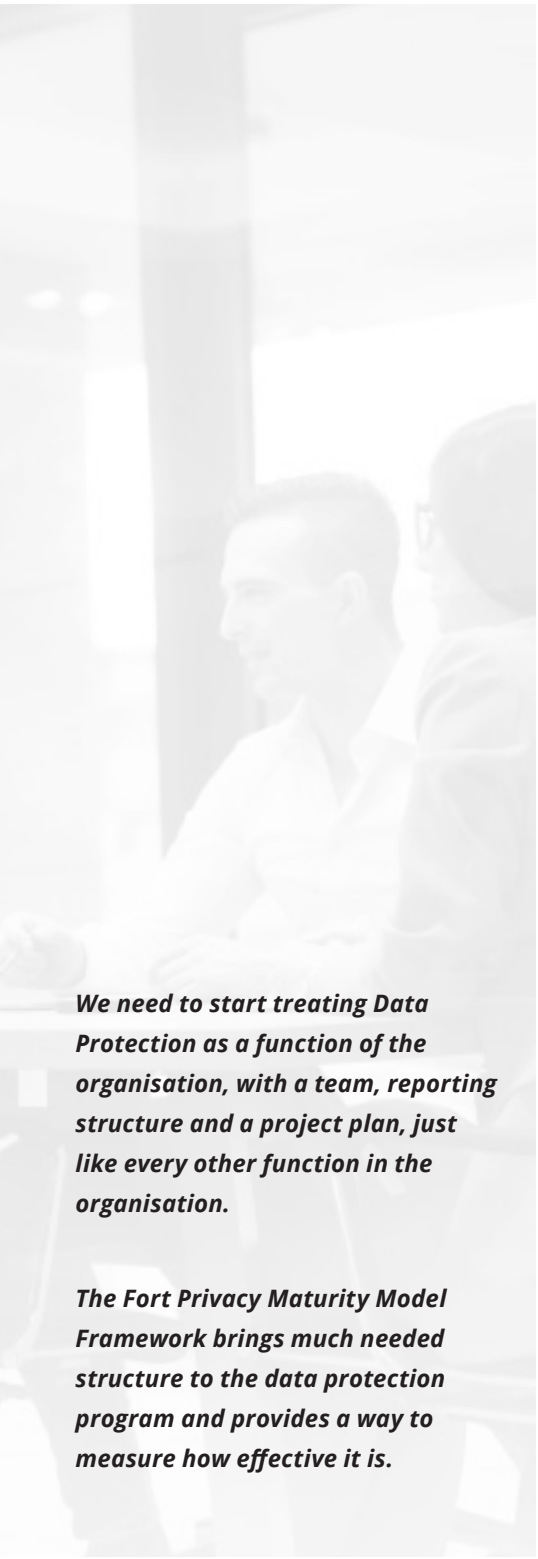
INTRODUCING THE FORT PRIVACY MATURITY MODEL FRAMEWORK

FORT PRIVACY

Getting Data Protection Right

www.fortprivacy.ie



We need to start treating Data Protection as a function of the organisation, with a team, reporting structure and a project plan, just like every other function in the organisation.

The Fort Privacy Maturity Model Framework brings much needed structure to the data protection program and provides a way to measure how effective it is.

"Organisational structures of today demand too much from few, and not much at all from everyone else"

Gary Hamel

This quote from Gary Hamel is very apt for data protection structures of today. In 2017 the IAPP estimated that the GDPR would create a need for 75,000 Data Protection Officers globally. A recent study estimates the number of registered Data Protection Officers in Europe is more like 500,000.

In our recent blog we identified Data Protection Officers as a new breed of superhero. All superhero's need a bit of a helping hand sometimes and we have developed the Fort Privacy Maturity Model with this in mind.

The GDPR is a complex piece of legislation and on it's first birthday, the importance of identifying a clear and structured approach to the data protection compliance program is clear. Many organisations have taken the approach of appointing a DPO (who is sometimes playing a double act on the C-suite team as the CTO, CEO, COO) in the hope that this will "tick the GDPR box".

This is not the right answer.

Embedding a data protection culture is key to compliance

Having the right data protection culture in the organisation requires buy in from everybody from the top, down to the most junior members of staff.

If we want to see results, we need to be proactive and not reactive, we need to work collectively and not individualistically.

We need to start treating Data Protection as a function of the organisation, with a team, reporting structure and a project plan, just like every other function in the organisation.

Effective implementation and management of the data protection program is critical to the success of the program. An organised and structured program will increase sales, reduce costs, improve staff morale and most importantly develop the right data protection culture within the organisation.

Taking a MATURE approach to compliance

Applying a structured approach to the data protection program ensures it lines up with the risk appetite of the organisation and addresses the areas that most require attention as a priority.

The Fort Privacy Maturity Model Framework brings much needed structure to the data protection program and provides a way to measure how effective it is.

The Fort Privacy Maturity Model Framework allows us to:

- identify and benchmark the current level of maturity of the organisation;
- assess the required levels of maturity;
- identify the most important areas that need work; and
- determine how to get there.

We use the Fort Privacy Maturity Model Framework approach for our client projects to carry out Data Protection Audits, to deliver outsourced Data Protection Officer services and in the design of our advanced Data Protection Program Management Training.

The use of the framework helps to move some of the roadblocks that are currently preventing progress being made and prevent the DPO from being isolated in their endeavours. Applying the Maturity Model helps to drive the culture of data protection in the organisation, secure buy in from senior management, enhance the reputation of the organisation and ensure clear delegation of responsibilities and identify measurements for success.

Using Maturity Models as a risk-based approach

Organisations need to address compliance with GDPR within the context of the data processing activities they are carrying out. Data Protection is essentially a risk and compliance activity. For instance, a large hospital dealing with sensitive patient information will need to take a very different approach to compliance compared to an SME selling widgets and maintaining sales and marketing lists.

The Fort Privacy Maturity Model supports the risk and compliance approach in a very effective way.

An organisation can assess its risk profile against the categories in the Maturity Model and set compliance priorities based on the outcome.

For instance, an organisation may identify that it is at a Level 2 in Breach Management and Data Subject Rights Management. It receives very few communications from data subjects seeking to exercise their rights, so Data Subject Rights Management is low risk. The organisation may prioritise getting to Level 3 in Breach Management before Data Subject Rights Management as a result.

The Use of Maturity Models in Industry

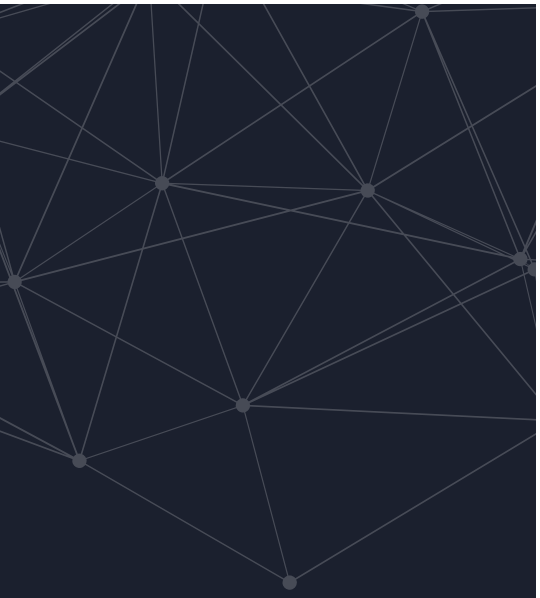
Maturity Models have long been used by industry to measure the ability of an organisation to continuously improve in a discipline.

If an organisation has a high level of maturity and an incident arises, the organisation will have the right structures in place

(i) to address the issue at hand and

(ii) to learn from that issue and implement changes to its program to reduce the impact of the incident and the likelihood of the incident recurring.

One of the more universally renowned Maturity Models is the CMMI (Capability Maturity Model Integration). The use of Maturity Models is not new to data protection. The US and Canada brought us the AICPA/CICAs Privacy Maturity Model based on the Generally Accepted Privacy Principles (GAPP) in 2011. Eight years on and Fort Privacy has extensively restructured and updated these to align with the GDPR, reflecting key concepts, terminology and requirements from the EU Law.



LEVEL 5
OPTIMISED

LEVEL 4
MEASURED

LEVEL 3
IMPLEMENTED

LEVEL 2
ESTABLISHED

LEVEL 1
AD HOC

Why use the Maturity Model Framework?

Fort Privacy has consistently seen client's struggle with their data protection programs. From those who only want to do the bare minimum to those who are going for gold! Organisations struggle consistently to understand how compliant they are at any moment in time, how compliant they need to be and how to assess themselves internally and indeed against other similar organisations.

The Maturity Model Framework addresses these issues and more.

Unfortunately, some organisations still think that compliance with the GDPR is a one-time endeavour (a resource here, a few policies there and that's me done!) when the reality is clearly very different.

The GDPR is written as a proactive regulation with ongoing compliance obligations that need to be kept on top of daily. It is not enough just to be compliant; you also need to demonstrate compliance.

In order to do that properly an effectively structured data protection program is key, and Fort Privacy has developed that structure using the Maturity Model Framework. It helps to bring order to the chaos and ensures that there's a very clear understanding of where the organisation is at in its compliance activities.

This is so important for the DPO and Privacy Team who sometimes can be left feeling that the immaturity of the organisation is their responsibility. A common acknowledgement of the current level of maturity of the organisation by management can give the organisation a real sense of purpose, drive and achievement instead of just flailing around from one crisis to the next with no coherent approach.

The 5 Levels of Maturity

The Maturity Model defines a five-level progression path of increasingly more organised and structured and purposefully more mature processes.

- Chaos reigns at level 1 in an "ad hoc" ill-defined and undocumented world. There is not enough documentation to enable any level of success or adherence to the requirements of the GDPR.
- At level 2 (Established) the organisation has, at the very least, documented the requisite procedures and processes that form part of its data protection program.
- An organisation meets the requirements of Level 3 (Implemented) when it has implemented and adopted the documented procedures and processes.
- Level 4 (Measured) captures the quantitative measurement of the effectiveness of the adopted procedures and processes.
- Level 5 (Optimised) is where procedures and processes are constantly being improved after reviewing the feedback and measurements being reported.

The 10 Categories

The Fort Privacy Maturity Model identifies 10 categories that the levels of maturity can be applied to. These address key compliance areas of the GDPR as follows:

- **Governance** - the organisation defines, documents and communicates Data Protection policies and procedures and assigns roles and responsibilities for the organisation's processing activities
- **Accountability** – the ability to demonstrate compliance and account for all data processing activities
- **Transparency** - the organisation provides statements to data subjects about its privacy policies and procedures and communicates the purposes for which personal data is collected, used, retained and disclosed
- **Legal Basis Management** - a legal basis exists for the collection, use and disclosure of personal data and the relevant options related to such processing are made available to the data subject
- **Data Management** – the use of personal data is managed in the organisation including, cataloguing of personal data; limiting use to the purposes identified; minimising personal data collection; ensuring accuracy; and retaining data for no longer than is necessary.
- **Data Subject Rights Management** - policies and processes are in place to facilitate and respond to Data Subjects who invoke their rights
- **Data Transfer Management** - disclosure of personal data outside the organisation (to third parties or intra-company transfers) is consistent with the purpose of processing and is only undertaken with the required controls in place
- **Security** - appropriate technical or organisational measures are in place to ensure security of the personal data
- **Data Breach Management** - the organisation provides and implements policies and procedures for reporting and managing personal data breaches.
- **Risk and Change Management** - the organisation provides and implements a framework for Data Protection risk and change management

Organisations are likely to be at different levels of maturity in each of the 10 categories.

Just like decathletes, DPOs and Privacy Teams need to prepare themselves for each category. A decathlon has 10 events and the successful decathlete and their team work through a regimented training program over a number of years continuously assessing progress and adjusting the program.

Similarly, the DPO (Management and the Privacy Team) need to work through the data protection program for each category improving areas where there are gaps and addressing issues and assigning priorities.


Governance

Accountability


Transparency


Data Subject Rights Management


Data Transfer Management


Legal Basis Management


Data Management


Data Breach Management


Security


Risk & Change Management

Each category of the Fort Privacy Maturity Model is broken down into a number of requirements and the requirements have individual maturity descriptions. An example of one of the requirements under the Governance Category is presented as follows:

CATEGORY	**Governance**
CRITERIA	**Data Protection Compliance**
DESCRIPTION	**Resources are provided by the organisation to implement and support its Data Protection Policies & Procedures.**

AD HOC

Resources are only allocated on an "as needed" basis to address privacy issues as they arise

ESTABLISHED

Privacy resources are in place; however, they may not have appropriate support or skillset

IMPLEMENTED

Individuals with responsibility and/ or accountability for privacy are empowered with appropriate authority and resources and have the right qualifications. Such resources are made available through-out the organisation and staff are aware of their existence.

MEASURED

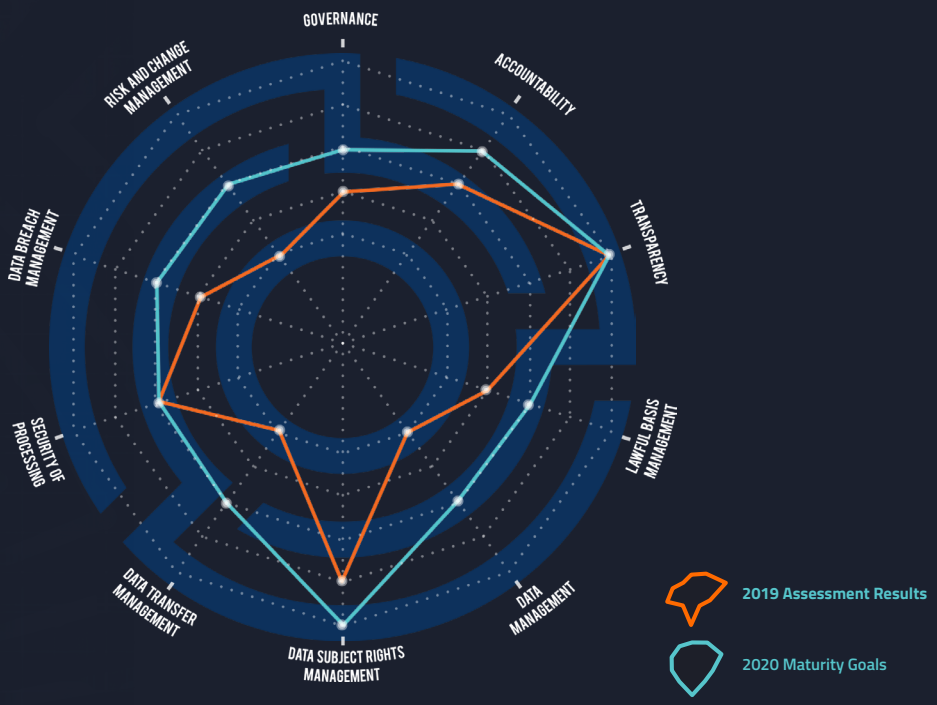
Management ensures that adequately qualified privacy resources are identified and made available throughout the organisation to support its various privacy initiatives. The effectives of such resources are measured, and training is provided.

OPTIMISED

Management annually reviews its privacy resources and seeks ways to improve the program's performance, including assessing the adequacy, availability and performance of its resources. Changes are made as required

THERE ARE KEY COMPLIANCE ARTEFACTS INCLUDING POLICIES, PROCEDURES, CATALOGUES, LOGS AND CONTRACTS REQUIRED TO ACHIEVE A HIGH LEVEL OF MATURITY IN EACH CATEGORY.

The Fort Privacy Maturity Model Framework helps organisations to set goals and review the effectiveness of the data protection program.



It's time to steady the ship

One year on and most organisations have, at the very least, grasped the enormity of the task.

Those still clinging on to the Y2K comparisons with GDPR are a dying breed and DPOs (and those lucky enough to have a team) are rolling up the sleeves and getting on with it.

The challenge for the year ahead is to steady the ship and run an organised and structured approach to the Data Protection activities in the organisation.

We have been testing the Fort Privacy Maturity Model with organisations informally for the past 6 months and it really resonates. There's still a lot of work to do. We have come across very few organisations who are operating their business at the right level of maturity for each category considering the personal data they are processing.

The DPOs and Privacy Teams generally know this, but management is taking longer to take responsibility and provide the right resources and input. This can be frustrating and demoralising.

Using the Maturity Model Framework can help with delivering a structure and approach that management will listen to and understand. Management reporting and governance is a key part of GDPR compliance, and that message comes out very clearly in the use of the Maturity Model.

Apply the Fort Privacy Maturity Framework to your Data Protection Program now and, when the second birthday of the GDPR comes around, your organisation is sure to be in much better shape!

Coming soon!

Our next publication will provide further information about how we use the Maturity Model Framework in our audit services. We use a risk-based compliance tool "CalQrisk" to provide an automated audit process that not only assesses your current level of maturity and to tell you exactly what you need to do in order to get to the next level.

"Someone's sitting in the shade today because someone planted a tree a long time ago."

Warren Buffet

*For more information about the Fort Privacy Maturity Model **"Contact Us",** we would be happy to hear from you and answer any questions you might have.*

Cork - City Quarter, Lapp's Quay
Dublin - Regus, Ballsbridge

info@fortprivacy.ie
(0)21 730 4641
www.fortprivacy.ie

FORT PRIVACY
Getting Data Protection Right