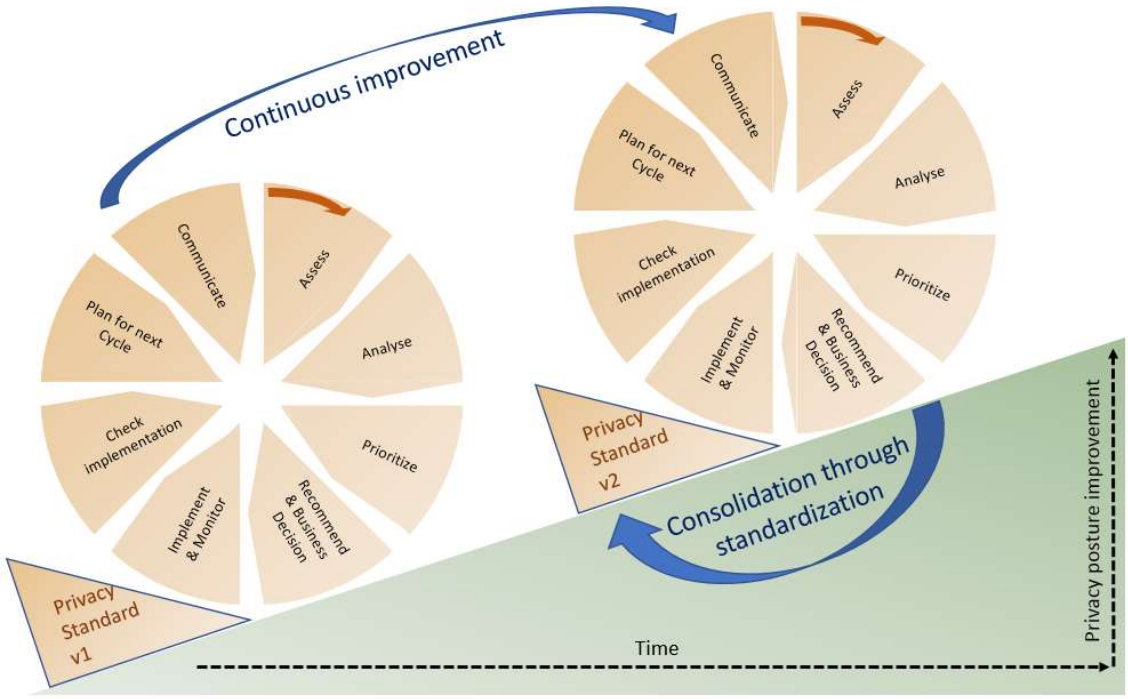

Fig.4: Continuous improvement program

Assess:

- ✓ In order to assess, the DPO should use any information or connections available, this is where a network helps substantially. The result of this phase is a decision if an action must be considered or not.
- ✓ As an example, if many peers on the market are considering a new view on data retention, the DPO needs to assess the organisation's current state regarding this new view and decide if an action is required.

Analyse:

- ✓ After deciding if an action is required, precisely analyse the situation and the risks of action versus no action.

Prioritise:

- ✓ Based on the attributed risk level, it is possible to prioritise and decide when and what will be the initial expected result of the action. Consider improvement cycles at this stage that will help achieve objectives.
- ✓ It is important to define quickly achievable targets, at this stage.

Recommendation & Business decision:

- ✓ As mentioned in the Risk Assessment process earlier, the DPO should only recommend actions, it is the business who must decide if and to what extent the recommended actions will be implemented in this cycle.
- ✓ It is also important to document recommendations, target situations and the current business decisions, and record the acknowledgment of all parties.

Implementation:

- ✓ Implementation can start and the DPO should monitor it.

Check Implementation:

- ✓ When finished, implemented actions must be checked against the initial objectives.
- ✓ Usually this is the best time to test the workability of the implemented solution and if this is not optimal it can be fixed in the next cycle.

Plan for next Cycle:

- ✓ If the objectives have not been fully met in this cycle, then investigate the possible next actions and record them for the next cycle.
- ✓ It is useful to detect any failure of the initial design of the objective and devise mitigating actions for the next cycle.

Communicate:

- ✓ It is very important to communicate with leaders the results and achievements along with the next cycle action points.
- ✓ The more buy-in from the management the program achieves, the faster the cycle will move next time.
- ✓ Remember that this is the perfect time to thank and recognise the work of all participants.

Consolidate:

When a cycle finishes with major accomplishments, the Privacy Standard should be revised to integrate new actions and implementations.

Procedures

Now that the Continuous Improvement Program is in practice, it should be used for the creation of procedures and policies.

Privacy Guidelines vs Privacy Policy

The creation at the outset of a "hard to follow" policy containing a multitude or complex rules is not an advisable way to gain support for adherence by management and colleagues.

My experience includes numerous occasions where organisations have well documented policies and procedures but their employees do not use them because the rules were difficult to follow, did not fit the reality of the business or were, in fact, not applicable. Making matters worse, most of the time the policy and procedure owners were not aware that people were not following them, as there was not any follow up conducted or reassessment in relation to the feasibility of what was mandated.

> "The one who adapts his policy to the times prospers, and likewise that the one whose policy clashes with the demands of the times does not."
>
> - Niccolo Machiavelli, Italian Writer (1469-1527)

One of the best ways to size the Privacy Policy correctly is to start by defining Privacy Guidelines. In contrary to policies, guidelines supply several "Should do" aspects that can be tested. This approach will also raise awareness as to which factors are important for success.

When tested, the "Should do" can simply become the "Must do" as the feasibility was tested before the final definition.

The following policies and requirements should be thought about but the list's needs should be adapted to the organisation's reality.

Privacy Requirements owned by the DPO

- Collection and use of sensitive personal data (including biometric data)
- Collection and use of children and minors' personal data
- Maintaining data quality
- De-identification of personal data
- Review processing conducted wholly or partially by automated means
- Secondary uses of personal data
- Obtaining valid consent
- Secure destruction of personal data

Privacy Requirements to be integrated in other policies

- Use of cookies and tracking mechanisms
- Records retention practices
- Direct marketing practices, e-mail marketing practices, telemarketing practices
- Digital advertising practices (e.g. online, mobile)
- Hiring practices
- Organisation's use of social media
- Bring Your Own Device (BYOD)
- Health & Safety practices
- Interactions with works' councils
- Practices for monitoring employees
- Use of CCTV/video surveillance
- Use of geo-location (tracking and or location) devices
- Policies/procedures regarding access to employees' company e-mail accounts
- E-discovery practices
- Conducting internal investigations
- Practices of disclosure for law enforcement purposes
- Research practices (e.g. scientific and historical research)

Incident/Breach Management Process

The key success factor for an efficient incident/breach management process is the adherence by all the organisation'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.

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

Proposed steps focus only on the Privacy aspects of an incident/breach but a comprehensive incident handling process can be found in the ISO27001 methodology.

There are 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

Each step is set out in further detail below. The first three steps should be carried out concurrently, where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

Step One: Contain the breach

Take whatever steps possible to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that led to the privacy breach, revoke and change access codes or passwords.

If a third party is in possession of the personal information and declines to return it, it may be necessary to seek legal advice on what action can be taken to recover the information. When recovering information, make sure that copies have not been made or, if they have, that all copies are recovered.

Be careful when taking steps to contain the breach and not to destroy information that may be needed to investigate the cause of the breach.

Tip: Reporting all privacy breaches in a designated system will support an organisation to maintain a central log of breaches which could then be used to identify training opportunities or improvements to information handling practices.

Step Two: Evaluate the associated risks

To determine what other steps are needed, assess the type of personal information involved in the breach and the risks associated with the breach. Factors to consider include:

- What type of personal information is involved? Some types of personal information are more likely to cause an individual harm, if it is compromised. For example, government-issued identifiers such as health care identifiers or driver's licence numbers, health information, and financial information such as credit or debit card numbers, will be more significant than names and email addresses on a newsletter subscription list. A combination of personal information will typically create a greater potential for harm than a single piece of personal information (for example, an address, date of birth and driver's licence number, if combined, could be used for identity theft).
- Who is affected by the breach? What individuals have been affected by the breach, how many individuals have been affected and do any of the individuals have personal circumstances which may put them at particular risk of harm?
- What was the cause of the breach? Did the breach occur as part of a targeted attack or through inadvertent oversight? Was it a one-off incident or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the personal information been recovered? Is the personal information encrypted or otherwise not readily accessible?
- What is the foreseeable harm to the affected individuals? Who is the recipient of the information? Is there evidence that suggests theft and was the information the target? Evidence of theft could suggest a greater intention to do harm and heighten the need to provide notification to the individual, as well as law enforcement. What are the possible uses for the personal information? For example, could it be used for identity theft, threats to physical safety, financial loss, workplace bullying, loss of employment opportunities, and humiliation or damage to reputation? What is the risk of further access, use or disclosure including via media or online?

Step Three: Consider notifying affected individuals and authorities

Some regulations specifically require an organisation to notify individuals who have been affected by a privacy breach. And sometimes, a failure to notify may compound the damage for the individuals affected by the breach and reflect negatively on an organisation's reputation. Notification can also demonstrate a commitment to open and transparent governance.

In general, if a data breach creates a risk of harm to individuals, the affected individuals should be notified. Prompt notification to individuals in these cases can help to avoid or lessen the damage by enabling individuals to take steps to protect themselves.

There are occasions where notification can be counter-productive. For example, notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors to consider when deciding whether notification is appropriate include:

- What is the risk of harm to the individual (as determined in the previous step)?
- What steps has your organisation taken to date to avoid or remedy any actual or potential harm?
- What is the ability of the individual to take further steps to avoid or remedy harm? For example, can the individual have a new credit card number issued to avoid potential financial harm?
- Even if the individual would not be able to take steps to fix the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?
- Are there any applicable legislative provisions or contractual obligations that requires your organisation to notify affected individuals?

The logistics of notifying affected individuals will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals. Considerations include the following:

When to notify

In general, individuals affected by the breach should be notified as soon as practicable. Circumstances where it may be appropriate to delay notification include when notification would compromise an investigation into the cause of the breach or reveal software vulnerabilities.

How to notify

It is recommended that affected individuals be notified directly - by telephone, letter, email or in person. Indirect notification – such as information posted on the organisation's website, a public notice in a newspaper, or a media release – should generally occur only where the contact information of affected individuals is not known or where direct notification is prohibitively expensive, or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information on it).

What to say

Tailor the content of the notification advice to the circumstances of the particular breach.
Content of a notification could include:

- Information about the breach, including when it happened
- A description of what personal information has been disclosed
- Assurances (as appropriate) about what personal information has not been disclosed
- What the organisation is doing to control or reduce the harm
- What steps the person can take to further protect themselves and what the organisation will do to assist with this
- Contact details within the organisation where questions or requests for information can be directed

Notifying authorities

Some jurisdictions' laws or regulations require notification of breaches when they represent a substantial harm for individuals, like:

- GDPR
- Most US state laws
- Canada
- Singapore

Processes dealing with this notification requirement should be considered and documented before any breaches happen. When mitigating a breach, time counts and this is not the best time to determine a course of action, procedures and actions should be predetermined for quick reaction from the organisation.

Best practices include adding contact numbers of data protection authorities into the Incident Management Plan, so they are easy to find.

Step Four: Prevent a repeat

Once the breach has been contained, further investigations on the circumstances of the breach and the determination of all relevant causes should be conducted. What short or long-term measures could be taken to prevent any reoccurrence?

Preventative actions could include a:

- Security audit of both physical and technical security controls
- Review of policies and procedures
- Review of employee training practices; or
- Review of contractual obligations with contracted service providers.

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.

The plan should set out contact details for appropriate staff to be notified in the event of a breach, clarification of roles and responsibilities and document processes which will assist your organisation to contain the breach, coordinate an investigation and assess the need for breach notifications.

Communications' Template

In the course of privacy activities, an organisation will have many contacts with the external world (individuals, authorities, the media, third parties, etc.).

In order to keep a consistent tone and to calibrate communications, it is advisable to draft communication templates. This will be even more important for international organisations where communications must be translated into many languages.

The other benefit of such templates is to enable any actor to communicate without requiring approvals from the DPO each time, quickening response times.

Some templates could be created for:

- Press releases for marketing organisation's privacy program
- Press releases for breach declaration
- Reply to individuals' rights requests
- Reply to third parties due diligence questions
- Reply to authorities' standard requests

Training/Awareness

To avoid human errors or unlawful management of personal data, a proper privacy program needs engagement, from both the employees and from management.

Building an efficient awareness and training plan is a key success factor to achieve this commitment. The plan should take into consideration an organisation's situation, risk appetite and type of activities but must also consider external context, such as privacy related news.

Another key aspect is how training and awareness plans are delivered. One successful self-tested way is to involve people specifically within their role; it is advisable to not issue standardised presentations one after the other.

> "Tell me and I forget,
> teach me and I may remember,
> involve me and I learn."
>
> – Benjamin Franklin

DPO awareness

One of the key actors who needs to be trained and maintain awareness, is the DPO. Cultivating a strong knowledge based on external factors, like privacy news, court decisions and peers' actions can support re-designing or re-targeting the organisation's goals for its privacy program.

Detect modifications of laws/regulations and court decisions

One the most important aspects to monitor is the legal privacy landscape. A DPO should know prior to any enforcement date, all new or modified laws/regulations containing privacy regulation.

This objective can be achieved by a combination of different means:

- Some tools supply legal landscape surveillance capabilities (like Nymity or OneTrust)
- Several associations or working groups supply dashboards (like IAPP)
- LinkedIn usually provides a lot of information through posts by your network connections
- Some law firms offer a surveillance service

Whatever plan is set, it is important to use the information gained from these awareness exercises, to adapt the organisation's privacy goals into concrete actions.

i.e. If the news mentions that a peer organisation has been fined for not being complaint with paper box storage, the organisation must assess its own position in that respect and decrease the likelihood score of the risk related to storage management.

Use your network

One way to achieve this view is by using your network and connections to summarise news which can be added to company informational feeds or blogs to keep the organisation informed as a whole.

This is the ideal way to benchmark the organisation's implementation efforts and compare those with those of peers.

Participate in webinars and seminars

Other mechanisms where a DPO can find useful knowledge and information are seminars (mostly free of charges) offered regularly by law firms, vendors or even data protection authorities.

Training employees

Involve your training audience

As mentioned before, a good training and awareness plan needs to involve employees and not just cover standardised aspects.

Several entry points can be used to create involvement:

- Using an incident as an example, through group analysis and explanation of what was correct or incorrect, provides context to the training
- Usage of an external news, like a peer being fined for inappropriate personal data management, gives more traction and connection to reality
- Using an open queries page and employees' real questions as training material connects employees to the material

Another way to keep the audience focused is by changing the training format as often as possible.

Several formats could be used like:

- Onsite training with different invitees
- E-Learning sessions
- Quiz sessions
- Lunch and learn sessions
- Poster campaigns

Different content for different roles

Consider a training plan which addresses the audience's level of access to personal data can help target the presented content.

If the job role entails an increased exposure to sensitive information, those individuals must be trained to a higher level.

i.e. A Human Resources director will handle more sensitive information than a receptionist, therefore, the training most be more focused to the appropriate risks.

Keep evidence

Most auditors and regulators will ask what kind of efforts the organisation has made to protect personal data. The first measure will be to answer that it trains its employees on how to properly manage and protect personal data.

In that respect everything that can prove what the organisation is doing in practice will be helpful, like:

- Training plan (per role level)
- Participation rate to trainings
- Score of quiz and tests
- Training material

Fig.5: example of an awareness and training plan

Reporting

Another, often forgotten, aspect of awareness is reporting to senior management. In order to be financed, a privacy program need to be visible, not only because of its risks but also for its achievements. I have been successful in achieving budgetary goals in most instances because my programs were very transparent to senior management.

Several key indicators should be considered:

- Daily activities (replies to individual requests, vendor management activities, number of breaches, etc.)
- Improvement activities (actions to implement the Privacy Framework, remedial actions, etc.)
- Workload of the Data Privacy office (tasks and their assignments, utilisation ratio, etc.)

> "Trust, honesty, humility, transparency and accountability are the building blocks of a positive reputation. Trust is the foundation of any relationship."
>
> - Mike Paul, Baseball player

Prepare for the future

Data Ethics (also called "Big Data Ethics")

Data science provides huge opportunities to improve private and public life, as well as our environment, consider the development of smart cities or the problems caused by carbon emissions. Unfortunately, such opportunities are also coupled with significant ethical challenges. There is an increasingly extensive use of ever more data, often personal or sensitive big data coupled with a growing reliance on algorithms (including machine learning, artificial intelligence and robotics) to analyse it, in order to shape choices and to make decisions. The gradual reduction of human involvement or even oversight of many automatic processes pose pressing issues of fairness, responsibility and respect of human rights.

> "The temptation to form premature theories upon insufficient data is the bane of our profession."
>
> - Sherlock Holmes (fictional detective)

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).

These issues should be considered in order to formulate and support morally positive solutions, as opposed to implementing mandatory required solutions.

Data ethics build on the foundations already laid by computer and information ethics while at the same time, refining the approach endorsed so far in this research field. It does so by shifting from the abstract of ethical enquiries as information-centric to data-centric. This shift brings into focus various moral dimensions of all kinds of data, including data that never translates directly into information but can be used to support actions or generate behaviours. It highlights the need for ethical analysis to concentrate on the content and nature of computational operations and the interactions among hardware, software and data rather than on the variety of digital technologies that enable them. Lastly, it emphasizes the complexity of the ethical challenges posed by data science.

Concretely, the next step of Privacy should focus on what an organisation 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?"

Data Ethics Framework Principles

1. Equality

Democratic data processing is based on an awareness of societal power relations that data systems sustain, reproduce or create. When processing data, special attention should be paid to vulnerable people, those who are particularly vulnerable to profiling which may adversely affect their self-determination and control or expose them to discrimination or stigmatisation, for example due to their financial, social or health-related conditions. Paying attention to vulnerable people also involves working actively to reduce bias in the development of self-learning algorithms.

Big Data should not interfere with human will, since Big Data analytics can moderate and even determine who we are before we make up our own minds. Organisations must begin to think about the kinds of predictions and inferences that should be allowed and those that should not.

Big Data should not institutionalize unfair biases like racism or sexism. Machine learning algorithms can absorb unconscious biases in a population and amplify them via training samples.

2. Radical Transparency

Data processing activities and automated decisions must make sense for the individual. They must be truly transparent and explainable. The purpose and interests of data processing must be clearly understood by the individual in terms of understanding risks, as well as social, ethical and societal consequences.
Tell individuals in real-time what sort of data is collected and for which purpose. Users understand that nothing is for free; they just want to be told intentions/purposes. Otherwise it would be like receiving a free book from the local bookstore and discovering later that the store charged your credit card. Always permit users to understand what data is collected and allow deletion, in case the data is not stored anonymously. Where an organisation wants to offer free services, it should be honest and transparent so users are advised of the organisation's intentions to when offering 'free' service. If possible, also create a paid version of the service that does not collect any data but still allows the user to use the service provided.

3. Simplicity by Design: give individuals data control

Users should be able to adjust simply and easily any privacy setting and determine what they want to share or not. This process should be simple and understandable. Companies should not make it a difficult process to understand what elements change on a regular basis. Privacy policies should be simple and understandable.

A good example of how not to amend a privacy policy is Facebook; they change their privacy policy every few weeks or months. Although changes to any setting are allowed, it is often difficult to navigate it. In addition, their privacy policy contains more words (5,830) than the United States Constitution (4,543 words not counting the amendments).

Humans should be in control of their data and even empowered by their data. A person's self-determination should be prioritised in all data processes and the person should be actively involved regarding the data recorded about them. The individual must have primary control over the usage of their data, the context in which his/her data is processed and how it is activated.

4. Preparation and Security are Key

With more data being collected and stored, organisations acquire valuable assets. Data is becoming the new gold, as such, an increasing number of criminals want it. Organisations should define upfront what information they actually require to conduct business and what information they can do without. Develop a crisis strategy, in case the company gets hacked and any data is stolen, which happens quite regularly lately, considering the hacking of Facebook, Evernote or LinkedIn. Or even better, test data scientists and IT personnel who perform ethical hacks.

5. Make Privacy Part of the DNA

When organisations embrace transparency, simplicity and security, customers will embrace them. Ignore these principles and customers will eventually ignore the organisation. It is a simple fact.

Hiring a Chief Privacy Officer or a Chief Data Officer (CPO) who is also responsible for data privacy and ethics will modify the organisation's DNA. Making the CPO accountable for whatever data is collected, stored, shared, sold or analysed as well as how it is collected, stored, shared, sold or analysed will mutate even this DNA. Big Data privacy and ethics are too important not to be discussed at C-level (executive level).

Certification(s)?

An organisation may be wondering whether it is worth the cost and trouble of getting Privacy certifications for its business. According to dozens of studies, the answer is a resounding YES!

In fact, 98% of companies with ISO certification rated it either a good or very good investment, according to a 2009 United Nations survey. A 2012 review of 82 studies on ISO found that certification had "clear benefits" in terms of operations, customer satisfaction and employee engagement.

A Privacy Certification:

1) Promotes best practices -- Standards give access to internationally recognized best practices across the business. Standards exist for everything from quality management to environmental performance, information security, food safety, risk management, health and safety and, of course, Privacy.

2) Helps to become more productive —Adhering to standards requires the organisation to clearly define, document and monitor business processes. It should set objectives and measure progress. This work is critical to building a lean, productive business.

3) Keeps customers happy —Standards help keep customers satisfied by improving complaint management, quality control and client satisfaction. Research indicates one of the top benefits from certification is reduced customer complaints.

> "Every business wants more clients but if you don't keep them satisfied, you'll just get more unhappy clients."

4) Improves revenues — Three out of five companies that adopt an ISO standard increased their revenues, according to a 2015 analysis of 92 studies. The revenue increase was significantly higher than for non-certified companies. The best performance results occur in companies that make a sustained effort to improve operations, not just before the next recertification audit. It is a good investment but it comes with some effort.

5) Opens doors to new markets—Standards give an organisation access to new markets. For example, it may be eligible for government contracts that require adherence to certain standards. Or, perhaps, it will be able to join the supply chain of a larger company or a megaproject. Many standards are recognised worldwide and can increase your credibility with customers in international markets.

6) Fosters team commitment—Meeting standards can help foster a more engaged and productive workforce. Certified businesses report better job satisfaction, turnover, absenteeism, employee motivation and manager-employee communication, according to the 2012 research review. The process of certification brings together managers and employees to work towards common objectives, using consistent processes. Managers and employees develop more commitment to improving the business.

7) Applies to all sizes—Certification is useful for businesses of all sizes, even those with only a few employees. Smaller businesses sometimes pursue certification because of supply chain requirements or when they want to adopt best practices in their operations.

Considerations

The organisation needs to select the proper certification scheme (local or global), so that it is meaningful for its size, culture and type of business. The goals and objectives in the aim of becoming certified should be considered when selecting the certification scheme.

i.e. A company managing financial personal data should look at a certification scheme that is recognised in the Financial Industry. Or if an organisation wants to be certified to reply to a Request For Proposal (RFP), it needs to evaluate certification schemes used by the RFP sender.

Properly defining the scope of the certification is also key. Many different things can be certified:

- Applications
- Websites
- Organisation as a whole
- Processes

Global certifications

Certifications will help a global organisation to prove consistency in its different locations. It will also ease the response process for Due Diligence from its customers.

The NIST has created one that can be found here:
https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering

The IAPP is working on a privacy one that can certify organisation as a whole:
https://iapp.org/certify/programs/

Local certifications

Some regulators, mostly in Europe, have developed certification schemes. Those will help for the organisation's relationship with regulators and may ease audits.

The Luxembourg regulator (the CNPD) introduced the CARPA recently. It is being discussed for approval with the European Data Protection Board (EDPB).

Consider Employees' certifications

Several certifications for employees exist and the most recognised ones are those from the IAPP.
https://iapp.org/certify/programs/

Having certified employees in key roles will help an organisation to demonstrate its compliance to Privacy principles. It is also demonstrates the willingness of the organisation to invest into Privacy, which will ease audits of various regulations.

Marketing/competitive advantage

To approach Privacy as a revenue-generating opportunity, certification and visibility are recommended.

The reality is, all customers want trust and control over their personal data, and this is precisely what a privacy framework enables. If companies can move past viewing privacy programs as expensive, overwhelming hurdles and instead view them as incentives to provide customers what they want, both sides stand to benefit. When customers know exactly how and why their data will be used (relating to Data Ethics), it is likely they will be more open to sharing their information with companies, moving forward. With more focused, meaningful customer data available companies can obtain further knowledge about each customer and use that information to create more relevant interactions and offers.

While GDPR is the first big step toward improving Data Privacy and customer trust, it is not by any means the final solution. In other words, achieving GDPR compliance and ultimately global Data Privacy, considering Data Ethics principles, is going to be a process - a long, laborious one - but this is the catalyst for companies to create the framework.

By considering Privacy as an opportunity to cultivate smarter, more effective customer data strategies and technologies, companies can provide customers with explicit, intelligent choices over the experiences that interest them. By delivering more relevant customer experiences, companies can finally become truly customer-centric, thereby generating greater brand loyalty and stronger bottom lines -- all the while complying with Privacy regulations, including the "infamous" GDPR.

But this fact is not universally recognised yet. Research from IDC demonstrates that across the board there is roughly a 50:50 split between companies that see GDPR as an opportunity and those who regard it as an obstacle. This split is more dramatic in less regulated industries, where businesses are far less likely to recognize the potential advantages associated with GDPR. For instance, 80% of organisations in the manufacturing sector believe GDPR is an obstacle because they are less experienced with processes around data regulation and compliance.

Considering this, an organisation that can demonstrate GDPR compliance and effective control over its data will be at an advantage to competitors who cannot make the same claims. Compliance with the Privacy principles, and even more with Data Ethics principles, will soon become a point of differentiation. The sooner businesses are compliant, the quicker it will be that they stand to reap the rewards, enabling them to stand out from the competition.

Conclusion

I hope this whitepaper helped you to oversee how Privacy ties in with your organisation's goals.

With a well-balanced Privacy Program, it can be assured that the organisation will be successful; with Privacy no longer an afterthought, it is now integral in the organisation's DNA. When this level of merging is reached, I am convinced that your organisation will also benefit from all the effort, not only the pecuniary aspects but also by gaining the trust of its consumers and its employees.

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